

Secure Network Solutions for Cloud Services

Chengcheng Huang

This thesis is submitted in total fulfillment
of the requirements for the degree of
Master of Computing

School of Science, Information Technology and Engineering

University of Ballarat
PO Box 663
University Drive, Mount Helen
Ballarat, Victoria 3353
Australia

Submitted in December 2013

ABSTRACT

Securing a cloud network is an important challenge for delivering cloud services to cloud users. There are a number of secure network protocols, such as VPN protocols, currently available to provide different secure network solutions for enterprise clouds. For example, PPTP, L2TP, GRE, IPsec and SSL/TLS are the most widely used VPN protocols in today's securing network solutions. However, there are some significant challenges in the implementation stage. For example, which VPN solution is easy to deploy in delivering cloud services? Which solution can provide the best network throughput in delivering the cloud services? Which solution can provide the lowest network latency in delivering the cloud services? This thesis addresses these issues by implementing different VPNs in a test bed environment set up by the Cisco routers. Open source measurement tools will be utilized to acquire the results. This thesis also reviews cloud computing and cloud services and look at their relationships. It also explores the benefits and the weaknesses of each securing network solution. The results can not only provide experimental evidence, but also facilitate the network implementers in development and deployment of secure network solutions for cloud services.

STATEMENT OF AUTHORSHIP

Except where explicit reference is made in the text of the thesis, this thesis contains no material published elsewhere or extracted in whole or in part from a thesis by which I have qualified for or been awarded another degree or diploma. No other person's work has been relied upon or used without due acknowledgement in the main text and bibliography of the thesis.

Signed: _____

Signed: _____

Dated: _____

Dated: _____

Chengcheng Huang

Dr. Zhaohao Sun

Candidate

Principal Supervisor

ACKNOWLEDGEMENTS

I would like to express my sincere thanks to my principal supervisor, Dr. Zhaohao Sun, School of Science, Information Technology and Engineering (SITE), for the enormous amount of time and support he has given me throughout this project. I also give sincere thanks to my associate supervisor Dr. Philip Smith, School of Science, Information Technology and Engineering (SITE), who has given me tremendous support throughout this project.

My thanks and appreciations are also extended to the following people who have supported me in undertaking this postgraduate research degree program: Mr Nicholas Andison, Dr. Sue Read and Mr Yi Chen.

Finally, I would like to acknowledge my family—my wife, Xinxin Hong, my father Bingxin Huang, my mother Huaixiang Guo, my sisters Liqing Huang and Yongqing—for always being there for me during the last two years of hard work.

TABLE OF CONTENTS

LIST OF FIGURES.....	viii
LIST OF TABLES	x
1 INTRODUCTION	1
2 LITERATURE REVIEW	2
2.1 Recent Studies	2
2.1.1 VPN Technology Comparison	3
2.1.2 Test Bed and Measurement Tool Comparison.....	6
2.1.3 Result Comparison	9
2.2 Research Aim.....	11
2.3 Conclusion	12
3 METHODOLOGY	12
3.1 Research Design	12
3.1.1 Preparation Stage.....	13
3.1.2 Implementation Stage.....	13
3.1.3 Analysis Stage	14
3.2 Instruments	15
3.3 Conclusion	16
4 CLOUD COMPUTING AND CLOUD SERVICES.....	16
4.1 Introduction to Cloud Computing.....	16
4.2 Cloud Deployment Models.....	18
4.2.1 Private Cloud.....	18
4.2.2 Public Cloud.....	19
4.2.3 Community Cloud	19
4.2.4 Hybrid Cloud.....	20
4.3 Cloud Services.....	20

4.3.1	Infrastructure as a Service (IaaS)	21
4.3.2	Platform as a Service (PaaS)	22
4.3.3	Software as a Service (SaaS).....	22
4.3.4	Other Cloud Services	22
4.4	Cloud Service Providers	23
4.5	Benefits and Challenges of Cloud Services.....	24
5	SECURE NETWORK SOLUTIONS	25
5.1	VPN Fundamentals.....	25
5.1.1	Definition of VPN	26
5.1.2	Types of VPN.....	26
5.1.3	Tunneling	28
5.1.4	Encryption	29
5.1.5	Authentication	31
5.2	VPN Protocols	37
5.2.1	Point-to-Point Tunneling Protocol (PPTP)	37
5.2.2	Layer 2 Tunneling Protocol (L2TP).....	39
5.2.3	Generic Routing Encapsulation (GRE).....	40
5.2.4	Internet Protocol Security (IPSec).....	41
5.2.5	Secure Sockets Layer/ Transport Layer Security (SSL/TLS)	43
5.3	Routing	44
5.3.1	Routing Algorithms.....	45
5.3.2	IP Routing Protocol.....	48
5.4	Conclusion	49
6	SECURE NETWORK SOLUTIONS DEPLOYMENT.....	49
6.1	Enterprise Inter-cloud Architecture	50
6.2	Network Topology.....	50

6.3	Test Bed Setup	51
6.4	Deployment Process	53
6.4.1	PPTP VPN Solution	54
6.4.2	L2TP with IPSec Security VPN Solution	56
6.4.3	GRE with IPSec Security VPN Solution.....	59
6.4.4	IPSec VPN Solution	61
6.4.5	SSL/TLS VPN Solution	62
6.5	Summary.....	66
7	RESULTS AND ANALYSIS	66
8	DISCUSSION AND RELATED WORK.....	73
9	FUTURE RESEARCH DIRECTIONS	74
10	CONCLUSION	75
11	REFERENCE	76
12	ADDITIONAL MATERIALS	85
13	KEY ITEMS AND DEFINITIONS	87

LIST OF FIGURES

Figure 1: The relationships among cloud services	21
Figure 2: Example of intranet VPN connection and extranet VPN connection.....	28
Figure 3: Example of symmetric encryption.....	30
Figure 4: Example of asymmetric encryption	31
Figure 5: How does receiver know who sent the message.....	32
Figure 6: Example of hashing process	33
Figure 7: Hashing in action	33
Figure 8: HMACs in action.....	34
Figure 9: Digital signatures in action	36
Figure 10: Structure of a PPTP packet	38
Figure 11: Structure of a GRE packet	40
Figure 12: IPsec's AH protocol protection.....	42
Figure 13: IPsec's ESP protocol protection.....	42
Figure 14: Packet format in transport mode and tunnel mode	42
Figure 15: Operation of distance vector routing algorithm.....	46
Figure 16: Operation of link state routing algorithm	47
Figure 17: Interior gateway routing protocols (IGP) and exterior gateway routing protocol (EGP)	49
Figure 18: An enterprise inter-cloud architecture	50
Figure 19: Network topology	51
Figure 20: Physical topology	52
Figure 21: Relationship between Windows 7 and VirtualBox.....	53
Figure 22: Virtual private network connection for PPTP VPN	55
Figure 23: PPTP VPN connectivity testing.....	56
Figure 24: IPsec setting in virtual private network connection for L2TP VPN	58

Figure 25: Error message from L2TP connection without pre-share key setting	58
Figure 26: VPN Type setting in virtual private network connection for L2TP VPN	59
Figure 27: GRE with IPSec security VPN connectivity testing.....	61
Figure 28: Security alert from SSL/TLS VPN connection	64
Figure 29: Cisco SSL VPN service home page	64
Figure 30: Cisco SSL VPN service user homepage.....	65
Figure 31: SSL/TLS VPN connection summary.....	65
Figure 32: SSL/TLS VPN connectivity testing.....	65
Figure 33: TCP throughput summary	67
Figure 34: UDP throughput summary.....	67
Figure 35: Latency of PPTP VPN.....	69
Figure 36: Latency of L2TP VPN.....	69
Figure 37: Latency of GRE VPN.....	69
Figure 38: Latency of IPSec VPN.....	70
Figure 39: Latency of SSL VPN	70
Figure 40: Latency of No VPN	70

LIST OF TABLES

Table 1: The relationship between OSI reference model, TCP/IP protocol suite and VPN technology.....	3
Table 2: Recent studies on VPN protocol evaluation from 2000.....	5
Table 3: Summary of test bed environment and measurement tool from reviewed studies	6
Table 4: Results and rankings of study [1].....	9
Table 5: Results and rankings of study [2].....	9
Table 6: Results and rankings of study [3].....	9
Table 7: Results and rankings of study [4].....	9
Table 8: Results and rankings of study [5].....	10
Table 9: Results and rankings of study [6].....	10
Table 10: Interface and Its corresponding IP address	53
Table 11: PPTP VPN solution on enterprise edge router and cloud provider router	55
Table 12: L2TP with IPSec security VPN solution on enterprise edge router and cloud provider router	57
Table 13: GRE with IPSec security VPN solution on enterprise edge router and cloud provider router	60
Table 14: IPSec VPN solution on enterprise edge router and cloud provider router.....	62
Table 15: SSL/TLS VPN solution on enterprise edge router and cloud provider router	63
Table 16: Networking technologies used in deployment.....	66
Table 17: Average throughput of TCP and UDP	67
Table 18: Latency measurement summary	70
Table 19: Performance rankings for each solution	71
Table 20: Results summary.....	72

1 INTRODUCTION

Cloud computing is one of the most significant developments in information technology (Bauer & Adams, 2012). Ried (2011) predicted that the cloud computing market will grow from \$40.7 billion in 2011 to \$240 billion in 2020. Cloud computing has been recognized as the fifth generation of computing after mainframe computing, personal computing, client-server computing and the web (Khmelevsky & Voytenko, 2010).

Cloud computing has two meanings. It can refer to either the applications delivered as services over the Internet or the hardware and system software in the data centers that provide those services (Yang, Tan, Dai, & Guo, 2009). Cloud computing provides its services according to the service models. Examples of the service models are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Buyya, Broberg, & Goscinski, 2010). Cloud services can be developed in different cloud environments, such as private cloud, public cloud, community cloud and hybrid Cloud, according to the deployment models (Sitaram & Manjunath, 2011). Enterprise cloud is developed on the service model and deployment model according to the business requirements and demands of the enterprise.

One of the challenges facing enterprise clouds and cloud services is cloud security. The problem of how to secure the cloud service connections, especially in a large geographic area without interference from unauthorized parties, has drawn considerable attention from the cloud developers. One of the popular solutions is to deploy Virtual Private Network (VPN) technologies.

VPN is a network technology that establishes a connection through a public network utilizing encryption technology to privatize and secure data for transmission between two enterprises (Gentry, 2001). There are a number of VPN protocols which provide different solutions to VPN deployment and guarantee the efficient delivery of cloud services from different areas. Popular VPN technologies include: PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), MPLS (Multiprotocol Label Switching), GRE (Generic Routing Encapsulation), IPsec (Internet Protocol Security), and TLS/SSL (Transport Layer Security/Secure Sockets Layer) based on RFC (Request For Comments) (RFC, 2012). Recent studies indicate that VPN technologies play an important role in cloud computing and bring significant advantages to enterprises in

securing cloud connections. For instance, Hao et al (2010) indicated that L2TP or IPSec can be utilized to provide connectivity and security for enterprises to access the cloud network. Jamil and Zaki (2011) stated that enterprises can use VPN connections to improve the cloud security and minimize network attacks such as DDoS (Distributed Denial of Service) attacks and network sniffing. Gupta and Verma (2012) concluded that dynamic IP-VPN can improve the security of an enterprise. However, different VPN solutions lead to significantly distinct results due to the weaknesses and strengths of deploying VPN protocols (Jaha, Shatwan, & Ashibani, 2008). Hence, implementing a suitable and secure VPN solution for the cloud is a significant challenge for network implementers and enterprises. Therefore, this study addresses this issue by evaluating the most popular VPN solutions in a virtual cloud network environment.

The remainder of this study is organized as follows. Firstly, the study reviews the recent literatures in this area and the methodology of the thesis. Moreover, it looks at the cloud computing and cloud services and their relationships. Besides, this study explores each of the most popular securing network solutions and related networking technologies. Furthermore, it elaborates on the inter-cloud architecture, the test bed setup and the deployment processes, summarizes the experiment results and discusses the related work. Finally it provides some future research directions and some concluding remarks.

2 LITERATURE REVIEW

The current research of network protocol includes design, analysis, specification, verification, implementation, and performance (ICNP, 2013). This study focuses on analysis, verification and performance of network protocols in VPN for cloud computing. The goals of this chapter are firstly to review the recent studies in this field, and then to identify a research direction for the future study.

2.1 Recent Studies

In order to perform a systematic review of recent studies in this field, the following literature reviews attempt to focus on three different major aspects to demonstrate and support the hypothesis, e.g. VPN technology comparison, test bed and measurement tool comparison and result comparison.

2.1.1 VPN Technology Comparison

There are three important VPN technologies: trusted VPNs, secure VPNs, and hybrid VPNs (VPN Consortium, 2008). To start with, trusted VPNs can be recognized as the customer lease circuits from the VPN provider. The VPN provider is responsible for maintaining the integrity of the circuits and utilizing the best available business practices to avoid snooping of the network traffic. Secure VPNs are the virtual private network built by using encryption algorithms. A Hybrid VPN is the combination of trusted VPN and secure VPN. All those VPNs can be implemented by using different VPN protocols. However, different VPN protocols operate on different levels based on the OSI (Open System Interconnection) Reference Model and the TCP/IP Protocol Suite as shown in Table 1. Different VPN protocols can be utilized to establish different types of VPN solutions such as Data link layer VPNs, Network Layer VPNs and Application Layer VPNs (Held, 2004). Different solutions might result in performance differences. We have found that the flowing studies showed the performance distinctions among different VPN protocols.

Table 1: The relationship between OSI reference model, TCP/IP protocol suite and VPN technology.

OSI Reference Model	TCP/IP Protocol Suite	VPN Technology
Application	Application	HTTPS S/MIME,PGP
Presentation		
Session		
Transport	Transport (TCP/UDP)	SOCKS SSL, TLS,SSH
Network Layer	Network Layer (Internet protocol e.g. OSPF, BGP)	IPSec (AH,ESP) MPLS VPNs
Data Link Layer	Data Link Layer	L2TP,PPTP, L2F,ATM, Frame-Relay

Note: This table is based on “IPsec Virtual Private Network Fundamentals,” by Carmouche (2007)

Berger (2006) compared three different VPN protocols, e.g. L2TP, PPTP and IPsec, which fall into the Data Link Layer and the Network Layer category respectively as indicated in Table 1. The evaluation was carried out by comparing the different aspects such as performance measurement, link quality, stability analysis, feature comparison, interaction with TIP/IP protocols and basic security attacks. After evaluating different

VPN protocols in different testing environments, the author concluded that one of the significant drawbacks of all tested protocols was the dramatic loss of performance and throughput when the complex encapsulation and authentication techniques had been applied. Moreover, Berger (2006) also indicated that the PPTP was the fastest of those three VPN technologies and that its only weakness was the insufficient security level for critical applications.

Narayan, Brooking, and Vere (2009) also confirmed that different VPN protocols result in significant distinctions in the network performance. They analyzed three different VPN protocols such as PPTP, IPsec and SSL from three different levels, Data link layer, Network Layer and Application Layer, on three different operating systems, e.g. Windows Vista, Windows Server 2003 and Linux Fedora Core 6. The performance indices included the throughput, CPU usage and VPN initiation time. After the evaluation, their results indicated that there was a clear distinction among the VPN network throughput of PPTP, IPsec and SSL protocols in Windows environment. However, this was not true in Linux environment. For instance, the lowest throughput occurred when SSL had been implemented with various algorithms in Windows environment whereas IPsec was the worst performer in Linux. Moreover, Linux throughput values were between 6Mbps and 95Mbps whereas windows values ranged from 15Mbps to 95Mbps. Furthermore, Linux used the highest CPU of the VPN end nodes when compared to Windows. Additionally, Linux VPN initiation time was significantly higher than Windows. Lastly, from all the evaluations and findings combined, it had been concluded that VPN generated different network performance metric values in different combinations of operation systems, VPN protocols and algorithms.

Kotuliak, Rybár and Trúchly (2011) compared two different VPN protocols, IPsec and SSL, in Linux environment. A few tests had been performed using different performance indices such as throughput, response time etc. The study summarized that it was difficult to choose the better of these two technologies based on the tests due to the different requirements from the end users. However, the authors also concluded that IPsec was somewhat faster and it had more support among hardware and software vendors than SSL VPN solutions.

Ali, Samad and Hashim (2011) evaluated the performances of the MPLS network and the ATM (Asynchronous Transfer Mode) network. The evaluations discussed the

performances of MPLS and ATM in delivering video using multicast protocol from five different aspects. The authors drew the conclusion that the performance of MPLS was better than ATM in multicasting video traffic because the ATM requires extra server to perform multicasting whereas MPLS does not. Besides, the authors also concluded that multicast MPLS handled multicast better compared to ATM.

Additionally, the other studies such as Khanvilkar and Khokhar (2004), Mache, et al. (2006), etc. are also verified that different VPN protocols resulted in performance differences. The following Table 2 summarizes the recent studies from year 2000. It should be noted that the studies prior to year 2000 are not taken into considerations in our study.

Table 2: Recent studies on VPN protocol evaluation from 2000

Year	Author(s)	protocols	Title
2004	Shashank Khanvilkar Ashfaq Khokhar	SSH, SSL/TLS, IPSec	Virtual Private Networks: An Overview with Performance Evaluation
2006	Thomas Berger	IPSec, L2TP,PPTP	Analysis of Current VPN Technologies
2006	Jens Mache Damon Tyman Andre Pinter Chris Allick	OpenVPN: (SSL/TSL) based	Performance Implications of Using VPN Technology for Cluster Integration and Grid Computing
2009	Shaneel Narayan Kris Brooking Simon de Vere	IPSec, PPTP,SSL	Network Performance Analysis of VPN Protocols: An empirical comparison on different operating systems
2011	Zakaria Bin Ali Mustaffa Samad Habibah Hashim	MPLS, ATM	Performance Comparison of Video Multicasting over Asynchronous Transfer Mode (ATM) & Multiprotocol Label Switching (MPLS) Networks
2011	I.Kotuliak P.Rybár P.Trúchly	IPSec TLS	Performance Comparison of IPSec and TLS Based VPN Technologies

From what has been discussed above, indisputably, performance differences exist between different VPN protocols. There are many reasons causing the performance diversities. One of the possibilities is the various test bed environments. The measurement tools might influence the results as well. Hence, another assumption can be made at this point: the different test bed environments might influence the VPN performance values as

well as the measurement tools. Therefore, it is necessary to take a further investigation into the test bed environments and the measurement tools used by the reviewed papers.

2.1.2 Test Bed and Measurement Tool Comparison

From the previous section, an assumption is made after reviewing the related works, which is the test bed environment and the measurement tool might influence the performance of different VPN protocols. Therefore, the following Table 3 summarizes the test bed environments used in previous reviewed papers as well as the measurement tools utilized in their experiments.

Table 3: Summary of test bed environment and measurement tool from reviewed studies

No.	Year	Author(s)	Test Bed Environment	Measurement Tools
[1]	2004	Khanvilkar & Khokhar	<ul style="list-style-type: none"> two OSLV (Open-Source Linux-Based VPN) routers (RedHat Linux 9.0 and RedHat Linux 8.0) two Linux desktop 	<ul style="list-style-type: none"> <i>ethereal</i> for packet analysis <i>Iperf</i> for bandwidth measurement <i>ping</i> for latency measurement
[2]	2006	Berger	<ul style="list-style-type: none"> Cisco System Pix 501 Netscreen 5XP Soho Watchguard WG2500 Symantec FW/PN 100 Linux workstation 	<ul style="list-style-type: none"> <i>Ethereal</i> for packet analysis <i>Iperf</i> for throughput and roundtrip time measurement <i>Hping</i> for self-designed packets
[3]	2006	Mache, et al	<ul style="list-style-type: none"> Linux 2.4 (Red Hat 9.0) as the operation system, and LAM MPI(7.0.6) Two clusters connect to switch 	<ul style="list-style-type: none"> <i>NetIO</i> measures the throughput <i>Ping</i> measures the latency
[4]	2009	Narayan, Brooking, & Vere	<ul style="list-style-type: none"> Windows Vista Windows Server 2003 Linux Fedora Core 6 	<ul style="list-style-type: none"> <i>Iperf</i> for throughput and roundtrip time measurement
[5]	2011	Ali, Samad & Hashim	<ul style="list-style-type: none"> All connecting link node-to-node and node-to-hosts are using PPP_E1 (2.048 Mbps). 	<ul style="list-style-type: none"> <i>OPNET</i> Modeler is used to perform all simulations
[6]	2011	Kotuliak, Rybar & Truchly	<ul style="list-style-type: none"> Linux operating system 	<ul style="list-style-type: none"> <i>IxChariot</i> used to test network equipment

Based on the test bed environments in Table 3, Khanvilkar and Khokhar (2004), Berger (2006), and Kotuliak, Rybár and Trúchly (2011) used Linux operating system to set up their test bed environment by connecting to different Linux machines directly using network cables or by plugging into a switch. Both VPN solutions and measurement tools were implemented on the Linux operating system. The performance results were extracted from the Linux machine as well. Therefore, in these studies, each Linux machine had three different roles, the VPN server, the testing machine, and the software

router. Besides, some experiments were performed in a combination of different operating systems such as the combination of Windows Vista, Windows Server 2003 and Linux Fedora Core 6 in the experiments performed by Narayan, Brooking, and Vere (2009). However, in their studies, each machine acted the same role as the Linux machines which were discussed previously. Therefore, a conclusion can be made based on those studies that the performance evaluations were operated on the operating system level. One of the benefits of using this method is that the network environment has been simplified and it is good at evaluating the VPN protocols in a particular operating system.

Moreover, apart from using operating system as the test bed, Berger (2006) evaluated the performances of different VPN protocols in different networking devices such as Cisco System Pix 501, Netscreen 5XP, Soho Watchguard WG2500 and Symantec FW/PN 100. They are popular networking devices used widely in the real network deployment and implementation. Moreover, Berger (2006) used Linux machine to emulate the end users in order to observe the performance distinctions among different VPN solutions. In his study, the Linux machine was utilized only for the testing purpose. The test bed environment developed in Berger's study is more suitable than the previously discussed test beds because it is closer to the real network environment. In general, the VPN solutions are implemented on the routers or VPN devices rather than on the operating systems.

