Cheat Sheet - General

FortiGate
for FortiOS 7.0

The cheat sheet from BOLL. Here you can find all important FortiGate CLI commands for the operation and troubleshooting of FortiGates with FortiOS 7.0.

System

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
diag debug cli 8	Shows webGUI changes in CLI

Process Information

get system performance status	General performance infos
diag sys top [sec] [number]	Process list Sort with P (CPU) / M (Memory)
diag debug crashlog history	Crash statistics
diag debug crashlog read	Crash log

Traffic Processing

General Debugging

diag debug appl [appl] [level]	Realtime debugger for different applications
diag test appl [appl] [test_level]	Monitor proxy operations
diag debug console timestamp enable	Enables timestamp in console
diag debug [enable/disable]	Enable/disable output for “diag debug” or “diag ip” commands
diag debug reset	Reset debug levels

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 and memory statistics, drops, clashes
diag firewall iprope clear 100004 [<id>]	Resets counter for all or specific firewall policy id

Packet Sniffer

diag sniffer packet [any/<if>] ‘[filter]’ [verbose] [count] [timestamp]	Packet sniffer. Use filters! Verbose levels 1-6 for different output

Flow Trace

diag debug flow filter [filter]	Use filters to narrow down trace results
diag debug flow show iprop en diag debug flow show fun en diag debug flow trace start [count]	Debug command for traffic flow

Network

Interface Information

diag ip address list	List of IPs on FGT interfaces
diag firewall iplist list	List of IPs on VIP and IP-Pools

Network Troubleshooting

get hardware nic [port]	Interface Information
diag ip arp list get system arp	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

Integrated Iperf 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

General 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

High Availability

HA General

exec ha manage [index] [admin]	Jump to cluster member
get sys ha status	Information about HA status
diag sys ha history read	Details about past HA events
diag sys ha dump-by vcluster	Show cluster member uptime
diag sys ha reset-uptime	Reset cluster member uptime
diag debug appl hatalk -1 diag debug appl hasync -1	Debugging of HA-Talk/-Sync protocol
exec ha ignore-hardware-revision status / enable / disable	Set ignore status for different HW revisions
exec ha failover status	View failover status
exec ha failover set <cluster_id>	Device stays in failover state regardless of condition. Triggers a HA failover on master device.

Cluster Synchronisation

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

Cheat Sheet - Firewalling

FortiGate
for FortiOS 7.0

UTM Services

FortiGuard Distibution Network (FDN)	
update.fortiguard.net service.fortiguard.net securefw.fortiguard.net	URLs to access the FortiGuard Distribution Network (FDN)
diag fdsm image-list / image-update-matrix	Download firmware image list and update-matrix

Signature Update	
diag autoupdate status	Summary of Fortiguard settings
diag autoupdate versions	Detailed versions of packages
diag debug appl update -1 exec update-now	Realtime debugging for updating process with manual update

Antivirus	
diag antivirus database-info	Antivirus database information
diagnose antivirus test …	Different tests for AV engine

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 IPS processes

Web-&Email-Filter	
diag debug rating	Webfilter / AntiSpam Server information
diag webfilter fortiguard statistics list	Statistics of FortiGuard requests
diag webfilter fortiguard cache dump	List content of webfilter cache
diag test appl urlfilter 1	Lists webfilter test commands
diag debug urlfilter src-addr x.x.x.x diag debug appl urlfiter -1	Filter and Realtime Debugging for Webfiltering
diag emailfilter fortishield servers	Displays FortiShield server list
diag emailfilter fortishield stat list	Statistics of FortiShield requests

DNS-Filter	
diag test appl dnsproxy 3	Shows server used for DNS-Filtering

Firewall Policy

Device Detection	
exec update-src-vis	Update device detection DB
diag user device list / clear	Show / clear detected devices

Internet Service Database (ISDB)	
diag internet-service-name list <internet-service-id>	Lists summary/details for specific Internet Service
diag internet-service info <vdom><proto><port><ip><prio>	Reverse ISDB lookup for specific IP, protocol or port
diag internet-service match <vdom> <ip> <netmask>	Reverse ISDB lookup for specific IP

