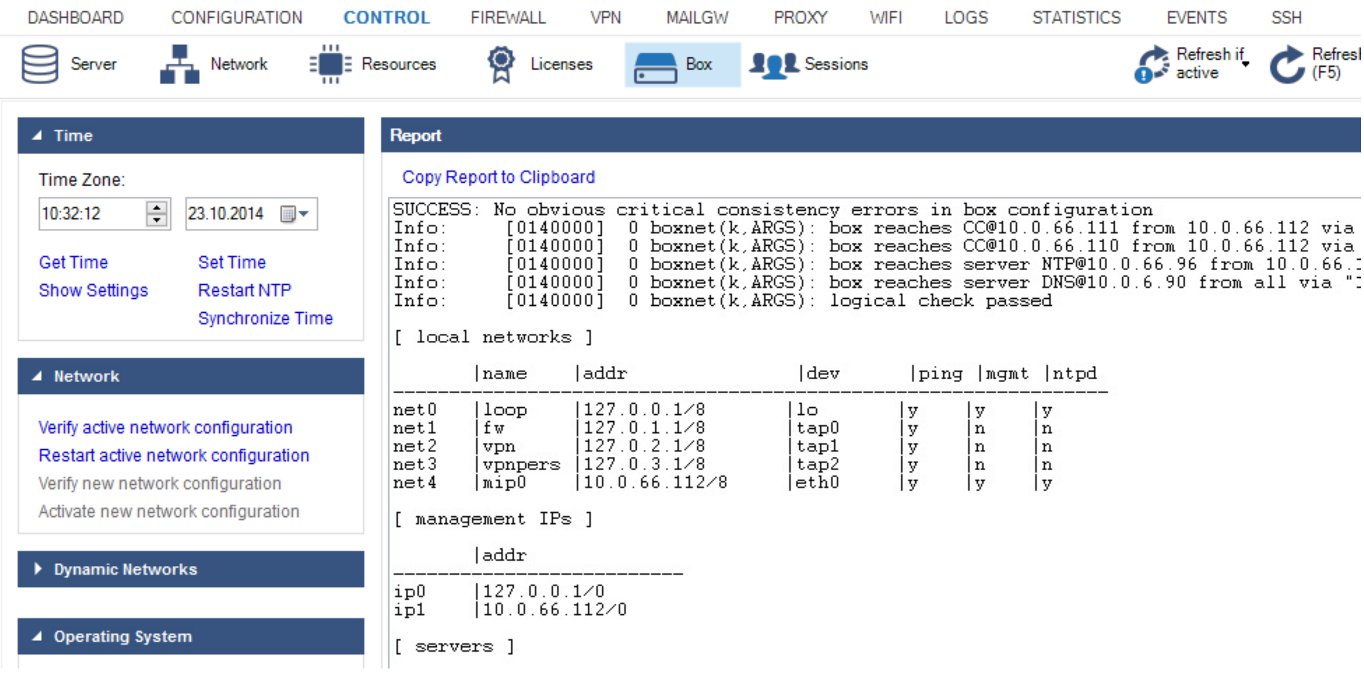
Box Page

https://campus.barracuda.com/doc/48202816/

On the **Box** page, you can configure and control key aspects of the Barracuda NextGen Firewall F-Series box operation. To access the **Box** page, open the **CONTROL** tab and click the **Box** icon in the ribbon bar.



Time Zone:

10:32:12 23.10.2014

```
SUCCESS: No obvious critical consistency errors in box configuration
Info:     [0140000]  0 boxnet(k,ARGS): box reaches CC@10.0.66.111 from 10.0.66.112 via
Info:     [0140000]  0 boxnet(k,ARGS): box reaches CC@10.0.66.110 from 10.0.66.112 via
Info:     [0140000]  0 boxnet(k,ARGS): box reaches server NTP@10.0.66.96 from 10.0.66.
Info:     [0140000]  0 boxnet(k,ARGS): box reaches server DNS@10.0.6.90 from all via "
Info:     [0140000]  0 boxnet(k,ARGS): logical check passed

[ local networks ]

       |name    |addr               |dev      |ping |mgmt |ntpd
-------------------------------------------------------------------
net0   |loop    |127.0.0.1/8        |lo       |y    |y    |y
net1   |fw      |127.0.1.1/8        |tap0     |y    |n    |n
net2   |vpn     |127.0.2.1/8        |tap1     |y    |n    |n
net3   |vpnpers |127.0.3.1/8        |tap2     |y    |n    |n
net4   |mip0    |10.0.66.112/8      |eth0     |y    |y    |y

[ management IPs ]

       |addr
---------------------------
ip0    |127.0.0.1/0
ip1    |10.0.66.112/0

[ servers ]
```