Additionally, Berger (2006) concluded that PPTP delivered the best performance values than the other examined protocols with 29.80Mbit/sec throughput values in 1 TCP section and 8.25Mbit/sec in 100 TCP sections. However, Narayan, Brooking, and Vere (2009) verified that PPTP throughput in Windows 2003 test bed environment returned the highest performance value all the time. However, the result was different in Linux environment, which showed the PPTP throughput values were poorer than SSL in a certain time. The measurement values derived from those two studies used the same measurement tool. Moreover, Khanvilkar and Khokhar (2004) indicated that the latency value in OpenVPN was 0.12 milliseconds in their testing environment. However, the value was different in the study performed by Mache, et al. (2006) with 0.224 milliseconds in VPN off and 0.736 milliseconds in VPN on in their test bed environment. Those two studies used the same measurement tool as well. Therefore, it can be confirmed that test bed environments influence the performance of the VPN solution.

According to Table 3, different measurement tools have been used in different studies. For instance, *ethtool* is a powerful tool used by network professionals around the world for troubleshooting, analysis, software and protocol development, and education (EtherealSoftware, 2006). *Iperf* was developed by NLANR/DAST originally as a modern alternative for measuring TCP and UDP bandwidth performance (Schroder, 2007). It is famous for throughput and roundtrip time measurement in recent studies. *Ping* or *Hping* is a free packet generator and analyzer for the TCP/IP protocol (Hping, 2009). It is used for latency measurement. *NetIO* is a powerful network tool designed to measure the net throughput of a network via TCP and UDP protocols using various packet sizes. Those are open-sourced test tools and they can be downloaded from the Internet freely. Besides, some of studies use commercial testing tools such as *IxChariot*. It is the industry's leading test tool for simulating real-world applications to evaluate the device and system performance under realistic load conditions (*IxChariot*, 2008).

Narayan, Brooking, and Vere (2009) showed that the throughput value of IPsec with 3DES encryption algorithm and MD5 authentication mechanism in Linux test bed environment was from approximate 40Mbps to 77 Mbps by using *Iperf*. However, Kotuliak, Rybár and Trúchly (2011) acquired the throughput value of IPsec with the same encryption algorithm and authentication method in Linux environment with less than 50Mbps by utilizing *IxChariot*. Those two values were different. One of the possibilities could be the measurement tool difference. Therefore, a conclusion can be made that the measurement tool plays an important role in performance measurements and it could influence the measurement value.

To conclude, it has been confirmed from the reviewed studies that different test bed environments could lead to distinctions in VPN performance and that measurement tools could influence the accuracy of the measurement values. Besides, it has been indicated that the VPNs were applied in the same test bed environment and the measurement values were acquired from the same measurement tool in each of the studies. Therefore, the results derived from each of the studies were valid and independent. However, we raised another hypothetical question: Which VPN solution has the best network performance based on all those research results? In order to answer the hypothetical question, it is necessary to take a further investigation into every result from each of the studies so as to identify the ranking of different VPNs.

2.1.3 Result Comparison

In order to answer the hypothetical questions raised in previous section, the following Table 4-9 summarized the results of each reviewed studies. It should be noted that the “[x]” represents the study number which corresponds to Table 3. Besides, each table contains ranking values, e.g. ②, which identifies the ranking of the performance in a particular protocol associated with the measurement parameter. For example, in Table 4, IPSec has the best ranking in “Latency” evaluation compared to PPTP and SSL/TLS in Khanvilkar & Khokhar’s study because it has the ranking of ①.

Table 4: Results and rankings of study [1]

	PPTP	SSL/TLS	IPSec
Latency	②	③	①
Throughput	①	③	②

Table 5: Results and rankings of study [2]

	No VPN	PPTP	L2TP	IPSec
Latency	①	②	③	④
Throughput	①	②	③	④

Table 6: Results and rankings of study [3]

	No VPN	SSL/TLS
Latency	①	②
Throughput	①	②

Table 7: Results and rankings of study [4]

Throughput	No VPN	IPSec	PPTP	SSL/TLS
Windows 2003	①	③	②	④
Windows Vista	①	③	②	④
Linux	①	④	②	③

CPU usage	No VPN	IPSec	PPTP	SSL/TLS
Windows 2003	①	④	②	③
Windows Vista	①	④	③	②
Linux	①	④	③	②

Table 8: Results and rankings of study [5]

	MPLS	ATM
Latency	①	②
Throughput	①	②

Table 9: Results and rankings of study [6]

	No VPN	IPSec			SSL/TLS		
		Blowfish	AES	3DES	Blowfish	AES	3DES
Latency	①	③	②	⑦	④	⑤	⑥
Throughput	①	③	②	⑦	⑤	④	⑥
CPU Usage	②	⑤	⑦	①	③	④	⑥

Table 5, 6, 7 and 9 illustrate that No VPN has the best ranking of ① in throughput and latency measurements and there is an exception in CPU Usage measurement in Kotuliak, Rybár and Trúchly's study with the ranking of ② (Kotuliak, Rybár, & Trúchly, 2011). Overall, the network performance is the best without applying VPN technologies.

Moreover, without taking No VPN into consideration, Table 5 and 7 indicate that PPTP has the best ranking of ① in throughput and latency performances compared to IPSec, L2TP and SSL/TLS. However, Kotuliak, Rybár and Trúchly observed that PPTP utilized more CPU than SSL/TLS in Windows Vista and Linux environment, but it performed extremely well in Windows 2003 (Kotuliak, Rybár, & Trúchly, 2011). Therefore, it can be concluded from different studies that PPTP has the best outcomes in throughput and latency measurements. Besides, Berger revealed that L2TP is better than IPSec in throughput and latency measurements (Berger, 2006).

Table 8 concludes that MPLS is better than ATM solutions in both latency and throughput evaluations (Mache, et al. 2006).

Table 4 shows that IPSec has better ratings than SSL/TLS in latency and throughput measurements in Khanvilkar & Khokhar's study (khanvilkar & Khokhar, 2004). Table 7 indicates that the throughput performance of IPSec is better than SSL/TLS in Windows environment, but it is poorer than SSL/TLS in Linux environment (Narayan, Brooking, & Vere, 2009). Moreover, the Table 7 also illustrates that IPSec uses more CPU resources than SSL/TLS in both Windows and Linux environment in the CPU usage evaluation. Additionally, in Table 9, IPSec with Blowfish or AES encryption algorithm is better than SSL/TLS with Blowfish or AES respectively in latency and throughput performance measurements (Kotuliak, Rybár, & Trúchly, 2011). However, IPSec with 3DES

encryption algorithm performs poorer than SSL/TLS with 3DES. On the other hand, in the CPU usage evaluation, IPsec with 3DES requires the lowest CPU resources whereas SSL/TLS with 3DES demands the highest CPU resources (Kotuliak, Rybár, & Trúchly, 2011). SSL/TLS with Blowfish or AES encryption algorithm is slightly better than IPsec with Blowfish or AES in CPU usage measurements. To conclude, IPsec performs better than SSL/TLS in latency and throughput evaluations with higher CPU usages.

It can be concluded from the discussions above that the PPTP has the best performance results in throughput and latency evaluations compared to L2TP, IPsec and SSL/TLS solutions. It also implies that the Data Link Layer VPN has the best network performances in terms of throughput and latency.

2.2 Research Aim

It has been verified that PPTP solution has the best performance results in network throughput and latency measurements. However, it is difficult to identify whether PPTP solution is still the best in terms of network performance in the cloud environment because there is limited literatures available online regarding this particular area. Moreover, the question of which popular secure network solution has the best performance results in terms of through and latency remains open. The answers to these questions are significant to the cloud designers because they provide valuable guidance and references in selecting the optimal solution for implementing the cloud connections. Therefore, our study is going to fill this gap.

Our study aims at exploring the distinctions of network performance among different secure network solutions in the cloud environment for the purpose of providing practical and experimental results in supporting the cloud network developers in selecting the proper solutions when establishing secure connections to deliver the cloud services to the end users. In order to achieve the research goal, three research questions have been identified and listed below:

- Which VPN solution is easy to deploy in delivering cloud services?
- Which solution can provide the best network throughput in delivering the cloud services?
- Which solution can provide the lowest network latency in delivering the cloud services?

2.3 Conclusion

This chapter reviewed the latest related literatures from three different aspects: VPN technology comparison, test bed and measurement tool comparison and result comparison. It has been confirmed the existence of the network performance distinctions among different VPN solutions. It has also been verified that different test bed environments could lead to distinctions in VPN performance and that measurement tools could influence the accuracy of the measurement values. It has been concluded that PPTP solution has the best performance results in network throughput and latency measurements. However, whether this conclusion is true in cloud environment has not been verified. Therefore, our research aim is to fill in this gap in order to provide practical and experimental results for the cloud networkers in implementing the suitable solution to deliver the cloud services. The research questions have been raised.

In order to achieve the research goal, it is necessary to establish a systematic and feasible research methodology to ensure the research staying on the track and making regular progress. The next chapter details the research methodology.

3 METHODOLOGY

This chapter describes the design adopted by this research to achieve the aims and objectives stated in the previous chapter, which is to explore the network performance of different secure network solutions in the cloud environment for purpose of providing practical and experimental results in supporting the challenges facing the cloud network developers when selecting secure solutions to deliver the cloud services to the end users.

The remainder of this chapter is organized as follows. Section 3.1 outlines the research design used in the study. Section 3.2 illustrates the instruments utilized in the study. Section 3.3 describes the procedure of the study. The last section concludes the problems and limitations of the methodology.

3.1 Research Design

In order to achieve the research goal, we have classified the research design into three stages: the preparation stage, the implementation stage and the analysis stage.

3.1.1 Preparation Stage

In the preparation stage, test bed setup plays an extremely critical role. As what we have discussed in Chapter 2, Khanvilkar and Khokhar (2004), Mache, et al. (2006), Narayan, Brooking, and Vere (2009) and Kotuliak, Rybár and Trúchly (2011) used operating system as the test bed to perform the experiments. However, one of the limitations of using the operating systems as the test bed environments is that the results derived from the test bed might be incorrect or inaccurate in the real network environment. It has been discussed, to a large extent, that VPN solutions are used to implement on the edge routers or VPN devices rather than on the operating systems to provide secure connections. So, using the operating system as the test bed environment is not suitable for this study. Therefore, a sound and indisputable test bed environment is significantly important to our project, which guarantees the quality of the research and the accuracy of the results. To conclude, we are going to set up a test bed environment by using physical devices rather than using operating systems.

3.1.2 Implementation Stage

In implementation stage, only the most popular secure network solutions will be deployed in the test bed environment one by one to observe the performance differences. This is because there are a number of secure network solutions nowadays and some of the solutions are obsolete or unpopular for the networkers in the cloud environment. Therefore, the solutions included in our study are PPTP VPN, L2TP VPN, GRE VPN, IPSec VPN and SSL/TLS VPN. Besides, in order to be close to the real network environment, some other networking technologies will be implemented as the supplement technologies, such as NAT (Network Address Translation), apart from the VPN technologies. NAT is a network protocol used in IPv4 networks which allows multiple devices to use the same public IPv4 address to connect a public network (Sosinsky, 2009). It also helps to improve the security by reusing the IP address. The reason why we take NAT into consideration is that, to our best knowledge, most of the companies and organizations as well as our home network use NAT at their edge router to allow the Internet access in IPv4 network. Hence, implementing supplement technologies will help us to build a comprehensive network environment and to improve the quality of our experiments and results.

3.1.3 Analysis Stage

In the analysis stage, throughput and latency are selected as our measurement parameters in our experiments because these two parameters have been identified as the most popular and critical measurement parameters in the network performance evaluation and they have been used by many researchers based on the discussions from the previous chapter. The network performance results of each secure network solution will be collected by using the most trusted open source measurement tools. All the results will be analyzed systematically and comprehensively to identify the distinctions of network performance of each mentioned secure network solutions.

Throughput refers to the average rate of successful message delivery over a communication channel (Wikipedia, 2013). It indicates the possible quantity of data that can be transmitted from one place to another in a given time period. Network bandwidth can be referred to both actual and theoretical throughput (Lowe, 2012). The greater the network capacity, the better the performance. Therefore, the throughput measurement is used to estimate the actual bandwidth of the network. Besides, network throughput is affected by factors such as the network protocols used and the capabilities of routers and switches etc., used to create a network (Solarwinds, 2013). Different network solutions could result in throughput differences under the same physical environment. Therefore, throughput is selected as one of the measurement parameters in our experiments.

Bandwidth is one of the elements that is perceived to be the speed of a network. Latency is another element that plays a critical role in contributing to the network speed (Lowe, 2012). Latency, especially the network latency, is an expression of how much time it takes for a packet of data to get from one designated point to another (Rouse, 2006). Generally, a low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays. Moreover, latency is measured using either one-way delay time or round-trip delay time. One-way delay time refers to the time from the source sending a packet to the destination receiving it. Round-trip delay time means that the one-way delay time from source to destination plus the one-way delay time from the destination back to the source. In general, latency indicates how fast the network responds to the action. Therefore, latency is another measurement parameter in our experiments.

To sum up, our experiments focus on comparing the throughput and latency of each selected secure network solution in a cloud network environment to observe the performance distinctions among each of the solutions in order to answer the research questions.

3.2 Instruments

As what has been discussed above, we are going to set up a test bed environment using physical devices. Therefore, the test bed environment is created with the help of Cisco 1800 series routers, computers and an open source software called VirtualBox.

Cisco 1800 series routers integrate a suite of enhanced router security technologies into the platform to protect the enterprise network (Cisco, 2013). It supports a number of VPN solutions such as GRE VPN, L2TP VPN, PPTP VPN, IPsec VPN, SSL VPN, DMVPN (Dynamic Multipoint VPN) and so on. It meets all our requirements and is competent to establish a quality test bed environment for our experiments. Therefore, Cisco 1800 series routers are selected as our most important physical devices in the test bed establishment.

Moreover, VirtualBox is one of the powerful virtualization products for enterprises to run different virtual operating systems such as Windows, Linux individually or at the same time on an existing computer (Oracle Corporation, 2009). It is readily available as an open source software (VirtualBox, 2009). VirtualBox can be used to simulate the virtual cloud servers as well as the cloud users. Hence, VirtualBox will be used in our study to emulate a cloud server and a cloud user for the testing purpose. The combination of Cisco 1800 series router with VirtualBox is one of the best solutions to establishing the test bed environment.

Besides, in order to obtain the reliable and accurate results from the experiments, two open source software have been used in measuring the throughput and latency respectively. Iperf is a modern powerful network performance management tool developed by the Distributed Applications Support Team (DAST) at the National Laboratory for Applied Network Research (NLNR) for measuring the TCP and UDP bandwidth performance (French forum for Iperf, 2011). Jperf is a GUI front of Iperf application which does the same job as Iperf and it is more user-friendly than Iperf. Thus, we will use Jperf as the throughput measurement tool in our experiments.

Furthermore, Colasoft Ping Tool is one of the free network tools used to measure the latency of the network (Colasoft, 2013). It was developed by Colasoft Co., Ltd for networkers in troubleshooting the internetwork. It supports ping multiple IP addresses simultaneously and lists all the comparative responding times in a graphic chart, which is competent to collect accurate values for our experiments. Therefore, we used Colasoft Ping Tool as the latency measurement tool in our experiments.

3.3 Conclusion

This chapter outlined the research design based on three different stages such as the preparation stage, the implementation stage and the analysis stage. It has been described that the most important step in the preparation stage is to establish a reliable test bed environment and that some physical devices will be used to guarantee the quality of the test bed for our experiments. Moreover, it has been discussed that only the popular secure network solutions will be taken into account in our study. Networking technologies will be implemented together with the secure network solution in order to improve the quality of the experiments. Furthermore, throughput and latency have been identified as the measurement parameters in our experiments based on reviewed papers. Open source measurement tools will be applied in data collections and data analysis.

Before getting into the secure network solutions development and the results and analysis, it is necessary to understand the concept of cloud computing and secure network solutions. Therefore, the next chapter reviews the fundamentals of the cloud computing and cloud services followed by secure network solutions and protocols.

4 CLOUD COMPUTING AND CLOUD SERVICES

In this chapter, we explore the fundamental of cloud computing and cloud services and look at the relationship between them. We also describe a number of popular cloud service providers nowadays. The chapter concludes by discussing the benefits and challenges of cloud services.

4.1 Introduction to Cloud Computing

There are many definitions of cloud computing and no definition is accepted by all scholars in the field (Thomas, 2012). Nonetheless, one of the most acceptable definitions for cloud computing provided by U.S. National Institute of Standards and Technology

(NIST) that is “*a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*” (Mell & Grance, 2011, p. 6).

Based on the definition, cloud computing is composed of five essential functional characteristics:

- **On-demand self-service** which means that resources are “instantly” available to the user requests via a service or provisioning website (Bauer & Adams, 2012).
- **Broad network access** which means that users intend to access the cloud services anywhere through any kinds of wire line or wireless network device they wish to use over whatever IP access network is most suitable (Bauer & Adams, 2012).
- **Resource pooling** which means that service providers deploy a pool of different physical and virtual resources such as servers, storage devices, and other data centre resources that are shared across multiple consumers to reduce costs to the service providers (Mell & Grance, 2011).
- **Rapid elasticity** which means the ability of a user to acquire computing resources quickly so that they can commence work within a short period of time and improve the efficiency, as well as enable application group to respond to business conditions extremely rapidly (Carstensen, Morgentha, & Golden, 2012).
- **Measured servicing** which means that measuring resource consumption and suitably pricing to cloud users for their cloud resource consumption inspires the consumer to release unneeded resources so that they can be used by other cloud consumers rather than squandering the resources (Bauer & Adams, 2012).

The concept of cloud computing was dated back to the 1950s, when large-scale mainframe computers became available in academia and corporations (Strachey, 1959). Large-scale mainframes as a service became popular at that time, that is, many institutions rented large-scale mainframes rather than purchased them subject to paying renting fees. However, cloud computing only becomes quite popular from the past several years and it is still in its infancy stage today (Thomas, 2012).

Cloud computing is a type of Internet-based computing platform (Chao, 2012). Unlike other types of Internet-based computing, cloud computing provides computing resources and services such as network infrastructure, hardware and software based on the demand

of users. Users only pay for the computing resources and services they use. Cloud services are provided by independent organizations or by cloud service providers to facilitate the cloud migration and the cloud management for the customers (Sosinsky, 2010). Shifting from the traditional computing network to cloud computing network helps enterprises to reduce the network administration costs and improve the efficiency of the services (Buyya, et al., 2010), because the enterprises do not have to invest upfront on expensive IT infrastructure. They can simply use the computing resources or services provided by cloud providers with agreements. The providers deal with all the maintenance tasks.

4.2 Cloud Deployment Models

There are a number of different ways to deploy cloud services depending upon factors such as security requirements, partnership with other organization, private or public accessibility, and type of network access. These deployment models provide different solutions to the way in which customers can control their resources, and the scale, cost, and availability of resources (Badger, Grance, Patt-Corner, & Voas, 2012). There are four different deployment models defined by the National Institute of Standards and Technology (NIST) and accepted by the majority of cloud stakeholders today: private cloud, public cloud, community cloud, and hybrid cloud (Buyya, et al., 2010).

4.2.1 Private Cloud

Private cloud, also called internal cloud, provides the cloud services built in a private network with existing resources provided by an internal enterprise for use in other internal enterprises (Halpert, 2011). A private cloud might be managed by the enterprise's IT department or a third party cloud provider. One of the advantages of a private cloud is that the enterprise can style the structure of cloud and modify the infrastructures or configurations any time to meet exactly what it needs (Finn, Vredevoort, Lownds, & Flynn, 2012). Private cloud is one of the popular solutions for public, private, and government organizations worldwide to exploit cloud benefits such as flexibility, cost reduction, agility etc. (Buyya, et al., 2010). Furthermore, private cloud is the best solution when the data security and privacy are of top priority to the enterprise (Thomas, 2012).

An enterprise deploying a private cloud may not benefit from the same degree of savings on up-front capital costs as using public cloud because the enterprise still needs to

purchase, install, and manage the cloud infrastructure (Thomas, 2012). Nonetheless, private clouds provide better flexibility, greater operational efficiency, high reliability and high data security and the capability to deliver other benefits of cloud computing while minimizing some of its shortcomings (Sosinsky, 2010).

4.2.2 Public Cloud

A public cloud, also called external cloud, is one in which the cloud infrastructure is provisioned for open use by the general public while being owned, managed, operated by an organization (Mell & Grance, 2011). In other words, a third party owned and operated hardware, networking, storage, services, application and interfaces can be used by not only individuals, but also other enterprises (Hurwitz, Kaufman, Halper, & Kirsch, 2012). Moreover, a public cloud is based on the standard cloud computing model. It might be provided on a free or pay-per-usage basis.

One of the advantages of a public cloud is that the service is always ready for use by the end users and they only need to pay if they access to those services (Hurwitz, et al., 2012). Enterprises can implement a new business application in a short time instead of investing significant resources in advance to set up and run the solution. The enterprise has no control of the cloud services and data when the services are external (Thomas, 2012). Amazon, Google, Microsoft, and Rackspace are the most popular public-cloud providers (Li, Yang, Kandula, & Zhang, 2011).

4.2.3 Community Cloud

A community cloud is a cloud in which groups of individuals and organizations with similar IT requirements share an infrastructure provided by a single service provider (BCS The Chartered Institute for IT, 2012). The groups could be an industry consortium, an awareness group, or another group altogether (Halpert, 2011). Community clouds could be managed by the organizations or a third party and may exist on premise or off premise. A community cloud is less expensive than a private cloud but more expensive than a public cloud, and it may provide a higher level of privacy, security and policy compliance than a public cloud (Williams, 2009).

One of the benefits of community clouds is that the costs of the cloud services are spread between all the customers which make it more economical than a single tenant arrangement with the service provider. Moreover, community cloud users usually benefit

from better security and privacy (Halpert, 2011). An example of community cloud is OpenCirrus formed by HP, Intel, Yahoo, etc (Buyya, et al., 2010).

4.2.4 Hybrid Cloud

A hybrid cloud is a composition of two or more clouds such as private, community or public clouds where those clouds remain their unique entities, but are bound together as a unit (Sosinsky, 2010). Hybrid cloud environments are usually implemented where a customer requires for a mix of cloud services (BCS The Chartered Institute for IT, 2012). For instance, an enterprise may store the sensitive data on its local dedicated server and less sensitive data in the cloud. The services are maintained by both internal and external providers (Thomas, 2012).

