

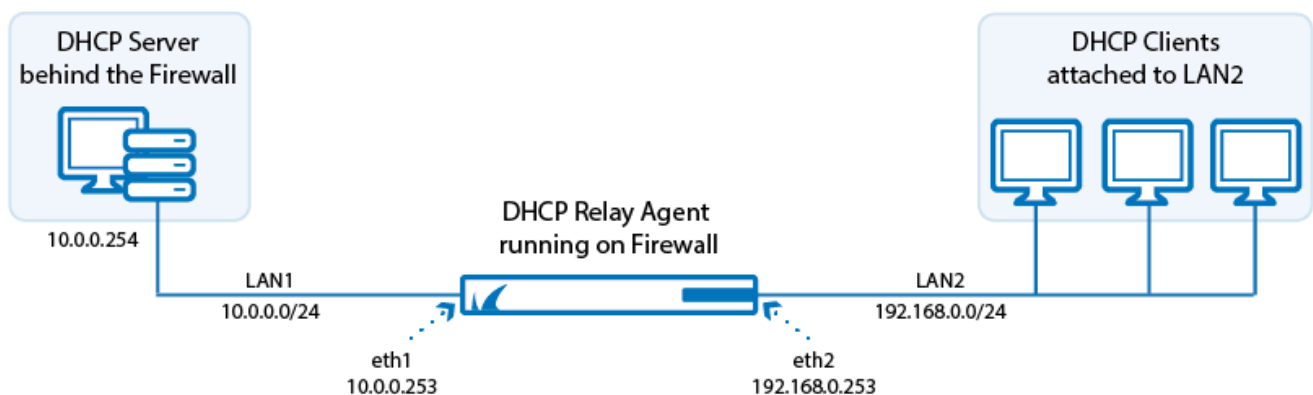
How to Configure the DHCP Relay Agent

<https://campus.barracuda.com/doc/53248945/>

The DHCP relay service allows you to pass DHCP broadcast messages to network segments that a client computer is not directly attached to. DHCP relaying can be used to share a single DHCP server across logical network segments that are separated by a firewall. The DHCP relay service does not handle IP addresses. It sends unicast messages instead of broadcast messages.

A client in need of a DHCP-assigned IP address sends its request as a broadcast message to the network attached to the corresponding interface. The DHCP relay service on the firewall receives the request on an interface attached to the same network, e.g., eth2, 192.168.0.0/24. The DHCP relay service sends a unicast request to all configured DHCP servers in the LAN and receives a DHCP IP address offer from a DHCP server (e.g., 10.0.0.254) that has an IP address range configured for the network segment of the requesting client (e.g., 192.168.0.0/24). This offer is forwarded to the requesting client. If the client accepts the offer, the DHCP address is acknowledged by the client and immediately assigned to its attached interface.

DHCP Relay Agent Between Two LANs:



Before You Begin

If you are using both a DHCP and a DHCP relay service on the same firewall, verify that both services are not using the same interface.

Configure the DHCP Relay Agent for IPv4

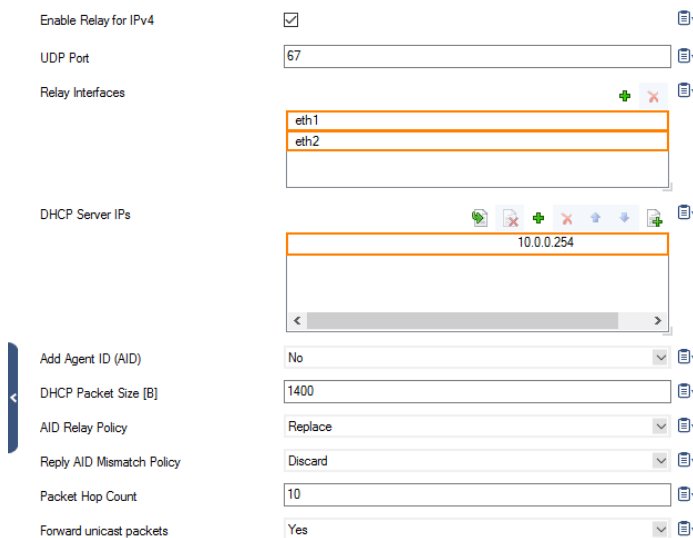
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual**

server > Assigned Services > DHCP-Relay.

2. Click **Lock**.
3. Select **Enable Relay for IPv4**.
4. Enter the **UDP Port** the relay agent is listening on (default: 67).
5. In the **Relay Interfaces** section, click **+** and add the network interfaces that are used by the DHCP relay agent to connect to the DHCP server and client networks.

If you must configure multiple relay agents in a cascaded environment, do not specify the server-side interface of the cascaded ('border') relay agent. For more information, read the following section.

6. In the **DHCP Server IPs** field, enter the IP addresses of the DHCP servers.



7. Enable **Add Agent ID (AID)** if you want the DHCP relay agent to add an Agent ID (AID) to the transmitted packets. An AID indicates that the data has been relayed.
8. Enter the maximum **DHCP Packet Size** in bytes (default: 1400).
9. From the **AID Relay Policy** list, select how your DHCP relay agent handles DHCP packets that are already flagged by an AID from another agent:
 - o **Append** (default) – Attaches your AID to the existing AID.
 - o **Replace** – Replaces the existing AID with your AID.
 - o **Forward** – Passes DHCP packets without any modification.
 - o **Discard** – Discards DHCP packets that are already flagged by an AID.
10. From the **Reply AID Mismatch Policy** list, select how your DHCP relay agent handles DHCP server replies that do not contain its AID:
 - o **Discard** – Default. Discards the DHCP packet.
 - o **Forward** – Forwards the DHCP packet to the DHCP client.

