雲端彈性虛擬資料中心服務平台之安全性提升

陳劭睿　　李忠信[1]　　楊睿豪　　王尉任
中央大學資訊工程系
[1]中華電信數據分公司
pj082473@csie.ncu.edu.tw ; lil.doph@gmail.com ;
hswayne77@gmail.com ; wjwang@csie.ncu.edu.tw

摘要

SAMEVED (System Architecture for Managing and Establishing Virtual Elastic Datacenters)是一個提供使用者建立、管理虛擬資料中心的雲端服務平台。SAMEVED 利用虛擬化技術並且整合了 VPN（Virtual Private Network）和虛擬路由器的功能，可以讓使用者自行定義虛擬資料中心的網路拓樸與運算環境。本篇論文針對 SAMEVED 的安全性進行研究，提出一些安全上的改良。SAMEVED 的 VPN 連線讓使用者可以把本地網路延伸到虛擬資料中心，但是這段連線卻缺乏加密保護，封包可能會遭到讀取，所以我們改採用 L2TP/IPsec VPN，以確保 VPN 連線的加密性和認證。另外，我們設計了私有雲繞送（Routing），形成與 Internet 隔離的子網路（subnet），可以存放私密資料於此。最後我們在 SAMEVED 系統開發安全群組功能。安全群組就像防火牆一般，可以控制虛擬機器群組允許哪些訊務（traffic）進出，可以更加提升虛擬資料中心的安全性。

關鍵詞：虛擬資料中心、虛擬化技術、雲端計算、安全群組。

Abstract

SAMEVED (System Architecture for Managing and Establishing Virtual Elastic Datacenters) is a system architecture which provides a cloud service that can allocate and manage a private, virtual elastic datacenter. The SAMEVED provides users the ability to define the network topology and the computing environment of virtual datacenter by virtualization technologies. This paper makes some security enhancement in SAMEVED. We implement L2TP/IPsec VPN which provides encryption and authentication. Also we design the routing mechanism in VPC to create a private subnet in which we can place protected server here. At last, we develop the Security Group function for SAMEVED. The Security Group acts as a firewall that controls the in-coming and out-going traffic of a group of VM instances.

Keywords: virtual datacenter; virtualization; cloud computing; security group.

1. 前言

雲端運算（Cloud Computing）[1][2][3][4] 本質大抵承襲自網格運算（Grid Computing）[5][6][7]，強調在本地端資源有限的情況下，利用網路取得遠方的運算資源。在雲端運算這計算模型中，計算資源如計算能力（computing power）、儲存空間、網路和軟體等等被抽象化成可以透過網際網路使用的服務（services on the Internet）。由於使用者的應用軟體與資料已存放在遠端伺服器，使用者只需要透過網路瀏覽器（Web browser）、小筆電或是手機 APP 即可使用雲端服務。

雲端運算服務可以廣泛的分為三種架構：IaaS[8]（Infrastructure as a Service，基礎架構即服務）、PaaS（Platform as a Service，平台即服務）、SaaS（Software as a Service，軟體即服務），其中 IaaS 是位於最下層的基礎架構。IaaS 提供者將計算資源如 CPU、記憶體、儲存空間等等以虛擬機器[9][10]（Virtual Machine）的方式提供給使用者，利用虛擬化技術[11]（Virtualization technology），IaaS 提供者可以提升實體資源的使用率，並且擴充實體資源到足以支援大量的虛擬機器。而 IaaS 使用者不需要再去建置高成本的資料中心（datacenter），只需要針對自己的需求申租足夠的虛擬機器，使用多少資源便付多少錢，節省企業 IT 成本。Amazon Web Services (AWS)是目前主要的 IaaS 供應商之一，Elastic Compute Cloud[12] (EC2)是其熱門的服務。

SAMEVED[13][14] (System Architecture for Managing and Establishing Virtual Elastic Datacenters)是一個穩定的基礎架構網路服務平台，使用者可以在平台上建立虛擬機房(Virtual Elastic Datacenter)，部署自己的網路拓樸與虛擬機器，建立一個混合雲(Hybrid cloud)[15][16][17]的服務環境。虛擬機房建立時，系統會自動在新的虛擬機房中建立一個 VPN Gateway，提供虛擬機房與使用者本地網路之間的 VPN（Virtual Private Network）連線。SAMEVED 雖然具備使用者身分認證、封閉虛擬網路環境等安全特性，但資訊安全總是有著改善的空間。如:VPN 連線缺乏加密與不具有群組控管虛擬機器進出網路的服務。這兩個安全性漏洞在混合雲中，都是具有可以影響整各系統運作的極大漏洞。

