BOLL

IT Security Distribution

CHEATSHEET

FORTIGATE FOR FORTIOS 6.2

© BOLL Engineering AG, FortiOS Cheat Sheet 1.1 (14.10.2019)

General

Default Device Information

`admin / no password`	Default login
`192.168.1.99`	Default IP on port1, internal or management port

`9600/8-N-1`
`hardware flow control disabled`
	Default serial console settings

General system commands

`get system status`	General system information
`exec tac report`	Generates report for support
`tree`	Lists all commands
`<command> ? / tab`	Use ? or tab in CLI for help
`<command> | grep [filter]`	Grep command to filter outputs

Fortinet Links

`docs.fortinet.com`	Documentation, Cookbooks, Release Notes
`kb.fortinet.com`	Knowledge base
`www.fortiguard.com`	FortiGuard Website
`support.fortinet.com`	Support site (Login required)
`forum.fortinet.com`	User forum (Login required)
`fndn.fortinet.net`	Fortinet Developer Network (Login)
`blog.boll.ch`	Boll-Blog

FortiGate most used ports

`UDP/53, UDP/8888`	FortiGuard Queries
`TCP/389, UDP/389`	LDAP, PKI Authentication
`TCP/443`	Contract Validation, FortIToken, Firmware Updates
`TCP/443, TCP/8890`	AV and IPS Update
`UDP/500, ESP`	IPSEC VPN
`UDP/500, UDP/4500`	IPSEC VPN with NAT-Traversal
`TCP/514`	FortiManager, FortiAnalyzer
`TCP/1812` `TCP/1813`	RADIUS Authentication RADIUS Accounting
`UDP/5246, UDP/5247`	CAPWAP
`TCP/8001`	FSSO
`TCP/8013`	Compliance and Security Fabric
`ETH Layer 0x8890, 0x8891 and 0x8893`	HA Heartbeat

Network

Interface information

`diag ip address list`	List of IP addresses on FortiGate interfaces
`diag firewall iplist list`	List of IP addresses on VIP and IP-Pools

Security Fabric

`diag sys csf upstream / downstream`	List of up/downstream devices
`diag sys csf neighbor list`	MAC/IP list of connected FG devices
`diag automation test <stich_name>`	Test stitches in the CLI
`diag test appl csfd 1 …`	Display security fabric statistics
`diag debug appl csfd -1`	Real-time debugger

Switch Controller

`diag switch-controller switch-info mac-table`	Managed FortiSwitch MAC address list
`diag switch-controller switch-info port-stats`	Managed FortiSwitch port statistics
`diag switch-controller switch-info trunk`	Trunk information
`diag switch-controller switch-info mclag`	Dumps MCLAG related information from FortiSwitch
`execute switch-controller get-conn-status`	Get FortiSwitch connection status
`execute switch-controller diagnose-connection`	Get FortiSwitch connection diagnostics

SD-WAN

`diag sys virtual-wan-link member`	Provide Interface details
`diag sys virtual-wan-link health-check <name>`	State of SLAs
`diag sys virtual-wan-link service <rule-id>`	SD-WAN-Rule-State
`diag sys virtual-wan-link intf-sla-log <intf-name>`	Link Traffic History
`diag sys virtual-wan-link sla-log <sla> <link_id>`	SLA-Log on specific interface
`diag test application lnkmtd 1 / 2 / 3`	Statistics of link-monitor
`diag debug application link-monitor -1`	Real-time debugger of link-monitor

Network Troubleshooting

`get hardware nic [port]`	Interface Information

`get system arp`
`diag ip arp list`
	ARP table

`exec clear system arp table`	Clears ARP table

`exec ping x.x.x.x`
`exec ping-options [option]`
	Ping utility

`exec traceroute x.x.x.x`
`exec traceroute-options [option]`
	Traceroute utility

`exec telnet x.x.x.x [port]`	Telnet utility

`diag traffictest server-intf`
`diag traffictest client-intf`
`diag traffictest port [port]`
`diag traffictest run -c [public_iperf_server_ip]`
	Iperf test directly run from FortiGate

Transparent Mode

`diag netlink brctl`	Bridge MAC table

Routing

Routing troubleshooting

`get router info routing-table all`	Routing table
`get router info routing-table details x.x.x.x`	Shows Routing decision for specified Destination-IP
`get router info routing-table database`	Routing table with inactive routes
`get router info kernel`	Forwarding information base
`diag firewall proute list`	List of policy-based routes
`diag ip rtcache list`	List of route cache
`get router info protocols`	Overview of dynamic routing protocol configuration
`exec router restart`	Restart of routing process
`diag sys link-monitor status/interface/launch`	Shows link monitor status / per interface / for WAN LLB

