How to Configure Time Server (NTP) Settings

https://campus.barracuda.com/doc/48202842/

Precise timekeeping is very important for the F-Series Firewall and Control Center. HA synchronization, data accounting, Control Center configuration updates, logging, event notification, and other time-based services rely on a correct time system. The NTP daemon can be configured to listen on the management IP, additional local IP addresses, and, if remote managed the VIP address of the managed firewall on port UDP/123. Connections to the NTP daemon are handled by the host firewall. Two synchronization methods are supported:

- **NTP Servers** – The firewall acts as a client and retrieves and sets the time according to the time retrieved from the NTP server. You can use multiple NTP servers. The time deviation between the NTP server and the firewall must be less than 1000 seconds for the synchronization to succeed. To continuously synchronize the time with a NTP server, you must enable the NTP daemon. If multiple time servers are used, the time server with the lower stratum value is preferred.
- **NTP Peers** – To keep the time in your network synchronized when the NTP servers are unavailable, use the two-way NTP peer synchronization. NTP peers will converge toward a median time in multiple steps. No synchronization step can exceed two minutes. This means that two systems might take some time to synchronize. You can use MD5, SHA, SHA1, Ripe-MD160, and autokey authentication.

When using a NextGen Control Center for multiple systems in different time zones, consider using UTC for all your systems.

> When you run the NTP, your system becomes vulnerable to NTP exploits and UDP-based DoS attacks. Never use untrusted reference time servers or run a time server in a hostile environment.

Before you begin

(optional) To use a FQDN or hostname as the NTP server the firewall must be able to resolve the hostname. For more information, see How to Configure DNS Settings.

Step 1. Configure time settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **Time Settings / NTP**.

3. Click **Lock**.
4. Select your **Timezone** in the form *country/city*.
   You can use Etc/GMT time, or UTC. Etc/GMT times do not support daylight saving time (DST). When using a Barracuda NextGen Control Center for multiple systems in different time zones, consider using UTC for all your systems.
5. Enable **Set HW Clock to UTC** to protect your system against unexpected time lapses caused by daylight saving time (DST).
6. Click **Send Changes** and **Activate**.

Step 2. Configure the time server

Configure the NTP servers you are using to set and synchronize the time for your Barracuda NextGen Firewall F-Series. NTP servers must be reachable from the management IP address of the firewall or Control Center for standalone systems. For managed firewalls the NTP server must be reachable through the remote management tunnel.

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **Time Settings / NTP**.
3. Click **Lock**.
4. Enable **NTP sync on Startup** to synchronize with an NTP server via ntpdate when starting. (You can also run an NTP daemon on the system for continuous time synchronization.)
5. In the **Time Server IP or Name** table, add the IP address or hostname of the NTP time server(s). A remote, managed NextGen Firewall F-Series as an NTP server can be used by entering its VIP address.
6. Enable **Start NTPd** to synchronize the NTP daemon with the NTP time server(s).
7. Set the **Local Clock Stratum** value for the NTPd. If you are configuring a Control Center, make sure to use a stratum value lower than the default stratum (10) of the NextGen Firewall F-Series.
8. (optional) Select the events that you want to be notified about (Event-IDs 2070-2073) in **Event on NTPd**:
   - **start-failure (default)**
   - **+stop-failure**
   - **++start-success**
   - **+++stop-success**

   The list is additive. Events further down the list automatically include all the events that are listed before them.
9. Click **Send Changes** and **Activate**.

Step 3. (optional) Configure NTP peers

Configure the NTP peers in your network. NTP peers should be on the same stratum. To authenticate

NTP peers, you can choose between passphrase/MD5 and NTP autokey authentication. NTP peers must be reachable from the management IP address of the NextGen Firewall F-Series.

1. Go to **CONFIGURATION > Configuration Tree > Box > Administrative Settings**.
2. In the left menu, click **Time Settings / NTP**.
3. Click **Lock**.
4. In the **Time Peers** section, click **+** to add your NTP peers. The **Time Peers** window opens.
5. Specify the following settings for each peer:
   - **Peer IP Address** – Enter the IP address for the NTP peer.
   - **Peer Authentication Type** – Select **None**, **MD5**, **SHA**, **SHA1**, **Ripe-MD160** or **Autokey** authentication.
   - **(MD5,SHA,SHA1, RipeMD160 authentication only) Peer Authentication ID** – Enter a number between 0 and 1000000. You must use the same Peer Authentication ID on all peers.
   - **(MD5,SHA,SHA1, RipeMD160 authentication only) Peer Authentication** – Enter the NTP peer authentication string.
   - **(Autokey authentication only) Peer Host Name** – Enter the FQDN for the trusted NTP peer.
   - **(Autokey authentication only) Trusted Public Key** – Import the public key for the NTP peer.
6. Click **OK**.
7. If you are using NTP autokey authentication, click **Set** next to **NTP Autokey Configuration**. The **NTP Autokey Configuration** window opens.
   1. Enter the **NTP Key Password** which is used to encrypt the private key.
   2. Click **Create New NTP Key**.
   3. Click **OK**. The NTP certificate is created.
   4. Click **Ex/Import** and select **Export to File**. Use the public key to authenticate to other NTP peers.
8. Click **Send Changes** and **Activate**.

Event processing

The event setting only pertains to NTPd behavior during controlled start or stop sequences. You will not be notified when NTPd is killed manually or just dies unexpectedly. Events are also triggered when the NTPd is restarted on the Box Page with the following options:

- **Restart NTP** – The control daemon restarts the NTPd.
- **Sync** – Starts the synchronization processes with the *ctrltime* script, which stops the NTPd and then executes *ntpdate* on port 123.

NTP troubleshooting

On the command line, enter: `ntpq -p` to check which NTP servers and peers your Barracuda NextGen Firewall F-Series is using. See below for an example of an NextGen Firewall F-Series using one NTP server (10.0.10.44) and three NTP peers. For more information, see http://ntp.org

```
[root@HQ-NG2:~]# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 LOCAL(0)        .LOCL.          10 l 1810   16    0    0.000    0.000   0.000
*10.0.10.44      194.11.27.31     3 u   22   32  377    0.396   -0.807   0.102
-10.0.10.88      10.0.10.63       5 u   42   64  376    0.335   -0.125   0.326
+10.0.10.70      10.0.10.44       4 u   43   64  376    0.611   -0.186  21.559
+10.0.10.63      10.0.10.44       4 u   40   64  376    0.374   -0.201   9.844
[2014-11-10 16:03 CET] [-root shell-] [-Barracuda Networks-]
[root@HQ-NG2:~]#
```

Figures

1. ntpq.png

© Barracuda Networks Inc., 2024 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.