網路安全管理

報告人：葉文章

課程內容

- 網路安全概論
- 防火牆與網路防禦機制實務
- 如何以Iptable/Snort保護Linux安全
- 如何以Personal Firewall確保Windows Server安全

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網路安全管理

網路安全概論

網際網路幾已成生活必需品

- 最新調查顯示，台灣網路使用人口已達1476萬人，個人上網普及率為64.4%
- 網路電話、部落格、即時通訊等應用的使用人口上，自2003至2007年的年複合成長率分別高達46.8%、40.7%與24.4%，成長急遽
- 88.2%主要上網地點為「家中」，其次為「工作地點、辦公場所」，占33.7%；另「學校（含宿舍）、研究機關」占25.5%；而網路咖啡店或其他公共場所

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網際網路成為溝通與交易之媒介

- 在家上網的應用行為中，仍是以「瀏覽資訊」及「收發E-Mail」最為普遍
- 「網路電話」、「線上轉帳或信用卡交易」及「即時短訊(IM)」的成長最為驚人
- 這顯示出越來越多人透過網際網路進行人際溝通，這不僅具有即時性和便利性，更有節費效益
- 另外，諸如：部落格（blog）、線上購物、線上拍賣、線上學習…等等應用，在近幾年間，使用人口皆有大幅度的成長

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網際網路的魅力

- 有網路真好！
- Internet: 是一個虛擬世界
- 實現我的夢想： 詩人、作家、商人
- 展現我的實力
- 實現地球村的理想
- 琳琅滿目的「生活資訊」
- 自由.. 免費.. 快速
- 不限時數全年無休
- 什麼都有，什麼都賣， 什麼都不奇怪！

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網路應用 vs 資安威脅

- ■網站瀏覽，電子商務
- ■電子郵件
- ■P2P檔案分享程式
- ■IM即時通訊工具
- ■網路電話
- ■Tunneling
- ....Many....



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

電子商務的安全威脅

表面上看起來是個正常的拍賣商品



說明頁面的最下方，有個BAN
要大家按進去他的賣場看看



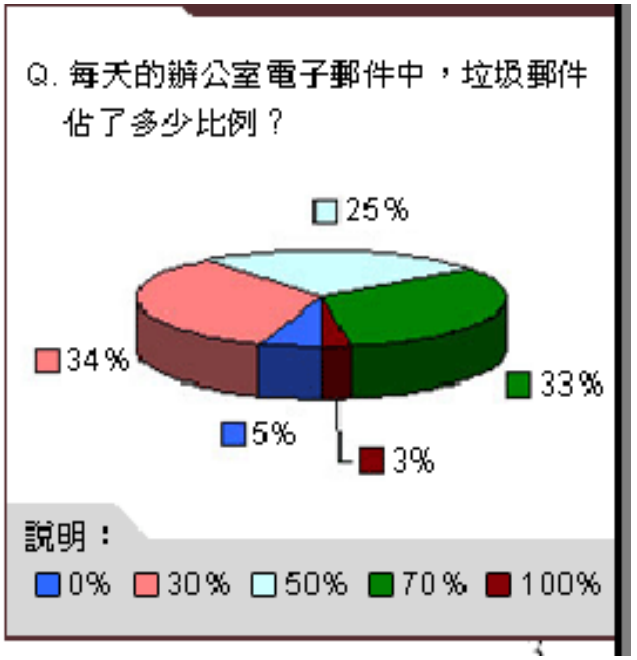
只要你輸入帳號、密碼，你的
帳號密碼就會被偷走了



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

電子郵件的隱憂

- 全球垃圾信件比例高達64%
- 垃圾信件造成企業額外的支出
- 全球前五大垃圾信件來源國：
  美國、中國、南韓、加拿大、台灣
- 刪除一封垃圾信件須花11秒
- 引進蠕蟲/木馬程式危害
  內部網路



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

P2P的風險

- P2P 除了檔案分享與即時通訊，也逐漸發展出不同應用
- 例如Skype。對個人用戶，利多於弊，但對企業，為資訊安全一大隱憂
- P2P 應用潛藏諸多風險，包括
  - 洩漏企業內部機密資訊
  - 成為病蟲擴散的管道
  - 下載非法檔案
  - 侵犯著作權
  - 佔用大量網路頻寬
  - 影響其他系統正常運作
  - 造成員工分心，降低生產力



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

即時通軟體的安全隱憂

台灣常見的即時通軟體













本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

即時通訊軟體資訊交流 隱藏資安危機



【大紀元11月13日報導】（中央社記者韋樞台北十三日電）在網路上互相傳遞交流訊息非常普通，但資訊安全公司強調，分享一個有趣動畫或小遊戲都可能會使公司機密資料遭竊，最近觀察發現，透過即時通訊軟體交流資訊不僅常有不易察覺的資安危機產生，更有一家知名的跨國服務業在一天中便有986次的機會受到同一惡意網站的威脅。

資訊安全公司趨勢科技曾發現一起案例，在萬聖節當天企業員工用MSN傳了一個有趣的小程式—「跳舞的骷髏」(Dancing Skeleton)遊戲網址分享給朋友，卻收到朋友警告，那個網站含有惡意攻擊行爲而被閘道端防毒系統攔截。

經過分析發現，那個網站內 Halloween.exe —「跳舞的骷髏」遊戲事實上是一個利用節慶活動作爲掩飾的攻擊程式。一旦瀏覽那個網頁即會自動下載執行，使用者根本不自覺已遭攻擊。

趨勢科技指出，偵查到的惡意程式屬於以惡意網頁聞名的「Storm家族系列」的最新社交攻擊模式。逢年底萬聖節、感恩節、聖誕節和新年等節慶時，與節慶相關的惡意遊戲小程式常被利用作爲欺騙網友的誘餌。

一旦網友不慎上當，特洛依木馬程式便會下載並啓動其他惡意檔案，連線到網站以建立點對點控制的殭屍網路 (botnet)，使個人電腦自動下載廣告軟體、間諜程式及其他惡意程式，成爲傳送

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

軟體BT的問題

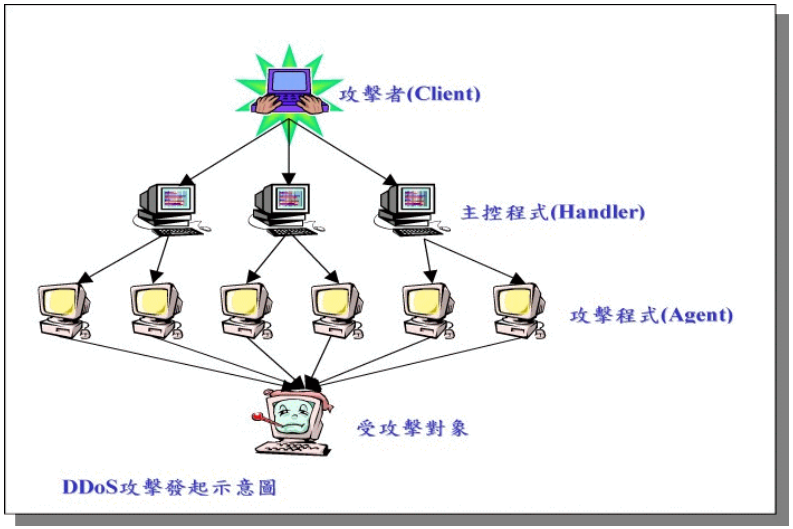
- BT，是一種下載工具軟體，為「Bit Torrent」的簡稱，中文有人翻譯為「比特洪流」。
- 同時間「下載的人數愈多，下載的速度愈快」，是ＢＴ最大的特色，令剛接觸的人，會有些匪夷所思，所以也有人取ＢＴ諧音，稱為「變態軟體」。
- ＢＴ下載需要原始種子，這些種子多半在亞洲，目前以中國大陸和香港最多。而且資訊最快，從還沒上映的院線電影、熱門影集、無碼Ａ片、流行音樂、遊戲軟體、電子書到電腦程式，都是ＢＴ傳輸的內容。
- 目前最大的問題，就是產生侵犯智慧財產權的法律問題。幾乎所有電影業者，一提到ＢＴ，就恨得牙癢癢的。更嚴重的是，大量色情圖片和Ａ片的下載，也使得情色散播的迅速和熱門，成為犯罪溫床。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、

