應用 SDN 技術在雲端虛擬環境中建構之網路安全防禦架構

蕭紋旭[a]、洪光耀[b]、吳嘉恩[b]、蘇暉凱[c]、陳景章[d]
吳鳳科技大學應用數位媒體系[a]
國立中正大學通訊工程研究所[b]
國立虎尾科技大學電機工程研究所[c]
國立中正大學電機工程研究所[d]

摘要 —由於雲端技術正大量被應用，各大企業莫不往虛擬化環境尋找更方便快速且省成本的方法。本論文針對虛擬環境中的網路管理以及安全防禦提出一架構來解決傳統實體 Data center 轉換到雲端後可能遇到之實體設備不適用虛擬環境之問題。本架構應用具封包轉向功能之 vSwitch 交換機系統結合具安全政策制定機制的 SPDS 防禦系統來實現虛擬環境中之安全防護架構，透過此系統希望能建構出更安全且快速之網路環境。

一、 簡介

自 2009 年雲端運算[1]的概念被提出以後，各種網路服務紛紛應運而生，各大企業如：Google、微軟、IBM、Amazon 等都大力推廣。使用者只需透過簡單的設備(ex：瀏覽器)連上雲端，便可使用各種龐大的虛擬資源，而不再需要透過實體設備來架設各種環境。透過各種虛擬伺服器與虛擬 Data center 的應用，不僅可以達到集中管理的效用，也能同時擁有低成本與便利性的優點。

本論文提出適用於雲端虛擬環境之安全防禦架構，運用虛擬交換機 Open vSwitch 結合 Openflow 協定來模擬虛擬防火牆，將傳統實體設備之技術與功能轉移到虛擬機器來實現。改善實體安全防禦架構無法運行在虛擬環境之缺點，應用 SDN 技術搭配網路管理元件，提供一便利及可動態管理之虛擬網路安全防禦系統。

二、 相關研究

2.1 雲端的相關安全議題

當實體環境轉換到虛擬環境，資料的管理及分配保存對管理者來說無疑是一大問題，而對於資源的區分規劃及使用者權限的分配等問題對服務提供商來說也是重要課題。以下將列出幾項在雲端環境中會遇到之相關隱憂：

(一). **傳統資安問題：**雖然在雲端環境使採用虛擬化，但由於底層實體機仍然是透過實體網路連接，所以以往在實體網路所會遇到之問題，如：木馬、殭屍、DoS、跳板攻擊、SSL 漏洞…等，還是依然存在。

(二). **跨虛擬機之攻擊：**在虛擬環境中，由於所有的 VM 皆共存於一空間中，所以 VM 與 VM 間的互相攻擊情況更容易發生，而且一旦發生將更容易拓展開來，實為不得不注意之議題。

(三). **網路資源虛擬化後之後續問題：**包括不同系統運行於 VM 中之相容性、各 VM 間之區隔、多租戶共存之應對辦法...等，都是虛擬化後必須克服之問題。

(四). **資料錯置與轉移：**不同使用者間之資料讀取權限由系統分配將更容易出現錯誤，而使用者資料的轉移也是跨雲端服務的重點項目之一。

(五). **個人隱私問題：**使用者在使用服務之時，包括基本資料與各項使用紀錄都將被上傳至雲端儲存，對於雲端服務提供者如何確保個人隱私不外洩將是一大重要挑戰。

本論文將結合前兩項重點做測試，著重在當傳統資安問題發生在虛擬機之間時，系統是否能有效偵測並控制，並且於架構中驗證第三項問題中虛擬機之間的區隔是否能由 vSwitch 來達到。

2.2 虛擬環境之安全防護實現

現行虛擬安全市場中，對於虛擬網路之防禦方法大致還是著重在建構防火牆為較大宗，同時也是許多使用者的基本需求。而常見的防火牆應用則可分為以下四種：

(一). **VLAN 分割：**在虛擬機內建的 Virtual Switch 上用 VLAN 的方式來劃分，切出不同的 VLAN ID 來對權限、網段做控管。

(二). **Agent-based(Ex：Trend Micro DeepSecurity)：**在每個 Guest OS 都安裝個人防火牆，因此在效能影響上較大，軟體授權與管理費用支出也會隨 VM 數量而增加。

