

ADVPN:

ADVPN (**Auto Discovery VPN**) is an IPsec technology that allows a traditional hub-and-spoke VPN's spokes to establish dynamic, on-demand, direct tunnels between each other to avoid routing through the topology's hub device. The primary advantage is that it provides full meshing capabilities to a standard hub-and-spoke topology. This greatly reduces the provisioning effort for full Spoke-to-Spoke low delay reachability, and addresses the scalability issues associated with very large fully meshed VPN networks.

ADVPN is a Fortinet proprietary solution based on IKE and IPsec that addresses the need for direct spoke-to-spoke communication in Hub-and-Spoke topologies by enabling the spokes to automatically negotiate on-demand IPsec tunnels—called **shortcuts**—between them without you having to make topology changes or make many configuration changes. After a shortcut is established and routing has converged, Spoke-to-Spoke traffic no longer needs to flow through the hub. It is incompatible with Cisco DMVPN which relies on mGRE-over-IPsec and NHRP. Both IPv4 IPsec & IPv6 IPsec are supported. BGP OSPF, and RIPv2/RIPng are supported.

The most important thing here to understand is that the Hub sees the network as point-to-multipoint (Hub has one IPsec tunnel to each Spoke) and each Spoke sees the network as point-to-point (Spoke has IPsec tunnel only to the Hub). To run Dynamic Routing Protocols over those IPsec tunnels, both Hub and Spoke must find a way to tell each other what are their respective tunnel IP addresses. FortiGate overcomes this limitation by using proprietary address exchanging mechanism during IPsec phase-1 negotiation (set exchange-interface-ip enable).

