STORMSHIELD

GUIDE
STORMSHIELD NETWORK SECURITY

CLI CONSOLE / SSH COMMANDS REFERENCE GUIDE

Version 4

Date: November 28, 2019

Reference: sns-en-cli_console_ssh_commands_reference_guide-v4

Introduction

This documents details all the Stormshield Network commands of the IPS-Firewall for the release version 4.0.0.

ATTENTION
This command list is dedicated to the partners that have been certified by NETASQ or Stormshield and who realize some support to their customers.

ATTENTION
These commands are normally called by "high level" configuration commands to activate parts of the configuration.

No verification are made about coherency when calling directly those commands. A direct call to those commands can put the IPS-firewall in an unstable state.

CONTENTS

The command list is an alphabetical order but organized by category. The categories are :

- Hardware
- Configuration low level
- Functionalities
- Factory tools
- Daemon
- Miscellaneous

Table of contents

CHAPTER 1: Category Description

Hardware

Description This category groups all the commands used to communicate and to manage the hardware.

Index The alphabetic list of each command of this category is the following :

hardwarectl
powerstatus

Low level Configuration

Description This category groups all the commands used to manage configuration at low level.

Index The alphabetic list of each command of this category is the following :

arpreset
arpsync
builddhcpd
builddialup
buildddns
buildevent
buildfilter
buildipsec
buildha
buildldapconf
buildntp
buildopenvpn
buildsnmp
buildsquid
buildssh
buildwifi

Functionalities

Description This category groups all the commands which use functionalities of the IPS-Firewall.

Index The alphabetic list of each command of this category is the following :

alivectl
autoupdate
checkcrl
certenrol
curltool
ddnsclient
dhclient
dhclient-script
dhlease-script
dumproot
gatemon
gatewayctl
hacheckstatus
hastart
keepalive
launchctl
ldapcheck
newldapbase
objectsync
setkey
sfctl
smartctl
statectl

High level configuration management

Description This category groups all the commands used to manage the configuration at high level.

Index The alphabetic list of each command of this category is the following :

avctl
backupinfo
date
defaultconfig
dialupstate
enalived
enantivirus
enasq
enauth
enbird
enbypass
enconsole
endhcp
endhcrelay
endialup
endns
enevent
enfilter
engatemon
enha
enkeyboard
enldap
enlock
slotinfo
enlog
ennat
ennetwork
enntp
enobject
enopenvpn
enpattern
enproxy
enservice
ensl
ensmcrouting
ensnmp
enswitch
entelemetryd
enthind
entimezone
enurl
enuserreqd
envpn
enwifi
ifinfo
setboot

Factory tools

Description This category groups all the commands used by the factory.
It is not recommended to launch these commands on your IPS-Firewall.

Index The alphabetic list of each command of this category is the following :

bonnie++
3 burnP6
checkintegrity
cleanfw
fwinit
fwtest
kldbgload.sh
netperf
netserver
udpsync

Daemon

Description This category groups all the daemons of the IPS-Firewall.

Index The alphabetic list of each command of this category is the following :

alived
asqd
avd
bird
bird6
clamavd
dhcpd
dhcrelay
dhclient
dnscache
eventd
gatewayd
hardwared
launchd
logd
mpd
ntpd
openvpn
racoon
serverd
sld
smcrouterd
snmpd
squid
stated
switchd
telemetryd
thind
tproxyd
userreqd

Category : Miscellaneous

Description This category groups all the commands that are not in a particular category.

Index The alphabetic list of each command of this category is the following :

certinfo
checkdb
checkfs
checkintegrity
checkinternet
checkversion
chpwd
clamdefault
cleanunwantedfiles
clearlog
crlinfo
decbackup
dhcpinfo
dkill
dstat
dumpcert
dynroute
encbackup
enroll
exportconf
formatdisk
fwpasswd
fwshutdown
fwsound
fwupdate
getalarmconf
getconf
getlicense
getmodel
getpci
getversion
globalgen
halt
hostcheck
imish
licenceupdate
licensemanager
logtools
modemctl
ndmesg
ngstat
nhup
nkill
nrestart
nsbsdstart
nsbsdstop
nsrpc
nstart
nstop
paygprep
ntpq
pppdown
pppdown2
pppup
pppup2
pvmdbsync
pvmgenconf
reboot
sendalarm
service_client
service_server
setconf
seturl
swaninfo
swapethernet
sysdbg
sysinfo
sysutil
tcpick
testldapbase
topic_monitor
topic_reader
topic_sender
vmreport

CHAPTER 2 : Commands Description

alivectl

Description Client application used to access to information provided by the icmp monitoring daemon (alived)

Command

```
alivectl [-h] [-v] [-d] -s <hostname> | -l | -r
-h, --help : show this help
 -v, --verbose : verbose mode
 -d, --debug : enable debug
 -s, --show <hostname> : show information for a specific host
 -l, --list : list all monitored hosts
 -r, --reset : reset hosts statistics
```

Results The list of monitored hosts.

Example

```
host "V50XXA07B8563A9_0" (172.16.0.2): down
 packet transmitted : 5
 packet received : 0
 packet loss : 100.00%
 packet send errors : 0
 maybe down transition : 1
 rtt min : 0.000 ms
 rtt avg : 0.000 ms
 rtt max : 0.000 ms
 deviation : 0.000 ms
 first pkt sent : 2017-09-21 10:33:06
 last pkt sent : 2017-09-21 10:33:10
 first pkt recv : <unknown>
 last pkt recv : <unknown>

 host "gateway" (10.2.0.1): up
 packet transmitted : 3
 packet received : 3
 packet loss : 0.00%
 packet send errors : 0
 maybe down transition : 0
 rtt min : 1.617 ms
 rtt avg : 1.748 ms
 rtt max : 1.837 ms
 deviation : 0.116 ms
 first pkt sent : 2017-09-21 10:33:06
 last pkt sent : 2017-09-21 10:33:26
 first pkt recv : 2017-09-21 10:33:06
 last pkt recv : 2017-09-21 10:33:26
```

alived

Description ICMP monitoring daemon. Monitor both PBR route and HA links.

Command

```
alived [-d] [-D] [-h] [-l] [-v]
    -D : will daemonize
     -d : debug mode
     -h : show help message
     -l : print the list of hosts to be monitored then exit
     -v : verbose mode
```

Results

Example

arpreset

Description Sends ARP packets to the interfaces in order to update the ARP tables.

Command

```
arpreset <-a|-A> | <interface>
-a -A : all interfaces
```

Results

Example

arpsync

Description Synchronize the local ARP table.

Command

```
arpsync -a|u|d -[4|6] [-n] [-v] [-h]
a: setup ARP/NDP table (deprecated)
 d: cleanup ARP/NDP table (deprecated)
 u: update ARP/NDP table
 4: only setup the ARP table
 6: only setup the NDP table
 n: setup/cleanup only NAT entry
 v: verbose mode
 h: help
```

Remarks :

By default, both ARP and NDP (if IPv6 is enabled) tables are setup, unless -4 or -6 option is specified

The -a and -d option have been deprecated since the introduction of the -u option.

Results

Example

asqd

Description Daemon of configuration and supervising ASQ

Command

```
asqd [-r user] [-D] [-d] [-v]
-r user : Run as the specified user.
-D : Daemon.
-d : Activate debug for the current running asqd (pvm debug).
-v : Display asqd version.
```

Results

Example	

asqstart

Description	
Command	asqstart (no argument)
Results	
Example	

autobackup.sh

Description	Automatic backup the configuration files
Command	autobackup.sh [-d] -d: debug
Results	
Example	

autoupdate

Description	Updates data for the modules listed below.
Command	autoupdate [-b] [-f] [-s] [-d] [-n] [-v <level>] [-t <module>] | [-?] -b Build data directories -f Force a master update -d Launch autoupdate in the background -n Accept non-signed updates -v Verbose level (1 for Errors only, 2 for Errors+Infos, 3 for Errors+Infos+Debug) -s Show config -t (Antispam|URLFiltering|Patterns|CustomPatterns|Kaspersky|Clamav|Vaderetro|Pvm|RootCertificates|IPData) module to update
Results	Database of the corresponding modules has been updated.
Example	

avctl

Description	Manages antivirus daemon

Command

```
avctl [-v] [-o] [-q] [-B] [-r <reload flags>] [-R <reason>] [-s <filepath>] [-b] [--sbx-profile-file
<profile>] [--sbx-ctx-file <context>] [-d] [-i] [-l]
-v Enable verbosity
 -o Specify the output format, arg may be "text|html|xml|json[,pretty]" (default is "text,pretty")
 -q Do not print the results to standard output
 -B Execute in background (will not print the results)
 -r Make avd reload partially or totaly its configuration. flags may be "all", "verbose", "kav_engine",
"kav_settings", "sbx_settings"
 -R Text to explain why the reload was made
 -s Scan the given file
 -b Perform a sandboxing analysis (applies only when action is scan-file)
 --sbx-profile-file File containing sandboxing profile
 --sbx-ctx-file File containing the sanboxing context parameters
 -d Dump avd current configuration
 -i Dump information about currently loaded database
 -l Dump information about currently loaded license.
```

Results

A command is sent to avd. Execution will hold until a response is recieved from avd, unless a background exection is asked

Example

avd

Description

Antivirus daemon for Kaspersky and Sandboxing analysis.

Command

```
avd [-d] [-D]
-d If an other process is already running, send it a signal to switch its verbose mode, otherwise
start with verbose mode enabled.
-D Daemonize, run in background.
```

Results

Example

backupinfo

Description

Display some information about the backup partition.
Display an information about active partition : main or backup.

Command

```
Backupinfo [-s | -I ]
-s : Print "[BackupInfo]" to the stdout
-I : Internal option.
```

Results

Example

```
F1003D011690999999>backupinfo
Active=Main
BackupVersion="delos.alpha-NO_OPTIM"
BackupBranch="INTERNE"
Date="2008-07-10 09:41:06"
Boot=Main
U2504C099999999999>
```

backuprestore

Description	Restore backup from file passed as argument
Command	backuprestore -f <file path> [-p <password>] [-u] [-v] -v : verbose mode -r : refresh after restore -p : password associated with backup file -f : backup file to restore

bird

Description	Fully functional dynamic IP routing daemon for IPv4
Command	bird [--version] [--help] [-c <config-file>] [OPTIONS] [-n <notification-cmd>]
Results	
Example	

bird6

Description	Fully functional dynamic IP routing daemon for IPv6
Command	bird6 [--version] [--help] [-c <config-file>] [OPTIONS] [-n <notification-cmd>]
Results	
Example	

birdc

Description	Bird comand-line interface client for IPv4
Command	birdc [-s <control-socket>] [-v] [-r] [-l]
Results	
Example	

birdc6

Description	Bird comand-line interface client for IPv6
Command	birdc6 [-s <control-socket>] [-v] [-r] [-l]
Results	
Example	

bonnie++

Description	Bonnie++ is a benchmark suite that is aimed at performing a number of simple tests of hard drive and file system performance.

Command	bonnie++ [-d scratch-dir] [-c concurrency] [-s size(Mb)[:chunk-size(b)]] [-n number-to-stat[:max-size[:min-size][:num-directories[:chunk-size]]]] [-m machine-name] [-r ram-size-in-Mb] [-x number-of-tests] [-u uid-to-use:gid-to-use] [-g gid-to-use] [-q] [-f] [-b] [-p processes | -y] [-z seed | -Z random-file]
Results	
Example	

builddhcpd

Description	Converts the configuration files of DHCP to the config file for the daemon dhcpd. This binary is called by endhcp.
Command	builddhcpd [-4|-6] [-r] [-t] -4 : IPv4 -6 : IPv6 -r : Setup dhcp relay configuration and exit -t : Make dhcpd tests after build
Results	
Example	

builddialup

Description	Converts the configuration files of mpd-netgraph to the config file for the daemon mpd. Dialup access (RTC, RNIS, PPPoE, PPTP). This binary is called by endialup.
Command	buildpdialup [-x <if>] -x : doesn't modify config files for the interfaces listed in <if>
Results	
Example	

builddns

Description	Converts the configuration files of DNS to the config file used by the dnscache. This binary is called by endns.
Command	builddns [-c] -c : update only clients information. This doesn't require a daemon restart to be effective.
Results	
Example	

buildevent

Description Converts the configuration files of the events to the config file for the daemon eventd.
This binary is called by enevent.

Command

```
buildevent [-s | -c <eventfile>] [-v]
 -s show only the valid events but don't write them to disk
 -c <event file> strict validation of the content of an event file
 -v display verbose on stdout
```

Results

Example

buildfilter

Description Converts the configuration files of filtering slot to the config file.
This binary is called by enfilter.

Command

```
buildfilter -h -v -s | -m [-x] | [-i] [-f <Global FilterFile> <FilterFile>] [-x] [-w] [-e]
-f <Global Filterfile> <Local Filterfile> : input
-o <ASQ filter rules> [<Proxy filter rules>] : output
 Possible outputs: 'none', 'stdout', 'stderr', <filename>
 Default for ASQ filter rules: 'stdout'
 Default for Proxy filter rules: 'none'
 -h help
 -i implicit filtering rules
 -m minimal filtering rules
 -v verbose
 -s display warning and error messages in a more easy-to-parse manner
 -x XML output
 -w suppress warning messages
 -e enforce rule checking policy, some warning are now considered errors
```

Results

Example

buildha

Description

Command

```
buildha:
-o : Check HA config and build Corosync config (default action)
-b : Do actions that must be done at boot (create cluster or join cluster)
-c <HA config file> : Create a cluster starting from the given HA config file
-j <HA config file> : Joins an existing HA cluster
-v : verbose
```

Results

Example

buildipsec

Description Converts the configuration files of the VPN IPSEC to the config file for the daemon racoon.
This binary is called by envpn.

Command	buildipsec <action> --global=<file> --local=<file> <action> is one of the following: --check check the configuration --dumpconf dump the parsed configuration --build build configuration
Results	
Example	

buildldapconf

Description	Converts the configuration files of the LDAP to the config file for the daemon ldapd. This binary is called by enldap
Command	buildldapconf [-p] [-a] [-v] [-h] -p : root password -a : activate HA -v : verbose -h : help
Results	
Example	

buildntp

Description	Converts the configuration files of NTP to the config file for the daemon ntpd. Sanity limit is set to 1 second This binary is called by enntp
Command	buildntp [-h]
Results	
Example	

buildopenvpn

Description	Converts the configuration files of NTP to the config file for the daemon ntpd. Sanity limit is set to 1 second This binary is called by enntp
Command	buildopenvpn [-d <dir>] [-v] [-h] -d : set directory to write the config to <dir> -v : set verbose level to debug -h : display this help
Results	
Example	

buildsnmp

Description	Converts the configuration files of net-snmp to the config file for the daemon snmpd. This binary is called by ensnmp.
Command	Buildsnmp (no argument)
Results	
Example	

buildsquid

Description	Converts the configuration files to the config file for the daemon squid. This binary is called by enproxy.
Command	buildsquid (no argument)
Results	
Example	

buildssh

Description	Converts the configuration files of SSH to the config file for the daemon sshd. This binary is called by enservice
Command	buildssh [-d] -d : defaultconfig mode (force ssh key mode!)
Results	
Example	

buildwifi

Description	Converts the configuration files of Wifi and Network to the config file for the daemon hostapd. This binary is called by enwifi Note: Only available on wifi models
Command	buildwifi [-h] [-t] -h : display help message -t : will print 1 on stdout if wifi is activated, regarding configuration and timeobject, 0 otherwise
Results	
Example	

burnP6

Description	This program is designed to load x86 CPUs as heavily as possible for the purposes of system testing.
Command	BurnP6 (no argument)
Results	
Example	

certinfo

Description	Display the information related to the certificate defined by the file in the argument.
Command	certinfo <certfile> <certfile> : Certificate file located in /usr/Firewall/System/
Results	This command displays the same information about the certificate as the serverd command PKI CERT SHOW

Example

```
U2504C099999999999>certinfo ConfigFiles/Certificates/C=FR\ O=Stormshield\ OU=QA\ team\
CN=OCSP\ Authority/C=FR\ O=Stormshield\ OU=QA\ team\
CN=OCSP.expired.Responder1.test.cert.pem
 [Certificate]
 IssuerHash="d8e46c44"
 SubjectHash="04767abd"
 Issuer="/C=FR/O=Stormshield/OU=QA team/CN=OCSP Authority"
 Subject="/C=FR/O=Stormshield/OU=QA team/CN=OCSP.expired.Responder1.test"
 Version="3"
 SerialNumber="09"
 NotBefore="Nov 25 08:24:50 2010 GMT"
 NotAfter="Aug 29 08:24:50 2018 GMT"
 PublicKeyAlgorithm="rsaEncryption"
 SignatureAlgorithm="sha256WithRSAEncryption"
 [Subject]
 countryName="FR"
 organizationName="Stormshield"
 organizationalUnitName="QA team"
 commonName="OCSP.expired.Responder1.test"
 [Issuer]
 countryName="FR"
 organizationName="Stormshield"
 organizationalUnitName="QA team"
 commonName="OCSP Authority"
 [config]
 OCSP="http://www.ocspserver.com/,http://www.ocspserver2.com/"
 CRLDP="http://www.crldp.com/ca.crl,http://www.crldp2.com/ca.crl"
U2504C099999999999>
```

checkcrl

Description Check the validity of CRL.
Return minor or major alarm (via alarmd) if CRL has expired or will expire in 3 days or less

Command

```
checkcrl [-h] [-?] [-d] [-i] [-v] [-s] [-w <days>] [-t <timeout>] [-g <authority name> -p
<password>] [-f <minutes>]
[-c <scope>]
-d toggle debug mode
-i show information of the currently running checkcrl
-s do not use dns name resolution
-w [1-30] number of days to warn the expiration. default : 3
-t [0-3600] second before timeout, 0 is for unlimited. default : 300
-g <authority name> Disable check and generate the CRL for the given authority
-p <password> Give the passphrase of the authority in CRL generation mode
-f <minutes> number of minutes before the expiration of the current CRL to fetch a new CRL
-c <scope> Allow to specify the scope of the CRLs we want to check. Can be 'local' (default) or
'global'
-h -? this help
-v version
During the run can use [CTRL]-t to show current taskset
```

Results

Example

certenrol

Description Perform the SCEP operation for certificate enrolment.