(三). **VM- based(Ex：Cisco ASA)：**主要是將舊有的軟、硬體架在虛擬機上，再將所有的流量，包括虛擬機上和各 VM 間的流量導入該設備，好處是對整體網路架構的變動小。

(四). **Kernel-based(Ex：VMware)：**以虛擬化廠商提供的 API 做為基礎，在 Kernel 模式上運行，可掌握 Hypervisor 層的資訊，流量溝通無需藉助 Agent。

本架構中運用了第一項 VLAN 切割之方法並加以改善，運用 vSwitch 來進行切割，並搭配 Openflow 協定與 SPDS 系統來取代實體防火牆進行過濾，達到方便管理及避免封包於虛擬與實體間往返之問題。

2.3 Software Defined Network (SDN)

2009 年的 IEEE INFOCOM 會議上提出了 SDN 架構的概念，而 SDN 網路的傳輸協定 Openflow 則是美國史丹佛大學在 2008 年的未來網路研究計畫中的其中一項專案[2]。

SDN 修改了傳統網路架構的控制模式，將網路分為控制層和資料層，將網路的管理權限交由控制層的控制器(Controller)軟體負責，採用集中控管的方式統一下達指令給網路設備，網路設備則專責於封包的傳遞。

2.4 Open vSwitch

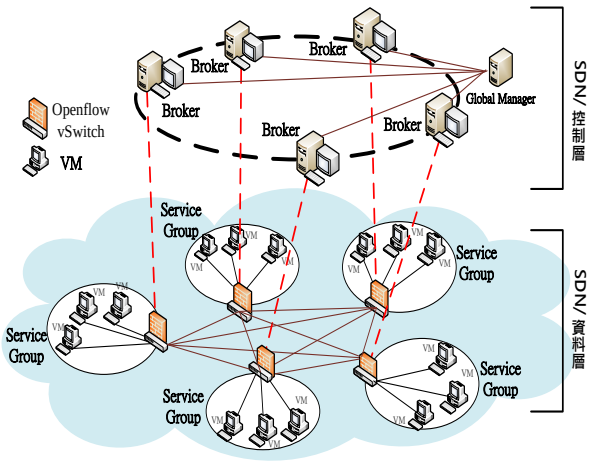
虛擬交換機具備兩項特點，一是配置更加靈活，一台普通的伺服器可以配置出數十台甚至上百台虛擬交換機，且 port 數目可以靈活選擇。二是成本更加低廉，通過虛擬交換機就可以獲得昂貴的普通交換機能達到的性能。而 Open vSwitch 是一個 Apache2.0 授權下的開放原始碼軟體，設計目標是方便管理和配置虛擬機器網路，檢測多物理主機在動態虛擬環境中的流量情況。

三、 系統架構

為了因應雲端環境使用的虛擬網路與虛擬伺服器及資料中心，本論文將結合分散式安全防禦架構[3][4]與安全政策決策系統(Security Policy Decision System)[3]，提出可在虛擬環境中運行之安全偵測與防禦架構。有別於傳統的網路設備及實體機防護，為了能在虛擬環境中運行，並且不失雲端環境的便利性及低成本，所以本架構利用上述兩大系統於虛擬環境中實現，來達到虛擬網路防禦之功效。