One of the advantages of hybrid cloud is that it allows enterprises to take advantage of the scalability and cost-effectiveness that a public cloud computing environment provides without exposing important applications and data to the third party vulnerabilities (Thomas, 2012). Some examples of offering hybrid cloud solutions include Amazon Virtual Private Cloud, Skytap Virtual Lab, and CohesiveFT VPN-Cubed (Buyya, et al., 2010).

4.3 Cloud Services

Cloud services are one of the critical components of cloud computing. A cloud service is any computing resource provided by the cloud computing providers over the Internet (Rouse, 2011). Cloud services are designed to be flexible, scalable to applications, resources and services, and fully managed by a cloud services provider. Therefore, a cloud service can dynamically scale to meet the needs of its customers so that the customers do not need to deploy their own resources for the service nor allocate IT staff to manage the service. Examples of cloud services can be online data storage and backup solutions, Web-based e-mail services.

Cloud services broadly comprise three different types of service: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) (Buyya, et al., 2010). In each case the services reside remotely and are accessed over a network, usually the Internet, through a user's web browser, rather than being deployed locally on a user's computer. Each service focuses on a specific layer in a computer's runtime stack such as hardware, system software (or platform) and application respectively (Sitaram &

Manjunath, 2011). The Figure 1 illustrates the relationship among these three cloud services.

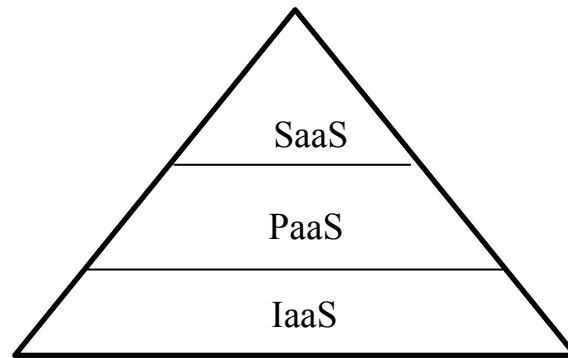


Figure 1: The relationships among cloud services

Note: This figure is based on “Reliability and Availability of Cloud Computing,” by Bauer and Adams (2012)

4.3.1 Infrastructure as a Service (IaaS)

IaaS corresponds to the bottom layer of cloud computing systems (Buyya, et al., 2010). IaaS allows users to gain access to different kinds of infrastructure. Typically, different services are provided by dividing a very large physical infrastructure resource into smaller virtual resources (Halpert, 2011). For instance, the service can be a virtual machine with an operating system, application platforms, middleware, database servers, enterprise service buses, third-party components and frameworks, and management and monitoring software (Kommalapati, 2010). The IT professionals who manage the infrastructure have full control of all the infrastructures and configurations, and they have responsibilities for maintaining all the facilities of the infrastructure.

In this form of cloud computing, the cloud provider rents the infrastructures to support the customer’s operations or business services (Arinze & Sylla, 2012). The client then only pays when they use the resources. One of the most popular IaaS providers is Amazon who provides their EC2 IaaS (Halpert, 2011).

4.3.2 Platform as a Service (PaaS)

PaaS is a higher level of cloud computing services which makes a cloud easily programmable (Buyya, et al., 2010). For example, PaaS allows users to create the applications using programming languages, libraries, and tools from the provider. In this form of cloud services, the users control the software deployment and configuration settings (Mell & Grance, 2011). PaaS also provides necessary supporting services such as storage, security, and integration infrastructure for a complete platform.

4.3.3 Software as a Service (SaaS)

SaaS resides on top of the cloud stack and provides a rich web-based interface to consumers (Halpert, 2011). Consumers can obtain the same software services and functionality on-line as locally installed computer program (Buyya, et al., 2010). SaaS is a pay-as-you-go paradigm so users only need to pay for the services provided when they access the resources. There are no upfront commitments or any long-term contracts for the end users. There are many free SaaS such as Internet email communication software.

SaaS is one of the best solutions for enterprises or organizations to deal with the shortage of skilled resources for managing their IT systems (Thomas, 2012). The possible cloud resources such as Gmail, Google Docs, and Facebook can be installed at the back-end to deliver the cloud services to the customers. SaaS is meant for all the end customers.

4.3.4 Other Cloud Services

Network as a service (NaaS) is one of the latest cloud services. NaaS was proposed in 2012 (Costa, Migliavacca, Pietzuch, & Wolf, 2012). The concept of NaaS is to outsource to the cloud networking service providers in order to limit the cost of data communications for the cloud consumers, as well as to improve network flexibility (Costa, et al., 2012). NaaS enable the cloud consumers to use network connectivity services and/or inter-cloud network connectivity services. It includes flexible and extended VPN, and bandwidth on demand (Focus Group, 2012). Besides, Costa, et al (2012) indicated that NaaS can significantly increase network quality by improving the application throughput and reducing the network traffic in order to deliver better cloud services performance to the cloud users.

Storage as a Service (StaaS) has drawn an increasing attention from some enterprises recently. StaaS is a business model that a giant enterprise leases or rents its storage

infrastructure to a small company or individual to store data (Rouse, 2009). StaaS is also being recognized as an alternative way to mitigate risks in disaster recovery, as well as offering long-term preservation for records for businesses, which improves both in business continuity and availability.

Additionally, the number of cloud based services increased rapidly in recent years. Shan (2009) published a comprehensive taxonomy model includes latest cloud services such as Strategy-as-a-Service, Collaboration-as-a-Service, Business Process-as-a-Service, Database-as-a-Service, etc. Besides, ITU (International Telecommunication Union) (2012) officially announced that Network as a service (NaaS), Communications as a Service (CaaS), Desktop as a Service (DaaS), Service Delivery Platform as a Service (SDPaaS) become a part of the essential cloud computing models, recognized service categories of a telecommunication-centric cloud ecosystem. Along with the rapid development of cloud computing, more and more cloud services will be proposed and implemented to satisfy the cloud consumers.

4.4 Cloud Service Providers

Amazon, one of the most famous cloud enterprises, provides access to a virtual computing environment and allows customers' applications run on a "virtual CPU". The cloud consumers pay 10 cents per clock hour to the enterprise and they can get as many "virtual CPUs" as they need (Barr, Varia, & Wood, 2006). Therefore, the enterprise earns income from providing cloud services to the cloud consumers. Amazon also launched Amazon Web Services (AWS) which provides scalable cost-efficient cloud solutions for education program to facilitate the most demanding research projects, course objectives at public and private universities, community colleges and so on (Amazon, 2011). After Amazon, other major IT companies such as Google, IBM and Microsoft also launched their own cloud computing projects.

Google App Engine is one of the famous cloud computing platforms designed to run Web applications on Google's infrastructure (Google, 2010). Application developers can use different program languages such as Java, JavaScript, Python or Ruby App Engine by Google to develop Google apps. Besides, Google offers its cloud computing services to the public through Google Apps and Google Docs (Martin J. A., 2010).

SmartCloud is one of the IBM cloud computing services (IBM, 2010). IBM SmartCloud provides the enterprise-class cloud computing technologies and services for

securely establishing and implementing private, public and hybrid clouds. IBM SmartCloud helps companies achieving new levels of innovation and efficiency with solutions for private cloud, Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS).

Microsoft releases its own cloud computing platform called Windows Azure (Kommalapati, 2010). The Windows Azure provides a hosted application server and the data storage, computing and networking infrastructure for building and running Windows applications. With Windows Azure, application developer can create scalable and highly available services and applications. Moreover, Microsoft provides a free application development package called Windows Azure Software Development Kit (SDK), which helps the application developer to create and test the cloud applications on local computers with Windows Azure and then upload the cloud application to Windows Azure directly.

Apart from the most well-known cloud provider listed above, Rackspace, CenturyLink/Savvis, Salesforce.com, Verizon/Terremark, Joyent, Citrix, Bluelock and VMware are also famous in USA (SearchCloudComputing, 2012). Moreover, in Australia, the most well-known cloud service provider includes Dimension Data, Fujitsu, Wipro, Emantra, Telstra, Melbourne IT (Carr, May, & Stewart, 2012). Different cloud services providers provide different cloud services with different cost. Cloud users can obtain most of the services from different cloud service providers so that they can focus on their business without paying too much attention to IT infrastructure and services.

4.5 Benefits and Challenges of Cloud Services

Cloud services have a number of benefits. Firstly, cloud users only pay for what they use because most of the pricing models are consumption-based. Secondly, cloud services are easy to use because cloud services allow you to avoid the hardware and software procurement and capital expenditure stage and to concentrate on implementation. Thirdly, cloud users can enjoy the up-to-date cloud services without worrying about extra costs because the cloud services providers constantly update their services (BCS The Chartered Institute for IT, 2012). Fourthly, the flexibility and scalability of cloud services enable to increase the needed infrastructure and services according to the need of the clients, and also it will reduce the precious time needed to offer a new service (Al-Masah & Al-

Sharafi, 2013). Fifthly, the mobility of cloud services allows cloud users access to the services from mobile workforce (BCS The Chartered Institute for IT, 2012).

However, there are some challenges of cloud services including privacy, reliability, and the possibility of being locked into one cloud service provider. There are also questions on the ability to seamlessly convert to cloud without interfering with the existing in-house systems and information resources (Harding, 2011). Some enterprises might hesitate to take advantage of cloud services due to these challenges and concerns. Moreover, experts indicate that the biggest challenge about cloud services is data security (Thomas, 2012). Data loss and leakage and account hijacking are the common security issues in cloud computing, which could lead to the gathering, modifying and stealing of the important data by unauthorized users (Neela, Kavitha, & Ramesh, 2013). Therefore, secure network solution is critical in offering high-quality cloud services to the cloud users, especially to the remote users who require secure and reliable connections. The following sections will look more deeply into secure network solutions.

5 SECURE NETWORK SOLUTIONS

Secure network solutions provide assurance that network operates its critical functions correctly without any harmful side effects (Joshi, 2008). VPN solutions are one of the most popular solutions in securing the cloud connections. It has been utilized extensively nowadays in cloud deployment. Moreover, VPN technology provides secure and seamless connection between consumers and the cloud, in order to protect the communication without meddling by unauthorized users (Wood, Ramakrishnan, Shenoy, & Merwe, 2012).

VPN solutions can be deployed by using different VPN protocols such as PPTP, IPSec and SSL/TLS and so on. The following sections review the fundamental of VPN and its protocols as well as the related technologies.

5.1 VPN Fundamentals

VPN dates back to the 1990s. It allows an organization to share private network services over a public or shared infrastructure such as the Internet or service provider backbone network (Lewis, 2006). Although VPN technologies have been widely used for more than two decades at different times, it still plays an important role in enterprise cloud development. The various types of VPNs provide different solutions to enterprises to meet different needs.

5.1.1 Definition of VPN

VPN is a network technology that is usually used to establish a connection through a public network such as Internet utilizing encryption technology to privatize data for transmission between two trusted parties (Gentry, 2001). A VPN connection can be simply described as a VPN tunnel that is built between the Branch Office and Corporate Hub across the Internet so that both sides of the enterprise can access each other privately (Lewis, 2006). VPN can also be utilized to access the cloud services remotely by establishing a VPN tunnel between cloud users and the cloud. There are many recognized and acknowledged definitions of VPN. One of the popular definitions of VPN is:

“A virtual private network is a combination of tunneling encryption, authentication and access control used to carry traffic over the Internet (or a managed Internet protocol (IP) network or a provider’s backbone) (Younglove, 2000)”.

Based on this definition, a VPN utilizes three different technologies to secure its connections, encryption, authentication and access control. Encryption is the process of converting plain text to cipher text in such a way that only authorized entities can read it (Goldreich, 2004). Examples include 3DES, the RC series (RC2/4/5/6) and RSA etc. Authentication is the process of confirming the identities of the message originator (Ferguson B. , 2012). Examples include hash functions and digital signatures. Access control is the process of verifying the user who has been given the permission or keys to access the information or resources (Strebe, 2006). If the user is not in the permission list, access is denied.

5.1.2 Types of VPN

VPNs can be classified into various types based on the construction of the VPN and the goals they are constructed to achieve. The following section introduces the different types of VPNs used in the industry today.

5.1.2.1 VPN Types Based on Encryption versus No-Encryption

Based on the use of encryption or lack of encryption, VPNs can be divided into two main categories: Encrypted VPN or Non-encrypted VPN (Malik, 2002).

Encrypted VPNs utilize different types of encryption mechanisms to encrypt the network packets in order to secure the traffic flow across the public accessible network such as Internet (Malik, 2002). IPSec (Internet Protocol Security) VPNs is a good

example of encrypted VPNs. IPSec VPN is constructed using IPSec protocol which encrypts traffic using an encryption algorithm to ensure the security of the packets crossing the public network like Internet.

On the other hand, non-encrypted VPNs are established to connect two or more private networks without using any encryption algorithms so that users on both networks can easily to access resources sitting on either network (Malik, 2002). GRE (Generic Routing Encapsulation) – based VPN, which is a good example that it provides VPN functionality between two different private networks without any security mechanism. In other word, GRE packets are sent without utilizing encryption mechanism to ensure the traffic security on the public network. However, those types of non-encrypted VPNs are always complemented by some forms of encryption such as using IPSec to provide data confidentiality.

5.1.2.2 VPN Types Based on OSI Model Layer

VPNs can also be divided into four different categories based on OSI model according to the Table 1, which are Data Link Layer VPN, Network Layer VPN, Transport Layer VPN, and Application Layer VPN.

Data Link Layer VPNs connect two private networks using a shared network infrastructure which is based on switched link layer technology such as Frame Relay or Asynchronous Transfer Mode (ATM) (Gleeson, Lin, Heinanen, Armitage, & Malis, 2000). Network Layer VPNs are constructed by using Layer 3 tunneling and/or encryption techniques such as IPSec tunneling and encryption protocol to create VPNs (Malik, 2002). The tunnel connects two points of a VPN across the public network infrastructure (Venkateswaran, 2001). Application Layer VPNs are developed to work particularly with specific applications (Malik, 2002). One of famous examples is SSL/TLS based VPNs. SSL/TLS based VPNs offer encryption between web browsers and servers in SSL connections.

5.1.2.3 VPN Types Based on Business Functionality

Based on the business goal, VPNs can be classified into two categories: Intranet VPNs and Extranet VPNs (Malik, 2002).

Intranet VPNs are constructed to connect two or more private network within the same organization or industry (Malik, 2002). Intranet VPNs often appears when a remote office

needs to be connected to headquarters or when a company is acquired and needs to integrate its own network into the acquirer's main network.

Extranet VPNs are utilized to connect private networks which the private networks belong to more than one organizational unit (Malik, 2002). For instance, the extranet VPNs often come into existence when two companies want to conduct business together so that, under this scenario, one of the companies can be allowed to utilize the other company's resources by giving them access through a VPN across the public network such as Internet. The following Figure 2 illustrates an example of Intranet VPN and Extranet VPN.

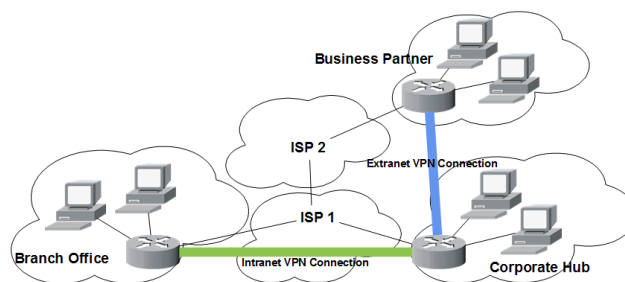


Figure 2: Example of intranet VPN connection and extranet VPN connection

5.1.3 Tunneling

Tunneling is a method of sending packets securely over a shared public infrastructure such as Internet (Younglove, 2000). In general, there are two methods for constructing VPN tunnels. They are “network based approach” and “Customer Premise Equipment (CPE) based approach” (Cohen & Kaempfer, 2000). In network based approach, tunnels are constructed between the routers across the public shared network. In CPE-based approach, tunnels are established only between CPE devices such as border router. Moreover, CPE-based approach is simpler than network based approach in VPN construction. However, network based approach is more scalable and economic than CPE-based approach (Cohen & Kaempfer, 2000). Besides, there are numerous tunneling mechanisms, which contain L2TP, PPTP, GRE, IPsec and MPLS (Ferguson & Huston, 1998). Those tunneling mechanisms are used to establish VPNs and they have been known as VPN protocols.

Tunneling has two advantages (Venkateswaran, 2001). Firstly, tunneling mechanism helps to route multiple protocols across the shared network infrastructure such as Internet. For instance, the original packet could be based on any layer 3 protocol such as IP, Apple

Talk, or Novel IPX. Moreover, constructing tunnels can minimize the influence on routing process due to different routing protocols and addressing mechanism might be applied on VPN and the shared network infrastructure.

However, there are some disadvantages of tunneling (Venkateswaran, 2001). Firstly, it is difficult to manage a numerous number of tunnels. Therefore, it doesn't scale well to the large number of VPN nodes. Secondly, the packets can be eavesdropped by others who attached to the shared network infrastructure in the case of encryption mechanism is not in use on the tunnel. Once the tunnel headers are stripped away and packets are readable in their original forms.

5.1.4 Encryption

As what has been discussed above that one of the disadvantages of tunneling is lack of privacy. This is a critical problem for organization who wants to construct VPN tunnels on shared public networks to transmit important information (Yuricik & Doss, 2001). Therefore, Encryption mechanism plays an extremely important role in providing data confidentiality for VPN tunnels to ensure the information security (Cisco, 2003).

Encryption is the process of converting plaintext to ciphertext in such a way that eavesdroppers or hacker cannot read it, but only the authorized entities can read it (Goldreich, 2004). The purpose of encryption is to guarantee confidentiality, so that the authorized entities can read the original data (Cisco, 2003).

In an encryption scheme, the packets or messages in cleartext form are encrypted by utilizing an encryption algorithm, converting all the plaintext information into unreadable ciphertext (Goldreich, 2004). This is usually done with the use of an encryption key, which defines how the message is to be encrypted.

Once the authorized entities received the encrypted messages, all the messages will be decoded into the readable plaintext format using a decryption algorithm. Therefore, decryption is the reversal process of encryption which turning the unreadable messages into readable format (Goldreich, 2004).

In modern encryption algorithms, there are two very different encryption algorithms to encrypt data, symmetric encryption algorithm and asymmetric encryption algorithm (Cisco, 2003). Each encryption algorithm has its own benefits and limitations. The following subsections reviews the basis of these two algorithms.

5.1.4.1 Symmetric Encryption Algorithm

Symmetric encryption, also known as secret key encryption, is a form of data encryption where a single secret key is utilized in both encryption and decryption (Li N. , 2009). For instance, the Figure 3 illustrates that the sender and the receiver use the same key to encrypt and decrypt the message. The security of a symmetric algorithm relies on the secrecy of the symmetric key. Anyone can encrypt and decrypt messages if they have the key.

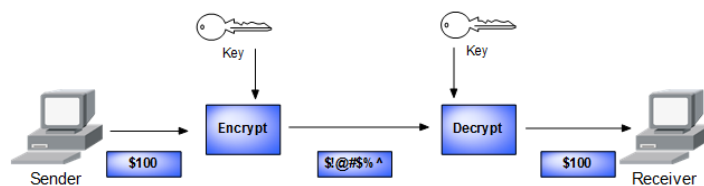


Figure 3: Example of symmetric encryption

Note: This figure is based on “Designing VPN Security,” by Cisco (2003).

There are numerous encryption algorithms use symmetric keys. The most well-known algorithms are DES, IDEA, the RC series (RC2/4/5/6), CAST and Blowfish (Delfs & Knebl, 2007). Generally, the key length in symmetric encryption algorithms ranges from 40 to 168 bits.

One of the advantages of the symmetric encryption algorithms is simple to use (Cisco, 2003). All users can begin to encrypt and decrypt the message once the secret key has been shared. Moreover, symmetric algorithms are much faster than asymmetric encryption algorithms and use less computer resources (Henríquez, Pérez, Saqib, & Koç, 2007). However, one of the drawbacks of symmetric encryption algorithms is sharing the secret key in the beginning of the encryption (Cisco, 2003). It does not guarantee that the secret key has been shared securely and completely so that two parties have to provide a secure channel before any encryption can occur. Hence, the security of a cryptographic system heavily relies on the security of the key exchange method.

5.1.4.2 Asymmetric Encryption Algorithm

While symmetric encryption utilizes the same key for encryption and decryption, asymmetric encryption use two completely different keys to perform the encryption and decryption (Coles & Landrum, 2009). In other words, the key used for encryption is

different from the key used for decryption. For example, the Figure 4 illustrates that the sender and the receiver need to use different key to encrypt and decrypt the messages. Moreover, the decryption key cannot be easily derived from the encryption key, at least in any reasonable amount of time, and vice versa.

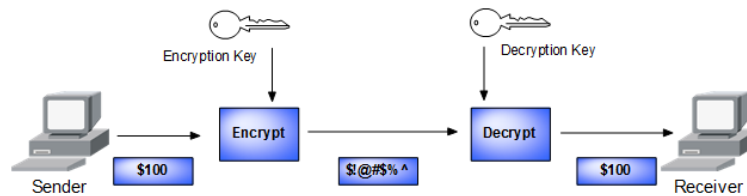


Figure 4: Example of asymmetric encryption

Note: This figure is based on “Designing VPN Security,” by Cisco (2003).

The two keys used in Asymmetric algorithms have been known as public key and private key (Henríquez, et al., 2007). The public key is available for every sender. However, a private or secret key is only known to the receiving ends. An important feature of any public key system is that the public and private keys are related to each other so that only the public key can be used to encrypt (decrypt) messages and only the corresponding private key can be used to decrypt (encrypt) them.

There are a number of asymmetric encryption algorithms such as RSA, ElGamal and elliptic curve algorithms (Cisco, 2003). In general, the key length for asymmetric algorithms ranges from 512 to 2048 bits, which is more than 10 times longer than symmetric encryption algorithms.

One of the benefits of using asymmetric encryption algorithms is that it solves the problem of disturbing the key for encryption. Everyone shares their public key and keeps the private key secret (Cisco, 2003). However, one of the drawbacks of asymmetric encryption algorithms is that they are up to 1,000 times slower than symmetric algorithms (Snyder, Myer, & Southwell, 2010).