常見的網路攻擊方式

- 傳統式Denial of Service 攻擊
- 分散式Denial of Service 攻擊



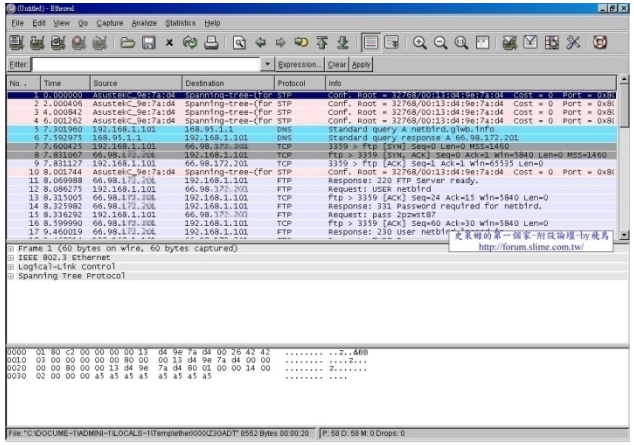
利用大量封包造成目標之網路伺服器或是線路壅塞以降低目標服務效能屬於常見攻擊之前奏

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

常見的網路攻擊方式

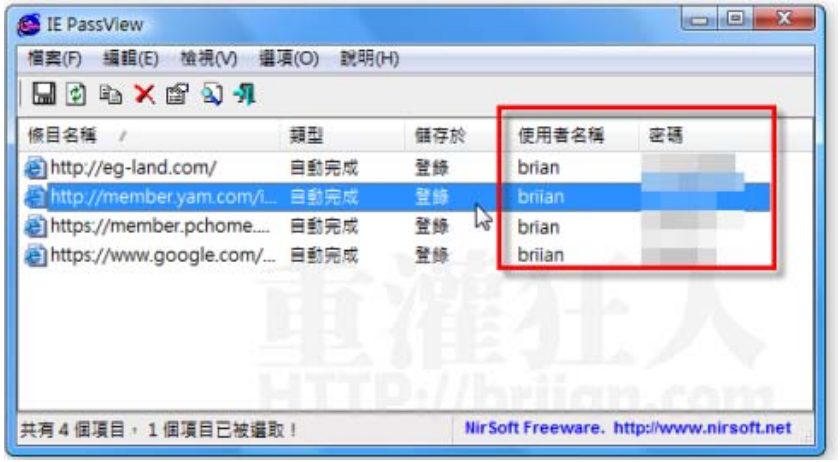
- 封包截取（*Packet Sniffer*）
- 利用封包擷取破解技術竊取重要系統間之通訊

以獲取重要個人或是交易
資料以便於執行下依步驟
之入侵行為



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

常見的網路攻擊方式



- 盜用帳號（*Account Compromise*）
- 盜用控管帳號（*Root Compromise*）

利用密碼破解技術或是濫用信任關係竊取重要帳號密碼對系統或重要資源進行竊取或是破壞常見於主機型之攻擊

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

常見的網路攻擊方式

- 惡意程式（***Malicious code***）



利用*Java*和*ActiveX*的特性來撰寫對使用者會造成不便的這些不懷好意的程式碼常見於網站以及來源不明的檔案



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網路安全管理

防火牆與網路防禦機制實務

何謂防火牆?

幾乎所有的公司爲了保護內部的資源，都會在企業的大門設置門禁或警衛來看守出入口，防止不相干的人進入公司內部；同樣的，爲了享受Internet的便利與企業e化的需求，大多數公司會向ISP（網路服務供應商）租一條網路專線或是xDSL（非對傳數位迴路），這個動作如同把馬路鋪到公司門口，雖然享受了四通八達的大眾運輸網路（Internet），卻同時也必須承受不當宵小（Hacker、Cracker）侵入的風險，防火牆即是提供相當於大門警衛的功能，藉由網路存取規則（ACL, Access Control List）的訂定，允許相關的人出入公司，並拒絕不相干或心懷[illegible]的人進入公司內部。
換言之，防火牆就是公司網路的大[illegible]，控制所有的進出公司內部的網路連線，檢查所有通過防火牆的[illegible]acket），並且留下詳細紀錄（log），以便日後稽核與追查。



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

為什麼需要防火牆？

防火牆主要是為了防範三種蓄意破壞的方式：

- 入侵：入侵後就可以正當使用電腦。入侵者就會變成合法的使用者，任意存取內部網路資源。
- 拒絕服務：駭客只要發出如洪水般的垃圾封包就可能癱瘓某部伺服主機，使得系統無法正常提供服務。
- 資訊竊盜：駭客利用漏洞竊取使用者的帳號及密碼，就可以進入電腦竊取所需的資訊。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

防火牆能作些什麼 ？

1. 網路安全的中心點

   防火牆爲一個網路中樞點，所有進入和出去的傳輸都必須通防火牆

2. 執行安全政策

   防火牆強制執行站安全政策，只讓『核准的』服務通過，而這些服務。

3. 記錄網路服務的活動

   由於所有的傳輸都經過防火牆，所以它成爲收集網路活動資訊的最佳地點。

4. 減少網路暴露的危機

   防火牆可以使得在防火牆內部的伺服主機與外界網路隔絕，避免有問題的封包影響到內部主機的安全。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

防火牆主要提供的功能

- 網路流量篩選(Packet Filter)
  - 過濾未經授權的網路流量
- 資料內容篩選(Application Filter)
- 網路位置轉譯(NAT、PAT)
  - 解決IP位址不足的問題
  - 保護內部網路位址配置
  - 隱藏網際網路服務的真實位址



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

軟體式 VS 硬體式

- 軟體式防火牆：這種類型的防火牆功能強大且應用上較具彈性，市場上最具代表性的產品有 CheckPoint及MS ISA Server等等，唯軟體式的架構必須安裝在其他獨立伺服器上，安裝及維護上有相當的門檻，效能也隨伺服器等級不同而有所不同，除了本身軟體防火牆的功能及效能間的差異，其中伺服器的效能也佔防火牆效能的重要因素。目前廠商為了解決伺服器的問題，推出了優化硬體架構及OS的設備，用來搭配軟體式防火牆來達到最高及最穩定的效能，如Nokia及Nortel等公司都有相關產品。

- 硬體式防火牆：這種類型的防火牆功能基於特有的ASIC晶片/NP設計，在效能及價格上都有亮眼的表現，如Netscreen、Fortinet、Sonicwall等公司的產品，但功能及應用彈性通常較不如軟體式的防火牆。

- 基本上，以上兩種類型的防火牆各有其優缺點，並無絕對的好或不好，端視組織的安全管理需求而定。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

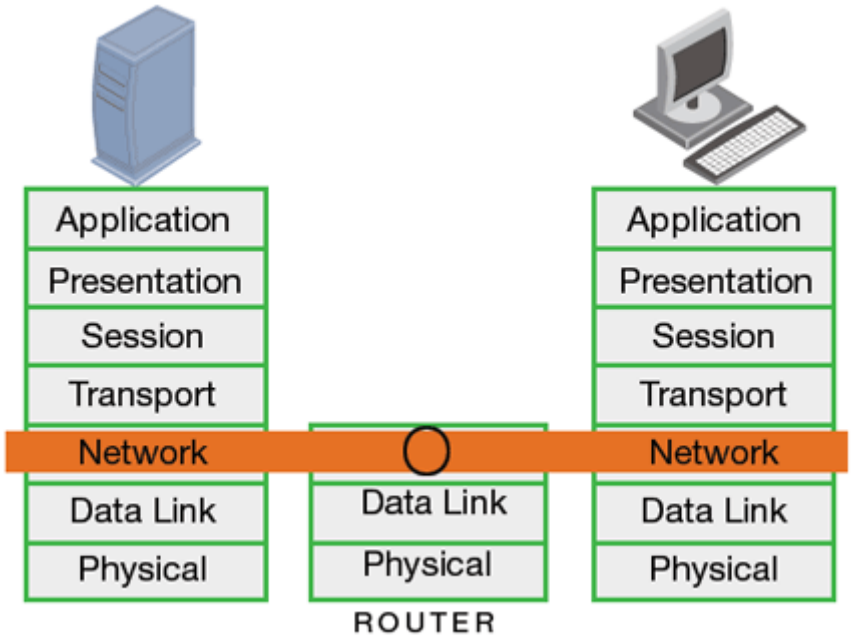
網路防火牆的基本技術

- 封包過濾式防火牆 (Packet Filter)
- 應用層閘道式防火牆 (Application-Level Gateway)
- 狀態檢驗式防火牆(Statefull Inspection)