3.1 論文系統架構

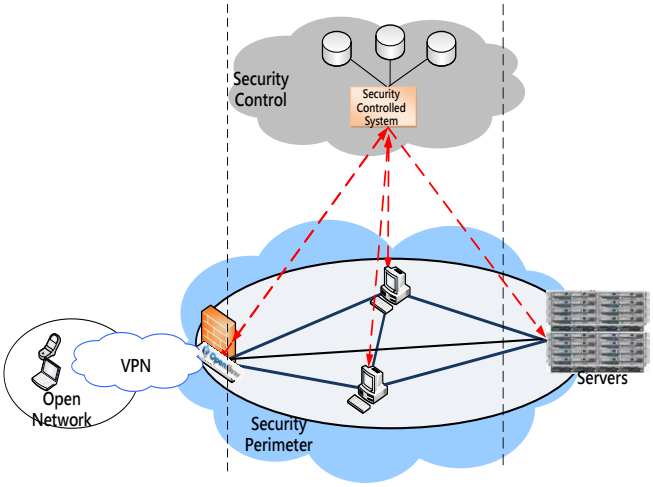
本系統架構如圖一所示，底層為雲端中心內部網路使用 SDN 建立的 Openflow 網路，可經由 Openflow Controller 動態配置 Openflow vSwitch 至每個服務群組中(Service Group)，利用此概念對每個 Service Group 形成一個自訂的安全邊界(Security Perimeter)。另外 Security Controlled System 在此架構中將與 Broker 結合在一起，形成每個 Service Group 的控制中心。透過這些 Broker 互相連結成為 SDN 網路的控制層。



圖一：系統架構圖

3.2 安全防護邊界

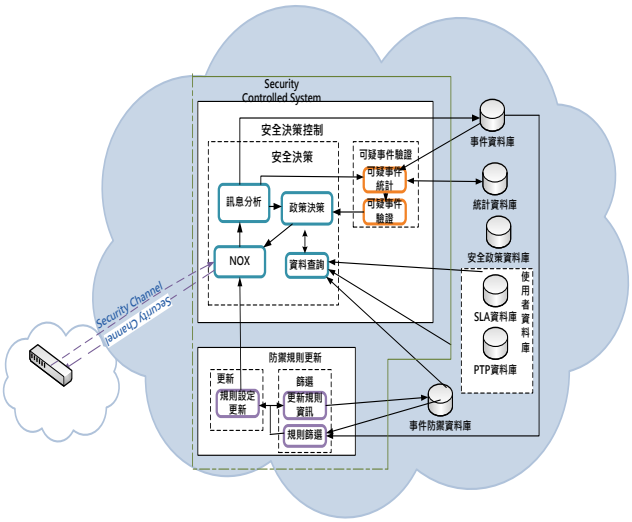
Security Perimeter 形成的防護，如圖二所示，進入的封包會由防火牆進行安全過濾，Openflow vSwitch 會進行 Flow Table 查表是否符合 Policy，如果有記錄就允許進入，提供在內部網路的安全監控，能夠即時的中斷、調整或隔離一些不正常或是具有傷害性的 Flow，一旦違反 Rule 就會被丟棄。相反，如果 Flow Table 並無相關記錄會將資料透過安全通道傳給 Security Controlled System 進行分析與決策，若尚未確認為具有攻擊型的 Flow，經過可疑事件驗證確定攻擊行為，進行政策決策，並將決策交由 Controller， Controller 將分析過的 Flow 透過安全通道傳送給資料層的 Openflow vSwitch 執行決策。



圖二：Switch 隔絕出安全網路示意圖

3.3 防禦制定-Security Controlled System (S.C.S)

Security Controlled System，如圖三所示，分為安全決策控制與防禦規則更新兩部分，安全決策控制有兩大功能分別為安全決策與可疑事件驗證。當 Service Group 中的 Openflow vSwitch 發現可疑 Flow，Flow 被轉送給 Broker 中的 S.C.S，進行訊息分析比對事件資料庫是否有記錄過此訊息，如果尚未有此訊息記錄就送至可疑事件驗證子系統進行驗證，分析或驗證過就進入政策決策，向資料查詢功能進行查詢事件相關資料，其資料庫主要存放網路攻擊防禦內容(Protection Type Profile, PTP)與 Policy 資料，包括安全政策資料庫、使用者資料庫、歷史事件防禦資料庫，根據得到的結果進行政策決策的防禦政策，將制訂出的防禦規則由 NOX Openflow Controller 傳給 Service Group 的 Openflow vSwitch 進行設置。S.C.S 另一部分防禦規則更新，主要是管理 Cloud Data Center 裡的網路設備，會定期詢問檢查各個網路設備，進行防禦規則的篩選和更新。

