

配置自适应安全设备(ASA)DHCP中继

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[数据包流](#)

[在ASA内部和外部接口上使用数据包捕获的DHCP中继](#)

[DHCP中继事务的调试和系统日志](#)

[配置](#)

[网络图](#)

[配置](#)

[使用CLI配置DHCP中继](#)

[DHCP 中继最终配置](#)

[DHCP 服务器配置](#)

[带有多个DHCP服务器的DHCP中继](#)

[使用多个DHCP服务器进行调试](#)

[使用多个DHCP服务器进行捕获](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍借助数据包捕获和调试在Cisco ASA上进行的DHCP中继，并提供配置示例。

先决条件

动态主机配置协议(DHCP)中继代理允许安全设备将DHCP请求从客户端转发到连接到不同接口的路由器或其他DHCP服务器。

以下限制仅适用于使用DHCP中继代理：

- 如果启用了DHCP服务器功能，则不能同时启用中继代理。
- 您必须直接连接到安全设备，并且不能通过其他中继代理或路由器发送请求。
- 对于多情景模式，不能在多个情景使用的接口上启用DHCP中继或配置DHCP中继服务器。

在透明防火墙模式下，DHCP中继服务不可用。透明防火墙模式的安全设备仅允许地址解析协议(ARP)流量通过。所有其他流量都要求使用访问控制列表(ACL)。为了允许在透明模式下通过安全设备进行DHCP请求和应答，必须配置两个ACL：

- 一个 ACL 允许从内部接口向外部发送 DHCP 请求.
- 一个 ACL 允许接收来自反方向的服务器的答复.

要求

Cisco建议您具备ASA CLI和Cisco IOS® CLI的基本知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 5500-x系列安全设备版本9.x或更高版本
- Cisco 1800 系列路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

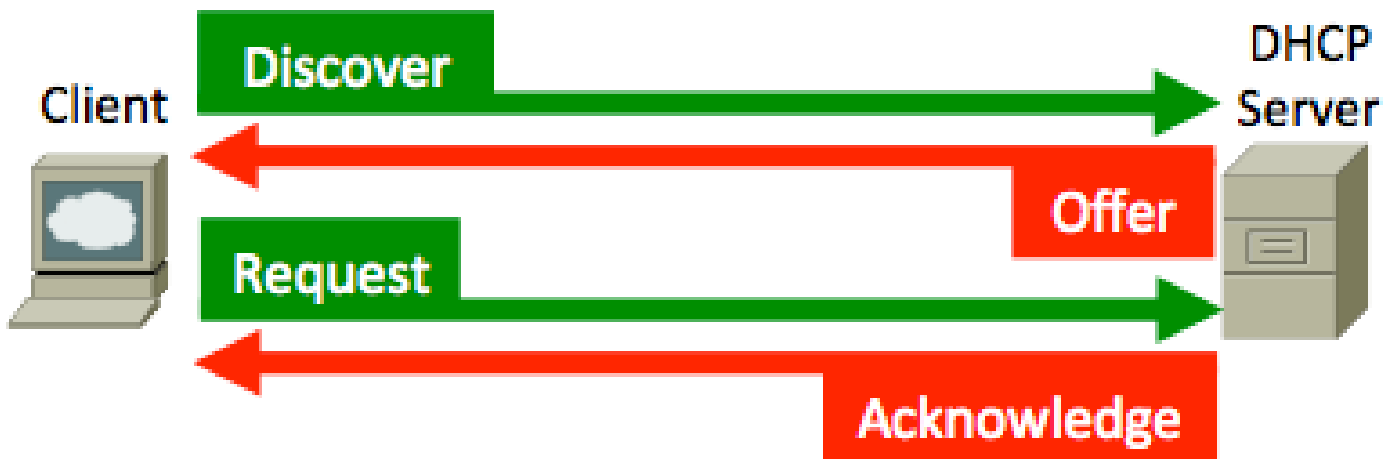
背景信息

DHCP协议为主机提供自动配置参数，例如带有子网掩码的IP地址、默认网关、DNS服务器地址和Windows Internet名称服务(WINS)地址。最初，DHCP 客户端没有其中的任何配置参数。为了获取此信息，他们发送广播请求获取此信息。当 DHCP 服务器看到此请求后，DHCP 服务器将提供必要信息。由于这些广播请求的特性，DHCP 客户端和服务器必须位于相同的子网上。默认情况下，第3层设备（如路由器和防火墙）通常不会转发这些广播请求。

