D-Link® CORPORATION

D-Link Firewall

SECURIWALL™

Network Security Firewall

CLI Manual

D-Link

Building Networks for People

(20040407)

Table Of Contents

Firewall Console

Firewall Console

This section includes the following topics:

- Serial Console
- Local Console

The D-Link Firewall console is a text-based command line interface. A more in-depth analysis of various statistical aspects of the firewall can be conducted here as well as advanced troubleshooting. The firewall cannot be configured from the console.

There are three ways to access the console, either by using the serial console (for example on D-Link Firewall Appliances), the keyboard and monitor on software firewalls

Serial Console

The firewall console can be accessed using the serial console port on the firewall hardware. For more information, please see the section Connecting the Console Port in the Getting Started guide.

Local Console

The firewall console is also available when attaching a VGA display and a keyboard to the firewall hardware. Please note that this is only applicable for products from the *D-Link Firewall Software series*.

```
  Clavister Firewall 8.00.00    : Below: 'pps,mbps', per interface
 2500,11.5  600,36.0  3500,20.5
CPU: 8% : Bufs: 2% : Conns: 3% : Frags: 0% : Drops: 5 : LogMsgs: 4

Clavister Firewall 8.00.00
Copyright Clavister 1996-2002. All rights reserved.
Build : Oct 1 2002

Reading previous random state from fwrand.bin...OK

Configuring from A:\FIREWALL\FWCORE.CFG
Configuration done

NetCon initialization complete

Memory: Buffer size is 2084 bytes, 1992 bytes raw data
Memory: Using a total of 180 packet buffers (375120 bytes)

Interfaces:
0 : int          IPAddr 10.20.250.2      HwAddr 00c0:df50:51d1
  Builtin "tulip" - Digital DS21143-xD Tulip  Slot 4/1 IRQ 9
1 : ext          IPAddr 10.20.0.1        HwAddr 0010:a060:77fd
  Builtin "tulip" - Digital DS21143-xD Tulip  Slot 5/1 IRQ 10
1 : dmz          IPAddr 192.168.234.1    HwAddr 0010:a060:77e9
  Builtin "tulip" - Digital DS21143-xD Tulip  Slot 6/1 IRQ 9

Previous shutdown: 2002-10-01 07:00:00: Shutdown due to console command

System running
```

The first status line shows information about the number of packets and bits that pass through each interface per second. The figures given in this example show that:

- The internal interface is currently passing:
  2500 packets per second
  11.5 Megabits per second
- The external interface is currently passing:
  6000 packets per second
  36 Megabits per second
- The DMZ interface is currently passing:
  3500 packets per second
  30.5 Megabits per second

These figures include the amount of data sent and received by each interface. No more than eight interfaces will be displayed on this status line.

The second status line provides the following information:

- **CPU** - The percentual load of the firewall's CPU.
- **Bufs** - Percentual use of available packet buffers. The total number of packet buffers is shown under the stats command.
- **Conns** - Percentual use of available connections. The maximum number of connections is determined by the Settings section. The default configuration sets a limit of 4096 concurrent connections. Each connection consumes 128 bytes of RAM. To see the actual amount of RAM used by the state table, see the memory console command, below.
- **Frags** - Percentual use of available fragment reassembly resources. *D-Link* Firewall limits the number of fragment reassembly attempts that can be under way at any one time.
- **Drops** - The number of packets that have been discarded due to failed structural tests or ruleset drops during the past second.
- **LogMsgs** - The number of log messages that have been generated during the past second. *D-Link* Firewall is able to limit how many log messages may be generated each second through the LogSendPerSecLimit setting in the Settings section.

Firewall Console Reference

Firewall Console Reference

This section includes the following topics:

- License
- Lockdown
- Loghosts
- Logout
- Netcon
- VPNStats

About

Brings up information pertaining to the version of the firewall core in use and a copyright notice.

Syntax: about

Example

```
Cmd> about
D-Link Firewall 8.00.00V
Copyright D-Link 1996-2002. All rights reserved
SSH IPSEC Express SSHIPM version 4.2.0 library 4.2.0
Copyright 1997-2001 SSH Communications Security Ltd.
Build : Sep 22 2002
```

Access

Displays the contents of the Access configuration section.

