

How to Create PAR or PCA Files on the Command Line

<https://campus.barracuda.com/doc/48202934/>

Use the [phionar](#) tool to back up the configuration of a single Barracuda NextGen Firewall F-Series or Barracuda NextGen 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 firewalls and Control Centers in a secure location.

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/box.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 NextGen Firewalls running version 6.0.0 on an 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 cd l -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 NextGen Firewall F-Series 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 NextGen Control Center, enter the following commands:

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

Please note that the archive.par file does not contain Firewall Secure Connector configurations of the Control Center. Please use the configuration backup feature of Barracuda NextGen Admin instead.

Example backup script

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

Basic script for Control Center

This script creates an archive.par and box.par for a NextGen Control Center. This script does not verify the upload and also does not write to a log file.

```
#!/bin/bash  
#####  
#echo "Backup-Script for Barracuda NextGen Firewall F-Series"
```

```

#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 <<END_SCRIPT
quote USER $USER
quote PASS $PASSWD
cd $DSTPATH
binary
put ${FILENAME1}
put ${FILENAME2}
quit
END_SCRIPT
#####
# Example of scp: Note: You have to exchange your keys with the
destination!
/usr/bin/scp /root/${FILENAME1} $USER@$HOST:${DSTPATH}/${FILENAME1}
/usr/bin/scp /root/${FILENAME2} $USER@$HOST:${DSTPATH}/${FILENAME2}
#####
# Garbage Collection
rm -f /root/${FILENAME1}
rm -f /root/${FILENAME2}
exit 0

```

Advanced backup script

This backup script creates a PAR file for a NextGen Firewall and uploads it via FTP. The upload is verified and the backup is logged to /tmp/Par_FTPbackup.log.

```
#!/bin/bash
```

```
#####
```

```
# ftp server credentials #
```

```
#####
```

```
HOST='192.168.0.16'
```

```
USER='USERNAME'
```

```
PW='PASSWORD'
```

```
FILENAME=box_`date +%e_%b_%Y_%H\UHR%M`.par
```

```
LOGFILE=/tmp/Par_FTPbackup.log
```

```
# Functions
```

```
gen_event() {
```

```
    /etc/phion/bin/events --type_id="131" --type_name="Logfile FTP backup" --layer_id="1" --  
layer_name="box" --class_id="1" --class_name="Storage" --data="Logfile FTP backup  
unsuccessful"
```

```
}
```

```
ftp_conn () {
```

```
    local i=$*
```

```
    # Call 1. Uses the ftp command with the -in switches. -i turns off interactive prompting. -n
```

Restrains FTP from attempting the auto-login feature.

```
/usr/bin/ftp -in $i > /tmp/ftp.worked 2> /tmp/ftp.failed <> ${LOGFILE}

echo "FTP transfer failed" >> ${LOGFILE}

elif [ ! -f retrieval.$$ ]

then

    gen_event

else

    return

fi

}

cleanup() {

    #rm -f /tmp/${FILENAME}

    rm -f /tmp/retrieval.*

    rm -f /tmp/ftp.worked

    rm -f /tmp/ftp.failed

}

echo "*****" >> ${LOGFILE}

date >> ${LOGFILE}
```

```
echo "Creating Par backup" >> ${LOGFILE}

# par file creation

cd /opt/phion/config/configroot/

sleep 5

/opt/phion/bin/phionar cdl /tmp/${FILENAME} *

sleep 10

echo "*****" >> ${LOGFILE}

echo "Trigger FTP Connection" >> ${LOGFILE}

# Actually triggers the backup

ftp_conn $HOST

echo "*****" >> ${LOGFILE}

echo "Garbage Collection" >> ${LOGFILE}

# Garbage Collection

cleanup
```

```
echo "*****" >> ${LOGFILE}

echo "Backup Completed on `date +%Y\ %m\ %d\ %T`">> ${LOGFILE}

echo "*****" >> ${LOGFILE}

exit 0;
```

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 NextGen Firewall F-Series or Control Center. The device label may vary depending on the Barracuda NextGen Firewall F-Series 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 NextGen Firewall F-Series
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 NextGen Firewall F-Series 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 NextGen Firewall F-Series.
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 box.pca box.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., 2021 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.