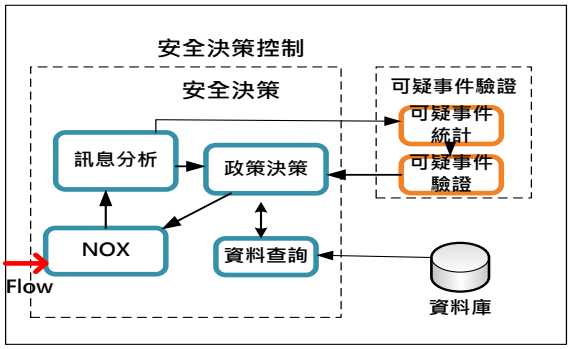


圖三：Security Controlled System 架構

安全決策系統是雲端安全決策控制的核心系統，如圖四所示，主要處理接收 Flow 資訊與網路攻擊事件的防禦政策決策，該子系統內部有幾個功能分別為訊息分析、政策決策、資訊查詢與 Openflow Controller。當 Openflow Controller 接收到 Flow 會傳送給訊息分析進行分析。Openflow Controller 接收到可疑 Flow 會先查詢 vSwitch Flow Table 是否有 Flow 記錄，若沒有記錄， Openflow Controller 做警報記號，當訊息分析收到訊息後，分析訊息會根據是否有警報記號決定是否將進行可疑事件驗證。再把分析的結果交給政策決策。

政策決策是做為決定網路攻擊事件要如何設置防禦規則的決策功能，所以該功能主要處理訊息分析送來的已確認惡意封包，每當收到已確認的攻擊事件訊息就會向資料查詢資料庫搜集與事件相關的訊號，根據得到的結果進行防禦政策的政策決策。

若攻擊行為未確認，便將資訊送至可疑事件驗證子系統，當可疑事件驗證接收到事件資訊，便會進行可疑事件統計，如果事件的統計累計達到門檻時，就會進一步進行可疑事件驗證，經過驗證後判斷為攻擊事件則進行防禦政策決策，判斷為非攻擊事件則將該事件的特徵規則從特徵規則庫移除。



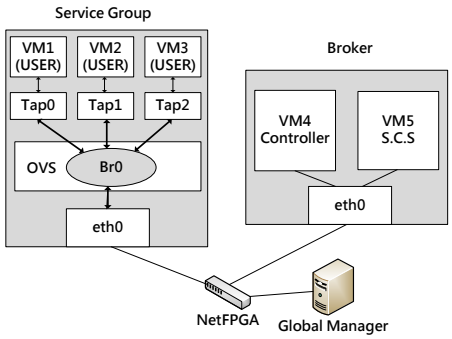
圖四：安全決策控制系統圖

3.4 Service Group 架構

本架構利用 Openflow vSwitch 當作封包過濾防火牆。在雲端環境內建立出眾多小型的 Service Group，並且由一個 Openflow vSwitch 來過濾所有流量及封包，藉此形成一安全邊界(Security Perimeter)。每個 Openflow vSwitch 擁有自己所屬 Service Group 的 Flow Table。透過建置在 Broker 中的 Controller 來下指令給 Openflow vSwitch 讓其執行封包流量處理並更新防禦列表。本論文採用網路管理中 Agent 的概念，來管理監控每一個 Service Group，並將其提升層次為 Broker。再與 S.C.S 結合，設置在每個 Service Group 中，由 Broker 來確實掌握每個 Service Group 中 VM 的狀況，定時回報給 Global manager 以便於系統管理員掌控整體雲端環境中的網路狀況。