Command

```
certenrol -o <"viewca"|"addca"|"getcert"|"checkcert"|"compca"|"cleanup"> [-p <profile>] [-u <URL>]
[-m <POST|GET>] [-t <transcation ID>] [-r <retry_count>] [-f <CA's fingerprint>] [-s
<"none"|"ondisk"$gt;]
 -o - Operation
 : "viewca" view the root CA\'s fingerprint
 : "addca" install the CA\'s from the SCEP server if it match the given fingerprint
 : "compca" compare the CA\'s fingerprint with the given one
 : "getcert" query for a certificate [renewal]
 : "checkcert" check for a previously pending certificate request
 : "cleanup" purge transaction IDs of previously accepted/rejected requests
 -p - Profile: The profile to use for this QUERY
 -u - Server URL: SCEP server entry point
 -m - Mode: HTTP Request mode (GET|POST)
 -t - The transaction ID from a previous pending certificate request
 -r - Number of attempt(s) left for a pending query
 -f - Fingerprint: The fingerprint to compare ("compca").
 -s - Seal TPM: ("none"|"ondisk").
```

Results

Example

curltool

Description Simple wrapper for the libfwcurl.

Command

```
curltool: -r <GET|POST> -u <URI(http://XXXXXXX> [-a <User Agent>] [-p <POST parameters>] [-o
(output filename)] -h
 -r Request : Send a GET or POST request
 -u URI : Uniform Resource Identifier (protocole + server + param)
 http://www.stormshield.eu/mapage.html?param1=value1&param2=value2...)
 -a User Agent : User Agent useed for this request
 Default agent is:<model>-<serial> : curltool (1.0)
 -p The POST parameters : post_param1=post_value1&post_param2=post_value2...
 -o Output File : Path to file for storing the output (!!! file is overwrite !!!)
 -h Help : Display this help
```

Results

Example

checkdb

Description Perform an integrity check on the given database.

Command

```
Usage: checkdb [-Bv] [-C] DBPATH
       checkdb [-Bv] -c   DBPATH
       checkdb -h
Actions:
  -c   Check the database integrity and update its backup if
not corrupted.
  -C   Check the database integrity, attempt to repair it if
corrupted and update its backup if not corrupted.
Default action is -C.
Options:
  -B : Don't create a backup of the database even if it pass
the integrity check.
  -v : Be verbose.
Exit Status:
  64 (USAGE)     Bad usage. Use -h to get some help.
  65 (DATAERR)   The database is corrupted and/or cannot be
repaired.
  70 (SOFTWARE)  Unforseen circumstances as in Half-Life.
  74 (IOERR)     Unable to empty the live database file.
  75 (TEMPFAIL)  Lock prevent operating on the live database.
  78 (CONFIG)    Missing live database file. Or unable to
create the backup directory.
```

Results

Exa
mple

checkfs

Description	Checks if the file system is clean or not. Must be used ONLY on UNMOUNTED filesystems !
Command	checkfs [-v] [-d] -[r] [-h]|<device> -v : Verbose mode -d : Dump mode -r : Root check -h : Help
Results	
Example	

checkfw

Description	Check firewall configuration
Command	checkfw [-v | --verbose] [-n | --nocolor] [-h | --help] -v, --verbose -n, --nocolor -h, --help
Results	
Example	

checkintegrity

Description	Check integrity of programs and files, based on MD5 file hashing
Command	checkintegrity : -h : this help -q : quiet mode
Results	
Example	U250XA0A0803770>checkintegrity < toto All checked files are correct U250XA0A0803770>

checkinternet

Description	Used by webd.
Command	checkinternet (no argument)
Results	Nothing if OK. Error message if KO.
Example	

checkversion

Description	Compare the current date with the date of the file /usr/Firewall/modules/ASQ.ko If the difference between this two dates is greater than 4 months, an alarm is sent.
Command	checkversion [-c][-h] -c : launch checkversion in command mode -h : display this help

Results	- Nothing if check is OK - Alarm sent if ASQ.ko is so old.
Example	

chpwd

Description	Mount the root device in rw access **(if error perform a filesystem check and try to mount it again)** Run script «enkeyboard» in order to set the language. Run «fwpasswd» program which change the SRP/SSH password for admin. Then finally reboot the firewall.
Command	Chpwd (no argument)
Results	New password is set for admin. 8 characters min. The firewall will reboot after password confirmation.
Example	U2504C099999999999>chpwd You are now with the keyboard langage configured on Firewall ## ## Change SRP/SSH password for admin ## ## setting password for admin enter password: verify: Modify SRP/SSH password of user 'admin' successful Firewall Rebooting ! Shutdown NOW! shutdown: [pid 738] *** FINAL System shutdown message from admin@U2504C099999999999 *** System going down IMMEDIATELY

clamavd

Description	Daemon of the antivirus clamav.
Command	**clamavd [-gdnvxh?]** **-d debug** **-h -? help** **-n <timeout in ms> noscan** **-v version** **-g full verbose for debug** **-x unpack cvd**
Results	
Example	

clamdefault

Description	Restore the clamav default configuration
Command	clamdefault
Results	
Example	

classifyhost

Description	Classifies an host based on his IP address
Command	classifyhost [-vht] <host_address> -v : verbose mode -h : show this help message -t : types of information to look for (geo, iprep, hostrep or all)
Results	Properties attached to this host
Example	Fw > classifyhost 8.8.8.8 GEOLOC: na:us HOSTREP: 0 IPREP: Fw > classifyhost -t geo 8.8.4.4 GEOLOC: na:us

classifyurl

Description	Classifies an url
Command	classifyurl [-v] <URL> -v:verbose mode
Results	Categories where url is classified
Example	Fw > classifyurl www.google.fr oemgroup=Search Engines & Portals

cleanfw

Description	Clean some files in the firewall
Command	cleanfw [-cls] -c : Clean the firewall after the script fwtest : Kill all test processes in progress : burnP6, bonnie++, netserver Restore default configuration, clear History -l : Remove all log in /log -s : Remove exlusives secrets of the firewall : CA, SSH keys, SMC information, SSL keys
Results	If -c option is used, the firewall must be rebooted.
Example	U2504C099999999999>cleanfw -c Kill all test process Remove all log Restore default configuration Restoration done, reboot recommended Clear History U2504C099999999999>

cleanpattern

Description	Remove obsolete files or directories related to the patterns.
Command	cleanpattern [-v][-h] -v : Verbose mode -h : Help
Results	
Example	

clearlog

Description	Clear log files.
Command	clearlog -a|<logname> [date] -a : clear all logs <logname> : clear <logname> file [date] : delete logs before this date Date format is "YYYY-mm-dd HH:MM:SS"
Results	
Example	

clearunwantedfiles

Description	Removes files from the Firewall, only applies to Kaspersky library files for the moment. A warning is displayed if High Availablity is enabled for this Firewall.
Command	clearunwantedfiles: -f: skips all usage controls of the Kaspersky libraries and forces the removal. -h: displays a help message with examples Kaspersky: Name for the files to remove. Kaspersky is the only option.
Results	Kaspersky library files are removed from the Firewall and a flag is set in the configuration files to prevent any reccurence (e.g. after an update).
Example	U2504C099999999999>removeunwantedfiles -f Kasperskyw Warning: HA is enabled, this action should be done on the passive UTM too.

conftuning

Description	Configuration tuning with CSV file List of supported operations : • **setconf** : set new configuration value to token • **delconf** : remove token or section • **setglobal** : set new global value • **createHA** : create HA cluster • **joinHA** : join HA cluster • **initTPM** : initialize TPM • **p12import** : import PKCS#12 file
Command	conftuning file.csv
Results	
Example	

corosync

Description	Corosync cluster engine.
Command	corosync: -f : Start application in foreground. -p : Do not set process priority. -v : Display version and SVN revision of Corosync and exit.
Results	
Example	

crlinfo

Description Display the information related to the CRL defined by the file in the argument.

Command

```
crlinfo <crlfile>
<crlfile> : certificate
```

Results This command display the result of the Hash function, the CRL version, the algorithm for signature and revoked certificates. (SignatureAlgorithm, RevokedCertificates)…

Example

```
U2504C099999999999>crlinfo stormshield_network_crl.pem
[Global]
Hash=99b2031a
Version=02
Issuer="/C=FR/ST=NORD/O=Stormshield/OU=NPI/L=VDA"
LastUpdate="Feb 18 15:08:45 2004 GMT"
NextUpdate="Mar 20 15:08:45 2004 GMT"
SignatureAlgorithm=md5WithRSAEncryption
[RevokedCertificates]
U2504C099999999999>
```

date

Description Get or set the current date and time of the Firewall.
The date cannot be changed if the NTP is running.

Command

```
date [-u] | [-d] | [-e] | [-b] «YYYY-MM-DD hh:mm:ss»
date : display system date in Stormshield format
 date [-b] "YYYY-MM-DD hh:mm:ss" : set new date in Stormshield Network format
 Remark : ntp daemon must be off
 -b: (for boot) do not send signal of date change to daemons
 date -u : display date in UNIX format
 date -d : display date in Stormshield Network format without timezone
 date -e : display date in seconds since Epoch
```

Results

Example

```
U2504C099999999999>date
"2004-01-15 15:37:29" zone=GMT tz=+0000 ntp=Off
U2504C099999999999>date -u
Thu Jan 15 15:37:32 GMT 2004
U2504C099999999999>date -d
2004-01-15 15:37:34
U2504C099999999999>date "2004-01-16"
"2004-01-16 15:37:47" zone=GMT tz=+0000 ntp=Off
U2504C099999999999>
```

ddnsclient

Description Updates the input of the dynamic DNS

Command

ddnsclient: [-t -vvv] {-i <interface>|-r} -a <ip address>
-h : print this usage message and exits
-i : interface name to check
-o : set offline
-r : parse every configuration to do renew and retry operations
-a : IP address
-f : run as a background daemon
-t : test mode : do not send request
-v : verbose level 1: print basic update steps
-vv : verbose level 2: more verbose, add steps and request
-vvv : verbose level 3: most verbose, add structure dump and different codes

Results

Example

decbackup

Description

Decypher a .na file (which is the save format of the configurations) to a .tgz file.

Command

decbackup -i <backup> -o <output archive>
[-p <password>] [-d]
-i <backup> : **name of encrypted backup input file**
-o <output archive> : **name of decrypted backup output file**
-p <password> : **password used for backup encryption**
-d : Dump backup header

Results

Example

defaultconfig

Description

Reset the configuration with the default one.
The current configuration is saved in the file «ConfigFiles.old»

Command

defaultconfig [options]
-f: Force
-r: Reboot after defaultconfig
-D: Only Restore the data partition
-p: Reset password
-u: Check usb token boot restoration
-d: Dump root partition after defaultconfig
-k: Keep autoupdate data (Pattern, Pvm, Clamav, Kaspersky, URLFiltering), default SSL proxy authority, default sslvpn full authority and ssh host keys
-l: Keep network configuration file
-n: Do not mark firewall as having a defaultconfig configuration
-c: No backup files (.old)
-L: Remove logs
-t: Reset TPM (TPM password is required)

Results

«Replacing current configuration with the default configuration»: The default configuration has been restored, the firewall must be rebooted to activate the modifications. The admin password is not modified.
«Previous defaultconfig found... remove it manually»: enter the following command :"rm -R /Firewall/ConfigFiles.old" and restart the procedure.

Example

```
U2504C099999999999>defaultconfig -f -p -r
deleting previous backup...
replacing current configuration with the default configuration...
restoring default password...
################################################
## Restore default SRP/SSH password for admin ##
################################################
Modify SRP/SSH password of user 'admin' successful
Shutdown NOW!
shutdown: [pid 990]
*** FINAL System shutdown message from admin@U2504C099999999999 ***
System going down IMMEDIATELY
U2504C099999999999>
System shutdown time has arrived
```

dhclient

Description The client DHCP.

Command

```
dhclient [-4|-6] [-SNTPRI1dvrxi] [-nw] [-p <port>]
 [-D LL|LLT] [--dad-wait-time seconds]
 [-s server-addr] [-cf config-file]
 [-df duid-file] [-lf lease-file]
 [-pf pid-file] [--no-pid] [-e VAR=val]
 [-sf script-file] [interface]*
```

Results

Example

dhclient-script

Description Called to modify the configuration DHCP client with the new IP address.

Command dhclient-script (no argument)

Results

Example

dhcpd

Description DHCP server.

Command

```
dhcpd
    [-p <UDP port#>] [-f] [-d] [-q] [-t|-T]
    [-4|-6] [-cf config-file] [-lf lease-file] [-tf trace-output-file]
    [-play trace-input-file]
    [-pf pid-file] [--no-pid] [-s server]
    [if0 [...ifN]]
```

Results

Example

dhcpinfo

Description Dump dhcp leases and return a section list

Command

```
dhcpinfo [-v] [-h]
-h : help
-v : verbose
```

Results

Example

dhcrelay

Description DHCP relay.

Command

```
dhcrelay [-4]
    [-d] [-q] [-a] [-D] [-A <length>] [-c <hops>] [-p <port>]
     [-b <BindAddr>]
     [-pf <pid-file>] [--no-pid]
     [-m append|replace|forward|discard]
     [-i interface0 [ ... -i interfaceN]
     [-iu interface0 [ ... -iu interfaceN]
     [-id interface0 [ ... -id interfaceN]
     [-U interface]
     server0 [ ... serverN]

dhcrelay -6
    [-d] [-q] [-I] [-c <hops>] [-p <port>]
     [-pf <pid-file>] [--no-pid]
     [-s <subscriber-id>]
     -l lower0 [... -l lowerN]
     -u upper0 [... -u upperN]

     lower (client link): [address%]interface[#index]
     upper (server link): [address%]interface
```

Results

Example

dhlease-script

Description This script is executed in synchronous mode by DHCP server

Command

```
dhlease-script (commit|release|expiry) <lease address> [<ethernet address> [<client hostname
option>]]
```

Results

Example

dialupstate

Description Display current state of dialups
Short delay exists between dialup state and link effective state.
Called during dialup boot and stop processes

Command

```
dialupstate [-h]
-h : Help
```

Results

Example

dkill

Description	Kill all daemons present in /var/supervise/ except the sshd daemon.
Command	dkill (no argument)
Results	Warning ! Calling this command will set the firewall in an unstable state because no more daemon are running. Launching this command is not recommended.
Example	U2504C099999999999>dkill No matching processes were found U2504C099999999999>

dmidecode

Description	Reports information about FW system's hardware.
Command	dmidecode [OPTIONS] Options are: -d, --dev-mem FILE Read memory from device FILE (default: /dev/mem) -h, --help Display this help text and exit -q, --quiet Less verbose output -s, --string KEYWORD Only display the value of the given DMI string -t, --type TYPE Only display the entries of given type -u, --dump Do not decode the entries --dump-bin FILE Dump the DMI data to a binary file --from-dump FILE Read the DMI data from a binary file -V, --version Display the version and exit
Results	
Example	

dnscache

Description	Cache DNS daemon.
Command	dnscache (no argument)
Results	
Example	

dstat

Description	Display the list of each daemon, with information of state (up or down) and with time duration from last change of the state.
Command	dstat [up|down|<daemon>]
Results	«asqd» : daemon name. «/var/supervise/asqd» : path of the daemon. «up / down» : daemon state. «pid xxx» : service number affected to the daemon. «xxx seconds » : time duration since the latest change of the state.

