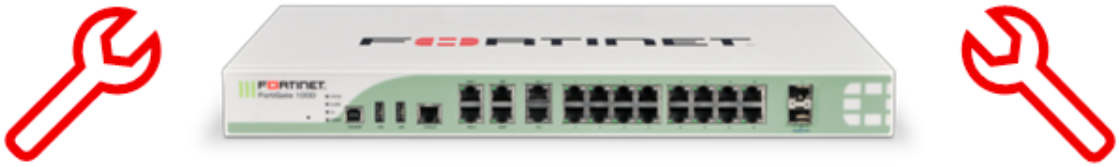
Blog Webernetz.net

IT-Security, Networks, IPv6, DNSSEC, Monitoring, Music, DIY



CLI Commands for Troubleshooting FortiGate Firewalls

2015-12-21 Fortinet, Memorandum, Network CLI, FortiGate, Fortinet, Quick Reference, Troubleshooting Johannes Weber

This blog post is a list of common **troubleshooting commands I am using on the FortiGate CLI**. It is not complete nor very detailled, but provides the basic commands for troubleshooting network related issues that are not resolvable via the GUI. I am not focused on too many memory, process, kernel, etc. details. These must only be used if there are really specific problems. I am more focused on the general troubleshooting stuff.

Coming from Cisco, everything is “show”. With Fortinet, you have the choice between **show | get | diagnose | execute**. Not that easy to remember. Likewise the **sys | system** keyword. It is always “diagnose sys” but “execute system”. 😉

Entering the correct vdom/gobal Config

Remember to enter the correct vdom or global configuration tree before configuring anything:

```
1 config global
2 config vdom
3     edit <vdom-name>
```

To show the **running configuration** (such as “show run”), simply type in:

```
1 show
```

```
1 show full-configuration
```

To omit the "–More–" stops when displaying many lines, you can set the terminal output to the following, which will display all lines at once. This is similar to "terminal length 0" from Cisco. Be careful with it, because this command is persistent. Set it to default after usage!

```
1 config system console
2   set output standard
3 end
```

To find a CLI command within the configuration, you can use the pipe sign "|" with "**grep**" (similar to "include" on Cisco devices). Note the "-f" flag to show the whole config tree in which the keywords was found, e.g.:

```
1 show | grep -f ipv6
2 show full-configuration | grep -f ipv6
```

General Information

The very basics:

```
rdware interfaces
ingle network interface, same as: diagnose hardware deviceinfo nic <nic-r
 command to see more interface stats such as errors

k usage
orked processed
cl. CPU and mem bars. Forks are displayed by [x13] or whatever




ck definition versions, last update, etc.
ossibe log entries
IP addresses of FQDN objects
, a status of 0 indicates a normal close of a process!
```

After rebooting a fresh device which is already **licensed**, it takes some time until it is "green" at the dashboard. The following commands can troubleshoot and start the "get license" process. Use the first three to enable debugging and start the process, while the last one disables the debugging again:

```
1 diag debug app update -1
2 diag debug enable
3 exec update-now
4 diag debug disable
```

General Network Troubleshooting

Which is basically **ping** and **traceroute**:

```
execute ping-options ?
execute ping-options source <ip-address-of-the-interface>
execute ping <hostname|ip>
execute ping6-options ?
execute ping6 <hostname|ip>
execute traceroute <hostname|ip>
execute tracert6 <hostname|ip>
```

Routing

```
get router info routing-table all    #routing table
get router info6 routing-table       #IPv6 without the "all" keyword
get router info kernel               #Forwarding Information Base
get router info6 kernel
get router <routing-protocol>        #basic information about the enab
diagnose firewall proute list        #policy-based routing
diagnose firewall proute6 list
diagnose ip rtcache list             #route cache = current sessions w
```

High Availability

```
diagnose sys ha status
execute ha manage ?                  #switch to the CLI of a secondary
execute ha manage <device-index>
diagnose sys ha showcsum             #verify the checksum of all synch
```

Session Table

Display the current active sessions:

```
get system session list              #rough view with NAT, only IPv4

diagnose sys session filter clear
diagnose sys session filter ?
diagnose sys session filter dst 8.8.8.8
diagnose sys session filter dport 53
```