BGP

`get router info bgp summary`	BGP summary of BGP status
`get router info bgp neighbors`	Information on BGP neighbors

`diag ip router bgp all enable`
`diag ip router bgp level info`
	Real-time debugging for BGP protocol

`exec router clear bgp all`	Restart of BGP session

OSPF

`get router info ospf status`	OSPF status
`get router info ospf interface`	Information on OSPF interfaces
`get router info ospf neighbor`	Information on OSPF neighbors
`get router info ospf database brief / router lsa`	Summary / Details of all LSDB entries
`get router info ospf database self-originate`	Information on LSAs originating from FortiGate

`diag ip router ospf all enable`
`diag ip router ospf level info`
	Real-time debugging of OSPF protocol

`exec router clear ospf process`	Restart of OSPF session

System

Process information

`get system performance status`	General performance information
`diag sys top [sec] [number]`	Process list Sort with P (CPU) / M (Memory)
`diag sys top-summary [sec]`	Process list with grouped processes and shared memory
`diag debug crashlog read`	Crash log

High availability

`execute ha manage [index] [admin]`	Jump to cluster member
`get sys ha status`	Information about current HA status
`diag sys ha dump-by vcluster`	Show cluster member uptime
`diag sys ha reset-uptime`	Reset cluster member uptime
`diag sys ha checksum cluster`	Show config checksums of all cluster member
`diag sys ha checksum show [vdom]`	Detailed config checksum for a VDOM
`diag sys ha checksum recalculate`	Recalculation of config checksums

`diag debug appl hatalk -1`
`diag debug appl hasync -1`
	Debugging of HA-Talk/-Sync protocols

`exec ha ignore-hardware-revision status / enable / disable`	Set ignore status for different HW revisions

VDOMs

`sudo global/ vdom-name`
`diag / execute / show / get`
	Sudo-command to access global / VDOM settings directly

FQDN

`diagnose test application dnsproxy 6`	Dump FQDN cache
`diagnose firewall fqdn list`	List all FQDN

Internet Service database (ISDB)

`diag internet-service info vdom proto port ip`	Lists summary/details for specific Internet Service
`diag internet-service info …`	Reverse ISDB lookup for specific IP, protocol or port
`diag internet-service match <vdom> <ip> <netmask>`	Reverse ISDB lookup for specific IP

Traffic Shaper

`diag firewall shaper traffic-shaper list / stats`	Traffic shaper list / statistics
`diag firewall shaper per-ip-shaper list / stats`	Per IP traffic shaper list / statistics

Logging

`diag log test`	Generates dummy log messages
`exec log list`	List log file information
`diag debug cli 8`	Shows webGUI changes in CLI

Firmware Update

`diag debug config-error-log read`	Show config errors after firmware upgrades

Factory reset

`exec factoryreset`	Reset whole configuration
`exec factoryreset2`	Reset with retaining admin, interfaces and static routing

Traffic Processing

General debugging

`diag debug appl [appl-name] [debug_level`	Realtime debugger for several applications
`diag test appl [appl-name] [test_level]`	Monitor proxy operations
`diag debug console timestamp enable`	Enables timestamp in console

`diag debug enable`
`diag debug disable`
	Enable/disable output for “diag debug” and “diag ip” commands

`diag debug reset`	Reset debug levels

Packet sniffer

`diag sniffer packet [if] ‘[filter]’ [verbose] [count] [ts]`	Packet sniffer. Use filters! Verbose levels 1-6 for different output

Flow Trace

`diag debug flow show iprop en`
`diag debug flow show fun en`
`diag debug flow trace start [packet count]`
	Debug command for traffic flow.

`diag debug flow filter [filter]`	Use filters to narrow down search results

Firewall session troubleshooting

`diag sys session filter`	Filter for session list
`diag sys session list[expect]`	Lists all (or expected) sessions
`diag sys session clear`	Clear all / filtered sessions
`diag sys session stat`	Session statistics, memory tension, ephemeral drops
`diag firewall iprope clear 100004 [<id>]`	Resets counter for all or specific firewall policy id

UTM Services

FortiGuard Distibution Network (FDN)

`update.fortiguard.net`
`service.fortiguard.net`
`support.fortinet.com`
	URLs to access the FortiGuard Distribution Network (FDN)

Signature update

`diag debug rating`	Webfilter / AntiSpam Server information
`diag autoupdate versions`	Detailed versions of packages

`diag debug appl update -1`
`exec update-now`
	Troubleshooting update process

IPS

`diag ips anomaly list`	Lists statistics of DoS-Policies
`diag ips packet status`	IPS packet statistics
`diag test appl ipsmonitor 2`	Enable / disable IPS engine
`diag test appl ipsmonitor 5`	Toggle bypass status
`diag test appl ipsmonitor 99`	Restart all ipsengine and monitor