Example

```
V50XXA3E0000000>dstat
asqd : /var/supervise/asqd: up (pid 913) 4992 seconds
bird : /var/supervise/bird: down 4993 seconds
clamavd : /var/supervise/clamavd: down 4993 seconds
corosync : /var/supervise/corosync: down 4993 seconds
dhclient : /var/supervise/dhclient: down 4993 seconds
dhcpd : /var/supervise/dhcpd: down 4993 seconds
dhcrelay : /var/supervise/dhcrelay: down 4993 seconds
dns : /var/supervise/dns: down 4993 seconds
eventd : /var/supervise/eventd: up (pid 1012) 4989 seconds
hardwared : /var/supervise/hardwared: up (pid 911) 4992 seconds
ldap : /var/supervise/ldap: down 4993 seconds
logd : /var/supervise/logd: up (pid 906) 4993 seconds
mpd : /var/supervise/mpd: down 4993 seconds
ntp : /var/supervise/ntp: down 4993 seconds
racoon : /var/supervise/racoon: down 4993 seconds
rtadvd : /var/supervise/rtadvd: down 4993 seconds
serverd : /var/supervise/serverd: up (pid 916) 4992 seconds
sld : /var/supervise/sld: up (pid 1214) 4987 seconds
snmpd : /var/supervise/snmpd: down 4993 seconds
sshd : /var/supervise/sshd: up (pid 930) 4991 seconds
stated : /var/supervise/stated: up (pid 1126) 4987 seconds
switchd : /var/supervise/switchd: down 4993 seconds
tproxyd : /var/supervise/tproxyd: down 4993 seconds
```

dumpcert

Description	Check coherency between licence and the type of the IPS-Firewall.
Command	dumpcert (no argument)
Results	- Return nothing if OK - Return error message related to the error type.
Example	U2504C099999999999>dumpcert U2504C099999999999>

dumproot

Description	Do a backup of the file system to the backup partition.
Command	dumproot [-b] [-v] -b : Exectue dumproot at the next reboot -v : Verbose
Results	- Return nothing if OK - Return error message related to the error type.
Example	U2504C099999999999>dumproot U2504C099999999999>

enalived

Description	Active/Reload the alived daemon.
Command	enalived
Results	
Example	

enantivirus

Description	Active the antivirus configuration.
Command	enantivirus [-a] [-v] [-e] [-s] [-u] [-t [clamav][,kaspersky]] [-R reason] [-h?] -a : Launch autoupdate if base is missing -v : Verbose mode activated -e : reload engine of selected antivirus -s : reload scan settings of selected antivirus -u : Force a complete reload of antivirus -R : arg arg is the reason explaining why enantivirus was executed -t : By default all antivirus are selected -t clamav : Select Clamav -t kaspersky : Select Kaspersky -t clamav,kaspersky : In order to cumulate antivirus
Results	
Example	U2504C099999999999>**enantivirus -d -t clamav,kaspersky** **enantivirus: clamav init successful** **enantivirus: kaspersky init successful** U2504C099999999999>

enasq

Description	Activates ASQ configuration
Command	enasq [-b] [-f] -b : Execute following command : setconf /var/tmp/asqd Reload Obj 1 -f : Force asqd to reload (asqd will restart)
Results	
Example	

enauth

Description	Activates authentication daemon according to it's configuration. enauth is an alias to «ensl»
Command	See ensl command
Example	U2504C099999999999>enauth U2504C099999999999>

enbird

Description	Starts or stops bird according to its state
Command	enbird [-f] -f: restarts BIRD instead of sending SIGHUP
Results	
Example	

enbypass

Description	Activates/deactivates the SNi40 hardware bypass or get its configuration

Command	enbypass [-r] [-i] [-v] [-h] -r : rearm Run-time Bypass watchdog -i : return Bypass status (from Bypass hardware registers) -v : set verbose level to info -h : print this help message without option, activate/deactivate Bypass according to configuration file.
Example	U2504C099999999999>enbypass -i FW major version: 1 FW minor version: 6 Module capability: System-Off bypass supported Just-On bypass supported Run-Time bypass supported Run-Time Watchdog1 timer supported Run-Time watchdog1 timer capability: 1~255 seconds System-Off Bypass setting: Enable Just-On Bypass setting: Enable Run-Time Bypass setting: Disable Run-Time watchdog1 timer status: Timer Running Run-Time watchdog1 pair setting: bypass will Enable while timeout Run-Time watchdog1 timer count: 60 seconds I2C Address: 55 U2504C099999999999>

dynroute

Description	Modify IPS protected addresses list
Command	dynroute <4|6>,<new IP/prefix>,<new itf>,<old IP/prefix>,<old itf>
Example	dynroute 4,192.168.2.0/24,eth0,192.168.2.0/24,eth1 dynroute 6,1234:1234:1234:1234:175:57:0:254/80,eth0,,

encbackup

Description	Encrypt backup file
Command	encbackup -i <archive to protect> -o <backup> -t <backup content> [-c comment] [-p password] -i : input file -o : output file -t : backup content list -c : backup comment -p : encryption password
Example	encbackup -i backup.network.tgz -o backup.network.na -t network

enconsole

Description	Activates the console configuration. Sends SIGHUP to init and reloads tty configuration.

Command	enconsole [modem | nomodem] modem : nomodem : modem and nomodem parameters are set by builddialup
Results	
Example	

endhcp

Description	Activates DHCP daemon according to its configuration
Command	endhcp [-4|-6] [-b] -4 activates dhcpd configuration for IPv4 only. -6 activates dhcpd configuration for IPv6 only. When no IP version is specified, both IPv4 and IPv6 dhcpd configurations are activated. -b for boot process
Example	U2504C099999999999>endhcp U2504C099999999999>

endhcrelay

Description	Activates DHCP relay according to its configuration
Command	endhcrelay [-4|-6] -4 enable only dhcrelay on IPv4. -6 enable only dhcrelay on IPv6. When no IP version is specified, both IPv4 and IPv6 dhcrelays are configured.
Example	U2504C099999999999>endhcrelay U2504C099999999999>

endialup

Description	Activates the dialups configuration.
Command	Endialup [-u] -u : reload only if conf files did change
Results	All the dialup connections are re-negociated. Warning, the internet connection, the NAT filtering and the VPN tunnels in progress are re-initialized.
Example	U2504C099999999999>endialup U2504C099999999999>

endns

Description	Activates DNS daemon according to its configuration Reload NAT and Filter slot if configuration has been modified. Flush nated DNS connections if authorized clients list have changed.
Command	endns [-b] [-u] -b : Boot process -u : Update clients list. Don't restart dnscache : cache isn't flushed.

Example	U2504C099999999999> endns U2504C099999999999>

enevent

Description	Activates events daemon according to its configuration
Command	enevent (no argument)
Example	U2504C099999999999> enevent U2504C099999999999> modem and nomodem parametres are set by builddialup

enfilter

Description	Activates or re-activates a filtering slot after having modified it.
Command	enfilter [on | off] [-b] [-f] [-s] [-w] <-u | FilterSlot [-g GfilterSlot]> on : activate the last active slot. off : deactivate filter, pass from any to any without modifying the active slot configuration. -b : no filter rules at boot. -f : force the activation of the slot. -c : force commit of the slot even if equal to previous one. -s : display warning and error messages in a more easy-to-parse manner (buildfilter option) -u : re-activate the current slot -w : do not display warnings (buildfilter option) FilterSlot : activate the filtering slot. FilterSlot = 00 to 10 -g GfilterSlot : activate the global filtering slot. GfilterSlot = 00 to 10
Results	
Example	U2504C099999999999>enfilter 10 No QoS rules, QoS disabled U2504C099999999999>

engatemon

Description	**Activates the configuration of the advanced routing. Removes host memory** Call enevent to build hostcheck rules Call endialup to update dialup configuration Call ennetwork to update routing
Command	engatemon (no argument)
Example	U2504C099999999999>engatemon U2504C099999999999>

enha

Description	Rebuilds corosync. If configuration differs, stops stated then restarts corosync, then starts stated. Else simply restarts stated.

Command	enha [-w] [-u] [-v] [-f] -w : don't wait for the HA cluster to be ready -u : soft reload (won't rebuild Corosync configuration) -v : verbose -f : force Corosync and Gatewayd restart
Results	«ha is disabled!»: This message indicates that the «high availability» is not available on your IPS-Firewall.
Example	U2504C099999999999>enha U2504C099999999999>

enkeyboard

Description	Activates the configuration parameters for the keyboard language from file /usr/Firewall/ConfigFiles/language.
Command	enkeyboard (no argument)
Example	U2504C099999999999>enkeyboard U2504C099999999999>

enldap

Description	Activates LDAP daemon according to its configuration.
Command	enldap [-h] [-n] [-f][-v] -h: prints this help and exit -n: generates a new internal base -f: forces refresh -v : verbose
Example	U2504C099999999999>enldap U2504C099999999999>

envoucher

Description	Activates voucher LDAP daemon according to its configuration.
Command	envoucher [-h] [-n] [-f] -h: prints this help and exit -n: generates a new internal base -f: forces refresh
Example	U2504C099999999999>envoucher U2504C099999999999>

enlock

Description	Lock or unlock a script for a duration time.

Command	enlock -s <scriptname> [-c (lock|unlock|trylock)] [-d <timeout>] [-p <pid>] -s <scriptname> : used to deduce the name of the lock -c <action> : -c lock : wait for the lock to be available and take it -c unlock : release the lock -c trylock : try to take the lock, but abort immediatly if it's held by another process -c : Default action = lock -d <timeout> : maximum time to wait to get the lock Only valid for '-c lock' and between 0 and 300 -1 = forever (default) -p <caller pid> : pid written in the lock file (by default, getppid())
Example	

enlog

Description	Restart logd
Command	enlog (no argument)
Example	

ennetwork

Description	Reload the configuration parameters from the file /usr/Firewall/ConfigFiles/network - generate new object in case of option «-b» is not set : - synchronize tty status - update stateful structure - load ARP entries - update filter rules because dynamic rule have not been updated with the new IP address - update NAT because dynamic rule have not been updated with the new IP address - update VPN because dynamic rule have not been updated with the new IP address - update events because dynamic dns might have been changed - update authentification because interfaces might have been changed - update snmp because interfaces speed might have been changed - try to reset arp entry of hosts for Firewall IP addresses - notify switch of configuration change in case of option «-b» is set : - notify switch of configuration change

Command	ennetwork [-b] [-c <old_network_file> [<old_hacluster_file>] [<old_ha_conf_file>] [-C <new_network_file> [<new_hacluster_file>] [<new_ha_conf_file>] [-d] [-f] [-v [<ERROR|WARN|INFO|DEBUG>]] [-r] [-h] [-z] [-i] [-H] -b boot -c <old_network_file> [<old_hacluster_file>] [<old_ha_conf_file>] : old network configuration file *Defaults are :* • */var/tmp/network* • */var/tmp/hacluster* • */var/tmp/highavailability* -C <new_network_file> [<new_hacluster_file>] [<new_ha_conf_file>] : new network configuration file *Defaults are :* • */usr/Firewall/ConfigFiles/network* • */usr/Firewall/ConfigFiles/HA/hacluster* • */usr/Firewall/ConfigFiles/HA/highavailability* -d dry-run mode (display the operations that would be executed but do not execute them, imply -v) -f force : refresh all interfaces even if configuration has not changed -H no HA -h dhcp -r route -s check static routes -v verbose -z dad -i only updates interfaces configuration
Example	U2504C099999999999>ennetwork U2504C099999999999>

enntp

Description	Activates NTP daemon according to its configuration.
Command	enntp [-u | off][-h] -h : help -u : starts ntpd off : stops ntpd
Example	U2504C099999999999>enntp U2504C099999999999>

enobject

Description	Synchronize the object base (protocols, hosts, network, services)
Command	enobject [-a] [-h] -a : Do NOT synchronize ARP table (do not call 'arpsync -a') -h : Help
Example	U2504C099999999999>enobject U2504C099999999999>

enopenvpn

Description	Generate OpenVPN configuration from configuration files
Command	enopenvpn [-v] -v : activate verbose
Example	

enpattern

Description	Compiles the signatures files of the ASQ.
Command	enpattern [options] -h : print this help message -r : generate resource language file and ASQ template -c <ctx> : process only the specified context <ctx> -a : same as -r + compile context -p : generate dynamic plugin configuration based on plugin.def -l : list all available ASQ pattern contexts -n : display the version of the downloaded files and the version of generated .match separated by a dot (<download version>.<.match version>) -f : force mode -v : verbose mode -t <filename> : test Patterns input file, results will be produced into "/usr/Firewall/Data/CustomPatterns/Download/" directory. -z : generate an active-update archive for Custom Patterns
Example	U2504C099999999999>enpattern U2504C099999999999>

enproxy

Description	Activates the proxy daemon according to its configuration for HTTP, POP3, SNMP and FTP . Warning: 'enproxy' (without -u) is obsolete, use 'enfilter -u' instead.
Command	enproxy [-u] [-c] | [-p] | [-r] -u refresh tproxyd -c clear ssl fake certificates -p purge Squid cache and restart Squid
Example	U2504C099999999999>enproxy -u U2504C099999999999>

enrefresh

Description	Refresh all modules.
Command	enrefresh
Example	

enreport

Description Reporting module management:

- Mount/Unmount the underlying memory disk.
- Reload the related daemons.
- HA cluster synchronization.

Command

```
Usage: enreport [-v] [-r]
       enreport [-v] -H
       enreport [-v] -m
       enreport [-v] -u
Actions:
  -H   Synchronize the reports on the HA cluster and exit.
  -m   Mount the memory disk and exit.
  -r   Reload the daemons and exit.
  -u   Umount the memory disk and exit.
Default action is -r.
Options:
  -v   Be verbose.
```

Example

enservice

Description Activates serverd daemon according to its configuration.

Command

```
enservice [-h] [-b] [-s]
-h: print this help and exits
-b: don't reload filter slot
-s: secure mode
```

Example

```
U2504C0999999999999>enservice
U2504C0999999999999>
```

enroll

Description PAYG virtual machine enrollment utility

Command

```
enroll [-h] [-q] [-v] -e
 enroll [-h] [-q] [-v] [-f] -r
-h, --help : show this help
 -e, --enroll : enroll PAYG Virtual Machine on the online service
 -r, --renew : renew the PAYG licence (if needed)
 -f, --force : force the renew
 -q, --quiet : disable output
 -v, --verbose : verbose in console
```

ensl

Description Activates sld daemon according to its configuration.

Command

```
ensl [-u] | [-b]
-u : soft update
-b : boot
```

Example

ensmcrouting

Description	Activates smcrouterd daemon according to its configuration.
Command	ensmcrouting
Example	

ensnmp

Description	Activates snmpd daemon according to its configuration.
Command	ensnmp [-u] -u : Only send a SIGHUP to net-snmp
Example	

enswitch

Description	Reload the configuration and active the daemon which manages the ports of the switch on the G2 models.
Command	enswitch [-v] -v : verbose
Example	U2504C099999999999>enswitch U2504C099999999999>

entelemetryd

Description	Activates the telemetryd daemon
Command	entelemetryd
Example	U2504C099999999999>entelemetryd U2504C099999999999>

enthind

Description	Activates the thind daemon
Command	enthind
Example	U2504C099999999999>enthind U2504C099999999999>

entimezone

Description	Updates timezone information. Must be done during upgrade process with no service running Firewall has to be rebooted after changing timezone.