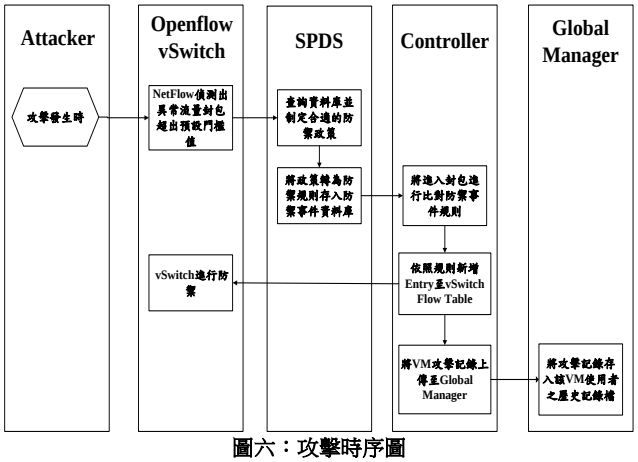
四、 系統流程與模擬

受限於實驗環境及工具有限，在本論文中先以單一一個 Service Group 為目標進行實作模擬。另外，為了測試系統的實用性，在模擬環境中先以 ICMP flood 為主要測試攻擊方法。模擬環境由三台實體機建構，並且都運用虛擬機來運作系統架構中之各元件。如圖五所示，以 NetFPGA 運行 Openflow protocol 當作交換機來讓三個虛擬環境能有效地運行及互相溝通。



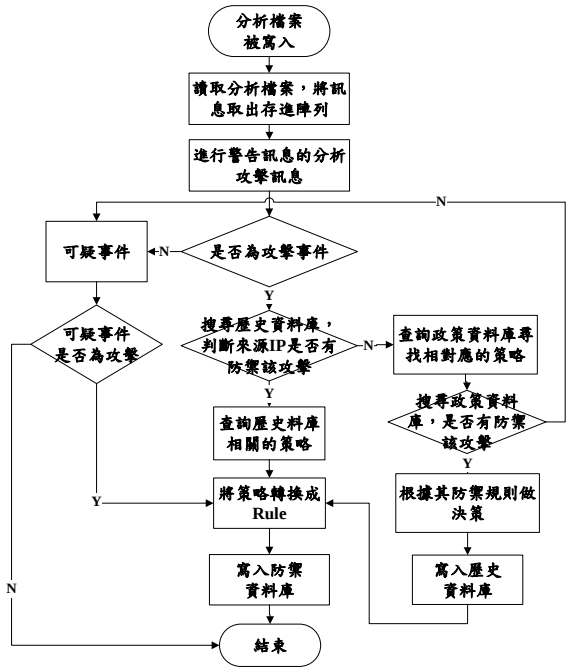
圖五：模擬環境架構圖

本論文引用[5]之統計 Threshold 當作監控系統預設值，於 VM 間互相進行 ICMP flood 攻擊，透過 vSwitch 及 NetFlow 偵測。圖六所示為各部份元件執行工作之攻擊時序圖。



圖六：攻擊時序圖

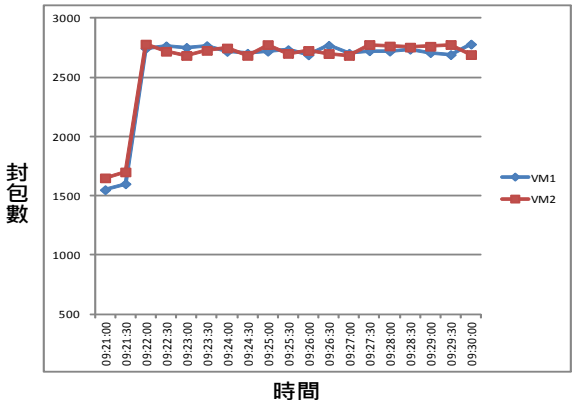
SPDS 收到確定為攻擊之訊息後會開始進行防禦行為判定，防禦行為決定後會新增防禦規則，並更新規則至事件資料庫。處理流程如圖七所示。