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

靜態封包篩選(Packet Filter)

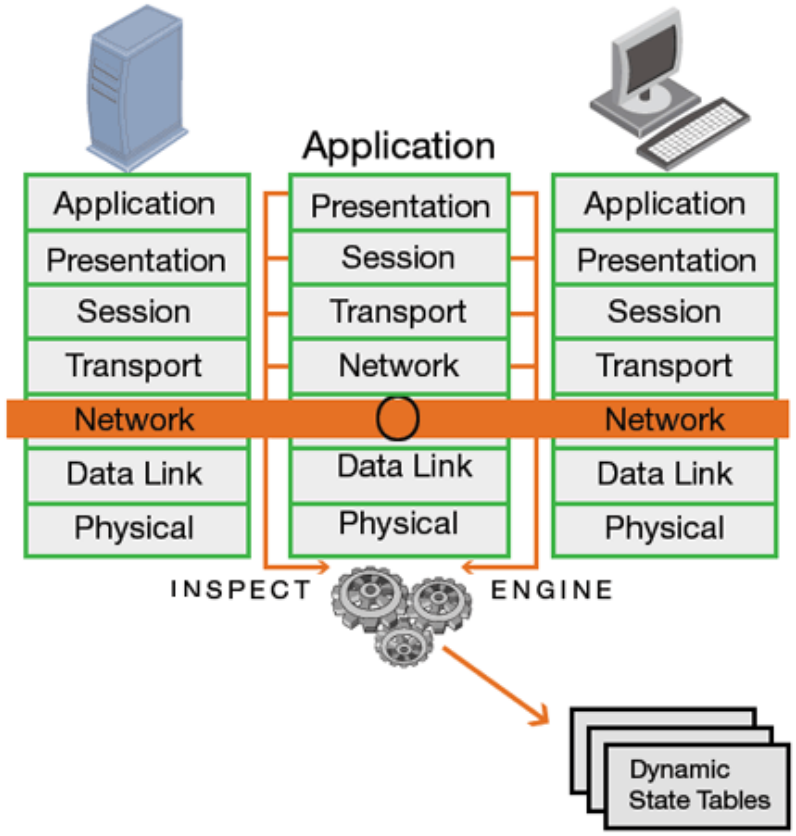
- 速度快高效能
- 低成本
- 僅檢查來源端與目的端的網路位址及埠號安全性較低



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

狀態檢驗式防火牆(Statefull Inspection)

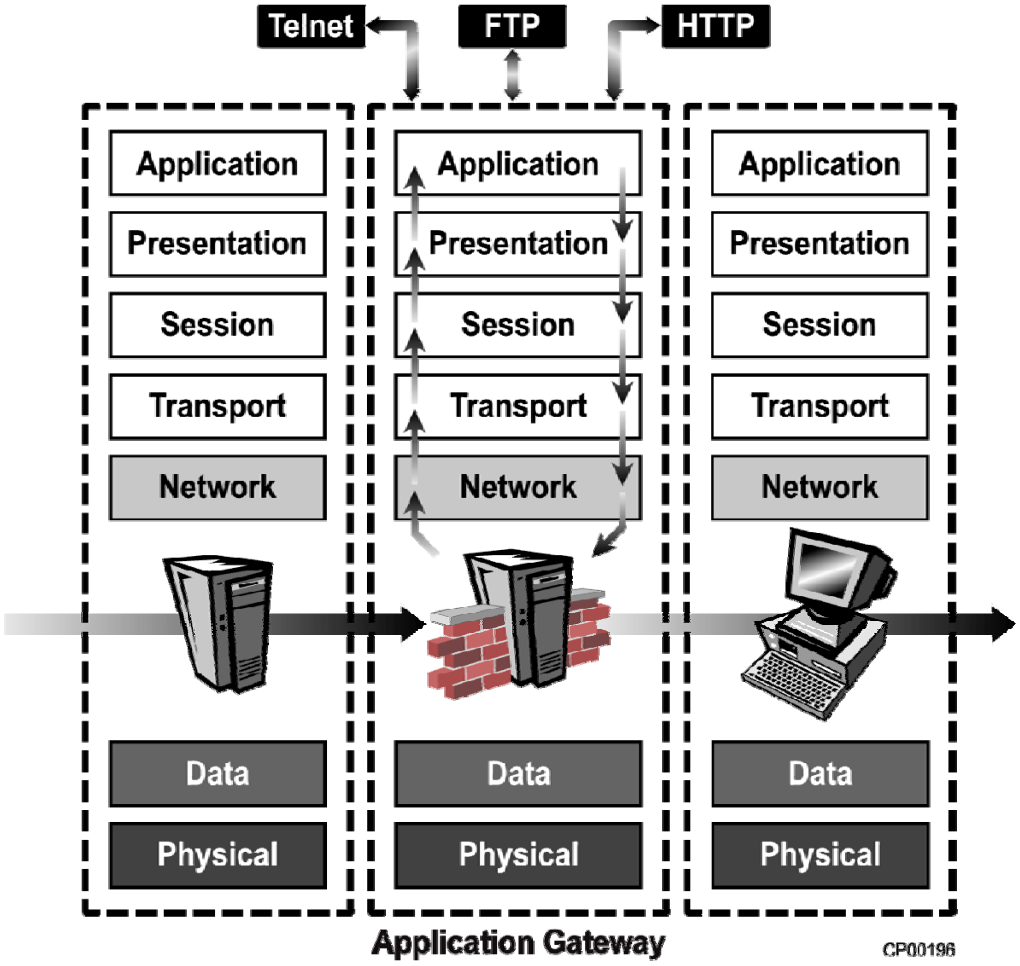
- 高效能
- 成本低
- 可檢驗部分應用層資訊安全性較高



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

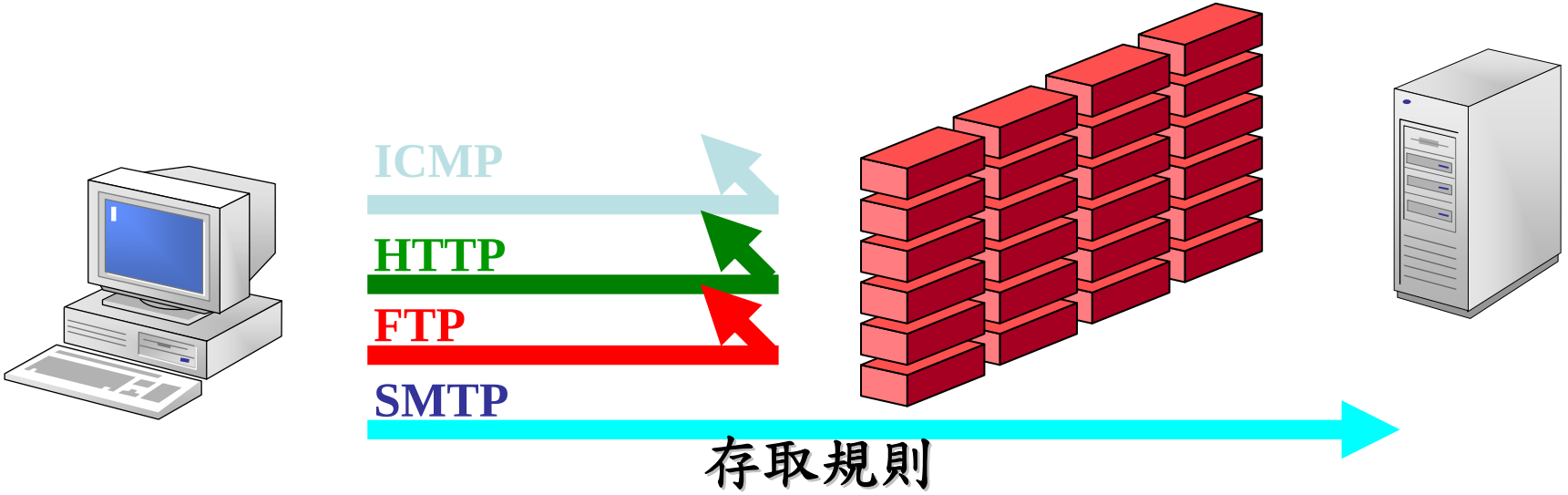
應用層閘道式防火牆 (Application-Level Gateway)