本文提出對 SAMEVED 的安全性特性進行強動作，其中針對 VPN 連線與安全性群組兩個特性，進行安全性的加強。VPN 連線透過 L2TP/ IPsec VPN

Server 加強使用者與 SAMEVED VPN gateway 得連線安全。並且加強虛擬機房內的虛擬機器的安全性群組部分，透過網頁介面讓使用者管理安全群組的虛擬機器成員，所以 SAMEVED 安全群組是一個能有效管理虛擬機器防火牆規則的機制。

本文架構在第二章會提到相關研究，內容包含目前雲端上的底層技術與趨勢。第三章提到私有雲使用情境實作，包括 L2TP/IPsec VPN 的建立與私有雲中 Routing 的實作。SAMEVED 安全群組功能，說明安全群組概念與使用權限，SAMEVED 各角色伺服器負責的工作與各角色間的互動情形以及安全群組於第四章詳細介紹。第五章是結論。

2. 相關研究

Citrix XenServer[18][19]採用 Xen hypervisor，[20][21]是一套完整可管理的伺服器虛擬化 (Server Virtualization)平台。Citrix XenServer 可以有效的管理 Windows 和 Linux 虛擬伺服器（virtual servers），並且有效的合併伺服器資源。XenServer 平台有三種網路物件，PIF 代表 XenServer host 的實體網路介面，VIF 代表虛擬機器的虛擬網路介面，而 network 是虛擬乙太網路交換器（virtual Ethernet switch）。XenServer 的虛擬網路（Virtual Network）又分為三種類別，分別是 Internal Network，External Network 和 VLAN。Internal Network 沒有和實體網路卡相關聯，和外在網路並無連接，只是讓與此網路相連接的虛擬機器彼此溝通。External Network 和實體網路卡相關聯，作為虛擬機器和實體網路卡之間的橋接器（bridge），可以讓虛擬機器連接到實體網卡之後的外部網路。VLAN（ Virtual Local Area Network ）由 IEEE 802.1Q 標準定義，可以將實體網路區分成數個邏輯網路。XenServer 可以連接虛擬機器的 VIF 至特定 VLAN，其中 VLAN 的 tagging/untagging 是由 Xenserver 實體機器（host）所執行，虛擬機器不曉得 VLAN 的存在。

OpenStack[22]是一個由 NASA 和 Rackspace 開始合作研發的 IaaS（Infrastructure as a Service）雲端運算平台，以 Apache 許可證授權，並且是一個自由軟件和開放原始碼項目，目前已有多家大型廠商參與這個專案，包括 AMD、Intel、HP、Red Hat、Cisco 等等。OpenStack 有著彈性的架構，沒有專有的軟硬體需求，並且支援 KVM、Xen、VirtualBox[23][24]、VMware[25]等等的虛擬機器軟體。 OpenStack 是一個雲端作業系統，由計算（compute）、儲存（storage）、與網路三個元件所組成，控制著資料中心（datacenter）的資源，而管理者透過 dashboard 控制提供給使用者的資源。OpenStack 計算提供與管理虛擬機器的大型網路。計算資源可以透過 APIs 的方式提供給雲端應用程式開發者，或是透過 Web 介面提供給一般使用者。OpenStack 儲存分為 Object Storage 和 Block Storage。Object Storage 提供分散式、API 可存取的儲存平台，可用於資料備份、保存或是整合成應用服務。Object Storage 不是由單點控制，因此具備可擴充與備援的特性。資料被複製散布在資料中心的數個磁碟，由 OpenStack 軟體確保資料的複製與完整性。Block Storage 允許磁碟裝置連接到 VM instance，作為擴充的儲存裝置。OpenStack 網路是可介接、可擴充且支援 API 的系統，用來管理網路和 IP 位址，並且確保網路不會是部署雲的瓶頸。

