

Scalable and Secure Peer-to-Peer Systems with Support for QoS

Jayant Shukla
Trlok, Inc.

jshukla@trlok.com

Abstract

Secure communication architecture is client-server based and not peer-to-peer based. NATs and firewalls tamper with or inspect data packets and that runs afoul with security protocols, such as IPSec and SSL/TLS. Client-server based architecture is not suitable for very high data rates when the server becomes a bottleneck in the communication. This architecture is not scalable and a single point of failure also makes it less reliable. Today's dominant security protocol, IPSec, is incompatible with NAT in any mode. Several attempts have been made to make IPSec compatible with other networking protocols, but the success has been limited. Imparting peer-to-peer capabilities to IPSec also makes support for QoS difficult and extensions to existing QoS protocols may be required. Even with these extensions, layer-7 switching cannot be supported with IPSec. Layer-7 switching is evolving as the dominant method for QoS provisioning by the web servers. Clearly, a better solution for security is needed.

We developed a new peer-to-peer communication protocol called NGISec that solves all the problems associated with client-server based secure communication system. Similar to client-server based architecture, there is a mechanism for centralized control and policy enforcement, but the compute intensive tasks are offloaded to the end-host. Therefore the system is more robust and scalable.

Another nice feature of NGISec is that it is compatible with all QoS protocols, something that is not true for the existing protocols such as IPSec or SSL/TLS. NGISec may have application in mobile IP as well.

We present a solution for peer-to-peer secure communication that supports IS/DS based QoS as well as layer-7 switching. This is the first secure communication protocol that is scalable and at the same time solves the incompatibility problems of security protocols with other networking protocols, such as, NAT, ICMP, RED, etc.