Upgrading a Checkpoint 4.1 (2000) Enterprise Management Console to NG FP3

Prerequisites/Assumptions

- This document will focus on Solaris 8.0 UltraSPARC as the platform for NG (Solaris 2.7 is not supported in FP3)
- **Production** platform running Checkpoint 4.1(2000)
- **Duplicate** platform running Solaris 8, pre-patched to be ready for NG (see below).
- Have all your software licenses ready for the production and duplicate machines
- For the latest pre-requisites: Visit: http://www.checkpoint.com/ng/fp3

NG requires the following Patches under Solaris 8 UltraSPARC

109147-18
108528-06
109326-07
32-bit: 108434-01
64-bit: 108435-01

To verify you have the patches installed, use: showrev -p | grep <patch number>

After Installation:

VPN-1/Firewall Build # will be: 53225 (check with $FWDIR/bin/fw ver)
SVN Foundation Build # will be: 52267 (check with $CPDIR/bin/cpshared_ver)

After you have built the duplicate machine O/S to NG FP3 specs:

1. Install Checkpoint 4.1 (2000) on the duplicate machine with the same features and service pack levels as the production machine. You may require the original Solaris Checkpoint 4.1 install CD. Verify you have connectivity to it, can log in with the GUI client, and see all your rules and objects.
2. On the production (4.1) machine, tar up the **$FWDIR/conf** directory & gzip it. Tar up the **$FWDIR/database** directory. FTP/transfer both the tar.gz files to /tmp (or elsewhere) on the duplicate machine.
3. On the duplicate machine, untar both the tar.gz files into separate folders.
4. On the duplicate machine, perform a **$FWDIR/bin/fwstop**.
5. From the $FWDIR/conf folder you unzipped, copy the following files to $FWDIR/conf:

rulebases.fws
objects.C
fwauth.NDB*
masters (if exists)
clients (if exists)
gui-clients (if exists)
*.W files (if exists)
product.conf (if exists)

6. From the $FWDIR/database folder you unzipped, copy the following files to $FWDIR/database:

   InternalCA.DB (if exists)

7. Restart the Checkpoint Software: **$FWDIR/bin/fwstart.**

1. Verify you have connectivity to it, can log in with the GUI client, and see all your rules and objects.

   - **At this stage, you have produced a Mirror of your existing production 4.1(2000) machine on the duplicate machine.**
   - **You are now ready to complete the presteps that will be required for NG FP3.**

Pre-Upgrade to NG: Running the Checkpoint Upgrade Verifiers

1. Download **upgrade_checker_B53061_1_solaris.tar.gz** (CP Upgrade Utilities) from the Checkpoint website.

2. FTP/transfer them to the duplicate machine. Unzip and untar the file in the $FWDIR/conf directory.

3. Change to $FWDIR/conf & run the executable: pre_upgrade_verifier with the following flags:

```
./pre_upgrade_verifier -p MngPath  -c CurrentVersion -t TargetVersion -f file
```

-p: specify path to $FWDIR on the duplicate machine
-c: 4.1
-t: NG_FP3
-f: results.txt (you can call this whatever you want)

4. After you execute this program, it will produce a file called results.txt. Download that file to your PC.

5. The file lists Errors & Warnings that must be fixed **prior** to upgrading to NG. You need to fix all issues identified. Errors must be fixed, warnings will need to be addressed immediately after the upgrade. It is strongly recommended you fix everything in this file or be prepared for the consequences of a failed upgrade.

6. Go into your policy on the duplicate machine to fix the items, save your changes, and re-run pre_upgrade_verifier with a differnet filename each time to see the differences. When you see no more errors/warnings you are ready for the final upgrade to FP3.

Upgrade to NG: After pre-upgrade verification has passed

1. You are now ready to finally upgrade to NG FP3. Download the NG FP3 file appropriate for Solaris 8 to the duplicate system, or have the CD ready.

2. Have all your software licenses ready for the production and duplicate machines

3. Start the NG FP3 Install. We will be doing an **Upgrade option.** The program should auto-detect you have the 4.1 code installed and will automatically continue. If you have an option to select **U(pgrade)** now, then do it.

4. Enter your licenses as required, NG will have you generate a Certificate, etc. Go through as prompted.

5. When the install finishes, you may need to log-out of the duplicate system and back in again to source the new environment variables necessary for NG.

6. Stop the NG code: **$FWDIR/bin/cpstop**, or just type: **cpstop**

7. Change to $FWDIR/conf and run: ./`post_upgrade_verifier management_path`

   Where management path is probably: /var/opt/CPfw1-53/

8. This will validate the integrity of the environment and make a few DB fixes.

9. Restart the NG code: $FWDIR/bin/cpstart, or just type: **cpstart**

10. Use the SMART Dashboard NG FP3 to connect to the duplicate machine.

11. Verify you have connectivity to it, can log in with the GUI client, and see all your rules and objects.

12. If you can't sign in, run "cpconfig" and select "Administrators" and ensure your ID exists.

At this point, you have completed the upgrade. Validate your environment, rules, and objects.
Do a verification Policy install. If you get errors, clean up. You may have to go into your FW objects, edit them and uncheck VPN-1, (by default this is checked) and can generate policy install errors. Just leave Firewall-1 checked.