在 Amazon Virtual Private Cloud (Amazon VPC)[26][27]中，使用者可以自訂自己的虛擬網路拓樸(virtual network topology)，就像在機房規劃網路環境一般。使用者可以自由的設計虛擬網路環境，包括 IP 位址範圍，子網路拓樸，網路路由(route table)，網路閘道 (network gateway)等等。使用者可以輕易的配置需要的網路拓樸，例如創造一個開放的子網路(public subnet)，讓 web servers 直接存取 Internet，或是創造一個與 Internet 隔離的私有子網路(private subnet)，來放置資料庫或應用程式伺服器。除此之外，使用者可以在自己的 datacenter 和 VPC 之間建立 Hardware Virtual Private Network (VPN) 連線，將 VPC 當作 datacenter 的延伸。

SAMEVED (System Architecture for Managing and Establishing Virtual Elastic Datacenters)是一個穩定且安全性高的基礎架構網路服務平台。SAMEVED 提供簡單且易操作的網路介面和 Remote API，使用者可以透過網路介面註冊自己的帳號和密碼，每個使用者有自己的使用權限，不同的身分權限可以使用的服務功能不同。一般的使用者可以群組管理自己的虛擬機器和虛擬機器映像檔範本 (VM image template)，進階的使用者可以建立多個虛擬機房 (Virtual Elastic Datacenter)，建立虛擬機房的動作包括建立一組計算結點 (Node)、虛擬路由器 (Virtual router) 和虛擬網路區段 (VLAN segment)，使用者可以決定這些計算結點、虛擬路由器、虛擬網路區段之間的連接方式。在虛擬機房中整個網路環境是封閉的，SAMEVED 結合了 Virtual Private Network (VPN) 的功能，當使用者在建立虛擬機房時，系統會自動在新的虛擬機房中建立一個 VPN Gateway，讓使用者可以在與 VPN Gateway 連線後，操作到虛擬機房中的虛擬路由器和計算結點。而系統管理員則可以透過網路介面管理系統中的實體機器，也可以查詢所有使用者操作系統的記錄，如此一來，系統管理員就可以快速又方便地對整個系統做除錯和維護的動作。SAMEVED 所建立的是一個混合雲的服務環境。

3. 私有雲實作

本文在 Citrix Xenserver 上建置一個混合 Public Subnets 和 VPN-Only Subnets 的私有雲（Virtual Private Cloud），模擬使用者需要的使用情境。私有雲網路拓樸如圖 1 所示，Public Subnet 是開放的子

網路，可以由 Internet 直接存取，用來建置例如 Web 應用般的服務。VPN-Only Subnet 是透過 VPN 與使用者自家網路相連，與 Internet 是隔離的，只有使用者自家網路和私有雲內部可以存取，可以將資料庫伺服器建置於此。使用者自家網路經過網際網路與私有雲建立 VPN 連線。本次實驗採用 L2TP/IPsec VPN，因為 IPsec 協定可以為 VPN 連線提供加密與認證。L2TP/IPsec VPN 建立後，使用者便能安全的將本地網路延伸至私有雲。實驗的結果會確認 VPN 連線是否經過加密與認證。

本文用圖 1 簡單說明本文中混合雲是如何連接，私有雲中的 Public Subnet 與 VPN-Only Subnet 為 Xenserver 所建的內部虛擬網路，分別接上 Web Server 與 DB server 的虛擬機器。圖 1 中的 R 表示私有雲中的網路路由（Routing），是由虛擬路由器所實現，讓私有雲內部網路互通，Public Subnet 與 Internet 互通，以及 VPN-Only Subnet 與使用者本地網路互通。虛擬路由器同時分別擔任 Internet Gateway 與 VPN Gateway。