Time

When expanded in the left pane, the **Time** menu shows the system time and provides you with the following options to view and configure the time settings for the F-Series Firewall:

- **Get Time** – Displays the current time and date on the firewall.
- **Show Settings** – Displays the current NTP settings in the **Report** window..
- **Set Time** – Changes the current time and date to the values selected from the time and date fields. If your firewall is synchronized with an external time server, this manual change is overwritten by the succeeding time synchronization.
- **Restart NTP** – Restarts all NTP services.
- **Synchronize Time** – Offers an option dialog to synchronize the time settings with an NTP server.

If the **Using Time Server** and **Own IP** settings are unspecified, the synchronization process binds to the firewall's primary management IP address. This method works well with a time server that is placed in the same network as the primary management IP address. For time synchronization with a public time server, enter the external IP address of the firewall into the **Own IP** field so that the time server's response is not blocked by the firewall.

Network

When you expand the **Network** menu, you are provided with the following options to verify, restart, and activate the network configuration of the F-Series Firewall:

Verify active network configuration

This option checks the currently active network configuration for errors. The result appears in the **Report** window.

Restart active network configuration

This option shuts down and then restarts the currently active network configuration.

The server subsystem is unaffected by this procedure, but the server and services will be unavailable for a short time while the network shuts down and restarts.

Verify new network configuration

This option checks new network configurations for errors after they have been successfully sent. The result appears in the **Report** window.

Because changing the network configuration of a remotely controlled Barracuda NextGen Control Center is a critical operation, new configurations are not automatically activated until after they have been verified. If the new network configuration is flawed, you must correct the errors and then verify the configuration again. The newly received network configuration file is stored in `/opt/phion/preserve/boxnet.conf`.

Activate new network configuration

This option activates new network configurations after they have been successfully verified. You can activate the new network configuration in the following modes:

- **Activate now** – The **Activate now** option is offered when a management IP address has been changed. With this mode, the firewall activates the network change and reconnects to the new IP address.

- **Failsafe** – Failsafe network activation is the safest way to activate configuration changes. Always use this activation method on productive firewalls, e.g., to do the following:
    - Add and delete network interfaces.
    - Change network interface configurations.
    - Add and delete policy routes.
    - Delete direct and gateway routes.

With this mode, the firewall creates a backup file of the active network configuration. It then temporarily activates the configuration changes and verifies that the firewall can still be contacted via Barracuda NextGen Admin. If this verification is successful, the network is restarted so that the changes are activated permanently. If verification fails within the timeout defined in the **Set Timeout** field, the original network configuration is restored.

You might lose connection to the firewall, especially when activating network configuration changes via a VPN connection. This causes a connection verification failure between the firewall and Barracuda NextGen Admin. As a result, the original configuration is then restored. If you experience this issue, try using 'Force' network activation.

- **Force** – Forced network activation immediately activates the new network configuration with a logical consistency check ,but without creating a backup file of the active network configuration.

Use forced network activation with due care.

- **Soft** – Soft network activation can only be used after you add direct routes or gateway routes to an existing configuration.
  Do not use 'Soft' network activation for the following:
    - Adding or deleting source-based routes.
    - Permanently deleting direct or gateway routes. Direct and gateway routes that have been deleted with 'Soft' network activation are marked as wild on the Network Page page. To delete these types of routes, use 'Failsafe' network activation instead, or restart the network. To restart the firewall, expand the **Operating System** menu.