- 所有封包皆檢驗至應用程因此安全性高
- 硬體規格需求高所需成本較高
- 效能較低



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

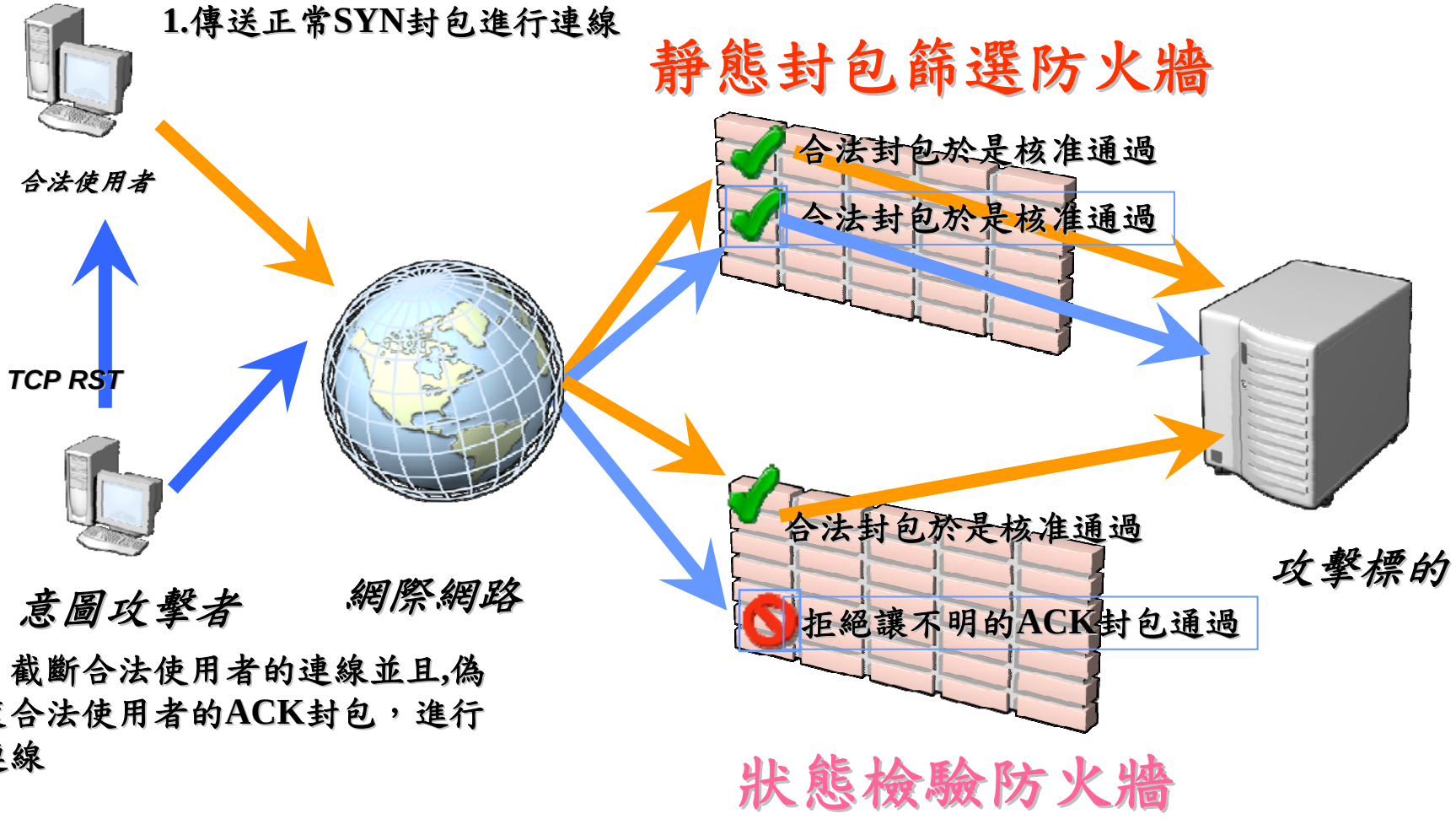
靜態封包篩選的運作



通訊協定	來源端		目的端		動作方式
	位址	埠號	位址	埠號	
TCP	Any	Any	Any	25	允許
TCP	Any	Any	Any	21	拒絕
TCP	Any	Any	Any	80	拒絕
ICMP	Any	Any	Any	---	拒絕
Any	Any	Any	Any	Any	拒絕

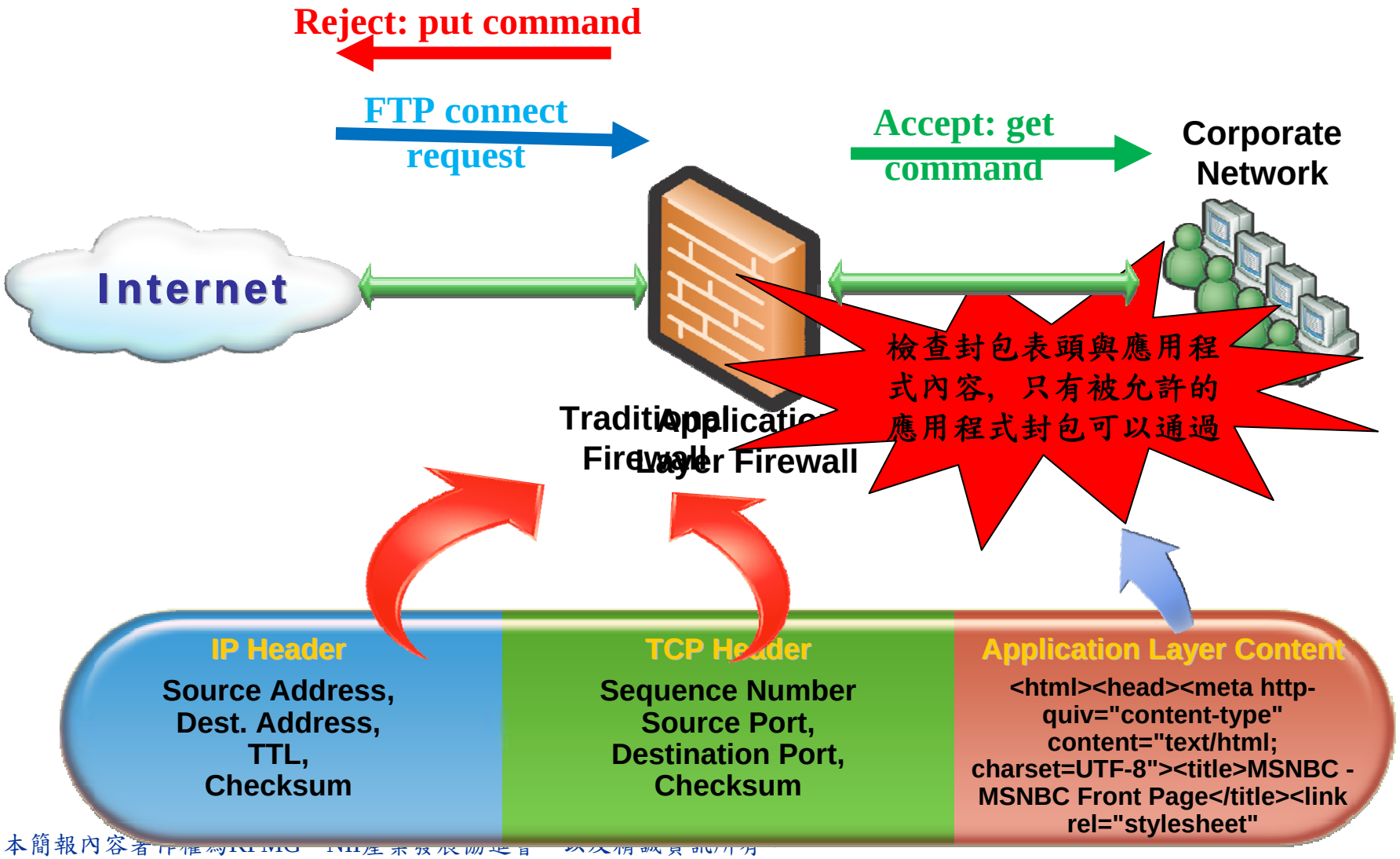
本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

