Abstract

SIP is a multimedia negotiation protocol transmitted in plain text mode thus has issues of security both in terms of credential that consists of extension user and password in the SIP message or media content contained in the RTP payload. SIP VoIP communications unsafe can be secured with VPN implementation, ZRTP and SIP - Secure.

Things to consider in VoIP is the minimum bandwidth requirements in order to produce a satisfactory communication. With the implementation of VPN security protocols, ZRTP and SIP-Secure it will increase the size of transmitted data packets. Bandwidth usage that does not comply with the minimum requirements will result in poor QoS bandwidth capacity to accommodate the resulting data packet overhead. QoS parameters are used in VoIP including delay, jitter and packet loss.

From the test results shown that the assumption of the use of the G.711 codec, both the IPSec/TLS VPN implementation, ZRTP and SIPS give good performance in bandwidth of 128/128. Judging from the safety factor, VPNs provide better overall protection of the credential and media content. While ZRTP only protect media content and SIPS only protect existing credential in the SIP message.

Keyword: *SIP, VPN, TLS, IPSec, ZRTP, bandwidth, QoS, TCP, UDP*