Network Page

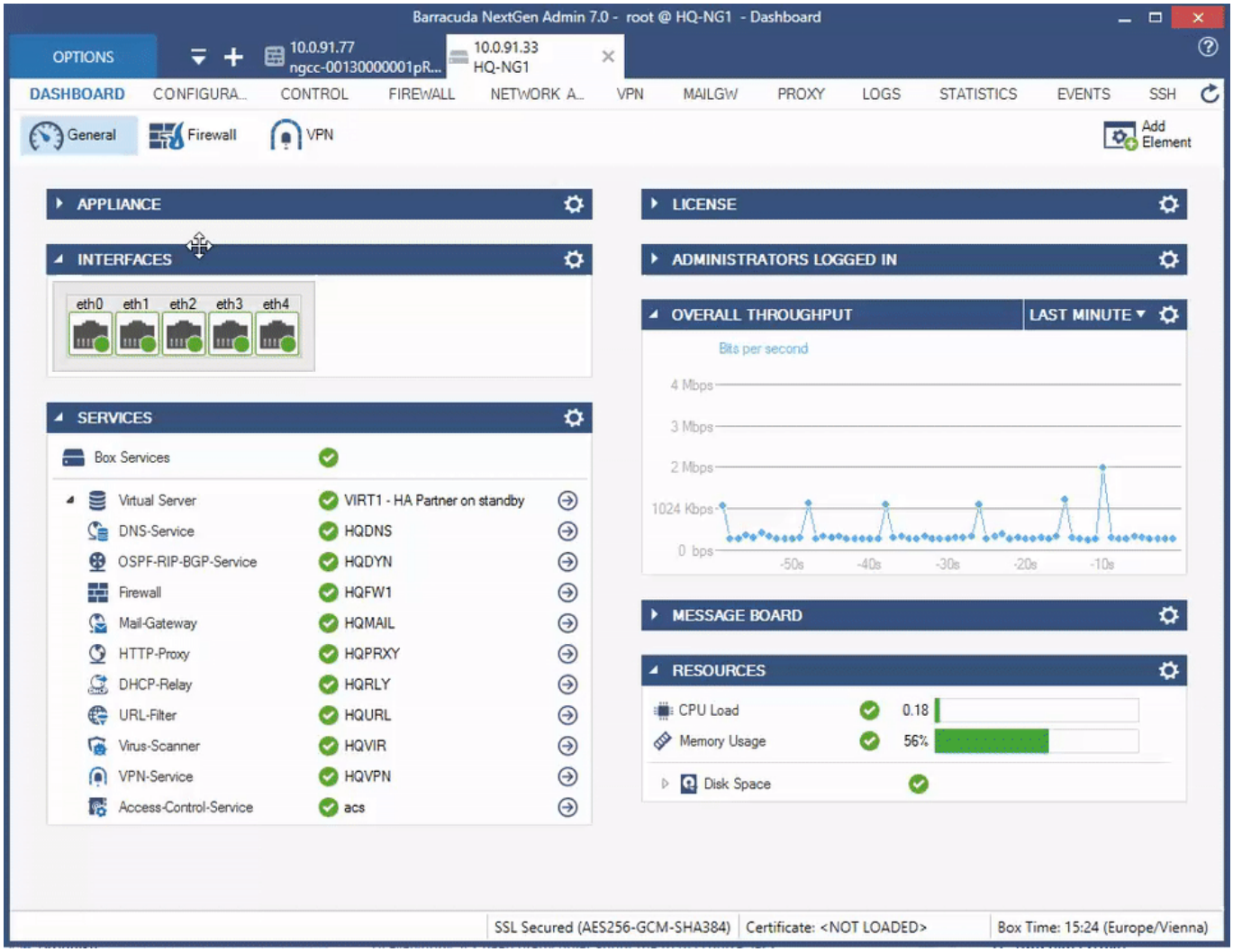
https://campus.barracuda.com/doc/48202881/

The **Network** page lets you monitor the current status of the network subsystem. To access the **Network** page, open the **CONTROL** tab on the Barracuda NextGen Firewall F-Series, and click the **Network** icon in the ribbon bar.