狀態檢驗式防火牆 VS 靜態封包篩選



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

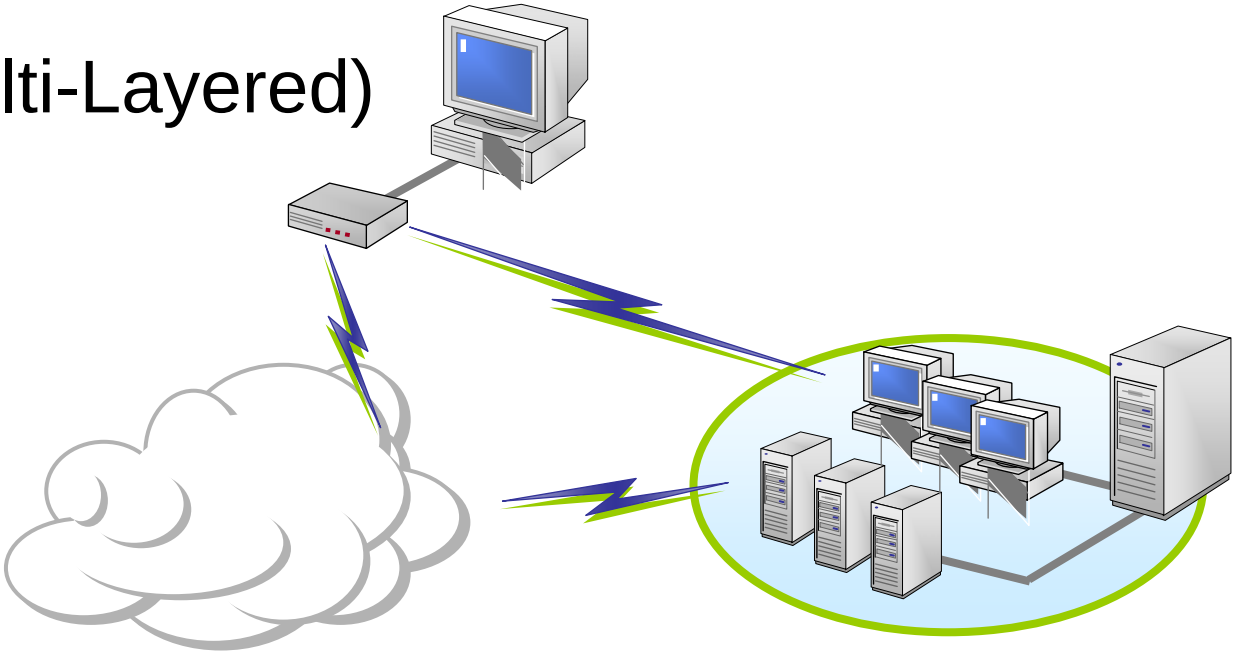
應用層篩選與傳統防火牆的差異性



本簡報內容著作權為[illegible]，以及精誠資訊所有
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

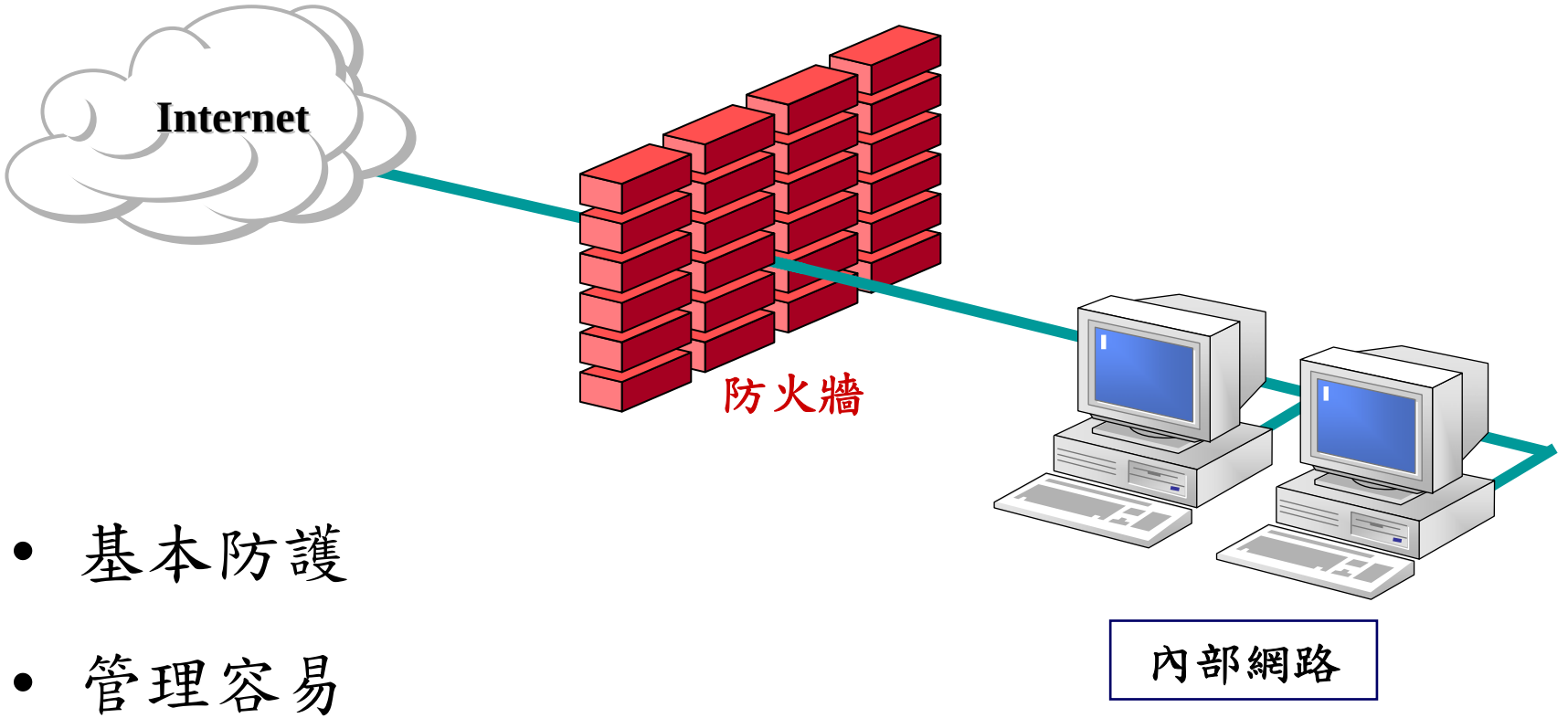
防火牆的網路架構

- 防禦主機架構(Bastion Host)
- 3-Homed架構
- 多層次架構(Multi-Layered)