Syntax: access

Example

```
Cmd> access
Source IP Address Access list (spoofing protection) - Default action is DROP
Symbolic Name     Action Iface  Source Range
----------------- ------ ------ -------------------------------
ExpectIntnet      Expect int    192.168.123.0/24
ExpectExtnet      Expect ext    194.2.1.0/24
ExpectWorld       Expect ext    0.0.0.0/0
```

ARP

Displays ARP entries for the specified interface(s). Published, static as well as dynamic items are shown.

Syntax: arp [options] <interface pattern>

Options:

-ip <ip address pattern>
-hw <hw address pattern>
-num <n>

Example

```
Cmd>arp ext
ARP cache of iface ext
Dynamic 194.2.1.1    = 0020:d216:5eec   Expire=141
```

ARPSnoop

Toggles the on-screen display of ARP queries. This command can be of great help in configuring firewall hardware, since it shows which IP addresses are heard on each interface.

Syntax: arpsnoop <interface pattern>

Toggle snooping on given interfaces.

Syntax: arpsnoop all

Snoop all interfaces.

Syntax: arpsnoop none

Disable all snooping.

Example

```
Cmd> arpsnoop all
ARP snooping active on interfaces: int ext dmz
ARP on ext: gw-world requesting ip_ext
ARP on int: 192.168.123.5 requesting ip_int
```

Buffers

This command can be useful in troubleshooting; e.g. if an unexpectedly large number of packets begin queuing in the firewall or when traffic does not seem to be flowing for some inexplicable reason. By analyzing the contents of the buffers, it is possible to determine whether such traffic is making it to the firewall at all.

Syntax: buffers

Brings up a list of most recently freed buffers.

Example

```
Cmd>buff
Displaying the 20 most recently freed buffers
RecvIf  Num  Size Protocol Sender                  Destination
------- ---- ---- -------- ----------------------- -----------------------
ext     1224  121 UDP      192.168.3.183           192.168.123.137
int      837  131 UDP      192.168.123.137         192.168.3.183
ext      474  112 UDP      192.168.3.183           192.168.123.137
ext      395   91 UDP      192.168.3.183           192.168.123.137
int      419  142 UDP      192.168.123.137         192.168.3.183
ext      543  322 UDP      194.2.1.50              192.168.123.182
int      962   60 UDP      192.168.123.182         194.2.1.50
int      687   60 ARP      0080:ad87:e592          ffff:ffff:ffff
ext      268   88 UDP      192.168.3.183           192.168.123.137
int      249  101 UDP      192.168.123.137         192.168.3.183
ext      219   60 TCP      193.12.33.105           192.168.123.12
int      647   60 ARP      0010:a707:dd31          ffff:ffff:ffff
ext     1185   98 UDP      192.168.3.183           192.168.123.137
int      912   98 UDP      192.168.123.137         192.168.3.183
ext      682  112 UDP      192.168.3.183           192.168.123.137
int      544   60 TCP      192.168.123.12          194.2.1.50
int      633   60 TCP      192.168.123.26          194.2.1.50
int      447   60 TCP      192.168.123.25          194.2.1.50
int      645   60 TCP      192.168.123.23          194.2.1.50
int      643  123 UDP      192.168.123.137         192.168.3.183
```

Syntax: buffer <number>

Shows the contents of the specified buffer.

Example

```
Cmd> buff 1059
Decode of buffer number 1059
int: Enet 0050:dadf:7bbf -> 0003:325c:cc00, type 0x0800, len 1058
IP 192.168.123.10->193.13.79.1  IHL:20  DataLen:1024 TTL:254 Proto:ICMP
ICMP Echo reply  ID:6666  Seq:0
```

Syntax: buffer .

Shows the contents of the most recently used buffer.

Example

```
Cmd> buff .
Decode of buffer number 1059
int: Enet 0050:dadf:7bbf -> 0003:325c:cc00, type 0x0800, len 1058
IP 192.168.123.10->193.13.79.1  IHL:20  DataLen:1024 TTL:254 Proto:ICMP
ICMP Echo reply  ID:6666  Seq:0
```

Certcache

Displays the contents of the certificate cache.

