

# 以合作式防火牆實現合作防禦與縱深防禦<sup>1</sup>

游啟勝

陳奕明<sup>2</sup>

中央大學資訊管理學系 電腦網路實驗室

skyo@mgt.ncu.edu.tw cym@mgt.ncu.edu.tw

## 摘要

隨著網路應用環境日益複雜與駭客攻擊技術的進步，目前已沒有單一的網路安全防禦機制能一次解決所有的網路安全問題，唯有同時使用多種不同的防禦機制才能加強安全防護。本文首先說明縱深防禦 (defense-in-depth) 與合作防禦 (cooperative defense) 的概念，並以合作防火牆為例，提出三種可能進行的合作防禦方式，對其合作對象、合作方法及能達到的效果進行說明。接下來探討各種合作防禦方式可能遭遇到的問題，及就目前已出現的可能解決方案進行說明。

**關鍵詞：**合作式防火牆、合作防禦、縱深防禦、網路安全防禦

## Abstract

Because of the popularity and variety of network applications, there is no single defense mechanism of network security that can solve all security threats. A possible solution is to use several different mechanisms to enhance the strength of defense. This article explains the concepts of defenses-in-depth and cooperative defense at first, and then propose three possible schemes of cooperative defense. Finally, we discuss their difficulties and collect possible solutions of it.

**Keywords:** Cooperative Firewall, Defense-in-Depth, Cooperative Defense, Defense of Network Security

## 1. 前言

隨著網際網路的普及與使用人數的增加，網路應用的種類也更加多元化，眾多的服務可以在網路

上取得，使得網路安全的議題逐漸被人們所重視。近幾年來，除了攻擊事件數目急劇增加之外，攻擊的手法也日新月異。因此，傳統的單一安全防禦機制已無法防禦所有的攻擊行為，結合多種防禦機制進行合作防禦及縱深防禦已成為未來趨勢。舉例來說，防火牆無法判斷已允許通過的網路連線是否含有攻擊行為，因此無法找出類似更改通訊埠的後門連線或是利用緩衝區溢位攻擊對外開放的伺服器服務等的攻擊行為。

為解決上述問題，本文提出以合作式防火牆 (cooperative firewall)[2] 結合其他重要的網路安全防禦機制(如入侵偵測系統)來進行合作防禦與縱深防禦，希冀能防禦更多的攻擊行為及加強防禦的強度。例如防火牆加上入侵偵測系統後，就可在偵測出攻擊行為的第一時間，就切斷攻擊連線以避免更大損害的發生。由於合作式防火牆是採用分散式的架構，擴充性良好，所以合作式防火牆的概念不但可用於區域網路，對於廣域骨幹網路(例如國家寬頻實驗網路, NBEN)也適合採用此種機制以提高整體網路的安全性。

本文共分五節。第二節介紹縱深防禦與合作防禦的概念。第三節以合作式防火牆為例，提出三種可進行合作防禦的對象及其合作方式。第四節說明三種合作方式目前面臨的問題及相關的解決方案。第五節做一簡要結論。

## 2. 縱深防禦與合作防禦

縱深防禦 (defense-in-depth) [1,3] 的基本概念是結合多種不同的安全防禦機制互相彌補個別安全機制的不足來加強防禦的強度。此外，縱深防禦也假設任何個別的防禦機制都可能失效，此時其他的防禦機制仍可以進行防禦。所以縱深防禦可以增廣防禦的範圍及提供更好的容錯程度。

合作防禦 (cooperative defense) 則強調各防禦

<sup>1</sup> 本研究由國科會補助研究，為國家寬頻實驗網路 (NBEN) 研究計畫一部份，計畫編號：NSC-91-2219-E008-009

<sup>2</sup> 本論文之聯絡人

機制間藉由交換資訊共同對某一攻擊進行防禦，兩個防禦機制可以是相同機制或是不同機制。

縱深防禦與合作防禦最大的不同是縱深防禦強調防禦機制的多元性，但各機制之間不一定需要互相交換資訊。而合作防禦則強調防禦機制間的溝通與合作。以圖 1 為例，此示意圖中含有防火牆、網路式入侵偵測系統、主機式入侵偵測系統及陷阱系統四道種防禦機制。其中，A 類攻擊可以被防火牆直接阻擋。B 類及 C 類攻擊雖然可以通過防火牆，但會被網路式入侵偵測系統所偵測，然後加以阻擋或導入陷阱系統。D 類攻擊可逃過防火牆及網路式入侵偵測系統的阻擋及偵測，但會被主機式入侵偵測系統所偵測，並導入陷阱系統。只有四種防禦機制都認為是正常連線的 E 類連線才可以通過各道防線存取網路資訊系統。

