

**Bachelor of Information Technology**

**School of Information Technology**

***IT6x19 – Operating Systems***

**Assignment 1**

Semester 2, 2017

Executive Summary

I have chosen Virtual Private Network (VPN), as there is an increasing demand from businesses for this technology.

Table of Content

Executive Summary 2

Table of Content 3

Introduction 4

Types of VPN 4

Common practices used by small, medium and large enterprises 5

Conclusion 7

References 8

Bibliography 9

Appendices 10

Introduction

The Virtual Private Networks or VPN is used to securely connect Clients and servers through tunnelling. It is not feasible for companies to rely on dedicated leased lines to enable them and their workers to connect from their homes or other temporary locations, whereas VPN offers them a secure means of connectivity which offers the encrypting of data and is a perfect solution for individual remote users or for small remote sites. Apart from the technological advantages, there is also the advantage of reduced costs, and if properly executed it can provide extensive area security, minimize the associated costs with traditional leased lines. Remote users and an organisation will save money as the company can relinquish the cost of their leased lines. These possibilities are thanks to the concept of a Virtual Tunnel which re-encapsulates data packets inside other data packets and transports it into the public internet.

As pointed out in Microsoft (2017), connections allow an organisation the ability to send their data between two computers through the Internet in such a way that it matches properties of a point-to-point connection. This means that VPN allows computers or entire networks to connect to each other over the Internet securely. For example if you working in Wellington and you need to connect to your business system in Auckland, then you would be able to do this securely using VPN.

Types of VPN

Site-to-site VPN is one of the types of VPN – with site-to-site VPN data is encrypted from one VPN gateway to another and offers a secure connection between these two sites through the internet. It permits both of these sites to share resources, for instance documents and other types of data over the VPN connection. Remote access VPN distribution or mobile VPN which is also known as is a secure connection made from individual computer to a VPN router. It allows the user to access their e-mail, files and other resources at work from anywhere outside their workplace as long as they have internet access.

There are four major networking protocols which VPN tunnels rely on and which provide different levels of security. One is PPTP or Point-to-point Tunnelling Protocol. This will allow remote users to gain access to their company network in a secure way, while using MS Windows Systems and other Point to Point tunnelling Protocol (PPP) proficient platforms. Another is L2TP or Layer 2 Tunnelling Protocol and is used most widely by internet service providers (ISP) in order for them to offer VPN services over the internet. This is a hybrid of Point-to-Point Tunnelling Protocol (PPTP) and Layer 2 Forwarding Protocol (L2F). IPsec (Internet Protocol Security) is the standard VPN and is used to generate connections between two networks and individual devices with networks. Traffic is encrypted and authenticated as it works at IP layer and is the best overall purpose VPN that is available. All levels of connectivity with IPsec has end to end security, but one of the issues with IPsec is in the application, which can vary from provider to provider and can often cause issues when interconnecting. SSL (Secure Socket Layer) is something that most internet users already use, but have little to no knowledge that they are actually using it. SSL is used to connect a single user to website portals such as ecommerce. SSL creates an encrypted VPN connections which protects transactions and loss of data. As the SSL uses web-browser interface, it makes it the easiest to use for small to medium sized businesses. The drawback of SSL is the limitation with functionality (VTNV Solutions, 2017).

Common practices used by small, medium and large enterprises

In the past businesses used Wide Area Networks or WANs to connect remote offices. These used LANs or Local Area Networks, but the installation and overhead of using LANs or WANs were very expensive. WANs needed lots of resources, but this has been superseded by VPN which they can rely and depend on and accessed via the Internet.

The day-to-day work that we now perform in our workplace will rely largely on technology, mainly our computers, laptops, tablets and smart phones. Businesses are increasingly having employees working from home, or other locations, either in the same town, city, or even in other countries. Staff need to access information which is located on the company network system, so using VPN is something that these businesses are having to look at or are using.

Security or more precisely the security of their data held on their computer system is something that businesses take very seriously. Businesses are often concerned with the lack of information security outside the confines of their organisation. They may feel that it is too big a risk to allow workers to remote into their network system from home or wherever else, but if they want to be completive in this day and age, they cannot afford to overlook the need to grant remote access to their employers.

For a small business who have limited number of staff, the need for remote access or VPN is not really necessary as their current system is enough. But this will be determined by the type of business they are in. If their field of business is in sales, then allowing their sales people access to resources on their network while out on the road is necessary and more productive.

Medium businesses may have more workers, so having the ability for them to work from home or elsewhere will reduce cost in office space and computer equipment as workers will be using their own equipment. This would be the same for larger organisations and these medium to larger organisation will have more money to put into implementing this type of technology. But before companies even look at VPN, they need to be aware of VPN networking best practices. It is common practice that businesses ensure that only their company equipment (hardware) is used by their workers, and that these are able to connect to their internal network even without VPN.

They need to make sure that authorised software is install by the company or users. They need to make sure that they have protection against Distributed Denial of Service or DDoS attacks. Other security measures which needs to be implemented is the installation of antivirus and firewall on all company provided hardware. Antivirus software will safe guard against malicious files, and firewalls will prevent more direct hacking attempts. Companies need to make sure that they have a three-layer defence working to protect remote access to their network system (anti-virus, firewall and VPN). Their ICT team should make sure that they monitor any alerts from these three-layer defences continuously. Businesses should also adopt a two factor authentication for VPN, as this will further increase their network security.

According to Kasacavage (2002) small, medium or large companies a secure remote access system needs to have the following features:

* *Reliable authentication of users and systems*
* *Easy-to-manage, granular control of access to particular computer systems, files, and other network resources*
* *Protection of confidential data*
* *Logging and auditing of system utilisation*
* *Transparent reproduction of the workplace environment*
* *Connectivity to a maximum number of remote users and locations*
* *Minimal costs for equipment, network connectivity, and support (p.166)*

Conclusion

References

Sequeira, A. (2012). Core principles of Virtual Private Networks (VPNs) for CompTIA Network+. Pearson education. Retrieved <http://www.pearsonitcertification.com/articles/article.aspx?p=1868074>

Microsoft (2017). How VPN Works. Retrieved <https://technet.microsoft.com/en-us/library/cc779919(v=ws.10).aspx>

VTNV Solutions 92017). The History of VPN. Retrieved <file:///D:/2017_S2/Op%20Systems/OP_Systems_Assignment_one_16082k17/Research/Saved_WebPages/The%20History%20of%20VPN%20creation%20_%20Purpose%20of%20VPN%20_%20Le%20VPN.htm>

Kasacavage, V. (2003). Complete book of remote access. Connectivity and security. London, UK: Auerbach Publications.

Bibliography

Appendices