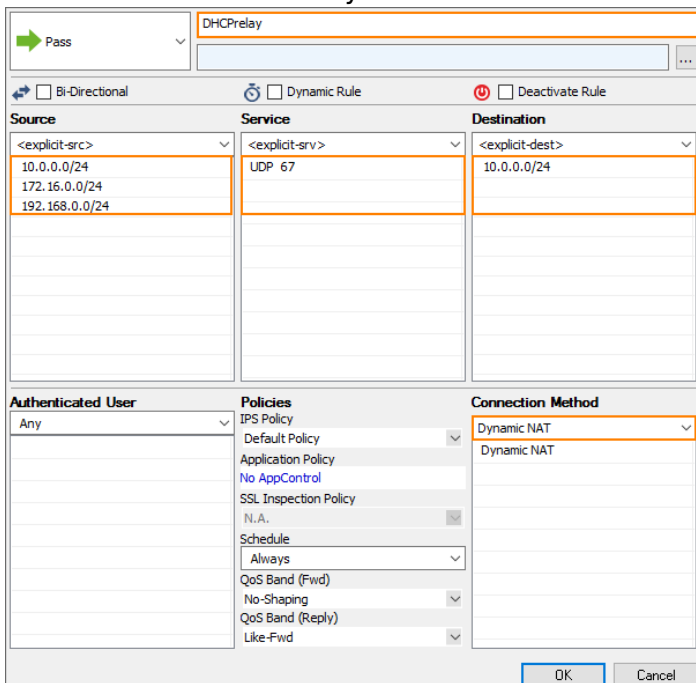
The **Reply AID Mismatch Policy** setting is important when multiple relay agents serve the DHCP server.

11. Specify the maximum **Packet Hop Count** to avoid infinite packet loops (default: 10).
12. Select **Forward unicast packets** if Bootstrap/BOOTP unicast messages should be forwarded by the DHCP relay.
13. Click **OK**.
14. Click **Send Changes** and **Activate**.

Create an Access Rule to Allow DHCP Requests

The relay agent must forward the request from the client to the DHCP server.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
4. Select **Pass** as the action.
5. Enter a **name** for the rule. For example, DHCPrequest.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
 - **Source** – The network address of the segment where the client is attached to, e.g., 192.168.0.0/24.
 - **Destination** – The network address of the segment where the DHCP server is attached to, e.g., 10.0.0.0/24.
 - **Service** – Either configure an explicit service for **UDP** and port **67** to let DHCP requests pass, or create a service object. For more information, see [How to Create Service Objects](#).
7. **Connection Method** – Dynamic NAT.



The screenshot shows the configuration window for a new access rule named "DHCPRelay". The action is set to "Pass". The rule is configured with the following settings:

- Source:** 10.0.0.0/24, 172.16.0.0/24, 192.168.0.0/24
- Service:** UDP 67
- Destination:** 10.0.0.0/24
- Connection Method:** Dynamic NAT

Other settings include: Bi-Directional (unchecked), Dynamic Rule (checked), Deactivate Rule (unchecked), Authenticated User (Any), Policies (IPS Policy, Default Policy, Application Policy, No AppControl, SSL Inspection Policy, N.A., Schedule: Always, QoS Band (Fwd): No-Shaping, QoS Band (Reply): Like-Fwd), and Connection Method (Dynamic NAT). The OK and Cancel buttons are visible at the bottom.

8. Click **OK**.
9. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
10. Click **Send Changes** and **Activate**.

The DHCP Server Must Be Able to Reach the Client Network

The DHCP server must return DHCP offers to the requesting client.

- (option #1) In case your DHCP server runs on a dedicated Barracuda firewall, create a gateway route to the client network. For more information, see [How to Configure Gateway Routes](#).
- (option #2) On any other appliance, configure the DHCP server to be able to reach the client network.

Configure the DHCP Relay Agent for IPv6

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > DHCP-Relay > DHCP-Relay Settings**.
2. Click **Lock**.
3. Select **Enable Relay for IPv6**
4. Enter the **UDP Port** the relay agent is listening on (default: 547).
5. Specify the maximum **Packet Hop Count** to avoid infinite packet loops (default: 10).
6. Select **Interface ID** to force the use of the DHCPv6 Interface-ID option. This option is automatically sent when there are two or more downstream interfaces in use, in order to disambiguate between them.
7. In the **Lower Network Interfaces** list, specify the network interface and link address on which queries will be received from clients or other relay agents. If no link address is specified, the first non-link local address is used.
8. In the **Upper Network Interfaces** list, specify the network interface and destination unicast or multicast address to which queries will be forwarded. If no destination address is specified, requests are forwarded to the `FF02::1:2` multicast address (All_DHCP_Relay_Agents_and_Servers)
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Figures

1. dhcp_relay1.png
2. dhcp_relay_config.png
3. access_rule_for_dhcp_relay_01.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.