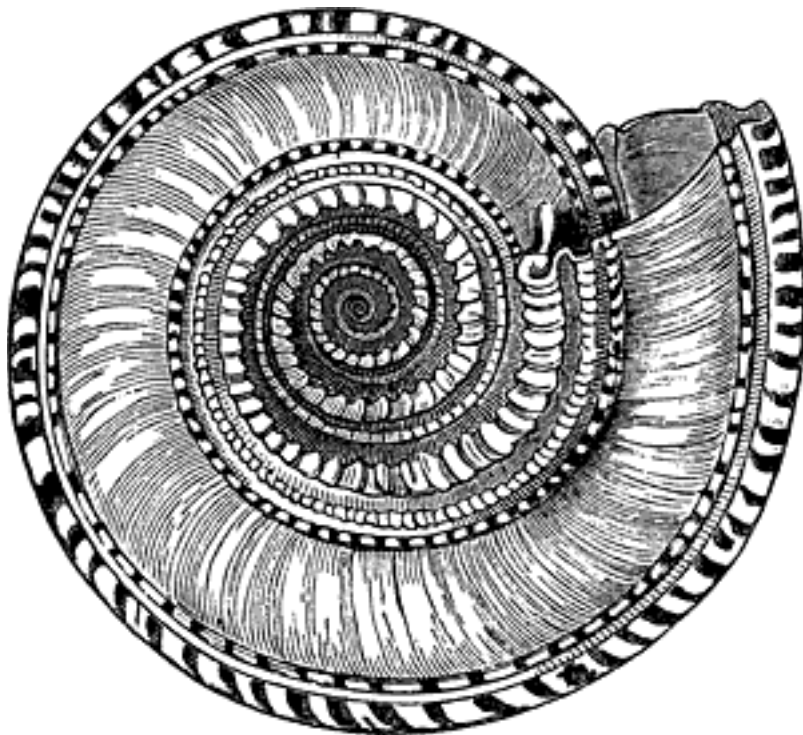


*Enhanced version - no round corners!*

**GAIA EDITION**  
**Updated for R77.30**

# UNIfw1lr

*Firewall log rotation made simple*



*Niels Thomas Haugård*

## Table of Contents

Table of Contents	1
Introduction	2
Prerequisites and caveats	2
Installation	2
How does UNIfw1lr work	2
What not to expect from UNIfw1lr	4
Using UNIfw1lr	4
Known limitations	5

## Introduction

**UNIfw1lr** - *UNI•C FireWall-1 Log Rotation* - is a simple firewall log rotation and log management solution for Check Point firewall-1 made by UNI•C, now i2.dk.

This version is compatible with [GAiA](#) and has been tested on Check Point R77.10, R77.20 and R77.30, and should work with all later R77.x versions, both appliances and open servers. It is not compatible with Secure Platform.

Once installed all firewall logs gets

1. rotated on a daily basis
2. exported to a CSV text file with each field described in the first line
3. processed by report generator that generates top 10 reports on
  - accepted traffic
  - dropped and rejected traffic
  - attacks

The log files will be visible through the *Check Point Log Viewer* for a specific number of days (default 10), then compressed and left in the filesystem for default 20 days more, before they are deleted.

All files are available for download from a SSL enabled WebServer (installed with the firewall) running on TCP port 9876. The WebServer uses the certificate from defaultCert.

**UNIfw1lr** is free software and released under a [modified BSD License](#), see LICENSE. Using the software requires a valid support contract with [Check Point Technologies](#).

## Prerequisites and caveats

Please *disable all Check Point log rotation configurations*, as it will interfere with **UNIfw1lr** and prevent purging of logs rotated by Check Point due to differences in log file naming.

## Installation

**UNIfw1lr** is installed as a package (RPM) and requires the package **UNIttools** to be installed first. UNIfw1lr is installed on the management station. It may also be installed on enforcement modules, to avoid filling the filesystem with log files in case of error(s).

## How does UNIfw1lr work

**UNIfw1lr** runs every day at **23:59**. It does log file house keeping according to its configuration file stored in `/var/opt/UNIfw1lr/etc/fw1logrotate.conf`.

- The *active firewall log* is switched and the old log file exported to a
- [cvs file](#). The first line describes the fields. The exported file may be quite large and on a busy system exceed 2,147.483.647 Gb which may cause problems on 32bit systems (see [2GB file-size limit](#)).

- Tree reports are made based on the exported log:
  - **top 10 accepted** for *rules, source, destination* and *protocol*.
  - **top 10 dropped and rejected** for *rules, source, destination* and *protocol*.
  - **top 10 attack** for *rules, source, destination* and *protocol*.
- Logfiles older than a specific date (default 10) is compressed.
- Compressed log files older than a specific date (default 20) is deleted.

