

Best Practice - Core System Configuration Files and Ports Overview

<https://campus.barracuda.com/doc/96025959/>

The underlying Linux system is designed to serve as a basis for the Barracuda CloudGen Firewall. Direct interfering on the command line is not necessary for normal operation. Such operations should be carried out only by authorized personnel with excellent knowledge of Linux systems and its special Barracuda Networks implementation.

The Barracuda CloudGen Firewall system basically consists of three parts. The following table provides a general overview of the Barracuda CloudGen Firewall OS Linux system and its licensing concepts:

Layer	Description	Licensing
Basic Linux	Standard Linux system with the modified NGFW OS kernel. Kernel sources are a part of the distribution.	Except for the Firewall engine, mostly under GPL or other Open Source Licenses.
Barracuda CloudGen networking	Handles all steps dealing with networking.	Barracuda Networks Public License. Can be used freely for all purposes except commercial redistribution.
Barracuda CloudGen operative	Operative Barracuda Networks Software; consists of box services (logging, statistics, control) and server (for example VPN, mail gateway, DNS, ...)	Proprietary Barracuda Networks License.

Networking Layer

The Barracuda CloudGen Firewall OS networking layer is installed by the *phionetc_box* package. It is called *phionetc_box* because almost all relevant files live in the directory */etc/phion*. The main purpose of the package is to control every part of the system that communicates over the network. In addition to the Barracuda CloudGen Firewall software modules, there are other packages like *openssh* or *ntp* that get their configuration and are started by specific scripts.

Configuration Files

There are three configuration files steering and controlling the networking behavior of the system:

- */etc/phion/options*
- */etc/phion/boxadm.conf*
- */etc/phion/boxnet.conf*

The options file is the only one that is not edited through the Barracuda Firewall Admin GUI. Template of the options file:

```
#####
## Systemwide options
## File is sourced by several start scripts
##
# start networking at all?
BOX_NETWORK="Y"
# Number of retries to bring up all devices, sometimes useful for token ring
devices
NET_RETRY=0
# should the NGFW Subsystem be started ?
PHION_START="Y"
#for some historical reason: should the NetDB subsystem be started?
#CAUTION: Activate only if you know very well what you are doing.
NETDB_START="N"
# for advanced Servers
START_ORA="N" #Y/N start ORACLE on BOOT
START_ADABAS="N" #Y/N start ADABAS on BOOT
```

- **BOX_NETWORK** - Do not change. If you do set it to **N**, the Barracuda CloudGen networking and the services depending on it will not start. The Barracuda CloudGen Firewall will not be functional if this option is set.
- **NET_RETRY** - Number of retries to establish a network link.
- **PHION_START** - If set to **N**, the Barracuda CloudGen Firewall OS operative layer will not be started at all. The Barracuda CloudGen Firewall will not be functional if this option is set to **N**.
- **NETDB_START** - Only of use if you have a legacy unit with a NetDB database system on it.
- **START_ORA** and **START_ADABAS** - Only of use for a Master configuration server with an Oracle or ADABAS D database.

The boxadm.conf file holds all information that does not need a network restart to be activated. In addition, it also holds information for Barracuda CloudGen Firewall box services. An example of an operative configuration file:

```
ACLLIST[] = 10.0.0.8/29 10.0.0.231
ACTBOXSERVICES = y
DNSSERVER[] = 10.1.103.179 10.1.100.204
DOMAIN = m086
ENABLESHOSTS = y
MAINADMIN = n
MASTER[] = 10.1.17.42
```

```
RID = 86
RMASTER[] = 10.1.17.42
RPASSWD = $1$someMD5encryption
SPASSWD = $1$someMD5encryption
STARTNTP = y
STATISTICS = y
SYNC = y
TMASTER[] = 10.1.16.21
TZONE = Europe/Vienna
UTC = y
[boxtuning]
FILEMAX = 32768
IDETUNING = y
INODEMAX = 65536
SYSTUNING = n
```

For an explanation of the parameters, see [How to Configure Advanced Barracuda OS System Settings](#).

Be extremely cautious when changing these files on the command line.

The `boxnet.conf` file holds all information that deals with network connections. These are the hostname and the network interfaces, IP addresses and routing information. Again, let us have a look on a sample file:

```
HOSTNAME = sega
[addnet_dmz]
BIND = n
CRIT = y
DEV = eth1
IP = 192.168.32.1
IPCHAINS = y
MASK = 8
PING = y
[addroute_default
]
DEST =
195.23.11.6
DEV =
FOREIGN = y
MASK = 32
PREF =
REACHIP[] =
SRC =
```

```
TARGET = 0.0.0.0
TYPE = gw
[addroute_QA]
DEST = 10.0.0.244
DEV = eth0
FOREIGN = y
MASK = 8
SRC = 10.0.0.8
TARGET = 192.168.10.0
TYPE = gw
[boxnet]
DEV = eth0
IP = 10.0.0.8
MASK = 8
[cards_eepro]
MOD = eeepro100.o
MODOPTIONS[] =
NUM = 1
TYPE = eth
[cards_realtek]
MOD = rtl18139.o
MODOPTIONS[] =
```

For an explanation of the parameters, see [How to Configure Advanced Barracuda OS System Settings](#).