Syntax: certcache

CfgLog

Shows the results of the most recent reconfiguration or start up of *D-Link* Firewall. This text is the same as is shown on-screen during reconfiguration or start up.

Syntax: cfglog

Example

```
Cmd> cfglog
Configuration log:
Configuring from FWCore_N.cfg
Configuration done

Configuration "FWCore_N.cfg" (v153) verified for bi-directional communication
```

Connections

Shows the last 20 connections opened through the firewall. Connections are created when traffic is permitted to pass via Allow or NAT rules. Traffic permitted to pass under FwdFast is not included in this list.

Each connection has two timeout values, one in each direction. These are updated when the firewall receives packets from each end of the connection. The value shown in the Timeout column is the lower of the two values.

Possible values in the State column include:

SYN_RECV TCP packet with SYN flag received

SYNACK_S TCP packet with SYN + ACK flags sent

ACK_RECV TCP packet with ACK flag received

TCP_OPEN TCP packet with ACK flag sent

FIN_RECV TCP packet with FIN / RST flag received

PING The connection is an ICMP ECHO connection

UDP The connection is a UDP connection

RAWIP The connection uses an IP protocol other than TCP, UDP or ICMP

Syntax: connections

Example

```
Cmd> conn
State     Prot Source              Destination   Time
TCP_OPEN  TCP  ext:60.20.37.6:5432 dmz:wwwsrv:80 3600
SYN_RECV  TCP  ext:60.20.37.6:5433 dmz:wwwsrv:80 30
UDP_OPEN  UDP  int:10.5.3.2:5433   dmz:dnssrv:53 50
```

Cpuid

Shows information regarding the CPU in the firewall hardware.

Syntax: cpuid

Example

```
Cmd> cpuid
Processor:          Intel Pentium III, III Xeon, or Celeron
Brand ID:           Intel Pentium III
Frequency:          996 Mhz
Family:             6
Model:              8
Stepping:           10
Vendor id:          GenuineIntel
Type:               Original OEM Processor
Feature flags:      fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
cmov pat pse-36 psn mmx fxsr sse
Cache and TLB information:
0x01: Instruction TLB, 4K pages, 4-way set associative, 32 entries
0x02: Instruction TLB, 4M pages, fully associative, 2 entries
0x03: Data TLB, 4K pages, 4-way set associative, 64 entries
0x08: Instruction cache 16K, 4-way set associative, 32 byte line size
0x04: Data TLB, 4M pages, 4-way set associative, 8 entries
0x0C: Data cache, 16K, 4-way set associative, 32 byte line size
```

DHCP

Syntax: dhcp [options] <interface>

Options:

-renew - Force interface to renew it's lease

-release - Force interface to release it's lease

Example

```
Cmd> dhcp -renew ext
```

DHCPRelay

Show the contents of the DHCP-relay configuration section.

Syntax: dhcprelay [options]

Options:

-release ip - Releases the IP and removes associated routes from the firewall.

Example

```
Cmd> dhcprelay
Content of the DHCP/BOOTP-relayer ruleset; default action is IGNORE
#  Act.     Source         HW-Filter  Server          Allowed
1  RELAY    vlan1,vlan2..  *          192.168.0.10    192.168.0.100 - 192.168.0.120

Dynamically added routes for relayed DHCP leases
Iface           Host-Route         Local IP        ProxyARP            Expire
vlan2           192.168.0.101/32                   internals              3539
vlan4           192.168.0.112/32                   internals              3539
```

Frags

Shows the 20 most recent fragment reassembly attempts. This includes both ongoing and completed attempts.

Syntax: frags

Example

```
Cmd> frags
RecvIf Num State Source Destination Proto Next Timeout
int 2 Done 10.5.3.2 26.23.5.4 ICMP 2000 58
ext 8 Accept 23.3.8.4 10.5.3.2 ICMP 1480 60
```

HA

Shows information about a HA cluster.

Example

```
Cmd> ha
This device is a HA SLAVE
This device is currently ACTIVE (will forward traffic)
HA cluster peer is ALIVE
```

HTTPposter

Show the configured httpposter urls.