5.1.5 Authentication

Although a VPN tunnel is established with encryption algorithms which provide confidentiality and security for the communication, there are still some problems that make the communication channel unsecure (Ferguson, Schneier, & Kohno, 2012). For example, based on Figure 5, sender tries to send the message *Hello* to receiver while an

interferer hacks into the communication channel, intercepts the message and replaces the *Hello* with *Hello'* then sends it to Receiver. At last, the receiver receives the message *Hello'*. Once the VPN tunnel has been hacked, interferer not only can delete the message so that receiver never receive the message, but also can alter the message, record the message and then send it to receiver later, or change the order of the message. In this case, receiver does not know the message has been altered by unauthorized personal. Therefore, there is no guarantee the integrity of the message as well as the origin of the message in this circumstance. Therefore, in order to solve this problem, message authentication is important to identify the authenticity in both message and originator.

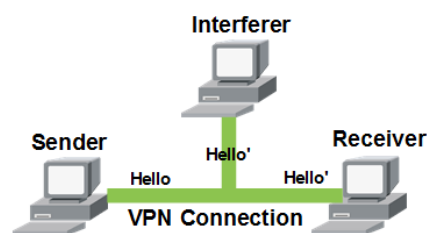


Figure 5: How does receiver know who sent the message

There are a number of authentication mechanisms provide message authentication in modern computing and networking. For instance, hash functions provide data integrity and digital signature guarantees the authenticity of a digital message or documents (Ferguson, Schneier, & Kohno, 2012). The following sections briefly discuss the hash functions and digital signatures.

5.1.5.1 Hash Functions

Hash functions are probably the most utility of all cryptographic primitives (Martin K. M., 2012). They are extremely useful and appear in all different surprising applications. Hash functions have been defined as taking input strings of arbitrary length and mapping these to short fixed length output strings (Preneel, 2011). The term hash function comes from computer science which it has been known as a function that compresses a arbitrary length string to a fixed length string.

The hashing process relies on a hash function, which is a one way function that it takes input strings of arbitrary (or very large) length and generates short fixed length output strings (Preneel, 2011). The output string is extremely strong. Therefore, it is impossible to compute the input data from its output string, even though the input data changes just a little bit, the output string will change substantially.

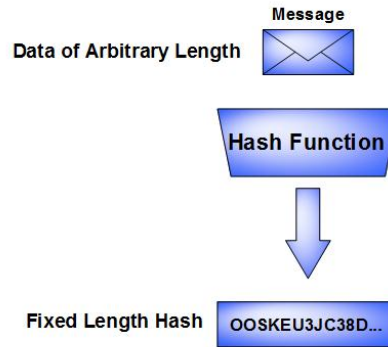


Figure 6: Example of hashing process

Note: This figure is based on “Designing VPN Security,” by Cisco (2003).

The Figure 6 illustrates how hashing is performed. Once the data of arbitrary length is input to the hash function, it will result in the hash function in the fixed length hash. With hash function, it is computationally infeasible for an interferer to generate data with the same hashing output value without giving the original data.

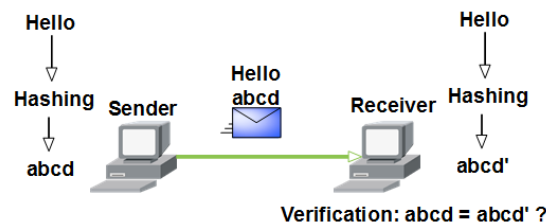


Figure 7: Hashing in action

The Figure 7 indicates hashing in action. Sender wants to ensure that the message *Hello* will not be modified on its way to the receiver. Firstly, the sender uses the message *Hello* as the input to a hashing algorithm and generates a fixed length output string *abcd*. This output string is then attached to the message *Hello* and sent to the receiver. Once the receiver obtained the message from sender, receiver removes the output string *abcd* from the message and uses the message *Hello* as the input to the same hashing algorithm. The receiver compares the output *abcd'* it computed with *abcd* it received from sender. The message will be identified as authenticated only if the hash *abcd'* computed by the receiver is equal to the one *abcd* attached to the message.

However, there is no encryption applied to the message in this example which a potential interferer could possibly intercept the message, modify it, recalculate the hash and attach it to the message then send it to the receiver. Hence, anyone can generate a

hash for any data and send it to the receiver as long as they use the correct hash function because there is nothing unique to identify the sender itself in hashing procedure. Therefore, it is important to understand that the hash functions are helpful to ensure the data has not altered accidentally, but cannot guarantee the data has not been purposely changed (Cisco, 2003). Besides, Message Digest 5 (MD5) and Secure Hash Algorithm 1 (SHA-1) are the most popular hash functions which have been using widely nowadays.

5.1.5.2 Message Authentication Code (MAC)

MAC, also known as a cryptographic checksum or a keyed hash function, is used in modern computing network widely (Paar & Pelzl, 2010). MAC is also one of the mechanisms for information authentication which a secret key shared between sender and recipient (Preneel, 2011). In terms of security functionality, MACs share some properties with digital signatures and they provide message integrity and message authentication. However, in technical terms, one of the differences between MACs and digital signatures is that MACs are symmetric key schemes and they do not provide non-repudiation (Paar & Pelzl, 2010).

An option for carrying out MACs is to use cryptographic hash functions such as SHA-1 or MD5 as a building block (Paar & Pelzl, 2010). Hash Message Authentication Code (HMAC) is one of the possible constructions and it becomes very famous in modern network technology over the last decade (Cisco, 2003). HMACs use hash function as the basis protection mechanism with the significant difference of adding an extra secret key as the input to the hash function. Only the sender and the recipient know the secret key. Moreover, the output of the hash function relies on the input data and the secret key. Hence, entities who have access to that secret key can only compute the output of an HMAC function, which this mechanism defeats man-in-the-middle attacks and also provides authentication of data origin. Additionally, there are some well-known HMAC functions like Keyed MD5 and Keyed SHA-1.

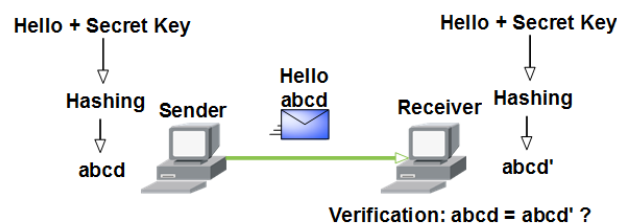


Figure 8: HMACs in action

The figure 8 illustrates HMACs in action. In this case, the sender wants to ensure that the message *Hello* did not alter by someone during the transmission and also wants the receiver to be acknowledged the origin of the message. In order to accomplish the requirements, firstly, the sender takes the message *Hello* and the secret key as input, uses a hashing algorithm and calculates the fixed length HMAC output *abcd*. This authorized output *abcd* will be attached to the message *Hello* and sent to the receiver. Once the receiver received the message, it removes the HMAC output *abcd* and uses the message *Hello* with the secret key as input to the same hashing function. After the HMAC output *abcd'* has been calculated by the receiver, it will be compared to the HMAC output computed by the sender in relation to whether the two HMAC outputs are equal in order to identify the origin and integrity of the message. If these two HMAC outputs are the same, it means that the message has not been altered during transmission. Besides, the origin of the message is authenticated only if the sender shares the secret key with receiver (Paar & Pelzl, 2010).

5.1.5.3 Digital Signatures

Digital signature is an alternative method which provides guarantees of data integrity and authenticity (Largent, Rogers, & Marsh, 2002). It operates by embedding a certain code into documents that certifies the origin of the message or document and verifies whether the content is changed during the transmission across the untrusted network. It has been used in modern computing and networking widely. Generally, digital signatures are operated using one of three methods: symmetric encryption, asymmetric encryption or signature dynamics (Saidman & Hairston, 1999).

Digital signature has the same functionality as handwritten signature which has been used as a proof of authorship or agreement to the contents of a document, but it has much more than handwritten signature (Katz, 2010). In general, digital signatures provide three fundamental security services in secure communication. Firstly, digital signatures guarantee the authenticity of digitally signed data and the authentication of the source. Moreover, digital signatures warrant that the data has not been altered since being signed by the singer, which ensure the integrity of digitally signed data. Furthermore, digital signatures assure the non-repudiation of the transaction, which means the recipient can take the data to a third party which it provides digital signature verification to verify the data exchange took place. All those security services are accomplished by the

characteristics of the digital signature, which the signature is authentic, un-forgable, un-reusable, unalterable and undeniable. Additionally, one of the well-known asymmetric algorithms used in digital signature is RSA (Cisco, 2003).

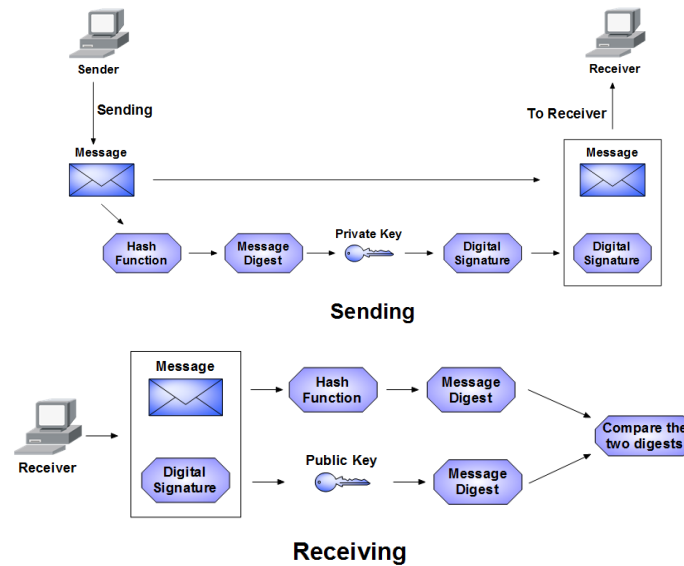


Figure 9: Digital signatures in action

The Figure 9 shows the action of digital signatures. Firstly, the sender generates two keys, one is signature key and the other is verification key. Generally, the signature key is a private key and only known to the signer. The verification key is a public key. Secondly, sender takes the message as input to a hashing algorithm and generates a message digest, then uses the message digest with private key to produce its digital signature. Sender attaches the message with the digital signature and sends it to the receiver. Once the receiver obtains the packet from sender, it extracts the packet into message and digital signature. Then, the receiver uses the message as the input to a hashing algorithm and acquires a message digest. The receiver uses the digital signature with the public key (received from sender) to produce another message digest. Those two message digests will be verified by receiver to confirm the validity and authenticity. The verification is successful only if the message has not been altered after signing by the sender.

One of the advantages of digital signature is that digital signature is more flexible in sending messages to multiple recipients compare to MAC (Katz, 2010). For example, if a sender wants to issue the same message to multiple recipients by using digital signature, the sender could only distribute a single public key and generate a single signature, which

the signature can be verified by any potential recipient. In contrast, with MAC, the sender needs to generate a separate secret key for each possible recipient and compute different outputs.

Moreover, digital signatures are public verifiable (Katz, 2010). For instance, if a recipient verifies the signature on a given message as valid, then the other potential receivers who receive this signed message will pass the verification of this message. This particular characteristic is not achieved by MAC, which a singer needs to share a separate key with each recipient.

However, compared to MAC, one of the drawbacks of digital signatures is that it is approximately 2-3 orders of magnitude less efficient than MAC (Katz, 2010). Hence, message authentication codes are preferred in situation where public verifiability, transferability and non-repudiation are not required or the sender only communicates with a single recipient most of the time.

5.2 VPN Protocols

VPN protocols are one of the secure network protocols provide essential privacy and security for users to access services in cyberspace without security threats (Buyya, et al., 2010). It also used to establish secure connections for cloud users in accessing the cloud services across the public shared infrastructures such as Internet. Different VPN protocols provide various secure solutions in VPN construction to achieve the requirements. However, not all of the VPN protocols have security mechanism embedded once they have been invented such as GRE (Cisco, 2003). A conjunction of different technologies not only can make up the shortcoming of the protocol itself, but also can improve the security and flexibility in secure network deployment. GRE with IPSec security is one of the examples.

The following section reviews the popular VPN protocols used widely nowadays in securing the cloud connections. It includes PPTP, L2TP, GRE, IPSec and SSL/TLS. It also discusses the advantage and limitation of each protocol.

5.2.1 Point-to-Point Tunneling Protocol (PPTP)

PPTP (Point-to-Point Tunneling Protocol) was developed by a vendor consortium including Microsoft, Ascend Communications (today part of Alcatel-Lucent), and 3Com, and published in 1999 (Hamzeh, Pall, Verthein, Taarud, Little, & Zorn, 1999). It is one of

the most popular dial-in protocols and it operates at the Data Link layer (Layer 2) of the OSI model (Cisco, 2003). PPTP is an extension of point-to-point protocol (PPP) (Narayan, Brooking, & Vere, 2009). It inherits many of features from PPP. PPTP uses TCP for its control channel and improved GRE tunnel for data transportation (Cisco, 2003). Basically, PPTP encapsulates PPP frames in IP datagrams for transmission over an IP network. The following Figure 10 illustrates the structure of a PPTP packet.

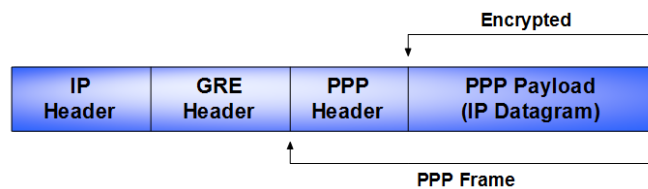


Figure 10: Structure of a PPTP packet

Note: This figure is based on “What is VPN?” by Microsoft (2003).

In particular, creating communication between two sites using PPTP involves three stages and each stage has to be completed prior to the next (Narayan, Brooking, & Vere, 2009). Firstly, a PPTP client will establish a link through IP network from the source to the destination using PPP type connection. Secondly, the PPTP protocol creates a control connection, using TCP, from the client to the PPTP server after the link has been established. Thirdly, PPTP protocol creates IP datagrams containing encrypted PPP packets which are transported through the tunnel.

Moreover, PPTP uses two different packet types to establish a VPN connection (Berger, 2006). The first packet type is the VPN payload, which is carried by GRE packets by adding the GRE header to the original packet, as shown in Figure 10. The second packet type is the PPTP control message, which is a TCP packet (port 1723) contains the control information such as connection requests and responses, connection parameters and error messages.

Additionally, PPTP always combines with additional security methods to guarantee the integrity of the messages and the security of the tunnel (Cisco, 2003). The standard PPP authentication methods such as Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) can be utilized in PPTP deployment. Besides, MS-CHAP, an enhanced version of the CHAP authentication method developed by Microsoft provides ability to use the security information. Moreover, Microsoft uses a

stronger encryption, Microsoft Point-to-Point Encryption (MPPE), for use with PPTP instead of utilizing PPP to encrypt data.

PPTP has a number of advantages (Cisco, 2003). Firstly, PPTP is a standard protocol which is interoperable between different systems. Moreover, PPTP has been used widely in Microsoft Windows operating systems. It can be applied to develop VPN connections between different private networks without installing additional VPN software because the client software has been embedded in Microsoft Windows.

However, PPTP has some limitations (Cisco, 2003). From the security point of view, PPTP has fault in weak authentication and encryption techniques. Moreover, the scalability is limit because one PPTP tunnel only can be used by one user. Besides, QoS has to be implemented with ISP involvement in order to make effective use of quality of service.

5.2.2 Layer 2 Tunneling Protocol (L2TP)

L2TP, Layer 2 Tunneling Protocol, which is a standard protocol proposed by Internet Engineering Task Force (IETF) for tunneling PPP sessions (Feilner, 2006). L2TP is also an extension to the PPP (Point-to-Point Protocol) described in RFC 2661 (Townesley, Rubens, Pall, Zorn, & Palter, 1999). L2TP provides a dynamic mechanism for tunneling layer 2 “circuits” across a packet-oriented data network such as IP network (Townesley, Lau, & Goyret, 2005). It has been accepted as an industry standard and widely used by manufactures such as Cisco and it is a key building block for access VPNs.

L2TP combines the best features of two other tunneling protocols: L2F (Layer 2 Forwarding) from Cisco system and PPTP from Microsoft and it is an important component of VPN solution to provide tunneling (Cisco, 2003). L2TP has different versions. The latest version of L2TP is version 3 which has been proposed in RFC 3931 (Townesley, Lau, & Goyret, 2005). The new version improves the transition session ID, tunnel ID control Connection ID and tunnel authentication mechanism and so on. The modification achieves the balance between code reuse and interoperability.

L2TP has a number of advantages (Cisco, 2003). For example, from user aspect, L2TP is a standard protocol. Therefore, all users can choose a wide range of service available from multiple vendors without requiring special client software. From service provider

aspect, L2TP solution offers a flexible and capable wide range of VPN services across different infrastructures.

However, one of the limitations of L2TP is that the protocol itself does not provide its own security mechanisms (Feilner, 2006). It needs to combine with other security mechanisms like IPsec to secure the data transmission.

5.2.3 Generic Routing Encapsulation (GRE)

GRE stands for Generic Routing Encapsulation, which is a tunneling protocol developed by Cisco Systems (Wikipedia, 2012). It is a simple tunneling protocol designed to provide a way to encapsulate any network layer protocol over any other network layer protocol (Cisco, 2003). It has also been described in RFC 1701. Unlike other newer technologies, GRE supports different protocols, multicasts, point-to-point or point-to-multipoint operation so that it can handle the transmission of multiprotocol and IP multicast between different networks.

GRE has been utilized widely nowadays to create simple Virtual Private Networks (VPNs) by establishing a tunnel between two different private networks through the Internet (Cisco, 2003). In this case, the local IP packets with private IP addresses can be transmitted successfully to a remote private IP network over the public network environment. GRE allows the routing protocols such as RIP, EIGRP or OSPF to be routed between two routers across the Internet.

In order to pass the IP packets with private IP addresses successfully across the Internet, GRE will encapsulate the payload by adding a GRE header between the IP Header and original packet (Cisco, 2003). Therefore, an IP packet routed through a GRE tunnel looks like this:



Figure 11: Structure of a GRE packet

Note: This figure is based on “What is VPN?” by Microsoft (2003).

By design, GRE tunnels are normally set up in a hub-and-spoke topology by establishing a clear data path between two sides (Hartpence, 2011). However, this data path is not secure. Therefore, one of the limitations of GRE tunneling protocol is that it neither provides authentication, integrity checking nor encryption. In order to solve this

problem, IPSec must be used on the GRE tunnels to ensure the data security (Cisco, 2003). Additionally, one of the significant advantages of GRE tunneling is that GRE supports quality of service (QoS) mechanisms to provide guarantees (Hartpence, 2011).

5.2.4 Internet Protocol Security (IPSec)

IPSec (Internet Protocol Security or IP security) was developed by Internet Engineering Task Force (IETF) in early 1990s (Ioannidis, 2011). IPSec is a collection of protocols, conventions, and mechanisms in order to ensure the authenticity and guarantee the confidentiality of the content of the IP packets (Bantoft & Wouters, 2006). From a security aspect, IPSec ensures the confidentiality, integrity and authenticity of data communication by providing a mechanism for secure data transmission over unprotected networks such as the Internet. From the deployment point of view, IPSec allows to construct a VPN tunnel between two private networks by using encryption algorithms. It also allows the authentication taking place at the both ends of the tunnel.

IPSec consists of three distinctive components to create a security framework: Internet Key Exchange (IKE), Encapsulating Security Protocol (ESP), and Authentication Header (AH) (Malik, 2002). IKE provides a framework that allows IPSec peers negotiating security parameters and creating authenticated key. In general, it is used to negotiate the parameters between two IPSec peers for constructing a tunnel. ESP and AH provides a framework for authenticating and securing of data (Bantoft & Wouters, 2006). On one hand, ESP provides encryption while AH does not. Specifically, ESP is the protocol utilized for encapsulating the original IP packet and providing encryption and authentication for the data. DES or 3DES is the most famous algorithm used in ESP which provides data confidentiality by encrypting the packet's contents. On the other hand, AH is the protocol utilized for authenticating the data as well as the IP header. Instead of providing encrypting the data, it provides a hash which allows the data and the packet's IP header to be checked to ensure that the data was not altered with in transit. Although AH is an important component of the IPSec protocol suite, it is not being deployed as many as ESP (Malik, 2002). Mostly, IKE and ESP are implemented together. Figures 12 and 13 show both IPSec's AH and ESP protections.

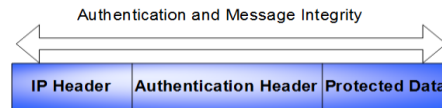


Figure 12: IPSec's AH protocol protection

Note: This figure is based on “Computer Network Security Protocols and Standards,” by Kizza (2005).

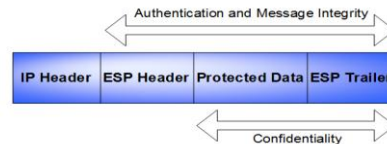


Figure 13: IPSec's ESP protocol protection

Note: This figure is based on “Computer Network Security Protocols and Standards,” by Kizza (2005).

Moreover, IPSec operates in two ways: Transport mode and Tunnel mode (Ioannidis, 2011). The Figure 14 indicates the packet format of transport mode and tunnel mode. In transport mode, only the payload of the IP packet is encrypted (Malik, 2002). An extra ESP or AH header will be inserted between the payload and its IP header once the ESP or AH is used. Transport mode requires the original IP header including addresses which can be routed by the router over the public network. Typically, transport mode is used for end-to-end communications. For example, transport mode can be used when an encrypted telnet or remote desktop session from a workstation to a server. Besides, in tunnel mode, a new IP header is generated and inserted in front of the ESP or AH header (Bantoft & Wouters, 2006). This new IP header includes the source and destination IP addresses of the two IPSec peers rather than the original host's IP addresses and the destination host's IP addresses. In general, tunnel mode is the most widely used mode in IPSec deployments especially in network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote access) and host-to-host communication (e.g. private chat).

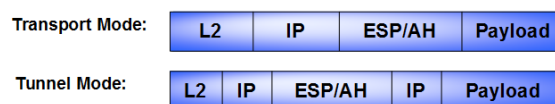


Figure 14: Packet format in transport mode and tunnel mode

Note: This figure is based on “Designing VPN Security,” by Cisco (2003).

IPSec has a lot of advantages. There are three major strengths made the IPSec VPN so popular among organizations and industrial (Csico System, 2004). Firstly, from the security aspect, IPsec utilizes a flexible collection of encryption and tunneling mechanisms to ensure the data privacy as they transport over the shared public infrastructure such as Internet. Peers are authenticated with digital certificates or preshared keys. Packets are dropped as long as they do not match to the security policy. Secondly, IPSec is easy to deploy. It can be implemented across any existing IP network with little or no change to the existing IP network infrastructure (Cisco, 2003). Thirdly, IPSec can take advantage of the Internet to reach any peers on the Internet as long as they have basic Internet connection. Therefore, the service provider does not need to invest extra infrastructure to support the IPSec VPN connection (Csico System, 2004).

