Design Concern	GRE	Mgre	IPSEC	DMVPN	GETVPN
Scalability	Not scalable. Point to point technology	Scalable,one tunnel interface for multiple tunnel endpoint	Not scalable,point to point technology	Scalable for routing but not scalable for IPSEC. DMVPN is used with IPSEC in general	Very scalable technology
Working on Full Mesh topology	It works but not scalable if there are too many devices to connect	It works very well on full mesh topology	It works but not scalable if there are too many devices to connect	Permanent hub and spoke tunnels and on demand spoke to spoke tunnels, it works but limited scalability	It works perfectly if the underlying routing architecture is full mesh topology, GET VPN needs underlay routing protocol
Working on Hub and Spoke	Yes, it is suitable on Hub and Spoke	Yes works well	It works but require too much processing power on the Hub site	It woks but require too much processing power on the Hub site from the IPSEC point of view, for the routing works very well	Works very well
Suitable on private WAN	Yes	Yes	Yes	Yes	Yes
Suitable over Public Internet	Yes	Yes	Yes	Yes	No. GETVPN cannot run over Public Internet because of IP header preservation
End point discovery	Tunnel Source and Destination needs to be manually defined	Tunnel destination is not specified manually,it is automatic	Manual configuration	To setup the Mgre tunnels uses underlay routing, for the private address discovery uses NHRP (Next hop Resolution Protocol)	It uses underlay routing to create VPN, there is no overlay tunnels
Tunnel Requirement	Yes,Point to Point tunnel is required	Yes tunnel is required	Yes tunnel is required	Yes, it uses Mgre(Multi Point GRE) tunnels to create overlays	It is tunnelles VPN, uses underlaying routing to encrypt the data between endpoints
Standard Protocol	Yes	Yes	Yes	No,Cisco proprietary	No,Cisco proprietary but Juniper also supports the same idea with Group VPN feature
Stuff Experince	Very well known	Well known	Very well known	Not well known	Not well known
Overlay Routing Protocol Support	Can run over all routing protocols	Can run over all routing protocols	Can run over all routing protocols	Except IS-IS other routing protocols are supported, IS-IS runs on top of Layer 2 but only IP protocols can run over DMVPN	It is tunnelles VPN so routing protocols cannot run on top of GETVPN but it requires underlaying routing protocols to setup the communication
Required Protocols	GRE tunnel and IP reachability between end points	Multipoint GRE tunnel and IP reachability between end points	IP reachability between end points,IKE and ESP	NHRP and Mgre	GDOI and ESP
QoS Support	Very well.Flexible QoS	Well	Supports with TOS byte preservation	Good, can support per tunnel QoS which uses shaping on the DMVPN Hub to protect capacity and SLA	Good, it uses underlaying network's QoS architecture,in addtion to queueing,shaping at the GET VPN Group Members to protect SLA is enabled
Multicast Support	Yes	Yes	No	Multicast over the tunnel is handled at the DMVPN Hub. Hub replicates multicast traffic which is not efficiend	Native multicast support.Multicast replication is done in the network, doesn't need Hub device to replicate. Multicast MDTs (Source , Shared) are used in the traditional way, so multicast handling of GETVPN is much better than DMVPN
Security	No	No	Yes,point to point IPSEC Sas	Point to Point IPSEC SA	Multipoint to Multipoint IPSEC SA
Resource Requirement	More	Less	More	More	Less
IPv6 Support	Yes	Yes	Yes	Yes,it can be setup over IPv6 transport or it can carry IPv6 payload. So IPv6 over DMVPN and DMVPN over IPv6 both are possible	Yes
Default Convergence	Slow	Slow	Slow	Slow	Fast
Can run over other VPN ?	Yes	Yes	Yes	DMVPN is already tunneled VPN technology so only routing is enough, it doesn't make sense to run tunnel over tunnel	GETVPN can run over DMVPN since GETVPN is tunnelless technology, use case of GETVPN over DMVPN is to carry private addressing over Internet. Most common use case of GETVPN is over MPLS VPN or VPLS since both VPN technologies are full mesh by default and GET VPN provides very good scalability for encryption