Migrating CP2000 management servers to CP NG FP3-HF2-HFA322

author: Benoit Dee
e-mail : benoit.dee@skynet.be

TABLE OF CONTENTS

1. INTRODUCTION 3

2. MIGRATION OF THE PRIMARY MANAGEMENT SERVER 3

2.1. MINIMUM SYSTEM REQUIREMENTS 3
2.2. UPGRADE PROCEDURE 4

3. INSTALLATION OF A SECONDARY MANAGEMENT SERVER 7

4. INSTALLATION OF HOTFIX 2 AND HFA322 ON THE PRIMARY AND SECONDARY MANAGEMENT SERVER 8

5. MIGRATION OF THE NOKIA-MODULES 9

5.1. INSTALLING IPSO3.7.1 & CP NG FP3. 9
5.2. INSTALLING HF2 & HFA322. 10

6. ADDITIONAL TOOLS 11

7. REFERENCE MATERIAL 12

DOCUMENT CONTENT

1. Introduction

This document describes the procedure to migrate the Firewall-1 software on the management-server and the Nokia-modules from CheckPoint Firewall-1 v4.1 to CheckPoint Firewall-1 Next Generation Feature Pack 3 Hotfix 2 (NG FP3-HF2) with HFA322. For the installation of the software on the managementservers, new hardware is used.

2. Migration of the primary management server

2.1. Minimum system Requirements

The Check Point NG FP3 management station needs to be a Solaris 8 (32 bit), with a minimum of 20 GB disk and 256 MB memory (512 MB recommended). The Solaris OS also needs the patches 109147-18, 108528-06, 109326-07, 108434 and 108435 to be installed and requires the following list of packages to allow Check Point FireWall-1 to function properly:

- `SUNWlibC`
- `SUNWlibCx`
- `SUNWter`
- `SUNWadmc`
- `SUNWadmfw`

To check the presence of this packages execute

```
pkginfo SUNWlibC SUNWlibCx SUNWter SUNWadmc SUNWadmfw
```

You should see a description of the 5 packages, without errors.

The Solaris 8 OS needs to be stripped using the earlier defined procedure. SSH, gunzip are required packages on the management station.

Control the proper installation of ssh using the command

```
ps -ef|grep sshd|grep -v grep
```

This should result in at least one line with any process number. To check the presence of gunzip execute

```
gunzip –h
```

to see the help file of the gunzip package.

The machine will be delivered with the user `root` using password `root.` This user will be modified later by your IT-Security departement.

2.2. Upgrade Procedure

The first thing to do is checking the CP2000 conf-files in the `$FWDIR/conf` directory using the “Upgrade Verifier” tools (Pre_upgrade_verifier & post_upgrade_verifier script) developed by Check Point. The Pre_upgrade_verifier script :

- warns of potential upgrade problems,
- recommends changes that will allow the upgrade to proceed successfully,
- informs of expected changes of behavior.

Copy the configuration `$FWDIR/conf` of the active management to your home directory `$HOME` on the new management server.

The tools need to be copied from to `$HOME` of the new management station and unzip the file using

```
gunzip ./upgrade_checker_B53039_sol.tgz
```

and untar the files using

```
tar -xvf upgrade_checker_B53039_sol.tar
```

The pre-upgrade script must be executed using the following command:

```
./pre_upgrade_verifier –p $HOME –c 4.1 –t NG_FP3> changes.txt 2>&1
```

(Type the previous command on 1 line)

Before proceeding, communicate the `“changes.txt”` file to the IT-security department of your organisation which will execute the required modifications on the existing management server.

Before installing the NG FP3 software on the new machine, back-up the configuration files of the existing CP2000 management server situated in the `$FWDIR/conf/` directory to a new `/41bu` folder in the root-directory.

You install the NG FP3 management station by using the CD Wrapper. This is done using the following steps:

- Insert the CDROM “Check Point NG FP3” in the CDROM drive,
- Change the directory using `cd /etc/rc2.d/` and start volume management using `./noS92volmgt start` ,
- Perform a `volcheck`,
- Go to the UNIX directory of the CDROM using `cd /cdrom/cpsuite-ng_fp3` and run `./UnixInstallScript .` This program will guide you through the installation process.
- Use “`n`” to go to the next screen.
- Press SPACE to read the license agreement and enter “`y`” to accept it.
- Once the install script has completed the SVN foundation installation, the next step is to select the products that you want to install from this CD. You’re going to type “`1`” to select `“VPN-1 & FireWall-1”`, then enter “`n`” to advance to the next screen.
- Next you will need to select the type of firewall installation you want on this server. Enter “`2`” to select Enterprise Management, and then press “`n`” to continue.
- Enter “`1`” to select Enterprise Primary Management, and then press “`n`” to continue.
- You will be asked if you want to install with or without backward compatibility for 4.1. Enter “`1`” for “`YES`” and press “`n`” to continue. The installation starts.

