Chapter 68
Secure Network Solutions for Enterprise Cloud Services

Chengcheng Huang
University of Ballarat, Australia

Phil Smith
University of Ballarat, Australia

Zhaohao Sun
University of Ballarat, Australia

ABSTRACT

Securing a cloud network is an important challenge for delivering cloud services to enterprise clouds. 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, 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 VPN solution is most user-friendly in enterprise clouds? This chapter explores these issues by implementing different VPNs in a virtual cloud network environment using open source software and tools. This chapter also reviews cloud computing and cloud services and looks at their relationships. The results not only provide experimental evidence but also facilitate the network implementers in deployment of secure network solutions for enterprise cloud services.

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 systems software in the data centers that provide those services (Yang, Tan, Dai, & Guo, 2009). Cloud computing provides its services based on the service model. Examples of the service model are infrastructure

DOI: 10.4018/978-1-4666-6539-2.ch068

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. In particular, 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 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 to access the cloud network for enterprises. Jamil and Zaki (2011) stated that enterprises can use VPN connections to increase 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 result in significant differences due to the weaknesses, strengths and vulnerabilities of deploying VPN protocols (Jaha, Shatwan, & Ashibani, 2008). Hence, implementing a suitable and secure VPN solution for the enterprise cloud is a significant challenge for network implementers and enterprises. Important questions faced by the cloud network developers include: Which VPN solution is easy to deploy in delivering cloud services? Which VPN solution is most user-friendly in enterprise cloud? This chapter addresses these issues by evaluating the most popular VPN solutions in a virtual cloud network environment.

The remainder of this chapter is organized as follows. Firstly, a review of cloud computing, enterprise cloud, and cloud services and their relationships are given in this chapter. Secondly, this chapter explores each securing network solution, describes the test bed setup, deployment process, and evaluates the experiment results and discusses related work. Finally some future research directions and some concluding remarks are provided.

CLOUD COMPUTING AND CLOUD SERVICES

This section reviews the definition of cloud computing, basic characteristics of cloud computing and discusses the cloud deployment models and cloud services. This section also illustrates the relationship between cloud computing and cloud services and introduces the enterprise cloud services. The section concludes by reviewing the benefits and challenges of cloud services.

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

Related Content