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

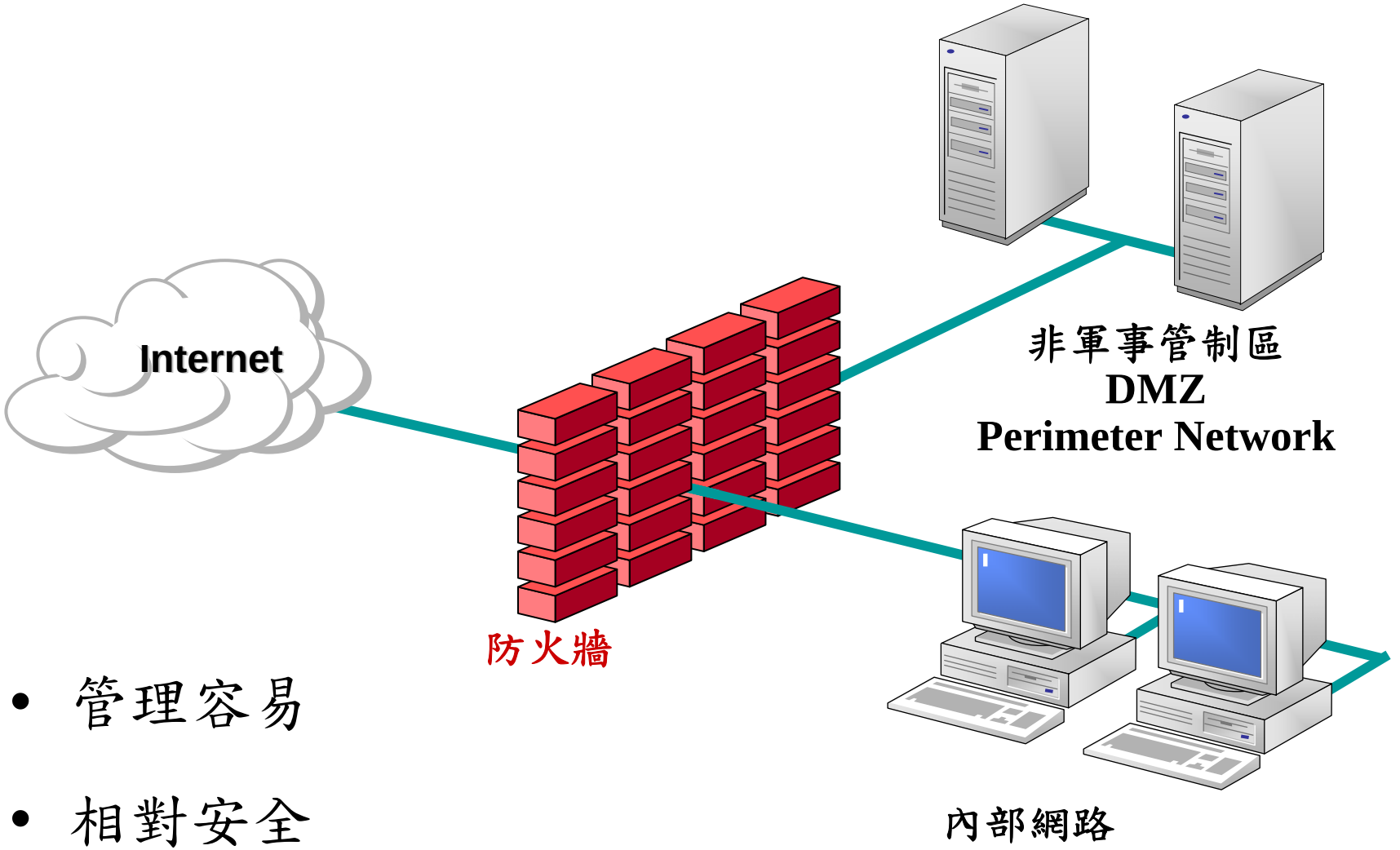
防禦主機架構(Bastion Host)



- 基本防護
- 管理容易
- 成本低

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

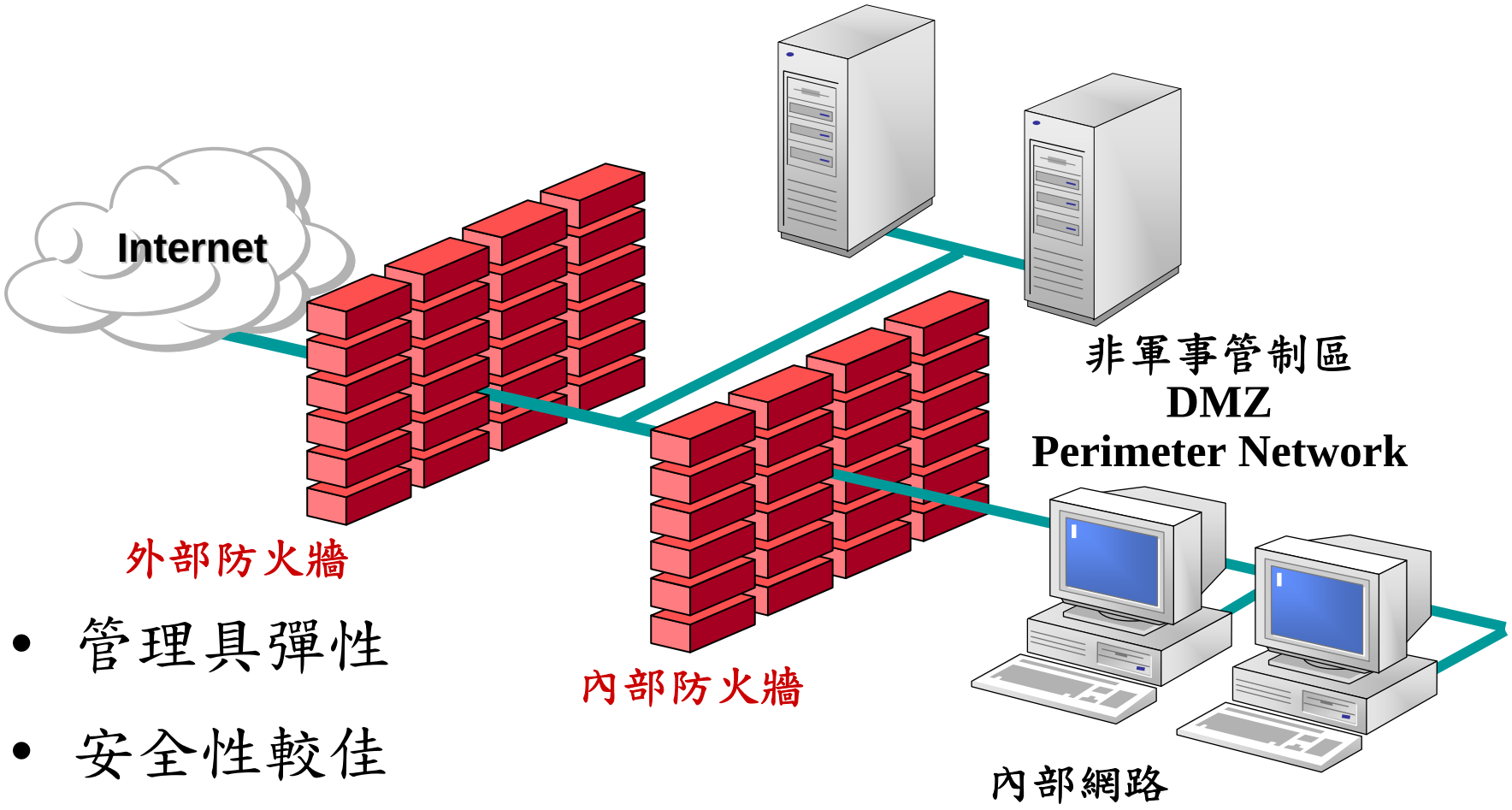
3-Homed架構



- 管理容易
- 相對安全

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

多層次架構(Multi-Layered)



- 管理具彈性
- 安全性較佳
- 成本較高

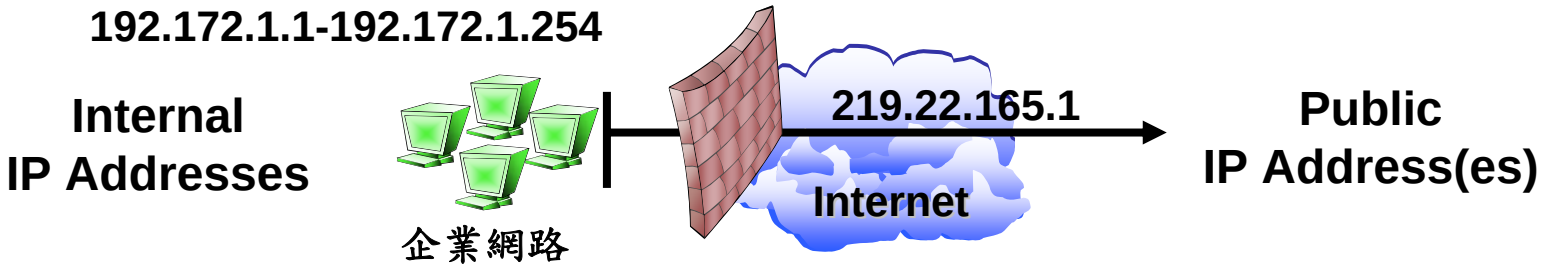
本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

常見的防火牆佈署方式

- 路由(Routing)
- 透通(Transparent)模式
- 網路位址轉譯(NAT、PAT)