- When asked to enter a license press “`n`”.
- You will be asked to a SVN administrator. Press `“y”` and enter “`fwadmin`” with the temp password “`abc123`” and give “`W`” write permissions. Permission to manage Administrators is granted, so press “y”.
- When asked to add another administrator, press “`n`”.
- Add a GUI client using “`A`” and add the IP address from the Management station itself.
- When asked to add another GUI client, press “`n`”.
- Press “`Return`” for no group permissions and confirm with “`y`”.
- Type random letters to initialize the Random Pool. When the bar is full you can stop.
- Press “`Return`” to initialize the Internal Certificate Authority and enter “`y`” to define the Fully Qualified Domain Name (FQDN). When asked to change it type “`n`”. Then confirm the chosen FQDN (coming from the `/etc/hosts` file) is the right one using “`y`”. You receive a confirmation that the FQDN was initialized successfully.
- When asked to save the fingerprint press “`n`”.
- You will be asked if you want to start the FireWall & VPN modules: press “`y`”.
- You will be asked to log again to activiate the Check Point Environment Variables. Disconnect your session and reconnect again.
- The final setup configuration of the management server using the cpconfig command, will be done by members of the IT-Security department.
- Ask IT-Security to check the initial connection to the new management server using the GUI client.

After you have installed the new software you need to merge the old CP2000 rulebase with the freshly installed default config files.

Step 1 : copy old 4.1 files

On the newly installed machine create following directory using `mkdir /41bu.` In this directory copy the following files from the current 4.1 production management server:

- `In the $FWDIR/conf directory:`

```
   objects.C
   rulebases.fws
   fwauth.NDB*
   fgrulebases.fws (if exists)
   xlate.conf (if exists)
   aftpd.conf (if exists)
   smtp.conf (if exists)
   sync.conf (if exists)
   masters (if exists)
   clients (if exists)
   fwmusers (if exists)
   gui-clients (if exists)
   slapd.conf (if exists)
   serverkeys (if exists)
   product.conf (if exists)
```

- `In the $FWDIR/database directory`

```
   InternalCA.DB (if exists)
```

Step 2 : Automatic upgrade with the upgrade-utility from Check Point.

- Download the upgrade utility from www.checkpoint.com. Untar the file `upgrade_53015.tar` using the command

  ```
  tar –xvf upgrade_53015.tar
  ```

  It uncompresses into a directory named `/upgrade`.
- Copy the content of the back-up directory `/41bu` to `/upgrade/4.1`
- Stop the FireWall-1

  ```
  Cpstop
  ```

- Go to `/upgrade` using `cd /upgrade,` make sure your shell is csh, and issue:

  ```
  chmod 755 upgrade.csh
  ./upgrade.csh /upgrade FP3> /upgrade/upgrade.txt 2>&1; tail -3
  /upgrade/upgrade.txt

  (Type the previous command on 1 line)
  ```

- **CONTINUE ONLY if the result gives "`upgrade completed !!!`" (this might take a moment). If the result is different, skipp what follows, and contact IT-security**

- The upgrade script will backup any modified file into `/upgrade/backup/` .

Step 3: Use the Post-Upgrade Verifier to correct posible errors generated during the upgrade.

- Go to the root-directory.

  ```
  cd /
  ```

- Create a back-up directory

  ```
  mkdir ngFP3bu
  ```

- Back up the merged configuration using the command

  ```
  cp –r $FWDIR/conf/* /ngFP3bu
  ```

  and check the new configuration with Post Upgrade Verifier script:

  ```
  ./post_upgrade_verifier $FWDIR
  ```

- Issue

  ```
  Cpstart
  ```

  to start G FP3.

A connection with the management-server using the NG GUI will be set up according to the new connection method described in "`Establishing a Secure Initial Rulebase with NG FP1 (3/3/2002)`" downloadable from the Checkpoint site. If the configuration is OK, the installation can continue with the next steps.