The reports are made with [fwlogsum 5.0.2](#) © 1996-2004 Peter Sundstrom, peter@ginini.com. This may be changed in [default.report.sh](#).

**UNIfw1lr** starts an SSL enabled WebServer on boot. The server is part of the base operating system and maintained by Check Point. The server binds to a specific IP address and TCP port 9876. The server does not require login and password and should be restricted to e.g. the admin group and e.g. a log consolidator system.

An example is shown here:

**Statistik og Gamle FireWall-1 Logfiler**

**Oversigt over gamle logfiler**

Denne side viser en oversigt over gamle firewall logfiler. Logfilerne roteres en gang i døgnet. De roterede logfiler gemmes sammen med en statistisk oversigt og en tekstuel eksport samlet i kataloger for en dag ad gangen. Katalogerne bevares i 10 dage, hvorefter de komprimeres og katalogerne slettes. De komprimerede arkiver gemmes yderligere i 10 dage før de slettes. Antallet af dage kan justeres i det omfang der er diskplads nok. [UN1-C](#) vil anbefale at dokumenterne på denne side regelmæssigt kopieres til et sikkert medie af arkivhensyn. De kan gøres automatisk med f.eks. det licensfrie program GNU Weget, der kan hentes på <http://wget.sunsite.dk/>. Programmet findes også i en version til Microsoft Windows.

**Online - bevares i 10 dage**

Online logfilerne er hardlinkede til dokumenter i FireWall-1 log kataloget. Dokumenterne kan derfor også læses med FireWall-1 logviewer GUI.

Katalognavn	Størrelse i Mb	Beskrivelse
<a href="#">2015_05_31_23-59-05</a>	7.55 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 31 05 2015
<a href="#">2015_06_01_23-59-05</a>	8.27 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 01 06 2015
<a href="#">2015_06_02_23-59-06</a>	8.33 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 02 06 2015
<a href="#">2015_06_03_23-59-05</a>	8.49 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 03 06 2015
<a href="#">2015_06_04_23-59-06</a>	9.39 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 04 06 2015
<a href="#">2015_06_05_23-59-05</a>	11.09 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 05 06 2015
<a href="#">2015_06_06_23-59-04</a>	6.99 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 06 06 2015
<a href="#">2015_06_07_23-59-06</a>	8.42 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 07 06 2015
<a href="#">2015_06_08_23-59-04</a>	7.80 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 08 06 2015
<a href="#">2015_06_09_23-59-05</a>	9.65 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 09 06 2015
<a href="#">2015_06_10_23-59-06</a>	12.44 Mb	Rapporter og FireWall-1 logfiler fra logswitch den 10 06 2015

**Komprimerede - bevares i 10 dage**

De komprimerede dokumenter er lavet som Posix Tar arkiver, komprimeret med GNU zip. De kan dekomprimeres med de fleste PC unzip værktøjer, f.eks. den gratis <http://www.aladdin.com/expander> - Aladdin Systems' Expander, der findes til Linux, Mac og Microsoft Windows.

Dokumentnavn	Størrelse	Beskrivelse
<a href="#">2015_05_21_23-59-05.tar.gz</a>	1.52 Mb	Komprimeret tar arkiv med rapporter og FireWall-1 logfiler fra logswitch den 21 05 2015
<a href="#">2015_05_22_23-59-08.tar.gz</a>	1.62 Mb	Komprimeret tar arkiv med rapporter og FireWall-1 logfiler fra logswitch den 22