Example

```
Cmd> httpposter
HTTPPoster_URL1:
Host  : ""
Port  : 0
Path  : ""
Post  : ""
User  : ""
Pass  : ""
Status: (not configured)

HTTPPoster_URL2:
Host  : ""
Port  : 0
Path  : ""
Post  : ""
User  : ""
Pass  : ""
Status: (not configured)

HTTPPoster_URL3:
Host  : ""
Port  : 0
Path  : ""
Post  : ""
User  : ""
Pass  : ""
Status: (not configured)
```

Ifacegroups

Shows the configured interface groups.

Syntax: ifacegroups <name pattern>

Example

```
Cmd> ifacegroups
Configured interface groups:
internals       int,vlan1,vlan2,vlan3
```

IfStat

Syntax: ifstat

Shows a list of the interfaces installed in the firewall.

Example

```
Cmd>ifstat
Interfaces:
int             IPAddr 192.168.123.1    HwAddr 0003:47ab:ea25
Builtin e1000 - Intel(R) PRO/1000 T Server Adapter  Slot 2/1  IRQ 5
ext             IPAddr 194.2.1.2        HwAddr 0003:49a3:ef43
Builtin e1000 - Intel(R) PRO/1000 T Server Adapter  Slot 3/1  IRQ 11
Do 'ifstat <iface name>' to see details
```

Syntax: ifstat <interface>

Shows hardware and software statistics for the specified NIC.

Example

```
Cmd> ifstat int
Iface int
Builtin e1000 - Intel(R) PRO/1000 T Server Adapter  Slot 2/1  IRQ 5
Media         : "1000BaseTx"
Speed         : 1000 Mbps Full Duplex
Link Partner  : 10BASE-T, 10BASE-T FD, 100BASE-TX, 100BASE-TX FD, 1000BASE-TX F
Bus Type      : PCI 64-bit/33MHz
IP Address    : 192.168.123.1
Hw Address    : 0003:47ab:ea25
Software Statistics:
Soft received :  193075  Soft sent     :  212480  Send failures :       0
Dropped       :       0  IP Input Errs :       0
Hardware statistics:
IN : packets=  193074   bytes=36524718   errors=      10   dropped=      10
OUT: packets=  212646   bytes=208065794   errors=       0   dropped=       0
Collisions            :        0
In : Length Errors    :        0
In : Overruns         :        0
In : CRC Errors       :        0
In : Frame Errors     :        0
In : FIFO Overruns    :        0
In : Packets Missed   :        0
Out: Sends Aborted    :        0
Out: Carrier Errors   :        0
Out: FIFO Underruns   :        0
Out: SQE Errors       :        0
Out: Late Collisions  :        0
```

The Dropped counter in the software section states the number of packets discarded as the result of structural integrity tests or firewall ruleset drops.

The IP Input Errs counter in the software section specifies the number of packets discarded due to checksum errors or IP headers broken beyond recognition. The latter is most likely the result of local network problems rather than remote attacks.

Ikesnoop

Ikesnoop is used to diagnose problems with IPsec tunnels.

Syntax: ikesnoop

Display current ikesnoop status.

Syntax: ikesnoop off

Turn IKE snooping off.

Syntax: ikesnoop on

Turn IKE snooping on.

Syntax: ikesnoop verbose

Enable verbose output

Ipseckeepalive

Show the status of the configured Ipsec keepalive connections.

Example

```
Cmd> ipseckeepalive
192.168.0.10 -> 192.168.1.10: Consecutive lost: 0, sent: 908, lost: 2
192.168.1.10 -> 192.168.0.10: Consecutive lost: 0, sent: 913, lost: 6
```

Killsa

Kills all IPsec and IKE SAs for the specified IP-address.

Syntax: killsa <ipaddr>

Example

```
Cmd> killsa 192.168.0.2
Destroying all IPsec & IKE SAs for remote peer 192.168.0.2
```

License

Shows the content of the license-file. It is also possible to remove a license from a running firewall with this command, by doing a license remove.