3. Installation of a secondary Management Server

You install the NG FP3 management station by using the CD Wrapper. This is done using the following steps:

- Insert the CDROM “Check Point NG FP3” in the CDROM drive,
- Change the directory using

```
cd /etc/rc2.d/
```

- and start volume management using

```
./noS92volmgt start
```

- Perform a

```
volcheck
```

- Go to the UNIX directory of the CDROM using

```
cd /cdrom/cp_ng_FP3
```

and run

```
./UnixInstallScript
```

- This program will guide you through the installation process. Use “`n`” to go to the next screen.
- Press SPACE to read the license agreement and enter “`y`” to accept it.
- Once the install script has completed the SVN foundation installation, the next step is to select the products that you want to install from this CD. You’re going to type “`1`” to select `“VPN-1 & FireWall-1”,` then enter “`n`” to advance to the next screen.
- Next you will need to select the type of firewall installation you want on this server. Enter “`2`” to select Enterprise Management, and then press “`n`” to continue.
- Enter “`2`” to select Enterprise Back-up Management, and then press “`n`” to continue.
- You will be asked if you want to install with or without backward compatibility for 4.1. Enter “`1`” for “`YES`” and press “`n`” to continue. The installation starts.
- When asked to enter a license press “`n`”.
- Next you will need to select the type of firewall installation you want on this server. Enter “4” to select “Enterprise Secondary Management”, and then press “`n`” to continue.
- You will be asked if you want to install with or without backward compatibility for 4.1. Enter “`1`” for “`YES`” and press “`n`” twice to continue.
- When asked to enter a license press “`n`”.
- Press “`Return`” for no group permissions and confirm with “`y`”.
- Type random letters to initialize the Random Pool. When the bar is full you can stop.
- Activate the SIC (Secure Internal Communication) by entering 2 times the following activation key:

```
Abc123
```

- You will be asked if you want to start the FW & VPN modules: press `“y”` ,
- After starting you will asked to press `<enter>` to finish the script and return to the prompt.

Ask the IT-Security department to connect to the Secondary Management Station and to control the proper working of SIC on the Primary Management Server.

The following step is to copy the Internal CA from the primary to secondary Management Server by copying following files in the `$FWDIR/conf` directory:

```
InternalCA.p12
InternalCA.NDB*
ICA.crl
InternalCA.crl (if present)
```

In the `$FWDIR/conf` directory also copy the `crls` directory containing 2 files:

```
ICA_CRL0.crl
ICA_CRL1.crl
```

- Reboot the computer using:

```
Init 6
```

4. Installation of Hotfix 2 and HFA322 on the Primary and Secondary Management Server

Hotfix 2 for Checkpoint NG FP3 can be installed using the Secure Update function from the management station or through a local install.
If the automated deployment using Secure Update wouldn't succeed a local install need to be done.

The 2 files needed for the Hotfix 2 local installation are:

```
SU_cpshared_NG_FP3_HF2_sol.tgz
SU_fw1_NG_FP3_HF2_sol.tgz
```

Copy both files to your `$HOME` directory of the new management station and unzip the file using

```
gunzip ./ SU_cpshared_NG_FP3_HF2_sol.tgz
```

and untar the files using

```
tar -xvf SU_cpshared_NG_FP3_HF2_sol.tar
```

First SVN foundation needs to be updated running

```
./cpshared_HF2_53957_4
```

When asked to press "y".

Second run the FW installation update script using

```
./fw1_HF2_53945_1
```

Run `cpstart`

Also install HFA-322 like described in the release notes. (same procedure as for HF2)

You should have the following build numbers after successfully installing the hotfixes:

```
cpman1[FWADMIN]:/export/home/FWADMIN# fw ver –k

This is Check Point VPN-1(TM) & FireWall-1(R) NG Feature Pack 3 Build
332253945.

cpman1[FWADMIN]:/export/home/FWADMIN# cpshared_ver

This is Check Point SVN Foundation (R) Version NG Feature Pack 3 Build
332253958
```

5. Migration of the Nokia-Modules

5.1. Installing IPSO3.7.1 & CP NG FP3.

Make sure the NSP (Nokia Security Platform) can be managed using the Voyager Management tool on port https (443) and using SSH, which is a standard component of IPSO. SSH & certificate authentication (https) can be activated using Voyager.

An account has to be created for the members of IT-security allowing read/write access using SSH to edit and change the FW config files on the NOKIA platform.

Before starting the new installation perform a `fwstop` to stop the fw service.
To start the installation on the NSP first deactive the CP2000 package using the Voyager webbased Management interface.