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

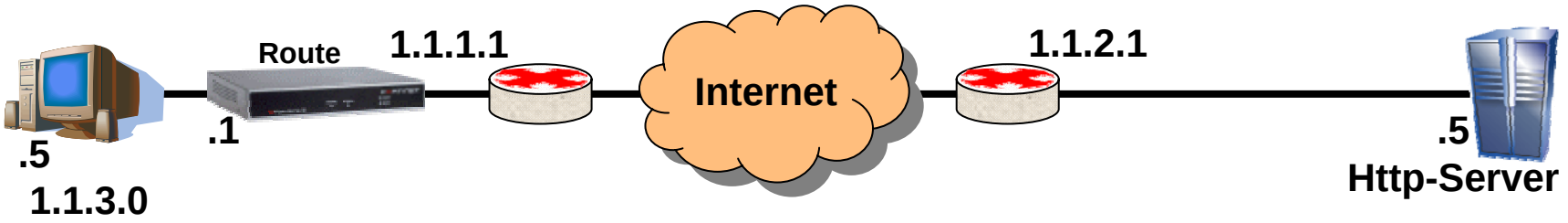
使用轉址(NAT)模式



- 將企業內部使用的保留位址轉換為合法位址
  - 隱藏內部主機的真實位址,被免遭受攻擊
    - 可以讓企業內部使用更多的主機

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

使用路由(Route)模式



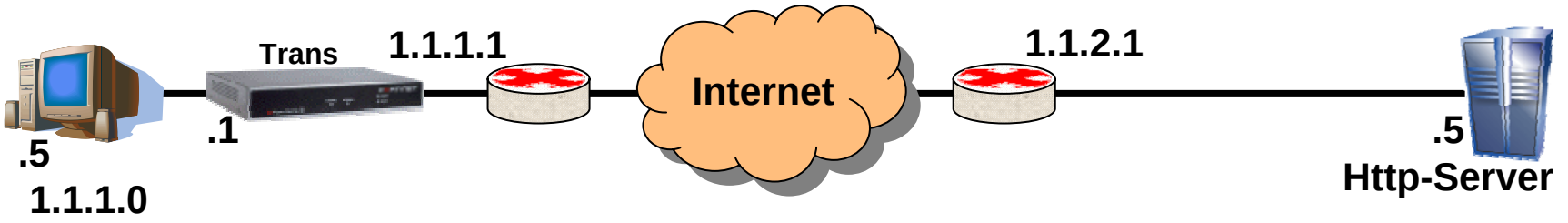
SrcIP	DstIP	Prot	SrcPort	DstPort	Data
1.1.3.5	1.1.2.5	6	12345	80	Get

SrcIP	DstIP	Prot	SrcPort	DstPort	Data
1.1.3.5	1.1.2.5	6	12345	80	Get

- 防火牆policy (不啓動NAT).
  - 只檢查路由表,根據路由表將封包送往所指定的位址,而不變動來源IP或來源埠

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

使用透通(Transparent)模式



SrcIP	DstIP	Prot	SrcPort	DstPort	Data
1.1.1.5	1.1.2.5	6	12345	80	Get

SrcIP	DstIP	Prot	SrcPort	DstPort	Data
1.1.1.5	1.1.2.5	6	12345	80	Get

- 防火牆policy
  - 沒有NAT或路由,單純地檢查經過的封包
  - 用戶意識不到防火牆存在
  - 其他網路設備無須改變設定

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

設定防火牆的存取控制原則

注意事項

- 注意”預設的狀態”
  - 全部啟用 or 全部拒絕
- 以最嚴格的方式進行設定
- 紀錄所有的拒絕存取日誌
- 定期稽核使用情形

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

有了防火牆就真的安全嗎?



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

防火牆不能保證絕對的安全

- 對某些攻擊保護很弱
- 不是所有的威脅來自防火牆外部
- 防火牆只是進出網路節點的鎖

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

入侵已經不是單純找漏洞了

很多入侵的第一步已經不是單純利用網路掃瞄找漏洞了，而是轉而使用社交工程(Social Engineering)進行第一步的滲透，最常見的就是先透過E-Mail/IM(MSN/Yahoo Messenger...etc)/惡意Web...等由內到外所發起的連線方式，誘使使用者被感染/植入惡意程式(木馬)，像是發送內含木馬的E- Mail或是MSN傳檔，或是誘使USER訪問具有惡意程式植入的網站。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

2008毒資新聞-假 YouTube 真偷帳號

偽造的 YouTube 網站，可以看功夫熊貓的精彩預告，也可以偷登入者的資料。

釣客可能藉此取得 YouTube 使用者名稱及密碼，並使用這些資訊販賣登入資料給廣告商或其他欲增加點擊率的人。

現在，Trend Micro Web Threat Protection 已將那兩個惡意網域加以封鎖。與往常一樣，我們會建議使用者使用他們未受污染的書籤去造訪線上常去的地方，並且忍住不要按下來路不明電子郵件中或 IM的連結。趨勢科技提供了最新的Web Threat Protection (WTP)工具，以過濾並阻擋有害網頁，確保上網瀏覽網頁時之安全，消費者可連結至 http://tw.trendmicro.com/tw/products/enterprise/wtp/index.html 免費下載。

過去，網路釣魚者的目標是與線上金融、信貸協會、金融部門及社群網路相關的網站，如今，他們把黑手伸進一個新的領域：視訊串流網站。

幾天前，趨勢科技內容安全小組發現了這個最新的網路釣魚技術。有好幾個網路釣魚網域（請見圖表 1）都帶有參考合法 YouTube 視訊連結的指令碼。

1) carry scripts that refer to legitimate YouTube video links.



本簡報內容著作權為RPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

入侵偵測(防禦)系統(IDS/IPS)

- 檢測來自內部的攻擊事件和越權訪問

  85%以上的攻擊事件來自於內部的攻擊，防火牆只能防外，難於防內

- 入侵偵測系統可作爲防火牆系統的一個有效的補強

  入侵偵測**(**防禦**)**系統可以有效的防範防火牆開放的服務入侵

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

入侵偵測(防禦)系統(IDS/IPS)能做什麼

- 提早發現入侵行為，儘早做好防範。
- 合法收集攻擊者的更多證據。
- 找出新的攻擊手法，更進一步保護重要的主機。
- 讓有心的攻擊者警惕，使他們不敢擅進。
- 監控(阻斷)網路上所有遭遇到的攻擊動作。
- 阻撓或拖延攻擊者的行為。

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

IDS vs IPS

IDS 適合對於內部行為監控、模式比對與內容控管

IPS 適合對於單純的對於異常行為進行防禦

***IDS*,(入侵偵測系統)是一種能夠在不影響網路的狀況下，能夠針對網路以及相關資源進行防禦之系統同時間也能夠對所防禦之網路環境中之使用者行為進行監控**

VS

***IPS*,(入侵防禦系統)是一種必須在閘道進行過濾並進行後續行為的防禦系統，強調能夠在發現可疑現象時主動攔阻相關行為**

哪種方案最適合使用 ？

看狀況!!!

