Your Question

Article: 00055
Question:

How do I do I Export Check Point Firewall-1 Log Files for Net Report?

Net Report Answer

Table of Contents

1.0 Introducing Check Point Firewall-1 Commands

To export Check Point Firewall-1 Log files for Net Report you must be familiar with the following Check Point commands:

- `fw logswitch` (please see Section 1.1).
- `fw logswitch old.log` (please see Section 1.2).
- `fw logexport` (please see Section 1.3).

This Article starts by describing the syntax and parameters for each of the above three commands before going on to explain how to export Check Point Firewall-1 Log Files for Net Report.

1.1 The fw logswitch Command

Description

`fw logswitch` creates a new Log File. The current Log File is closed and renamed:

```
$FWDIR/log/fw.logcurrent date.
```

A new Log File with the following default name is created:

```
$FWDIR/log/fw.log
```

The Old Log Files are located in the same directory. You must have the appropriate file privileges to run `fw logswitch`. In addition a Management Station can use `fw logswitch` to switch a Log File on a remote machine and transfer the Log File to the Management Station.

Syntax

```
fw logswitch [-h target] [+|-][""|old_log]
```

1.0.1 Parameters Table

Parameter	Definition
`target`	The resolvable name or IP address of the remote machine (either running a FireWall Module or a Management Module) on which the Log File is located. The Management Station (on which the fw log switch is executed) must be defined as one of `target`'s Management Stations. In addition you must perform fw putkey to establish a control channel between the Management Station and the `target`.
`+`	The Log File is transferred from `target` to the Management Station. The transferred Log File is compressed and encrypted. The name of the copied Log File on the Management Station is prefixed by `target`. This parameter is ignored if `target` is not specified. There should be no white space between this parameter and the next one.
–	The same as `+`, however the Log File is deleted on `target`.
`""`	Delete the current Log File (on `target` if specified; otherwise on the Management Station).
`old_log`	The new name of the old Log File.

1.0.2 File Name Details Table

The following table lists the files created in the following directory:

```
$FWDIR/log directory
```

On both target and the Management Station when the + or – parameters are specified. Note that if "-" is specified, the Log File on target is deleted rather than renamed.

Target	Definition	
target specified	On target, the old Log File is renamed to old_log. On the Management Station, the copied file will have the same name, but be prefixed by target's name. For example, the following command: fw logswitch -h venus +xyz creates a file named: venus.xyz on the Management Station.	On target, the new name is: current.date. For example: 04Dec04-10:04:20 in Unix and 04Dec04-100420 in NT On the Management Station, the copied file will have the same name, but will be prefixed by target's name: target.04Dec04-10:04:20 in Unix and target.04Dec04-100420 in NT.
target not specified	On the Management Station, the old Log File is renamed to old_log.	On the Management Station, the old Log File is renamed to current date (please see the row above).

Note: if either the Management Station or target is an NT machine, the files will be created using the NT naming convention.

How can I switch my Log File on a Periodic Basis?

You can do this in NT with the following command:

```
at < time> c:\winnt\fw\bin\fw logswitch
```

1.2 The fw logswitch old.log Command

Explanation

The following command creates a new Log File and moves (renames) the old Log File to `old.log`.

Syntax

```
fw logswitch old.log
```

1.3 The fw logexport Command

Definition

`fw logexport` exports the Log File to an ASCII readable file.

Syntax

```
fw logexport [-d delimiter] [-i inputfile] [-o outputfile] [-r record_chunk_size] [-n]
```

1.3.1 Parameters Table

Parameter	Definition
-d delimiter	Output fields will be separated by this character – default is comma (,).
-i inputfile	Name of the input Log File.
-o outputfile	Name of the output ASCII file.
-r record_chunk_size	Determines how many records should be read (during a single access to the Log File) into the internal buffer for processing.
-n	Do not perform DNS resolution of the IP addresses in the Log File (this option significantly speeds up the processing).

2.0 Exporting Check Point Firewall-1 Log Files for Net Report

Check Point Firewall-1 constantly generates fw.log files which Net Report cannot read in their untreated state. You must therefore switch and export these fw.log files a certain manner for Net Report to correctly process them. Therefore, the Linux and Unix CheckPoint versions provide a command line tool to generate these readable text files which Net Report can process.

2.1 Recommended Procedure for Exporting Log Files for Net Report

To export Log Files for Net Report, you must ensure the following prerequisites are fulfilled:

Prerequisites

1. Execute the `fw logswitch` command daily (for example at 00:15), to create a new log file, the current Log File is closed and renamed with a date format:

```
$FWDIR/log/fw.logcurrent date.
```

For example, `fw-logswitched-ddmmyy-hhmm.log`.
A new Log File with the following default name is created, this avoids your `fw.log` file overloading, by daily archiving the previous day’s Log File and replacing it with a fresh Log File for the next 24 hours:

```
$FWDIR/log/fw.log
```

You must have the appropriate file privileges to run `fw logswitch`.

2. Ensure you regularly archive the Old Log Files, the following command creates a new Log File and moves (renames) the old Log File to `old.log`.

```
fw logswitch old.log
```

Note: the Old Log Files are located in the same directory, you must ensure the backup of your Old Log Files.

3. Export the log switched files

```
$FWDIR/log/fw.logcurrent date.
```

to a readable format by using the `fw logexport` command (please see Section 1.3).

```
fw logexport [-d delimiter] [-i inputfile] [-o outputfile]
[-r record_chunk_size] [-n]
```

Parameter	Definition
`-d delimiter`	Output fields will be separated by this character – default is comma (,).
`-i inputfile`	Name of the input Log File.
`-o outputfile`	Name of the output ASCII file.
`-r record_chunk_size`	Determines how many records should be read (during a single access to the Log File) into the internal buffer for processing.
`-n`	Do not perform DNS resolution of the IP addresses in the Log File (this option significantly speeds up the processing).

⚠ **Warning:** you must include [-n] parameter at the end of the `fw logexport` command. This parameter ensures that no DNS Resolution of IP addresses is carried out in the Log File). Net Report needs the IP addresses in order to process the Log File. If DNS resolution is performed, Net Report will be unable to correctly process the Log File.

For example:

```
fw logexport –I fw-logswitched<date>.log –o fw<date>-export.log -n
```

4. Either:
4a. Upload the Log File generated in Step 3 above (that is, the Net Report readable and dated log file) to an FTP site, for example to the Net Report Server FTP directory.
Or
4b. Save the Log File generated in Step 3 above (that is, the Net Report readable and dated log file) to a Shared Directory (shared by the machine Check Point Firewall-1 is installed on and the machine Net Report is installed on).

5. Clean the following directory regularly.

```
$FWDIR/log/fw.log
```

Status: you have successfully set up a scheduled manner to export your Check Point Firewall-1 Log Files in a format Net Report can correctly process!

Further Information

Please see our Net Report Knowledge Base at:
http://www.netreport.fr/us/support/sup_knowledgebase.asp