VPN 프로토콜에 기반한 네트워크 성능 분석

장창환, 이민석, 조성호, 김정태
목원대학교

Analyses of Network Performance Based on VPN Protocols

Chang-Whan Jang, Min-Suk Lee, Sung-Ho, Jung Tae Kim
Mokwon University
E-mail : jtkim3050@mokwon.ac.kr

Abstract

Virtual Private Network (VPN) is commonly used in business situations to provide secure communication channels over public infrastructure such as Internet. This is important matters because these networks can be set-up with a lower cost of ownership compared to other means of securing communications. VPN is a proven technology that does provide security strong enough for business use. However, performance of these networks is also important in that lowering network and server resources can lower costs and improve user satisfaction. We analyzed network performance analysis of VPN protocols.

Keyword

Security, VPN Gateway, Privacy, WSN

Ⅰ. Introduction

VPN is an end-point technology. This makes VPN an attractive proposition for any organization that uses Public Switch Telephone Network (PSTN) to connect different parts of their private network. To implement VPN, there are numerous protocols and products available on the market, each having its own capabilities and features. Three protocols that are frequently used with operating systems are IPSec, PPTP and SSL. These provide encryption and integrity to data in transition. Each of these VPN protocols can be implemented with different algorithms. Data Encryption Standards (DES, 3DES) and Blowfish algorithms are used for encryption, while Message-Digest 5 (MD5) and Secure Hash Algorithm (SHA) for integrity [1]. When a client needs to connect to an internal application server, at first, the client should request to create a VPN connection with SSL VPN gateway, and then the VPN peers authenticate each other through their digital certificates and negotiate security parameters. After the VPN peers were authenticated, a SSL VPN tunnel will be created, connecting the client and the SSL VPN gateway. Then the SSL VPN gateway sets up a TCP connect to the internal application server on behalf of the client. Thereafter, the SSL VPN gateway relays data between the client and the internal application server, all data flows of the VPN should be encapsulated or unwrapped at the SSL VPN gateway according to SSL protocol. Inside the LAN, communication data between the SSL VPN gateway and the internal application server can be either in plain text, or protected by additional internal SSL tunnels, it's up to internal security requirement. Compared with IPSec VPN, SSL VPN has some outstanding advantages, like easy-to deploy, fine-grained access control [2].

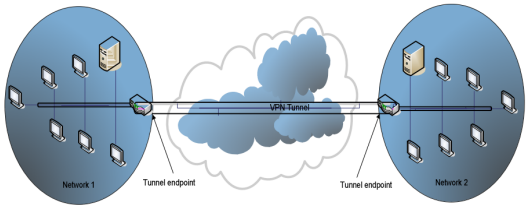

Figure 1. Topology of virtual private network

II. IPSec Architecture

IPSec VPN is used to solve VPN connection between one gateway and another gateway, which function includes access control, confidentiality, integrity checking and original data authentication etc. Compared with IPSec VPN, SSL VPN achieves information remote connection through a simple method. One of the main concerns is security of data when it traverses a public network. In other words, how can we prevent malicious eavesdropping of data in a VPN. Encrypting the data is one way to protect it. Data encryption may be achieved by deploying encryption/decryption devices at each site. IPSec is a suite of protocols developed under the auspices of the IETF to achieve secure services over IP packet-switched networks. The Internet is the most ubiquitous packet-switched public network; therefore, a VPN tunnel deployed over the public Internet can mean significant cost savings to a corporation as compared to a leased-line point to point. Toward this purpose, IPSec services provide authentication, integrity, access control, and confidentiality. It allows the information exchanged between remote sites can be encrypted and verified. Both remote access clients and site-to-site VPNs can be deployed using IPSec [3]. For remote access, SSL VPN is more flexible and easier to deploy while high security level. The user with a PC-installed SSL VPN client can remotely access all policy-permitted and business-required IP applications. With a web-only interface, SSL VPN access to any internal web based applications, including e-mail, calendar, and file services. Finally, for a broader range of application access without a client, an SSL VPN can provide web access to Java applets, providing a very lightweight VPN client. SSL VPN supports strong user-level authentication as well as very granular application level access control through application proxies [4].

The main advantages of SSL VPN are as follows [5]:

- Simple client support and maintenance.
- Enhanced remote secure access features.
- More fine-grained access control.
- The ability to through the NET and firewall.
- Better withstand external virus and Trojan attacks.
- Flexiable network deployment.

III. Conclusion

The advances in the smart objects systems and Internet of Things approach are remarkable developed. To realize this application in industrial field, we surveyed the research status in this field from encryption mechanism, communication security, protecting sensor data, and encryption algorithm.

Acknowledgments. This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2015-071892)

Reference

[1] Shaneel Narayan, Kris Brooking and Simon de Vere, "Network Performance Analysis of VPN Protocols", 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp.645-648

[2]Dingguo Yu,Nan Chen and Chengxiang Tan, "Design and Implementation of Mobile Security Access System (MSAS) Based on SSL VPN", 2009 First International Workshop on Education Technology and Computer Science, 2009, pp.152-155

[3] Abdelmajid Lakbabi, Ghizlane Orhanou and Said EI Hajji, "VPN IPSEC & SSL Technology", 2012 Next Generation Networks and Services, 2012, pp.202-208.

[4] Su Hua Sun, “The Advantages and the Implementation of SSL VPN”, 2011 IEEE, pp.548-551

[5] Zhang Lan, “Application of SSL VPN Technology in Power Utilities Mobile Office,” Telecommunications for Electric Power System, vol. 29, pp. 53-56, Jan 2008.