14. If you still have problems, you might have to do: **fwm sic_reset** to regenerate a new CA on the duplicate machine. Please refer to this Phoneboy Link:

    http://www.phoneboy.com/fom/fom.pl?_highlightWords=sic&file=165

    - If you are still have problems, you might want to call Checkpoint support or VAR.

Phase II: Upgrading the NOKIA IP Platform to NG FP3.

1. FTP the appropriate NG FP3 IPSO package for your IPSO platform into */var/admin* on the Nokia appliance.
2. On the Nokia, run: **newpkg -i** and follow instructions to install from local filesystem
3. After the package has been installed, you can delete the original ftp file (CP_FP3_IPSO.tgz)
4. Turn OFF the old 4.1 (2000) package, turn ON the new package.
5. Run "**cpconfig"**
6. **Be sure to Install this package on BOTH gateways**

Welcome to Check Point Configuration Program
==========
Please read the following license agreement.
Hit 'ENTER' to continue...

This End-user License Agreement (the "Agreement") is an agreement between you (b
oth the individual installing the Product and any legal entity on whose behalf s
uch individual is acting) (hereinafter "You" or " Your") and Check Point Softwar
e Technologies Ltd. (hereinafter "Check Point").

<snip, snip> the author

Do you accept all the terms of this license agreement (y/n) ? **y**

---
(1) VPN-1 & FireWall-1 Enterprise Primary Management and Enforcement Modulere th
(2) VPN-1 & FireWall-1 Enforcement Module
(3) VPN-1 & FireWall-1 Enterprise Primary Managementn applies to Product acquire

Enter your selection (1-3/a-abort) [1]: **2**

Would you like to install a Check Point clustering product (CPHA, CPLS or State
Synchronization)? (y/n) [ ] ? **no**

IP forwarding disabled

Hardening OS Security: IP forwarding will be disabled during boot
Generating default filter

At any later time, you can reconfigure these parameters by
running cpconfig

Configuring Licenses...
==========
Host Expiration Features

Note: The recommended way of managing licenses is using SecureUpdate.
This window can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [y] ? **y**

Do you want to add licenses [M]anually or [F]etch from file: **M**
IP Address: **eval**
Expiration Date: **01Aug2002**
Signature Key: **dhwAhULoQ-Fbp24AjYV-ba2B9wzjs-r5HYNbK6g**
SKU/Features: **CPMP-EVAL-1-3DES-NG CK-CP**

License was added successfully

License will be put into kernel after cpstart

Configuring Groups...
==========
Check Point access and execution permissions

Usually, a Check Point module is given group permission
for access and execution.
You may now name such a group or instruct the installation

Please keep typing until you hear the beep and the bar is full.

[**.....**]

Thank you.

Configuring Secure Internal Communication...
==========
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized
Enter Activation Key: **password**
Again Activation Key: **password**

The Secure Internal Communication was successfully initialized

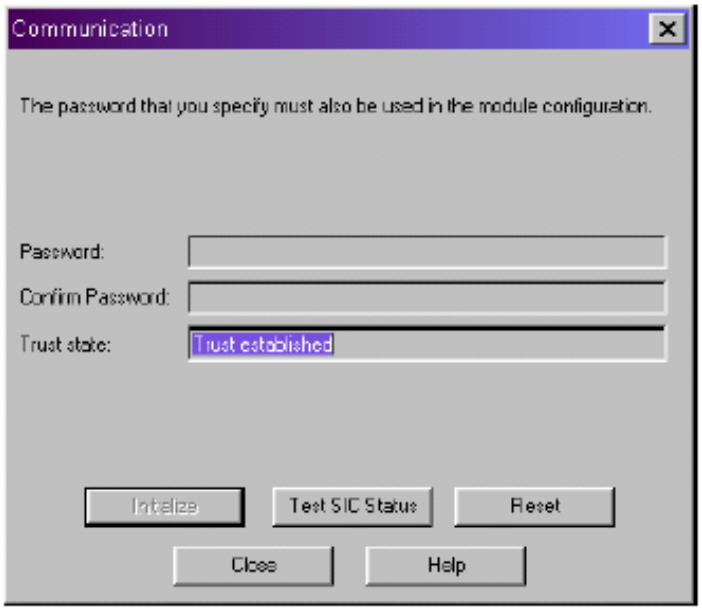
initial_module:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed

In order to complete the installation of module
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? **y**

On the Management Station (duplicate machine)

1. Unload the default NG filter policy on both gateways first: **fw unload localhost**
2. Create a workstation object defining the Management Station.
3. When you are finished, it will auto-gen a certificate to be used for SIC. SIC replaces Putkeys used in 4.1
4. Go to the Firewall object you had created, under General Properties, click the **Communications** tab



5. If you receive an error "Error: Failed to connect to module" perform the following:

   - On FW module machine, use **cpconfig** to re-initialize SIC and enter a new password
   - In the Policy Editor, in the **Communication** window of the module object, **Reset** SIC communication
   - Re-initialize SIC by typing the same password as used on the FW module.
   - Verify SIC status by pushing the button: **Test SIC Status**

6. Edit the FW Modules. Click "Get Topology" to obtain interface configuraiton.

7. **Configure Anti-Spoofing for both FW modules.**

8. Install the Policy to the FW modules.

This completes the 4.1 to NG FP3 Migration

Email: karimi@ca.ibm.com