Check Point Based Firewalls

This configuration guide specifically focuses on Check Point firewall devices and those devices that run Check Point software such as Nokia IP and Crossbeam devices (collectively known as Check Point from this point on).

Check Point software can run on a variety of different operating systems and platforms. Nipper Studio requires a number of different configuration files from Check Point devices in order to perform the audit and these files can change between different configurations. This procedure will outline how to identify the configuration files that are required and how you can transfer them to your computer for processing with Nipper Studio. Ultimately, you will end up with a directory containing Check Point configuration files that you can use

Please read the instructions fully to assure that the correct directory is retrieved from your Check Point device. If the correct directory is not retrieved then you may receive false information within your audit report.

Identifying the Configuration Files

Before continuing, **it is important to note that not all of these files may be on your system**. On some deployments, the information needed is stored in files with a different name. The sub-sections following this will show you how to search for those files depending on the firewall operating system/firmware.

The key files that you should look for are (names are case-sensitive on some systems and not all files will be present):

objects.C

objects.C_41

objects_5_0.C

rules.C

rulebases.fws

rulebases_5_0.fws

The files that you are looking for will be stored in a directory called "conf" or "database".

NOTE: If your device contains both directories called "**conf**" and "**database**" with a number of the files listed above, you should select the "database" directory. Choosing the wrong directory will usually lead to Nipper Studio reporting that there are no firewall rules.

NOTE: The file list above does not represent a full list of the files used by Nipper Studio; you will need to get copy the entire configuration directory.

IPSO and Other UNIX Check Point Systems

On IPSO and other UNIX type systems, you will most likely need to use a command line interface to search for configuration files. The command line interface possibilities are SSH, Telnet (not recommended) or using a direct console connection. Mac OS X and GNU/Linux systems will already have tools to connect to those services ("ssh" and "telnet"), for Windows users you will probably need to download a tool such as PuTTY.

Once you are logged into your Check Point device you can search for files using the "find" command. For example, you can search your entire system for the "objects.C" file using the following command:

The results will be zero or more locations of that file on your system. So if you get no results, try the next file from the list above. On one of our test systems, we get the following result from the command:

From that we can see that we will need the "/var/opt/CPsuite-R62/fw 1/conf" directory from the system. If we were to change to the directory (using the "cd" command) and list the contents (using the "ls" command) we can see that some of the other files are present in the same directory.

```
bash# cd /var/opt/CPsuite-R62/fw1/conf

bash# ls -l    conf

total 21056

-rw-r-----    1 root  wheel  7168   Dec   22    1998 CPMILinksMgr.db.private

drwx------    3 root  wheel  512    Dec   22    1998 ConversionCache

-rw-r--r--    1 root  wheel  1309   Oct   2     20:56 InoDistLocal.ini

-rwxr-xr-x    1 root  wheel  169    Oct   2     20:56 InternalCA.C

-rwxr-xr-x    1 root  wheel  1759   Oct   2     20:56 MVS_Default.W

-rw-rw----    1 root  wheel  2904   Dec   22    1998 SDS_objects.c

...

-rw-r--r--    1 root  wheel  57549 Oct    2     20:57 objects.C

-rwxr-xr-x    1 root  wheel  36876 Oct    2     20:56 objects.C_41

-rw-rw----    1 root  wheel  594000       Dec   22    1998 objects_5_0.C

...

-rw-rw----    1 root  wheel  21     Dec   22    1998 rulebases_5_0.fws

...
```

It will probably be easiest to transfer the configuration to your system as a single file rather than as a large number of individual files. Therefore, we would recommend using the "tar" tool, which should be available on your system. The "tar" command to create an archive stored as "/tmp/my-config.tar" has the following format:

- tar -cvf /tmp/my-config.tar <directory>

To make it easier to navigate to the configuration directory latter, we will change to the directory below the “**conf**” directory first. Then on our system, we could use the commands:

- cd   /var/opt/CPsuite-R62/fw1/
- tar -cvf /tmp/my-config.tar conf

The method of transfer will depend on what you have available. Standard systems will support SCP and FTP. You may also be able to make use of a USB pen device. To secure copy the file to a device that offers FTP you could use the following commands:

- ftp
- ftp> bin
- ftp> hash
- ftp> put /tmp/my-config.tar
- ftp> quit

To Secure CoPy (SCP) the file to a SSH service with Secure Copy enabled, you could use the following command:

- scp /tmp/my-config.tar <username>@<ip-address>:<file-destination>

If you have SCP capabilities from your computer, you could use the following to connect from your computer to the firewall

If your firewall has a USB port, you may be able to use that in order to transfer your configuration. These procedures may vary slightly depending on the UNIX varient:

1. Insert the USB storage device into the USB port of the firewall.
2. Wait a few seconds and use the "df" command to see if it has been automatically detected and mounted.
3. If it has not been mounted, use "dmesg" to view the system messages to see what /dev/<devicename> it has been assigned. Then mount the device using the "mount /dev/devicename /mnt" command.
4. Copy the file to the mounted USB device using a command such as "cp /tmp/my-config.tar /mnt/".
5. Unmount the USB device, for example using the command "umount /mnt"

Windows Check Point Systems

On Check Point-based Windows systems, you can use the Windows search facility in order to find the files. You can do this by right clicking on a disk or directory in Windows Explorer and selecting the "search" option. On some versions, the search facility is shown at the top of the Windows Explorer window.

NOTE: The installation of Smart Dashboard and other Check Point tools may have included demo configuration files (accessed using the demo mode t ick box in the interface). This may be picked up by your search and probably stored in a "PROGRAM\textbackslash cpml_dir\textbackslash conf" directory. If you have several installations then you will probably have several copies of the demo files.

It will probably be easiest to transfer the configuration to your system as a single file rather than as a large number of individual files. You can do this under Windows using the compress folder facility. Using the right mouse button on the folder, select the “Send To" and then "Compressed (zipped) Folder" option. This will create the compressed folder containing the configuration files in the same directory.

Depending on your system setup, the archived configuration file could be transferred to your system using a USB pen, FTP or using a network share.

Using the Configuration with Nipper Studio

Before you can use the configuration with Nipper Studio, you will have to extract it from the archive file. The configuration can then be selected in Nipper Studio using the "Add Directory" option in the "New Report" wizard.