Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Home > Advisory services > Multi-site Connectivity Advisory Service > Technical guides > Different flavours of VPN: technology and applications > Appendix 2: Table of VPN-enabling technologies

Appendix 2: Table of VPN-enabling technologies

Technology	Provisioned by	Security	Private user address space	Independent transport technology for end user sites	Improved performance (guaranteed bandwidth, limits for delays and loss)	Multi-domain capability
Encrypted VPN (IPSec or SSL based secure channels) Two versions: - remote access, when a user accesses the central site of an organisation - site-to-site, when sites of an organisation connected to each other create a mesh.	Mostly: IT Support staff of an organisation. Quite rare: by a provider who manages VPN gateways on the central site and VPN software clients on remote PCs.	Confidentiality – excellent as all fields of packet can be encrypted. protection of end site – good as only VPN end-point need have an Internet-routable address.	Yes	In practice, no, as the two currently popular technologies – IPSec and SSL – are IP-oriented.	QoS Yes, as security tunnels are transparent for providers. neutral	In practice probably not, but there is an ongoing activity in IETF.

GRE or L2TP tunnels-based VPN	Users and providers	Confidentiality – encryption can be added on top of tunnels. Protection of end site – moderate: only the paired endpoint can insert traffic into the tunnel.	Yes	Yes, packets/ frames of different technologies – ‘passengers’ could be encapsulated in IP.	QoS neutral	Yes, as tunnels are transparent for intermediate providers.
Policy-based routing VPN (no tunnelling)	Providers	Confidentiality – no. Protection of end site – possible if policy only permits traffic from other trusted sites.	No	No	Possible stronger basis for QoS as control over flows is tighter than for a plain IP network.	Yes

MPLS VPN (layer 2 or 3)	Providers	Confidentiality – moderate: traffic is protected by separation due to using different LSPs; independent tests have showed good degree of protection. Protection of end site – possible if the site only accepts MPLS tagged traffic (as for (3)).	Yes	Yes	Advanced support for guaranteed QoS if provider supports MPLS-based traffic engineering.	Not widespread, but some providers have started to do this.
SDH and DWDM private optical networks	Providers and customers (through software like UCLP from CANARIE)	Confidentiality – good (network provider may be able to read traffic unless additional encryption is used). Protection of end site – excellent.	Yes	Yes, including non-standard physical coding of optical signals.	Yes: excellent performance is provided natively as it is circuit-switched technology which guarantees bandwidth per user.	Unknown

None of the technologies listed in the table improves performance natively. However this can be done by deploying QoS across networks. For example, if IP QoS is implemented over the whole path of the L2TP tunnel it can give some guarantee of performance/bandwidth to tunnelled traffic. However, some of the VPN-enabling technologies can be called QoS supportive as they have functionality which can simplify QoS deployment or strengthen QoS guarantees. Other VPN-enabling technologies are QoS neutral as they have no additional functionality which QoS can exploit and benefit from; their traffic looks like standard IP traffic. Of course, both QoS supportive and QoS neutral VPN-enabling technologies can benefit from QoS if it is deployed across a network but in the case of QoS supportive technology the level of QoS guarantees tends to be higher and QoS deployment tends to be simpler. There are some VPN-enabling technologies which have built-in QoS functionality, e.g. ATM and some versions of Frame Relay, but they are rather in decline and not in widespread use within Janet.

Source URL: https://community-stg.jisc.ac.uk/library/advisory-services/appendix-2-table-vpn-enabling-technologies