Activation Scripts

There are two scripts that are intended to be started from the command line:

- /etc/rc.d/init.d/phion (which is actually a link to /etc/phion/rc.d/phionrc).
- /etc/phion/bin/activate

All other scripts should not be started on the command line but are invoked by the 2 scripts above.

Operative Layer

Static Data

The whole operative data resides in /opt/phion .

It is not recommended to change anything below this directory.

The full configuration of a Barracuda CloudGen Firewall box is held under `/opt/phion/config/active`. The configuration files may be modified manually by a Barracuda Networks support engineer or by a specially trained system engineer. If you are not absolutely sure about what you are doing, do not change anything here.

Dynamic Data

Log files and statistics data reside in `/var/phion`. This directory has the following substructure:

- `/var/phion/logs` – All log files are stored here. You can read it with any editor.
DO NOT write to it, DO NOT rename it, DO NOT put any files in here. Any manual action can result in strange behavior of the log interface.
- `/var/phion/stat` – Root directory for the statistics data structure. The data files are Berkeley DB files in binary form. They can be viewed with the `showstat` utility (`/opt/phion/bin/`).
Again: Do NOT change anything in this directory manually.
- `/var/phion/logcache` – Home of the Log Access Files (*.laf). These are Berkeley DB files for fast access to large log files.
- `/var/phion/run/<module>` – Services may store operational data in these directories.

Intervention on command line is generally not intended on the NGFW OS operative layer. Nevertheless, there is one powerful tool to steer the processes. It can be used to gather comprehensive information about system state, routing, servers, processes. Furthermore, it can start / stop / block / disable servers and box processes. It is called `phionctrl` and resides in `/opt/phion/bin`. For more information, see [phionctrl](#).

Ports Overview

The following table enlists the ports of a Barracuda CloudGen Firewall / Control Center that are required for communication:

Port	Protocol	Type	Daemon	Traffic Direction
22	TCP	service	sshd (SSH)	inbound firewall and Control Center
691 and 443	TCP/UDP	service	vpn	inbound firewall
450	TCP	service	fwauth	inbound firewall (block URL notification)
680	TCP	service	FW-audit (Firewall Audit Viewer)	inbound firewall and Control Center
688	TCP	service	firewall (Firewall Service)	inbound firewall and Control Center
689	UDP	box	controld/HA-Sync	inbound and outbound for both firewall and Control Center

692	TCP/UDP	VPN	management tunnel	inbound Control Center / Access Controller
694	TCP	VPN	AutoVPN TINA tunnel	inbound and outbound for firewall
801	TCP	box	controld/status (Control Status)	inbound and outbound for both firewall and Control Center
801	UDP	box	controld/ HA-heartbeat	inbound and outbound for both firewall and Control Center
802	TCP	box	phibsd	local listener only
803	TCP	box	logd (Log-Viewer)	inbound firewall (Barracuda Firewall Admin UI)
805	TCP	box	distd	inbound firewall and Control Center
806	TCP	service	SPoE (Single Point of Entry Control Center) and qstatd (Statistics Viewer)	inbound firewall and Control Center
807	TCP	box	SPoE (Single Point of Entry firewall) and qstatd	inbound firewall and Control Center
808	TCP/UDP	box	event (Event Viewer)	inbound firewall and Control Center (Barracuda Firewall Admin UI)
808	TCP/UDP	service	event	inbound firewall and Control Center
809	TCP	box	boxconfig (Configuration Service)	inbound firewall and Control Center
810	TCP	service	masterconfig (Master Configuration Service)	inbound Control Center
811	TCP	service	Master event	inbound Control Center
814	TCP	service	vpnserver (VPN Service, Master VPN Service)	inbound firewall and Control Center
815	TCP	service	mailgw (Mail Gateway Service)	inbound firewall and Control Center
816	TCP	service	DHCP	inbound firewall and Control Center
817	UDP	service	trans7	inbound firewall and Control Center
818	TCP	service	PKI	inbound Control Center
844	TCP	service	policyserver (Policy Service, Master Policy Service)	inbound firewall and Control Center
845	TCP	box	distd	inbound and outbound firewall and Control Center
850	TCP	service	Virus Scanning service	inbound firewall
880	TCP	service	HTTP Proxy	inbound firewall and Control Center
889	TCP	service	Barracuda Secure Connector	inbound and outbound Control Center

8001	TCP	service	Barracuda Firewall Insights	inbound and outbound firewall and Control Center
8443	TCP (HTTPS)	service	REST API	inbound firewall and Control Center
44000 and 44001	TCP	service	policyserver	inbound firewall and Control Center

© 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.