Command	entimezone [-F] [-u] [-d] [-r <1|2>] [-f] [-l] [-b] [-s <zone_name>] -F : Force (used with -u and -r options to prevent mistakes) -u : update timezone -r <1|2> : (disabled) configuration handled by ha if -r 1 -l : list timezones -s <zone_name> : set timezone to <zone_name> (format given by entimezone -l) -f : force reloading of the current timezone -b : check/restore timezone configuration regarding configuration flag : currentZone. (used at boot time only) -d : update timezone configuration file to "localtime"
Example	U2504C099999999999>entimezone -l Africa/ Africa/Algiers Africa/Luanda Africa/Porto-Novo Africa/Gaborone Africa/Ouagadougou Africa/Bujumbura ... Pacific/Midway Pacific/Wake Pacific/Efate Pacific/Wallis Pacific/Honolulu Pacific/Easter Pacific/Galapagos WET U2504C099999999999>entimezone -s Europe/Paris timezone change : GMT -> Europe/Paris. Needs reboot. If HA is enabled, needs HA synchronisation U2504C099999999999>

enurl

Description	Activate specified URL filtering.. Special slot 00 desactivates URL filtering configuration.
Command	enurl [--copyonly] --copyonly : allow bypassing call enproxy -u
Example	U2504C099999999999>enurl U2504C099999999999>

enuserreqd

Description	Activates the userreqd daemon
Command	enuserreqd
Example	U2504C099999999999>enuserreqd U2504C099999999999>

envpn

Description

Activate specified VPN configuration
Special slot 00 desactivates VPN configuration.
Note: envpn -u without changes in slot does NOTHING.

Command

envpn [-u | on | off | -h | slotnumber | -g globalslotnumber] [--dry-run]
-h : Help
-u|on : re-activate the current slot
off : deactivate the current slot
slotnumber : activate the local filtering slot (00<=slot<=10)
-g globalslotnumber: activate the global filtering slot (00<=slot<=10)
--dry-run: perform a trial run with no changes made (checks are run)

Example

```
U2504C099999999999>envpn 01
Activating new VPN tunnel...
Done.
current global slot =
current slot = IPsec 01
No QoS rules, QoS disabled
U2504C099999999999>
```

enwifi

Description

Build and refresh configuration for wifi. Will Start or Stop hostapd if needed.
Note: Only available on wifi models

Command

enwifi [-h]
enwifi -s
-h : display help message
-s : turn on/off wifi, if configuration allows it. It will rebuild hostapd config (only if hostapd is not in the state it must be) but not eventd's one.

Results

Example

eventd

Description

Events scheduler
Handle events (HA)
Handle slots programmation (ennat, enurl, envpn, enfilter)
Handle cron events (sfctl, ipnat)

Command

eventd (no argument)

Results

Example

```
U2504C099999999999>eventd
U2504C099999999999>
```

exportconf

Description

This program exports type of configuration to a file stored in /tmp by default

Command	exportconf -t filter -s index_number -g index_number [-o output_file_format] [-d directory_name] [-v] [-h] This program exports type of configuration to a file stored in /tmp by default. -t|--type filter : type of configuration to export -s|--slot index_number : export rules of the slot index of the local policy (default is slot index equal to 0) -g|--global index_number : export rules of the slot index of the global policy (default is slot index equal to 0) -o|--output output_file_format : output format of the created file (default is : csv) -d|--directory directory_name : indicate a directory to store the created file -v|--verbose : enable verbose -h|--help : print this help message
Example	SNI40A16B0743A8>exportconf -t filter Creating file: /tmp/SNI40A16B0743A8_policy0_filter_nat_rules_local_2017-04-18_1200.csv SNI40A16B0743A8> SNI40A16B0743A8>exportconf -t filter -g 10 -d /data/tmp Creating file: /data/tmp/SNI40A16B0743A8_policy10_filter_nat_rules_global_2017-04-18_1100.csv SNI40A16B0743A8>

fwinit

Description	Generate firewall key
Command	fwinit -f file
Example	

fwpasswd

Description	Change SRP and SSH password for admin.
Command	fwpasswd [-d] [-u] [-h] [-p password] : By default : change only SRP/SSH password for admin -d : Restore default SRP/SSH password for admin -u : Change UNIX password for admin -p password : Set "password" non interactively -h : Print help
Example	U2504C099999999999>fwpasswd ## ## Change SRP/SSH password for admin ## ## setting password for admin enter password: verify: Modify SRP/SSH password of user 'admin' successful U2504C099999999999>

fwshutdown

Description	This command does a virtual shutdown of the Firewall. The following commands are launched : enfilter 00 enservice -s
Command	fwshutdown (no argument)
Results	
Example	U2504C099999999999>fwshutdown U2504C099999999999>

fwsound

Description	Play sound on the Firewall speaker.
Command	fwsound [1 | 2 | 3 | 4] 1 : Start sound 2 : Stop sound 3 : Play predefined sound 1 4 : Play predefined sound 2
Results	
Example	U2504C099999999999>fwsound 3 U2504C099999999999>

fwtest

Description	Firewall tester Test hardware and various functions of the product. Used in production, between master and initialisation. fwtest tests a couple of firewall (2 modes), it test : network, cpu, ram, ... fwtest rounds a set of primary tests during by default 48 hours;
Command	fwtest [mode [-hvnbfd] [-l time] [-c count] [-p pktloss] [-i nb_if,duration[,nb_if,duration...]]] With no parameters, run in user friendly mode Parameters description (advanced mode) : mode: 1 or 2 (mandatory in advanced mode) -v: be verbose -l: test duration in hours (default: 24) -c: number of rounds before stop (default: infinite) -s: synchro timeout in seconds (default: 1200) -n: test network only (skip hd, led, sound, button and stress tests) -b: disable harddrive test result analyse -p: max packetloss for ping test (default: 0.001) -f: force interface media of one of firewall (mode 1) -d: disable daemons crash test -i: custom netperf test. Syntax : nb_if,duration,nb_if,duration,... Each couple (nb_if, duration) corresponds to a netperf test nb_if is the number of interfaces tested at the same time. duration is the duration of each test in seconds (default: 1,600) -h: display this help
Results	
Example	

fwupdate

Description

Install or update the Firewall.

Command

```
fwupdate [-r] [-F] (-f <file path> | -s)
 -r : reboot at the end, if no error
 -F : Force install (same version)
 -f : install one maj given by <file path>
 -s : install one maj given from stdin
```

Results

Example

```
U2504C099999999999>fwupdate
U2504C099999999999>
```

gatemon

Description

This is an internal tool used to configure the default route regarding the gateways' availability. Currently, it gets the returned information of the periodic «hostcheck» and decides, according to the configuration, to add or remove the default route of ASQ and/or FreeBSD.

Command

```
gatemon [-v] [-b] [-r] [-6] [-d <dhcp-mac-ifce-name>] [-i <dialup-mac-ifce-name>] [-o <router>]
[-g <gateway-host>] [-s <UP|DOWN>]
    -v : Force Verbosity to verbose file
     -b : Boot mode. (won't run enfilter)
     -r : Refresh IPv4 and IPv6 default routes
     -d : <dhcp-mac-ifce-name>: Can only be used for DHCPv4 interfaces ( ex: eth0 )
     -i : <dialup-mac-ifce-name>: Can only be used for dialup interfaces ( ex: ng0 )
     -o : <router>: Router object
     -g : <gateway-host>: Gateway host member of the router object
     -s : <UP|DOWN>: State of the specified gateway
     -6 : Manage IPv6 routes instead of IPv4 ones
```

Results

Example

gatemon [-v] [-b] -r

Refresh IPv4 and IPv6 default routes

gatemon [-v] [-b] [-6] -o <router-object> -g<gateway-host> -s <UP|DOWN>

Update the state of a gateway of a given router

gatemon [-v] [-b] [-6] -d <dhcp-mac-ifce-name> -s <UP|DOWN>

Update the state of the gateway corresponding to the generated object (Firewall_<dhcp-ifce>_router) representating the router of a dhcp client interface in all the router objects using this generated object as a gateway

gatemon [-v] [-b] [-6] -i <dialup-mac-ifce-name> -s <UP|DOWN>

Update the state of the gateway corresponding to the generated object (Firewall_<dialup-ifce>_peer) representating the dialup interface in all the router objects using this generated object as a gateway

gatewayctl

Description

Gatewayctl can communicate with gatewayd to change its configuration

Command gatewayctl

-h [--help] Display this message

-v [--verbose] Enable verbosity

--update_peer <peer_uid>:<peer_ip>
Update a member in the cluster with a serial number and the new IPv4. If it didn't exist in the cluster already, it will be added automatically.

--remove_peer <peer_uid>
Remove a member in the cluster with a serial number.

--list_peers
List members in the cluster.

--update_channel <channel_name>:<channel_type>:<channel_prio>
Update replication of a channel. It needs the channel name, its type ('topic' or 'service') and a priority ('high' or 'low'). If the replication of the channel didn't exist, it will be added.

--remove_channel <channel_name>:<channel_type>
Remove a replication of a channel. It need the channel name, its type ('topic' or 'service')

--list_channels
List replication of channels.

Results

```
Result of the commands.
```

Example

```
$> gatewayctl --list_channels
[test/topic-low_prio]
type=topic
priority=low
[test/topic-high_prio]
type=topic
priority=high

$> gatewayctl --remove_channel test/topic-high_prio:topic
[Result]
OK

$> gatewayctl --list_channels
[test/topic-low_prio]
type=topic
priority=low
```

gatewayd

Description Gatewayd replicates messages from internal messaging to members of an HA cluster.

Command gatewayd [-h] [-D] [-d]
-h [--help] Display this message.
-D [--daemonize] Daemonize, run in background.
-d [--debug] If another process is already running, send it a signal to switch its verbose mode, otherwise start with verbose mode enabled.

Results

Example

getalarmconf

Description Display alarm configuration

Command

```
getalarmconf
    -i <config index> [-p <protocol>] [-c "protocol|<ASQ context>"] [-a <alarm id>]
    [-v]
```

Results

Example

```
U250XA0A0803770>getalarmconf -i 1
protocol=dns context=protocol id=32 action=block level=major dump=0 new=0 origin=profile_template msg="RÃ©cursion de label DNS" modify=0 sensible=0 category=""
protocol=dns context=protocol id=38 action=block level=major dump=0 new=0 origin=profile_template msg="DNS id spoofing" modify=0 sensible=0 category=""
U250XA0A0803770>
```

getconf

Description Return the field value of the specified «file + section + item»

Command

```
getconf [-i <index>] <file> <section> [<item>] [<default>]
-i <index> :
 <file> : Path+name of the configuration file
 <section> : Section name inside the conf file
 <item> : Item inside the section
 <default> : Default value
 getconf -l <section> <item> [<default>]
-l :
 <section> : Section name inside the conf file
 <item> : Item inside the section
 <default> : Default value
 getconf -d <licencedateitem>
<licencedateitem> : One item of the following list :
 Update
Pattern
VulnBase
URLFiltering
URLVendor
AntiVirus
VirusVendor
AntiSPAM
SPAMVendor
NotBefore
NotAfter
Warranty
ExpressWarranty
 getconf -y <section> <item> [<default>]
-y :
 <section> : Section name inside the payg licence
 <item> : Item inside the section
 <default> : Default value
 getconf -p
```

Remarks	* getconf -i <index> <file> <section> returns the index-th "token=value" or only "token" (if no value) * getconf -i <index> <file> <section> <item> returns the index-th value for <item>, values must be coma separated * getconf -y <section> <item> [<default>] returns the PAYG licence item value * getconf -p checks if the PAYG licence is valid
Results	
Example	U2504C099999999999>getconf /usr/Firewall/ConfigFiles/network ethernet1 address 10.X.X.X U2504C099999999999>

getlicence

Description	Display licence information.
Command	getlicence
Results	List of all information and dates related to the licenses.

Example	V50XXA3E0000000>getlicence
	[Global]
	Version=9
	Temporary=0
	Comment=
	[Flags]
	PKI=1
	…
	ExpressWarranty=2037-12-31
	NotBefore=2002-05-14
	NotAfter=2037-12-31
	V50XXA3E0000000>

getmodel

Description	Display information about type and version number of the Firewall.
Command	getmodel [-a | -b | -t | -m | -p | -A | -B | -H | -S | -s | -n] -a : Display all version numbers and type of the Firewall. -b : Display Build model. -t : Display type value. -m : Display main model value. -p: Display equivalent running model for VM. -A: Display the generic model used. -B : Display branch name. -H : Display hardware type. -S : Display product serial number. -s : Display manufacturer serial. -n : Display hardware type name.
Example	U2504C099999999999>getmodel U250-B U2504C099999999999>

getpci

Description Display the list of PCI devices.

Command

```
getpci [-h] [-v/-e] [-c <PCI class>] [-s <PCI subclass>] [-C <chip>] [-d]
-h: help and display PCI classes and subclasses
-v: verbose
-e: enumerate (ignore -v option)
-c: get PCI class (format: -c "a class")
-s: get PCI subclass (format: -s "a subclass")
-C: get chip (format: -C 0x1234abcd)
-d: get attached driver (format: -d "attached driver")
```

Results

Example

```
U2504C099999999999>getpci
hostb0@pci0:0:0: class=0x060000 card=0x00000000 chip=0x06011106 rev=0x05 hdr=0x00
pcib1@pci0:1:0: class=0x060400 card=0x00000000 chip=0x86011106 rev=0x00 hdr=0x01
isab0@pci0:7:0: class=0x060100 card=0x00000000 chip=0x06861106 rev=0x40 hdr=0x00
atapci0@pci0:7:1: class=0x01018a card=0x00000000 chip=0x05711106 rev=0x06 hdr=0x00
uhci0@pci0:7:2: class=0x0c0300 card=0x12340925 chip=0x30381106 rev=0x1a hdr=0x00
uhci1@pci0:7:3: class=0x0c0300 card=0x12340925 chip=0x30381106 rev=0x1a hdr=0x00
none0@pci0:7:4: class=0x000000 card=0x00000000 chip=0x30571106 rev=0x40 hdr=0x00
fxp0@pci0:8:0: class=0x020000 card=0x020011d6 chip=0x12098086 rev=0x10 hdr=0x00
fxp1@pci0:9:0: class=0x020000 card=0x020011d6 chip=0x12098086 rev=0x10 hdr=0x00
fxp2@pci0:10:0: class=0x020000 card=0x020011d6 chip=0x12098086 rev=0x10 hdr=0x00
fxp3@pci0:11:0: class=0x020000 card=0x020011d6 chip=0x12098086 rev=0x10 hdr=0x00
none1@pci1:0:0: class=0x030000 card=0x85001023 chip=0x85001023 rev=0x6a hdr=0x00
U2504C099999999999>
```

getversion

Description Display Firewall software version

Command

```
getversion [-a|-b|-v|-d]
: By default, displays Firewall software name version
-a : Display ASQ name version
-b : Display build version
-d : Display devel branch, git SHA and the timestamp of the build
-v : Display revision number
```

Example

```
U2504C099999999999>getversion
Firewall software version 7.0.4
U2504C099999999999>
```

globalgen

Description Generate mapping between real network interface name and internal name

Command globalgen (no argument)

Results

Example

```
U2504C099999999999>globalgen
globalgen: 4 ethernet interfaces detected
globalgen: 0 WIFI interfaces detected
U2504C099999999999>
```

hadiff

Description	Compare local and peer configuration files
Command	hadiff <filter to diff>
Results	
Example	

halt

Description	Stops the IPS-Firewall. Warning ! No confirmation is required. This action stops the HA monitoring.
Command	When HA is enabled : Halt [-f] [-v] [-r] -f : Force -v : Verbose -r : Reboot
Example	1003D011690200701>halt Shutdown NOW! shutdown: [pid 829] *** FINAL System shutdown message from admin@U2504C099999999999 *** System going down IMMEDIATELY

hamode

Description	Display ha mode (active or passive fw)
Command	hamode
Example	V50XXA3E0000000>hamode HA Mode : Active

hardwarectl

Description	Send command to hardwared, like setting the front panel lights or setting the watchdog timer
Command	hardwarectl -c <command> [-a <command_arg>] arg must be an integer between 0 and 255 Commands list : HWD_STATE_WARNING HWD_STATE_NORMAL HWD_STATE_READY HWD_STATE_HA_READY HWD_STATE_SHUTTING_DOWN HWD_STATE_SYSTEM_OFF HWD_STATE_AMNESIAC HWD_CMD_STOPWATCHDOG HWD_CMD_SETWATCHDOG (argument needed) HWD_CMD_KEEPWATCHDOG HWD_CMD_STOPREFRESHBYPASSHW

Results	
Example	U2504C099999999999>hardwarectl -c HWD_STATE_WARNING U2504C099999999999>

hardwared

Description	Single point of communication with hardware addon Wait for button state change and react accordingly Animate minor/major LED Restore default configuration when button is pressed
Command	hardwared [-s] [-S on|off|blink] [-o on|off|blink] [-v] -s: print status -S: on|off|blink: status led test mode -o: on|off|blink: online led test mode -v: print hardware version
Results	
Example	U2504C099999999999>hardwared -v hardwared delos.alpha-NO_OPTIM U2504C099999999999>

hascp

Description	Scp to ha peer
Command	hascp
Results	
Example	

hassh

Description	Ssh ha peer
Command	hassh
Results	
Example	

hasynctest

Description	Tests rsync of hasync in dry mode
Command	hasynctest
Results	
Example	

hostcheck

Description Used by gatemon program. Test the availability of a specified host.

