AN IMPLEMENTATION OF A VIRTUAL PRIVATE NETWORK IN LINUX

BY

Dulatre, Cristina Lourdes C.

Estrera, Lionel Harvey G.

Villaflores, Josarie A.

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

MARCH 2003

AN IMPLEMENTATION OF A VIRTUAL PRIVATE NETWORK IN LINUX

An Independent Research
Presented to
The Faculty of the Computer Studies Division
Ateneo de Davao University

In Partial Fulfillment
of the Requirements for the Degree
Bachelor of Science major in Computer Science

by
Dulatre, Cristina Lourdes C.
Estrera, Lionel Harvey G.
Villaflores, Josarie A.

SCHOOL OF ARTS AND SCIENCES
ATENEO DE DAVAO UNIVERSITY

MARCH 2003

TABLE OF CONTENTS

ABSTRACT

The trend of businesses nowadays is cost cutting. The less cost a project would entail, the better for an organization. To keep up with this, there must be a solution to getting cheaper access to an organization's data without sacrificing security, reliability, and efficiency of the system.

Networking provides communication among users along great distances. For two well–known networking schemes, Local Area Networks (LAN) and Wide Area Networks (WAN), the distances of both depend on the invested physical connections made. That is why Virtual Private Networks (VPNs) were created making use of secured tunnels using the Internet, or any other public connection. Clients would then be able to access their organization's systems from locations hundreds of miles away from the main server by using a dial–up connection.

This study will focus on the implementation of a VPN in a Linux system. A VPN prototype will be created to demonstrate the working model. This is done by first researching on the current studies done to attain Virtual Private Networks. This includes the methods of packet travel, security measures implemented and different methods of implementation done. After gathering the data on VPNs the proponents then have to decide on an implementation that will be used as a model for the prototype to be created. Last but not the least is the implementation stage which is the coding and debugging stage of the prototype to ensure it is functioning and reliable enough.

CHAPTER I

INTRODUCTION

1.1 Background of the Study

A Virtual Private Network (VPN) is an ideal way to connect branch offices, telecommuting workers, field representatives, business partners and other users to a corporate network. Through the Internet, the information can be carried through at a small fraction of cost of long distance calls or private leased–lines, using secured tunnels, thus providing the means to make a corporate network available all over the globe. This entails a lesser budget, which is a great advantage to businesses especially nowadays when cost–cutting is ideal.

With the many intruders that come about and have access to the Internet the sensitive or proprietary data must be protected. That is why specific security measures have been implemented to Virtual Private Networks such as encryption, authentication and filtering processes – the best example of this that can be given is IPSec Authentication. This measure is considered secure since in accessing and sending data, an IPSec header is attached ensuring that the packet cannot be easily decrypted by the recipient nor can it be sent without this security technique.

Many companies and individuals have created specific software and hardware to make creation of VPNs easier and marketable. However, since this is a new technology, many limitations still face these investors in the technology. Nowadays, operating systems such as Windows NT Server have support capabilities for VPN creation. It is not as efficient though since the connections of the different entities within the relationship VPN are not 100% working. This entails a problem in terms of the communication between the central controller, or server, and the clients, or users. Also investments in commercial VPNs entail great cost since each entity to be added has separate licenses, which means that each connection made is paid for separately and not in bulk. A possible solution is for an organization not only to invest in software, specifically for VPNs, but also on special routers to ensure that it can function. However, this is a major disadvantage since the cost efficient characteristic of VPN technology cannot be achieved through this method.

With this in mind the proponents have decided to venture on the possibility of the implementation of a VPN in Linux. This entails that a working model be made to function. Linux was chosen because of the many capabilities of its environment to specific functions and the portability it has to other operating systems.

1.2 Statement of the Problem

The main problem of the study is:

How can a Virtual Private Network solution be implemented in Linux?

The following questions decompose the main problem further;

- What are the advantages of a Virtual Private Network?
- How do packets (data) travel across a VPN?
- What are the security measures needed?
- What architectural model can be used for the VPNs?
- What methods of application be used in the Linux OS?

1.3 Objectives of the Study

The objectives of this study are the following:

- To learn of the different security measures implemented on VPNs.
- To learn how the security measure work on VPNs.
- To create an architectural model of a VPN.
- To identify a specific method of application to be used in the Linux OS.
- To develop a working prototype of a VPN.

1.4 Scope and Limitation of the Study

This study will be on Virtual Private Networks – how they are created and what security measures are implemented to have a secure VPN. The focus will be on the Secure Sockets Layer (SSL) VPN being the latest concept in VPN creation. The idea behind the SSL-based VPN is using the encryption technology embedded in a Web browser to provide a secure connection to corporate data or applications.

This study seeks to create a VPN that is a working prototype running on PPP–over–SSL. To test that the prototype is working the proponents have decided to demonstrate simple PING sessions to both ends of the VPN. This ensures that a connection and tunnel has been established. Though there are different types of VPNs, the proponents will be creating a REMOTE ACCESS / SITE–TO–SITE VPN since the two are interrelated in terms of access. This is also inline that the proponents' focus on mobile users or clients having access at any point through a DIAL–UP Internet Service Provider (ISP).

In view of the time constraints of the said project the VPN that will be created would consist of two computers, one as the dial–up client and the other as the VPN server. The VPN server listens to any incoming connection to the VPN. When a client tries to connect, it checks if that client is a registered user. If the user is allowed access, a VPN tunnel is created from the VPN server to the dial-up client.

1.5 Significance of the Study

The benefits of implementing a working Virtual Private Networks(VPN) are:

1.5.1 Less Cost

The VPN technology boasts of a wider range of sites reducing the cost of communication infrastructure of organizations. Using the Internet to distribute network services over long distances means companies no longer have to purchase expensive leased lines to branch or partner offices as a VPN connection needs only to use a relatively short dedicated connection. It can further reduce costs by lessening the need for long-distance telephone charges, as clients can gain access by dialing into the nearest service provider's access point.

Since Linux will be used as the operating system and is freeware, the cost for the OS itself is relatively minimal which is another advantage in terms of achieving less cost.

1.5.2 Less dependent on Physical Connection in comparison to LANs and WANs.

This entails that a broader share of users can access the system through different methods such as a PC in a different area or a laptop when work is needed. Thus mobile users and branch offices can dial into the protected network via their local ISP. There is no need of investment in cable and

hardware that can only span limited distances.

1.5.3 Dynamic Network

In comparison to the leased lines that are traditionally being used VPN maintains no permanent links between the end points that make up the basic network. A VPN connection between two sites is created when needed, and when the connection is no longer needed for a particular user, then it is torn down. Through this method, other users can use the bandwidth and resources.

1.5.4 Remarkably Secure

The VPN technology is also considered remarkably secure since it has introduced tunneling protocols wherein data protection has become more standardized among service providers. Data that are sent over VPNs are confidential, and not susceptible to hacking authorization is required before passing through the "tunnel". Users can authenticate packets to establish the validity of the information, and the integrity of the data is usually guaranteed.