Indeks for FireWall-1 logfiler og rapporter(er)		
Første loginlinje:		30May2015 23:59:22
Sidste loginlinje:		31May2015 23:59:10
Dokument	Størrelse i Mb	Beskrivelse
<a href="#">accepts.2015_05_31_23-59-05.html</a>	0.023 Mb	Oversigtsrapport over alle tilladte forbindelser, sorteret efter antal, FQDN i stedet for IP adresser, incl. domæne oversigt.
<a href="#">dropsrejects.2015_05_31_23-59-05.html</a>	0.020 Mb	Oversigtsrapport over alle afviste forbindelser, sorteret efter antal, FQDN i stedet for IP adresser, incl. domæne oversigt.
<a href="#">attacks.2015_05_31_23-59-05.html</a>	0.008 Mb	Oversigtsrapport over alle angreb rapporteret af SmartDefence, sorteret efter antal, FQDN i stedet for IP adresser, incl. domæne oversigt. Rapporten kræver NG AI og kan være tom.
<a href="#">2015_05_31_23-59-05.log</a>	6.371 Mb	Binær FireWall-1 logfil.
<a href="#">2015_05_31_23-59-05.logaccount_ptr</a>	0.004 Mb	Logpointer (Binær FireWall-1 logfil)
<a href="#">2015_05_31_23-59-05.loginitial_ptr</a>	0.184 Mb	Logpointer (Binær FireWall-1 logfil)
<a href="#">2015_05_31_23-59-05.logptr</a>	0.184 Mb	Binær FireWall-1 logfil.
<a href="#">2015_05_31_23-59-05.txt.gz</a>	0.719 Mb	Eksporteret log i tekstformat. Der anvendes ':' som skille tegn og felterne er beskrevet i den første linie. Filen skal i Årst pakkes ud
<a href="#">accepts.2015_05_31_23-59-05.html.verbose.log</a>	0.004 Mb	Kørselslog for generering af rapporten accepts.2015_05_31_23-59-05.html.html
<a href="#">attacks.2015_05_31_23-59-05.html.verbose.log</a>	0.004 Mb	Kørselslog for generering af rapporten attacks.2015_05_31_23-59-05.html.html
<a href="#">dropsrejects.2015_05_31_23-59-05.html.verbose.log</a>	0.004 Mb	Kørselslog for generering af rapporten dropsrejects.2015_05_31_23-59-05.html.html
<a href="#">fw1logrotate.log</a>	0.012 Mb	Kørselslog for logrotation.
<b>Bemærkninger</b>		
<ul style="list-style-type: none"> <li>Rapporterne er et <i>udtræk af hvad der logges</i>. I et forsøg på at reducere logfilernes størrelse vil man typisk smide information væk, firewall'en ingen indflydelse har på (f.eks. lokal trafik på samme interface).</li> <li>Rapporterne kan vise et skævt billede af trafikmængden; kun regler i firewall'en der logger med <i>account</i> gemmer oplysninger om den overførte datamængde. Et mere præcist totalbillede fås ved f.eks. snmp forespørgsel af internet routeren.</li> <li>Rapporterne indeholder simple grafer, der vises bedst i IE; Netscape Opera og Mozilla viser ikke graferne i farve.</li> <li>Det er kun muligt, at anvende de binære FireWall-1 logfiler på en FireWall-1 management station med passende licens. Det er ikke muligt, at gennemse loggen lokalt med GUI'en.</li> <li>Den eksporterede logfil <i>2015_05_31_23-59-05.txt</i>, kan indlæses i et loganalyseværktøj, regneark eller database for videre behandling; <i>men bemærk dens størrelse før det gøres!</i></li> <li>Logfilerne bør kopieres til et sikkert medie; de vil blive slettet fra firewall'en efter behov.</li> </ul>		
<b>Kørselsstatistik for rapportgenerering</b>		
Start:		01 June 2015 00:07:11
Slut:		01 June 2015 00:19:20

In the example the server is bound on `192.168.112.1` so the server URL is

```
https://192.168.112.1:9876
```

Notice that the [SSL certificate](#) will cause a browser warning.

The servers configuration file is `/var/opt/UNIfw1lr/etc/httpd2.conf`. The default bind address is 127.0.0.1.

## What not to expect from UNIfw1lr

UNIfw1lr is not a replacement for [Check Point SmartLog](#) but primarily a tool to rotate and compress log files, and make them available for a log archiver.

## Using UNIfw1lr

UNIfw1lr should be accessed by a [log consolidator](#) for collecting and archiving log files. A simple shell script (`get_firewall_logs.sh`) which will collect the log files from an external server is located in `/var/opt/UNIfw1lr/docs`.

If you choose to use [GNU wget](#) / [wget for windows](#) you may use the [bash for windows](#) snippet:

```
wget -N --reject 'index.html' -r -m --no-check-certificate \
https://${SRVR}:${PORT} > ${TMPFILE} 2>&1
ERRORS=$?
case $ERRORS in
0) MSG="wget: No problems occurred."
;;
1) MSG="wget: Generic error code."
;;
2) MSG="wget: Parse error"
;;
3) MSG="wget: File I/O error."
;;
4) MSG="wget: Network failure."
;;
5) MSG="wget: SSL verification failure."
;;
6) MSG="wget: Username/password authentication failure."
;;
7) MSG="wget: Protocol errors."
;;
8) MSG="wget: Server issued an error response"
;;
esac
```

## Known limitations

- **UNIfw1lr** uses [hard links](#) to minimize disk usage. This requires all files to reside on the same partition: `$FWDIR/log` and the directory used by **UNIfw1lr** to store files must be on the same partition. This is ensured during package installation.
- R77.xx comes in two flavors: 32bit and 64bit. Smaller appliances like the [2200 series](#) has a 32bit CPU and therefore suffers from the 2.1Gb file size limitation.