結合四種防禦機制進行縱深防禦可以防禦較多的攻擊種類。另外，即使有其中一道機制失效，例如：防火牆失去防禦功能，A 類攻擊仍可能會被兩種入侵偵測系統所偵測到。這也是縱深防禦最主要的兩個優點。

在示意圖中，也可以看見各種防禦機制進行合作防禦。在圖 1 中，入侵偵測系統發現 C 類與 D 類攻擊時，入侵偵測系統必須與防火牆或路由器溝通，告知防火牆哪一個是可疑的攻擊連線，防火牆才能將連線導入陷阱系統中觀察。此時，入侵偵測系統便與防火牆進行合作防禦。另一個常見的例子是利用多個防火牆進行合作防禦來防治分散式阻斷服務攻擊。

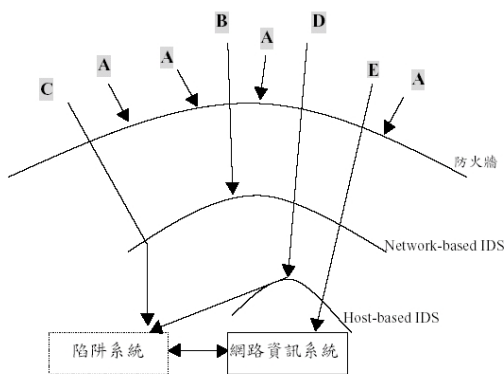


圖 1 縱深防禦與合作防禦示意圖  
(資料來源：[1])

### 3. 以合作式防火牆達成縱深與合作防禦

防火牆藉由控制網路的重要出入口，如同公司大門的警衛，檢查來往的網路通訊，再根據組織制訂的通行規則來決定放行與阻擋連線，成為網路安全防禦的第一道防線。雖然目前網路安全防禦機制相當眾多，除了防火牆之外，還有入侵偵測系統、誘補系統等。但防火牆仍是目前最有效的攻擊回應機制，因為藉由阻擋攻擊連線才能確實中斷攻擊的

進行。舉例來說，入侵偵測系統偵測到攻擊後，仍需要與防火牆配合來對攻擊連線進行阻擋。防火牆對網路安全防禦的重要性可見一斑。

本文以合作式防火牆為例，說明合作式防火牆可能進行合作防禦的對象及方式，及可能遭遇的問題及解決方式。本文的合作式防火牆定義為採用分散式防火牆[4,5,6]架構，並能與各種防禦機制進行合作防禦的防火牆系統。所謂分散式防火牆是具有中央控制端及多個分散於欲防禦主機上的防火牆系統，中央控制端負責制訂規則，而規則的執行與判斷則在各個欲防禦的主機上，就架構而言，我們認為它是可中央控管的分散式主機型防火牆(Host-based IDS)系統，與主機型防火牆不同的是分散式防火牆以憑證來識別通訊對象及具有中央制訂規則的特性。

分散式防火牆並不提供防火牆與其他安全機制間的合作，而這正是合作式防火牆的特點，以下說明合作式防火牆與三種安全防禦機制如何進行合作：

#### 3.1 防火牆之間進行合作防禦

防火牆之間所進行的合作防禦主要利用互相傳遞防火牆的政策規則 (policy rule) 來達成 (參見圖 2)。

因為合作式防火牆使用分散式防火牆的架構，屬於主機式防火牆。因此可以與目前最常用的網路式防火牆(Network-based IDS)進行合作。藉由交換規則，網路式防火牆能在負擔過重時，將部份較特定的規則 (例如阻擋某些主機的 http 連線) 交由合作式防火牆處理，將處理動作分散至各台主機中，藉此減少網路式防火牆的負擔。另外，由於分散式防火牆屬於主機式防火牆，能以直接查詢本機應用程式開啟的通訊埠或連線來輕易地處理類似 FTP 動態分配通訊埠的協定。因此，此類應用的防火牆規則便可集中在主機上的合作式防火牆中。當真正要連線時，合作式防火牆再通知網路式防火牆開啟對應的通訊埠即可，一旦連線結束，也可再通知網路式防火牆關閉該通訊埠。如此一來，網路式防火牆不需要解析應用層協定就能處理有關動態分配通訊埠的協定，同時網路式防火牆只需開啟真正需要使用的通訊埠，避免非必要的連線開啟，因此降低網路遭到攻擊的風險。