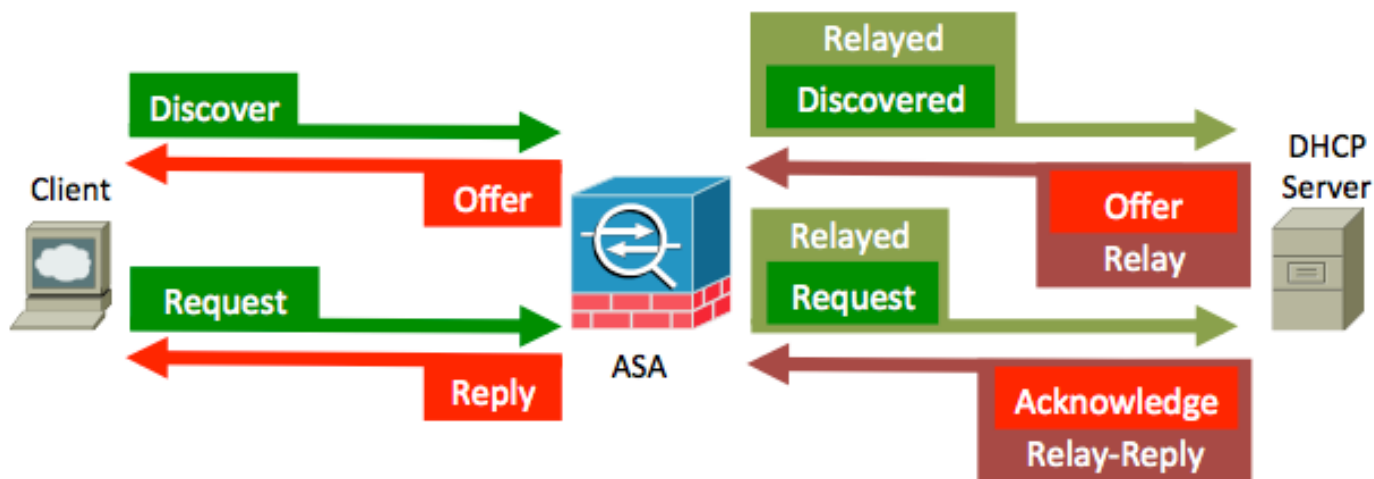
尝试在同一子网中查找DHCP客户端和DHCP服务器并不总是方便的。在这种情况下，可以使用DHCP 中继。当安全设备上的 DHCP 中继代理收到来自内部接口上的主机的 DHCP 请求时，它会将该请求转发至外部接口上的其中一个指定 DHCP 服务器。当 DHCP 服务器答复客户端时，安全设备会将该中继转发回来。因此，在与 DHCP 服务器的对话中，DHCP 中继代理充当了 DHCP 客户端的代理。

数据包流

下图说明未使用DHCP中继代理时的DHCP数据包流：



ASA拦截这些数据包并将其封装为DHCP中继格式：




在ASA内部和外部接口上使用数据包捕获的DHCP中继

记下以红色突出显示的内容，因为ASA就是这样修改各个字段的。

1. 要启动DHCP进程，请启动系统并向目标地址255.255.255.255 - UDP端口67发送广播消息 (DHCPDISCOVER)。


```

* 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
    Message type: Boot Request (1)
    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: 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
  Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  Option: (t=61,l=7) client identifier
  Option: (t=12,l=14) Host Name = 
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End Option
  Padding
  