Command Hostcheck [-h|i|o] [-v] [-c <CheckHost>] [-t <Type>] <Host> <MaxWait> <MaxTries>
-h: The host address must be resolved using hosts file
-i: The host address is an IP address
-o: The host address must be resolved using the object database
-v: Force Verbosity to stdout
-c: Check <CheckHost> through <Host> instead of <Host>
-t: set a type of check (string used in the state file name, must not contain '/')
-q: Do not raise a system alarm
<Host>: The host to check. Can be an IP address, a resolvable host or an object depending on the configuration parameter Resolve in ConfigFiles/route at section [Config]
<MaxWait>: maximum time to wait for the response to the "ping" test before considering it a failure
Must be >=1 and <=10 (expressed in seconds)
<MaxTries>: maximum number of "ping" tries before returning that the host is considered DOWN or inactive
Must be >=1 and <=10

Results Returns 0|1|2|3
0 : if there has been NO change in the state of the checked host
1 : if there HAS been a change in the state of the checked host and it is UP
2 : if there HAS been a change in the state of the checked host and it is DOWN
3 : for invalid argument

Example

ifinfo

Description Gives the information of the network interfaces configurations.

Command	ifinfo <name> <command> [<index>] <name> : **in** **out** **dialup** **pptp** **ethernet** **vlan** **ipsec** **gretun** **gretap** **loopback** <command> : **mac_name** : get the name of the network interface **mac_address** : get the MAC address of the network interface **mac_throughput** : get the maximum media throughput **ip_address** : get the configured IP address **ip_netmask** : get the network address **ip_broadcast** : get the broadcast address **ip_network** : get the network address **count** : get the count of interface type (<name> = dialup, pptp, ethernet, vlan, ipsec, gretun, gretap, loopback) **ip_config** : get the configured IP address/mask **bridge_name** : if bridged, return bridgename **peer_address** : get the peer address of P2P interface [<index>] : optional.
Results	
Example	U2504C099999999999>ifinfo interface list: bridge0 10.2.32.254/255.255.0.0 out (fxp1) in (protected,fxp0) dmz1 (protected,fxp2) dmz2 (protected,fxp3) ipsec (enc0) U2504C099999999999>

keepalive

Description	Sends IPSec keepalive packets
Command	Keepalive [time_value] time_value : 30, 60, 120, 300, 600, 0
Results	
Example	

kgdbload.sh

Description	Load kernel debugger on core file name /log/crash/vmcore.

Command	kdbgload.sh [coresuffix] coresuffix: index appended to the core filename
Results	
Example	kdbgload.sh 2

launchctl

Description	launchd interface for daemons management.
Command	launchctl <subcommand> help This help output. load Load configuration files and/or directories. unload Unload configuration files and/or directories. remove Remove/stop specified job. list List jobs and information about jobs. sig Send a signal to a specified job. -u Start the specified job (will be restarted on exit). -o Start the specified job (will not be restarted on exit). -d Stop specified job. -p Send a STOP signal to the service. -c Send a CONT signal to the service. -h Send a HUP signal to the service. -a Send a ALRM signal to the service. -i Send a INT signal to the service. -t Send a TERM signal to the service. -k Send a KILL signal to the service. -1 Send a USR1 signal to the service. -2 Send a USR2 signal to the service. -x Prepare for launchd shutdown. wd Svwaitdown -k. wu Svwaitup.
Results	
Example	

launchd

Description	Daemon which manages other daemons.
Command	launchd [-d | -f | -h] -d : Daemonize. -h : This usage statement. -f : Force.
Results	
Example	

ldapcheck

Description	Command line program to check information in a ldap

Command

ldapcheck --user <userid>[--domain <domain>] [--group <group>] --check <command>
--user : id of the user to be checked
--domain : domain used for the check, default one if not specified
--group : group used for the check
--check : the kind of check you want like 'belongs-to-group'
* 'belongs-to-domain': check if the user belongs to the domain passed in parameters
* 'belongs-to-group': check if the user belong to the group passed in parameters

Results

[ldapcheck]
Result=ko|ok

Example

ldapcheck --user "test" --group "testgroup" --check "belongs-to-group"

licenceupdate

Description

Command line program to download and activate the firewall license

Command

licenceupdate [-d|-D] [-a|-A] [-f | (-P <proxyhost> -p <proxy_port> [-u <proxy_user> [-s <proxy_pass>]])]
-d : download new licence
-D : force download new licence
-a : activate licence
-A : force activate licence
-c : check if a new licence has been downloaded
-P, -p, -u, -s : http proxy settings
-f : use configuration file for proxy settings
-t : number of retries per licence
<no arg> : use configuration file

Results

Example

U2504C099999999999>licenceupdate -d
-- Prepare --
-- Download -- (/usr/Firewall/Data/Licence/U2504C099999999999.licence)

logctl

Description

Display information logs and reports

Command

```
logctl [-c [-ri]] [-h] [-t <log_id>] [-q] [-v]
options:
-h: this help.
-c [-ri]: print information about SHM and failure counters.
    -r: reset information after printing them
    -i: print information on one line
 -t <log_id>: Test reports regex. Read fake log lines from stdin
-T <log_id>: Send log lines to Logd. Read log lines from stdin
    + Valid values for log_id are:
    l_alarm, l_connection, l_filter, l_web, l_smtp, l_date, l_ftp,
    l_system, l_plugin, l_vpn, l_auth, l_server, l_pop3, l_xvpn,
    l_monitor, l_pvm, l_count, l_filterstat, l_ssl
 -o <report> <period> : Get the requested report.
Unable to load reports configuration: Nothing to do (State=0 ?)
    + Possible periods are:
    lasthour, day-0, day-1, day-2, day-3, day-4, day-5, day-6,
    day-7, last7days, last30days, all
 -q: Quiet, don't insert info in log files
-v: Verbose (-vv enables debug)
```

Results

Example

logd

Description Log daemon

Command

```
logd [-t] [-d] [-D] [-h?] [-v]
-t check if logd is ready
-d activate verbose mode
-D daemonize
-h -? help
-v version
```

Results

```
U2504C099999999999>logd -d
LOGD starts in verbose mode.
2011-04-11 16:26:34 | logd_config_deb | LOGD verbose ON
2011-04-11 16:26:34 | logd_config_deb | Verbose=0, no verbose activated. Please put the wanted debug level into this token (between 1 and 3)
2011-04-11 16:26:34 | logd_config_deb | LOGD verbose OFF
```

Example

```
U2504C099999999999>logd -D
```

logdisk

Description Manage partition logs.

Command

```
logdisk ( -s | -l | -f [<disk/partition> [-w]] | -m [<partition>] | -u | -c | -b | -h ) [-v]
-s : Display log partition status
-l : List all available disks/partitions.
-f [<disk/partition>] : Format current/specified log disk/partition.
    For current partition, unmount, format and mount it automatically.
    -w option forces the add of a swap partition even if model does not require it
 -m [<partition>] : Mount current/specified partition. Unmount last partition if necessary.
-u : Unmount current partition.
-c : Do sanity checks on log partition. Try to mount back partition in case of problem.
-b : Used during boot to mount log partition if necessary. Skip daemons interaction.
-h : Display this usage.
-v : Verbose mode
```

Results

Example

modemctl

Description Configuration helper for usb modem

Command

```
modemctl ( devinfos [<device>] | eject <device> | reset <device> ) [-v]
A device is referenced by its unit address with the ugen<unit>.<addr> form (ugen4.2)

devinfos : Display information about all plugged USB devices.
eject : Power off <device> to eject safely.
reset : Restart <device>. Useful to trigger probing by the kernel.

-v --verbose : Verbose mode
-h --help : This help
```

Results

Example

```
./modemctl devinfos
ugen4.2: <Mass Storage Generic> at usbus4, cfg=255 md=HOST spd=HIGH (480Mbps) pwr=OFF
(200mA)
VendorId=058f
ProductId=6387

ugen4.3: <USB Modem USB Modem> at usbus4, cfg=0 md=HOST spd=HIGH (480Mbps) pwr=ON
(500mA)
VendorId=1c9e
ProductId=9603

ugen4.4: <HUAWEIMOBILE HUAWEIMOBILE> at usbus4, cfg=0 md=HOST spd=HIGH (480Mbps)
pwr=ON (2mA)
VendorId=12d1
ProductId=15cf

./modemctl eject ugen4.4
ugen4.4 has been powered off and can be ejected safely
```

mpd

Description Multi network protocol daemon

Command	mpd [options] [system] Options: -b, --background : Run as a background daemon -d, --directory config-dir : Set config file directory -k, --kill : Kill running mpd process before start -f, --file config-file : Set configuration file -o, --one-shot : Terminate daemon after last link shutdown -p, --pidfile filename : Set PID filename -s, --syslog-ident ident : Identifier to use for syslog -m, --pam-service service : PAM service name -v, --version : Show version information -h, --help : Show usage information
Results	
Example	

ndmesg

Description	Print the kernel ring buffer with date
Command	ndmesg (no argument)
Results	
Example	

netperf

Description	Network performance benchmark server. For those options taking two parameters, at least one must be specified; specifying one value without a comma will set both parameters to that value, specifying a value with a leading comma will just set the second parameter, a value with a trailing comma will just set the first. To set each parameter to unique values, specify both and separate them with a comma. * For these options taking two parameters, specifying one value with no comma will only set the first parameter and will leave the second at the default value. To set the second value it must be preceded with a comma or be a comma-separated pair. This is to retain previous netperf behaviour.

Command

netperf [global options] -- [test options]
-a send,recv : Set the local send,recv buffer alignment
-A send,recv : Set the remote send,recv buffer alignment
-B brandstr : Specify a string to be emitted with brief output
-c [cpu_rate] : Report local CPU usage
-C [cpu_rate] : Report remote CPU usage
-d : Increase debugging output
-D [secs,units] : * Display interim results at least every secs seconds
using units as the initial guess for units per second
-f G|M|K|g|m|k : Set the output units
-F fill_file : Pre-fill buffers with data from fill_file
-h : Display this text
-H name|ip,fam : * Specify the target machine and/or local ip and family
-i max,min : Specify the max and min number of iterations (15,1)
-I lvl[,intvl] : Specify confidence level (95 or 99) (99)
and confidence interval in percentage (10)
-l testlen : Specify test duration (>0 secs) (<0 bytes|trans)
-L name|ip,fam * : Specify the local ip|name and address family
-o send,recv : Set the local send,recv buffer offsets
-O send,recv : Set the remote send,recv buffer offset
-n numcpu : Set the number of processors for CPU util
-N : Establish no control connection, do 'send' side only
-p port,lport : * Specify netserver port number and/or local port
-P 0|1 : Don't/Do display test headers
-r : Allow confidence to be hit on result only
-t testname : Specify test to perform
-T lcpu,rcpu : Request netperf/netserver be bound to local/remote cpu
-v verbosity : Specify the verbosity level
-W send,recv : Set the number of send,recv buffers
-v level : Set the verbosity level (default 1, min 0)
-V : Display the netperf version and exit

Results

Example

netserver

Description

It's a network performance benchmark server.
Listens for connections from a benchmark, and responds accordingly.
It can either be run from or as a standalone daemon (with the -p flag).
If run from, the -p option should not be used.

Command

Usage: netserver [options]
Options:
-h : Display this text
-d : Increase debugging output
-L name,family : Use name to pick listen address and family for family
-p portnum : Listen for connect requests on portnum.
-4 : Do IPv4
-6 : Do IPv6
-v verbosity : Specify the verbosity level
-V : Display version information and exit

Results

Example

newldapbase

Description	Generate an LDAP base. Called by enldap.
Command	Usage: newldapbase [-o Orgname -d DC [-p tmppass]] [-v] -o Orgname : organization name -d DC : domain component -p tmppassword : temporary password -v : verbose -h : displays help
Results	
Example	

ngstat

Description	Gives information on the interfaces generated by mpd daemon.
Command	ngstat [name] [protocol] name : netgraph interface name listed in /var/run/mpd.pid protocol : <PPTP | pptp> <PPPOE | PPPoE | pppoe> <L2TP | l2tp >
Results	
Example	

nhup

Description	Sends SIGHUP signal to specified daemon (must be a daemon from /var/supervise)

Command	nhup [daemon name] Here is the daemons name list : alived asqd bird clamavd corosync dhclient dhcpd dhcrelay dns eventd hardwared ldap logd mpd ntp racoon rtadvd serverd sld smcrouterd snmpd sshd stated switchd tproxyd
Results	
Example	

nkill

Description	Kill the specified daemon (must be a daemon listed in /var/supervise)

Command

nkill [daemon name]
Here is the daemons name list :
alived
asqd
bird
clamavd
corosync
dhclient
dhcpd
dhcrelay
dns
eventd
hardwared
ldap
logd
mpd
ntp
racoon
rtadvd
serverd
sld
smcrouterd
snmpd
sshd
stated
switchd
tproxyd

Results

Example

nmemstat

Description Retrieve memory usage statistics.