Sniffer

Sniff packets like tcpdump does. This can be used for investigating connection problems between two hosts. There are no details of the firewall policy decisions. Use the debug flow (next paragraph) for analysis about firewall policies, etc.

```
1 diagnose sniffer packet <interface|any> '<tcpdump-filter>' <verbose>
   <count> <time-format>
```

with:

verbose:
1: print header of packets
2: print header and data from ip of packets
3: print header and data from ethernet of packets (if available)
4: print header of packets with interface name
5: print header and data from ip of packets with interface name
6: print header and data from ethernet of packets (if available) with intf name
count: number of packets
time-format:
a: UTC time
l: local time

Examples: (Thanks to the comment from Ulrich for the IPv6 example)

```
1 diagnose sniffer packet any 'host 8.8.8.8' 4 4 l
2 diagnose sniffer packet any 'host 8.8.8.8 and dst port 53' 4 10 a
3 diagnose sniffer packet wan1 'dst port (80 or 443)' 2 50 l
4 diagnose sniffer packet any 'net 2001:db8::/32' 6 1000 l
```

Here are two more examples on how **to show LLDP or CDP packets** in order to reveal the connected layer 2 ports from switches. Kudos to Joachim Schwierzeck.

```
1 LLDP:
2 diagnose sniffer packet port1 'ether proto 0x88cc' 4 1 a
3
4 CDP:
5 diagnose sniffer packet port1 'ether[20:2] == 0x2000' 6 1 a
```

Flow

If you want to see the **FortiGate details about a connection**, use this kind of debug. E.g., it shows the routing decision and the policy, which allowed the connection.

```
diagnose debug flow filter daddr 8.8.8.8
diagnose debug flow show console enable
diagnose debug enable
diagnose debug flow trace start 10  #display the next 10 packets, aft
diagnose debug disable
```

Example:

```
fd-wv-fw04 # diagnose debug reset

fd-wv-fw04 # diagnose debug flow filter daddr 8.8.8.8

fd-wv-fw04 # diagnose debug flow show console enable
show trace messages on console

fd-wv-fw04 # diagnose debug enable

fd-wv-fw04 # diagnose debug flow trace start 20
id=20085 trace_id=11 func=print_pkt_detail line=4420 msg="vd-root re
id=20085 trace_id=11 func=init_ip_session_common line=4569 msg="allo
id=20085 trace_id=11 func=vf_ip4_route_input line=1596 msg="find a r
id=20085 trace_id=11 func=fw_forward_handler line=671 msg="Allowed b
id=20085 trace_id=11 func=__ip_session_run_tuple line=2601 msg="run
id=20085 trace_id=12 func=print_pkt_detail line=4420 msg="vd-root re
id=20085 trace_id=12 func=init_ip_session_common line=4569 msg="allo
id=20085 trace_id=12 func=vf_ip4_route_input line=1596 msg="find a r
id=20085 trace_id=12 func=fw_forward_handler line=671 msg="Allowed b
id=20085 trace_id=12 func=__ip_session_run_tuple line=2601 msg="run

fd-wv-fw04 # diagnose debug disable
```

VPN

To **show** details about IKE/IPsec connections, use these commands:

```
get vpn ike gateway <name>
get vpn ipsec tunnel name <name>
get vpn ipsec tunnel details
diagnose vpn tunnel list
diagnose vpn ipsec status           #shows all crypto devices with co
get router info routing-table all
```

To **debug** IKE/IPsec sessions, use the VPN debug:

```
diagnose debug reset
diagnose vpn ike log-filter clear
diagnose vpn ike log-filter ?
diagnose vpn ike log-filter dst-addr4 1.2.3.4
diagnose debug app ike 255          #shows phase 1 and phase 2 output
diagnose debug enable               #after enough output, disable the
diagnose debug disable
```

```
diag vpn tunnel reset <phase1 name>
```

Log

For investigating the log entries (similar to the GUI), use the following filters, etc.:

```
execute log filter reset
execute log filter category event
execute log filter field            #press enter for options
execute log filter field dstport 8001
execute log filter view-lines 1000
execute log filter start-line 1
execute log display
```

Defaults

Just a reminder for myself:

- IP: 192.168.1.99
- Login: admin
- Password: <blank>

To change the IP address of the mgmt interface (or any other) via the CLI, these commands can be used:

```
config system interface
edit mgmt
set ip 192.168.1.1 255.255.255.0
set allowaccess ping https ssh
next
end
```

Links

- Fortinet: FortiOS 5.2 CLI Reference
- itsecworks: Fortigate troubleshooting commands