Download the ipso.tgz from IPSO3.7.1 build4 into your home directory `$HOME` into a new directory

```
/IPSO371/
```

Execute the following command:

```
newimage –k –l $HOME/IPSO371/
reboot
```

Deactivate the previous active IPSO image and activate IPSO371build4. Next delete the images older than the CURRENT active one, before starting the installation of CP NG FP3 to free up some space. Reboot the machine before proceeding.

Copy NGFP3 to your `$HOME` directory on the Nokia boxes.

Execute the following command in command shell:

```
newpkg -m LOCAL -n $HOME/CPNGFP3/CP_FP3_IPSO.tgz
newpkg -m LOCAL -n $HOME/IPSO371/nic-doc3.7.1tgz
reboot
```

After the reboot check that the new packages (SVN FP3 & FW FP3) are activated using Voyager. The CPNG module needs to be configured using `cpconfig` before installing the patches:

- You will be asked to read the license agreement and to hit `“SPACE”` to continue reading,
- When asked to accept the license agreement press `“y”`,
- When asked which module you want to install press `“1”` for VPN-1 & FireWall-1 Enforcement Module,
- Then you will be asked if you want to install HA. Press “y” (clustering),

- When asked to add licence press `“n”`. The license will be pushed from the Management station after the SIC (Secure Internal Communication) is activated successfully,
- When asked to create a group name for group permissions press `“ENTER”` for no group permissions,
- When asked to confirm this setting press `“y”`,
- You will be asked to created a random pool by hitting random keys on your keyboard until the bar is full,
- Activate the SIC by entering 2 times the following activation key:

```
Abc123
```

- When the intial policy (allows only CP traffic) is compiled you will be asked to `reboot` by pressing `“y”`,
- After the reboot ask IT-Security to control SIC on the management server by testing connectivity, pushing the license and installing the policy.

5.2. Installing HF2 & HFA322.

Hotfix 2 for Checkpoint NG FP3 should be installed using the Secure Update function from the management station or through a local install .

If the automated deployment using Secure Update wouldn’t succeed a local install need to be done.

The 2 files needed for the Hotfix 1 local installation are:

```
SU_cpshared_NG_FP3_HF2_ipso.tgz
SU_fw1_NG_FP3_HF2_ipso.tgz
```

Copy both files to your `$HOME` directory of the new management station and unzip the file using

```
gunzip ./ SU_cpshared_NG_FP3_HF2_ipso.tgz
```

and untar the files using

```
tar -xvf SU_cpshared_NG_FP3_HF2_ipso.tar
```

First SVN foundation needs to be updated running

```
./cpshared_HF2_53957_4
```

When asked to press “y”.

Second run the FW installation update script using

```
./fw1_HF2_53945_1
```

Run `cpstart`

Also install HFA-322 like described in the release notes (same procedure as for HF2)

You should have the following build numbers after successfully installing the hotfixes:

cpman1[FWADMIN]:/export/home/FWADMIN# `fw ver –k`

```
This is Check Point VPN-1(TM) & FireWall-1(R) NG Feature Pack 3 Build
332253945
```

```
cpman1[FWADMIN]:/export/home/FWADMIN# cpshared_ver

This is Check Point SVN Foundation (R) Version NG Feature Pack 3 Build
332253958
```

6. Additional Tools

An additional debugging tool “Cpinfo” needs to be installed on both the management server and the modules. The tool can be found at the Checkpoint support site.

Gunzip the appropriate file: `cpinfo_sol.gz` for solaris and `cpinfo_ipso.gz` for IPSO, and copy it to `$FWDIR/bin`.

To make the file executable change the rights of cpinfo using:

```
      chmod 700 cpinfo
```

Once Secure Internal Communication is configured on the modules and in the Nodes object via the NG FP3 Management Server GUI, the communication between the modules and the management server will be tested. If this is OK, the policy will be installed and the proper working will be verified.

7. reference material

MAIN SOURCES

Source Document Summary Information
[1] “Solaris 8 packages required for VPN-1/FireWall-1 NG” from CheckPoint Technologies Ltd.
[2] “How to remotely upgrade to CheckPoint NG FP1” from CheckPoint Technologies Ltd.
[3] “CheckPoint Security Servers hotfix 2 Version NG FP3 Release Notes” from CheckPoint Technologies Ltd.
[4] “CheckPoint Entreprise Suite NG FP3 Release Notes” from CheckPoint Technologies Ltd.
[5]