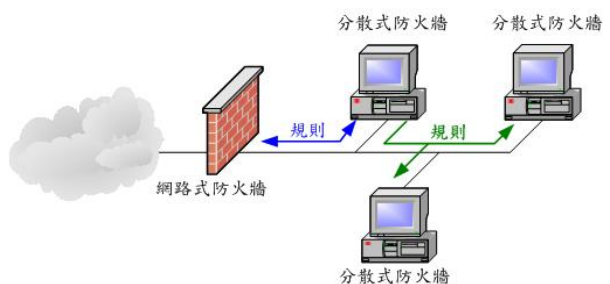


圖 2 防火牆之間進行合作防禦

### 3.2 與入侵偵測系統進行合作防禦

入侵偵測系統與防火牆進行合作防禦的最終目的是在入侵偵測系統發現攻擊時，能及時用防火牆來阻擋攻擊（如圖 3 所示）。要達到這個目的，目前的方法是使用入侵偵測系統的主動回應機制 [19]，以 snort [7] 為例，提供了 TCP Reset 與 ICMP Unreachable 兩種主動式回應機制，但這兩個方式可能會因有時間差無法有效地阻擋攻擊連線。另外，這兩個方法皆使用假造封包動作產生 TCP Reset 與 ICMP Unreachable，並不適用於往後 IPv6 的應用環境。

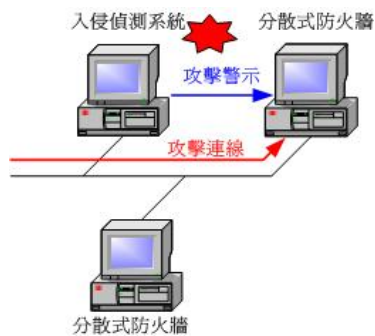


圖 3 合作式防火牆與入侵偵測系統進行合作防禦

防火牆與入侵偵測系統合作防禦可能的實作方式有二種，第一種方式是將入侵偵測系統及防火牆分為兩個不同的系統，在發現攻擊時，入侵偵測系統與防火牆溝通，利用防火牆來阻擋攻擊。第二種是將入侵偵測系統與防火牆合而為一，也就是入侵偵測及防禦系統 (IDPS, Intrusion Detection and Prevention System)，所有的連線必須經過攻擊檢驗確定不是攻擊連線才能放行，目前業界熱門的 IPS [9,10] 即屬此類，目前業界認為入侵偵測與預防系統就是入侵預防系統，也是下一代的入侵偵測系統，能「在偵測到攻擊行為後，自動採取回應動作來阻止或減小攻擊行為所造成的傷害」。自由軟體領域中則以 snort-inline [8] 計畫最為熱門。

以第一種方式而言，優點是可以使用多個不同的入侵偵測系統來增加偵測的攻擊種類，但是面臨的最大問題是偵測到攻擊後，可能無法及時利用防火牆來阻擋攻擊，但仍能有效防禦後續攻擊連線。而第二種方式最大的優點是被判斷為攻擊連線可以完全被阻擋，但因為入侵偵測及防禦系統本質上是防火牆，會面臨效能及發生誤判時影響程度大等問題。目前最普遍的入侵偵測方式仍使用誤用偵測 (misuse detection) 方式。因此，來往的通訊可能需要比對眾多的攻擊特徵才能確定此通訊不是攻擊行為，比對的動作會比原本的防火牆更多，對效能的影響會比防火牆來得更嚴重。

### 3.3 與漏洞掃描系統進行合作防禦

漏洞掃描系統，如：Nessus [11]、SARA [12]、ISS Internet Scanner [13]，最主要的功能是用來偵測一個系統存在的漏洞或是錯誤設定。因為大多數的攻擊都是針對某個漏洞或是錯誤設定而來，漏洞掃描系統的目的就是找出這些可能遭受攻擊的漏洞或設定，再利用修正這些漏洞及錯誤設定來避免被入侵。

