

# Competitive Analysis: G/On vs. VPN

This table highlights differences between G/On and the two main types of VPN on the market. Please allow for the fact that comparing one specific product to two technologies cannot take into account

specific features of specific VPNs. More detailed information on G/On's unique architecture is described in the White Paper "Secure by Design" or visit [www.giritech.com](http://www.giritech.com).

	IPSec VPN	SSL VPN	G/On
<b>Required user rights</b>			
<ul style="list-style-type: none"> <li>for installation</li> <li>for execution</li> </ul>	Admin User	User + rights for plugins User	Guest Guest
<b>Authentication</b>			
<ul style="list-style-type: none"> <li>Hardware authentication</li> <li>User authentication</li> <li>"Trusted" PC required?</li> </ul>	3rd party Yes Yes	3rd party Yes No, but advisable for plugins & cache	Built-in Yes No
<ul style="list-style-type: none"> <li>Mutual client/server authentication to prevent phishing</li> </ul>	Yes, using a pre-shared secret	Yes, using certificates	Yes, using true mutual authentication
<b>Access Security</b>			
<ul style="list-style-type: none"> <li>Authorization</li> <li>Security Zones</li> <li>Active Directory connection</li> <li>Own user management</li> <li>End-point information (useable data in cache e.g. passwords)</li> <li>Data encryption</li> </ul>	3rd party No Vendor-specific Vendor-specific Yes	3rd party No Vendor-specific Vendor-specific Yes	Built-in Yes Built-in Built-in No
<ul style="list-style-type: none"> <li>Protection against "man-in-the-middle" and replay attacks?</li> </ul>	Yes, if pre-shared key is well protected	Yes, if certificate is well-protected	Yes, using checksums and timestamps attached to each packet
<ul style="list-style-type: none"> <li>Tunneling protocols used</li> </ul>	L2TP, P2PP and others (vendor specific)	L2TP, P2PP and others (vendor specific)	None
<b>Securing of devices</b>			
<ul style="list-style-type: none"> <li>Antivirus</li> <li>Firewall</li> <li>Client filtering</li> </ul>	Required Required MAC/IP Address	Required Required MAC/IP Address	Optional Optional Hardware EDC number + more
<ul style="list-style-type: none"> <li>Unsolicited processes / malware-process control</li> <li>Defence against attacks</li> </ul>	3rd party DMZ or application server	3rd party DMZ or application server	Integrated "lock to process" Directly on client side outside of the company
<b>Access Layer</b>			
<ul style="list-style-type: none"> <li>Type of access</li> <li>Member of LAN</li> </ul>	Network layer Yes	Application layer Depends on product and setup	Application layer Nodeless client i.e. PC is not a member of the network.
<ul style="list-style-type: none"> <li>Open ports</li> </ul>	Yes	Yes	Single port connection between G/On client and G/On Server multiplexing of application ports
<b>Administration and management</b>			
	Decentralized management using tools and browser, additional management of 3rd party products and security applications	Decentralized management using tools and browser, additional management of 3rd party products and security applications	Centralized management only via G/On Server
<b>Infrastructure</b>			
	Typically 2-4 different vendors	Typically 2-4 different vendors	One product (all-in-one)