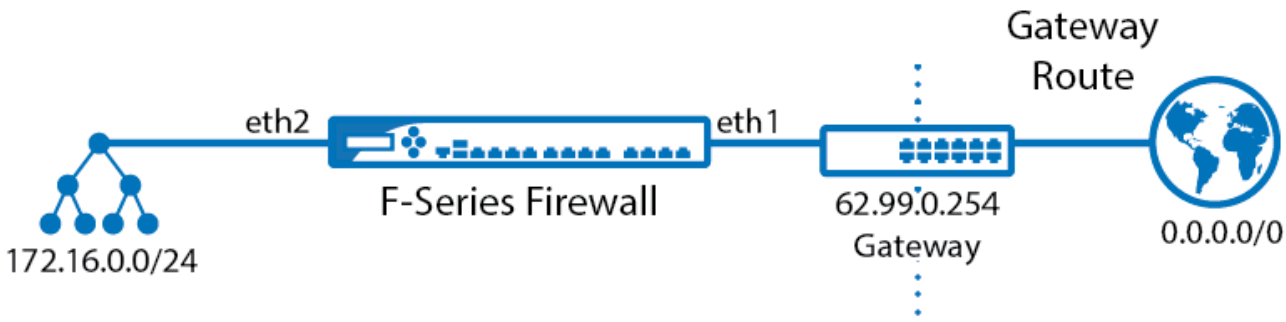
Routing

https://campus.barracuda.com/doc/46208934/

Routing tables are used to store the best path to a remote network. The Barracuda NextGen Firewall F-Series uses the routing tables to forward traffic to the correct interfaces, next hop gateways, or VPN tunnels. Routes are first evaluated by destination, route metric (preference) and. optionally, source address of an IP packet and then by the scope (network size) to determine which routes matches. Two routes of the same scope (e.g., /24) and metric can not be created. The Management IP address always uses a preference of 0.

- If two routes with different preferences exist, the route with the lower preference is chosen. E.g., 10.0.10.0/25 (preference 10) is preferred over 10.0.10.0/25 (preference 100)
- If two routes with the same preference exist to a destination the route with the smaller subnet mask is used. E.g., 10.0.10.0/24 is preferred over 10.0.0.0/16
- VPN routes are source-based routes by default. If **single routing table** is enabled in the VPN Settings, VPN routes are inserted with a preference of 10. For more information, see Authentication, Encryption, Transport, and VPN Routing.



Directly Attached Network Routes (Direct Routing)

Define how to reach networks that are directly plugged in to a port (virtual or physical) of the Barracuda NextGen Firewall F-Series. To define a directly attached network route, you must enter:

- **Target network in CIDR Format** – E.g., `172.16.0.0/24`
- **Interface** – The network interface on the Barracuda NextGen Firewall F-Series the network is attached to. E.g., `eth2` or `port 2`

After you have introduced the directly attached route and activated the network, the route is in a pending state. Pending routes are marked with the icon in **CONTROL > Network** and are not

active. When an suitable source network address (virtual server IP or additional IP address on box level) has been introduced, the route becomes active and the icon is displayed for the route.

In the example above, you must create a direct route for the ISP issued 62.99.0.0/24. To reach the Internet, a gateway route (see below) must be created. If you enter the optional **gateway IP** address when creating the direct attached route, the default gateway route is created automatically.

You do not need to create a directly attached route for the network the management IP address is in. This route is created automatically when the management IP address is configured.

For setup instructions, see How to Configure Direct Routes.

Gateway Routes (Next Hop Routing)

To reach networks that cannot be directly accessed, you must define gateway routes. A common gateway route is the default route (0.0.0.0/0), which will forward all packets not belonging to one of the trusted networks to the remote gateway provided by the ISP. Before adding a gateway route, a direct route must be configured. Otherwise, you cannot contact the next hop IP address. To define a gateway route, you must enter:

- **Target network** – Target network in CIDR format. E.g., 0.0.0.0/0 for the default route
- **Next hop address** – IP Address of the gateway device the traffic is sent to. E.g., 62.99.0.254

After adding the gateway route, you must initiate a **Soft** network activation for the route to become active (in **CONTROL > Network**)

For setup instructions, see How to Configure Gateway Routes.

Multipath Routing

The Barracuda NextGen Firewall F-Series supports standard Linux multipath routing and Firewall-assisted multipath routing. Standard Linux multipath routing balances does not offer dead next hop detection or session packet balancing. Simple redundancy by next hop detection can be provided by adding multiple routing entries with different route preference numbers. Firewall-assisted multipath routing supports per packet balancing between next hops and dead next peer detection and is configured in the Forwarding Firewall service.

For setup instructions, see:

- How to Create a Custom Connection Object.
- How to Configure Linux Standard Multipath Routing

Source-Based Routes (Policy Based Routing)

Source-based or policy routing is a way to implement more complex routing scenarios. The implementation provided by the Barracuda NextGen Firewall F-Series only uses a subset of the functional scope of policy routing. The source address used to establish a connection determines whether or not a routing table is consulted.

Because the firewall configuration (on a per rule basis) lets you specify the address with which an allowed connection is established, policy routing represents an extremely powerful instrument to manage routing on the NextGen Firewall F-Series in complex topologies. VPN tunnels make use of policy routing.

Policy routing rules assign an IP address range (source addresses) to a named routing table. These rules are organized in an ordered list, so that each rule is associated with a preference number. Routing decisions are made by evaluating the ruleset starting with lowest preference number rule. The first ruleset (route table) that matches the source IP address is chosen. If a matching route to the desired destination address is found in the table, the route is applied. Otherwise, the Barracuda NextGen Firewall F-Series continues to evaluate the routing tables (rules) until a match is found. If none of the rules match, the destination is unreachable.

For setup instructions, see How to Configure Source-Based Routes.

Figures

1. Routing_Overview.png
2. route_pending.png
3. route_active.png
4. route_active.png