遺憾的是，目前在做完漏洞掃描動作之後，仍沒有一個好的機制能在修正漏洞前，防止這些漏洞遭受攻擊。這是因為以往的網路式防火牆只能以網路連線為基礎來阻擋連線，無法阻擋外表正常的漏洞攻擊（如 Buffer overflow 攻擊）。而使用合作式防火牆之後，一旦發現漏洞，能藉由阻擋漏洞應用程式的所有連線來防止此漏洞遭受攻擊。也能利用漏洞掃描系統加上漏洞修正判斷機制，在漏洞或是錯誤修正之後，與防火牆溝通，自動恢復程式的正常通訊。

圖 4 說明了分散式防火牆如何與兩種不同種類的漏洞掃描系統進行合作防禦。與網路式漏洞掃描系統合作時，漏洞掃描系統結束漏洞掃描動作後，可產生漏洞應用程式列表，再轉換成漏洞規則傳送至合作式防火牆中，合作式防火牆就可以對漏洞應用程式連線進行阻擋，達到防禦的目的。使用主機式漏洞掃描系統時，可以發送漏洞描述給分散式防火牆，防火牆再觸發主機式漏洞掃描系統檢查該漏洞，如果該漏洞存在，則阻擋該漏洞應用程式連線。主機式漏洞掃描系統也可以作為分散式防火牆的漏洞修正判斷機制，防火牆可定時呼叫主機式漏洞掃描系統檢查之前有漏洞或含有錯誤設定的應用程式是否已做修正，來決定是否移除連線阻擋規則。如此一來，我們可以得到一個自動化的漏洞防禦機制，能在應用程式有漏洞時阻擋其連線，防止被攻擊，而在漏洞應用程式進行修正後，恢復其連線通訊。

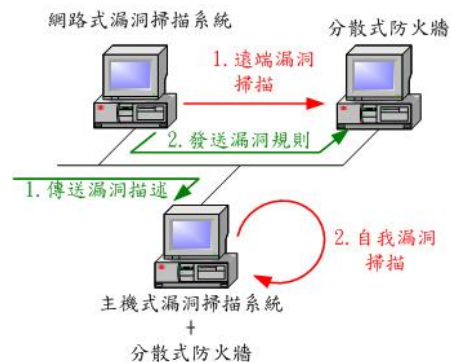


圖 4 合作式防火牆與漏洞掃描系統進行合作防禦

## 4. 目前的問題及解決方式

雖然上述的合作防禦方式都能夠加強防禦效果，但是三種合作方式仍需要解決一些問題。以下分別描述它們所遭遇的問題：

### 4.1 目前的問題

#### ● 問題一：防火牆之間如何交換防禦規則？

合作式防火牆與網路式防火牆合作防禦時，只能交換網路式防火牆能接受的以網路連線式政策規則，而主機式防火牆特有的應用程式式政策規則則無法使用。

合作式防火牆之間的合作防禦是藉由交換互相的規則來達成，但是相同的安全問題只會發生在運作環境相似的情形下。各主機的運作環境不同時，交換的防火牆政策規則可能還會造成誤擋正常連線。另外，交換的規則可能也無法直接套用在主機上，一個常見的例子是同樣的服務可能使用不同的通訊埠號，此時若是直接套用固定通訊埠號的政策規則，反而會造成套用不適當的規則。

解決方式是使用較抽象化的政策規則語言，避免描述會隨每台主機不同的運作細節，而這些隨主機不同的資訊等到在主機端後再取得。FireHOL 計畫[14] 實現了通訊埠的抽象化，藉由只描述服務名稱，再從主機端取得真正的通訊埠號。另一個方式是以應用程式為基礎來設定政策規則，再判斷系統上的應用程式環境是否符合。

外，還需要加入對系統平台資訊的資訊來描述運作環境，因為分散式防火牆可能運作於不同平台的主機上，加入系統平台描述，可以使規則能更精確地套用於合適的分散式防火牆主機上。