Syntax: license [remove]

Example

```
Cmd> lic
Contents of the License file
----------------------------
Registration key:     1234-1234-1234-1234
Bound to MAC address: 00-48-54-00-3b-00
Company:              D-Link AB
Registration date:    2002-11-20 00:00:00.000
Issued date:          2002-11-20 19:22:38
Last modified:        2002-11-20 19:22:27
New upgrades until:   2003-02-14 00:00:00.000
Ethernet Interfaces:  4
Max Connections:      128000
Max Routes:           2048
Max Rules:            16000
Max Throughput:       200
Max VPN Tunnels:      20
Max VLANs:            2048
```

Lockdown

Sets local lockdown on or off. During local lockdown, only traffic from admin nets to the firewall itself is allowed. Everything else is dropped.

Note: If local lockdown has been set by the core itself due to licensing / configuration problems, this command will NOT remove such a lock.

Syntax: lockdown [on | off]

Loghosts

Shows the list of log recipients the firewall is configured to send log data to.

Syntax: loghosts

Example

```
Cmd> loghosts
Log hosts:
SysLog   192.168.123.10    Facility: local0
Usage logging in 3600 second intervals
```

Logout

Only works on the serial or local console, it is used to logout the current user and enable the password.

Netcon

Shows a list of users currently connected to the firewall via the netcon management protocol, i.e. from *D-Link* Firewall Manager.

Syntax: netcon

Example

```
Cmd> netcon
Currently connected NetCon users:
Iface    IP address        port
int      192.168.123.11   39495
```

Netobjects

Shows the contents of the Nets configuration section.

Syntax: netobjects

Example

```
Cmd> netobjects
List of named network objects:
extnet          194.2.1.0/24
intnet          192.168.123.0/24
all-nets        0.0.0.0/0
ip_ext          194.2.1.2/32
br_ext          194.2.1.255/32
br_int          192.168.123.255/32
ip_int          192.168.123.1/32
gw-world        194.2.1.1/32
```

Ping

Sends a specified number of ICMP Echo Request packets to a given destination. All packets are sent in immediate succession rather than one per second. This behavior is the best one suited for diagnosing connectivity problems.

Syntax: ping <IPAddr> [<options] [<# of packets> [<size>]]

Options:

-r <recvif> Run through the ruleset, simulating that the packet was received by <recvif>

-s <srcip> Use this source IP.

Example

```
Cmd> ping gw-world
Sending 1 ping to 194.2.1.1
Echo reply from 194.2.1.1    seq=0     time=<10 ms  TTL=128
```

Pipes

Shows the list of configured pipes; the contents of the Pipes configuration section, along with basic throughput figures of each pipe.

Syntax: pipes

Displays all configured pipes.

Example

```
Cmd>pipes
Configured pipes:
Name            Grouping        Bits/s Pkts/s Precedence
--------------- --------------- ------ ------ --------
std-in          Per DestIP                   0  1  7
Current: 42.5 K 21.0
std-out         Per SrcIP                    0  1  7
Current: 89.1 K 21.0
```

Syntax: pipes <name>

Displays in-depth details about the given pipe.

Syntax: pipes -u <name>

Displays the 20 currently most active users of the given pipe.

Proplists

Lists the configured proposal lists.

Syntax: proplists [<vpnconn>]

Example

```
Cmd> propl
Displaying all configured proposal lists:
ike-default
Type  : ISAKMP
Life    : 5000KB, 43200s
Cipher  : cast128-cbc
Hash    : sha1
Type  : ISAKMP
Life    : 5000KB, 43200s
Cipher  : cast128-cbc
Hash    : md5
Type  : ISAKMP
Life    : 5000KB, 43200s
Cipher  : 3des-cbc
Hash    : sha1
Type  : ISAKMP
Life    : 5000KB, 43200s
Cipher  : 3des-cbc
Hash    : md5
esp-tn-lantolan
Type  : ESP
Life    : 50000KB, 21600s
Cipher  : blowfish-cbc
Hmac    : hmac-sha1-96
Type  : ESP
Life    : 50000KB, 21600s
Cipher  : blowfish-cbc
Hmac    : hmac-md5-96
Type  : ESP
Life    : 50000KB, 21600s
Cipher  : cast128-cbc
Hmac    : hmac-sha1-96
Type  : ESP
Life    : 50000KB, 21600s
Cipher  : cast128-cbc
Hmac    : hmac-md5-96
```

ReConfigure

Re-reads the FWCore.cfg file from disk. This process takes approximately one second if done from floppy disk, and approximately a tenth of a second from hard disk or flash disk. If there is a FWCore_N.cfg file present on the disk, this will be read instead. However, as there is no Firewall Manager to attempt two-way communication with the firewall, it will conclude that the configuration is incorrect and revert to FWCore.cfg after the bi-directional verification timeout period has expired (typically 30 seconds).

