
Virtual Servers and Services

<https://campus.barracuda.com/doc/46209512/>

Virtual servers represent the main operative instance on the NextGen Firewall F-Series next to global settings and box configuration objects. The virtual server layer manages all IP addresses that are required for the services running on the virtual servers. It introduces all IP addresses that are needed for proper operation except remote management and HA IP addresses. Depending on your requirements, you can create multiple virtual servers on a stand-alone box or in a Control Center cluster.

Virtual Servers

The virtual server layer runs on the box layer of the F-Series. It is a purely logical layer whose most important function is to make IP addresses available for the services (service layer). By default, the virtual server S1 is already created on every F-Series Firewall except the larger hardware models. When a virtual server is started, it assigns IP addresses to its services, causing the box layer to automatically activate pending routes of directly attached network routes.

On a virtual server you must introduce all IP addresses that should be managed by the server and assigned to the services under it. These IP addresses must be in one of the networks for which a directly attached network route exists on box level. Do not use the IP addresses configured on the box layer, such as the management IP address or additional local IP addresses, because this causes problems in HA setups. The encryption level is also configured at the virtual service level. If your F-Series Firewall is running without a valid license (demo mode) or in an export-restricted country, you can only use export-restricted encryption until your system gets licensed. Virtual servers are bound to the product type and name. Once created, they cannot be renamed.

For more information, see [How to Configure Virtual Servers](#).

HA Monitoring and Transparent Failover

A virtual server is transferable between members of a high availability cluster. If the primary unit fails, the virtual server, including its assigned IP addresses and all services, is instantly transferred to the secondary unit. You can also create virtual servers with services to run only on a secondary unit that, in case of a failover, are transferred to the primary unit and vice versa.

For HA failover, the management IP address and the 1st virtual server IP address are monitored by default. To configure transparent monitoring for HA clusters, create monitoring policies for interfaces and IP addresses. The virtual server stays up as long as these health check targets are reachable.

For more information, see [Virtual Server Monitoring](#) and [High Availability](#).

Virtual Servers in the Barracuda NextGen Control Center

On the Barracuda NextGen Control Center, virtual servers are created in the Control Center cluster. The setup procedure is very similar to the procedure on an F-Series Firewall, which means that you can create a server and assign the network IP addresses and services. Virtual servers act as separate configuration entities, so you can copy them from one to another cluster. For example, you can assign the virtual server S1 once per cluster. When assigning virtual servers to different clusters, the setup requires the matching product type. For example, you cannot assign a VF25 virtual server to a Barracuda NextGen Firewall F-Series F10.

For more information, see [How to Configure Virtual Servers](#).

Services

The service layer runs on the virtual server layer of the F-Series. It introduces the services such as firewall, HTTP proxy, VPN, and DHCP. The services use the configured IP addresses of the virtual server on which they are running. If the virtual server shuts down, all of the assigned services and IP addresses are also shut down and made unavailable. If the Firewall F-Series Firewall is deployed in a high availability cluster, the services and necessary IP addresses transparently failover to the other HA unit.

For more information, see [How to Configure Services](#), [NextGen F-Series Services](#) or [Shared Services](#)

© Barracuda Networks Inc., 2019 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.