Information display

The network information display is divided into two tables:

- The top table displays information about configured network interfaces, network addresses, and routes. To view this information, click the tabs that are below the table.
- The bottom table displays information about the routing tables.



Interface/IPs tab

To view information on network interfaces and the IP addresses that are assigned to them, click the **Interfaces/IP** tab. In the top table, information about each interface is organized into the following columns:

- **Interface/IP** – The network interface names and their assigned IP addresses. For Ethernet network adapters, additional information on speed and duplex settings are also displayed. To expand and collapse the list of IP addresses with corresponding netmasks (inverted CIDR notation), double-click the interface name. The network interface type and network connection status are indicated by the following icons:

Network Interface Type Icons

Icon	Description
	Ethernet network adapter.
	Loopback Interface.
	◦ Barracuda Netwokrs queuing interface (used for traffic shaping). ◦ DHCP interface, used for xDSL/DHCP connections. ◦ gre0, used for IP-to-IP tunnelling.
	Tap interface (internal interface for SYN proxying & VPN.
	Tunnel Interface.

Network Connection Status Icons

Icon	Description
	Up.
	Not enabled.
	WWAN signal strength: no connection.
	WWAN signal strength: RSSI value below 10.
	WWAN signal strength: RSSI value from 21 to 31.
	Down or duplicate.

- **Label** – A label is available for every interface that is 'up' (green icon). Multiple predefined labels are available, such as:
  - **mip0** – for the primary administrative network of the box.
  - **loop** – for the loopback interface 127.0.0.1/24.
  - **fw** – for network 127.0.1.1/24 on interface tap0.
  - **vpn** – for network 127.0.2.1/24 on interface tap1.
  - **vpnpers** – for network 127.0.3.1/24 on interface tap3.

  IP addresses associated with server processes are labeled according to the name of the server. Additional networks are named according to the label name in the network in the configuration file/dialog.
- **Ping** – This column indicates whether the corresponding IP address is configured to reply to pings (**ok**) or not (**NO**).
- **MAC of duplicate IP** – If an IP address is used twice, the MAC address of the other interface is displayed in this column.
- **Info** – Contains additional information, if applicable.

IPs tab

To monitor your networks, click the **IPs** tab. A list of your network addresses is displayed in the top table. Information about each network address is organized into the following columns:

- **IP** – The network address.
- **State** – The status of the network.
- **Interface** – The interface that the network is assigned to. The interface name is displayed, followed by a colon and the interface label. E.g., eth0:mip0
- **Ping** – This column indicates whether the corresponding IP address is configured to reply to pings (**ok**) or not (**NO**).
- **MAC of duplicate IP** – If an IP address is used twice, the MAC address of the other interface is displayed in this column.

Interfaces tab

To view the settings for your network interfaces, click the **Interfaces** tab. A list of your interfaces is displayed in the top table. Information about each interface is organized in the following columns:

- **Interface** – The interface name.
- **MAC** – The unique MAC address for the interface.
- **Link** – Indicates if the interface is physically connected or not.
- **Speed** – For adapters, the maximum transfer rate in Mbit/s.
- **Duplex** – The duplex settings of the NIC (Half or Full).
- **Neg.** – Indicates if auto-negotiation is on or off.
- **MTU** – The Maximum Transmission Unit (MTU) of the NIC.
- **Bytes** – The byte throughput, which is calculated by the average number of bytes/s (obtained from a 10-second sampling interval) passing through the interface.
- **Packets** – The packet throughput, which is calculated by the average number of packets/s (obtained from a 10-second sampling interval) passing through the interface.
- **Errors** – The total number of errors, which is calculated by the average number of all errors on the interface (obtained from a 10-second sampling interval).
- **Realm** – The Trust Level.
- **Flags** – The following entries are possible:
  - **UP** – Interface is up.
  - **BROADCAST** – Broadcast active.
  - **LOOPBACK** – Loopback active.
  - **NOARP –** ARP requests will not be responded.
  - **POINT-TO-POINT** – Used for PPTP.
  - **PROMISC** – Accepts every packet, regardless of whether the MAC address matches.
- **Features** – The following entries are possible:

    - **SGI/O 0** – Scather gather Input/Output (DMA).
    - **NOCSUM** – No checksum required.
    - **HWCSUM** – Interface is capable of hardware checksum.
    - **IPCSUM** – Interface is capable of checksum for IP packets.
    - **HW-VLAN-TX** – Interface is capable of VLAN tagging transmits.
    - **HW-VLAN-RX** – Interface is capable of VLAN tagging receives.
    - **HIGH-DMA** – I/O memory above 64 K.
    - **DYNALLOC** – Used for virtual interfaces.
- **IRQ** – The IRQ number (ReQuest line) for each interface.
- **Base-Addr** – The I/O port address.
- **Switch** – The switch, if configured.

Proxy ARPs tab

Proxy ARPs are additional IP addresses/netmasks that the firewall responds to. To view the list of proxy ARPs, click the **Proxy ARPs** tab. In the top table, information about each proxy ARP is organized into the following columns:

- **IP/Mask** – The IP addresses/netmasks.
- **Interface** – The interface where the IP address/netmask resides.
- **Origin** – The origin of the proxy ARP (by whom it is created).
- **Exclude** – The networks that are excluded from proxy APR creation.
- **Source Restriction** – The network addresses to which the proxy ARP request has been limited.

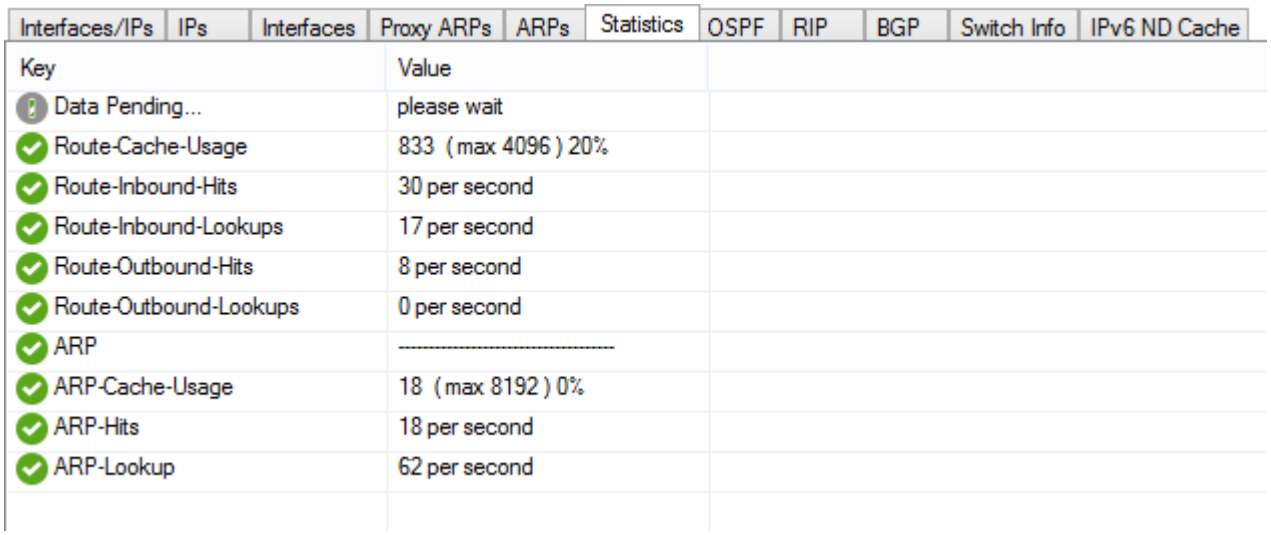
ARPs tab

The Address Resolution Protocol (ARP) is needed for translating an IP address into a physical address. To view the list of ARP requests, click the **ARPs** tab. In the top table, information about each ARP is organized into the following columns:

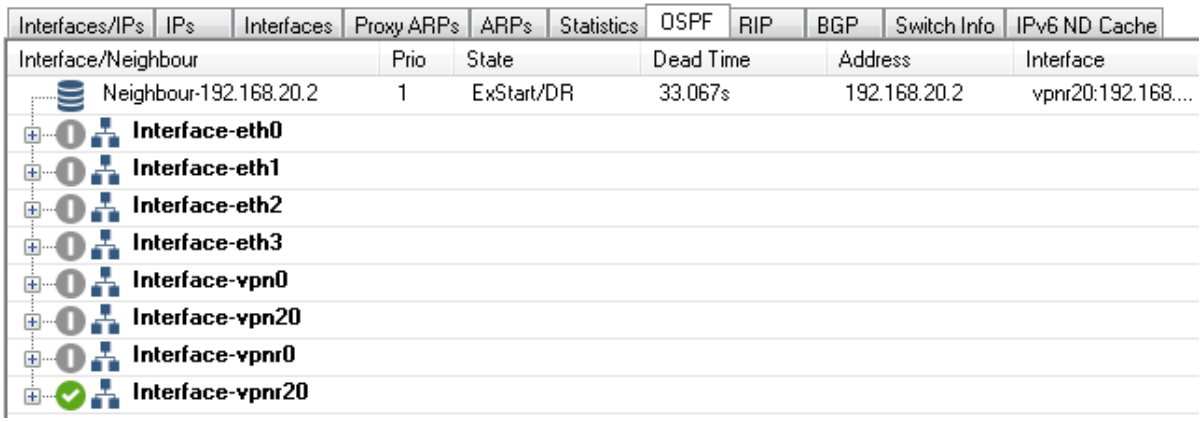
- **IP** – The IP addresses that were used.
- **MAC** – The MAC address of each assigned IP address.
- **Vendor** – The manufacturer of the network interface.
- **Interface** – The interface.
- **Switch**
- **VLAN**
- **Port**
- **Uplinks**

Statistics tab

Shows statistics about the routing and ARP cache utilization of the firewall. This information can be useful when optimizing the size of the routing and ARP cache. For more information, see How to Configure Advanced Barracuda OS System Settings



OSPF, RIP, and BGP tabs



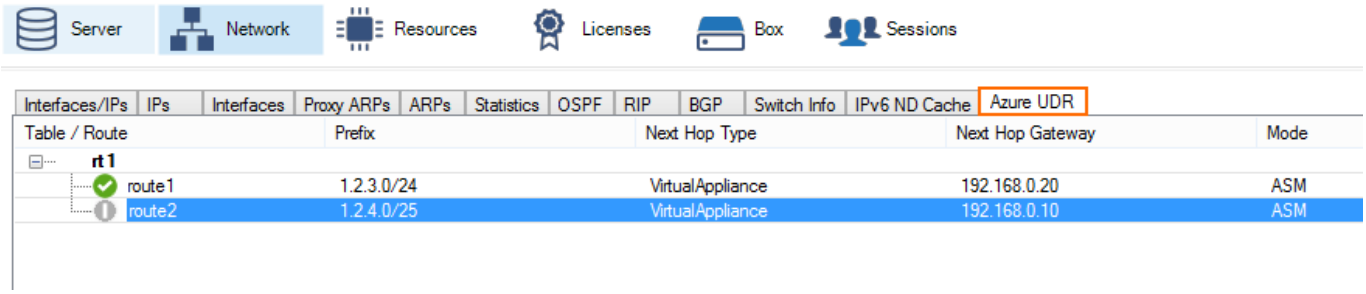
If you configured the OSPF, RIP, or BGP service on your system, click the **OSPF**, **RIP**, or **BGP** tab to view information about the neighbors and interfaces.

For more information, see Dynamic Routing Protocols (OSPF/RIP/BGP).

IPv6 ND Cache

Displays the content of the IPv6 neighbor discovery cache. For more information, see IPv6.