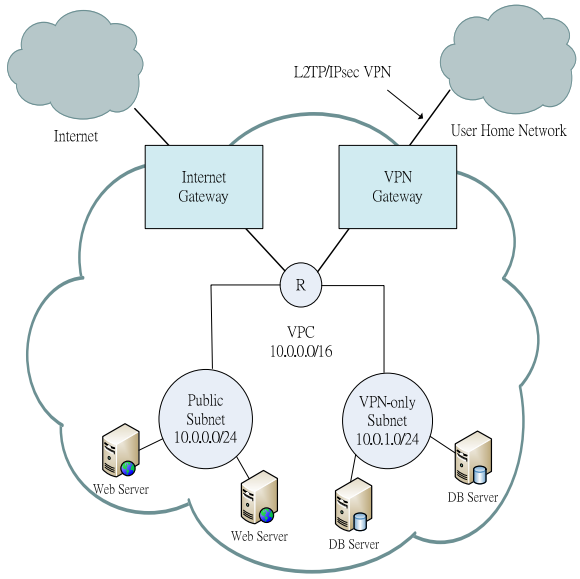

圖1　私有雲實作網路拓樸

在私有雲的建立中，將分成兩個部分進行實作，分別是 L2TP/Ipsec VPN 與私有雲的路由(routing)。本文將針對這兩個部分再詳細說明。

3.1 L2TP/Ipsec VPN

本文 L2TP/IPsec VPN 實作，L2TP 是以 xl2tpd[28] daemon 實現，IPsec 則是以 openswan[29] 套件實現，VPN Server 所安裝套件如[30]所列。L2TP 以 CHAP（Challenge-Handshake Authentication Protocol）方式認證使用者，而 IPsec 的金鑰採用 pre-shared secrets。實作上遇到的困難點在於 VPN server 防火牆沒有開啟 UPD port 1701（L2TP）與 UDP port 500、4500（IPsec），導致 L2TP/IPsec 的溝通無法建立，是一個值得注意的地方。L2TP/IPsec VPN 設定概要如圖 2，VPN server 的 eth1 介面 IP 為 192.168.1.98，ppp0 介面 IP 設定為 192.168.1.99，保留給 VPN client 的 IP 範圍是 192.168.1.128 到 192.168.1.254。當 L2TP/IPsec VPN 連線成功建立時，外層的 IPsec tunnel 保護 VPN 連線，L2TP tunnel 內建立起 PPP session，於是 VPN client 拿到 IP 192.168.1.128，邏輯上可以看成位在私有雲的內部網段上。

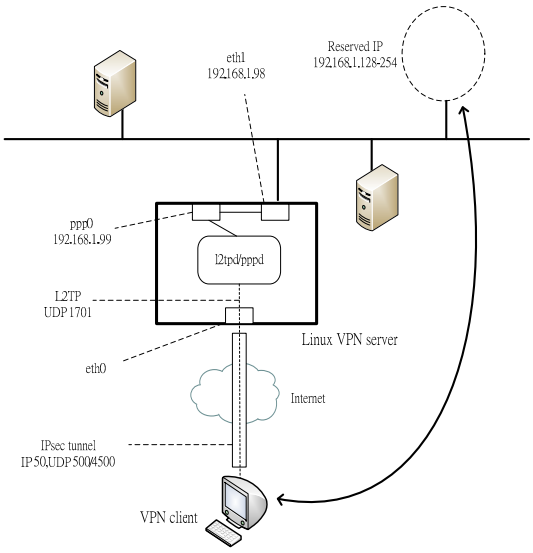

圖2　L2TP/IPsec VPN 設定概要圖

3.2 私有雲 Routing

私有雲的 routing 如圖 3所示，虛線表示 traffic 繞送的路徑。VPN-Only subnet 的 routing 如 VPN route table 的內容。在 VPN route table 中存在兩筆路由，預設路由（default route） 0.0.0.0/0 的目標（target）為 VPN Gateway，10.0.0.0/16 該筆路由為私有雲的內部網段，target 是私有雲內部。所以 VPN-Only subnet 只會與使用者自家網路和私有雲內部互通，和 Internet 是隔離的。這樣的封閉 Subnet 可以部署 Database Server，存放重要的私密資料。Public Subnet 的 routing 如 Public route table 的內容。在 Public route table 中存在兩筆路由，預設路由（default route）0.0.0.0/0 的目標為 Internet Gateway，10.0.0.0/16 該筆路由為私有雲內部網段的路由。所以 Public subnet 與 Internet 和私有雲內部是互通的，可以部署開放的 Web Service。私有雲的 Routing 實作架構如

圖 4所示。Subnets 是由 XenServer 的 Internal Network（Virtual Switch）所構成，而 routing 是利用虛擬路由器 (Virtual Router)來完成。虛擬路由器是 Linux CentOS 5.4 的虛擬機器，安裝了 Quagga[30]套件。Quagga 是 routing 的軟體套件，提供 Unix 平台諸如

