Performance and Overhead Analysis of Security Mechanisms in Virtual Private Networks

Daniel R. Garcia, Otto Carlos M. B. Duarte
Universidade Federal do Rio de Janeiro - GTA/COPPE - Rio de Janeiro, Brazil

Abstract—**Future Internet Testbed with Security (FITS) project creates a colaborative experimental facility for future Internet research built on network and machine virtualization tecnology. The testing environment is geographically distributed, with the collaboration of Brazilian and European institutions, it utilizes virtualization to provide a realistic condition environment with isolated connections and secure access for experimenting new Internet proposals. Cryptographic algorithms guarantee virtual network isolation, securing communication in the presence of third parties. This paper analyzes processing time, throughput and delay of different cryptographic ciphers deployed in FITS Virtual Private Networks.**

I. Introduction

With the popularization of the Internet, the number of users has increased and also the necessity of security, mobility and Quality of Service (QoS). Nevertheless the current Internet is not able to cope with the requirements of existing and new applications. Furthermore, it is very difficult, if at all possible, to deploy new mechanisms in the core of the Internet. As consequence, a new Internet is required. Future Internet Testbed with Security (FITS) [1], an experimentation environment based on virtual networks that offers network isolation, secure access, and quality of service differentiation.

FITS is based on virtualization tools Xen and OpenFlow [2] and it makes possible to create multiple virtual networks in parallel. FITS nodes act as physical substrate for virtual network formation and uses Generic Routing Encapsulation (GRE) tunnels and Virtual Private Networks (VPNs) to create connections between islands.

VPN is a secure and reliable way to share information across the Internet. The use of VPN makes possible to establish a private network connection across a public network, it povides authentication, integrity and, with cryptographic algorithms as Security Mechanism, isolates the network access, preventing eavesdropping and spoofing.

The tests presented in this paper aims to identify which is the most efficient cryptographic algorithm to be applied in FITS Virtual Private Networks and if the use of data compression is a better option.

II. OpenVPN

OpenVPN is an open source software, used in FITS, that creates VPN connections using Authentication and Encryption:

Authentication: OpenVPN offers two ways to authenticate peers: Static Key; and TLS (Transport Layer Security).

In the Static Key authentication, a pre-shared key is generated and shared between peers before connection. This is the simplest setup, and is ideal for point-to-point VPNs. TLS authentication uses certificates, for both sides, and RSA key exchange to establish connection and is also possible add usernames and passwords for peers.

Encryption: OpenVPN uses the OpenSSL (Secure Socket Layer) library for encryption. OpenSSL is an open-source implementation of the SSL and TLS protocols.

The ciphers can be used in two cases: With data compression; and without data compression. For each supported cipher, there are three modes of operation supported in openVPN: CBC (cipher-Block Chaining), CFB (Cipher Feedback) and OFB (Output Feedback).

III. Implementation

The tests were made with the purpose of analyze the performance of Virtual Private Networks when applied different cryptographic algorithms in its configuration.

To produce the tests, for each supported cipher, one VPN was created using data compression and other without data compression. Individually, in these connections, were measured the delay, processing time and throughput. Also, as a better case scenario, a VPN without encryption was tested for comparison.

For the tests, two isolated computers were connected and the softwares used for measuring were: fping, for the delay, and Netperf, for throughput and processing time.

IV. Conclusion and Future Work

Currently the ciphers were only tested in CBC mode of operation, however, the tests showed that even if the delay is greater, use data compression is still better option because of the higher throughput values.

The results of measuring throughput, delay and processing time showed that the AES (Advanced Encryption Standard) was one of the most efficient cryptographic algorithms in the evaluated scenarios.

Acknowledgements

The authors would like to thank by FINEP, FUNTTEL, CNPq, CAPES, FAPERJ and UOL for their financial support.

References

[1] D. M. Mattos, L. H. Mauricio, L. P. Cardoso, I. D. Alvarenga, L. H. G. Ferraz, and O. C. M. Duarte, "Uma rede de testes interuniversitária com técnicas de virtualização híbridas," *XXX Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2012), Ouro Preto, MG, Brazil*, 2012.

[2] D. M. Mattos, L. H. G. Ferraz, L. H. M. Costa, and O. C. Duarte, "Virtual network performance evaluation for future internet architectures," *Journal of Emerging Technologies in Web Intelligence*, vol. 4, no. 4, pp. 304–314, 2012.