Fortigate debug and diagnose commands complete cheat sheet

NOTE	To enable debug set by any of the commands below, you need to run **diagnose debug enable**. This is assumed and not reminded any further.
NOTE	To disable and stop immediately any debug, run **dia deb res** which is short for **diagnose debug reset**.

IPSEC VPN debug

Table 1. IPSEC VPN Debug

Command	Description
diagnose vpn ike log-filter <parameter>	Filter VPN debug messages using various parameters: • `list` Display the current filter. • `clear` Erase the current filter. • `name` Phase1 name to filter by. • `src-addr4`/`src-addr6` IPv4/IPv6 source address range to filter by. • `dst-addr4`/`dst-addr6` IPv4/IPv6 destination address range to filter by. • `src-port` Source port range • `dst-port` Destination port range • `vd` Index of virtual domain. -1 matches all. • `interface` Interface that IKE connection is negotiated over. • `negate` Negate the specified filter parameter.
diagnose debug application ike -1	Enable IPSec VPN debug, shows phase 1 and phase 2 negotiations (for IKEv1) and everything for IKEv2. "-1" sets the verbosity level to maximum, any other number will show less output.
diagnose vpn ike gateway flush name <vpn_name>	Flush (delete) all SAs of the given VPN peer only. Identify the peer by its Phase 1 name.

Command	Description
get vpn ipsec tunnel details	Detailed info about the tunnels: Rx/Tx packets/bytes, IP addresses of the peers, algorithms used, detailed selectors info, lifetime, whether NAT Traversal is enabled or not.
get vpn ipsec stats tunnel	Short general statistics about tunnels: number, kind, number of selectors, state
get vpn ipsec tunnel summary	Short statistics per each tunnel: number of selectors up/down, number of packets Rx/Tx.
get vpn ipsec stats crypto	Statistics of the crypto component (ASIC/software) of the Fortigate: encryption algorithm, hasshing algorithm.

Static Routing Debug

Table 2. Static and Policy Based Routing debug & diagnostics

Command	Description
get router info kernel	View the kernel routing table (FIB). This is the list of resolved routes actually being used by the FortiOS kernel. `tab` Table number, either 254 for unicast or 255 for multicast. `vf` Virtual domain index, if no VDOMs are enabled will be 0. `type` 0 - unspecific, 1 - unicast, 2 - local , 3 - broadcast, 4 - anycast , 5 - multicast, 6 - blackhole, 7 - unreachable , 8 - prohibited. `proto` Type of installation, i.e. where did it come from: 0 - unspecific, 2 - kernel, 11 zebOS module, 14 - FortiOS, 15 - HA, 16 - authentication based, 17 - HA1 `prio` priority of the route, lower is better. `pref` preferred next hop for this route. `Gwy` the address of the gateway this route will use `dev` outgoing interface index. If VDOMs enabled, VDOM will be included as well, if alias is set it will be shown.
get router info routing-table all	Show RIB - active routing table with installed and actively used routes. It will not show routes with worse priority, multiple routes to the same destination if unused.
get router info routing database	Show ALL routes, the Fortigate knows of - including not currently used.
get router info routing-table details <route>	Show verbose info about specific route, e.g. `get router info routing-table details 0.0.0.0/0`
get firewall proute	Get all configured Policy Based Routes on the Fortigate.

NTP debug

Table 3. NTP daemon diagnostics and debug

Command	Description
diag sys ntp status	Current status of NTP time synchronization. Shows all NTP peers and their detailed info: reachability, stratum, clock offset, delay, NTP version.
execute date	Show current date as seen by Fortigate
exec time	Show current time as seen by Fortigate

BGP

Table 4. BGP debug

Command	Description
diagnose ip router bgp level info **diagnose ip router bgp all enable**	Set BGP debug level to INFO (the default is ERROR which gives very little info) and enable the BGP debug.
exec router clear bgp all	Disconnect all BGP peering sessions and clear BGP routes in BGP table and RIB. Use with care, involves downtime.
get router info bgp summary	State of BGP peering sessions with peers, one per line.
get router info bgp network <prefix>	Detailed info about <prefix> from the BGP process table. Output includes all learned via BGP routes, even those not currently installed in RIB. E.g. `get router info bgp network 0.0.0.0/0`. The <prefix> is optional, if absent shows the whole BGP table.
get router info routing-table bgp	Show BGP routes actually installed in the RIB.
get router info bgp neighbors	Detailed info on BGP peers: BGP version, state, supported capabilities, how many hops away, reason for the last reset.
get router info bgp neighbors <IP of the neighbor> advertised-routes	Show all routes advertised by us to the specific neighbor.
get router info bgp neighbors <IP of the neighbor> routes	Show all routes learned from this BGP peer. It shows routes AFTER filtering on local peer, if any.
get router info bgp neighbors <IP of the neighbor> received-routes	Show all received routes from the neighbor BEFORE any local filtering is being applied. It only works if `set soft-reconfiguration enable` is set for this peer under `router bgp` configuration.
diagnose sys tcpsock | grep 179	List all incoming/outgoing TCP port 179 sessions for BGP.