

How to Configure Box-Level Monitoring

<https://campus.barracuda.com/doc/53248725/>

Define polling intervals for network routes, HA partner units and other parameters that are monitored to ensure that the box layer of the NextGen Firewall F-Series or Control Center is running. HA units can be configured to use an additional network connection for heartbeat communication.

Configure Monitoring Settings

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Control**.
2. Click **Lock**.
3. In the **Monitoring Parameters** section, specify the monitoring interval and which services or daemons should not be monitored:
 - **Startup Poll Interval [Secs]** – The period of time that has to expire after booting or activating the network until a HA action can take place (default: 10). This is important especially with "slow learning" NICs that need quite a time after booting/activating until the link is activated.
 - **Regular Poll Interval [Secs]** – The number of seconds between HA heartbeats. This setting also specifies the reaction time for activating and deactivating routes and the server (Monitor IPs). For faster HA failovers, you can decrease the default poll interval of 5 seconds.

When you are using the firewall with transparent failover, you can enter 1 second. However, the HA partner will instantly perform a takeover during server starts and stops or network activation. In this case, first block the server before doing anything else.
4. In the **HA Monitoring Parameters** section, define a translation table specifying the IP addresses to use for communication in network setups that provide a private uplink between two HA partners. In the **Translated HA IP** table, specify the following settings for each entry:
 - **Translated HA IP** – The primary management IP address of the HA unit as specified in the **Management IP** field on the **Network** page (**Config > Full Config > Box**).
 - **Alternative HA IP** – The alternative HA IP is part of the private uplink network as specified in the **Additional Local IPs** section on the **Network** page (**Config > Full Config > Box**).

You must also add the **Alternative IP addresses** into the corresponding firewall rule (inbound).
 - **Usage Policy** – Specify how to proceed if the alternative HA IP becomes unavailable.
 - **Description** – Optional description.
5. In the **ICMP Gateway Monitoring Exemptions** section, specify the interfaces on which the gateway cannot be reachable via regular ICMP-based probing. In the **No Probing for Interfaces** table, select the interfaces.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

© 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.