Syntax: reconfiure

Example

```
Cmd>reconfigure
Shutdown RECONFIGURE. Active in 1 seconds.
Shutdown reason: Reconfigure due to console command
```

Remotes

Shows the contents of the Remotes configuration section.

Syntax: remotes

Example

```
Cmd> remotes
Hosts/nets with remote control of firewall:
int               192.168.0.12/32                 Configure/Update Access
```

Routes

Shows the contents of the Routes configuration section.

Syntax: routes

Example

```
Cmd>routes
Iface   Net               Gateway         Local IP        ProxyARP
ext     194.2.1.0/24
int     192.168.123.0/24
ext     0.0.0.0/0         194.2.1.1
```

Rules

Syntax: rules [<options>] [<range>]

Shows the contents of the Rules configuration section.

Options:

-u, Append usage information

-l, Append logging information

-n, Append symbolic rule names

-p, Append pipe information

-a, Append all the information above

The range parameter specifies which rules to include in the output of this command.

Example

```
Cmd> rule -u 11-12
ontents of ruleset; default action is DROP
Act.  Source                Destination           Protocol/Ports
1 Drop  any:0.0.0.0/0         any:0.0.0.0/0         PORTS ALL > 135-139
Use: 0
2 Drop  any:0.0.0.0/0         any:0.0.0.0/0         PORTS ALL > 445
Use: 0
```

Scrsave

Activates the screensaver included with the firewall core.

Syntax: scrsave

Example

```
Cmd>scr
Activating screen saver...
```

Services

Displays the list of named services. Services implicitly defined inside rules are not displayed.

Syntax: services [<name or wildcard>]

Settings

Shows the contents of the Settings configuration section.

Syntax: settings

Shows available groups of settings.

Example

```
Cmd>sett
Available categories in the Settings section:
IP           - IP (Internet Protocol) Settings
TCP          - TCP (Transmission Control Protocol) Settings
ICMP         - ICMP (Internet Control Message Protocol) Settings
ARP          - ARP (Address Resolution Protocol) Settings
State        - Stateful Inspection Settings
ConnTimeouts - Default Connection timeouts
LengthLim    - Default Length limits on Sub-IP Protocols
Frag         - Fragmentation Settings
VLAN         - VLAN Settings
SNMP         - SNMP Settings
DHCP         - DHCP (Dynamic Host Configuration Protocol) Settings
Log          - Log Settings
Misc         - Miscellaneous Settings
```

Syntax: settings <group_name>

Shows the settings of the specified group.

Example

```
Cmd> settings arp
ARP (Address Resolution Protocol) Settings
ARPMatchEnetSender     : DropLog
ARPQueryNoSenderIP     : DropLog
ARPSenderIP            : Validate
UnsolicitedARPReplies  : DropLog
ARPRequests            : Drop
ARPChanges             : AcceptLog
StaticARPChanges       : DropLog
ARPExpire              : 900       ARPExpireUnknown       : 15
ARPMulticast           : DropLog
ARPBroadcast           : DropLog
ARPCacheSize           : 4096      ARPHashSize            : 512
ARPHashSizeVLAN        : 64
```

Shutdown

Instructs the firewall to perform a shutdown in a given number of seconds. It is not necessary to perform a shutdown before the firewall is powered off, as it does not keep any open files while running.

Syntax: shutdown <seconds>

Example

```
Cmd> shutdown
```

Stats

Shows various vital stats and counters.

