Solutions for Network Traffic Security: VPN through IPsec and PKI

Mihai-Alexandru PAULIȘ
EUROQUALROM, University POLITEHNICA of Bucharest, Romania
alexandru.paulis@gmail.com

Abstract

Internet traffic is susceptible to a series of treats and maybe the most important treats are the eavesdroppers. These types of attacks have known a huge increase in numbers but also a huge diversification in time. The scope of this article is to present a solution for this treat. In the first part of the article is presented this solution, VPN, the use and the types of this technology, its security mechanisms and some protocols that implement this solution. In the second part is presented the most used and reliable protocol that is used to ensure VPN, IPsec, and how IPsec ensures security. In the third part is presented the encryption process. In the last part is presented PKI and how its implementation assures the security mechanisms.

Index terms: VPN, IPsec, cryptography, PKI

References:

[1]. http://en.wikipedia.org/wiki/Virtual_private_network
[2]. Mason, Andrew G., Cisco Secure Virtual Private Network, 2002.
[3]. Network-based VPNs – Generic architecture and service requirements, ITU-T recommendation.
[4]. http://hacked-key.blogspot.ro/2013/06/free-vpn-list.html
[5]. http://what-when-how.com/ipv6-for-enterprise-networks/transition-mechanisms-ipv6-part-2/
[6]. http://blog.tuvpn.com/2011/08/typical-vpn-openvpn-l2tpipsec-pptp-sstp-vs-ssh2-tunnels-vs-high-anonymity-web-proxies/
[7]. http://en.wikipedia.org/wiki/IPsec
[8]. RFC 4301, Security Architecture for the Internet Protocol, IETF Standard.
[9]. RFC 2437, RSA Cryptography Specifications, IETF Standard.
[10]. http://en.wikipedia.org/wiki/Public_key_infrastructure
[11]. http://en.wikipedia.org/wiki/Public_key_certificate
[12]. X.509, Public-key and attribute certificate frameworks, ITU-T recommendation.