FireWall-1 Management Stations

The FW-1 Management Stations can be configured to provide redundancy in the event of a failure.

Note: Although this redundancy solution is based upon a Check Point document, Check Point do not support this configuration. There are a number of caveats and management processes that must be adhered to for it to work.

The management stations are configured as primary and secondary. It is important that under normal operation, all management of the firewalls is carried out via the primary management station - the secondary should only be used when the primary has failed. When a policy or user database is downloaded from the primary management station to the firewalls, then the updated files are automatically transferred via FTP to the secondary firewall. Therefore if the primary management station fails, then the secondary will have up to date copies of both the rulebase and the user database, and management can be carried out via the secondary, until the primary is back online again.

Restrictions

- All management must be carried out via the primary management station
- In the event of a failure, management can be carried out from the secondary management station, but any changes made must be manually transferred back to the primary - either by file copy, or else by applying the same changes to the primary rulebases.
- For the user database to transfer successfully, the FireWall-1 service on the secondary must not be running. This is because the fwauth.NDB* files are held open by the FireWall-1 service, and any changes will not be picked up. Therefore the FireWall-1 files are copied over into temporary holding directories on fwmngr02. A separate script runs every 15mins to see if any files have been transferred over. If so, then the FW-1 service is stopped on fwmngr02, the files moved from the temporary directories to the correct FW-1 directories, and then the FW-1 service is restarted. If no new files have been transferred over then the script will exit without doing anything
- The FTP script used to transfer the files has no error handling built in. It is the responsibility of the person installing the rulebase to check the log output to ensure that all of the files have transferred over successfully. FTP transfers can take a few minutes to complete, and the regular check for the updated files could easily overlap a transfer in progress. This would result in the secondary running the update batch file with an incomplete database. To overcome this, create a file called “ftpdone.txt” in the c:\winnt\fw directory containing some arbitrary explanation text. This file is then copied over last. It is this file that is checked for in the remote management server update batch file.

Configuration - fwmngr01

The primary management station (fwmngr01) has been configured to automatically copy the firewall configuration files via FTP to the secondary management station (fwmngr02) whenever a new firewall policy or user database is loaded.

This has been achieved by making the following changes to the file C:\winnt\fw\lib\setup.c on fwmngr01:

```
(
        :setup_version (300)
        :load_program ("C:\batch\hamgr.bat")      << ADDED
        :dbload_program ("C:\batch\hamgr.bat") << ADDED
        :has_iiicom (true)
```

The effect of these 2 lines is that whenever a new security policy or user database is downloaded, the script C:\batch\hamgr.bat will be executed. This script downloads the policy/user database to the firewall module, and then executes the FTP script c:\batch\ftpbits.txt

Note that when the FireWall-1 software is upgraded, these changes to setup.c will be overridden, and will have to be re-applied.

C:\batch\hamgr.bat

```
@echo off
C:\winnt\fw\bin\fw %1 %2 %3 %4 %5 %6 %7 %8 %9

echo Do not close window until files have copied over!!!
ftp -s:c:\batch\ftpbits.txt
echo Completed - check log output for errors
```

C:\batch\ftpbits.txt

```
open 10.x.y.z
fw1
***PASSWORD***
ascii
prompt
cd /conf
mput c:\winnt\fw\conf\*.*
bin
mput c:\winnt\fw\conf\fwauth.NDB*
ascii
cd /state
mput c:\winnt\fw\state\*.*
cd /db
mput c:\winnt\fw\database\*.*
cd ..
put c:\winnt\fw\ftpdone.txt
close
bye
```

Configuration - fwmngr02

The secondary management server has the Microsoft FTP Server installed and configured (subset of IIS V4.0). IIS requires that Microsoft networking is installed and running, However there is a requirement that the server is not visible to Microsoft clients on the internal network. This has been achieved by configuring the MS Loopback Adapter with an address of 12.0.0.1. Microsoft Networking has been bound to the loopback interface and removed from the Ethernet card.

The FTP server has been setup to only allow connections from the address 10.a.b.c (fwmngr01). The directory structure has been created thus:

C:\Firewall_transfer\

\conf

\state

\database

The default ftp login directory has been set to c:\firewall_transfer.

The following batch file, fwtxcfgs.bat, has been configured as a Scheduled Task to run every 15mins. This can be done using the at command thus;

at 07:00 /every: cmd /c c:\batch\fwtxcfgs.bat	run daily at 0700hrs
at 07:15 /every: cmd /c c:\batch\fwtxcfgs.bat	run daily at 0715hrs
at 07:30 /every: cmd /c c:\batch\fwtxcfgs.bat	run daily at 0730hrs

etc…..for every 15 minutes that it is required to run. Very tedious and clumsy to set up but it works and the author doesn’t know another way to do it!!! I ended up only running it during working hours, +/- 2 hours.

If ftpdone.txt exists in the c:\Firewall_transfer directory, then the rest of the script is executed, and the files are transferred over.

C:\batch\txfwcfgs.bat

```
rem Batch file to check for updated firewall configs
if not exist "C:\FireWall_transfer\ftpdone.txt" goto end

rem Need to shutdown the FW-1 Management server first
call c:\winnt\fw\bin\fwstop

rem Remove old user databases
del C:\winnt\fw\conf\*.ND*
del C:\winnt\fw\database\*.ND*
xcopy C:\FireWall_transfer\conf\*.* C:\winnt\fw\conf /c
xcopy C:\FireWall_transfer\state\*.* C:\winnt\fw\state /c
xcopy C:\FireWall_transfer\database\*.* C:\winnt\fw\database /c

rem Tidyup
del /Q C:\FireWall_transfer\conf\*.*
del /Q C:\FireWall_transfer\state\*.*
del /Q C:\FireWall_transfer\database\*.*
del /Q C:\FireWall_transfer\*.*

rem Restart FW-1 Management server
call c:\winnt\fw\bin\fwstart
:end
```

Adapted from various sources by Andy Kendall, Wincanton Logistics. andy.kendall@wincanton.co.uk