Cheatography

Fortigate troubleshooting Cheat Sheet

by logiweb via cheatography.com/63715/cs/16164/

CLI Basics

show s full-configuration	show configuration
config vdom	enter the correct vdom or global configuration
edit **<vdom-name>**	select vdom
show | grep -f ipv6	To find a CLI command within the configuration, you can use the pipe sign "|"
execute backup config flash	save your config
config system global set revision-backup-on-logout enable end	aves a backup of your configuration after each logout automatically
get system interface physical	overview of hardware interfaces
get hardware nic <nic-name>	Details of a single network interface, same as: diagnose hardware deviceinfo nic <nic-name>
fnsysctl ifconfig	kind of hidden command to see more interface stats such as errors
get system status	==show version
get system performance status	CPU and network usage
diagnose sys top	top with all forked processed
diagnose sys top-summary	top easier, incl. CPU and mem bars.
diagnose test application dnsproxy 6	shows the IP addresses of FQDN objects
diagnose debug crashlog read	shows crashlog, a status of 0 indicates a normal close of a process!
execute reboot	reboot your device
config system interface edit mgmt set ip **192.168.1.1 255.255.255.0** set allowaccess ping https ssh next end	To change the IP address of the mgmt interface

By **logiweb**
cheatography.com/logiweb/

Not published yet.
Last updated 22nd June, 2018.

Cheatography

Fortigate troubleshooting Cheat Sheet

by logiweb via cheatography.com/63715/cs/16164/

General Network Troubleshooting

execute ping-options ? execute ping-options source <source-interface-IP> execute ping <hostname|ip>	Ping from another source address
execute traceroute <hostname|ip> execute traceroute-options ?	traceroute
execute ping-options view-settings	view settings
execute ping6-options view-settings	view settings
execute traceroute-options view-settings	view settings

Remote Server Authentication Test

diagnose test authserver ldap <server_name> <username> <password>
diagnose test authserver radius <server_name> <chap | pap | mschap | mschap2> <username> <password> diagnose test authserver local <group_name> <username> <password>
diagnose test authserver local <group_name> <username> <password>

Session Table

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 diagnose sys session list	show the session table with the filter just set

Routing

get router info routing-table all	IPv4 needs an "all" at the end
get router info6 kernel	Forwarding Information Base
diagnose firewall proute6 list	#Policy Routes + WAN Load Balancing
2 3 4 diagnose sys ha status execute ha manage ? execute ha manage **<device-index>** diagnose sys ha showcsum	verify the checksum of all synchronized peers

Flow

display the next 10 packets, after that, disable the flow: diagnose debug disable

diagnose debug reset
diagnose debug flow filter ?
diagnose debug flow filter saddr 172.16.27.148
diagnose debug flow filter daddr 8.8.8.8
diagnose debug flow show console enable
diagnose debug enable
diagnose debug flow trace start
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 counters that are used by the VPN
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 debug:*
diagnose debug **disable**

To reset a certain VPN connection

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

Defaults

Just a reminder for myself:
IP: 192.168.1.99
Login: admin
Password: <blank>

Backup and Restore

execute backup full-config tftp <full-config-filename> <tftp server ip>	Backup command with tftp server
execute restore config tftp <full-config-filename> <tftp server ip>	Restore command with tftp server