```

 注：如果VPN客户端请求IP地址，则中继代理IP地址是通过dhcp-network-scope命令在group-policy下定义的第一个可用IP地址。

2. 通常，ASA会丢弃广播，但由于它被配置为充当DHCP中继，因此它会将DHCPDISCOVER消息作为单播数据包转发到DHCP服务器的IP源，该IP源来自面向服务器的接口IP。在本例中，它是外部接口IP地址。注意IP报头和中介代理字段的变化：

```
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
Ethernet II, Src: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7), Dst: Cisco_dd:48:c8 (00:19:e7:dd:48:c8)
Internet Protocol Version 4, Src: 198.51.100.1 (198.51.100.1), Dst: 198.51.100.2 (198.51.100.2)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 1
  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: 0.0.0.0 (0.0.0.0)
  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 Discover
  Option: (t=116,l=1) DHCP Auto-Configuration = AutoConfigure
  Option: (t=61,l=7) client identifier
  Option: (t=12,l=14) Host Name = 
  Option: (t=60,l=8) vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End Option
  Padding
```

 注：由于Cisco Bug ID [CSCuo8924](#)中引入的修复，版本9.1(5.7)、9.3(1)及更高版本的ASA可以将单播数据包转发到DHCP服务器的IP源，该源地址来自启用了dhcprelay的客户端(giaddr)的接口IP地址。在这种情况下，它可以是内部接口IP地址。

3. 服务器将DHCP OFFER消息作为单播数据包发回ASA，发往在DHCPDISCOVER - UDP端口67中设置的中继代理IP。在本例中，它是内部接口(giaddr)的IP地址，在该接口上启用了dhcprelay。注意第3层报头中的目标IP：

```

④ Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
④ Ethernet II, Src: Cisco_dd:48:c8 (00:19:e7:dd:48:c8), Dst: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7)
④ Internet Protocol Version 4, Src: 198.51.100.2 (198.51.100.2), Dst: 192.0.2.1 (192.0.2.1)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
④ Bootstrap Protocol
    Src: DHCP server
    Dst: Relay agent IP
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x79dbf3a7
    Seconds elapsed: 0
④ 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) Offered IP
    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
④ Option: (t=53,l=1) DHCP Message Type = DHCP Offer
    DHCP offer
④ Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
    DHCP server IP
④ Option: (t=51,l=4) IP Address Lease Time = 1 day
    Lease
④ Option: (t=58,l=4) Renewal Time Value = 12 hours
④ Option: (t=59,l=4) Rebinding Time Value = 21 hours
④ Option: (t=1,l=4) Subnet Mask = 255.255.255.0
    Subnet mask info
④ Option: (t=6,l=8) Domain Name Server
④ Option: (t=15,l=9) Domain Name = "cisco.com"
    Domain name
    End option
    Padding

```

4. ASA将此数据包从内部接口 (UDP端口68) 发送出去。注意 , 当数据包离开内部接口时 , IP报头会发生变化 :


```

④ Frame 2: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits)
④ Ethernet II, Src: Cisco_6c:b8:c6 (58:8d:09:6c:b8:c6), Dst: Vmware_84:39:6a (00:50:56:84:39:6a)
④ Internet Protocol Version 4, Src: 192.0.2.1 (192.0.2.1), Dst: 192.0.2.4 (192.0.2.4)
④ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
④ Bootstrap Protocol
    Src: ASA interface/Relay agent IP
    Dst: Offered IP
    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) Offered IP
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 192.0.2.1 (192.0.2.1) ASA interface IP
    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 DHCP Offer
    Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2 DHCP server IP
    Option: (t=51,l=4) IP Address Lease Time = 1 day Lease
    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 Subnet mask info
    Option: (t=6,l=8) Domain Name Server
    Option: (t=15,l=9) Domain Name = "cisco.com" Domain name
    Option: (t=3,l=4) Router = 192.0.2.1 Default Gateway for client
    End option
    Padding