#### ● 問題二：合作式防火牆與入侵偵測系統合作後的效用與效能問題

合作式防火牆與入侵偵測系統合作的第一種方式是防火牆與入侵偵測系統分散在不同的主機上，此時入侵偵測系統在查覺攻擊行為後，只需將連線資訊，如 IP、通訊埠等，送給防火牆即可進行連線阻擋，所交換的資訊並不需要額外的描述內容。另一種方式則是防火牆與入侵偵測系統合而為一的入侵偵測及防禦系統，這時只要將防火牆中原本的規則比對動作改變為入侵偵測動作，也沒有資訊傳遞問題。

因此，防火牆與入侵偵測系統合作防禦最大的問題在有效阻擋攻擊及效能兩方面。若是上述第一種合作方式，發現攻擊後，入侵偵測系統傳送欲阻擋的連線資訊給防火牆進行阻擋與第一時間有不定時間差，可能無法即時阻擋攻擊，但仍有可能以阻擋來源位址的方式阻擋後續攻擊。第二類入侵及防禦系統最大問題則在效能，因為所有連線都必須比對過所有的攻擊特徵才能決定此連線不為攻

擊連線，而且攻擊特徵必定會逐日累積而愈變愈多，效能也會愈來愈低。

另外，入侵偵測的偵測率與正確性是決定入侵偵測系統與防火牆防禦是否成功的關鍵。過高的誤報率（false positive rate）會使防火牆阻擋過多的正常連線，過高的漏報率（false negative rate）會減低合作防禦的效用，許多攻擊將會無法進行防禦被偵測及防禦。

#### ● 問題三：合作式防火牆與漏洞掃描系統應交換哪些資訊？

要使用防火牆來阻擋漏洞應用程式的連線與定時檢查漏洞應用程式的修補狀況來自動移除阻擋規則，在網路式漏洞掃描系統發送給分散式防火牆的漏洞描述中，至少需要漏洞應用程式的相關資訊來讓分散式防火牆進行阻擋動作，例如程式名稱、版本等。也應包該漏洞編號來供主機式漏洞掃描系統將來再次檢查此漏洞。

### 4.2 現有解決方式

以上三種合作防禦的主要問題是缺乏一個完整的規則描述語言，能用來描述各合作防禦安全機制間所需要交換的資訊。以上一節所描述的情形為例，這個規則語言必須至少能夠描述基本的主機運作環境，如：主機作業系統種類及版本、硬體平台、應用程式名稱及版本，供防火牆判斷交換的規則是否適用於自身的主機。要能描述漏洞基本資訊，例如：漏洞名稱、漏洞編號、漏洞說明、漏洞程式名稱，供漏洞掃描系統將漏洞描述資訊送給防火牆阻擋漏洞應用程式或是做進一步判斷程式是否仍有漏洞之用。

以下我們針對目前已經出現的相關研究進行討論。

#### ● High Level Firewall Language (HLFL) [15]

HLFL 提供了一個較高階的防火牆語言，目的是用來解決不同種類防火牆管理困難的問題。藉由使用 HLFL 來描述防火牆規則，可以將同一個規則轉換成各種真正運作的防火牆規則，例如同一個 HLFL 規則可以轉換成 ipfw、Cisco ACL、IPFilter、IPFWadm、IPChains、NetFilter/IPTables 這些防火牆的規則。對於各種防火牆具有的特殊功能，也可以藉由 HLFL 提供的條件命令註解來加以描述。舉例來說，HLFL 用來阻擋所有連線的規則如下：  
*all (any) X log (any)*

它可以轉成三種不同的防火牆系統規則。

ipfilter :

```
block out log quick from 0.0.0.0 to 0.0.0.0  
block in log quick from 0.0.0.0 to 0.0.0.0
```

```
ipfw :
ipfw="/sbin/ipfw -q"
$ipfw -f flush
```

```
$ipfw -f add deny log all from 0.0.0.0/0 to 0.0.0.0/0
out
$ipfw -f add deny log all from 0.0.0.0/0 to 0.0.0.0/0
in
```

```
netfilter :
iptables="/sbin/iptables"
$Iiptables -F
$Iiptables -X
$Iiptables -A OUTPUT -l -s 0.0.0.0/0 -d 0.0.0.0/0 -p all
-j DROP
$Iiptables -A INPUT -l -s 0.0.0.0/0 -d 0.0.0.0/0 -p all
-j DROP
```