RIP、OSPF、BGP 等動態路由協定的實現。虛擬路由器同時扮演了 VPN Gateway 和 Internet Gateway 的角色。

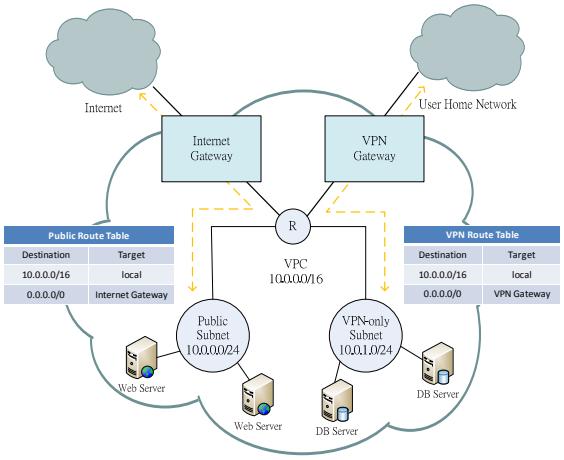

圖3　私有雲 Routing Table

在 VPN-Only Subnet 的 Internal Network 設定 default route，目標（target）為 VPN virtual router，並且在 VPN virtual router 上設定 default route，指向 VPN 連線，如此 VPN-Only Subnet 往使用者自家網路的 routing 便設置完成。類似的，在 Public Subnet 的 Internal Network 設定 default route，目標為 Public virtual router，並且在 Public virtual router 上設定 default route，指向 Internet，如此 Public Subnet 往 Internet 的 routing 便設置完成。私有雲內部 Subnets 之間的路由（route），是在 Virtual Router 之間以動態路由協定 RIPv2 交換分享。把 Quagga 的 RIP 設定好後，Virtual Router 間便建立起 RIP neighbor 關係，而動態學習到往其他 subnet 的路由，於是完成了私有雲內部 Subnets 之間的 routing。RIPv2 的建立過程中，值得注意的是防火牆 iptables 必須開啟 RIP UDP port 520，才能順利建立 RIP neighbor 關係。

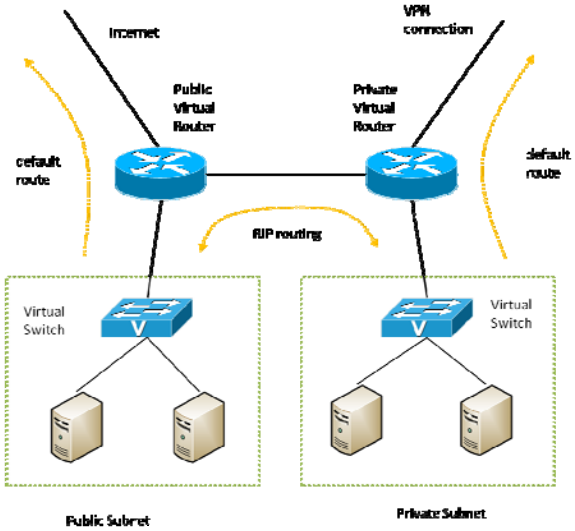

圖4　私有雲 Routing 實作架構

4. SAMEVED 安全性群組

基於安全的考量，VM 上必須設置網路規則（ACLs)來控管進出的訊務。在 VPC 中，可能存在多個相同類型、功能的 VM，例如 Web Server 或 Database。倘若需要去每個 VM 逐一設定相同的 Network ACLs (Access Control List)，那會是極為繁瑣的工作，而且日後只要 Network ACLs 有所異動，又必須重新修改每一台 VM，相當麻煩，因此我們在 SAMEVED 開發安全群組功能。

安全群組是一個虛擬機器的的集合，透過安全群組所定義的網路規則（ACLs），像防火牆一般控制虛擬機器群組允許哪些進出訊務。以 Web Server 的安全群組為例，通常會訂定網路規則如表 1。

表1　WebServerSG 網路規則

Inbound			
Source	**Protocol**	**Port**	**Action**
0.0.0.0/0	TCP	80	allow
0.0.0.0/0	TCP	443	allow
Outbound			
Destination	**Protocol**	**Port**	**Action**
0.0.0.0/0	TCP	80	allow
0.0.0.0/0	TCP	443	allow

Web Server 安全群組在進端方向允許任意來源 IP 的 http、https 連線，在出端方向允許任意目的 IP 的 http、https 連線。安全群組控制群組內 VM 成員的進出訊務，就如同圖 5所示。

