Procedure to migrate a Checkpoint NG management station with multiple rulebases to a Provider-1 server with multiple CMA's

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

Table of Contents

DOCUMENT CONTENT

1. Introduction

This document describes the procedure to migrate the Firewall-1 software on the management-server from CheckPoint Firewall-1 Next Generation Feature Pack 3 Hotfix 2 (NG FP3-HF2) HFA 322 to a multi site Checkpoint Provider1 FP3-HF2 HFA322 management environment. For the installation of the software on the MDS (Multi domain Server), new hardware must be used.

2. Installation of the primary management server to a provider-1 MDS (Multi Domain Server)

2.1. Minimum system Requirements

The Check Point Provider-1 FP3 MDS server needs to be a Solaris 8-9 (64 bit), with a minimum of 20 GB disk and 256 MB memory (512 MB recommended).
The Solaris system must be properly patched to allow Check Point FireWall-1 to function properly and the presence of the following patches and packages should be checked:

- `109147-18`
- `108528-06`
- `109326-07`
- `108434`
- `108435`
- `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 OS needs to be stripped using the earlier defined procedure. SSH and 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 IT-Security.

2.2. Install Procedure

Copy the MDS file `mds_release_fp3_pr29_solaris2.tgz` to $HOME
Unzip and untar the installation file:

```
gunzip mds_release_fp3_pr29_solaris2.tgz
tar -xvf mds_release_fp3_pr29_solaris2.tar
```

To start the installation, run the script `./mds_install`. To do so, you must have superuser permissions. Answer the questions presented by the installation scripts. When questioned about which type of installation you want to perform, press `3 Provider-1 MDS+container`. You will be asked if this is a Primary MDS press `Y.`It is possible to abort the installation at any time.

At the end of the installation, the configuration utility `mdsconfig` is activated, and you will be prompted to specify necessary information.

The information specified can be modified later, by running the `mdsconfig` utility manually.
To start the MDS, run the script `mdsstart.`

3. Installation of a back-up Provider-1 MDS server

Copy the MDS file `mds_release_fp3_pr29_solaris2.tgz` to $HOME
Unzip and untar the installation file:

```
gunzip mds_release_fp3_pr29_solaris2.tgz
tar -xvf mds_release_fp3_pr29_solaris2.tar
```

To start the installation run the script `./mds_install`. To do so, you must have superuser permissions. Answer the questions presented by the installation scripts. When questioned about which type of installation you want to perform, press `3 Provider-1 MDS+container`. You will be asked if this is a the Primary MDS press `N.`It is possible to abort the installation at any time.

At the end of the installation, the configuration utility `mdsconfig` is activated, and you will be prompted to specify necessary information.

The information specified can be modified later, by running the `mdsconfig` utility manually.
To start the MDS, run the script `mdsstart.`

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

Hotfix 2 for Provider-1 NG FP3 can be installed using the Secure Update function from the management station (this is performed by IT-Sec) or through a local install.
If the automated deployment using Secure Update wouldn't succeed a local install need to be done.

The file needed for the Hotfix 2 local installation is:

```
mds_Hf2_6.tgz
```

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

```
      ./mds_Hf2_6.tgz
```

and untar the files using

```
      tar -xvf mds_Hf2_6.tar
```

Run the MDS installation update script using

```
      ./install_hf
```

Run `reboot`

Then install HFA322:

The file needed for the Hotfix 2 local installation is:

```
      mds_HFA_322_provider.tgz
```

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

```
      ./mds_HFA_322_provider.tgz
```

and untar the files using

```
      tar -xvf mds_Hf2_6. mds_HFA_322_provider.tar
```

Run the MDS installation update script using

```
      ./install_hf
```

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

```
      fw ver
```

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

```
      cpshared_ver
```

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

5. Migration of the CP management station rulebase to a CMA (Customer Management Add-on) on the Primary & Secondary MDS.

5.1. Migrating the Checkpoint Rulebase

First allow CPMI traffic on original Management station to the prime and back-up MDS and CMA.
In each CMA revoke all SIC communication and delete the modules which will not be managed by the CMA.

Provider-1 offers a CMA Migrate function, which allows to importing existing Management servers running 4.1 and NG into the Provider-1 environment.

First copy the following directories from the existing management server to $HOME on the MDS servers:

```
provmds1[ADMINUSER]:$CPDIR/conf
provmds1[ADMINUSER]:$CPDIR/database
```

Rename the Cpshared `conf` directory to `conf.cpdir`
Rename the Cpshared `database` directory to `database.cpdir`

Then copy the following directories from the existing management server to $HOME on the MDS servers:

```
provmds1[ADMINUSER]:$FWDIR/conf
provmds1[ADMINUSER]:$FWDIR/database
provmds1[ADMINUSER]:$FWDIR/log
```

In a newly created CMA (NOT yet started) import the CMA by entering $HOME when the MDG asks for a path.

On the newly created CMA delete all IKE certificates for the modules you will control in the current CMA, using the GUIdebit utily. Search for the network object and reset certificate.