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

Logging	
diag log test	Generates dummy log messages
exec log list	List log file information
diag test app miglogd 6	Show log queue and fails

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

SIP	
diag sys sip status	SIP session helper status
diag sys sip-proxy stats list	SIP ALG session status
diag sys sip-proxy calls list/clear	List/Clear active SIP calls
diag debug appl sip -1	Realtime Debugger for SIP

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 authd -1	Debugging of local authentication protocol
diag debug appl fnbamd -1	Debugging of remote authentication protocol

FortiToken	
diag fortitoken info	Current FortiToken status
exec fortitoken activate [Forti-TokenSN]	Manual FortiToken activation
diag deb appl forticldd 255	FortiToken activation debugging
diag fortitoken debug enable	FortiToken debugging
exec fortitoken-mobile import 0000-0000-0000-0000-0000	Recover Trial FortiToken (delete existing Trial Token before)

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

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

Cheat Sheet - Networking

FortiGate
for FortiOS 7.0

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 ike gateway	Detailed gateway information
get vpn ipsec tunnel details	Detailed tunnel information
get vpn ipsec state tunnel	Detailed tunnel statistics
diag vpn ipsec status	Shows IPSEC crypto status

SD-WAN & Security Fabric

SD-WAN

diag sys sdwan member	Provide Interface details
diag sys sdwan health-check status | filter <name>	State of SLAs
diag sys sdwan service <rule-id>	SD-WAN-Rule-State
diag sys sdwan intf-sla-log <intf-name>	Link Traffic History
diag sys sdwan sla-log <sla> <link_id>	SLA-Log on specific interface
diag test appl lnkmtd 0/1/2	Statistics of link-monitor
diag debug appl link-mon -1	Real-time debugger of link-monitor

Security Fabric

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

BGP, OSPF

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

Wireless, Switch, FortiExtender

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 –s / -c	List / Save config on FortiAP
cfg -x	Reset to factory default

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
exec wireless-controller spectral-scan <wtp-id> <radio-id > <on | off> <duration> <channel> <report-interval>	Start or stop spectrum analysis
diag wireless-controller wlac -c rf-sa <wtp-id> <radio-id> <channel> get wireless-controller spectral-info <wtp-id> <radio-id>	Show spectrum analysis results

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
exec switch-controller get-conn-status	Get FortiSwitch connection status
exec switch-controller diagnose-connection	Get FortiSwitch connection diagnostics
diag switch-controller mac-device known / clear	Show / Clear MAC devices

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 appl extenderd -1	FortiExtender 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

Cheat Sheet – Other

FortiGate
for FortiOS 7.0

System

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

Factory Reset	
exec factoryreset	Reset whole configuration
exec factoryreset-shutdown	Reset config and shutdown
exec factoryreset2	Reset with retaining admin, interfaces and static routing
exec factoryreset keepvmlicense	Reset whole config but license

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

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

Transparent Mode	
diag netlink brctl name host	Bridge MAC table

Workspace Mode	
exec config-transaction start/abort/commit	Start/abort/commit of Workspace Mode
diag sys config-transaction status	State of Workspace Mode (enabled/disabled)
diag sys config-transaction show txn-info	Shows all active Workspace Modes
diag sys config-transaction show txn-cli-commands	Pending CLI commands of Workspace Mode

Hardware

Hardware Information	
diag hardware sysinfo cpu	CPU information
diag hardware sysinfo conserve	Conserve Mode details. "Mem": Memory / "FD": File descriptor
diag hardware sysinfo memory	Memory size, utilization
diag hardware test suite all	Hardware test (available only on newer models)
get hardware status	ASIC and NP information
get vpn status ssl hw-acceleration-status	Show HW acceleration status for SSL VPN
get hardware nic [port]	Physical interface information
get system interface physical / transceiver	Signal information for Copper or SFP/SFP+ interfaces

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 reboots the system
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

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

General Information

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	
TCP/443, TCP & UDP/53 TCP & 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, 0x8893	HA Heartbeat / Sync