

CheckPoint Firewall-1 Commands

>fwstop

Stops the FireWall-1 daemon, management server (fwm), SNMP (snmpd) and authentication daemon (authd).

(To stop Firewall-1 NG and load the default filter: **fwstop -default**, **fwstop -proc**)

>fwstart

Loads the FireWall-1 and starts the processes killed by *fwstop*.

>cpstop

Stops all Check Point applications running, except *cprid*.

>cpstart

Starts all Check Point applications.

>cpconfig

In NT, opens Check Point Configuration Tool GUI. (licenses, admins ...)

>cpstat options

Provides status of the target hosts.

Usage: cpstat [-h host][-p port][-f flavour][-o polling [-c count] [-e period]] [-d] application_flag

-h A resolvable hostname, a dot-notation address, or a DAIP object name.

Default is localhost.

-p Port number of the AMON server.

Default is the standard AMON port (18192).

-f The flavour of the output (as appears in the configuration file).

Default is to use the first flavour found in the configuration file.

-o Polling interval (seconds) specifies the pace of the results.

Default is 0, meaning the results are shown only once.

-c Specifying how many times the results are shown.

Default is 0, meaning the results are repeatedly shown.

-e Period interval (seconds) specifies the interval over which "statistical" oids are computed. Ignored for regular oids.

-d Debug mode

Available application_flags:

Flag	Flavours
------	----------

fw	default, policy, perf, hmem, kmem, inspect, cookies, chains, fragments, totals, ufp, http, ftp, telnet, rlogin, smtp, sync, all
-----------	---

ha	default, all
-----------	--------------

ls	default
-----------	---------

mg	default
-----------	---------

os	default, routing, memory, old_memory, cpu, disk, perf, all, average_cpu, average_memory, statistics
-----------	---

persistency	product, TableConfig, SourceConfig
--------------------	------------------------------------

polsrv	default, all
---------------	--------------

vpn	default, product, IKE, ipsec, traffic, compression, accelerator, nic, statistics, watermarks, all
------------	---

FireWall-1 Commands

>fw **ver** [-h] ..

Display version

This is Check Point VPN-1(TM) & FireWall-1(R) NG Feature Pack 3 Build 53920

>fw **kill** [-sig_no] procname

Send signal to a daemon

>fw **putkey** -n *ip_address_host ip_address_of_closest_interface*

Client server keys; helpful if you are integrating an NG Management Server with 4.x enforcement modules. Will install an authenticating password; used to authenticate SIC between the Management Server and the module.

>fw **sam** (**Suspicious Activities Monitoring**)

Usage:

sam [-v] [-s *sam-server*] [-S *server-sic-name*] [-t *timeout*] [-l *log*] [-f *fw-host*]
[-C] -((n|i|I|j|J) <criteria>

sam [-v] [-s *sam-server*] [-S *server-sic-name*] [-f *fw-host*] -M -ijn <criteria>

sam [-v] [-s *sam-server*] [-S *server-sic-name*] [-f *fw-host*] -D

Criteria may be one of:

src <ip>

dst <ip>

any <ip>

subsrc <ip> <net mask>

subdst <ip> <net-mask>

subany <ip> <net-mask>

srv <src-ip> <dst-ip> <service> <protocol>

subsrv <src-ip> <net-mask> <dst-ip> <net-mask> <service> <protocol>

subsrvs <src-ip> <net-mask> <dst-ip> <service> <protocol>

subsrvd <src-ip> <dst-ip> <net-mask> <service> <protocol>

dstersrv <dst-ip> <service> <protocol>

subdstersrv <dst-ip> <net-mask> <service> <protocol>

srcpr <ip> <protocol>

dstpr <ip> <protocol>

subsrcpr <ip> <net mask> <protocol>

subdstpr <ip> <net mask> <protocol>

>fw **fetch** *ip_address_management_station*

Used to fetch Inspection code from a specified host and install it to the kernel of the current host.

>fw **tab** [-h] ...

Displays the contents of FireWall-1's various tables

>fw **tab** -t *connections* -s tells how many **connections** in state table

>fw **monitor** [-h] ...

Monitor VPN-1/FW-1 traffic

>fw **ctl** [*args*] install, uninstall, pstat, iflist, arp, debug, kdebug, chain, conn
Control kernel

>fw **ctl pstat** shows the internal statistics – memory/connections

>fw **ctl arp** shows firewall's ARP cache – IP addresses via **NAT**

>fw **lichosts**

Display protected hosts

>fw **log** [-h] ...

Display logs

>fw **logswitch** [-h target] [+|-][oldlog]

Create a new log file; the old log is moved

>fw **repairlog** ...

Log index recreation

>fw **mergefiles** ...

log files merger

>fw **lslogs** ...

Remote machine log file list

>fw **fetchlogs** ...

Fetch logs from a remote host

FireWall Management Server Commands

>fwm **ver** [-h] ...

Display version

>fwm **load** [opts] [filter-file|rule-base] targets

Will convert the *.W file from the GUI to a *.pf file and compile into Inspection code, installing a Security Policy on an enforcement module.

>fwm **load** Standard.W all.all@localgateway

>fwm **unload** [opts] targets

Uninstall Security Policy from the specified target(s).

>fwm **dbload** [targets]

Download the database

>fwm **logexport** [-h] ...

Export log to ascii file

>fwm **logexport** [-d delimiter] [-i filename] [-o filename] [-n] [-f] [-m
<initial | semi | raw>] [-a]

Where:

-d - Set the output delimiter. Default is ;

-i - Input file name. Default is the active log file, fw.log

-o - Output file name. Default is printing to the screen

-n - No IP resolving. Default is to resolve all IPs

-f - In case of active file (fw.log), wait for new records and export them

-m - Unification mode. *Default is initial order.*

Initial - initial order mode

Raw - No unification

Semi - Semi-unified mode

-a - Take account records only. Default is export all records

Once your logs files have been written to a backup file you can begin to export them into an ASCII format so you may begin to analyze them. The command that accomplishes this is the *fw logexport* command. The format of this command is as follows:

```
C:\WINNT\FW1\NG\log>fwm logexport -d , -i 2003-03-19_235900_1.log -o fwlog2003-03-19.txt
```

The **-d switch** specifies a delimiter character with the default being the semi-colon.

The **-i switch** specifies the input file and the **-o switch** specifies the output file. The **-n switch** tells the program to not perform any name resolution on the IP addresses. This will greatly speed up the export process. If you have the time and want to see the domain names instead of IP addresses you may omit this switch. One word of caution though, the size of the output files that get created grow an average of 2.5 times the input file.

>fwm **gen** [-RouterType [-import]] rule-base

Generate an inspection script or a router access-list

>fwm **dbexport** [-h] ...

Export the database

>fwm **ikecrypt** <key> <password>

Crypt a secret with a key (for the dbexport command)

>fwm **dbimport** [-h] ...

Import to database

SmartUpdate commands – *Requires license*

```
>cppkg add <package-full-path | CD drive>  
>cppkg del [vendor] [product] [version] [os] [sp]  
>cppkg print  
>cppkg setroot <repository-root-directory-full-path>  
>cppkg getroot
```