

# IPsec vs. SSL

	Pros	Cons
<b>IPsec</b>	<ul style="list-style-type: none"><li>• Provides an extra layer of security</li><li>• Allows for complete application access at network layer (good for all IP traffic)</li><li>• Standards-based</li></ul>	<ul style="list-style-type: none"><li>• Can be costly to maintain licenses for the client software</li><li>• Some firewalls may interfere with access</li><li>• Less flexible as users are tied to a single machine</li></ul>
<b>SSL</b>	<ul style="list-style-type: none"><li>• Good interoperability</li><li>• Since SSL is a common protocol, most Web browsers have SSL capabilities already built in</li><li>• Lower TCO than IPsec-based VPN</li></ul>	<ul style="list-style-type: none"><li>• Doesn't give users access to network resources (e.g., printers, centralized storage)</li><li>• Users may enter VPN from unknown or untrusted sources</li><li>• Only works with Web-based applications</li></ul>