

## How to Create PAR or PCA Files on the Command Line

<https://campus.barracuda.com/doc/43846902/>

Use the [phionar](#) tool to back up the configuration of a single Barracuda NG Firewall or Barracuda NG Control Center. A cron job can be used to automate the configuration backups.

Always keep PAR or PCA files of a functioning configuration for all your Barracuda NG Firewalls and NG Control Centers in a secure location.

### In this article:

#### Create an Unencrypted box.par File

Enter the following command to create a complete, unencrypted archive of the current configuration:

```
cd /opt/phion/config/configroot/ /opt/phion/bin/phionar cdl  
/backuppath/archive.par *
```

#### Create an Encrypted box.pca File

PCA files can be created by using the serial number as the password, or by specifying a manual password.

PCA files are available for firmware 6.0.1 or later. PCA files created for Barracuda NG Firewalls running version 6.0.0 on an NG Control Center must be decrypted manually. For more information, see [phionar and conftool](#).

#### Using a Manual Password

Enter the following command to create a complete encrypted archive of your configuration with a custom password:

```
cd /opt/phion/config/configroot/ /opt/phion/bin/phionar cdl -P YOURPASSWORD
```

```
/backuppath/box.pca *
```

### Using the Serial Number as the Password

Enter the following command to create a complete, encrypted archive of your configuration by using the serial number as the password for the archive.

```
cd /opt/phion/config/configroot/ /opt/phion/bin/phionar cdl -Q
/backuppath/box.pca *
```

### Decrypting a PCA File

Virtual and Public Cloud appliances can only be restored by using unencrypted PAR files. To decrypt the PCA file, you can use phionar on a Barracuda NG Firewall or OpenSSL on any Linux or Windows host.

For more information, see [phionar and conftool](#).

## Create an archive.par PAR File

To create an archive of a Barracuda NG Control Center, enter the following commands:

```
cd /opt/phion/rangetree/ /opt/phion/bin/phionar cdl /tmp/archive.par
./configroot/*
```

### Example Backup Script

The following table contains an example backup script that can be used to back up the configurations on a Barracuda NG Control Center. Modify this script to use encrypted archives for NG Firewalls with version 6.0.1 or later.

```
#!/bin/bash ##### #echo "Backup-Script for Barracuda NG
Firewall" #echo "-----" #echo "Creation of
archive files" #echo "ftp or scp -transfer onto 10.0.0.1" #echo "-----
-----" HOST='10.0.0.1' USER='yourusername'
PASSWD='yourpassword' DSTPATH='/root/' FILENAME1=CC-tree_`date
+%Y_%m_%d_%H_%M`.par FILENAME2=CC-box_`date +%Y_%m_%d_%H_%M`.par cd
/opt/phion/maintree/ /opt/phion/bin/phionar cdl /root/${FILENAME1}
configroot/* history/* cd /opt/phion/config/configroot/
/opt/phion/bin/phionar cdl /root/${FILENAME2} * ##### #
Example of ftp: cd /root/ ftp -n $HOST
```

---

## Emergency Restore

---

In case of a severe misconfiguration, you can perform an emergency restore with a PAR or PCA file containing a working configuration. You can perform the restore by USB stick or via SSH shell. Barracuda Networks recommends performing emergency restore via USB stick for hardware appliances.

### Restore for Hardware Appliances using an USB Stick

1. Retrieve the **box.par** or **box.pca** file with the last working configuration and copy it to a USB flash drive. Plug the USB stick into the affected system.
2. Identify the storage device label for the USB flash drive. Enter **fdisk -l** to locate the USB flash drive on the Barracuda NG Firewall or NG Control Center. The device label may vary depending on the Barracuda NG Firewall model. If you use a SATA, SCSI or a RAID controller, the sda1 partition is already in use. In this case, the USB flash drive will use the next free device label. E.g., **/dev/sdb1** USB sticks are typically formatted with FAT32. Check the **System** column for **W95 FAT32 (LBA)** to help you identify the USB stick formatted with FAT32.
3. Log into the Barracuda NG Firewall
4. Mount the USB stick and copy the PAR or PCA file by entering the following commands (Replace **/dev/sdb1** with the storage device from the previous step):

```
mkdir /mnt/usb modprobe usb-storage mount -t vfat /dev/sdb1 /mnt/usb cp /mnt/usb/box.par /opt/phion/update/ umount /mnt/usb
```
5. If you are restoring the configuration with a PCA file created with the **-P** option, or the serial number used as the password of the PCA file does not match the appliance, decrypt the file by using the following command:

```
phionar D -P YOURPASSWORD myarchive.pca myarchive.par
```
6. Restart the **phion** service to initiate the emergency restore:

```
/etc/rc.d/init.d/phion stop /etc/rc.d/init.d/phion start
```
7. Use **ifconfig** to verify the system interfaces and IP addresses are configured as expected.

### Emergency Restore via SSH

If you can reach your Barracuda NG Firewall via SSH, you can also perform an emergency restore via SSH.

1. If necessary, rename the PCA or PAR file to **box.par** or **box.pca**.
2. Copy the **box.par** or **box.pca** file to the **/opt/phion/update/** directory on the Barracuda NG Firewall.
3. If you are restoring the configuration with a PCA file created with the **-P** option, or the serial number used as the password of the PCA file does not match the appliance, decrypt the file using the following command:

```
phionar D -P YOURPASSWORD myarchive.pca myarchive.par
```
4. Restart the **phion** service to initiate the emergency restore:

```
/etc/rc.d/init.d/phion stop /etc/rc.d/init.d/phion start
```

For more information, see [How to Back Up and Restore Your Systems](#).

© Barracuda Networks Inc., 2020 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.