

Rainer Enders, VPN expert

SearchEnterpriseWAN

Rainer Enders
January 11, 2012

How secure is a PPTP VPN in comparison with other types of VPNs?

[Point-to-Point Tunneling Protocol](#) (PPTP) is a VPN technology that was specified by a group of system vendors intended to promote easy VPN deployments. It exists in multiple implementations, which are vendor specific, such as Microsoft PPTP. The most commonly-used underlying mechanisms for authentication and encryption have been found highly vulnerable. Even after many attempts to fix issues in the [PPTP security hole](#), it can be stated that the mechanisms for authentication and encryption used in PPTP still exhibit major vulnerabilities and are not state-of-the-art. I recommend not deploying PPTP as a VPN solution and argue to deprecate this protocol. The only somewhat safe way of deploying PPTP would be by using [Transport Layer Security](#) (TLS), which requires the implementation of an entire [PKI infrastructure](#), which is why most people stay away from it. But even then, you run into similar security issues that plague SSL VPNs today. The two only serious VPN technologies are [Secure Sockets Layer](#) (SSL) and [Internet Protocol Security](#) (IPsec) VPN. SSL VPN is similar to PPTP in that it is easier to deploy than other [VPN types](#). The strength of IPsec VPN is its transparency over the IP network layer, which works in both versions of IP: IPv4 and IPv6. But its key strength results from the fact that it is an IETF standard, a framework of open standards protocols that support state-of-the-art strong authentication, authorization and encryption schemes and can be implemented in various standards-based ways.

Why am I experiencing issues with VoIP over VPN?

There are many factors that influence [Voice over IP](#) (VoIP). Generally speaking, VoIP is sensitive to packet loss and latency so you need to provide sufficient bandwidth for the number of VoIP connections that you will be using. Also, a good ISP helps. As for your VPN, it depends on the type of VPN technology that you are using. If you use a VPN with your VoIP solution, you must account for extra bandwidth due to packet overhead. I have seen tests that state that [Secure Socket Layer](#) (SSL) VPNs actually improve VoIP quality due to [Transmission Control Protocol](#) (TCP) encapsulation. Besides throwing bandwidth at the problem, treating VoIP traffic with a certain [quality of service](#) (QoS) is recommended and will help your VoIP quality. For

Rainer Enders, VPN expert



Rainer Enders, VPN expert

Rainer Enders is CTO of Americas for NCP engineering, a secure remote access and VPN solution provider. He has 20 years of experience in the networking and security industry. His other areas of expertise are test automation in quality assurance and the testing and verification of complex network and system architectures. Prior to joining NCP in January 2010, Rainer headed his own strategic consulting firm, Rainer Enders Consulting Enterprises, which focused on computer network security and storage networking. Before that, he held a variety of technical roles at Identity Engines, NeoScale Systems, Yipes Enterprise Services and Ericsson.

an [Internet Protocol Security](#) (IPsec) VPN that means the client should be able to identify VoIP traffic and prioritize it accordingly.

Do I need to change the [maximum transmission unit \(MTU\)](#) for the VPN header?

[Internet Protocol Security](#) (IPsec) adds protocol overhead to each packet, which can lead to fragmentation. Fragmented packets then need to be reassembled at the receiving gateway, which can lead to performance degradation. Pre-fragmentation of packets can help keep the packet size at a level where fragmentation is not likely to occur, which aids performance in the network. The protocol overhead depends on the type of encryption that is chosen and can be calculated accordingly.