Syntax: stats

Example

```
Cmd> stats
Uptime             : 10 days, 23:11:59
Last shutdown      : Unknown reason ('shutdown.txt' is empty)
CPU Load           : 6%
Connections        : 4919 out of 32768
Fragments          : 17 out of 1024 (17 lingering)
Buffers allocated  : 1252
Buffers memory     : 1252 x 2292 = 2802 KB
Fragbufs allocated : 16
Fragbufs memory    : 16 x 10040 = 156 KB
Out-of-buffers     : 0
ARP one-shot cache : Hits : 409979144  Misses : 186865338
Interfaces: Phys:2 VLAN:5 VPN:0
Access entries:18  Rule entries:75
Using configuration file "FWCore.cfg", ver 199
```

Sysmsgs

Show the contents of the OS sysmsg buffer.

Syntax: sysmsgs

Example

```
Cmd> sysmsg
Contents of OS sysmsg buffer:
2003-04-24 00:03:46 Boot device number is 0x80
2003-04-24 00:03:46 Available LowPoolMemory:    360424 Bytes (LBlock: 360424 bytes)
2003-04-24 00:03:46 Available KernelPoolMemory: 1048560 bytes (LBlock: 1048560 bytes)
2003-04-24 00:03:46 Available UserPoolMemory:   198868948 bytes
2003-04-24 00:03:46 Drive 0x00 present: (C/H/S/SC/M): (0x50/0x2/0x12/0x24/0xb3f)
2003-04-24 00:03:46 Drive 0x80 present: (C/H/S/SC/M): (0x3f2/0x10/0x33/0x330/0xc935f)
2003-04-24 00:03:46 Drive 0x80 is using a FAT-16 filesystem
2003-04-24 00:03:46 Firewall loader up and running!
```

Time

Displays the system date and time

Syntax: time

Uarules

Shows configured user authentication rules.

Syntax: Uarules

Example

```
Cmd> uarules
Contents of the User Authentication ruleset
#  Source Net             Agent    Auth source Authentication Server
-- ---------------------- -------- ----------- --------------------
1  if1:192.168.0.0/24     HTTPAuth RADIUS      FreeRadius
2  *:0.0.0.0/0            XAuth    RADIUS      IASRadius
```

Userauth

Syntax: Userauth <options>

Display information about authenticated users, known privileges.

Options:

–l Displays a list of all authenticated users

–p Displays a list of all known privileges (usernames and groups)

–r <ip> Removes an authenticated user (=logout)

Example

```
Cmd> userauth -l
Currently authenticated users:
Login name: user1
User IP: 192.168.0.207   Idle Timeout: 1799
Privileges: members

Login name: user1
User IP: 192.168.0.214   Idle Timeout: 1800
Privileges: members

Login name: user2
User IP: 192.168.0.116   Idle Timeout: 1799
Privileges: members
```

Vlan

Syntax: vlan

Shows information about configured VLANs.

Example

```
Cmd> vlan
VLANs:
vlan1           IPAddr: 192.168.123.1    ID: 1  Iface: int
vlan2           IPAddr: 192.168.123.1    ID: 2  Iface: int
vlan3           IPAddr: 192.168.123.1    ID: 3  Iface: int
vlan4           IPAddr: 192.168.123.1    ID: 4  Iface: int
```

Syntax: vlan <vlan>

Show information about specified VLAN.

Example

```
Cmd> vlan vlan1
VLAN vlan1
Iface int, VLAN ID: 1
Iface         : int
IP Address    : 192.168.123.1
Hw Address    : 0003:474e:25f9
Software Statistics:
Soft received :       0  Soft sent     :       0  Send failures :       0
Dropped       :       0  IP Input Errs :       0
```

VPNConns

Display configured VPN connections.

Syntax: vpnconns

Example

```
Cmd>vpnconn
VPN Conns list
No Name       Local Net          Remote Net         Remote GW
0  vpn-home   192.168.123.0/24   0.0.0.0/0          None
MAIN_MODE SA_PER_NET DONT_VERIFY_PAD IKE group: 2
IKE proplist: ike-default, IPsec proplist: esp-tn-roamingclients
```

VPNStats

Display connected VPN gateways and remote clients.

Syntax: vpnstats <options>

Options:

-u - Append SA usage

-num <n>

Example

```
Cmd> vpnstat

--- IPsec SAs:

Displaying one line per SA-bundle

VPN Tunnel         Local net          Remote net         Remote GW
------------------ ------------------ ------------------ ------------------
vpn-home           192.168.123.0/24   192.168.1.2/32     192.168.1.2/32
```