支援 SAMEVED 運作的五個角色伺服器各負責不同的工作。我們根據使用者跟角色伺服器的互動方式把角色伺服器配置圖（圖 6）分成兩個部分，第一層是 User Interaction Layer，這一層有 Web Server、Database、Remote API Server 這三種角色伺服器，第二層是 Internal Operation Layer，這一層有 Image Repository 和 XenServer Controller 這兩種角色伺服器。

在 Web Server 提供使用者 Web 介面，輸入使用者需求，例如新增安全群組，管理安全群組成員等等選項。使用者輸入完需求後，Web Server 會到 Database 擷取相關資料，並且將指令與資料傳送到 Xenserver controller，開始執行使用者需求。而使用者需求執行完後，Web Server 會顯示執行結果，並且依據執行結果異動 Database。

Database 存放所有 SAMEVED 需要保存的資料，例如安全群組的網路規則、成員及群組擁有者等資料。

Xenserver Controller 在 XenServer Cluster 上執

行使用者需求。以新增安全群組 VM 成員為例，Xenserver Controller 存放套用安全群組網路規則的腳本（script），腳本內容是根據 VM uuid 查詢 VM 所在的 Xenserver Cluster host 與 domain，然後至該 host 存取 VM console，套用安全群組的網路規則。

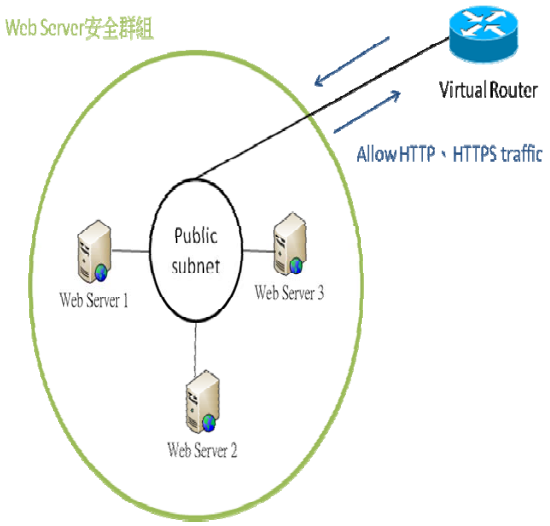

圖5　安全群組示意圖

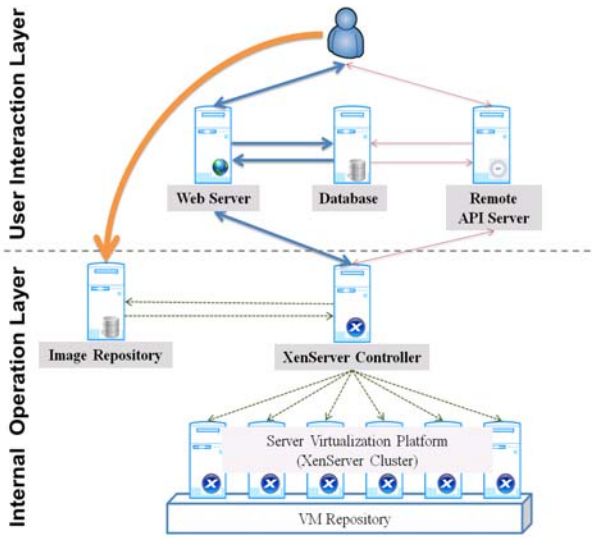

圖6　SAMEVED 角色伺服器配置圖

5. 結論

私有雲使用情境中，在使用者自家網路和私有雲 VPN Gateway 之間建立 L2TP（Layer 2 Tunneling Protocol） over IPsec（Internet Protocol Security）VPN，透過 VPN 連線將使用者的自家網路延伸到私有雲，並且藉由 IPsec 協定，讓封包在經過 Internet 時能確保加密性與存取控制。實作後的 VPN Gateway 可以轉成虛擬機器 template，供 SAMEVED 在建立虛擬機房的 VPN Gateway 時使用，提高 VPN 連線的安全性。

本文在 SAMEVED 上開發安全群組（Security Group）功能。安全群組就像防火牆一般，透過安全群組所定義的網路規則（Network Access Control Lists）控制安全群組允許的進出訊務，僅開啟必要的網路服務 port 並且限制特定 IP 存取服務，可以降低虛擬機器被攻擊的機率，藉此可以更加提升 SAMEVED 虛擬機房的安全性。另外只要定義好安全群組的網路規則和虛擬機器成員，網路規則便能套用到所有的虛擬機器成員，是一個能有效管理虛擬機器防火牆規則的機制。

參考文獻

[1] M. Armbrust et al., “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009.