  You can also use soft network activation after changing the **VPN** **Point of Entry** for a management tunnel on an F-Series Firewall. In this case, you can verify the configuration change by going to the Live Page and checking the **Destination IP** on port 692.

Dynamic Networks

If dynamic network connections have been configured, you can control them with options (off, on, start, stop, restart, reset) from the **Dynamic Networks** menu. You can control the following types of network connections:

- xDSL
- ISDN
- DHCP (cable)-connections
- Wireless WAN (WWAN)
- MGMT (box management)
- Tunnel connections

Operating System

From the **Operating System** menu, you can control the F-Series Firewall. The menu provides you with the following options:

- **Reboot Box** – Reboots the firewall. If the firewall is not easily accessible, use caution when using this option because some firewalls might have problems with BIOS settings and fail to reboot or get stuck on a lower layer.
- **Firmware Restart** – Shuts down and then restarts all servers and services belonging to the firewall subsystem, including the firewall engine.

  > All connections will be lost, including non-Barracuda proprietary services such as Secure Shell (SSHd) and Network Time Protocol (NTPd).

  Using this option is similar to running the `/opt/phion/bin/phionctrl shutdown` and `/opt/phion/bin/phionctrl startup` commands, except the control daemon itself is not stopped and started.
- **Shutdown Box** – Turns off the firewall.
- **Save current Config for ART** – Saves the current configuration of the firewall to the ART crash recovery OS. If the firewall must be reinstalled remotely, it uses the current system configuration for the recovery process.
- **Install Update** – Installs the selected firmware updates, hotfixes, or patches. The update process can be triggered after the package is successfully uploaded to the unit.
- **Generate System Report** – Creates a system report.
- **Reset SMS Counter** – Resets the counter for the number of successive SMS commands that have been accepted by the interface.

Domain Control

From the **Domain Control** menu, you can register the F-Series Firewall as a Windows domain member or view its domain registration status. The menu provides you with the following options:

- **Show Registration Status** – Displays the registration status of the firewall at a Windows domain.

- **Register at Domain** – Registers the firewall as a Windows domain member at a domain controller. In the **User Authentication** window, enter the username and password for the user with the appropriate administrative rights to add the firewall to the domain. Before you can use this option, configure an Authentication service.
- **Register Proxy at Domain** – Registers the HTTP Proxy at the Windows domain.

Authentication Level

You can specify the level of authentication that is required for non-interactive Barracuda NextGen Control Center logins and HA synchronization.

Authentication level changes are effective immediately.

After you expand the **Authentication Level** menu, you can select one of the following options:

- **No Authentication** – Level -1; no authentication is required to send or retrieve configuration data.
  Use this option only when necessary, and revoke it as soon as possible.
- **Check Key or IP address** – Level 0; an IP address or key challenge is required. This option is still quite unsecure.
- **Check IP address** – Level 1, still quite unsecure.
- **Check Key** – Level 2, still quite unsecure.
- **Check Key and IP address** – Level 3, default setting. Do not change it unless you must temporarily lower the security level. A change might be required when either the IP addresses of the Control Center or HA partner change, or the key of the Control Center changes.

SCEP Control

You can view and configure SCEP settings. When you expand the **SCEP Control** menu, you can select the following options from the **Cmd** list:

- **Show Certificate Info** – Displays information about the certificate retrieved by SCEP.
- **Save Certificate to Clipboard** – Exports the certificate to the clipboard (PEM).
- **Save Certificate to File** – Exports the certificate to a file (PEM).
- **Initiate Pending Request** – Starts the enrollment process immediately.
- **Force SCEP Update** – Starts an SCEP update.
- **Set SCEP Debug ON** – Turns SCEP debugging on. Additional debugging information is included in the SCEP log (**Box > Control > SCEP**).
- **Set SCEP Debug OFF** – Turns SCEP debugging off.

- **Set SCEP Password** – Prompts for the SCEP password. This option is available only if the SCEP password policy is set to *Enter-Password-At-Box*.

Report

The **Report** window displays the results of operations selected in the above sections. For example, if a new network configuration is sent to the F-Series Firewall and has been verified, the **Report** window shows the results of the consistency check.

Figures