因此，防火牆管理者依實際情況可以在撰寫一次規則後，將它使用在多個不同的防火牆上。因為這些防火牆需要交換規則時，可以先轉成 HFHL 規則，再轉成真正要運作的防火牆規則種類。這個方法可解決大部份的防火牆之間的網路連線規則溝通問題，但無法解決與防火牆以外的安全機制之合作防禦問題。

- FireHOL [14]

FireHOL 也是一種高階的防火牆語言，但只能轉換成 iptables 規則，它的主要目的是增加規則的易讀性及易學性，使得規則的設定變得更容易及更直覺。同時，它可以視服務被設定為客戶端(client)或是伺服器端(server)來決定這個服務實際的通訊埠為何，在 FireHOL 的規則中，只會出現應用程式名稱，而不會直接出現通訊埠號，通訊埠號由存在於各主機的設定檔取得。就某種程度來說，FireHOL 已經具有一定的抽象化概念，能避免描述會隨主機不同運作細節，因此規則比較可能在不同主機上使用。相同地，FireHOL 無法解決與防火牆以外的安全機制之合作防禦問題。

- VulXML [16]

VulXML 提出了一個 XML 格式的漏洞描述語言，目的是用來描述漏洞與安全通報。利用 VulXML 來描述的漏洞可以直接被漏洞掃描系統直接用來檢查漏洞，或是其他工具來取得此漏洞的相關資訊。但目前 VulXML 只能描述 Web 應用程式的漏洞，藉由真正建立連線，送出檢查要求，並視對應的回應訊息來找出漏洞。

- Open Vulnerability Assessment Language (OVAL)

OVAL [17] 提供一種類似 SQL 語法的漏洞描述語言，可用來描述漏洞資訊，供漏洞掃描系統檢查漏洞是否存在。與 VulXML 最大的不同是檢查的漏洞不限於 Web 應用程式，而可以是 Windows NT、Windows 2000、Solaris 作業系統上

的任一漏洞。OVAL 利用類似主機式漏洞掃描系統中檢查應用程式狀態、應用程式的執行身份等動作來檢查漏洞是否存在。

- Application Vulnerability Description Language (AVDL)

AVDL [18]的目的是使用一致的 XML 格式文件來描述相同的漏洞，這個漏洞描述並能成為各種防禦機制溝通的媒介。例如同一個漏洞描述可供漏洞掃描系統找出漏洞、供防火牆阻擋漏洞應用程式、供事件管理系統產生事件報告、及漏洞修正系統修正漏洞。

圖 4 是目前使用多種安全機制的情況，我們可能使用漏洞掃描系統發現漏洞(FIND)，希望使用防火牆阻擋漏洞程式 (BLOCK)，或是利用漏洞修正系統修正漏洞 (FIX)，最後利用報表系統產生此漏洞的修正及事件報告 (REPORT)。整個流程中，有許多資訊是重疊及相關的，但因為各安全機制無法互相交換需要的資訊。因此在此例中，發現、阻擋、修正、報告此數個動作仍無法自動地整合在一起，仍需要人力的介入。

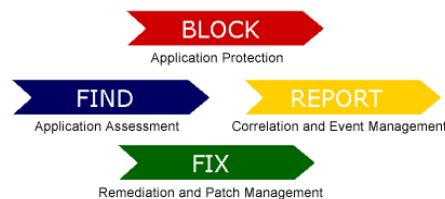


圖 5 獨立運作的安全防禦機制 (資料來源：[18])

AVDL 希望能提出一個 XML 格式的語言能完整描述這些資訊，然後便可以自化動整個流程。圖 5 的四個安全防禦機制便可以整合成如圖 6。而這也是本文提出的合作防禦概念。

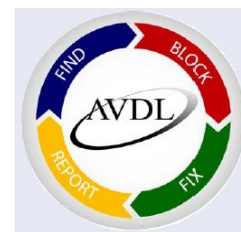


圖 6 進行合作防禦的安全防禦機制 (資料來源：[18])

根據以上現有的相關研究，AVDL 比較接近合作式防火牆的需要，因為它提供了各安全機制整合之間的溝通語言，但是它仍在草擬階段，未提出足夠的實例，我們無法得知是否真正足夠描述主機的運作環境來支援多個防火牆的管理。HLFL 及 FireHOL 雖然解決防火牆的管理問題，使得防火牆之間的管理及規則的制訂變得更容易，但是仍然少