Besides, one of the limitations of IPSec is that it only allows to encrypt and encapsulate the IP data (Malik, 2002). Hence, for the non-IP-based data, IPSec needs to be implemented in conjunction with an additional protocol which it is capable to deliver the non-IP traffic, such as GRE.

5.2.5 Secure Sockets Layer/ Transport Layer Security (SSL/TLS)

SSL stands for Secure Sockets Layer and was originally developed by Netscape Communications as a way to provide communication security over the Internet (Davies, 2011). SSL has been implemented in the major Web browsers such as Internet Explorer, Netscape, and Firefox. SSL protocol is a client/server protocol that provides basic security services to the communicating peers such as authentication, connection confidentiality services, and connection integrity services (Oppliger, 2009). SSL protocol evolved in three versions: SSL 1.0, SSL 2.0, and SSL 3.0. The TLS (Transport Layer Security) is structurally identical to the SSL protocol. TLS was developed based on the SSL 3.0. Usually, TLS 1.0 can be recognized as SSL 3.1 (Chou, 2002). The latest version of TLS is TLS 1.2, which is specified in RFC 5246 (Dierks & Rescorla, 2008). TLS operates in the same general manner as SSL. However, TLS uses stronger authentication and encryption protocols (Stewart & Chapple, 2011). Moreover, TLS is able to encrypt UDP and Session Initiation Protocol (SIP, which is a protocol associated with VoIP) connections.

SSL/TLS VPN is another secure solution for the enterprise cloud in securing end-to-end communication over the Internet (Park & Park, 2011). It establishes connectivity

using SSL/TLS, which operates at Level 4-5 (Transport Layer and Session Layer). Information is encapsulated at Level 6-7 (Presentation Layer and Application Layer). Hence, SSL/TLS VPN communicates at the highest levels in the OSI model (Fortinet, 2013). Moreover, SSL 3.0 operates in two stages: one is connection establishment; the other is data transfer (Weaver, 2006). In connection establishment state, authentication is required from users before allowing access so that only the authorized peers can establish the SSL/TLS VPN tunnel. To do so, SSL/TLS will encrypt the section between peers so that applications can exchange and authenticate user names and passwords without interfering by the eavesdroppers (Steinberg & Speed, 2005). In data transfer stage, the SSL/TLS tunnel will be activated and all the data will be encrypted before transmitting. SSL/TLS supports different encryption algorithms within each SSL/TLS session and only the SSL/TLS peers are able to read and understand the messages (Steinberg & Speed, 2005).

Besides, SSL/TLS VPN delivers three modes of SSL/TLS VPN access: clientless, thin client and tunnel mode (Cisco, 2012). Clientless mode provides secure connection to private web resources and web content. This mode is significantly useful for visiting most contents that you would like to access in a web browser such as Internet access, databases, and online tools that employ a web interface. Thin client mode enhances the abilities of the cryptographic functions of the web browser to access remotely to TCP-based applications such as Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, and Secure Shell (SSH) (Cisco, 2012). Tunnel mode enables remote users to connect to the internal network freely from anywhere by utilizing traditionally means of web-based access from computers or other terminal devices (Fortinet, 2013). This mode supports most IP-based applications, such as Microsoft Outlook, Microsoft Exchange, and Lotus Notes E-mail.

5.3 Routing

Routing plays an important role in providing the essential network connectivity between the users and the cloud so that the VPN connections can be established between them. Routing is the process of selecting a path used for forwarding the traffic from a source to each destination in a communication network (Hoang, 2012). Routing is operated via routing protocols which create and update routing table automatically and

consistently in every router in the network. Therefore, a packet can be forwarded to the right destination with the best route.

Routing can be classified as dynamic routing and static routing based on how the routing tables are built (Oki, Rojas-Cessa, Tatipamula, & Vogt, 2012). Dynamic routing means that the affected routers will update the routing table dynamically and automatically once a link failure occurs and they will determine an alternative route to deliver the data. The opposite of dynamic routing is static routing, which means the network administrators need to configure and update the routing table manually. It should be noticed that it is impossible for network administrators to manage all the routing tables immediately and consistently in the network if the network size grows large or/and the network condition changes.

The following sub-sections briefly review the routing algorithms and IP routing protocol.

5.3.1 Routing Algorithms

Routing algorithms are extremely important for dynamic routing protocols. This section reviews two important well-known routing algorithms: the distance vector routing algorithm and link state routing algorithm. The section also discusses how the router determines the best route, updates their topology information and maintains its routing table.

5.3.1.1 Distance Vector Routing Algorithm

Distance vector routing algorithm is also called Bellman-Ford (For the original designers) which it enables a router to inform its neighbors its distance to every routers in the network, commonly in terms of hop count (number of routers) (Hartpence, 2011). Each router in the network maintains a distance vector routing database for every destination network which it consists of the number of hops (known as cost) away from itself associated with the next hop IP address or interface. Distance vector routers periodically send the update messages to each router in the network to ensure the routing table is up-to-date as well as to maintain the relationship between each neighbor. Once the router receives the update message from its neighbor, it compares the current cost with the costs from the neighbor and selects the path with smaller cost. Only the shortest

path/paths from this router to the destination will be selected and wrote in the routing table. Example of distance vector protocol includes RIP (Routing Information Protocol).

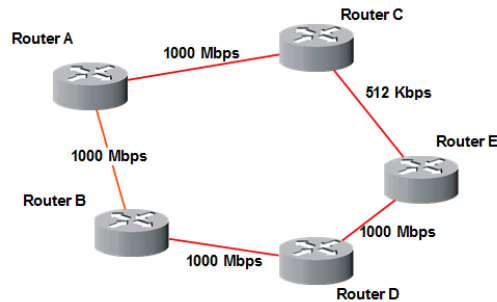


Figure 15: Operation of distance vector routing algorithm

Figure 15 illustrates how the distance vector router operates in path calculation. For instance, assume that Router A is going to forward a packet to Router E. There are two options for Router A to process the packet, one is $A \rightarrow C \rightarrow E$, the other is $A \rightarrow B \rightarrow D \rightarrow E$. Assume that all the routers in this example are running the same distance vector routing protocol, Router A knows that the costs to Router E via Router C is 2 and via Router B is 3 once Router A receives the update message from both Router B and Router C. After comparing the costs, Router A will choose the shortest path $A \rightarrow C \rightarrow E$ as the best route and update its routing table.

One of the disadvantages of distance vector routing algorithm is that router is difficult to make a decision based on the quality of the path (Hartpence, 2011). For instance, with the same example above, if the available bandwidth between Router C and Router E is 512kbps, selecting the route $A \rightarrow C \rightarrow E$ as the best route to Route E is not a wise decision for Router A because the traffic congestion occurs easily on the low speed link between Router C and Router E, which may result in high delay or connection failure. Moreover, distance vector routing protocols are slower than link state protocols in network convergence when any changes occurred in the network.

5.3.1.2 Link State Routing Algorithm

Link state routing algorithm is another fundamental routing algorithm utilized greater detail about the links or connection between routers in order to obtain the best route to the destination (Hartpence, 2011). Unlike the distance vector routing algorithm informs its neighbors its distance to every router in the network, link state routing algorithm sends the network topology information with the cost of each link to all routers in the network

(Hoang, 2012). Once the router receives the topology information from the neighbor, it updates this topology information in its local link state advertisement database (LSA database). Then, the router calculates the cost-effective paths to every destination independently by using the topology information in its LSA database and updates its routing table once the best route has been calculated. In other word, all routers calculate the shortest path based on link cost and construct the routing table based on its calculation digests. Additionally, after all the routers have updated their routing table, routers send “hello” message to its neighbors periodically to maintain the relationships and latest routing tables. This mechanism speeds up the network convergence when any changes occurred in the network. OSPF (Open Shortest Path First) is an example of the Link State Protocol.

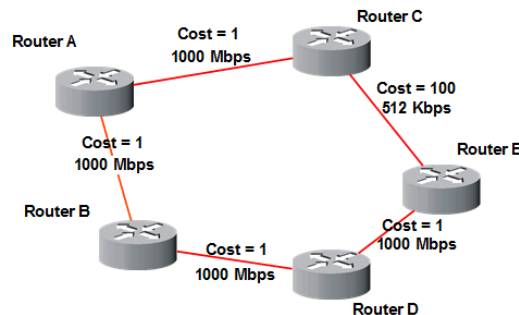


Figure 16: Operation of link state routing algorithm

The Figure 16 shows how the link state routers operate in its path selection. For example, assume that the Router A is trying to send a packet to Router E. In this case, there are still two options for Router A, one is $A \rightarrow C \rightarrow E$, and the other is $A \rightarrow B \rightarrow D \rightarrow E$. Assume all the routers in this example are using link state routing protocols. Router A receives the topology information messages from Router C which indicate that the cost to Router E via Router C is 100. Therefore, with regard to Router A, the total cost of the first option, $A \rightarrow C \rightarrow E$, is 101. Besides, Router A will also receive the topology information messages from Router B which show that the cost to Router E via Router B is 2. Hence, the total cost of the second option, $A \rightarrow B \rightarrow D \rightarrow E$, is 3. So, the Router A will select the second option, $A \rightarrow B \rightarrow D \rightarrow E$, as the best path to process the packet from Router A to Router E.

5.3.2 IP Routing Protocol

IP routing protocols are used to dynamically determine the optimal routes to forward data from a source to a destination by means of routers or networks (Oki, et al., 2012). IP routing protocol plays an important role in VPN construction because VPN can be established only if the network connectivity is available between two nodes.

In general, a routing protocol usually shares the information with neighbor routers and throughout the network (Oki, et al., 2012). Therefore, IP routing protocols enable routers to construct, maintain and update their routing table dynamically. The routing table includes the destination address associated with the corresponding output interface. Therefore, the router can send the packet to the right interface based on the routing table when a packet arrives at the router. Besides, the data will be delivered from the source to the destination in a hop-by-hop manner by following the routing table of each router on the node. Additionally, IP routing protocols, to a great extent, are classified as dynamic routing.

IP routing protocols can be classified into interior gateway routing protocols (IGP) and exterior gateway routing protocol (EGP) based on the operation areas. (Hoang, 2012). For example, The Figure 17 illustrates the relationships between IGP and EGP. IGP operates inside the AS whereas EGP operates between the ASs. An AS (Autonomous System) has been known as either a single network or a group of networks managed by either a network administrator or a group of administrator on behalf of a single administrative entity (Sosinsky, 2009). University, a business enterprise or a business division can be recognized as an AS. Besides, IGP includes RIP, OSPF, IS-IS (Intermediate System to Intermediate System), and EIGRP (Enhanced Interior Gateway Routing Protocol). On the other hand, BGP (Border Gateway Protocol) is one of the EGPs.

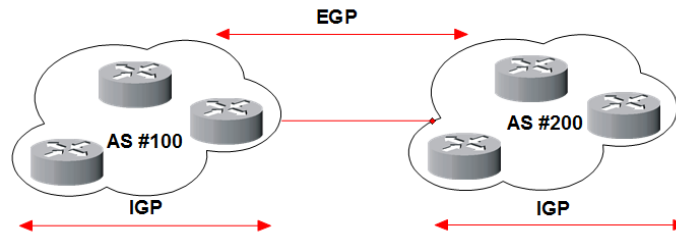


Figure 17: Interior gateway routing protocols (IGP) and exterior gateway routing protocol (EGP)

Note: This figure is based on “Advanced Internet Protocols, Services, and Applications,” by Oki, et al. (2012).

5.4 Conclusion

In this chapter, we reviewed the fundamentals of VPN, VPN protocols and its related technologies. The technologies we discussed above play extremely important role in delivering secure network solutions for the cloud users in accessing the cloud services. Specifically, tunneling technology enable the connection between the user and the cloud. Encryption and authentication technologies secure the connections. VPN protocols provide different deployment options and routing provides the essential network connectivity. These technologies are compulsory in applying secure network solutions in the cloud. In next chapter, the deployment process of secure network solutions will be explored.

6 SECURE NETWORK SOLUTIONS DEPLOYMENT

As discussed above, VPN is one of the popular secure network solutions used in cloud deployment in securing the cloud connections for cloud users. It has also been discussed that Data link layer VPNs can be developed using PPTP, L2TP protocol. Network Layer VPNs can be implemented by GRE, IPsec protocol. Application Layer VPNs can be constructed by SSL/TLS protocol. It is important to understand that each solution has its own deployment method and corresponding connection method to connect to the cloud from the consumer’s end. Moreover, the complexity of each implementation is different as well. Therefore, this chapter tries to observe the differences by implementing each solution in a test bed environment in order to answer the research questions.

The following sections explore the enterprise inter-cloud architecture, network topology, test bed set up, and deployment processes and connection method of each of the solutions.

6.1 Enterprise Inter-cloud Architecture

Dayananda and Kumar (2012) proposed an enterprise inter-cloud architecture as shown in Figure 18. Basically, in this enterprise inter-cloud computing architecture, it consists of three critical components: corporate cloud network, Internet and cloud network (Cloud A and Cloud B). Both corporate cloud network and cloud network are linked to the Internet. Each network can communicate to each other only if a proper solution has been implemented on each side of the network. This is because Cloud A, Cloud B and Corporate network are private networks and they cannot be accessed from the outside. Therefore, VPN is one of the popular solutions in this scenario because it is more economical than leased line and is secure and scalable (Cohen & Kaempfer, 2000). In this case, we decided to develop a test bed environment based on this architecture. In order to do so, the network topology needs to be carried out in advance.

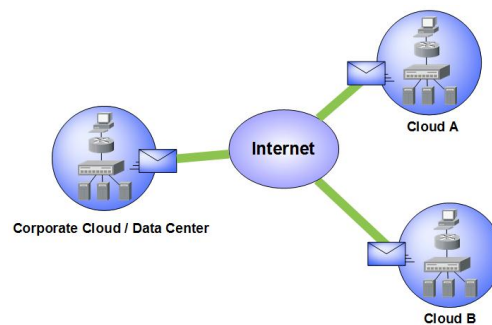


Figure 18: An enterprise inter-cloud architecture

Note: This figure is based on “Architecture for Inter-cloud Services Using IPsec VPN,” by Dayananda and Kumar (2012).

6.2 Network Topology

Network topology is one of the critical components in establishing the test bed environment. Network topology is recognized as the shape of the computers and other network components are connected to each other (Lowe, 2012). It is also considered as the topological structure of a network, which can be depicted physically or logically (Chiang & Yang, 2004). Physical topology means the placement of the network components such as device location and cable installation. Logical topology outlines how

data flows within a network, regardless of its physical design. Different network topologies offer different advantages and disadvantages. A poor network topology may result in traffic congestion and network flapping. Therefore, creating a suitable network topology is critical in this study.

6.3 Test Bed Setup

According to the aforementioned enterprise inter-cloud computing architecture, we propose our network topology for our experiment, as shown in Figure 19. The topology is composed of three critical components: Enterprise, Internet and Cloud. Enterprise acts as the cloud consumer in this architecture. Cloud plays the role of cloud provider. Supposing all the cloud services are stored on the cloud server, a VPN tunnel needs to be constructed between each edge router so that the users from the enterprise network can access the cloud services on the cloud side. For the purpose of collecting the reliable results from the experiments, we are using Cisco 1800 series routers to simulate the Enterprise Edge, Internet and Cloud Provider based on Figure 19.

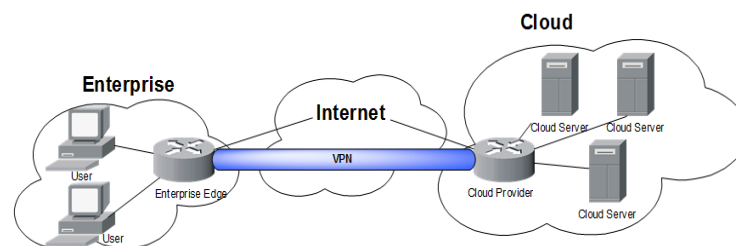


Figure 19: Network topology

Based on the network topology above, we also propose the physical topology as shown in Figure 20. The physical topology illustrates the physical connections between each network component.

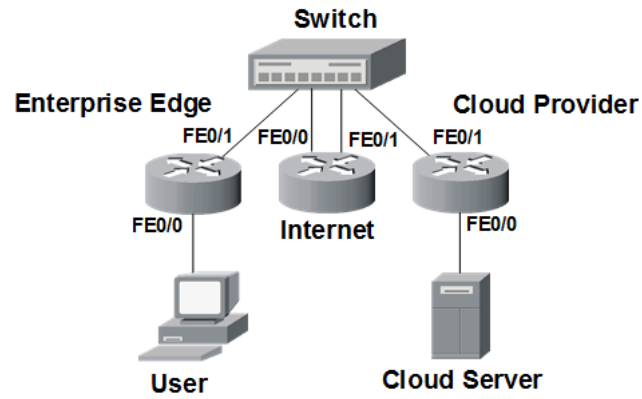


Figure 20: Physical topology

Referring to Figure 20, all the routers (Enterprise Edge, Internet and Cloud Provider) are connected to a switch using Fast Ethernet interface with 100Mbps bandwidth. User and Cloud Server are directly connected to Enterprise Edge and Cloud Provider respectively. Additionally, for experimental purposes, we also assign an IP address to each interface on each device based on Figure 20. The following Table 10 summarizes the interface and its corresponding IP address.

Table 10: Interface and Its corresponding IP address

Device	Interface	IP Address
User	User	192.168.1.1/24
Enterprise Edge	FastEthernet0/0	192.168.1.254/24
	FastEthernet0/1	202.12.12.1/24
Internet	FastEthernet0/0	202.12.12.2/24
	FastEthernet0/1	202.23.23.2/24
Cloud Provider	FastEthernet0/0	192.168.3.254/24
	FastEthernet0/1	202.23.23.3/24
Cloud Server	Cloud Server	192.168.3.1/24

Furthermore, there are two PC running Windows 7 operating system used to simulate the User and Cloud Server respectively. The relationship between the operating system and the VirtualBox application is showing in Figure 21. VirtualBox is running on top of the Windows 7 to emulate different operating systems. For example, Windows XP is emulated by the VirtualBox on the User's PC as the testing operating system. Windows 2003 is used as the Cloud Server. The cloud applications are installed in Windows 2003 to provide cloud services to the user. The VPN solutions will be applied on both edge routers to establish the secure connection so that the user can access the cloud services stored on the cloud. Besides, the performance measurement tools will be installed on both Window XP and Windows 2003. The performance evaluation will take place from the user side to the cloud server and all the experimental results will be collected on the user side in Windows XP environment.

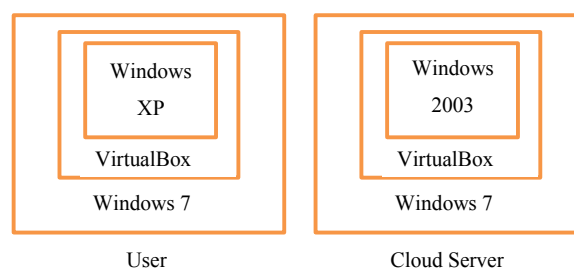


Figure 21: Relationship between Windows 7 and VirtualBox

6.4 Deployment Process

According to the Figure 19, in order to gain access to the cloud service stored on the Cloud, VPN can be implemented on both Enterprise Edge router and Cloud Provider router to provide secure connections between Enterprise Network and Cloud Network. The secure network solutions can be applied by utilizing different VPN protocols such as

PPTP, L2TP, GRE, IPSec and SSL/TLS to develop Data link layer VPNs, Network Layer VPNs and Application Layer VPNs. The following sub-sections include the detailed configurations of each solution and the verification of the connectivity. It should be noticed that only the most popular encryption algorithms will be applied in our experiments.

6.4.1 PPTP VPN Solution

The following Table 11 highlights the most important configurations of PPTP VPN solution on Enterprise Edge router and Cloud Provider router. Based on Table 11, it should be noted that static routing (ip route 0.0.0.0 0.0.0.0 202.12.12.2 or 202.23.23.2) associated with NAT technology has been deployed on both sides of the router, which enables the devices inside their private network to access the Internet. Moreover, PPTP VPN configurations only need to be configured on the cloud provider router, which means that the enterprise does not need to manage the PPTP VPN. Besides, the username and the password need to be defined and applied on the cloud provider router in advance in order to authenticate the remote user.

Table 11: PPTP VPN solution on enterprise edge router and cloud provider router

Enterprise Edge Router	Cloud Provider Router
interface FastEthernet0/0	vpdn enable
ip nat inside	!
!	vpdn-group 1
interface FastEthernet0/1	! Default PPTP VPDN group
ip nat outside	accept-dialin
!	protocol pptp
ip route 0.0.0.0 0.0.0.0	virtual-template 1
202.12.12.2	!
!	username test password 0 test
ip nat inside source list 1 interface	!
FastEthernet0/1 overload	interface FastEthernet0/0
!	ip nat inside
access-list 1 permit 192.168.1.0	!
0.0.0.255	interface FastEthernet0/1
	ip nat outside
	!
	interface Virtual-Template1
	ip unnumbered FastEthernet0/1
	peer default ip address pool test
	no keepalive
	ppp encrypt mppe auto
	ppp authentication ms-chap-v2 ms-chap
	eap pap
	!
	ip local pool test 192.168.3.3 192.168.3.5
	!
	ip route 0.0.0.0 0.0.0.0 202.23.23.2
	!
	ip nat inside source list 1 interface
	FastEthernet0/1 overload
	!
	access-list 1 permit 192.168.3.0 0.0.0.255

After successfully applying the configurations on the router, cloud users still cannot access the cloud server unless the Virtual Private Network Connection has been set up appropriately in Window XP, as shown in the following Figure 22.

