

Check Point Software Technologies LTD.ä

How to Customize CP HA Fail-over on NT

Date: June 20, 2000

Revision 1.0

Author: Barak Dabush, Project Manager

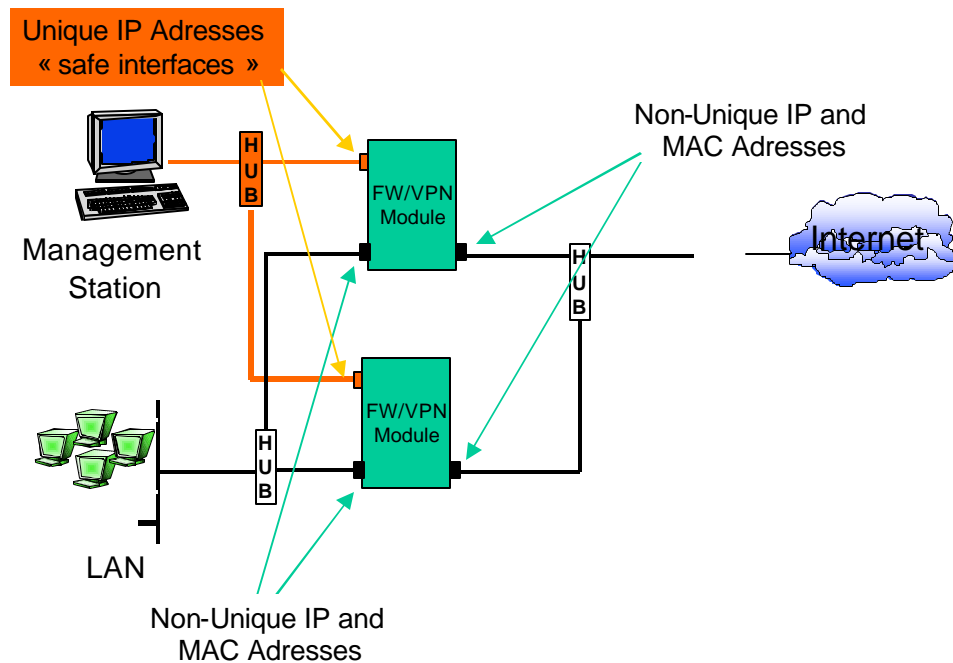
Laurent Petroque, Regional Technical Consultant, South Europe

Jerome Breton, Regional Technical Consultant, South Europe

Goal of the Demo:

- Use cphaprob to customize fail-over of Check Point HA Module (CP2000) on NT
- 2 examples :
 - force fail-over for maintenance purpose.
 - force fail-over when disk space is not enough.

Network Diagram:



Necessary Equipment:

- NT 4.0 Ressource Kit

One of the advantage of a software HA solution vs a hardware (boxes, VRRP) is the fact that we can test several parameters on the machine to declare it available or not ; with a software HA solution, we are not limited to test interface state or TCP/UDP port availability.

Check Point High Availability module gives the ability to define any kind of parameter (Hard Disk space, process running...) to be critical for the machine ; according to those critical parameters, the fail-over will occur. This can be done by using cphaprob command.

The 2 examples below are given for instructive purpose only.

cphaprob command :

cphaprob command is documented in "VPN-1 / FireWall-1 Administration Guide", Chapter 16 p.563 (CP2000 version) available at :

<http://www.checkpoint.com/support/technical/documents/index.html>

Here is a extract :

```
cphaprob -d <device> -t <timeout(sec)> -s <ok|init|problem> register
cphaprob -d <device> unregister
cphaprob -a unregister
cphaprob -d <device> -s <ok|init|problem> report
cphaprob [-i[a]] [-e] list
cphaprob state
cphaprob [-a] if
```

-d <device>	Add <device> to the list of devices that must be running for the VPN/FireWall Module to be considered active (in other words, if <device> fails, then the VPN/FireWall Module is considered to have failed)
-s	The status to be reported — one of: ■ "ok" — <device> is alive ■ "init" — <device> is initializing (the machine is down) ■ "problem" — <device> has failed
-t	<timeout> If <device> fails to contact the VPN/FireWall Module in <timeout> seconds, <device> will be considered to have failed. To disable this parameter, enter <0> as the timeout value.
register	Register <device> as a critical process.
unregister	Unregister <device> as a critical process.
state	Display the state of this VPN/FireWall Module and all the other VPN/FireWall Modules in the High Availability configuration.
-i[a] -e list	Display the state of devices.
report	Report the status of High Availability VPN/FireWall Modules and their status.
if	Display the state of interfaces.

For example:

```
> cphaprob.exe -d DiskMon -t 10 -s ok register
```

will register the device named "DiskMon" with a 10 seconds timeout. It means that the HA module will fail the machine if not getting an OK status report from this device at least every 10 seconds. To report an okay status, the device (the third party program) should report by

```
> cphaprob.exe -d DiskMon -s ok report
```

Or when the program detects that the disk is full it can cause a fail-over by reporting a "problem" status (so the module will not wait 10 seconds).

The time out is not mandatory and any program can report a "problem" status at any given time (and to cause a failover), but registering with timeout will enforce the critical process (in this example the disk monitor) to report (imagine that this process dies).

By default, Check Point HA module is using this mechanism to check fwd state (every 2 seconds), and watch that the policy is loaded and that the sync works.

Example 1 : Forcing fail-over for maintenance purpose.

Create the following ha.bat file :

```
@echo OFF
IF %1==FAIL GOTO FAIL
IF %1==UP GOTO UP
echo "usage : ha FAIL|UP"
GOTO END
:FAIL
cphaprob.exe -d ForcedFailOver -s problem report
GOTO END
:UP
cphaprob.exe -d ForcedFailOver unregister
GOTO END
:END
```

This batch file has to reside on a FireWall-1/VPN-1 module. Make sure that `cphaprob.exe` is in the PATH.

Command `ha FAIL` will report an error for device " ForcedFailOver".
The fail-over will occur, and maintenance can be done on the machine.

Command `ha UP` will unregister device " ForcedFailOver", and the module will be available again if "Return Control to the highest priority ready machine" was checked in Check Point Configuration tool of the module.

Note that a "fwstop" command will also force the fail-over... (but the module will appear with an unknown status on the Status Viewer).

Example 2 : Forcing fail-over if free disk space is too low.

This example requires the two executables `sleep.exe` and `freedisk.exe` (available in NT4 Ressource Kit).

Create the following `diskfree.bat` file :

```
@echo OFF
REM cphaprob.exe -d FreeSpace unregister
:START
cphaprob.exe -d FreeSpace -t 30 -s ok register
:CHECKSPACE
freedisk C: 1400000000
if errorlevel 1 goto NOTENOUGH
cphaprob.exe -d FreeSpace -s ok report
SLEEP 20
GOTO CHECKSPACE
:NOTENOUGH
cphaprob.exe -d FreeSpace -s problem report
:BYE
```

This batch file has to reside on a FireWall-1/VPN-1 module. Make sure that `cphaprob.exe`, `sleep.exe` and `freedisk.exe` are in the PATH.

Second line of the batch is optional.

First action is to register device "FreeSpace", with a timeout of 30 seconds. If the batch process dies, the fail-over will occur within a period of 30 second maximum.

Then we check the disk space (here we want to force the fail-over if free disk space is lower than 1,400,000,000 bytes), and report an "ok" to "FreeSpace" every 20 seconds if free disk space is enough.

If free disk space is not enough, we report an error to "FreeSpace", causing the fail-over to occur.