BOLL
IT Security Distribution

CHEATSHEET

FORTIGATE FOR FORTIOS 5.6

General

Default device information	
admin / [no password]	Defaultv
192.168.1.99/24	Default IP on port1, internal or management port
9600/8-N-1 hardware flow control disabled	Default serial console settings

Fortinet Links	
docs.fortinet.com	Documentation
kb.fortinet.com	Knowledge base
cookbook.fortinet.com	Cookbook
support.fortinet.com	Support site (Login required)
forum.fortinet.com	User forum (Login required)
wiki.diagnose.fortinet.com	Diagnose Wiki

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

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

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

Logging	
diag log test	Generates dummy log messages

Network

Network Troubleshooting	
get hardware nic [port]	Interface information
get system arp diag ip arp list	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

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

Transparent Mode	
diag netlink brctl	Bridge MAC table

Routing

Routing troubleshooting	
get router info routing-table all	Routing table
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	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 neighbors	Information on OSPF neighbors
get router info ospf database brief	Summary of all LSDB entries
get router info ospf database router lsa	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	Restart of OSPF session

Traffic Processing

General debugging	
diag debug appl [appl-name] [debug_level] diag test appl [appl-name] [test_level]	Debugger for several applications
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

Paket Sniffer	
diag sniffer packet [interface] ‘[filter]’ [verbose] [count] [tsformat]	Packet sniffer. Use filters to narrow down search results. Verbose levels 1-6 for different output.

Flow Trace	
diag debug flow filter [filter] diag debug flow show fun ena diag debug flow trace start [packet count]	Debug command for traffic flow. 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 00100004 [<id>]	Resets counter for all or specific firewall policy id

Internet Services Database	
get application internet-service status | grep <name>	Finds ISDB for specific Internet Service
diag internet-service id-summary/id <id>	Lists summary/details for specific Internet Service
diag internet-service info …	Reverse ISDB lookup for specific IP, protocol, port

UTM Services

Signature Update	
diag debug rating	Service 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

Spamfilter

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

Webfilter

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

Authentication

Authentication

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

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

System

Process information

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

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 tunnel list	Phase 2 state
diag vpn ike gateway flush	Delete Phase 1
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 operations

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
get hardware npu npx list	Interface / NPx affiliation

Hardware information

diag hardware sysinfo cpu	CPU information
diag hardware sysinfo memory	Memory size, utilization
diag hardware sysinfo shm	Conserve Mode details: “Mem”: Memory / “FD”: File descriptor
diag hardware test suite all	Hardware test (available only on certain 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
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_NETMASK=”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 [FXTserial]	Check the FortiExtender status
get extender modem-status [FXTserial]	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

Miscellaneous

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

High Availability

execute ha manage [index]	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
exec 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} {diagnose|execute|show|get}	Sudo-command to access global / VDOM settings directly

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