Command

nmemstat
[-v] [-M core] [-N system] [-w interval] [-a | pid | core ...] [-i | -s]
-a : Display the Memory usage of all loaded lib and binaries on the UTM
-s : Display the overall Memory usage and the rate of current user memory of the UTM
-i : (with -s only) ONLY display the rate of current user memory
-w : refresh interval in ???
-M : core ???
-N : system ???
-v : verbose

Results

Physical memory	: 1003MB
User memory	: 727MB
Wired memory	: 275MB
Current user memory	: 84MB
Used user memory	: 12%

Example nmemstat -i -s

nraid

Description	Creates and rebuilds raid.
Command	nraid -h | -c | -s | -z | -a | -w <disk> | -r -h : print this help and exit -c : create the RAID array -s: show current disks status -z: reset raid ata port and probe new plugged disk -w: wipe disk info and make it blank -r : rebuild raid if one disk has failed -a: try to create automaticaly RAID silently
Results	
Example	

nrestart

Description	Restart the specified daemon (must be a daemon listed in /var/supervise)
Command	nrestart [daemon name] Here is the daemons name list : alived asqd bird clamavd corosync dhclient dhcpd dhcrelay dns eventd hardwared ldap logd mpd ntp racoon rtadvd serverd sld smcrouterd snmpd sshd stated switchd tproxyd
Results	
Example	

nsbsdstart

Description	Called during boot to set up some system values.
Command	nsbsdstart (no argument)

Results	
Example	

nsbsdstop

Description	Updates /boot/loader.conf according to the configuration. Called during shutdown.
Command	nsbsdstop [-d] -d : Activate debugging
Results	Information written in file /boot/loader.conf
Example	

nsrpc

Description	This command is used to have access to the serverd commands. The -f option is used to force the « admin » connection. The -r option is used to specify the access rights of the user. The list of access rights is written as a string with each right separated by a comma. The rights that can be specified are the following : modify, base, other, log, filter, vpn, url, pki, object, user, admin. Encoding depend on the locale LC_ALL
Command	nsrpc [-a|-d|-f] [-C connection timeout] [-R reading timeout] [(-4|-6)] [-c command file] [-l log file] [-r rights] user[:password]@server[:port] nsrpc [-d|-f] [-C connection timeout] [-R reading timeout] [(-4|-6)] -t targets file -c command file [-l log file] [-r rights] -a: automatically connect with default password -c: set file with firewall commands -C: set connection timeout (min: 5 ; max: 600 ; default: 600) -d: activate debug -f: force login -l: set file to output commands and firewall results -r: set rights -R: set reading timeout (min: 5 ; max: 600 ; default: 600) -t: set file with target firewalls ("IP[;port];login;password" on each line) -h: this usage -4: connect using IPv4 (default) -6: connect using IPv6 WARNING : stormshield_network.ca file must be in the same path as nsrpc
Results	

Example

```
U2504C0999999999999>nsrpc admin@127.0.0.1
Welcome to Cipher/SRP client
Enter password:
Connecting to 127.0.0.1...
Using SRP authentication only.
User=admin Level="modify,mon_
write,base,other,log,filter,vpn,url,pki,object,user,admin,network,route,maintenance,asq,pvm,globalo
bject,globalfilter,globalother" SessionLevel="modify,mon_
write,base,other,log,filter,vpn,url,pki,object,user,admin,network,route,maintenance,asq,pvm,globalo
bject,globalfilter,globalother"
Srpclient>
```

nstart

Description Start the specified daemon (must be a daemon listed in /var/supervise)

Command nstart [daemon name]

Here is the daemons name list :

alived
asqd
bird
clamavd
corosync
dhclient
dhcpd
dhcrelay
dns
eventd
hardwared
ldap
logd
mpd
ntp
racoon
rtadvd
serverd
sld
smcrouterd
snmpd
sshd
stated
switchd
tproxyd

Results

Example

nstop

Description Stop the specified daemon (must be a daemon listed in /var/supervise).

Command	nstop [daemon name] Here is the daemons name list : alived asqd bird clamavd corosync dhclient dhcpd dhcrelay dns eventd hardwared ldap logd mpd ntp racoon rtadvd serverd sld smcrouterd snmpd sshd stated switchd tproxyd
Results	
Example	

ntpd

Description	NTP daemon program.
Command	ntpd [-<flag> [<val>] | --<name>[{=| }<val>]]..[<server1> ... <serverN>]

Flag	Arg	Option-Name	Description
-4	no	ipv4	Force IPv4 DNS name resolution - prohibits the option 'ipv6'
-6	no	ipv6	Force IPv6 DNS name resolution - prohibits the option 'ipv4'
-a	no	authreq	Require crypto authentication - prohibits the option 'authnoreq'
-A	no	authnoreq	Do not require crypto authentication - prohibits the option 'authreq'
-b	no	bcastsync	Allow to sync to broadcast servers
-c	Str	configfile	Configuration file name
-d	no	debug-level	Increase output debug message level - may appear multiple times
-D	Str	set-debug-level	Set the output debug message level - may appear multiple times

-f	Str	driftfile	Frequency drift file name
-g	no	panicgate	Allow the first adjustment to be Big - may appear multiple times
-G	no	force-step-once	Step any initial offset correction.
-i	no	jaildir	Built without --enable-clockctl or --enable-linuxcaps or --enable-solarisprivs
-I	Str	interface	Listen to an interface name or address - may appear multiple times
-k	Str	keyfile	Path to symmetric keys
-l	Str	logfile	Path to log file
-L	no		
-n	no	nofork	Do not fork - prohibits the option 'wait-sync'
-N	no	nice	Run at high priority
-p	Str	pidfile	Path to PID file
-P	Num	priority	priority Process priority
-q	no	quit	Set the time and quit - prohibits these options: saveconfigquit wait-sync
-r	Str Str	propagationdelay saveconfigquit	Broadcast/propagation delay Save parsed configuration and quit - prohibits these options: quit wait-sync
-s	Str	statsdir	Statistics file location
-t	Str	trustedkey	Trusted key number
-u	---	user	built without --enable-clockctl or --enable-linuxcaps or --enable-solarisprivs
-U	Num Str Str	updateinterval var dvar	interval in seconds between scans for new or dropped interfaces make ARG an ntp variable (RW). May appear multiple times. make ARG an ntp variable (RW|DEF). May appear multiple times.
-w	Num	wait-sync	Seconds to wait for first clock sync - prohibits these options: nofork quit saveconfigquit
-x	no	slew	Slew up to 600 seconds opt version Output version information and exit
-?	no	help	Display extended usage information and exit
-!	no	more-help	Extended usage information passed thru pager

Options are specified by doubled hyphens and their name or by a single hyphen and the flag character.

The following option preset mechanisms are supported:

- examining environment variables named NTPD_*

Results

Example

ntpq

Description

Standard NTP query program

Command

ntpq [-<flag> [<val>] | --<name>[{=| }<val>]]... [host ...]

Flag	Arg	Option-Name	Description
-4	no	ipv4	Force IPv4 DNS name resolution - prohibits the option 'ipv6'
-6	no	ipv6	Force IPv6 DNS name resolution - prohibits the option 'ipv4'
-c	Str	command	run a command and exit - may appear multiple times
-d	no	debug-level	Increase output debug message level - may appear multiple times
-D	Str	set-debug-level	Set the output debug message level - may appear multiple times
-i	no	interactive	-i no interactive Force ntpq to operate in interactive mode - prohibits these options: command peers
-n	no	numeric	numeric host addresses
	no	old-rv	Always output status line with readvar
	opt	version	Output version information and exit
-p	no	peers	Print a list of the peers -prohibits the option 'interactive'
-w	no	wide	Display the full 'remote' value
	opt	version	output version information and exit
-?	no	help	Display extended usage information and exit
-!	no	more-help	Extended usage information passed thru pager

-> opt save-opts Save the option state to a config file
-< Str load-opts Load options from a config file

Results

Example

```
U2504C099999999999>ntpq
ntpq>
...
ntpq>quit
U2504C099999999999>
```

objectsync

Description

Synchronize the dynamic objects.

Command

objectsync [-v] [-c] [-t <host> | -4 <host> | -6 <host>]
-h: this help
-v: turn verbose on
-c: use the cached value of the dynamic object, if it doesn't exist, then perform a DNS query
-t <host>: resolve the IPv4 and IPv6 address of host <host>
-4 <host>: resolve the IPv4 address of host <host>
-6 <host>: resolve the IPv6 address of host <host>

Results

Example

objecttest

Description Tests, benchmarks and dumps objects configurations.

Command

```
objecttest
    [-i <num>] [-ng]
     [-d <all | host | net | router | group | expanded_group | proto | service | interface>] |
     [-p <refresh | gethost | getnet | getrouter | findgroup>]
     [-u host | net | router | group|service|servicegroup|proto|user|qid]
```

Remark :default action is equivalent to "objecttest -d all"

```
-h : print this usage message and exits
 -v : more verbose
 -ng : don't print generated host or network
 -nc : don't print configuration
 -d : dump object structures or list configurations.
 -c : configuration directory (requires a libnbase in debug mode).
 -p : execute benchmark
 -u : usage. Check if object is in use somewhere in the configuration
 -t : inventory. list all objects used in the configuration
 : at least one object refresh is done per action
 -i : number of iteration for performing action or dumping
```

Results

Example

ldapmanager

Description Manage an internal LDAP base.

Command

```
ldapmanager
    ldapmanager -m export -f <LDIF output file path>
     ldapmanager -m import -f <LDIF input file path>
     ldapmanager -m adduser -u <uid> -n <name> [-g <gname>]
     ldapmanager -m remuser -u <uid>
     ldapmanager -m listuser
     ldapmanager -m raz
```

Remark :default action is equivalent to "objecttest -d all"

```
ldapmanager -m export : Export the LOCAL LDAP base to LDIF file
 ldapmanager -m import : Import a LDIF file to the LOCAL LDAP
 ldapmanager -m adduser : Add an user to the LOCAL LDAP
 ldapmanager -m remuser : Remove an user from the LOCAL LDAP
 ldapmanager -m listuser : List the user(s) in the LOCAL LDAP
 ldapmanager -m raz : Remove ALL UER(S) from the LOCAL LDAP
```

Results

Example

```
ldapmanager -m export -f ~/Configfiles/data/base.ldif
 ldapmanager -m import -f ~/Configfiles/data/base.ldif
 ldapmanager -m adduser -u user_uid -n user_name -g user_gname
 ldapmanager -m remuser -u user_uid
 ldapmanager -m listuser
 ldapmanager -m raz
```

openvpn

Description	OpenVPN Daemon
Command	
Results	
Example	

openvpn_auth

Description	Authenticate user and control his access
Command	openvpn_auth tcp|udp openvpn_auth tcp : Authenticate TCP user openvpn_auth udp : Authenticate UDP user
Results	
Example	

openvpn_auth_tcp

Description	Authenticate TCP user and control his access
Command	openvpn_auth_tcp (no argument)
Results	
Example	

openvpn_auth_udp

Description	Authenticate UDP user and control his access
Command	openvpn_auth_udp (no argument)
Results	
Example	

openvpn_clean_usertable

Description	Called by launchd on OpenVPN daemon shutdown and ensures to clean ASQ users table entries flagged with OPENVPN method
Command	openvpn_clean tcp|udp openvpn_clean tcp : Clean ASQ TCP users table entries flagged with OPENVPN method openvpn_clean udp : Clean ASQ UDP users table entries flagged with OPENVPN method openvpn_clean all : Clean ASQ TCP and UDP users table entries flagged with OPENVPN method
Results	
Example	

openvpn_connect

Description	Register user in ASQ users table
Command	openvpn_connect tcp|udp openvpn_connect tcp : Register TCP user in ASQ users table openvpn_connect udp : Register UDP user in ASQ users table
Results	
Example	

openvpn_connect tcp

Description	Register OpenVPN TCP user in ASQ users table
Command	openvpn_connect tcp
Results	
Example	

openvpn_connect udp

Description	Register OpenVPN UDP user in ASQ users table
Command	openvpn_connect udp
Results	
Example	

openvpn_disconnect

Description	Remove user in ASQ users table
Command	openvpn_disconnect tcp|udp openvpn_disconnect tcp openvpn_disconnect udp
Results	
Example	

openvpn_disconnect udp

Description	Remove OpenVPN UDP user in ASQ users table
Command	openvpn_disconnect udp
Results	
Example	

openvpn_disconnect_tcp

Description	Remove OpenVPN TCP user in ASQ users table
Command	openvpn_disconnect_tcp
Results	
Example	

p12import

Description	Import PKCS#12 file
Command	p12import -f <file path> [-p <password>] [-v] -v : verbose mode -t : if specified, TPM seal is forced to ONDISK, NONE otherwise -p : password associated with PKCS#12 file -f : import PKCS#12 file given by <file path>

paygprep

Description	PAYG template provisioning utility
Command	paygprep This wizard provisions the virtual machine to a PAYG template.

powerstatus

Description	Display status of power slots
Command	powerstatus [-s <0|1>] -s <0|1>: slot to display (if missing, display all slots)
Results	
Example	SN6KXA04F0015A8>powerstatus POWER0: OK POWER1: OK

pppdown

Description	Called when a PPP link is down.
Command	pppdown <dialup-interface> dialup-interface : interface name to check
Results	
Example	

pppdown2

Description	Called in background when a PPP link is down.
Command	pppdown <dialup-interface> dialup-interface : interface name to check
Results	
Example	

pppup

Description	Called when a PPP link is up.
Command	pppup <interface> inet <local-ip> <remote-ip> <authname> [dns1 ip] [dns2 ip] <ifname> : Interface name <local-ip> : IP address of link's local endpoint <remote-ip> : IP address of link's remote endpoint <authname> : authentication name <dns1 ip> : Domain name server primary IP address <dns2 ip> : Domain name server secondary IP address
Results	
Example	

pppup2

Description	Called in background when a PPP link is up.
Command	pppup <interface> inet <local-ip> <remote-ip> <authname> [dns1 ip] [dns2 ip] <ifname> : Interface name <local-ip> : IP address of link's local endpoint <remote-ip> : IP address of link's remote endpoint <authname> : authentication name <dns1 ip> : Domain name server primary IP address <dns2 ip> : Domain name server secondary IP address
Results	
Example	

pvmgenconf

Description	Used by autoupdate in order to generate the configuration files for pvm from the downloaded files.

Command	pvmgenconf -d <autoupdate files dir> [-c <core dir>] [-s <sodb dir>] [-b <banner dir>] [-v <vuln rules file>] [-V <vuln descs file>] [-p <pof rules file>] [-l <us|fr>:<language file> [-l ...]] -d <autoupd files dir> : Autoupdate download directory -c <core dir> : Pvm main directory -s <sodb dir> : Service OS Database directory -b <banner dir> : Service Banner directory -v <vuln rules file> : Vulnerability rules file -V <vuln descs file> : Vulnerability description file -p <pof rules file> : OS Signature file -l <us|fr>:<language file> [-l ...] : language file
Results	generates pvm conf files for ASQ <= "ASQ_VERSION"
Example	

racoon

Description	Daemon for IKE negotiations.
Command	racoon [-BdFv46] [-f (file)] [-l (file)] [-p (port)] [-P (natt port)] -B: install SA to the kernel from the file specified by the configuration file. -d: debug level, more -d will generate more debug message. -C: dump parsed config file. -L: include location in debug messages -F: run in foreground, do not become daemon. -v: be more verbose -V: print version and exit -4: IPv4 mode. -6: IPv6 mode. -f: pathname for configuration file. -l: pathname for log file. -p: port number for isakmp (default: 500). -P: port number for NAT-T (default: 4500).
Results	
Example	

reboot

Description	Reboot the IPS-Firewall. Warning !! No confirmation is requested. This action stops the HA monitoring.
Command	Reboot (no argument)

Example

```
U2504C0999999999999>reboot
Shutdown NOW!
shutdown: [pid 712]
*** FINAL System shutdown message from admin@U2504C0999999999999 ***
System going down IMMEDIATELY
U2504C0999999999999>
System shutdown time has arrived
```

sendalarm

Description Used to send alarms from shell scripts

Command

```
sendalarm -i <id> [-m message] [-u login] [-s src addr] [-d -dst addr]
-i <id> : id of the alarm message.
-m message : alarm message related to the issue.
-u login : user login.
-s : source address.
-d : destination address.
```

Results

Example

sendfile

Description Used to send file from shell scripts

Command

```
sendfile -s <server> -p <port> -f <path> -t <protocol> -m (basic|digest|post) -d <directory> -n
<name> [-c <controlname>] [-u <username>] [-a <password>] [-x <ca:cert>] [-r <ca:cert>] [-v]
-s server : object http server
-f path : filepath on server
-t protocol : http | https
-m mode : basic | digest | post
-d directory : file directory
-n name : filename
-c controlname : http control name
-u username : username for http authentication
-a password : password for http authentication
-x ca:cert : client certificate (default : fw certificate)
-r ca:cert : reference server certificate
-v : verbose
```

Results

Example

serverd

Description Configuration of the daemon. Configuration is set by the user with commands lines.

Command

usage: serverd [<-b | -B> ipaddr] [-p port] [-r user] [-d]
-b ipaddr Bind to the specified ipaddr (ipv4).
-B ipdaddr Bind to the specified ipaddr (ipv6).
-p port Attach to the specified port.
-r user Run as the specified user.
-d debug Set or launch serverd in verbose mode.

Results

Example

service_client

Description Test binary that use the internal messaging to communicate. It will create a client, send and receive messages from a specific service.

Command

service_client
-h [--help] Display this message
-v [--verbose] Enable verbosity
-t [--service] service_name Set the service name
-m [--message] arg Set the message
-s [--startup] arg Set the delay in seconds at startup before the first message (default: 1 second)
-i [--interval] arg Set the interval in seconds between successive sends (default: 1 second)
-c [--count] arg Set the number of times to send the message before exiting (default: do not stop sending)

Results Responses received from the service.

Example

```
 $> service_client --message test_request --service test_service -
-count 3
 Received response: <test_response>
 Received response: <test_response>
 Received response: <test_response>
```

service_server

Description Test binary that use the internal messaging to communicate. It will create a server, recevie and send messages to a specific service.

