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

陳昆宏、黃培壝
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
[15] MOZILLA DEVELOPER NETWORK,Introduction to SSL,


The SSL Handshake


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