(Azure Firewalls Only) Azure UDR

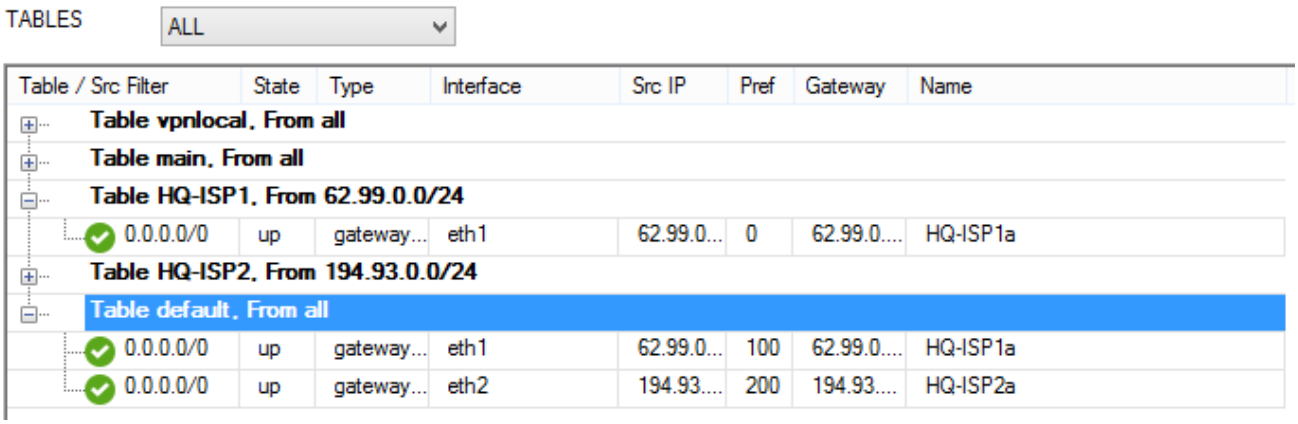


F-Series Firewalls in Azure can manipulate the Azure User Defined Routing (UDR) Table to change the routing table for the backend VMs in case of a failover. This tab shows the User Defined Routing table that is currently active for this cloud service. Azure UDR is supported for both ASM (Azure Service Manager) and ARM (Azure Resource Manger). Grey routes are routes that do not use a F-Series Firewall as the destination. Red status indicates that the changes to the routing table are currently in progress.

For more information, see How to Configure a High Availability Cluster in Azure using PowerShell and ARM or How to Configure a High Availability Cluster in Azure via PowerShell and ASM.

Routing Tables

In the bottom table on the **Network** page, you can view information about your routing tables. If you have not configured policy routing, information is only provided for the main and default tables. Default routes are contained in the default table.



To display information for only certain routing tables, select the table name from the **TABLES** list. Without policy routing activated, all routes except the default routes will go into the main table. Default routes go into the default table. With policy routing activated, additional tables become available as specified in the configuration dialog. In the table, information for each route is organized into the following columns:

- **Table / Src Filter** – The routing table name and its routed netmasks. This column lists routing tables by name. To expand and collapse the list of netmasks for a table, double-click the table name.
- **State** – The state of the routing. Available entries are **up**, **down**, **wild**, **disabled**, and **off**.
- **Type** – The route type:
  - **Direct** – Direct routes point to directly connected networks. No next hop is involved. The network is directly accessible via the specified interface.
  - **Gateway** – Gateway routes are routes to networks that are only accessible via a next hop. The next hop must be reachable through a direct route.
- **Interface** – The interface through which traffic to the destination network passes.
  For direct routes, the interface must be specified within the network configuration. For gateway routes, it is automatically determined from the available direct routes.
- **Src IP** – The route source IP address.
  The control daemon automatically picks the most appropriate source address from the pool of available IP addresses unless a source address has been explicitly specified in the network configuration.
- **Pref** – The preference of the route, with **0** indicating the highest preference.
- **Gateway** – The address of the next hop for gateway routes. For direct routes, this field is left empty (denoted by a single -).
- **Name** – The given name of the route.

If you added routes at the command line or deleted direct and gateway routes with a 'Soft' network activation, you might see routes that are marked as 'wild'. These are routes for which there is no corresponding entry in the network configuration file. To delete a wild route, right-click it and select **Delete Wild Route**.

Figures

1. Control-Network.gif
2. eth_ico.png
3. dir_ico.png
4. conn_ico.png
5. vpn_ico.png
6. two_ico.png
7. ok_ico.png
8. grey_ico.png
9. load0_ico.png
10. load1_ico.png
11. load5_ico.png
12. cross_ico.png
13. net_stat.png
14. net_ospf.png
15. net_azure.png
16. net_table.png