

# 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.

## IPSEC VPN debug

Table 1. IPSEC VPN Debug

Command	Description
<b>diagnose vpn ike log-filter &lt;parameter&gt;</b>	Filter VPN debug messages using various parameters: <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.
<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.
<b>get vpn ipsec stats tunnel</b>	Short general statistics about tunnels: number, kind, number of selectors, state

Command	Description
<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.