

# Implementation of a Fault-Tolerant and Load-Balanced Virtual Private Network

陳昆宏、黃培壘

E-mail: 381995@mail.dyu.edu.tw

## ABSTRACT

In recent years, with the mature development of Internet technology, the use of virtual private network (VPN) has become increasingly common. Therefore, this paper implements of a fault-tolerant and load-balanced virtual private network base on PPTP technology. In general, a company or organization only uses one VPN server for VPN connection. In this way, the entire load will be on this VPN server, this VPN server will become the bottleneck of the VPN connection. If the VPN server failed, VPN connections will be unavailable. The proposed method can overcome this problem. The proposed method adopts multiple PPTP VPN server, database, and distribution server architecture. The proposed method also implements a proprietary client program. The client program can be stored on the flash drive. To start VPN connection, the user simply starts the client program and type the user 's account and password. The user does not need to know the VPN password or doing complex settings. The client program gets the PPTP VPN server list, the temporary PPTP VPN account and the password from be distribution server via SSL encrypted HTTP connection. The client program will automatically select the most appropriate PPTP VPN server, and then use the temporary PPTP VPN account and password to establish PPTP VPN connection. Temporary PPTP VPN username and password are generated by the distribution server periodically. And the expired temporary PPTP VPN account and password are cleared, in order to increase security.

Keywords : HTTP Request、VPN、PPTP、SSL

## Table of Contents

封面內頁 簽名頁 中文摘要 iii 英文摘要 iv 誌謝 v 目錄 vi 圖目錄 viii 表目錄 ix 第一章 緒論 1 第二章 相關研究 3 2.1 VPN介紹 3 2.1.1 VPN的優缺點 5 2.2 PPTP協定 6 2.2.1 PPTP控制連接 7 2.2.2 PPTP的優點與缺點 7 2.3 HTTP協定 7 2.4 SSL協定 8 2.4.1 SSL交握協定 10 2.4.2 SSL紀錄協定 15 第三章 具容錯及負載平衡之虛擬私人網路實作 16 3.1 系統架構簡介 16 3.2 系統設計 19 3.2.1 Server端功能設計 19 3.2.2 客戶端功能設計 25 3.3系統介面 27 3.4 實驗結果 29 第四章 結論 35 參考文獻 36

## REFERENCES

- [1] Chengcheng Li , Design and Implement an Interconnected VPN system for Campuses in Multiple Geographical Locations , 2010 2nd International Conference on Education Technology and Computer (ICETC) , 2010.
- [2] Weili Huang、 Fanzheng Kong , The research of VPN on WLAN , 2010 International Conference on Computational and Information Sciences , 2010.
- [3] Yanfei Zhao、 Zhaohai Deng、 A Design of WAN Architecture for Large Enterprise Group Based on MPLS VPN , 2012 International Conference on Computing, Measurement, Control and Sensor Network , 2012.
- [4] Pham Ngoc Thanh、 Keecheon Kim\* , A methodology for implementation and integration Two-Factor Authentication into VPN , 2012 IEEE , 2012.
- [5] Introduction to VPN , [http://www.caconsultant.com/Article/VPN/introduction\\_to\\_vpn.htm](http://www.caconsultant.com/Article/VPN/introduction_to_vpn.htm).
- [6] 精元科技全球資訊網, 解讀VPN優點與缺陷 , [http://www.jing-yuan.com.tw/index.php?option=com\\_content&task=view&id=34](http://www.jing-yuan.com.tw/index.php?option=com_content&task=view&id=34).
- [7] Viscosity , INTRODUCTION TO VPN , <http://www.sparklabs.com/viscosity/introtovpn/>.
- [8] HOME-NETWORK-HELP.com , Virtual Private Network (VPN) Introduction , <http://www.home-network-help.com/virtual-private-network.html>.
- [9] About.com , Introduction to PPTP - Point-to-Point Tunneling Protocol , <http://compnetworking.about.com/od/vpn/l/aa030103a.htm>.
- [10] Hypertext Transfer Protocol -- HTTP/1.1 , <http://www.w3.org/Protocols/rfc2616/rfc2616.html>.
- [11] HttpWatch-Introduction to http , <http://www.httpwatch.com/httpgallery/introduction/>.
- [12] HTTP Introduction and Debugging , <http://www.gmckinney.info/resources/http/>.
- [13] Edgis , Introduction to SSL: 02 The Protocol , <http://edgis-security.org/cryptography-and-protocols/introduction-to-ssl-02-the-protocol/>.
- [14] Introduction to SSL , <http://www.cs.ucla.edu/classes/spring03/cs111/l2/docs/ssl.html>.
- [15] MOZILLA DEVELOPER NETWORK , Introduction to SSL ,

[https://developer.mozilla.org/en-US/docs/Introduction\\_to\\_SSL#The\\_SSL\\_Handshake](https://developer.mozilla.org/en-US/docs/Introduction_to_SSL#The_SSL_Handshake).

[16] codeguru , An Introduction to SSL ,

<http://www.codeguru.com/cpp/i-n/internet/securesocketlayerssl/article.php/c6187/An-Introduction-to-SSL.htm>.

[17] Berners-Lee, T., Fielding, R. and H. Frystyk , Hypertext Transfer Protocol -- HTTP/1.0 , RFC 1945 , May 1996.

[18] Freed, N. and N. Borenstein , Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies , RFC 2045 , November 1996.

[19] Crocker, D., Standard for The Format of ARPA Internet Text Messages , STD 11, RFC 822, August 1982.

[20] Postel, J., Simple Mail Transfer Protocol , STD 10, RFC 821, August 1982.

[21] Kantor, B. and P. Lapsley, Network News Transfer Protocol , RFC 977, February 1986.

[22] Postel, J. and J. Reynolds, File Transfer Protocol , STD 9, RFC 959, October 1985.

[23] Anklesaria, F., McCahill, M., Lindner, P., Johnson, D., Torrey, D. and B. Alberti, The Internet Gopher Protocol (a distributed document search and retrieval protocol) , RFC 1436, March 1993.

[24] Davis, F., Kahle, B., Morris, H., Salem, J., Shen, T., Wang, R., Sui, J., and M. Grinbaum, WAIS Interface Protocol Prototype Functional Specification, (v1.5), Thinking Machines Corporation, April 1990.