Fortigate SD-WAN debug and verification commands cheat sheet

Yuri Slobodyanyuk, https://yurisk.info

SD-WAN verification and debug

Command	Description
diagnose sys sdwan health-check (6.4 and newer) **diagnose sys virtual-link health-check** (5.6 up to 6.4)	Show state of all the health checks/probes. Successful probes are marked `alive`, failed probes are marked `dead`. Also displays `packet-loss, latency, jitter` for each probe.
diagnose sys sdwan member (6.4 and newer) **diagnose sys virtual-wan-link member**	Show list of SD-WAN zone/interface members. Also gives each interface gateway IP (if was set, 0.0.0.0 if not), `priority`, and `weight` both by default equal `0`, used with some SLA Types.
diagnose sys sdwan service (6.4 and newer) **diagnose sys virtual-wan-link service**	List configured SD-WAN rules (aka `services`), except the Implied one which is always present and cannot be disabled, but is editable for the default load balancing method used. Shows member interfaces and their status `alive` or `dead` for this rule.
diag sys sdwan intf-sla-log <interface name> (6.4 and newer) **diag sys virtual-wan-link intf-sla-log <interface name>**	Print log of <interface name> usage for the last 10 minutes. The statistics shown in bps: `inbandwidth`, `outbandwidth`, `bibandwidth`, `tx bytes`, `rx bytes`.
diag netlink interface clear <interface name>	Clear traffic statistics on the given interface, this resets statistics of the SD-WAN Monitor GUI widget for this interface as well. Needed, if, for example, you changed SD-WAN rules, but not sure if it's already active. E.g. `diag netlink interface clear port1`.

Command	Description
diagnose firewall proute list	List ALL Policy Based Routes (PBR). SD-WAN in Fortigate, after all, is implemented as a variation of PBR. This command lists manual (classic) PBR rules, along with SD-WAN created via SD-WAN rules. **Important**: Manually created PBR rules (via `Network → Policy Routes` or on CLI `config route policy`) always have preference over the SD-WAN rules, and this command will show them higher up.
diagnose debug flow filter **diagnose debug flow filter <filtering param>** **diagnose debug flow show function-name enable** **diagnose debug flow trace start [number]** **diagnose debug enable**	Use `diagnose debug flow` to see how the traffic is being routed via SD-WAN. Look for something like `Match policy routing id=2131951617: to 10.10.10.13 via ifindex-3` and `out port1 vwl_zone_id 2, state2 0x1,` here `id=2131951617` is SD-WAN PBR rule as seen in `diagnose firewall proute list` and `vwl_zone_id 2` is the SD-WAN zone in alist of virtual-links.