圖七：SPDS 制定規則流程

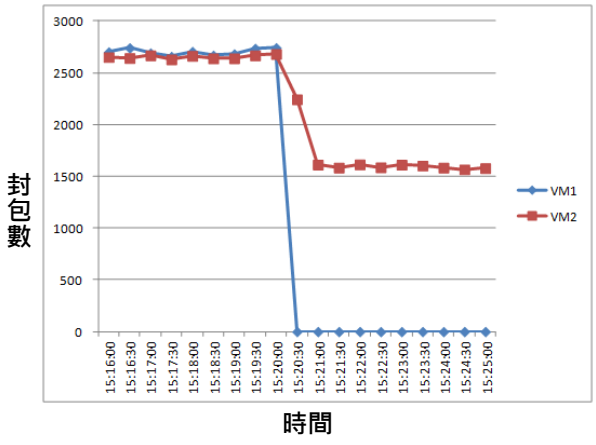
SPDS 制定完防禦規則後，Controller 會根據此防禦規則新增 Entry 到 Openflow vSwitch 的 Flow Table 中，最後由 vSwitch 進行攻擊阻擋。

透過 NetFlow 偵測出在每個 VM 中之背景流量，以 Iperf 工具，每 30 秒變換一次封包數並以固定頻率打入每個 VM 中。再透過 vSwitch 上配給每台 VM 之 port 端口流量來做偵測，接著再以 ping death 工具從 VM1 對 VM2 送出大量攻擊封包，偵測到 VM1 與 VM2 封包流量皆瞬間衝高，如圖八所示。



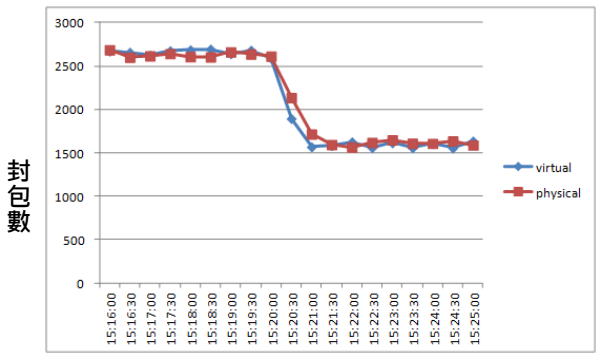
圖八：送入攻擊後流量

後續進度為結合 MySql 資料庫及 SPDS 系統來進行自動判斷及阻止攻擊。Controller 修改與配合 Openflow vSwitch 之 Flow Entry 新增機制，來達到阻斷攻擊，受攻擊目標之流量也在短時間內回復正常流量值，如圖九所示。



圖九：攻擊阻擋後流量

在防禦效果方面，為了比較傳統 VLAN Segmentation 之透過實體防火牆之防禦方法與透過虛擬防火牆之防禦方法的效能差別，本論文利用從攻擊發起後到防禦處理時間表來比較兩者的差別，如圖十所示。



圖十：實體與虛擬之反應時間比較

五、 結論

本論文將實體設備使用虛擬設備來取代，以因應雲端虛擬環境之安全需求，但是虛擬設備在效能的比較上確實較無法優於實體設備，但相對優點卻是擁有較高的佈置彈性及使用便利性。

參考文獻

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing,"

[2] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner," Openflow : Enabling Innovation in Campus Networks",ACMSIGCOMM Computer Communication Review, Vo1 38, pp.69-74,April 2008

[3] 余孟儒, "以服務等級協定為基礎的網路安全聯防策略管理之研究與實作", 國立中正大學電機研究所碩士論文, 2010.

[4] 魏宇翔 "以服務等級協定為基礎的網路安全防禦系統之防禦資源管理機制研究", 國立中正大學電機研究所碩士論文, 2011

[5] 葉曉霈,蕭紋旭,陳景章,“以OpenFlow 交換器建構網路安全防禦系統之研究與實　現”,2013全國電信研討會, 國立中正大學通訊研究所碩士論文,2013