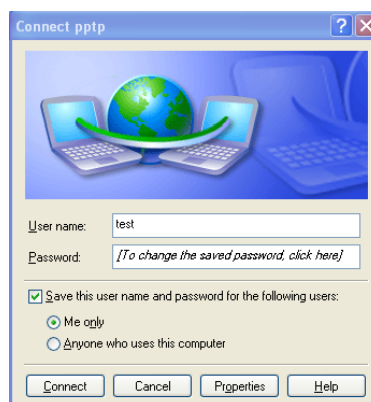
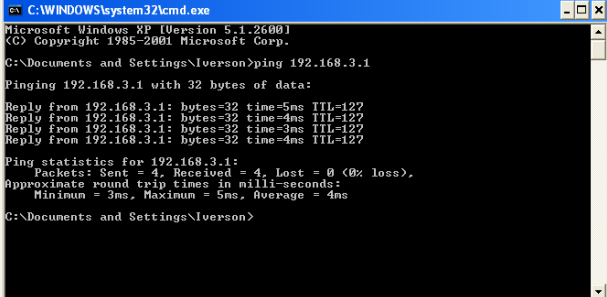


Figure 22: Virtual private network connection for PPTP VPN

It should be noted that the User name and Password shown on the Figure 22 need to be the same as the username and password defined on the cloud provider router. In other words, the cloud provider needs to provide the authentication to the cloud user so that the secure network connection between the user and the cloud can be established successfully. Once the connection has been set up, the user is able to access the cloud server and use the available cloud services on the cloud. Besides, all the data from the user to the cloud is encrypted in this connection in order to protect the privacy of the conversation.

In order to test the connectivity between the user and the cloud server, in general, one of the simplest ways is to use the Ping service embedded in Windows operating system. The following Figure 23 shows the Ping results from the user. It indicates that the user can reach the cloud server at the IP address of 192.168.3.1. It also implies that the PPTP VPN connection between user and the cloud server has been established successfully.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\lverson>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.3.1: bytes=32 time=5ms TTL=127
Reply from 192.168.3.1: bytes=32 time=4ms TTL=127
Reply from 192.168.3.1: bytes=32 time=3ms TTL=127
Reply from 192.168.3.1: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms
C:\Documents and Settings\lverson>

```

Figure 23: PPTP VPN connectivity testing

6.4.2 L2TP with IPSec Security VPN Solution

The following Table 12 summarizes the core configurations of L2TP with IPSec security VPN solution on Enterprise Edge router and Cloud Provider router. It shows that static routing associated with NAT technology has also been configured on both sides of the router. The configurations of L2TP VPN are similar to PPTP VPN, which only need to be applied on the cloud provider router. The cloud provider is responsible for the VPN maintenance and management. The username and password also need to be defined on the cloud provider router in advance for the remote users. One of the differences between L2TP VPN and PPTP VPN is that the L2TP can use IPSec to provide stronger authentication and encryption for the VPN traffic.

Table 12: L2TP with IPSec security VPN solution on enterprise edge router and cloud provider router

Enterprise Edge Router	Cloud Provider Router
interface FastEthernet0/0	vpdn enable
ip nat inside	!
!	vpdn-group 1
interface FastEthernet0/1	! Default L2TP VPDN group
ip nat outside	accept-dialin
!	protocol l2tp
ip route 0.0.0.0 0.0.0.0	virtual-template 1
202.12.12.2	no l2tp tunnel authentication
!	!
ip nat inside source list 1 interface	username test privilege 15 password 0 test
FastEthernet0/1 overload	!
!	crypto isakmp policy 10
access-list 1 permit 192.168.1.0	encr 3des
0.0.0.255	hash md5
	authentication pre-share
	group 2
	crypto isakmp key cisco address 0.0.0.0
	0.0.0.0 no-xauth
	!
	crypto ipsec transform-set MYSET esp-
	3des esp-md5-hmac
	mode transport
	!
	crypto dynamic-map MYMAP 10
	set transform-set MYSET
	!
	crypto map L2TP-MAP 10 ipsec-isakmp
	dynamic MYMAP
	!
	interface FastEthernet0/0
	ip nat inside
	!
	interface FastEthernet0/1
	ip nat outside
	crypto map L2TP-MAP
	!
	interface Virtual-Template1
	ip unnumbered FastEthernet0/1
	peer default ip address pool test
	no keepalive
	ppp encrypt mppe auto
	ppp authentication ms-chap ms-chap-v2
	!
	ip local pool test 192.168.3.100
	192.168.3.200
	ip route 0.0.0.0 0.0.0.0 202.23.23.2
	!
	ip nat inside source list 1 interface
	FastEthernet0/1 overload
	!
	access-list 1 permit 192.168.3.0 0.0.0.255

Once the configurations have been applied on both sides of the router correctly, the user needs to create the Virtual Private Network Connection to connect to the cloud

server as well. However, with IPsec technology, some parameters in Virtual Private Network Connection need to be modified in order to support L2TP VPN with IPsec, which is as shown in Figure 24.

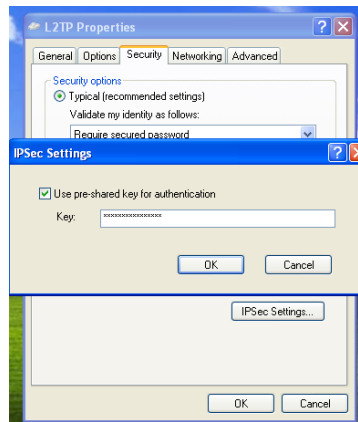


Figure 24: IPsec setting in virtual private network connection for L2TP VPN

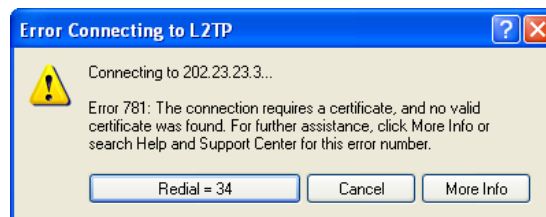


Figure 25: Error message from L2TP connection without pre-share key setting

Firstly, the IPsec uses pre-share key as the authentication method, therefore, the pre-share key needs to be input manually in IPsec setting under L2TP VPN connection security setting, as shown in Figure 24. Otherwise, it will cause an error message which requires a certificate for the connection, and no valid certificate can be found, as shown in Figure 25.

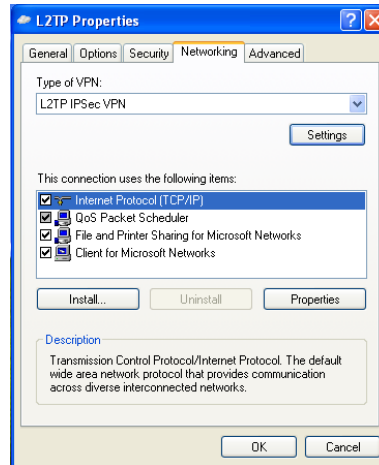


Figure 26: VPN Type setting in virtual private network connection for L2TP VPN

Secondly, according to Figure 26, the VPN type can be modified from Automatic to L2TP IPsec VPN under the networking setting. This is not compulsory. However, it will cause an error message during the L2TP VPN initiation if PPTP VPN has also been deployed on the cloud provider router. Therefore, the best way to avoid the potential problems is to select the right VPN type.

Once the parameters have been modified correctly, the L2TP VPN connection can be established successfully between the user and the cloud. The traffic inside this VPN tunnel will be encrypted by using IPsec. Besides, Ping service can also be used for the connectivity testing.

6.4.3 GRE with IPsec Security VPN Solution

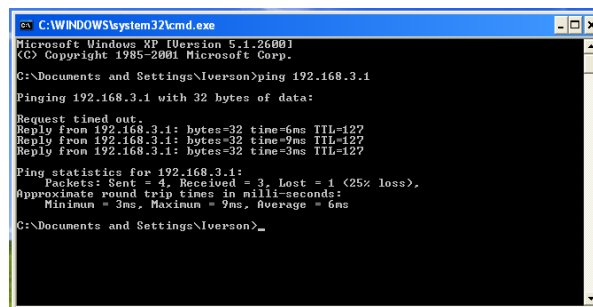
The following Table 13 illustrates the primary configurations of GRE with IPsec security VPN solution on Enterprise Edge router and Cloud Provider router. In this solution, NAT technology and static routing provide the connectivity for the user to access the Internet. Moreover, GRE tunnel has been set up by using virtual tunnel interface. The IPsec has been applied on the tunnel interface to provide security. Dynamic routing protocol OSPF has also been used to provide network connectivity between enterprise private network (192.168.1.0/24) and cloud private network (192.168.3.0/24). This solution is also suitable to be used to develop a private cloud network, which can be deemed as the branch office and the cloud provider network can be recognized as the head office.

Table 13: GRE with IPsec security VPN solution on enterprise edge router and cloud provider router

Enterprise Edge Router	Cloud Provider Router
crypto isakmp policy 10	crypto isakmp policy 10
encr 3des	encr 3des
hash md5	hash md5
authentication pre-share	authentication pre-share
group 2	group 2
crypto isakmp key cisco address	crypto isakmp key cisco address
202.23.23.3	202.12.12.1
!	!
crypto ipsec transform-set	crypto ipsec transform-set
MYSET esp-3des esp-md5-hmac	MYSET esp-3des esp-md5-hmac
!	!
crypto map GRE 10 ipsec-isakmp	crypto map GRE 10 ipsec-isakmp
set peer 202.23.23.3	set peer 202.12.12.1
set transform-set MYSET	set transform-set MYSET
match address VPN	match address VPN
!	!
interface Tunnel0	interface Tunnel0
ip address 13.13.13.1	ip address 13.13.13.3
255.255.255.0	255.255.255.0
tunnel source 202.12.12.1	tunnel source 202.23.23.3
tunnel destination 202.23.23.3	tunnel destination 202.12.12.1
crypto map GRE	crypto map GRE
!	!
interface FastEthernet0/0	interface FastEthernet0/0
ip nat inside	ip nat inside
!	!
interface FastEthernet0/1	interface FastEthernet0/1
ip nat outside	ip nat outside
!	!
router ospf 100	router ospf 100
router-id 1.1.1.1	router-id 3.3.3.3
log-adjacency-changes	log-adjacency-changes
network 13.13.13.0 0.0.0.255 area	network 13.13.13.0 0.0.0.255 area
0	0
network 192.168.1.0 0.0.0.255	network 192.168.3.0 0.0.0.255
area 0	area 0
!	!
ip route 0.0.0.0 0.0.0.0	ip route 0.0.0.0 0.0.0.0
202.12.12.2	202.23.23.2
!	!
ip nat inside source list 1 interface	ip nat inside source list 1 interface
FastEthernet0/1 overload	FastEthernet0/1 overload
!	!
ip access-list extended VPN	ip access-list extended VPN
permit ip 192.168.1.0 0.0.0.255	permit ip 192.168.3.0 0.0.0.255
192.168.3.0 0.0.0.255	192.168.1.0 0.0.0.255
!	!
access-list 1 permit 192.168.1.0	access-list 1 permit 192.168.3.0
0.0.0.255	0.0.0.255

After the configurations on both sides of the routers have been successfully applied, the VPN connection will be initiated automatically as long as the user within the enterprise network (192.168.1.0/24) starts a conversation to the cloud server at cloud network

(192.168.3.0/24). All the traffic will be encrypted by IPSec once the VPN connection has been established. The VPN connection will be terminated in a period of time if there is no conversation alive. The Figure 27 illustrates the Ping results from the user to the cloud server. The first packet is always dropped because of the request time out. It means that the IPSec initiation process is taking place and needs a period of time to complete the IPSec initiation, which results in the request time out (Cisco, 2003). The VPN connection between the user and the cloud server has been established once the rest of the packets are transmitted successfully.