[2] M. Armbrust et al., “A view of cloud computing,” Communications of the ACM, vol. 53, pp. 50–58, Apr. 2010.

[3] I. Foster, Yong Zhao, I. Raicu, and S. Lu, “Cloud Computing and Grid Computing 360-Degree Compared,” pp. 1-10, Nov. 2008.

[4] B. Furht and A. Escalante, Handbook of Cloud Computing. Springer, 2010.

[5] I. Foster, "What is the Grid? A Three Point Checklist," GRIDtoday, vol. 6, no. 1, 22 Jul 2002.

[6] A. M. Braverman, "Father of the Grid," The University of Chicago Magazine, vol. 4, no. 96, Apr 2004.

[7] Klaus Krauter, Rajkumar Buyya, Muthucumaru Maheswaran, "A taxonomy and survey of grid resource management systems for distributed computing," Software: Practice and Experience, vol. 2, no. 32, pp. 135-164, Feb 2002.

[8] A. Guirao Villalonga, “Infrastructure as a Service (IaaS): application case for TrustedX.”

[9] J. E. Smith and R. Nair, “The architecture of virtual machines,” Computer, vol. 38, no. 5, pp. 32–38, 2005.

[10] R. J. Figueiredo, P. A. Dinda, and others, “A case for grid computing on virtual machines,” 2003.

[11] S. N. T. Chiueh, “A Survey on Virtualization Technologies,” RPE Report, pp. 1–42, 2005.

[12] “Amazon Elastic Compute Cloud (Amazon EC2).” [Online]. Available: http://aws.amazon.com/ec2/.

[13] H. Jing-Ying, "SAMEVED : System Architecture for Managing and Establishing Virtual Elastic Datacenters," 2011.

[14] Jing-Ying Huang, Cheng-Ta Huang and Wei-Jen Wang, "Providing Virtual Elastic Datacenters as a Service," in Symposium on Cloud and Services Computing, National Taiwan University, Taipei, 2011.

[15] E. Walker, W. Brisken, and J. Romney, “To Lease or Not to Lease from Storage Clouds,” Computer, vol. 43, no. 4, pp. 44-50, Apr. 2010.

[16] M. Schumann, An economic decision model for business software application deployment on hybrid Cloud environments. Universitätsverlag Göttingen, 2010.

[17] U. Ermler, G. Fritzsch, S. K. Buchanan, and H. Michel, “Hybrid Clouds : Comparing Cloud Toolkits,” Structure, vol. 2, no. 10, pp. 925–936, 1994.

[18] D. E. Williams, Virtualization with Xen: including XenEnterprise, XenServer, and XenExpress. Syngress, 2007.

[19] “Citrix Systems» Citrix XenServer: Efficient Server Virtualization Software.” [Online]. Available: http://www.citrix.com/xenserver/.

[20] P. Barham et al., “Xen and the art of virtualization,” in ACM SIGOPS Operating Systems Review, New York, NY, USA, 2003, pp. 164–177.

[21] “Xen® hypervisor.” [Online]. Available: http://www.xen.org/.

[22] “OpenStack：Open source software for building private and public clouds.” http://www.openstack.org/

[22]

[23] J. Watson, “VirtualBox: bits and bytes masquerading as machines,” Linux Journal, vol. 2008, Feb. 2008.

[24] “VirtualBox.” [Online]. Available: http://www.virtualbox.org/.

[25] “VMware Virtualization Software for Desktops, Servers & Virtual Machines for Public and Private Cloud Solutions.” [Online]. Available: http://www.vmware.com/.

[26] “Amazon Virtual Private Cloud.” http://aws.amazon.com/vpc/

[27] "Extend Your IT Infrastructure with Amazon Virtual Private Cloud," [Online]. http://d36cz9buwru1tt.cloudfront.net/Extend_your_IT_infrastructure_with_Amazon_VPC.pdf

[28] “xl2tpd” [Online]. Available: http://www.xelerance.com/services/software/xl2tpd/

[29] “Openswan” [Online]. Available: https://www.openswan.org/projects/openswan/

[30] “Quagga” [Online]. Available: http://www.nongnu.org/quagga/