Useful CLI commands FortiOS

Cheatsheets

- FortiOS 6.2 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-version-6-2/)
- FortiOS 7.0 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-7-0/)
- FortiOS 7.2 CheatSheet (https://blog.boll.ch/cheatsheet-fortios-v7-2/)

CLI Commands

> To start a transaction in CLI use ***execute config-transaction start***.

> A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded

> Commit config changes with ***execute config-transaction commit.***
> Abort with ***execute config-transaction abort.***

Generic Commands

Default Device Information

admin / no password	Default login
192.168.1.99	Default IP on port1, internal or management port
9600/8-N-1, hw flow control disabled	Default serial console settings

General system commands

get system status	General system information

exec tac support	Generates report for support
tree	List all commands
<command> ? / tab	Use ? or tab in CLI for help
<command> | grep [filter]	Grep commands to filter output

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 Auth & Accounting
UDP/5246, UDP/5247	CAPWAP
TCP/8001	FSSO
TCP/8013	Compliance and Security Fabric
ETH Layer 0x8890, 0x8891 and 0x8893	HA Heartbeat For HA The virtual MAC address is determined based on following formula: 00-09-0f-09-<group-id_hex>-(<vcluster_integer> + <idx>)

Network commands

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 releated 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 **get system arp | grep x.x.x.x** **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
exec dhcp lease-list	Show DHCP Leases
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	Show routing table
get router info routing-table details x.x.x.x	Show 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
exec router restart	Restart of routing process
diag sys link-monitor status/interface/launch	Show link monitor status / per interface / for WAN LB

BGP

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

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 statistics
get vpn ipsec tunnel summary	Detailed tunnel information
diag vpn ipsec status	Shows IPSEC crypto status
show full vpn certificate local	Export all keys and certs

Revision #18
Created 20 May 2021 12:43:17
Updated 13 March 2024 09:19:30 by Peter Baumann