```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Iverson>ping 192.168.3.1
Pinging 192.168.3.1 with 32 bytes of data:
Request timed out.
Reply from 192.168.3.1: bytes=32 time=6ms TTL=127
Reply from 192.168.3.1: bytes=32 time=9ms TTL=127
Reply from 192.168.3.1: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 9ms, Average = 6ms
C:\Documents and Settings\Iverson>

```

Figure 27: GRE with IPSec security VPN connectivity testing

6.4.4 IPSec VPN Solution

The following Table 14 shows the configurations of IPSec VPN solution on Enterprise Edge router and Cloud Provider router. It should be noted that NAT technology has been utilized on both sides of the routers as well as the static routing. Therefore, static NAT maps (ip nat inside/outside source static) need to be defined in advance to allow the IPSec initiations between these two routers. Besides, additional access-lists (access-list 100) need to be applied after the static NAT maps in order to avoid the private IP address being translated into public IP address by NAT, which results in VPN connection failure. To conclude, IPSec VPN cannot be established without these additional static NAT maps and access-lists if NAT technology has been activated.

Table 14: IPSec VPN solution on enterprise edge router and cloud provider router

Enterprise Edge Router	Cloud Provider Router
crypto isakmp policy 10	crypto isakmp policy 10
encr 3des	encr 3des
hash md5	hash md5
authentication pre-share	authentication pre-share
group 2	group 2
crypto isakmp key cisco address	crypto isakmp key cisco address
202.23.23.3	202.12.12.1
!	!
crypto ipsec transform-set	crypto ipsec transform-set
MYSET esp-3des esp-md5-hmac	MYSET esp-3des esp-md5-hmac
!	!
crypto map MYMAP 10 ipsec-	crypto map MYMAP 10 ipsec-
isakmp	isakmp
set peer 202.23.23.3	set peer 202.12.12.1
set transform-set MYSET	set transform-set MYSET
match address VPN	match address VPN
!	!
interface FastEthernet0/0	interface FastEthernet0/0
ip nat inside	ip nat inside
!	!
interface FastEthernet0/1	interface FastEthernet0/1
ip nat outside	ip nat outside
crypto map MYMAP	crypto map MYMAP
!	!
ip route 0.0.0.0 0.0.0.0	ip route 0.0.0.0 0.0.0.0
202.12.12.2	202.23.23.2
!	!
ip nat inside source list 100	ip nat inside source list 100
interface FastEthernet0/1 overload	interface FastEthernet0/1 overload
ip nat inside source static esp	ip nat inside source static esp
192.168.1.0 interface FastEthernet0/0	192.168.3.0 interface FastEthernet0/0
ip nat inside source static udp	ip nat inside source static udp
192.168.1.0 500 interface	192.168.3.0 500 interface
FastEthernet0/1 500	FastEthernet0/1 500
!	!
ip access-list extended VPN	ip access-list extended VPN
permit ip 192.168.1.0 0.0.0.255	permit ip 192.168.3.0 0.0.0.255
192.168.3.0 0.0.0.255	192.168.1.0 0.0.0.255
!	!
access-list 100 deny ip	access-list 100 deny ip
192.168.1.0 0.0.0.255 192.168.3.0	192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255	0.0.0.255
access-list 100 permit ip	access-list 100 permit ip
192.168.1.0 0.0.0.255 any	192.168.3.0 0.0.0.255 any

Once the above configurations have been applied, VPN will be turned on automatically once it meets the requirements, which is similar to GRE with IPSec VPN solution. The same method can be used to test the connectivity.

6.4.5 SSL/TLS VPN Solution

The following Table 16 indicates the critical configurations of SSL/TLS VPN solution on Enterprise Edge router and cloud provider router. The VPN configurations only need

to be applied on the cloud provider router. Besides, a Cisco SSL VPN Client needs to be installed on the cloud provider router in advance.

Table 15: SSL/TLS VPN solution on enterprise edge router and cloud provider router

Enterprise Edge Router	Cloud Provider Router
interface FastEthernet0/0	hostname R3
ip nat inside	!
!	aaa new-model
interface FastEthernet0/1	!
ip nat outside	aaa authentication login webvpn
!	local
ip route 0.0.0.0 0.0.0.0	!
202.12.12.2	username test privilege 15
	password 0 test
ip nat inside source list 1 interface	!
FastEthernet0/1 overload	interface FastEthernet0/0
!	ip nat inside
access-list 1 permit 192.168.1.0	!
0.0.0.255	interface FastEthernet0/1
	ip nat outside
	!
	ip local pool sslvpn-pool
	192.168.3.100 192.168.3.200
	ip route 0.0.0.0 0.0.0.0
	202.23.23.2
	!
	ip nat inside source list 1 interface
	FastEthernet0/1 overload
	!
	access-list 1 permit 192.168.3.0
	0.0.0.255
	!
	webvpn gateway VPNGW
	ip address 202.23.23.3 port 443
	ssl trustpoint TP-self-signed-
	55817042
	inservice
	!
	webvpn install svc
	flash:/webvpn/svc_1.pkg sequence 1
	!
	webvpn context WEBTEXT
	ssl authenticate verify all
	!
	policy group SSLVPN-POLICY
	functions svc-enabled
	banner "This is Cisco IOS SSL
	VPN"
	svc address-pool "sslvpn-pool"
	default-group-policy SSLVPN-
	POLICY
	aaa authentication list webvpn
	gateway VPNGW
	inservice

After the configurations on the cloud provider router have been correctly applied, the user is required to activate the VPN connection by using the Internet browser. By doing this, `https://202.23.23.3` is the address to be used in the user's browser. A security alert message will pop out once the user tries to connect to this address. The message requires the certificate being installed on user's devices in order to provide authentication, as shown in Figure 28.



Figure 28: Security alert from SSL/TLS VPN connection

The Cisco SSL VPN Service login page will be displayed on the user's browser after the certificate is correctly installed, as shown in Figure 29. The user can only login to the services by using the username and the password pre-defined on the cloud provider router. User's homepage will be displayed once the user passed the login authentication, as shown in Figure 30.



Figure 29: Cisco SSL VPN service home page

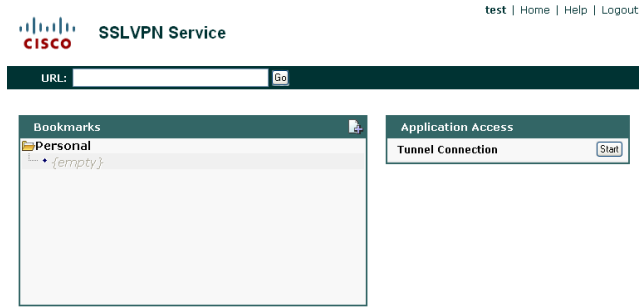


Figure 30: Cisco SSL VPN service user homepage

The SSL/TLS VPN can be established by simply clicking on the “Start” button of Tunnel Connection on the right hand side. The web page will be redirected to ActiveX Control, which requires the user to download the software called stcweb.cab. It also asks the user to install the certificate once the software has been downloaded. After the software and the certificate have been successfully installed, the VPN connection will be established and ready to be used, as shown in Figure 31. The Figure 32 shows the Ping results from the user.

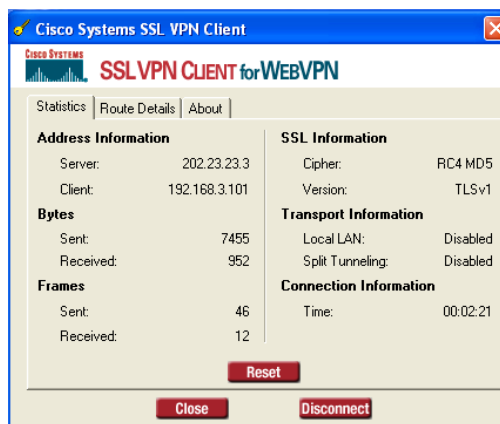


Figure 31: SSL/TLS VPN connection summary

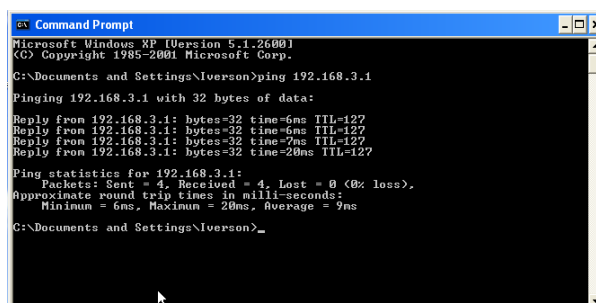


Figure 32: SSL/TLS VPN connectivity testing

6.5 Summary

In this chapter, we proposed that our own inter-cloud architecture to meet our research aim. Our test bed environment was developed based on our inter-cloud architecture by using Cisco routers, computers and VirtualBox software. Five popular secure network solutions were implemented on the test bed one after another. The following Table summarizes each solution with networking technologies used in our deployments. Besides, the complete configurations as well as the connection method of each solution have been addressed in this chapter.

Table 16: Networking technologies used in deployment

	NAT	Static Routing	Encryption & Authentication	Additional Technology
PPTP VPN	✓	✓	mppe, ms-chap-v2	---
L2TP with IPSec VPN	✓	✓	3des, md5, HMAC	---
GRE with IPSec VPN	✓	✓	3des, md5, HMAC	OSPF
IPSec VPN	✓	✓	3des, md5, HMAC	NAT map
SSL/TLS VPN	✓	✓	AAA Authentication	Cisco SSL VPN Client

In the next chapter, the research results will be presented as well as the analysis and discussion of the research outcomes.

7 RESULTS AND ANALYSIS

In this chapter, we present the findings of this research. Each of the most popular secure network solutions was implemented on the Cisco routers and the measurements were taken on Windows operating systems such as Windows XP and Windows 2003. Moreover, in order to ensure the integrity of the measurement values, multiple runs were executed for sufficient duration. Re-runs were executed if measurement values fell outside of 95% confidence interval.

For throughput performance evaluation, we used Jperf as the measurement tool to exchange traffic between the user and the cloud server. Two measurements were operated. One is TCP throughput measurement, the other is UDP throughput measurement. In each measurement, the same amount of traffic was exchanged. For example, user sent 100 packets in 100 seconds to the cloud server. The Jperf listed the throughput information of each transmitted packet and the average throughput at the end of the list once the tests were completed. TCP and UDP throughput values were converted into the charts as shown in Figure 33 and 34 respectively. Table 17 summarizes the average throughput of TCP and UDP for each solution.

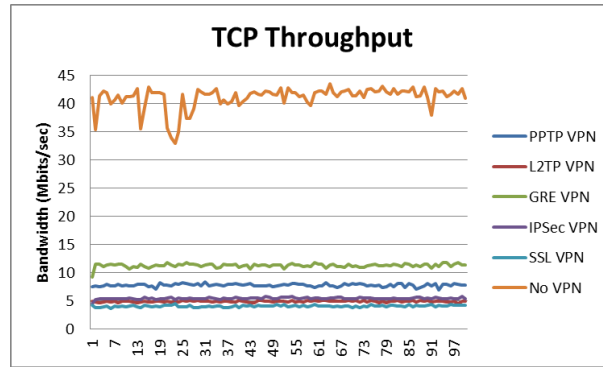


Figure 33: TCP throughput summary

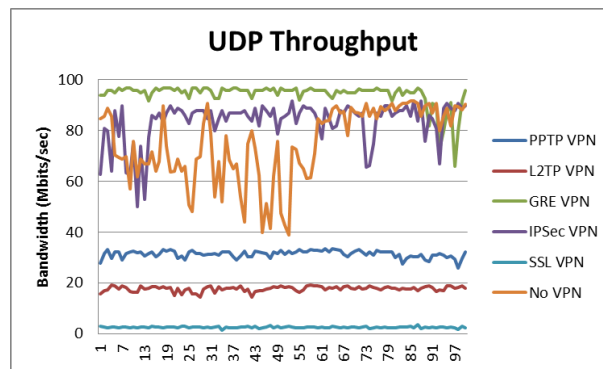


Figure 34: UDP throughput summary

Table 17: Average throughput of TCP and UDP

	TCP Throughput	UDP Throughput
No VPN	41.1 Mbits/sec	75.0 Mbits/sec
PPTP VPN	7.74 Mbits/sec	31.3 Mbits/sec
L2TP with IPSec Security VPN	4.85 Mbits/sec	17.7 Mbits/sec
GRE with IPSec Security VPN	11.2 Mbits/sec	94.1 Mbits/sec
IPSec VPN	5.39 Mbits/sec	83.6 Mbits/sec
SSL/TLS VPN	4.02 Mbits/sec	2.48 Mbits/sec

Table 17 illustrates that an average data rate of 41.1 Mbits/sec was achieved without VPN, which approximately corresponds to the maximum TCP throughput that can be reached by means of 100 Mbit fast Ethernet connections. There was a dramatic loss of performance when VPN solutions were implemented. In our experiment, No VPN solution meant that all the routers were running OSPF routing protocol to connect each other without taking the public IP and private IP into consideration. In other words, the private IP could be routed over the public environment in this experiment which was not possible in the real environment. Therefore, the data extracted from this solution was only used as a reference in comparing different secure network solutions.

Based on Table 17 and Figure 33, with GRE VPN, the TCP throughput was on average approximately 11.2 Mbits/sec after the initial ramping up, which was the best performance in TCP throughput measurement. PPTP VPN values were the second best in our TCP throughput measurements with an average of 7.74 Mbits/sec. Moreover, IPsec VPN was slightly better than L2TP VPN with about 5.39 Mbits/sec and 4.85 Mbits/sec respectively. However, SSL VPN values were the poorest in our experiments with an average of 4.02 Mbit/sec TCP throughput. Therefore, rankings from the best solution to the poorest solution in our TCP throughput measurements were GRE VPN, PPTP VPN, IPsec VPN, L2TP VPN and SSL/TLS VPN.

However, the order was different in UDP throughput measurement. Based on Table 17 and Figure 34, the best performance in UDP throughput measurement was GRE VPN with an average of 94.1 Mbits/sec in 100 tests, which was even better than the No VPN environment with 75.0 Mbits/sec. IPsec was the second best in this measurement with 83.6 Mbits/sec on average. PPTP VPN was better than L2TP with approximate 31.3 Mbits/sec and 17.7 Mbits/sec respectively. SSL VPN was the poorest in UDP throughput performance measurement in our experiment with only 2.48 Mbits/sec, which was nearly 38 times worse than GRE VPN. Hence, the order of the UDP throughput measurements from the best solution to the poorest solution was: GRE VPN, IPsec VPN, PPTP VPN, L2TP VPN and SSL/TLS VPN.

From the throughput measurements, the conclusion can be made that GRE with IPsec security VPN is the best in throughput performance while the SSL/TLS VPN is the worst. GRE VPN is about 1.4 times better than PPTP VPN, about 2 times greater than IPsec VPN and L2TP VPN and more than 2.7 times more effective than SSL/TLS VPN in the TCP throughput measurement. Moreover, GRE with IPsec security VPN is about 1.12 times faster than IPsec VPN. It is 3 times and 5 times quicker than PPTP VPN and L2TP respectively and more than 37 times more effective than SSL VPN in UDP throughput measurement based on our experimental data. Indisputably, GRE VPN is the best in the throughput measurement and SSL VPN is the worst.

On the other hand, for latency measurement, we used Colasoft Ping to test the network delay between the user and the cloud server. The values were collected by sending 100 packets from the user to the cloud server in each secure network solution. The following Figure 35 – 40 summarize the measurement values of each solution.

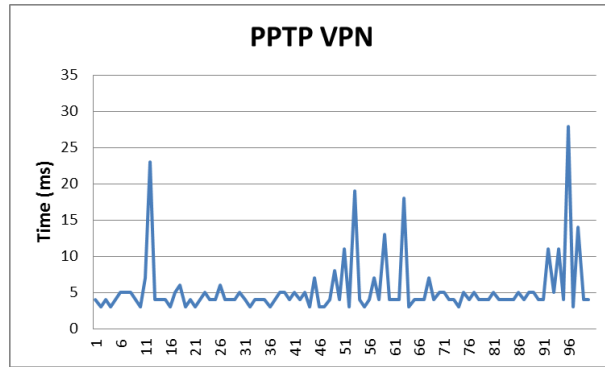


Figure 35: Latency of PPTP VPN

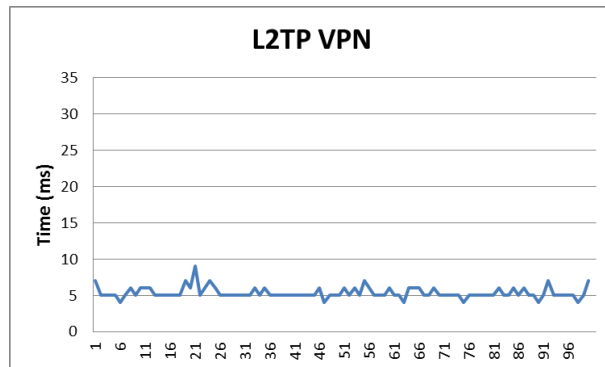


Figure 36: Latency of L2TP VPN

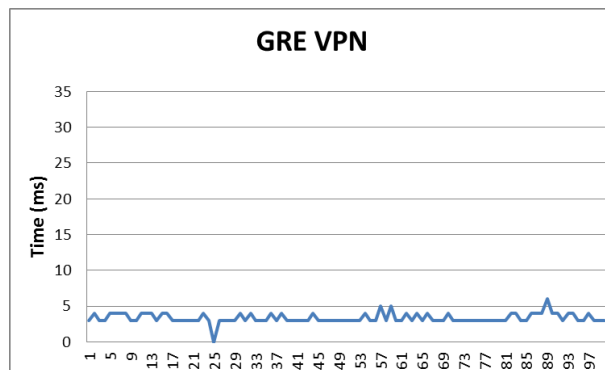


Figure 37: Latency of GRE VPN

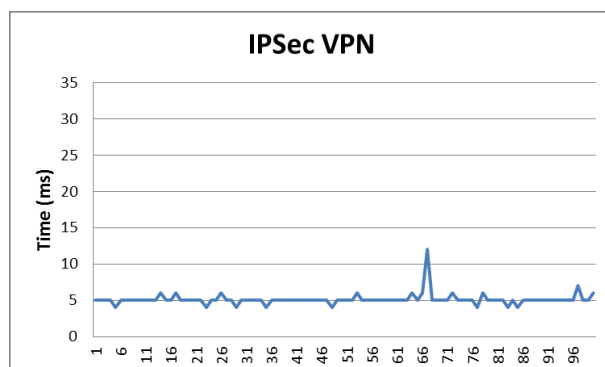


Figure 38: Latency of IPsec VPN

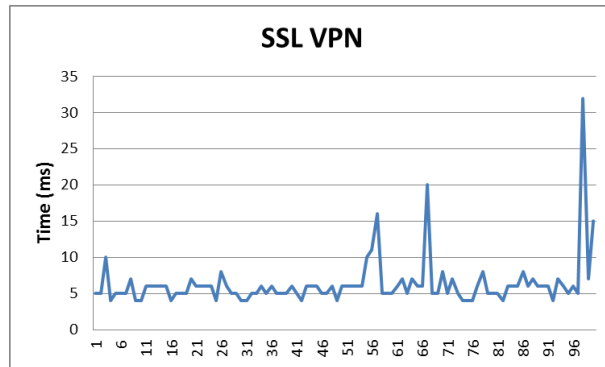


Figure 39: Latency of SSL VPN

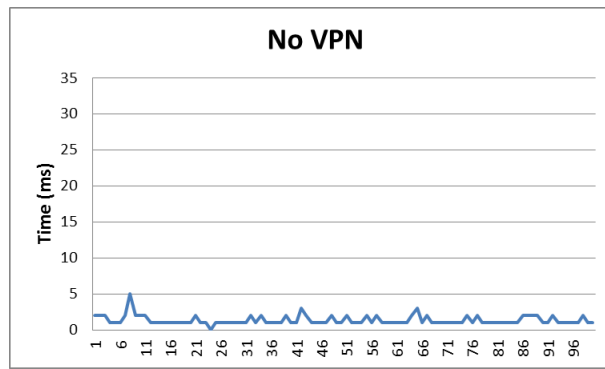


Figure 40: Latency of No VPN

Table 18: Latency measurement summary

Solution	Response Time	Minimum	Maximum	Average
No VPN		1ms	5ms	1ms
PPTP VPN		3ms	28ms	5ms
L2TP with IPsec Security VPN		4ms	9ms	5ms
GRE with IPsec Security VPN		3ms	6ms	3ms
IPsec VPN		4ms	12ms	5ms
SSL/TLS VPN		4ms	32ms	6ms

Figure 40 and Table 18 show that an average response time of 1ms was achieved without VPN, which approximately corresponds to the maximum response time that can be reached by means of 100 Mbit fast Ethernet connections. Apart from this, GRE VPN is the best in latency performance with an average response time of 3ms, minimum response time of 3ms and maximum response time of 6ms. PPTP VPN, L2TP VPN and IPsec VPN have the same average response time of 5ms in our experiments. However, L2TP VPN values are comparatively better than PPTP VPN values because the maximum response time of L2TP VPN is 9ms, which is lower than PPTP VPN with 28ms. The minimum

response time of L2TP VPN is higher than PPTP VPN, which are 4ms and 3ms respectively. Besides, the fluctuation of L2TP VPN is small compared with PPTP VPN based on Figure 35 and 36. Hence, L2TP VPN is comparatively better than PPTP VPN in the latency measurement. The minimum response time of IPsec VPN is 4ms, which is the same as L2TP VPN. However, IPsec VPN is slightly better than L2TP VPN because there is less fluctuation than L2TP VPN based on Figure 36 and 38, despite that the maximum response time of IPsec VPN is higher than L2TP VPN, which is 12ms. The poorest performance value in latency measurement is SSL/TLS VPN with an average response time of 6ms while the minimum and maximum response time is 4ms and 32 respectively. To sum up, GRE VPN can provide the lowest latency connection to the user and SSL/TLS VPN solution has the highest latency measurement values in our experiments.

The following Table 19 ranks the performance of each VPN solution based on the results and discussions above. The table illustrates that the GRE with IPsec security VPN has the best ranking of ① in TCP throughput, UDP throughput and latency measurements. Therefore, we ranked GRE VPN with ① in overall. On the contrary, the SSL/TLS VPN solution has the poorest performance in our experiments so it has been ranked ⑤ in overall. IPsec VPN has two rankings of ② in UDP throughput and Latency with a ranking of ③ in TCP throughput measurement and thus it has been given the ranking of ② in overall. PPTP VPN is slightly better than L2TP VPN with the ranking of ② in TCP throughput compared to ④ in L2TP VPN, ③ in UDP throughput compared to ④ in L2TP VPN and is comparatively lower than L2TP VPN in latency measurement with ranking of ④ compared to ranking of ③. Therefore, the PPTP VPN is ranked ③ in overall and L2TP VPN is ④.

Table 19: Performance rankings for each solution

	TCP Throughput	UDP Throughput	Latency	Overall
PPTP VPN	②	③	④	③
L2TP with IPsec Security VPN	④	④	③	④
GRE with IPsec Security VPN	①	①	①	①
IPsec VPN	③	②	②	②
SSL/TLS VPN	⑤	⑤	⑤	⑤

In order to answer the research questions, we summarize all the findings from our experiments laid out in Table 20.

Table 20: Results summary

	PPTP VPN	L2TP VPN	GRE VPN	IPSec VPN	SSL/TLS VPN
Type of the VPN	Data Link Layer VPN	Data Link Layer VPN	Network Layer VPN	Network Layer VPN	Application Layer VPN
VPN Configurations Required on the Enterprise Router	NO	NO	YES	YES	NO
Deploy Difficulty	Very Easy	Easy	Very Difficult	Difficult	Neutral
Throughput Performance	Neutral	Poor	Very Good	Good	Very Poor
Latency Performance	Poor	Neutral	Very Good	Good	Very Poor

For the question: which VPN solution is easy to deploy in delivering cloud services? It can be observed that PPTP VPN, L2TP VPN and SSL/TLS VPN are easier than GRE VPN, IPSec VPN in deployment because the enterprise edge router does not have any configuration requirements. All the configurations only need to be deployed on the Cloud side. In other words, the user does not need to manage and maintain the VPN configurations. Besides, deploying Data Link Layer VPN is relatively simpler than Application Layer VPN to the Cloud Provider because, in our experiments, SSL/TLS VPN needs to install Cisco SSL VPN Client on the Cisco router in advance to provide authentication and it also requires a specific router and IOS. For example, Cisco 2500 series router supported PPTP VPN but did not support SSL/TLS VPN (Cisco, 2007). Furthermore, PPTP VPN is relatively simpler than L2TP VPN because L2TP needs to be deployed with IPSec in the cloud provider edge router in order to provide VPN connections for the Windows users whereas PPTP VPN does not require any additional security mechanism. Then, PPTP VPN is the easiest and simplest to deploy based on this experiments.

For the question: which solution can provide the best network throughput in delivering the cloud services? It can be observed that GRE with IPSec security VPN is the best in terms of network throughput performance in our experiments. It also implies that GRE VPN can provide more bandwidth than the other secure network solutions included in our study. However, it is the most difficult solution in terms of deployment compared with the other four solutions. The second best solution is the IPSec VPN solution followed by the PPTP VPN and the L2TP VPN solution. SSL/TLS VPN solution is the poorest in

throughput performance. Overall, Network Layer VPNs can provide better network bandwidth than the other VPNs based on our experiments.

For the question: which solution can provide the lowest network latency in delivering the cloud services? It can be observed that GRE with IPsec security VPN solution is also the best in terms of latency performance in our experiments. It also implies that GRE VPN has the fastest network speed compared to the other four solutions. The second best solution is IPsec VPN followed by the L2TP VPN and PPTP VPN. SSL/TLS VPN solution is also the poorest in latency performance. In short, Network Layer VPNs are better than Data Link Layer VPNs and Application Layer VPN which can provide a low latency network connection based on our experiments.

8 DISCUSSION AND RELATED WORK

We have mentioned some of the researches relating to this field, particularly those associated with cloud computing, cloud services and enterprise cloud services. We now discuss some related work in terms of secure network solution, VPN comparison, VPN for cloud services.

Chen, Nepal, and Liu (2011) focused on performance observation by comparing with or without application layer VPN for intra-cloud and inter-cloud communication and proposed an electronic contract based solution that provides a secure connectivity as a service (CaaS) for intra-cloud and inter-cloud communications. They completed two tests to evaluate the performance cost of using the proposed secure connectivity service for intra-cloud and inter-cloud communication. The first test evaluated the overhead of using and not using VPN for intra-cloud communication. The second test evaluated the cost of using and not using VPN for inter-cloud communication by comparing the latencies and throughput. In contrast, our research focuses on user experience such as cloud users and cloud implementers by comparing different VPN solutions in enterprise cloud network. Therefore, our research, to the best of our knowledge, is the first attempt to look at the user side in enterprise cloud services by implementing different secure network solutions.

Gou and Liu (2012) examined dynamic IPsec VPN architecture for private cloud services. Liao and Su (2011) looked at A dynamic VPN architecture for private cloud computing. Hiroaki et al (2010) explored dynamic IP-VPN architecture for cloud computing. Although these three papers discuss the dynamic VPN in the cloud, they

mainly pay attention to the dynamic VPN architecture in the cloud environment. In contrast, our research focuses on secure network solutions for cloud services.

In conclusion, to the best of our knowledge, our research appears to be the first attempt to look at the secure network solutions for cloud services. More specifically, we evaluated five different VPN solutions in the cloud environment by implementing the VPN protocols on physical devices. The evaluation focused on the throughput and latency measurement as well as the difficulty in deployment.

9 FUTURE RESEARCH DIRECTIONS

This study explored the popular secure network solutions for cloud services. The discussions and the experiments provided in this study only present an early stage research of secure network solutions for cloud services. Further research will focus on two possible directions based on this study. They are:

- Performance evaluation in secure network solution with encryption algorithms and authentication mechanisms for cloud services,
- VPN as a Service for enterprise cloud services.

In what follows, we expound each of these areas in some details.

There are a number of VPN protocols such as PPTP, L2TP, MPLS, GRE, IPsec, and SSL/TLS to develop a VPN network nowadays (Lewis, 2006). Different VPN protocols, together with different encryption algorithms and authentication mechanisms cloud, result in performance distinctions. It brings enormous challenges to the network designers in selecting the right VPN solution(s) with suitable encryption and authentication methods for the cloud network. Then it is worthwhile to investigate the performance distinctions such as bandwidth utilization and latency among different VPN solutions with different encryption and authentication methods in the cloud network. The outcomes of this future study might provide some experimental reference for cloud network designers and implementers.

VPN as a Service is one of the subsets of the Network as a service (NaaS). NaaS is one of the latest cloud services (Costa, et al., 2012) .NaaS brings a huge attraction to the enterprises and industries nowadays because it reduces the cost of data communications for the cloud consumers and improves the network flexibility. It is important to thoroughly study the benefits and shortcomings of NaaS, taking into account the influence

and impact on enterprise network as well as the security issues. This might improve the understanding of NaaS in enterprise cloud computing network.

10 CONCLUSION

After the review of cloud computing, cloud services and their relationships, this thesis examined the secure network solutions for cloud services. A test bed environment was developed by utilizing physical devices with open software and measurement tools for the purpose of understanding the distinctions of each of the solutions. An inter-cloud network architecture was proposed and the process of the experiments were demonstrated. Our experiment shows that PPTP VPN solution is the easiest and simplest to deploy compared to the other four solutions. Moreover, GRE with IPSec security VPN solution is the best in throughput and latency measurements followed by the IPSec VPN solution. It means that Network Layer VPNs are better than Data Link Layer VPNs and Application Layer VPN in terms of network throughput and latency measurements based on our experiments. Besides, SSL/TLS VPN solution is the poorest solution in our experiments. Additionally, this thesis also looked at one of the popular secure network solutions by using VPN technologies to secure the cloud connections between cloud consumers and the cloud network. This provides experimental reference of secure network solution deployment to the cloud network developers.