```

5. 收到DHCP OFFER消息后，请发送DHCP REQUEST消息以指示您接受该提议。

```

④ Frame 3: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
④ Ethernet II, Src: Vmware_84:39:6a (00:50:56:84:39:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
④ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
④ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
④ Bootstrap Protocol
    Src: 0.0.0.0 as client hasn't
    Dst: L3 broadcast
    Message type: Boot Request (1)
    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: 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 Request DHCP request
    Option: (t=61,l=7) Client identifier
    Option: (t=50,l=4) Requested IP Address = 192.0.2.4 Requested IP
    Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2 DHCP server IP
    Option: (t=12,l=14) Host Name = ████████████████████ Hostname
    Option: (t=81,l=18) Client Fully Qualified Domain Name
    Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
    Option: (t=55,l=11) Parameter Request List
    End option

```

6. ASA将DHCPREQUEST传递到DHCP服务器。

```
Frame 3: 366 bytes on wire (2928 bits), 366 bytes captured (2928 bits)
Ethernet II, Src: Cisco_6c:b8:c7 (58:8d:09:6c:b8:c7), Dst: Cisco_dd:48:c8 (00:19:e7:dd:48:c8)
Internet Protocol Version 4, Src: 198.51.100.1 (198.51.100.1), Dst: 198.51.100.2 (198.51.100.2)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootps (67)
Bootstrap Protocol
  Message type: Boot Request (1)
  Hardware type: Ethernet
  Hardware address length: 6
  Hops: 1
  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: 0.0.0.0 (0.0.0.0)
  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 Request
  Option: (t=61,l=7) Client identifier
  Option: (t=50,l=4) Requested IP Address = 192.0.2.4
  Option: (t=54,l=4) DHCP Server Identifier = 198.51.100.2
  Option: (t=12,l=14) Host Name = 
  Option: (t=81,l=18) Client Fully Qualified Domain Name
  Option: (t=60,l=8) Vendor class identifier = "MSFT 5.0"
  Option: (t=55,l=11) Parameter Request List
  End option
```

Src: ASA outside interface
Dst: DHCP server

DHCP request
Requested IP
DHCP server IP
Hostname

7. 服务器获得DHCPREQUEST后，会将DHCPACK发送回，以确认提供的IP。

```

⊕ Frame 4: 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
    Src: DHCP server
    Dst: Relay agent IP
    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 ACK
⊕ 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

```

Current IP on client
IP offered to client

DHCP Ack
DHCP server IP
Lease

Subnet mask info

Domain name
Default gateway for client

8. ASA将DHCPACK从DHCP服务器传递给您，从而完成事务。

```

⊕ Frame 4: 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
    Src: Relay agent IP/ASA int
    Dst: IP offered to client
    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 ACK
⊕ 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

```

Current IP on client
IP offered to client

DHCP Ack
DHCP server IP
Lease

Subnet mask info

Domain name
Default gateway for client

DHCP中继事务的调试和系统日志

这是转发到DHCP服务器接口198.51.100.2的DHCP请求：

```
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
```

从DHCP服务器收到应答后，安全设备会将其转发到MAC地址为0050.5684.396a的DHCP客户端，并将网关地址更改为自己的内部接口。

```
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.
```