Reset the ICA on all CMA using following procedure:

```
Change  the  environment  variables  to  the  appropriate  customer
(container name) using the command:

mdsenv <customername>
check the change with cd $FWDIR
perform fwm sic_reset
***************** Warning: ****************
This operation will reset the Secure Internal Communication (SIC).
The internal Certificate Authority will be destroyed and Check
Point Components will not be able to communicate.
You will have to perform the following operations to enable
communication:
1. Re-initialize the internal Certificate Authority (use cpconfig).
2. Restart Check Point Services (cpstart, cpridstart).
3. Reset SIC on each Station that is managed by this SmartCenter
Server.
4. Re-establish Trust with each Station that is managed by
   this SmartCenter Server.
*******************************************
This operation will stop all Check Point Services (cpstop)
Are you sure you want to reset? (y/n) [n] ? y

*** Checking IKE Certificates ***

*** Stopping services ***
Stopping CMA Services...
Stopping fg-1 for CMA <customername> <customer_ip>
Cannot get pid of fgd: No such file or directory
Stopping fw-1 for CMA <customername> <customer_ip>
VPN-1/FW-1 stopped
Stopping CPshared for CMA <customername> <customer_ip>
CPD stopped
```

```
*** Destroying internal Certificate Authority ***

*** Updating objects database ***

SIC Reset operation completed successfully
```

Recreate a new ICA

```
provmds1[ADMINUSER]:/opt/CPmds-53/customers/<customername>/CPfw1-
53# $MDSDIR/bin/mdsconfig -ca <customername> <customer_ip>

Internal Certificate Authority created successfully Certificate was
created successfully
Setting FQDN to: <customer_ip>
Executing "/opt/CPshrd-53/bin/cp_conf ca fqdn <customer_ip>" in
order to set FQDN
Trying to contact CA. It can take up to 4 seconds...
FQDN initialized successfully
The FQDN was successfully sent to the CA
Executing "/opt/CPshrd-53/bin/cp_conf ca fqdn <customer_ip>" in
order to set FQDN - Done
CA initiation ended successfully!
The following text is the fingerprint of this Management machine:
TRAM BIT RUBY GAP DUET GUS DOW WELT CHUB VEND AIDA HOBO
```

Once this is done check the connectivity and the rulebase and try to recreate certificate for the users and the Checkpoint objects used in VPN's.

5.2. Changing the rulebase in each CMA of the Provider-1 MDS

In each rulebase of every CMA allow management traffic between the CMA+MDS and the managed modules.

5.3. Synchronizing the Primary MDS to the back-up MDS.

Mirror primary MDS to secondary MDS:

```
mdscmd mirrorcma -s <Primary MDS> -t <Secondary MDS>
```

5.4. Modifying the base.def and user.def files on the new MDS servers for FTP and syn drops

Changes to be executed in every `base.def` file on the MDS server:

Backup the $FWDIR/lib/base.def in every CMA on the MDS server
Edit the $FWDIR/lib/base.def on the management server and make the following two changes:

1. Allowing CP NG to recognize the PORT command in an FTP request without an EOL (end of line):

Find the following line:

```
#define FTPPORT(match) (call KFUNC_FTPPORT <0x1|(match)>)
```

and change it to be:

```
      //#define FTPPORT(match) (call KFUNC_FTPPORT <0x1|(match)>)
```

Then, find an un-remark the following line:

```
      //#define FTPPORT(match) (call KFUNC_FTPPORT <(match)>)
```

will change to be

```
      #define FTPPORT(match) (call KFUNC_FTPPORT <(match)>)
```

Comment out:

```
      #define FTP_ENFORCE_NL
```

which will become

```
      // #define FTP_ENFORCE_NL
```

2. For FTP (to allow data connections using high TCP ports - above 1024):

Edit the lines:

```
define NOTSERVER_TCP_PORT(p) {
(not is_version_at_least(FP2_VER), NOTSERVER_TCP_PORT_BC(p))
or
(is_version_at_least(FP2_VER), call KFUNC_NOTSERVER_PORT<p, PROTO_tcp>)
};
```

Change them to:

```
/* INSPECT modification - sk11922 */
define NOTSERVER_TCP_PORT(p) {not SMALL_PORT(p)};
/* End of INSPECT modification */
```

Changes to be executed in every `user.def` file of the MDS server:

Add the following line:

```
deffunc user_accept_non_syn() { dport = 80 or dport = 443 or dport = 8080
or dport = 33000 };
```

5.5. Changing rulebase on the original Management Station to allow MDS and CMA traffic.

On the original management station add all CMA and MDS addresses in the management group and reinstall rulebases. This will allow management traffic between the modules and the new Provider-1 MDS servers.

Otherwise you won’t be able to perform the SIC reset of the next step.

5.6. Performing SIC reset on all modules and CMA’s

Perform a SIC reset on every modules using `CPCONFIG`. This will restart the FW with its initial policy. Perform this SIC reset in every CMA for each managed module.

Test the SIC communication in the GUI and install the rulebase on every module.

6. Additional Remarks

Don’t gorget to test the switch over to the back up CMA’s and to install the policies. This will activate the logging on the backup CMA’s and test the HA setup of the MDS servers.

7. Adding a new CMA

See manual chapter “Adding new CMA”

8. reference material

MAIN SOURCES

Source Document Summary Information
[1] “Solaris 8 packages required for VPN-1/FireWall-1 NG” from Check Point Technologies Ltd.
[2] “Check Point Provider-1/SiteManager1 Part1 & Part2” from Check Point Technologies Ltd.
[3] “Check Point Provider-1/Sitemanager-1 NG FP3 HF2 Release Notes” from Check Point Technologies Ltd.
[4] “Check Point Provider-1/Sitemanager-1 NG FP3 HFA322 Rel. Notes” from Check Point Technologies Ltd.
[5] “Managing Multiple Customer Sites Using Provider-1 NF FP3” from Check Point Press