Although the aim of the experiment has been attained, there are some unavoidable limitations and shortcomings. First of all, the experiments only include the popular VPN solutions. A number of well-known technologies can be utilized in securing the cloud connections for the enterprise cloud services. Those technologies that are not included in this thesis will be explored in the future study. Second, although the experiments are performed in a solid test bed environment created by physical devices with open source software and measurement tools, the complexity of the cloud network has been minimized compared to the real cloud network environment. Therefore, the configurations might be different in a complex cloud network if additional network techniques have been deployed such as QoS. Third, the outcomes and discussions are only based on the experiments and the configurations. The results purposed in this thesis could be different in various scenarios. Those results will be improved in future investigation in order to minimize the potential mistakes.

11 REFERENCE

1. Ali, Z. B., Samad, M., & Hashim, H. (2011). Performance Comparison of Video Multicasting over Asynchronous Transfer Mode (ATM) & Multiprotocol Label Switching (MPLS) Networks. *System Engineering and Technology (ICSET), 2011 IEEE International Conference* (pp. 177-182). USA: IEEE.
2. Al-Masah, A. S., & Al-Sharafi, A. M. (2013). Benefits of cloud computing for network infrastructure monitoring service. *International Journal of Advances in Engineering and Technology*, 46-51.
3. Amazon. (2011). Retrieved Nov 27, 2012, from Amazon web services: <http://aws.amazon.com/education/>
4. Arinze, B., & Sylla, C. (2012). Conducting research in the cloud. In L. Chao, *Cloud computing for teaching and learning strategies for design and implementation* (p. 57). USA: Information Science Reference.
5. Badger, L., Grance, T., Patt-Corner, R., & Voas, J. (2012). *Draft cloud computing synopsis and recommendations*. Gaithersburg: NIST.
6. Bantoft, K., & Wouters, P. (2006). *Openswan building and integrating virtual private networks*. Birmingham: Packt Publishing.
7. Barr, J., Varia, J., & Wood, M. (2006). *Amazon EC2 beta*. Retrieved November 27, 2012, from http://aws.typepad.com/aws/2006/08/amazon_ec2_beta.html
8. Bauer, E., & Adams, R. (2012). *Reliability and availability of cloud computing*. New York: John Wiley & Sons.
9. BCS The Chartered Institute for IT. (2012). *Cloud computing : Moving IT out of the office*. Swindon: British Informatics Society Limited.
10. Berger, T. (2006). Analysis of current VPN technologies. *First International Conference on Availability, Reliability and Security*. Salzburg: IEEE Computer Society.
11. Buyya, R., Broberg, J., & Goscinski, A. M. (2010). *Cloud computing principles and paradigms*. Hoboken: John Wiley & Sons, Inc.
12. Carmouche, J. H. (2007). *IPsec virtual private network fundamentals*. Indianapolis: Cisco Press.

13. Carr, P., May, T., & Stewart, S. (2012). *Australia's trusted infrastructure-as-a-service cloud provider market 2012*. Retrieved November 28, 2012, from <http://www.longhausshop.com/reports/single-user-online-version-1.html>
14. Carstensen, J., Morgentha, J., & Golden, B. (2012). *Cloud computing assessing the risks*. Ely: IT Governance Publishing.
15. Chao, L. (2012). Overview of cloud computing and its application in e-learning. In L. Chao, *Cloud computing for teaching and learning: Strategies for design and implementation* (p. 4). USA: Information Science Reference.
16. Chen, S., Nepal, S., & Liu, R. (2011). Secure connectivity for intra-cloud and inter-cloud communication. *International Conference on Parallel Processing Workshops* (pp. 154 - 159). Taipei: Elsevier.
17. Chiang, M., & Yang, M. (2004). Towards network X-ities from a topological point of view: Evolvability and scalability. *Proc., Allerton Conf. on Comm., Control, and Computing*.
18. Chou, W. (2002). Inside SSL: the secure sockets layer protocol. *IT Professional*, 4(4), 47-52.
19. Cisco. (2003). *Designing VPN security*. USA: Cisco Press.
20. Cisco. (2007). *Cisco router and security device manager*. Retrieved July 30, 2013, from http://www.cisco.com/en/US/prod/collateral/routers/ps5318/product_data_sheet0900aecd800fd118.html
21. Cisco. (2012). *SSL VPN configuration guide, Cisco IOS release 15M&T*. USA: Cisco Press.
22. Cisco. (2013). *Router security*. Retrieved 11 10, 2013, from <http://www.cisco.com/en/US/products/ps6540/index.html>
23. Cohen , R., & Kaempfer, G. (2000). On the cost of virtual private networks. *IEEE/ACM Transactions on Networking*, 8(6), 775-784.
24. Colasoft. (2013). *Colasoft ping tool*. Retrieved 12 2, 2013, from http://www.colasoft.com/ping_tool/

25. Coles, M., & Landrum, R. (2009). Asymmetric Encryption. In M. Coles, & R. Landrum, *Expert SQL Server 2008 Encryption* (pp. 73-110). New York: Apress.
26. Costa, P., Migliavacca, M., Pietzuch, P., & Wolf, A. L. (2012). NaaS: Network-as-a-service in the cloud. In *Proceedings of the 2nd USENIX Conference on Hot Topics in Management of Internet, Cloud, and Enterprise Networks and Services, Hot-ICE* (pp. 1-1). Berkeley: USENIX Association.
27. Cisco System. (2004). *Comparing MPLS-Based VPNs, IPSec-Based VPNs, and a combined approach from cisco systems -- White Paper*. Retrieved 04 19, 2013, from http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/solmk_wp.pdf
28. Davies, J. (2011). *Implementing SSL / TLS using cryptography and PKI*. Hoboken: John Wiley & Sons.
29. Dayananda, S. M., & Kumar, A. (2012). Architecture for inter-cloud services using IPSec VPN. *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference* (pp. 463-467). Rohtak: IEEE Computer Society.
30. Delfs, H., & Knebl, H. (2007). *Introduction to Cryptography: Principles and Applications*. New York: Springer.
31. Dierks, T., & Rescorla, E. (2008). *The transport layer security (TLS) protocol version 1.2*. Retrieved June 18, 2013, from http://datatracker.ietf.org/doc/rfc5246/?include_text=1
32. EtherealSoftware. (2006). *Ethereal - Network Protocol Analyzer*. Retrieved 05 15, 2013, from Download.com: http://download.cnet.com/Ethereal-Network-Protocol-Analyzer/3000-2085_4-10492160.html
33. Feilner, M. (2006). *OpenVPN Building and Integrating Virtual Private Networks*. Birmingham: Packt Publishing.
34. Ferguson, B. (2012). *CompTIA network+ review guide exam: N10-005*. Hoboken: John Wiley & Sons.
35. Ferguson, N., Schneier, B., & Kohno, T. (2012). *Cryptography Engineering : Design Principles and Practical Applications*. Canada: WILEY.

36. Ferguson, P., & Huston, G. (1998). What is a VPN? - Part I. *The Internet Protocol Journal*, 1, 1.
37. Finn, A., Vredevoort, H., Lownds, P., & Flynn, D. (2012). *Microsoft private cloud computing*. Hoboken: John Wiley & Sons.
38. Focus Group. (2012). *Focus group on cloud computing technical report part 1*. Geneva: International Telecommunication Union.
39. Fortinet. (2013). *FortiOS™ handbook SSL VPN for FortiOS 5.0*. USA: Fortinet.
40. French forum for Iperf. (2011). *What is Iperf?* Retrieved 11 25, 2013, from What is Iperf?
41. Gentry, P. B. (2001). What is a VPN? *Information Security Technical Report*, 6(1), 15-22.
42. Gleeson, B., Lin, A., Heinanen, J., Armitage, G., & Malis, A. (2000). *A framework for IP based virtual private networks*. Retrieved March 26, 2013, from <http://www.rfc-editor.org/rfc/rfc2764.txt>
43. Goldreich, O. (2004). *Foundations of cryptography: volume 2, basic applications*. Cambridge: Cambridge university press.
44. Google. (2010). Retrieved Nov 27, 2012, from Google Apps For Education: <http://www.google.com/enterprise/apps/education/>
45. Gou, Q.-D., & Liu, Y.-H. (2012). Dynamic IPsec VPN architecture for private cloud services. *2012 International Conference on Wavelet Active Media Technology and Information Processing* (pp. 250-253). Sichuan: IEEE Xplore.
46. Gupta, P., & Verma, A. (2012). Concept of VPN on cloud computing for elasticity by simple load balancing technique. *International Journal of Engineering and Innovative Technology (IJEIT)*, 274-278.
47. Halpert, B. (2011). *Auditing cloud computing: A security and privacy guide*. Canada: John Wiley & Sons, Inc.
48. Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., & Zorn, G. (1999). *Point-to-point tunneling protocol (PPTP)*. USA: Internet Engineering Task Force.

49. Hao, F., Lakshman, T. V., Mukherjee, S., & Song, H. (2010). Secure cloud computing with a virtualized network infrastructure. *2nd USENIX Conference on Hot topics in Cloud Computing* (pp. 16-16). Boston: MA.
50. Harding, C. (2011). *Cloud computing for business -The open group guide*. Zaltbommel: Van Haren Publishing.
51. Hartpence, B. (2011). *Packet Guide to Routing and Switching*. Sebastopol: O'Reilly Media.
52. Hata, H., Kamizuru, Y., Honda, A., Hashimoto, T., Shimizu, K., & Yao, H. (2010). Dynamic IP-VPN architecture for cloud computing. *8th Asia-Pacific Symposium on Information and Telecommunication Technologies* (pp. 1-5). Kuching: NTT Communications.
53. Held, G. (2004). *Virtual private networking : A construction, operation and utilization guide*. Chichester: John Wiley & Sons, Ltd.
54. Henríquez, F. R., Pérez, A. D., Saqib, N. A., & Koç, Ç. K. (2007). A brief introduction to modern cryptography. In F. R. Henríquez, A. D. Pérez, N. A. Saqib, & Ç. K. Koç, *Cryptographic algorithms on reconfigurable hardware signals and communication technology* (pp. 7-33). USA: Springer US.
55. Hoang, T.-T.-M. (2012). *Computer Networks, the Internet and Next Generation Networks : A Protocol-based and Architecture-based Perspective*. Frankfurt: Lang, Peter, GmbH, Internationaler Verlag der Wissenschaften.
56. Hping. (2009). *Welcome to the hping wiki*. Retrieved 05 15, 2013, from hping wiki: <http://wiki.hping.org/>
57. Hurwitz, J., Kaufman, M., Halper, F., & Kirsch, D. (2012). *Hybrid cloud for dummies*. Hoboken: John Wiley & Sons.
58. IBM. (2010). *IBM Smart Cloud*. Retrieved NOV 27, 2012, from <http://www.ibm.com/cloud-computing/us/en/index.html>
59. ICNP. (2013). *Welcome to ICNP 2013*. Retrieved 05 10, 2013, from 21st IEEE International Conference on Network Protocols: <http://icnp13.informatik.uni-goettingen.de/home.html>

60. Ioannidis, J. (2011). IPsec. In H. C. Tilborg, & S. Jajodia, *Encyclopedia of cryptography and security* (pp. 635-638). USA: Springer US.
61. IxChariot. (2008). *IxChariot*. Retrieved 05 15, 2013, from IxChariot: <http://www.ixchariot.com/products/datasheets/ixchariot.html>
62. Jaha, A. A., Shatwan, F. B., & Ashibani, M. (2008). Proper virtual private network (VPN) solution. *The Second International Conference on Next Generation Mobile Applications, Services and Technologies* (pp. 309-314). Libya: IEEE Computer Society.
63. Jamil, D., & Zaki, H. (2011, April). Cloud computing security. *International Journal of Engineering Science and Technology (IJEST)*, 3, 4.
64. Joshi, J. (2008). *Network security*. Burlington: Elsevier.
65. Katz, J. (2010). Digital Signatures: Background and Definitions. In J. Katz, *Digital Signatures* (pp. 3-33). USA: Springer US.
66. Khanvilkar, S., & Khokhar, A. (2004). Virtual private networks: an overview with performance evaluation. *Communications Magazine, IEEE*, 146--154.
67. Khmelevsky, Y., & Voytenko, V. (2010). Cloud computing infrastructure prototype for university education and research. *WCCCE '10 Proceedings of the 15th Western Canadian Conference on Computing Education*. Kelowna: WCCCE.
68. Kizza, J. M. (2005). Computer network security protocols and standards. In J. M. Kizza, *Computer network security* (pp. 425-461). USA: Springer US.
69. Kommalapati, H. (2010). *Windows Azure for enterprises*. Retrieved Nov 28, 2012, from <http://msdn.microsoft.com/en-us/magazine/ee309870.aspx>
70. Kotuliak, I., Rybár, P., & Trúchly, P. (2011). Performance comparison of IPsec and TLS based VPN technologies. *9th International Conference on Emerging eLearning Technologies and Applications* (pp. 217-221). USA: IEEE.
71. Largent, B., Rogers, V. C., & Marsh, T. A. (2002). Digital Signatures. *Journal of Internet Commerce*, 65-73.
72. Lewis, M. (2006). *Comparing, designing, and deploying VPNs*. USA: Cisco Press.
73. Li, A., Yang, X., Kandula, S., & Zhang, M. (2011). Comparing public-cloud providers. *IEEE Internet Computing*, 50-53.

74. Li, N. (2009). *Encyclopedia of Database Systems*. USA: Springer US.
75. Liao, W., & Su, S. (2011). A dynamic VPN architecture for private cloud computing . *4th IEEE/ACM International Conference on Cloud and Utility Computing* (pp. 409-414). Melbourne: IEEE.
76. Lowe, D. (2012). *Networking all-in-one for dummies*. New York: Wiley .
77. Mache, J., Tyman, D., Pinter, A., & Allick, C. (2006). Performance implications of using VPN technology for cluster integration and grid computing. *International conference on Networking (ICNS'06)* (p. 75). Silicon Valley: IEEEExplore.
78. Malik, S. (2002). *Network security principles and practices*. USA: Cisco Press.
79. Martin, J. A. (2010). *Should you move your small business to the cloud?* Retrieved Nov 27, 2012, from http://www.pcworld.com/article/188173/should_you_move_your_business_to_the_cloud.html
80. Martin, K. M. (2012). *Everyday Cryptography : Fundamental Principles and Applications*. Oxford: OUP Oxford.
81. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. USA: National Institute of Standards and Technology.
82. Microsoft. (2003). *What is VPN?* USA: Microsoft.
83. Narayan, S., Brooking, K., & Vere, S. d. (2009). Network performance analysis of VPN protocols: An empirical comparison on different operating systems. *2009 International Conference on Networks Security, Wireless Communications and Trusted Computing*. New Zealand: IEEE Computer Society.
84. Neela, K. L., Kavitha, V., & Ramesh, R. K. (2013). Cloud computing: threats and security issues. *International Journal of Engineering Sciences & Research*, 2070-2072.
85. Oki, E., Rojas-Cessa, R., Tatipamula, M., & Vogt, C. (2012). *Advanced internet protocols, services, and applications*. Hoboken: John Wiley & Sons.
86. Oppliger, R. (2009). *SSL and TLS : Theory and practice*. Norwood: Artech House.
87. Oracle Corporation. (2009). *Documentation*. Retrieved June 5, 2013, from <https://www.virtualbox.org/wiki/Documentation>

88. Paar, C., & Pelzl, J. (2010). Message Authentication Codes (MACs). In C. Paar, & J. Pelzl, *Understanding Cryptography* (pp. 319-330). Berlin Heidelberg: Springer.
89. Park, K.-w., & Park, K. H. (2011). ACCENT: Cognitive cryptography plugged compression for SSL/TLS-based cloud computing services. *ACM Transactions on Internet Technology (TOIT)*, 11(2), 1-30.
90. Preneel, B. (2011). Hash Functions. In S. Jajodia, & H. C. van Tilborg, *Encyclopedia of Cryptography and Security* (p. 553). USA: Springer US.
91. RFC. (2012). *RFC editor*. Retrieved Nov 15, 2013, from <http://www.rfc-editor.org/>
92. Ried, S. (2011). *Sizing the cloud*. USA: Forrester.
93. Rouse, M. (2006). *latency*. Retrieved 11 21, 2013, from <http://searchcio-midmarket.techtarget.com/definition/latency>
94. Rouse, M. (2009). *Storage as a service (SaaS)*. Retrieved July 11, 2013, from <http://searchstorage.techtarget.com/definition/Storage-as-a-Service-SaaS>
95. Rouse, M. (2011). *Cloud services*. Retrieved July 03, 2013, from <http://searchcloudprovider.techtarget.com/definition/cloud-services>
96. Saidman, G. K., & Hairston, T. (1999). Electronic signatures: authenticating identities online confidence. *The Internet Newsletter: Legal & Business Aspects*, 9.
97. Schroder, C. (2007). *Measure Network Performance with iperf*. Retrieved 05 15, 2013, from Enterprise Networking Planet: <http://www.enterprisenetworkingplanet.com/netos/article.php/3657236/Measure-Network-Performance-with-iperf.htm>
98. SearchCloudComputing. (2012). *Top 10 cloud computing providers of 2012*. Retrieved Nov 28, 2012, from <http://searchcloudcomputing.techtarget.com/photostory/2240149038/Top-10-cloud-providers-of-2012/1/Introduction#contentCompress>
99. Shan, T. (2009). *Cloud taxonomy and ontology*. Retrieved August 1, 2013, from <http://tonyshan.ulitzer.com/node/1469454>

100. Sitaram, D., & Manjunath, G. (2011). *Moving to the cloud developing apps in the new world of cloud computing*. Burlington: Elsevier Science.
101. Snyder, C., Myer, T., & Southwell, M. (2010). Michael. In C. Snyder, T. Myer, & M. Southwell, *Pro PHP Security* (pp. 229-266). New York: Apress.
102. Solarwinds. (2013). *What is network throughput*. Retrieved 11 21, 2013, from <http://www.solarwinds.com/it-management-glossary/what-is-network-throughput.aspx>
103. Sosinsky, B. (2009). *Networking bible*. Hoboken: John Wiley & Sons.
104. Sosinsky, B. (2010). *Cloud computing bible*. Hoboken: John Wiley & Sons.
105. Steinberg, J., & Speed, T. (2005). *SSL VPN understanding, evaluating and planning secure, web-based remote access*. Birmingham: Packt Publishing.
106. Stewart, J. M., & Chapple, M. (2011). *CISSP certified information systems security professional study guide*. Hoboken: John Wiley & Sons.
107. Strachey, C. (1959). Time Sharing in Large Fast Computers. *International Conference on Information processing Congress* (pp. 336–341). Paris: UNESCO.
108. Strebe, M. (2006). *Network security foundations : technology fundamentals for IT success*. Hoboken: John Wiley & Sons, Inc.
109. Thomas, P. Y. (2012). Harnessing the potential of cloud computing to transform higher education. In L. Chao, *Cloud computing for teaching and learning strategies for design and implementation* (pp. 147-158). USA: IGI Global.
110. Townsley, . M., Lau, J., & Goyret, I. (2005). *Layer two tunneling protocol version 3 (L2TPv3)*. USA: Internet Engineering Task Force.
111. Townsley, W., Rubens, A., Pall, G., Zorn, G., & Palter, B. (1999). *Layer two tunneling protocol "L2TP"*. USA: Internet Engineering Task Force.
112. Venkateswaran, R. (2001). Virtual private networks. *Potentials, IEEE, XX(1)*, 11-15.
113. VirtualBox. (2009). *Welcome to VirtualBox.org*. Retrieved June 5, 2013, from <https://www.virtualbox.org/>

114. VPN Consortium. (2008, July). *VPN technologies: Definitions and requirements*. Retrieved Dec 11, 2012, from <http://www.vpnc.org/vpn-technologies.html>
115. Weaver, A. C. (2006). Secure sockets layer. *Computer*, 88-90.
116. Wikipedia. (2012). *Generic routing encapsulation*. Retrieved Aug 19, 2012, from http://en.wikipedia.org/wiki/Generic_Routing_Encapsulation
117. Wikipedia. (2013). *Throughput*. Retrieved 11 21, 2013, from http://en.wikipedia.org/wiki/Network_throughput
118. Williams, A. (2009). *The feds, not forrester, are developing better definitions for cloud computing*. Retrieved July 03, 2013, from <http://readwrite.com/2009/10/13/forrester-says-we-need-better#awesm=~oav2IHYSRCoG>
119. Wood, T., Ramakrishnan, K. K., Shenoy, P., & Merwe, J. V. (2012). Enterprise-ready virtual cloud pools: Vision, opportunities and challenges. *Special Focus on Security and Performance of Networks and Clouds*, 995-1004.
120. Yang, B., Tan, F., Dai, Y.-S., & Guo, S. (2009). Performance evaluation of cloud service considering fault recovery. In M. G. Jaatun, G. Zhao, & C. Rong, *Cloud computing* (pp. 571-576). Berlin: Springer Berlin Heidelberg.
121. Younglove, R. W. (2000). Virtual private networks - How they work. *Computing & Control Engineering Journal*, 11(6), 260-262.
122. Yuricik, W., & Doss, D. (2001). A Planning Framework for Implementing Virtual Private Networks. *IT Professional*, 3(3), 41-44.

12 ADDITIONAL MATERIALS

1. Chang, W. Y., Abu-Amara, H., & Sanford, J. F. (2010). *Transforming enterprise cloud services*. Dordrecht: Springer Science+Business Media B.V. .
2. Chee, B. J., & Jr., C. F. (2010). *Cloud computing: Technologies and strategies of the ubiquitous data center*. USA: CRC Press.
3. Chorafas, D. N. (2010). *Cloud computing strategies*. Hoboken: CRC Press.

4. Cisco System. (2004). Comparing MPLS-based VPNs, IPSec-based VPNs, and a combined approach Retrieved April 19, 2013, from http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/solmk_wp.pdf
5. Dasgupta, D., & Rahman, M. (2011). Estimating security coverage for cloud services. 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing (pp. 1064-1071). Boston: IEEE Xplore.
6. Deal, R. (2005). The complete Cisco VPN configuration guide. USA: Cisco Press.
7. Feilner, M. (2006). OpenVPN building and integrating virtual private networks. Birmingham: Packt Publishing.
8. Ferguson, N., Schneier, B., & Kohno, T. (2012). Cryptography engineering: Design principles and practical applications. Canada: WILEY.
9. Furht, B., & Escalante, A. (2010). Handbook of cloud computing. New York: Springer.
10. Hartpence, B. (2011). Packet guide to routing and switching. Sebastopol: O'Reilly Media .
11. Head, M. R., Sailer, A., Shaikh, H., & Shea, D. G. (2010). Towards self-assisted troubleshooting for the deployment of private clouds. 2010 IEEE 3rd International Conference on Cloud Computing (pp. 156-163). Miami: IEEE.
12. Held, G. (2004). Virtual private networking: A construction, operation and utilization guide. Chichester: John Wiley & Sons, Ltd.
13. Hoang, T.-T.-M. (2012). Computer networks, the internet and next generation networks: A protocol-based and architecture-based perspective. Frankfurt: Lang, Peter, GmbH, Internationaler Verlag der Wissenschaften.
14. Ivanov, I., Sinderen, M. v., & Shishkov, B. (2012). Cloud computing and services science. New York: NY : Springer New York.
15. Jennings, R. (2009). Cloud computing with the windows azure platform. Hoboken: John Wiley & Sons, Inc.
16. Krutz, R. L., & Vines, R. D. (2010). Cloud security a comprehensive guide to secure cloud computing. Hoboken: John Wiley & Sons.
17. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy an enterprise perspective on risks and compliance. Sebastopol: O'Reilly Media, Inc. .

18. McDonald, K. T. (2010). Above the clouds: Managing risk in the world of cloud computing. Ely: IT Governance Publishing.
19. McGrath, M. (2012). Understanding PaaS. Sebastopol: O'Reilly Media.
20. Miller, M. (2009). Cloud computing: Web-based applications that change the way you work and collaborate online. USA: Que Publishing.
21. Newcombe, L. (2012). Securing cloud services a pragmatic approach to security architecture in the cloud. Ely: IT Governance Publishing.
22. Oki, E., Rojas-Cessa, R., Tatipamula, M., & Vogt, C. (2012). Advanced internet protocols, services, and applications. Hoboken: John Wiley & Sons.
23. Raj, P. (2013). Cloud enterprise architecture. USA: CRC Press.
24. Shroff, G. (2010). Enterprise cloud computing: Technology, architecture, applications. New York: Cambridge University Press.
25. Tang, L., Dong, J., Zhao, Y., & Zhang, L.-J. (2010). Enterprise cloud service architecture. Cloud Computing (CLOUD) (pp. 27 - 34). USA: IEEEExplore.
26. Yuricik, W., & Doss, D. (2001). A planning framework for implementing virtual private networks. IT Professional, 3(3), 41-44. USA: IEEEExplore.

13 KEY ITEMS AND DEFINITIONS

Cloud Computing: It refers to applications and services that run on a distributed network using virtualized resources and accessed via a computer network such as Internet.

Enterprise Cloud: It is the cloud that provides private access and is controlled by either a single enterprise or consortium of businesses.

Security: It refers to a broad set of policies, technologies, and controls implemented to protect data, applications and infrastructure.

Internet Protocol Security (IPSec): It is a collection of protocols, conventions, and mechanisms used for ensure the authenticity and guarantee the confidentiality of the content of the IP packets. It operates at the Network layer (Layer 3) of the OSI model.

Point-to-Point Tunneling Protocol (PPTP): It is one of the most popular dial-in protocols operates at the Data Link layer (Layer 2) of the OSI model.

Private Cloud: Cloud infrastructures are controlled solely for a single organization. Cloud infrastructures can be managed internally or by a third-party and hosted internally or externally.

Public Cloud: Cloud infrastructure is open for public use and it can be owned, managed, operated by an organization.

Secure Sockets Layer/Transport Layer Security (SSL/TLS): It is one of the most popular protocols provides communication security over the Internet. It has been classified as one of the Transport Layer Protocols (Layer 4) according to the OSI model.

Software as a Service (SaaS): It is one of the most important cloud services which makes the application software available to the cloud customers.

Virtual Private Network (VPN): One of the most popular solutions in establishing a connection though a public network utilizing encryption technology to privatize data for transmission between two trusted parties.