系统日志中也显示相同的事务：

```
%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)

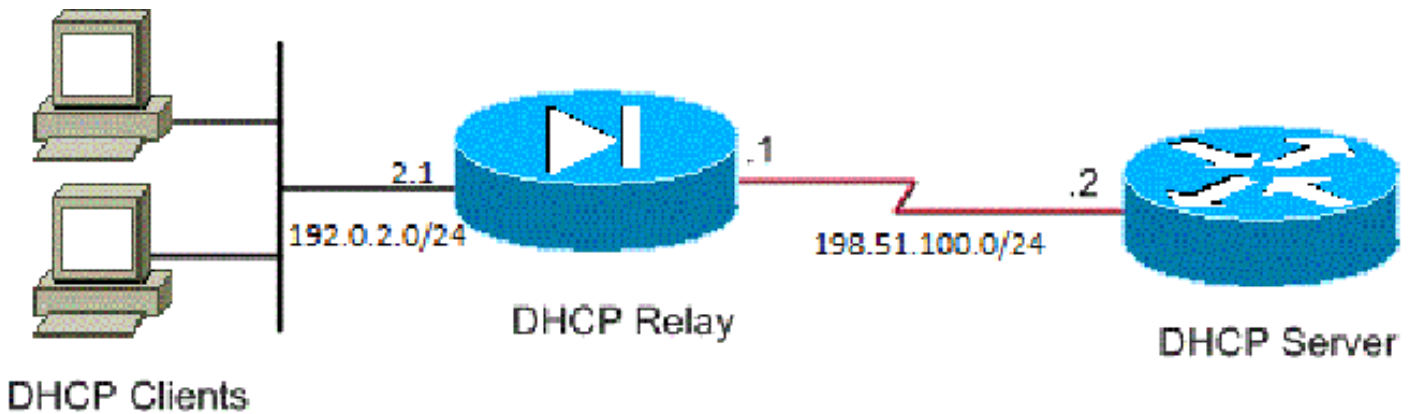
%ASA-7-609001: Built local-host inside:192.0.2.4
%ASA-6-302020: Built outbound ICMP connection for
  faddr 192.0.2.4/0 gaddr 198.51.100.2/1 laddr 198.51.100.2/1
%ASA-7-609001: Built local-host identity:192.0.2.1
%ASA-6-302015: Built inbound UDP connection 16 for outside:
  198.51.100.2/67 (198.51.100.2/67)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

配置

本部分提供用于配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 使用CLI配置DHCP中继
- DHCP 中继最终配置
- DHCP 服务器配置

使用CLI配置DHCP中继

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

DHCP 中继最终配置

```
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 服务器配置

```
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 CISC01811W-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

```

带有多个DHCP服务器的DHCP中继

最多可以定义十个DHCP服务器。当客户端发送DHCP Discover数据包时，该数据包将转发到所有DHCP服务器。

例如：

```

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

```

使用多个DHCP服务器进行调试

以下是使用多个DHCP服务器时的一些调试示例：

```
DHCP: Received a BOOTREQUEST from interface 2 (size = 300)
DHCPR: relay binding found for client 000c.291c.34b5.
DHCPR: 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.
```

使用多个DHCP服务器进行捕获

以下是使用多个DHCP服务器时数据包捕获的示例：

```
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
```

验证

使用本部分可确认配置能否正常运行。

要查看有关DHCP中继服务的统计信息，请在ASA CLI上输入show dhcprelay statistics命令：

```
ASA# show dhcprelay statistics
```

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

```
Packets Relayed
```

```
BOOTREQUEST          0
DHCPDISCOVER         1
DHCYPREQUEST         1
DHCPCDECLINE         0
DHCPCRELEASE         0
DHCPCINFORM          0

BOOTREPLY            0
DHCPCOFFER           1
DHCPCACK             1
DHCPCNAK             0
```

此输出提供有关多种DHCP消息类型的信息，例如DHCPDISCOVER、DHCP REQUEST、DHCP OFFER、DHCP RELEASE和DHCP ACK。

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

故障排除

本部分提供了可用于对配置进行故障排除的信息。

```
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
DHCPRREQUEST        1
DHCPDECLINE         0
DHCPRELEASE         0
DHCPINFORM          0

Message               Sent
BOOTREPLY           0
DHCPPOFFER         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
```

您还可以使用以下debug命令：

- debug dhcprelay packet
- debug dhcprelay event
- 捕获
- 系统日志



注意：使用[debug命令之前](#)，请参阅有关Debug命令的重要信息。

相关信息

- [在ASA上捕获](#)

- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。