Command

service_server
-h [--help] Display this message
-v [--verbose] Enable verbosity
-s [--service] service_name Set the service name
-m [--message] arg Set the message

Results Requests received from the service.

Example

```
 $> service_server --service test_service -m test_response
 Got request: "test_request"
 Got request: "test_request"
 Got request: "test_request"
 ...
```

setboot

Description
Used to select the boot partition for the next reboot.
During the boot, if you select manually the partition on which you want to boot, it has the same effect that this command.

Command

```
setboot <Main|Backup>
Main : Set main partition for next reboot
Backup : set Backup partition for next reboot.
```

Results

Example

setconf

Description
Write a section value to a configuration file. This command is generally called from scripts.

Command

```
setconf <file> <section> [<token>] <value>
  Adds <token>=<value> to <section> in configuration file <file>
  If <token> is not set, the section is appended with <value>
setconf -n, --no-protect <file> <section> <value>
  Sets <section> to <value> in configuration file <file> without protecting with \"\"
setconf -d, --delete <file> <section> [<token> [<value>]]
  Removes section <section> from configuration file <file>
  If <token> is set, removes only the token from <section>
  If <value> is set, check token value before removing
```

Results

Example

```
U2504C099999999999>setconf /usr/Firewall/ConfigFiles/network Ethernet1 Address 10.x.x.x
U2504C099999999999>
```

setkey

Description
PFKEYv2 userland tool used to manage kernel information related to IPSec.

Command

```
setkey [-v] file ...
setkey [-nv] -c
setkey [-nv] -f filename
setkey [-Palpv] -D
setkey [-Pv] -F
setkey [-H] -x
setkey [-V] [-h]
```

Results

Example

seturl

Description
Set the field «URLFiltering» in the file /usr/Firewall/ConfigFiles/proxy
for CLOUDURL case : Cloudurl State is set to 1 and URLFiltering State is set to 0
for STORMSHIELD NETWORK case : Cloudurl State 0 URLFiltering State is set to 1
for NONE case : both Cloudurl and URLFiltering State are set to 0

Command	seturl [SN|CLOUDURL|NONE] SN : Set value «SN» CLOUDURL : Set value «CLOUDURL» NONE : Set value «SN»
Results	
Example	

swaninfo

Description	Display current configuration and connection status in strongSwan
Command	swaninfo <element> [--noresolve] <element> is one of the following: conn: Display configured connections conn-status: Display connection status ike-sa [--state=<value>]: Display IKE SAs and associated CHILD SAs get-counters [--name=<value>]: Display counters for all of 1 (named) connection(s) stats: Display statistics based on IKE status and all connections counters
Results	
Example	

sfctl

Description	Get or set ASQ module parameters. **Warning !** This command uses some advanced functions of the firewall. Its usage must be done very carefully and with some very good knowledges. Some commands can cut current network connexions.

Command	sfctl

Opt	Arg	Description
-e		set module state
		1 = enable
		0 = disable
-T		top alike mode
-f		force operation
-v		verbose mode
-n		disable the reverse object lookup
-O	level	optimize ruleset at level
		0 = none
		1 = skip rules
-F	modifier	flush one of the following
		addrlist = flush address list
		filter = flush filter rules
		state = flush state information
		etherstate = flush all ether state information
		count = flush count rule
		stat = flush statistics
		fpstat = flush fastpath statistics
		pof = flush os signature list (pof)
		qosq = flush qos queues
		host = flush host (see -H hstate=...)
		sipr = flush the sip requests
		sip = flush the sip register table
		ipstate = flush flows managed by ipstate
		fpstate = flush fastpath state
		hproperties = flush hostproperties
		assoc = flush SCTP assoc informations
		all = all the above
-b	t,o,a[,to]	manage blacklist entry
		t = BlackList|WhiteList...
		o = add or delete
		a = string identifier or '*'
		to = timeout
-C	configdir	load and activate a ASQ configuration
-R	rulefile	load a filter rule file and activate it
-c		commit filter rules even if equal to old ones
-P	rulefile	load finger printing rule file and activate it
-Q		load QoS queues config and activate it
-q		set QoS state
		1 = enable
		0 = disable

-s	modifier	dump one of the following addrlist = show address list assoc = show SCTP association table content conn = show connection table content connstat = show TCP conn stats per state count = show count rule etherstate = show Ethernet connection table content filter = show current filter rules fpstat = show fastpath statistics fpstate = show fastpath state table global = show if statistics ha = show ha cluster info host = show host table content if = show interface information ioctl = show ioctl statistics ipstate = show flows managed by ipstate limit = show ASQ limits log = show last log message mem = show memory stats nat = show current nat rules natpool = show reserved nat ports pof = show os signature list (pof) protaddr = show protected address list qos = show QoS rule revrt = show reverse router table route = show route information rulestat = show rulesmatch sip = show sip register table (nat) sipr = show sip request table stat = show statistics state = show state table content table = show filter tables content user = show user table content all = all the above

-l	modifier	write a log entry
		count = log count rule
		stat = log statistics
		all = all the above

-H	type=modifier	modify output. type can be	
		host	= display information for host
		shost	= display information for client
		dhost	= display information for server
		port	= display information for port
		sport	= display information for source
		dport	= display information for
		plugin	= display information associated
		iface	= display information associated
		siface	= display information associated
		diface	= display information associated
		proto	= display information associated
		section	= filter information for show
		state	= display information according
		hstate	= display information for host
		htype	= display information for host
		sigid	= display information for host
		ctype	= display connections of a given
		qid	= display connections of a given
		rtname	= display connections of a given
		auth	= display users authenticated
		name	= display user table for a given
		conn	= all to flush all connections
		rule	= filter the connections by the
		natrule	= filter the connections by the
		macaddr	= display information for mac
		iptype	= display information by IP type
		cpu	= display information by CPU
		bytes	= display connections with total
		lastuse	= display connections used within
		bandwidth	= display host with a total
		hostrep	= display host with reputation
		maxcount	= limit number of elements returned by -s
		geo	= geo location filter
		iprep	= iprep filter

-A	<key>[=<val>][,<key>[=<val>][, ...]];[...]	manually add/update authenticated user(s)	
		address	= user address
		name	= user name
		domain	= user domain
		group	= group membership ("g a,g b")
		timeout	= timeout
		multiuser	= adress is multi-user (no value)
		authmethod	= authentication method
		admin	= user is an admin (no value)
		sslvpn	= user have access to sslvpn (no value)
		sslrdr	= user have access to sslrdr (no value)
		openvpn	= user have access to openvpn (no value)
		sponsoring	= user has the rights to sponsor (no value)
-a	<key>[=<val>][,<key>[=<val>][, ...]];[...]	manually remove authenticated user(s)	
		name	= user name
		domain	= user domain
		address	= user address
		all	= all authenticated user (no value)
-r	old,new	rename a user domain	
-t	op,val	manually add/remove objects from filter tables (experimental)	
		name	= name of the table
		op	= add or del
		val	= addresses separated by comma
-B	op,host,conn,assoc	backup operation	
		op	= backup or restore
		host	= host filename
		conn	= conn filename
		assoc	= assoc filename
-h	modifier	HA ethernet mode	
		active	= set as active mode
		passive	= set as passive mode
		show	= display current mode
		swap	= do a swap
		bulk	= send a bulk update to peer
		<local IP>,<peer IP>,mtu	= configure HA sync in IPS
-o	filename	write output data to filename (work only with -s)	
-i	source	data source (work only with -s)	
		asq	= use ASQ data (default)

-p	<key>[=<val>][,<key>[=<val>][, ...]];[...]	manually add or tweak a host
		addr = mandatory address of the host
		if = interface name
		state = desired state
		mac = MAC address
		geo = geo IP ("eu:fr")
		iprep = IP reputation ("botnet,spam")
		hostrep = host reputation
		dns = DNS cache
		nogeo = remove geo IP from host (no value)
		noiprep = remove IP reputation from host (no value)
		nohostrep = remove reputation from host (no value)
		nodns = remove DNS cache from host (no value)

--libxo	params	Pass params to libxo, see libxo possible parameters here.
Token		**Action**
color		Enable colors/effects for display styles (TEXT, HTML)

Results

Examples

```
U2504C0999999999999>sfctl -s host
Host (ASQ):
host if state packet bytes throughput
10.1.20.249 in active 0.00 p 0.00 B 1.26MB 0.00 b/s 0.00 b/s
10.1.20.10 in active 0.00 p 0.00 B 490KB 0.00 b/s 12.2Kb/s
10.1.20.103 in active 0.00 p 0.00 B 2.13KB 0.00 b/s 984 b/s
10.1.20.254 in active 5.00 p 320 B 400 B 0.00 b/s 0.00 b/s
10.1.20.251 in active 0.00 p 0.00 B 8.75KB 0.00 b/s 0.00 b/s
204.13.248.112 learning learning / / /
10.1.4.50 in active 0.00 p 0.00 B 80.4KB 0.00 b/s 0.00 b/s
10.1.204.11 in active 0.00 p 0.00 B 189KB 0.00 b/s 2.69Kb/s
10.1.20.101 in active 0.00 p 0.00 B 2.13KB 0.00 b/s 16.0 b/s
10.1.6.1 in active 51.0 p 15.7KB 6.86KB 3.38Kb/s 4.11Kb/s
10.1.20.102 in active 0.00 p 0.00 B 2.13KB 0.00 b/s 16.0 b/s
10.1.5.1 in active 0.00 p 0.00 B 328KB 0.00 b/s 7.25Kb/s
U2504C0999999999999>
```

slapd

Description LDAP daemon

Command

```
slapd options
-4 IPv4 only
-6 IPv6 only
-T {acl|add|auth|cat|dn|index|passwd|test} : Run in Tool mode
-c cookie : Sync cookie of consumer
-d level : Debug level
-f filename : Configuration file
-F dir : Configuration directory
-g group : Group (id or name) to run as
-h URLs : List of URLs to serve
-l facility : Syslog facility (default: LOCAL4)
-n serverName : Service name
-o <opt>[=val] : Generic means to specify options
    supported options: slp[={on|off|(attrs)}] enable/disable SLP using (attrs)
 -r directory : Sandbox directory to chroot to
-s level : Syslog level
-u user : User (id or name) to run as
-V : Print version info (-VV exit afterwards, -VVV print info about static overlays and backends)
```

Results

Example

sld

Description Daemon sld.

Command

```
sld [-d] [-i] [-s] [-v]
-d : Toogle verbose
-i : Show information
-s : Show config
-h : Help
-v : Version
```

Results	
Example	

slotinfo

Description	Manage the different slots of configuration of the firewall (filtering, translation, VPN, ...)
Command	Slotinfo [-A index [-v]] [-g index] [-f] [-a] [-n] [-S] [-s state] <slotname> -h : This help message -A : Set Active SlotNumber / -v verify -f : Get Current Slot Filename -a : Get Current SlotNumber -g : Get Slot Filename from index -i : Get Slot index from Filename -n : Get Current SlotName -S : Get Sync -s : Set Sync The list of <slotname> = globalfilter globalvpn filter vpn
Results	
Example	U2504C099999999999>slotinfo -a filter 10 U2504C099999999999>slotinfo -n filter pass all U2504C099999999999>slotinfo -f filter /usr/Firewall/ConfigFiles/Filter/10 U2504C099999999999>

smartck

Description	Check Utility for SMART Disks
Command	smartck -h | -H [device(s)] | -A [device(s)] -h: print this help and exit -H: check disk health -A: dump information about disk state If device is not defined, all disks are checked.
Results	

smartctl

Description	Control and Monitor Utility for SMART Disks

Command	Usage: smartctl [options] device

Opt	LongOpt	Arg	Description
			SHOW INFORMATION OPTIONS
-h	--help		Display this help and exit
-V	--version		Print license, copyright, and version information and exit
-i	--info		Show identity information for device
	--identify		Show words and bits from IDENTIFY DEVICE data (ATA)
-g	--get	NAME	Get device setting: all, aam, apm, lookahead, security, wcache, rcache, wcreorder
-a	--all		Show all SMART information for device
-x	--xall		Show all information for device
	--scan		Scan for devices
	--scan-open		Scan for devices and try to open each device
			SMARTCTL RUN-TIME BEHAVIOR OPTIONS
-q	--quietmode	TYPE	Set smartctl quiet mode to one of: errorsonly, silent, noserial
-d	--device	TYPE	Specify device type to one of: ata, scsi, sat[,auto][,N][+TYPE], usbcypress[,X], usbjmicron[,p][,x][,N], usbsunplus, 3ware,N, hpt,L/M/N, cciss,N, areca,N/E, atacam, auto, test
-T	--tolerance	TYPE	Tolerance: normal, conservative, permissive, verypermissive
-b	--badsum	TYPE	Set action on bad checksum to one of: warn, exit, ignore
-r	--report	TYPE	Report transactions (see man page)
-n	--nocheck	MODE	No check if: never, sleep, standby, idle (see man page)
-s	--smart	VALUE	Enable/disable SMART on device (on/off)
-o	--offlineauto	VALUE	Enable/disable automatic offline testing on device (on/off)
-S	--saveauto	VALUE	Enable/disable Attribute autosave on device (on/off)
-s	--set	NAME [,VALUE]	Enable/disable/change device setting: aam,[N|off], apm,[N|off], lookahead,[on|off], security-freeze, standby,[N|off|now], wcache,[on|off], rcache,[on|off], wcreorder,[on|off]
			READ AND DISPLAY DATA OPTIONS
-H	--health		Show device SMART health status
-c	--capabilities		Show device SMART capabilities
-A	--attributes		Show device SMART vendor-specific Attributes and values
-f	--format	FORMAT	Set output format for attributes: old, brief, hex[,id|val]
-l	--log	TYPE	Show device log. TYPE: error, selftest, selective, directory[,g|s], xerror[,N][,error], xselftest[,N][,selftest], background, sasphy [,reset], sataphy[,reset], scttemp[sts,hist], scttempint,N[,p], scterc[,N,M], devstat[,N], ssd, gplog,N[,RANGE], smartlog,N [,RANGE]
-v	--vendorattribute	N,OPTION	Set display OPTION for vendor Attribute N (see man page)
-F	--firmwarebug	TYPE	Use firmware bug workaround: none, nologdir, samsung, samsung2, samsung3, xerrorlba, swapid
-P	--presets	TYPE	Drive-specific presets: use, ignore, show, showall
-B	--drivedb	[+]FILE	Read and replace [add] drive database from FILE and then /usr/local/share/smartmontools/drivedb.h]
			DEVICE SELF-TEST OPTIONS
-t	--test	TEST	Run test. TEST: offline, short, long, conveyance, force, vendor,N, select,M-N, pending,N, afterselect,[on|off]
-C	--captive		Do test in captive mode (along with -t)

	-X --abort	Abort any non-captive test on device
Results		
Example	smartctl -a /dev/ad0 (Prints all SMART information) smartctl --smart=on --offlineauto=on --saveauto=on /dev/ad0 Enables SMART on first disk) smartctl -t long /dev/ad0 (Executes extended disk self-test) smartctl --attributes --log=selftest --quietmode=errorsonly /dev/ad0 (Prints Self-Test & Attribute errors) smartctl -a --device=3ware,2 /dev/twa0 smartctl -a --device=3ware,2 /dev/twe0 (Prints all SMART information for ATA disk on third port of first 3ware RAID controller) smartctl -a --device=cciss,0 /dev/ciss0 (Prints all SMART information for first disk on Common Interface for SCSI-3 Support driver)	

smcrouterd

Description	Daemon smcrouterd.
Command	smcrouterd [-v] [-i] [-f <file>] -i: get info on the configuration and exit -h: show this help -f: force config file -v: activate verbose mode
Results	
Example	

snmpd

Description	Daemon snmp.

