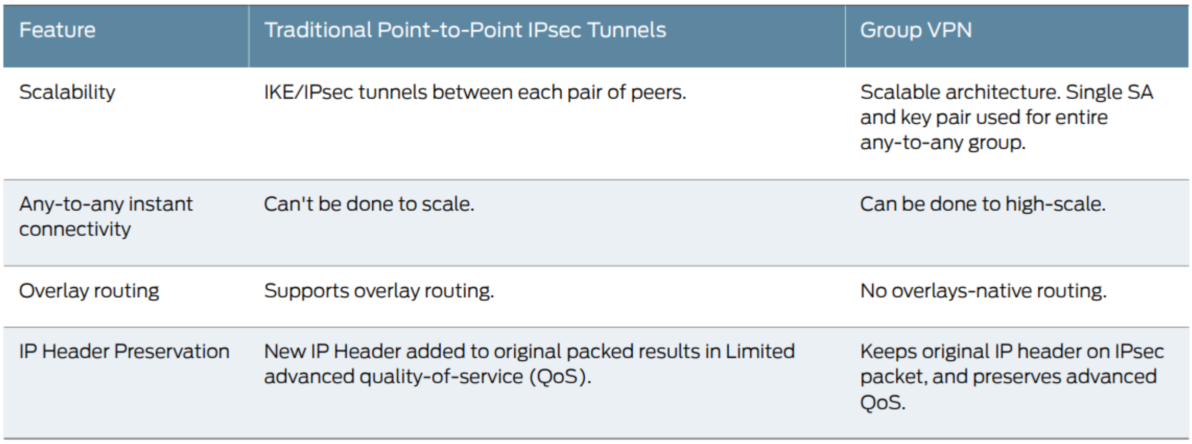
Multi Group VPN with vertical Management

As we have shown in the slide presentation that we propose a method “Group VPN with GDOI), so we would like to give a little more detail about this protocol. However, we are going to start with the comparison of Group VPN to Traditional Point-to-Point IPSec as below



Feature	Traditional Point-to-Point IPsec Tunnels	Group VPN
Scalability	IKE/IPsec tunnels between each pair of peers.	Scalable architecture. Single SA and key pair used for entire any-to-any group.
Any-to-any instant connectivity	Can't be done to scale.	Can be done to high-scale.
Overlay routing	Supports overlay routing.	No overlays-native routing.
IP Header Preservation	New IP Header added to original packed results in Limited advanced quality-of-service (QoS).	Keeps original IP header on IPsec packet, and preserves advanced QoS.

Table 1: Group VPN vs Traditional Point-to-Point IPSec

Group VPN is similar to multicast group that can be joined by member with same multicast IP. And only single SA and key pair is used for the entire any-to-any VPN group while Traditional Point-to-Point IPSec requires encrypted key for each peer. And we use GDOI for generating the key pair.

[1] The GDOI (Group Domain of Interpretation) distributes security association (SAs) for IPsec Authentication Hader (AH) [RFC4302] and Encapsulating security protocols used in group applications. [2] GDOI introduces two different encryption keys:

- Key encryption key (KEK) is used to secure the control plan and is used by the group member to decrypt rekey message from the GC/KS.
- Traffic Encryption Key (TEK) is used to secure data plan and is used by the group member to encrypt or decrypt communication between them.

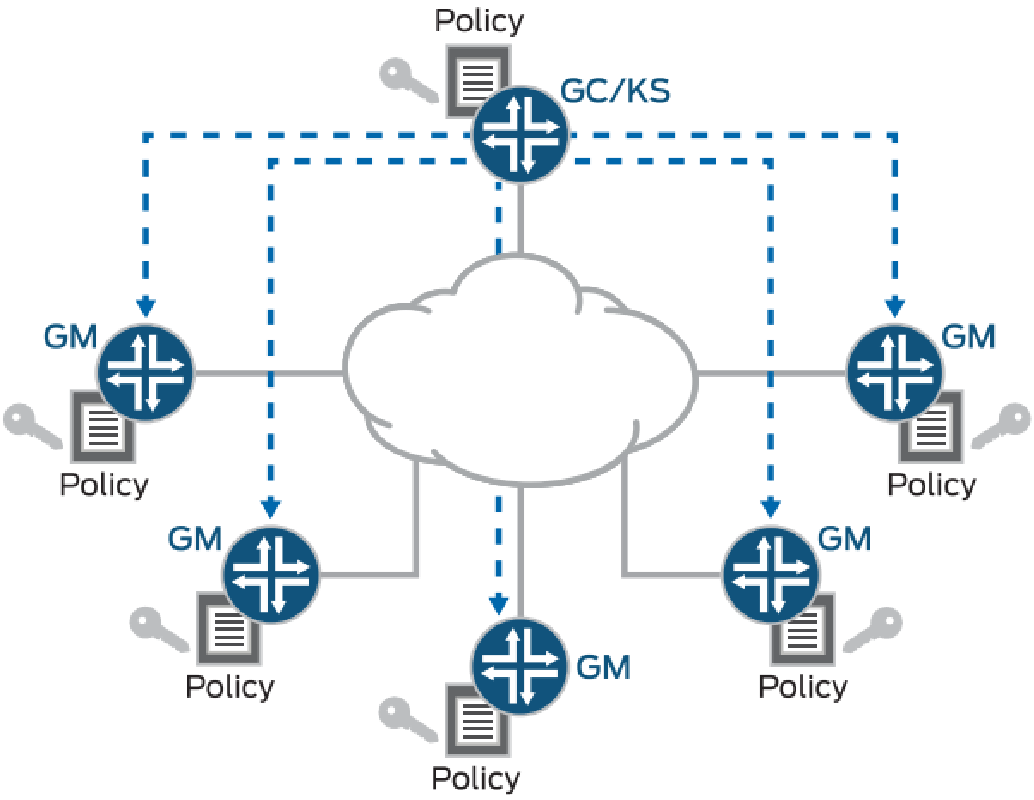


Figure 1: Group VPN Using GDOI

GC/KS (Group Controller / Key Server) - functions as policy and key distributor which controls encryption protocol, security association, rekey timer and so on.

GSA (Group Security Association) – shared GSA and encryption policy is used by all members in the group VPN group for communication.

GM (Group Member) – is used for the traffic encryption process and is responsible for the actual encryption and decryption of data traffic.

References:

[1] Weis. B, Rowles .S & Hardjono .T (2011), The group Domain of Interpretation, 3-4

[2] Juniper Networks (2017), Configuration Group VPN on Routing Devices, 5-12