Emailfilter

`diag emailfilter fortishield servers`	Displays FortiShield server list.
`diag debug appl emailfilter 255`	Debugger for spamfilter

Webfilter

diag webfilter fortiguard statistics list	Statistics of FortiGuard requests
diag test appl urlfilter 1	Lists webfilter test commands

SIP

diag system sip status	SIP session helper status
diagnose sys sip-proxy stats list	SIP ALG session status

Authentication

Authentication

diag firewall auth filter	Filter for authentication list
diag firewall auth list	List of authenticated user
diag test authserver [auth-protocol] [server] [user] [password]	Authentication test
diag debug appl auth -1	Debugging of local authentication protocol
diag debug appl fnbamd -1	Debugging of Remote authentication protocol

Explicit proxy

diag wad user list/clear	List / clear of explicit proxy user
diag wad filter diag wad session list	Filtering / listing of web proxy sessions
diag test appl wad 104	DNS statistics for explicit proxy
diag test appl wad 110	Current proxy user
diag test appl wad 112	Enables output of subsequent commands
diag test appl wad 2200	Maximum number of users

FortiToken

diag fortitoken info	Current FortiToken status
exec fortitoken activate [FortiTokenSN]	Manual FortiToken activation
diag deb appl forticldd 255	FortiToken activation debugging
exec fortitoken-mobile import 0000-0000-0000-0000	Recover Trial FortiToken

FSSO

diag debug authd fsso filter	Filter for FSSO user list.
diag debug authd fsso list	List of FSSO authenticated user
diag debug authd fsso server-status	List of FSSO collector agents
diag debug fsso-polling …	Info for clientless polling FSSO
diag debug appl fssod -1	Debugging of clientless polling FSSO

VPN

IPSEC VPN

diag debug appl ike 63	Debugging of IKE negotiation
diag vpn ike log filter	Filter for IKE negotiation output
diag vpn ike gateway list	Phase 1 state
diag vpn ike gateway flush	Delete Phase 1
diag vpn tunnel list	Phase 2 state
diag vpn tunnel flush	Delete Phase 2
get vpn ipsec tunnel details	Detailed tunnel information
get vpn ipsec state tunnel	Detailed tunnel statistics
diag vpn ipsec status	Shows IPSEC crypto status

Hardware

Disk operation

diag hardware deviceinfo disk	List disks with partitions
exec disk list	List the disks and partitions
exec disk scan [ref_int]	Run a disk check operation
exec disk format [ref_int]	Format the specified partitions or disks and then reboots the system if a reboot is required
exec formatlogdisk	Formatting the log disk, reboot included

Hardware acceleration

set auto-asic-offload disable	Disable session offloading per firewall policy
set npu-offload disable	Disable VPN offloading per Phase 1

Hardware information

diag hardware sysinfo cpu	CPU information
diag hardware sysinfo memory	Memory size, utilization
diag hardware sysinfo conserve	Conserve Mode details: “Mem”: Memory / “FD”: File descriptor
diag hardware test suite all	Hardware test (available only on newer models)
get hardware nic [port]	Physical interface information
get system interface physical / transceiver	Signal information for Copper or SFP/SFP+ interfaces

HQIP hardware check

https://support.fortinet.com → Download → HQIP	Download Hardware Quick Inspection Package (HQIP) Images to scan hardware for possible faults

Wireless, FortiExtender, Modem

Wireless Controller

exec wireless-controller restart-acd	Restart wireless controller daemon
exec wireless-controller reset-wtp	Restart FortiAPs
diag wireless-controller wlac -c ap-rogue	List rogue APs

Access point (CLI commands on Access point)

cfg -a ADDR_MODE=DHCP|STATIC	Change IP from DHCP to static on FortiAP
cfg -a AP_IPADDR=”xxx.xxx.xxx.xx”	Set static IP on FortiAP
cfg -a AP_NET-MASK=”255.255.255.0”	Set subnet mask on FortiAP
cfg -a IPGW=”yyy.yyy.yyy.yyy”	Set gateway on FortiAP
cfg -a AC_IPADDR_1=”zzz.zzz.zzz.zzz”	Specify IP of Wireless Controller on FortiAP
cfg -c	Save config on FortiAP
cfg -s	List config on FortiAP
cfg -x	Reset to factory default

FortiExtender

get extender sys-info [FXT SN]	Check the FortiExtender status
get extender modem-status [FXT SN]	Get the detailed modem status of the FortiExtender
diag debug application extender -1	Enable FortiExtender logging and debugging, collect information for about 5 minutes
exec extender reset-fortiextender	Restart managed FortiExtender
exec extender restart-fortiextender-daemon	Restart for AC daemon

Modem

diag sys modem detect	Detect attached modem
diag debug appl modemd 3	Debugger for modem commands