Command

```
snmpd [OPTIONS] [LISTENING ADDRESSES]
-a : log addresses
-A : append to the logfile rather than truncating it
-c FILE[,...] : read FILE(s) as configuration file(s)
-C : do not read the default configuration files
(config search path:
/usr/local/etc/snmp:/usr/local/share/snmp:/usr/local/lib/snmp:/usr/Firewall/.snmp)
-d : dump sent and received SNMP packets
-D[TOKEN[,...]] : turn on debugging output for the given TOKEN(s)
(try ALL for extremely verbose output)
Don't put space(s) between -D and TOKEN(s).
-f : do not fork from the shell
-g GID : change to this numeric gid after opening
transport endpoints
-h, --help : display this usage message
-H : display configuration file directives understood
-I [-]INITLIST : list of mib modules to initialize (or not)
(run snmpd with -Dmib_init for a list)
-L <LOGOPTS> : toggle options controlling where to log to
    e: log to standard error
    o: log to standard output
    n: don't log at all
    f file: log to the specified file
    s facility: log to syslog (via the specified facility)
    (variants)
    [EON] pri: log to standard error, output or /dev/null for level 'pri' and above
    [EON] p1-p2: log to standard error, output or /dev/null for levels 'p1' to 'p2'
    [FS] pri token: log to file/syslog for level 'pri' and above
    [FS] p1-p2 token: log to file/syslog for levels 'p1' to 'p2'
 -m MIBLIST : use MIBLIST instead of the default MIB list
-M DIRLIST : use DIRLIST as the list of locations to look for MIBs (default no)
-p FILE : store process id in FILE
-q : print information in a more parsable format
-r : do not exit if files only accessible to root cannot be opened
-u UID : change to this uid (numeric or textual) after opening transport endpoints
-v, --version : display version information
-V : verbose display
-x ADDRESS : use ADDRESS as AgentX address
-X : run as an AgentX subagent rather than as an SNMP master agent
Deprecated options:
-l FILE : use -Lf <FILE> instead
-P : use -p instead
-s : use -Lsd instead
-S d|i|0-7 : use -Ls <facility> instead
```

Results

Example

squid

Description Daemon squid.

Command

squid [-hvzCDFINRYX] [-d level] [-s | -l facility] [-f config-file] [-u port] [-k signal]
-d : level Write debugging to stderr also.
-f file : Use given config-file instead of /usr/local/etc/squid/squid.conf
-h : Print help message.
-k reconfigure|rotate|shutdown|interrupt|kill|debug|check|parse :
Parse configuration file, then send signal to running copy (except -k parse) and exit.
-s | -l facility : Enable logging to syslog.
-u port : Specify ICP port number (default: 3130), disable with 0.
-v : Print version.
-z : Create swap directories
-C : Do not catch fatal signals.
-D : Disable initial DNS tests.
-F : Don't serve any requests until store is rebuilt.
-I : Override HTTP port with the bound socket passed in on stdin.
-N : No daemon mode.
-R : Do not set REUSEADDR on port.
-S : Double-check swap during rebuild.
-X : Force full debugging.
-Y : Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.

Results

Example

squidclient

Description

Squid tool for performing web requests

Command

squidclient
    [-arsv] [-i IMS] [-h remote host] [-l local host] [-p port] [-m method] [-t count]
    [-I ping-interval] [-H 'strings'] [-T timeout] [-j 'hostheader'] url
-P file : PUT request.
-a : Do NOT include Accept: header.
-r : Force cache to reload URL.
-s : Silent. Do not print data to stdout.
-v : Verbose. Print outgoing message to stderr.
-i IMS : If-Modified-Since time (in Epoch seconds).
-h host : Retrieve URL from cache on hostname. Default is localhost.
-l host : Specify a local IP address to bind to. Default is none.
-j hosthdr : Host header content
-p port : Port number of cache. Default is 3128.
-m method : Request method, default is GET.
-t count : Trace count cache-hops
-g count : Ping mode, "count" iterations (0 to loop until interrupted).
-I interval : Ping interval in seconds (default 1 second).
-H 'string' : Extra headers to send. Use '\n' for new lines.
-T timeout : Timeout value (seconds) for read/write operations.
-u user : Proxy authentication username
-w password : Proxy authentication password
-U user : WWW authentication username
-W password : WWW authentication password
-V version : HTTP Version

Results

Example

sslinit

Description	Initialize some SSL secure keys.
Command	sslinit [-p] [-f] -p : only configure proxy Certification Authorities -f : do not perform any check on CA generation conditions
Results	
Example	

statectl

<table>
<tr><td><b>Descriptio
n</b></td><td>Command line utility to set state daemon parameters when firewall is in HA mode.</td></tr>
<tr><td><b>Command</b></td><td>statectl
All usage:
-v : verbose mode
-t <0-9999> : timeout
Usage:
<table>
<tr><th>Op
t</th><th>Arg</th><th>Description</th></tr>
<tr><td>-s</td><td>&lt;infos&gt;</td><td>dump information
<infos> :
cluster = show HA cluster node info
sync = show HA node sync status
interfaces = show interfaces HA status
all = all the above
(default target host: all)</td></tr>
</table></td></tr>
</table>

-c	<command>	send a command to the cluster. <command>:	
		halt	stop firewall
		reboot	reboot firewall
		force_active	force firewall to become the active one
		force_passive	force firewall to become the passive one
		unforce	cancel previous forcing
		relink	reactivate faulty links
		sync[,<type>[,<source>[,nowait]]]	synchronize files Synchronizations options (-c sync[,<type>[,<source>]]): type : Type of synchronization everything (default) config ldap ssh cert ha au_Clamav au_Kaspersky au_Antispam au_RootCertificates au_Patterns au_URLFiltering au_Vaderetro au_Pvm pvmdb utm_secrets source : specify from which node the files must be downloaded <serial> = specific host local = from local firewall active = from an active firewall (default)
		dumproot	run dumproo
		enha	run enha
		ennetwork	run ennetwork
		pause_balancing[<,reason>[<,duration>]]	will freeze HA balancing <reason> : [enha|enfilter|ennetwork|enswitch|forced] <duration> : max time during which the HA will be frozen (target host: all)
		resume_balancing	resume HA balancing if frozen
		has_logdisk	indicates if the firewall has a log disk
-w	<channel>	watch HA message between cluster <channel>: 'SYNC-<serial>' or 'command', or 'all' (default target host: all)	
-S	<serial>	specify a target cluster member <serial>: specific host	

		local = local host
		all = all cluster members

	-a	(re)generate Corosync authentification key file
	-d	display Corosync statistics and diagnostics info
	-W <nb fw>	wait for the HA cluster to be operationnal <nb fw> number of firewalls to wait for
Results		
Example		

stated

Description	State daemon. Monitors various firewall states like connected host, connections in progress, connected users, HA, network interfaces, etc... Allows HA configuration synchronization.
Command	stated [-d] [-t <option1>(,<option2>(,...))] [-k] -d Activate debugging -t <option1>(,<option2>(,...)) Testing options: 'generate_events' : generate random events/connections 'no_passive_eth' : never switch ethernet interfaces to passive mode 'no_asq_events' : do no get connections lists from the ASQ 'no_asq_restoration' : do not restore peer connections into the ASQ when becoming active -k : Kill all SSH redirections
Results	
Example	

strongswan_auth

Description	Control user access
Command	strongswan_auth [-v] <user_id> -v : verbose mode user_id : id of the user to be checked
Results	
Example	

switchctl

Description	Manages switch. (Only models with switch)
Command	switchctl [-e "cmd"] [-s] [-r] -e "cmd" : send cmd command to switch and display result -r : reboot the switch -s : spy on communications with the switch. Commands can be input from stdin (leave with ^C) -b : prevent network traffic from going through the switch

Results	
Example	

switchd

Description	Switch daemon. It is not possible to run two instances of **switchd** without argument. (Only models with switch)
Command	switchd [-i] [-c] [-f file] [-d] -i : create ethX interfaces (no daemon) -c : write /var/switch (no daemon) -f <firmware> : reset switch and flash it **DANGEROUS** -d : run in verbose mode (no daemon)
Results	
Example	

sysdbg

Description	Active the debugging. Launch each line from command_list file and log it in /dbg/..
Command	/usr/Firewall/sbin/sysdbg [-q] [-c <commands>] [-S <hastate>] /usr/Firewall/sbin/sysdbg -h When run without arguments, simply create the /dbg directory and if it already exists, compress its content. -c <commands> : execute the commands listed in <commands> -h : display help and exit -q : quiet, no output -S <hastate> : expected licence HA state.
Results	
Example	

sysinfo

Description	Display a detailed list of the configuration and activity of the Firewall.

Command

```
sysinfo
    [-arp] [-ndp] [-host] [-conn] [-raid] [-safety] [-proxy] [-global] [-ipmi] [-time]
    [-fastpath] [-ipstate] [-sysctl] [-vmstat] [-socket] [-wifi] | [-a]
    -arp: add ARP table
    -ndp: add NDP table
    -host: add ASQ host table
    -conn: add ASQ Connection table
    -raid: add RAID informations
    -safety: add Safety mode information
    -proxy: add PROXY informations
    -global: add GLOBAL informations
    -ipmi: add IPMI informations
    -time: display time objects informations
    -fastpath: add FASTPATH information
    -ipstate: add IPSTATE information
    -sysctl: display sysctl informations
    -vmstat: display vmstat informations
    -socket: add SOCKET INET informations
    -wifi: display WIFI informations
    -a: add all optional informations
WARNING: Dumping all informations can overload the appliance !
```

Results

There is a great amount of information returned by this command, it is then advised to output the results in a file : sysinfo > /tmp/sysinfo for example.

Example

```
U2504C099999999999>sysinfo
################################
# Software information #
################################
current date : "2011-04-06 18:35:44" zone=CEST tz=+0200 ntp=Off
Serial : U250XA0A0803770
Model : U250-A
Software : Stormshield Network Security Firewall software version trunk.dev-2011-03-29-10:56-
NO_OPTIM
ASQ : Firewall ASQ version 5.0.0
Branch/Build : INTERNE / M
Partitions : Active=Main BackupVersion="8.1.2.beta-8-NO_OPTIM" BackupBranch="INTERNE"
Boot=Main
...
```

sysutil

Description

Provide general information about the system.

Command

```
sysutil
    [ -h ] [ -p ] [ -d ] [-k]
     -h --help
     -p --labeltopartition
     -d --labeltodisk
     -k --keyconvert
```

Results

Example

```
U2504C099999999999>sysutil -p ufs/main
ad0s1a
```

tcpick

Description tcpick is a textmode sniffer libpcap-based that can track, reassemble and reorder tcp streams

Command

```
tcpick
    [ -a ] [ -n ] [ -C ]
    [ -i interface ]
    [ -yH ] [ -yP ] [ -yR ] [ -yU ] [ -yx ] [ -yX ]
    [ -bH ] [ -bP ] [ -bR ] [ -bU ] [ -bx ] [ -bX ]
    [ -wH ] [ -wP ] [ -wR ] [ -wU ]
    [ -v [ verbosity ]]
    [ -S ] [ -h ] [ --separator ]
    [ "filter" ] [ -r file ]
    [ --help ] [ --version ]
```

Results

Example

```
U2504C0999999999999>tcpick -i eth1 -yP -C -h "port 22"
Starting tcpick 0.2.1 at 2011-04-11 16:54 CEST
Timeout for connections is 600
tcpick: listening on eth1
ERROR: eth1: no IPv4 address assigned
setting filter: "port 22"
172.17.6.1:62278 AP > 172.17.6.254:ssh (48)
|....(..'06.c..............-..`$\.{z...-.k.x(.G.
172.17.6.254:ssh AP > 172.17.6.1:62278 (48)
.......E...ku.w.......4.....t.u.....#yj..)...../
^C
2 packets captured
0 tcp sessions detected
U2504C0999999999999>
```

telemetryd

Description Telemetry daemon.

Command

```
telemetryd [-D] [-d] [-h]
  -D : will daemonize
   -d : debug mode
   -h : show help message
```

Results

Example

```
U2504C0999999999999>telemetryd -d
 telemetryd (pid 2444) is already running
 Signal SIGINFO was sent to current process
 Verbose status is modified
```

testldapbase

Description Check if openldap is up and accessible.

Command

```
testldapbase [-n number] [-t delay][-v]
-n number of tests
-t delay in milliseconds between tests
-v verbose
```

Results

Example	U2504C099999999999>testldapbase U2504C099999999999>

thind

Description	Threat intelligence daemon.
Command	thind
Results	
Example	

tpmctl

Description	Control TPM (initialization, configuration,reset)
Command	tpmctl [-v] [-i|-r|-a] -p <password> [-d] -v : verbose mode -i : initialize TPM -r : reset TPM -a : run TPM diagnostic -p : password associated with TPM -d : derive TPM key from password when initializing TPM

tproxyd

Description	Display information about each proxy used on the Firewall (HTTP, SMTP, POP3, FTP, SSL).
Command	tproxyd [-d] [-L | -gX | -s <opt> | -v | -h] -d : debug mode -h -? : help -L : show ICAP proxy licences -gX : show all groups, X as verbose level (g1 to only dump the groups name, g2 to show their content) -s <http|smtp|pop3|ftp|ssl|av|antispam|rules|all> : show config -v : version
Results	

Example

```
U2504C099999999999>tproxyd -L
[2011-04-07 10:49:29] Icap url (reqmod) licence ok
[2011-04-07 10:49:29] Icap virus (respmod) licence ok
U2504C099999999999>
U2504C099999999999>tproxyd -s http
OEM groups loaded
URL groups loaded
CN groups loaded
-- Http proxy : enabled
. BindAddr=0.0.0.0
. FullTransparent=1
. Postprocessing :
- policy: pass on failed
- datasize limit of 100000 Ko
. Antivirus:
- using default antiviral solution
- policy: block on failed
- policy: block on infected
. BindAddr=0.0.0.0
----- URL Filtering part -----
(Default action = Block) :
/usr/Firewall/ConfigFiles/URLFiltering/02
1: bypass_proxy ==> Pass
5: anonymizers ==> Blockpage
6: anorexia_and_bulimia ==> Blockpage
7: antivirus_bypass ==> Blockpage
8: art ==> Pass
...
...
...
U2504C099999999999>
```

topic_monitor

Description Binary that uses the internal messaging to communicate. It will create a subscriber and receive messages from a specific topic, and then dump them in a readable format.

Command topic_monitor

-h [--help] Display this message

-v [--verbose] Enable verbosity

-t [--topic] topic_name Set the topic name

--dump arg Specify the message dump format, arg may be "asc|hex|all" (default is "asc")

--width arg Specify the message dump width, arg is an integer (default is 16)

Results Messages from the topic.

Example

```
$> topic_monitor --topic test_topic
test
test
test
...
```

topic_reader

Description Test binary that use the internal messaging to communicate. It will create a subscriber and receive message from a specific topic.

Command topic_reader
-h [--help] Display this message
-v [--verbose] Enable verbosity
-t [--topic] topic_name Set the topic name

Results Messages from the topic.

Example

```
$> topic_reader --topic test_topic
test
test
test
...
```

topic_sender

Description Test binary that use the internal messaging to communicate. It will create a publisher and send messages to a specific topic.

Command topic_sender
-h [--help] Display this message
-v [--verbose] Enable verbosity
-t [--topic] topic_name Set the topic name
-m [--message] arg Set the message
-s [--startup] arg Set the delay in seconds at startup before the first message (default: 1 second)
-i [--interval] arg Set the interval in seconds between successive sends (default: 1 second)
-c [--count] arg Set the number of times to send the message before exiting (default: do not stop sending)

Results Nothing without verbose.

Example

```
$> topic_sender --topic test_topic --message test --count 3
$>
```

udpsync

Description Factory tool.

Command udpsync [-s] [-p <port>] [-i <phase>] [-t <timeout>] [-v] [<host>]
-s : Server
-p <port> : host port (default: 1991)
-i <phase> : ???
-t <timeout> : time before timeout in seconds (default: 60s)
-v : verbose mode enabled

Results

Example

userreqd

Description User Requests daemon.

Command	userreqd [-d] [-D] [-h] -D : will daemonize -d : debug mode -h : show help message
Results	
Example	U2504C099999999999>userreqd -d userreqd (pid 2517) is already running Signal SIGINFO was sent to current process Verbose status is modified

wizardinit

Description	First install wizard.
Command	wizardinit
Results	
Example	

vmreport

Description	PAYG virtual machine reporting utility
Command	vmreport -S vmreport -U vmreport -E -S, --start : report Start event -U, --up : report UP event -E, --stop : report Stop event -v, --verbose : verbose in console -q, --quiet : quiet mode -h, --help : display help Whithout parameters, sync the events if needed.

STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.