了對運作環境描述，無法讓防火牆自動判斷規則是否應該套用，但 FireHOL 已將避免直接描述通訊埠號，而以服務名稱代替後再取得實際通訊埠的概念符合部份通用規則的目的。VulXML 及 OVAL 提供了二種漏洞描述語言，但它們仍偏重於供漏洞掃描系統找出漏洞，而事實上，檢查漏洞不是合作防禦的重點，我們只需要知道漏洞的編號，就可以利用漏洞掃描系統檢查漏洞，我們需要的是漏洞掃描系統在找到漏洞後，能傳出什麼資訊供防火牆來阻擋漏洞攻擊，而不在乎漏洞的檢查方法。因此，目前的幾個解決方式仍無法滿足我們的需求，仍需要一個新的規則描述語言來整合各種防禦機制。

## 5. 結論

目前的網路應用環境，已沒有單一的網路安全防禦機制能一次解決所有的網路安全問題，唯有同時使用多種不同的防禦機制才能加強安全防護。本文提出的合作式防火牆能整合防火牆、入侵偵測系統及漏洞掃描系統等網路安全機制。這些機制間若能進行合作防禦將能加強防禦的強度。但目前各安全機制間在溝通時的交換資訊動作仍有相當困難，最主要是沒有一個完整的描述語言來描述各種防禦機制所需要的資訊。本文中，我們對這個問題探討了目前可能的解決方式，結論是認為還需要一個新的描述語言來整合各個安全防禦機制。這個語言需要可以完整描述系統運作環境及漏洞的資訊供各個防禦機制使用。一旦擁有完整的描述語言，聯合各種安全防禦機制的合作防禦即可以達到自動化及即時化。

## 參考文獻

- [1] 曾宇瑞，「網路安全縱深防禦機制之研究」，國立中央大學資訊管理學系碩士論文，民國 89 年 6 月。
- [2] 游啟勝，「合作式防火牆之設計與應用」，國立中央大學資訊管理學系碩士論文，民國 92 年 6 月。
- [3] Steve Bridge, “Achieving Defense-in-Depth with Internal Firewalls”, August 2001.
- [4] Steven M. Bellovin, “Distributed Firewalls”, ;login:, November 1999, pp. 39-47.
- [5] Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith, “Implementing a Distributed Firewall”, ACM Conference on Computer and Communications Security, Athens, Greece, November 2000.
- [6] Wei Li, “Distributed Firewall”, December 2000.
- [7] Snort: The Open Source Network Intrusion Detection System, <http://www.snort.org/>.
- [8] Snort-inline Projects, <http://www.honeynet.org/papers/honeynet/tools/>.
- [9] ISS Guard NIDP 100, [http://www.iss.com.tw/product/iss\\_guard.php](http://www.iss.com.tw/product/iss_guard.php).
- [10] NetScreen-IDP, [http://www.netscreen.com/products/datasheets/ds\\_ns\\_idp.jsp](http://www.netscreen.com/products/datasheets/ds_ns_idp.jsp).
- [11] Nessus Project: A free, powerful, up-to-date and easy to use remote security scanner, <http://www.nessus.org/>.
- [12] SARA Project: Security Auditor's Research Assistant, <http://www-arc.com/sara/>.
- [13] ISS Internet Scanner, [http://www.iss.net/products\\_services/enterprise\\_protection/vulnerability\\_assessment/scanner\\_internet.php](http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php).
- [14] FireHOL Project, <http://firehol.sourceforge.net/>, September 2002.
- [15] High Level Firewall Language Projects, <http://www.hlfl.org/> and <http://freshmeat.net/projects/hlfl/>.
- [16] VulXML Project: A Web Application Security Vulnerability Description Language, <http://www.owasp.org/vulnxml/>, October 2002.
- [17] OVAL, Open Vulnerability Assessment Language, <http://oval.mitre.org/>, October 2002.
- [18] AVDL, Application Vulnerability Description Language, <http://www.avdl.org/>, April 2003.
- [19] Kathleen A. Jackson, “Intrusion Detection System Product Survey”, June 1999. <http://downloads.securityfocus.com/library/idssurvey.pdf>