

# ASA DHCP Proxy Behavior with Backup DHCP Server List

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Diagram](#)

[Previous Behavior](#)

[New Behavior](#)

[DHCP Proxy Client States](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes the new Adaptive Security Appliance (ASA) behavior acting as a DHCP Proxy Client with multiple DHCP servers.

## Prerequisites

### Requirements

There are no specific requirements for this document.

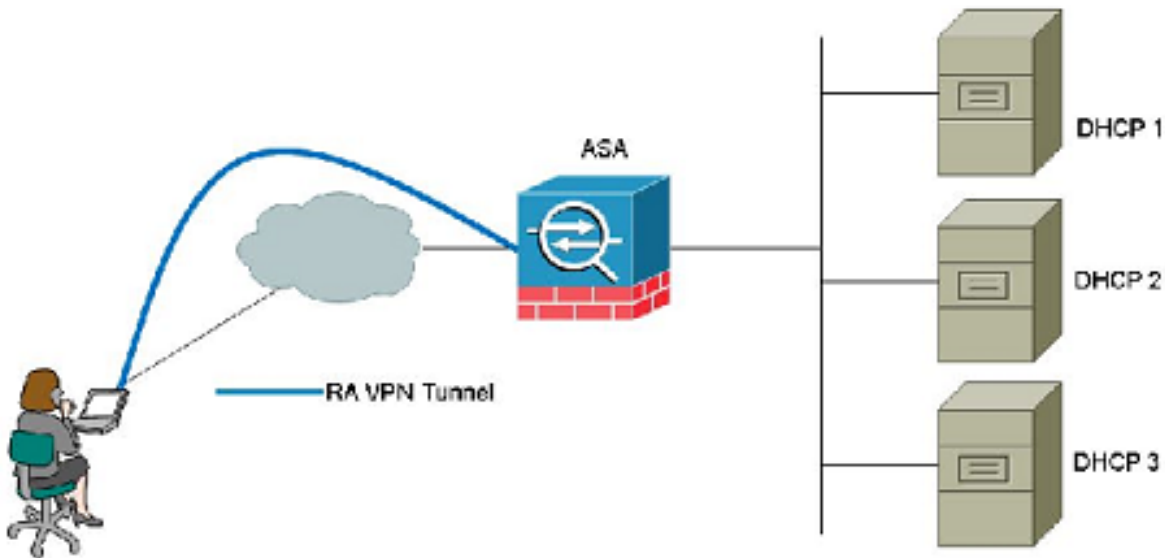
### Components Used

The information in this document is based on these software and hardware versions:

- Cisco ASA 5500-X Series
- Behavior-change introduced in 9.2(1) and 9.1(4)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Diagram



## Previous Behavior

Here is an example of the old design of the DHCP functionality when ASA acted as a proxy client in an HA setup of DHCP servers:

DHCP address assigned for VPN clients used a **backup server model - server list**.

- When a VPN client connected, the ASA tried each DHCP server serially until it received a lease or it had depleted the list.
- When it was time to renew, it attempted to renew to the server of record. If the DHCP renew phase failed, it moved to the DHCP rebind phase. Since the ASA is using a backup algorithm, you only attempted to rebind with the same failed server.

## New Behavior

With the Enhancement CSCuc04072, Cisco changed the algorithm to an **HA server model - server group**.

When a client connects:

- ASA sends **Discovers** to all servers in the group.
- ASA selects the first offer received and drops the other offers.
- When an address needs to be renewed, it attempts to renew with the lease server (server from which the address was acquired).

- If the DHCP renew fails after a certain number of retries, state machine moves to the DHCP rebind phase after predefined period.
- During the rebind phase, the ASA will send requests to all the servers in the group in parallel. In an HA environment, lease information is shared, so other servers can ACK the lease and the ASA will go back to the bound state.

**Note:** During the rebind phase, if there is no response from any of the servers in the servers list, then the ASA will move to purge state and after that, remove the rules added to the interface from which the servers were reachable.

## DHCP Proxy Client States

- **DHCP discover:** In this state the ASA sends discover packets to the servers in the server list under tunnel group (server refers to servers in the server list under tunnel-group) that have a route and have a client enabled on the interface through which the server is reachable. The servers which do not have a route and do not have client enabled are not sent a discover packet.
- **DHCP offer:** The servers send an offer. The ASA selects the offer based on a first come, first serve basis.
- **DHCP request:** The ASA generates a packet which includes the server address from which the address is selected and sends this packet to the servers (route available and client enabled). This packet helps the other servers identify that an address is selected from the server specified in the packet and acts as NAK to other servers.
- **DHCP bound:** The ASA comes to this state if an ACK is received from the server requested [the server in DHCP request state].
- **DHCP renew:** Renew occurs when half of the lease time is passed. During this state, the ASA sends a request to the lease server (the server which provided the address to the client). If for some reason the lease server is down, then the ASA retries four times to the lease server. If the server is still not reachable or not responding, then the ASA moves to rebind state.
- **DHCP rebind:** Rebind occurs when  $7/8^{\text{th}}$  of the lease time is passed. During the rebind state all the servers (route-available and client-enabled) in the list are sent a request. If the lease server is down at this state, then the server in lease syncs with the lease server (HA setup of the servers where the leases are synced between the servers) will provide the lease to the client.

## Verify

To view the lease details, use the enhanced **show** command and filter the view for proxy and server.

The previous CLI was:

```
show ip address <interface> dhcp lease
```

and it was enhanced to

```
show ip address <interface> dhcp lease [proxy/server] [summary]
```

The syntax is here:

```
show ip address <interface> dhcp lease [proxy/server] [summary]
```

exec mode commands/options:

**proxy** Show proxy entries in IPL table

**server** Show server entries in the IPL table

**summary** Show summary for the entry

| Output modifiers

## Troubleshoot

**Note:** Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

```
debug dhcpc detail 255
```

```
debug dhcpc error 255
```

```
debug dhcpc packet 255
```