# 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. |

## Security rulebase debug (diagnose debug flow)

*Table 1. Security rulebase diagnostics with* `diagnose debug flow`

| Command | Description |
|---|---|
| **diagnose debug flow filter** | Show the active filter for the flow debug |
| **diagnose debug filter clear** | Remove any filtering of the debug output set |

| Command | Description |
| --- | --- |
| **diagnose debug flow filter <filtering param>** | Set filter for security rulebase processing packets output. You can set multiple filters - act as AND, by issuing this command multiple times. Parameters:<br><br>`vd` - id number of the vdom. When entering the vdom with `edit vdom`, this number is shown first.<br><br>`vd-name`<br><br>`proto` - Protocol number.<br><br>`addr` - IP address of the packet(s), be it a destination or/and a source.<br><br>`saddr` - IP source address of the packet(s).<br><br>`daddr` - IP destination address of the packet(s).<br><br>`port` - Source or/and destination port in the packet(s).<br><br>`sport` - Source port of the packet(s).<br><br>`dport` - Destination port of the packet(s).<br><br>`negate <parameter>` - negate the match, i.e. match if a packet does NOT contain `<parameter`. Where `parameter` is one of the above: `vd`, `addr`, `saddr`, `port`, `sport`, `dport` |
| **diagnose debug filter6 <parameter>** | Same as `diagnose debug filter` but for IPv6 packets. The rest of matching and conditions remain of the same syntax. |
| **diagnose debug flow show function-name enable** | Some |
| **diagnose debug flow trace start [number]** | Actually start the debug with optional `number` to limit number of packets traced. |

# General Health, CPU, and Memory

*Table 2. General Health, CPU, and Memory loads*

| Command | Description |
| --- | --- |
| **get sys stat** | Get statistics about the FOrtigate device: FortiOS used, license status, Operation mode, VDOMs configured, last update dates for AntiVirus, IPS, Application Control databases. |
| **get sys performance stat** | Show real-time operational statistics: CPU load per CPU, memory usage, average network/session, uptime. |
| **diagnose debug crashlog read** | Display crash log. Records all daemons crashes and restarts. Some daemons are more critical than others. |
| **diagnose debug crashlog clear** | Clear the crash log. |
| **get hardware memory** | Show memory statistics: free, cached, swap, shared |

# IPSEC VPN debug

*Table 3. IPSEC VPN Debug*

| Command | Description |
| --- | --- |
| **diagnose vpn ike log-filter <parameter>** | Filter VPN debug messages using various parameters:<br>• `list` Display the current filter.<br>• `clear` Erase the current filter.<br>• `name` Phase1 name to filter by.<br>• `src-addr4`/`src-addr6` IPv4/IPv6 source address range to filter by.<br>• `dst-addr4`/`dst-addr6` IPv4/IPv6 destination address range to filter by.<br>• `src-port` Source port range<br>• `dst-port` Destination port range<br>• `vd` Index of virtual domain. -1 matches all.<br>• `interface` Interface that IKE connection is negotiated over.<br>• `negate` Negate the specified filter parameter. |

| Command | Description |
| --- | --- |
| **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. |
| **diagnose vpn tunnel list [name <Phase1 name>]** | Show operational parameters for all or just specific tunnels: Type (dynamic dial up or static), packets/bytes passed, NAT traversal state, Quick Mode selectors/Proxy Ids, mtu, algorithms used, whether NPU-offloaded or not, lifetime, DPD state. |
| **diagnose vpn ike gateway list** | Show each tunnel details, including user for XAuth dial-up connection. |
| **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** | Crypto stats per component (ASIC/software) of the Fortigate: encryption algorithm, hashing algorithm. Useful to see if unwanted situation of software encryption/decryption occurs. |

# Static Routing Debug

*Table 4. 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.<br><br>`tab` Table number, either 254 for unicast or 255 for multicast.<br><br>`vf` Virtual domain index, if no VDOMs are enabled will be 0.<br><br>`type` 0 - unspecific, 1 - unicast, 2 - local , 3 - broadcast, 4 - anycast , 5 - multicast, 6 - blackhole, 7 - unreachable , 8 - prohibited.<br><br>`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<br><br>`prio` priority of the route, lower is better.<br><br>`pref` preferred next hop for this route.<br><br>`Gwy` the address of the gateway this route will use<br><br>`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. |

# Interfaces

*Table 5. Interafces of all kinds diagnostics*

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

# NTP debug

*Table 6. 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. |

# SNMP daemon debug

*Table 7. SNMP daemon debug*

| Command | Description |
| --- | --- |
| **diagnose debug application snmpd -1** | ENable SNMP daemon messages debug. |
| **show system snmp community** | Show SNMP community and allowed hosts configuration |

# BGP

*Table 8. BGP debug*

| Command | Description |
|---|---|
| **diagnose ip router bgp level info**<br><br>**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. |

# Admin sessions

*Table 9. Admin sessions management*

| Command | Description |
|---|---|
| **get sys info admin status** | List logged in administrators showing `INDEX` value for each session |

| Command | Description |
| --- | --- |
| **execute disconnect-admin-session <INDEX>** | Disconnect logged in administrator by the session INDEX. |

# Authentication

*Table 10. Authentication in all kinds LDAP, Radius, FSSO*

| Command | Description |
| --- | --- |
| **diagnose test authserver ldap <LDAP server name in FG> <username> <password>** | Test user authenticaiton on Fortigate CLI against Active Directory via LDAP. E.g. test user `Tara Addison` against LDAP server configured in Fortigate as `LDAP-full-tree` having password `secret`: `diagnose test authserver ldap LDAP-full-tree "Tara Addison" secret`. |