

# 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**.

## NOTE

All debug will run for 30 minutes by default, to increase use **diagnose debug duration <minutes>**, setting to 0 means unlimited by time. Reboot will reset this setting.

## General Health, CPU, and Memory

Table 1. General Health, CPU, and Memory loads

Command	Description
<b>get sys stat</b>	Get statistics about the Fortigate device: FortiOS used, license status, Operation mode, VDOMs configured, last update dates for AntiVirus, IPS, Application Control databases.
<b>get sys performance stat</b>	Show real-time operational statistics: CPU load per CPU, memory usage, average network/session, uptime.

## IPSEC VPN debug

Table 2. IPSEC VPN Debug

Command	Description
<b>diagnose vpn ike log-filter &lt;parameter&gt;</b>	<p>Filter VPN debug messages using various parameters:</p> <ul style="list-style-type: none"> <li>• <b>list</b> Display the current filter.</li> <li>• <b>clear</b> Erase the current filter.</li> <li>• <b>name</b> Phase1 name to filter by.</li> <li>• <b>src-addr4/src-addr6</b> IPv4/IPv6 source address range to filter by.</li> <li>• <b>dst-addr4/dst-addr6</b> IPv4/IPv6 destination address range to filter by.</li> <li>• <b>src-port</b> Source port range</li> <li>• <b>dst-port</b> Destination port range</li> <li>• <b>vd</b> Index of virtual domain. -1 matches all.</li> <li>• <b>interface</b> Interface that IKE connection is negotiated over.</li> <li>• <b>negate</b> Negate the specified filter parameter.</li> </ul>
<b>diagnose debug application ike -1</b>	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.
<b>diagnose vpn ike gateway flush name &lt;vpn_name&gt;</b>	Flush (delete) all SAs of the given VPN peer only. Identify the peer by its Phase 1 name.
<b>get vpn ipsec tunnel details</b>	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.
<b>get vpn ipsec stats tunnel</b>	Short general statistics about tunnels: number, kind, number of selectors, state
<b>get vpn ipsec tunnel summary</b>	Short statistics per each tunnel: number of selectors up/down, number of packets Rx/Tx.
<b>get vpn ipsec stats crypto</b>	Statistics of the crypto component (ASIC/software) of the Fortigate: encryption algorithm, hashing algorithm.

## Static Routing Debug

Table 3. Static and Policy Based Routing debug & diagnostics

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

## Interfaces

Table 4. Interafces of all kinds diagnostics

Command	Description
<b>get hardware nic &lt;interface name&gt;</b>	Hardware info of the interface: MAC address, state (up/down), duplex (full, half), Rx/Tx packets, drops.
<b>diagnose hardware deviceinfo nic &lt;nic name&gt;</b>	Same as above.
<b>get hardware npu np6 port-list</b>	Show on which interfaces the NPU offloading is enabled
<b>diagnose npu np6lite port-list</b>	Same as above but for NP6-lite
<b>fnsysctl ifconfig &lt;interface name&gt;</b>	Gives the same info as Linux <b>ifconfig</b>
<b>diagnose ip address list</b>	Show IP addresses configured on all the Fortigate interfaces
<b>diag debug application pppoe -1</b>  <b>dia debug application pppoe -1</b>  <b>dia debug applicaiton ppp -1</b>	Enable all ADSL-related debug
<b>execute interface pppoe-reconnect</b>	Force ADSL re-connection

## NTP debug

Table 5. NTP daemon diagnostics and debug

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

## SNMP daemon debug

Table 6. SNMP daemon debug

Command	Description
<b>diagnose debug application snmpd -1</b>	ENable SNMP daemon messages debug
<b>show system snmp community</b>	Show SNMP community and allowed hosts configuration

# BGP

Table 7. BGP debug

Command	Description
<b>diagnose ip router bgp level info</b> <b>diagnose ip router bgp all enable</b>	Set BGP debug level to INFO (the default is ERROR which gives very little info) and enable the BGP debug.
<b>exec router clear bgp all</b>	Disconnect all BGP peering sessions and clear BGP routes in BGP table and RIB. Use with care, involves downtime.
<b>get router info bgp summary</b>	State of BGP peering sessions with peers, one per line.
<b>get router info bgp network &lt;prefix&gt;</b>	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. <code>get router info bgp network 0.0.0.0/0</code> . The <prefix> is optional, if absent shows the whole BGP table.
<b>get router info routing-table bgp</b>	Show BGP routes actually installed in the RIB.
<b>get router info bgp neighbors</b>	Detailed info on BGP peers: BGP version, state, supported capabilities, how many hops away, reason for the last reset.
<b>get router info bgp neighbors &lt;IP of the neighbor&gt; advertised-routes</b>	Show all routes advertised by us to the specific neighbor.
<b>get router info bgp neighbors &lt;IP of the neighbor&gt; routes</b>	Show all routes learned from this BGP peer. It shows routes AFTER filtering on local peer, if any.
<b>get router info bgp neighbors &lt;IP of the neighbor&gt; received-routes</b>	Show all received routes from the neighbor BEFORE any local filtering is being applied. It only works if <code>set soft-reconfiguration enable</code> is set for this peer under <code>router bgp</code> configuration.
<b>diagnose sys tcpsock   grep 179</b>	List all incoming/outgoing TCP port 179 sessions for BGP.