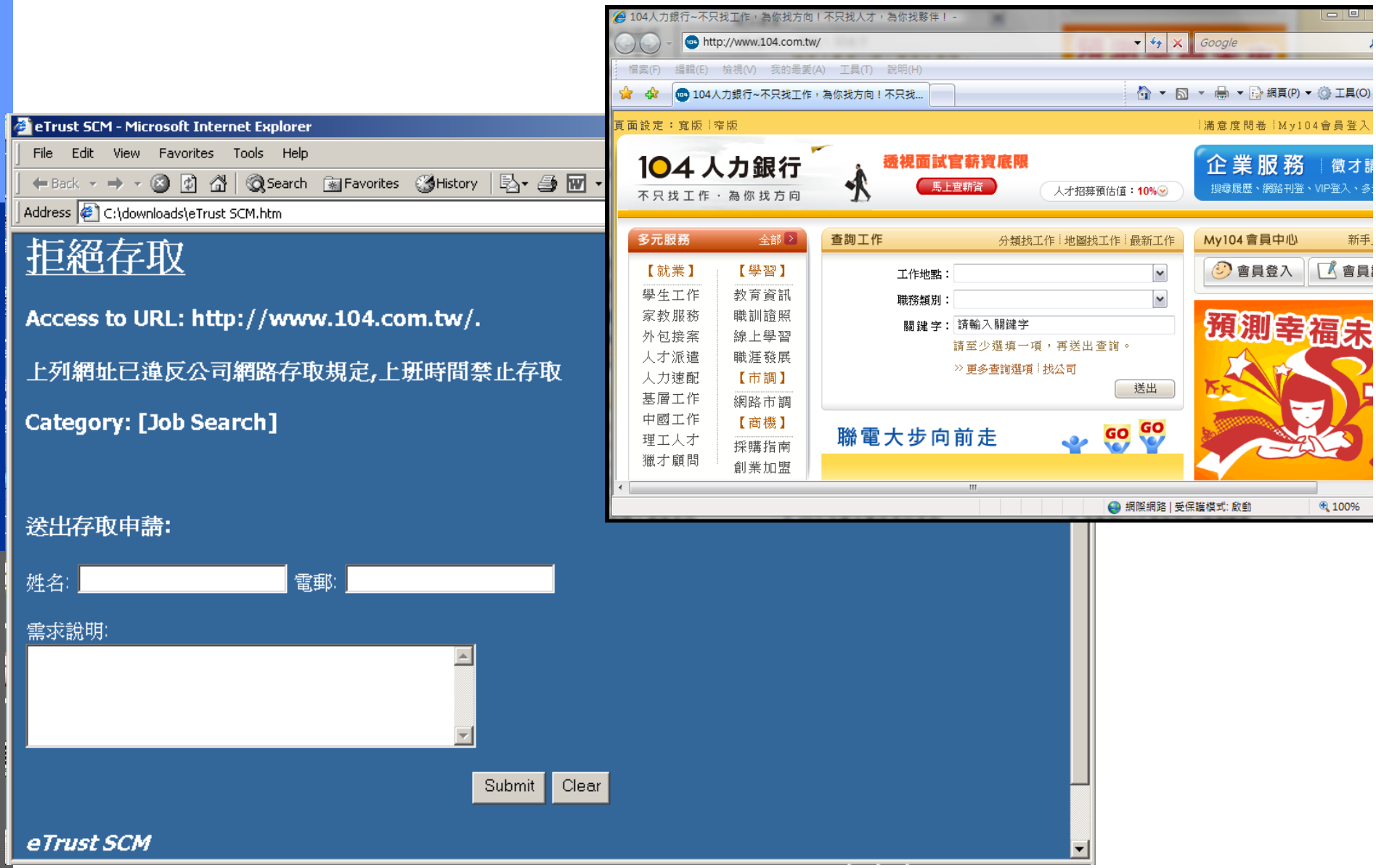
本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

還有什麼防禦措施



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

網頁瀏覽控制



非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

垃圾郵件管理

《本郵件由 SPAM SQR 系統定時自動發送，請勿回覆。請使用支援 HTML 郵件軟體開啟》
※請注意！攔截郵件保存時效為 15 天※
Don't reply this mail. It was sent by SPAM SQR. Please open it with e-mail client support HTML.
*** Attention please!! System will keep interception mail for 15 days. ***
您也可以選擇登入 安全模式 即時查看攔截郵件並接收郵件！
You can also login Secure Mode to check and resend interception mail in time.

郵件攔截記錄（共有 4 筆資料 - 低危險群: 0 筆資料 ,中危險群: 0 筆資料 ,高危險群: 4 筆資料）

查詢日期:2008-07-17 20:47:45 (CST)　過濾名單上限 400 筆，尚餘 345 筆

	選取	加入白名單	回報	寄信人	信件主旨	日期	大小(KB)
	接收	接收並加入白名單	不是垃圾信	marketing.tw@citi.com	花旗網路銀行24小時全年無休 讓您隨時隨地安心理財	2008-07-17 18:21:54(CST)	19
	接收	接收並加入白名單	不是垃圾信	Fogwill tcirtsbo_2002@indymacbank.com	Disagreements that will cause World War III	2008-07-17 19:33:23(CST)	1
	接收	接收並加入白名單	不是垃圾信	tigges matumoto@emparque.pt	Afghan bombing kills President Bush	2008-07-17 20:15:57(CST)	2
	接收	接收並加入白名單	不是垃圾信	Fylling erargern1953@2000service.it	Week review about your health!	2008-07-17 20:19:58(CST)	2

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

如何安裝Snort與設定Iptablet以保護Linux安全

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

Snort安裝

以root身份登入Linux（使用文字介面）

增加SSH安全性

vi /etc/ssh/sshd_config 以文字編輯器編輯/etc/ssh/sshd_config並更改下列三行（如果被註解的話請移除行首註解符號#）

Protocol 2
PermitRootLogin no
PermitEmptyPasswords no

啟動服務

chkconfig httpd on
chkconfig mysqld on
service httpd start
service mysqld start

測試Apache

在/var/www/html資料匣下新增一個test.php的檔案，並在檔案內加入此行

<?php phpinfo(); ?>

然後以瀏覽器開啟http://你的ip/test.php，應該會顯示你的系統、Apache和 PHP的資訊

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

安裝Snort

cd /root ←切換資料匣
mkdir /tmp ←新建資料匣，將下載的套件全放在此資料匣中
cd /root/tmp ←切換資料匣，安裝以下套件

rpm -ivh snort-2.2.0-0.fdr.1.i386.rpm
rpm -ivh snort-mysql-2.2.0-0.fdr.1.i386.rpm

修改snort.conf內容

cd /etc/snort
vi snort.conf

更改以下資訊
var HOME_NET 140.115.10.0/24 ← 藍色字體爲欲偵測的內部網域

（請依自己的網域做更改）
var EXTERNAL_NET !$HOME_NET ←藍色字體爲欲偵測的外部網域

（範例爲設定非內部即外部）
output database: log, mysql, user=snort password=snort dbname=snort
host=localhost

在**output**區段更改成如此的設定，
才能讓**MySQL**做記錄的動作，
請牢記**user**及**password**，待會會用到

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

修正initial script

cd /
chkconfig snortd off
cp /usr/share/doc/snort-2.2.0/contrib/S99snort /etc/init.d/snort
vi /etc/init.d/snort 編輯此檔如下

 # set config file & path to snort executable
SNORT_PATH=/usr/sbin
CONFIG=/etc/snort/snort.conf

 # set GID/Group Name
SNORT_GID=snort
完成後再輸入
rm -rf /etc/init.d/snortd
cd /etc/rc3.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
cd /etc/rc5.d
ln -s ../init.d/snort S99snort
ln -s ../init.d/snort K99snort
現在Snort會自動起動了

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

Setup MySQL

藍字爲你所需要輸入的指令

```
mysql
mysql> SET PASSWORD FOR root@localhost=PASSWORD('password');
>Query OK, 0 rows affected (0.25 sec)
mysql> create database snort;
>Query OK, 1 row affected (0.01 sec)
mysql> grant INSERT,SELECT on root.* to snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> SET PASSWORD FOR

snort@localhost=PASSWORD('password_from_snort.conf');
>Query OK, 0 rows affected (0.25 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to
                    snort@localhost;
>Query OK, 0 rows affected (0.02 sec)
mysql> grant CREATE, INSERT, SELECT, DELETE, UPDATE on snort.* to snort;
>Query OK, 0 rows affected (0.02 sec)
mysql> exit
>Bye
```

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

執行下列指令來建立表格

mysql -u root -p < /usr/share/doc/snort-2.2.0/contrib/create_mysql snort
Enter password: the mysql root password 密碼自定

zcat /usr/share/doc/snort-2.2.0/contrib/snortdb-extra.gz |mysql -p snort
Enter password: the mysql root password 密碼自定
mysql -p
>Enter password:你剛剛設定的密碼
mysql> SHOW DATABASES; 你應該會看到以下表格

```
+------------+
| Database
+------------+
| mysql
| Snort
| test
+------------+
3 rows in set (0.00 sec)
```

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

```
mysql> use Snort
        >Database changed
        mysql> SHOW TABLES;
        +-----------------+
        | Tables_in_Snort
        +-----------------+
        | data
        | detail
        | encoding
        | event
        | flags
        | icmphdr
        | iphdr
        | opt
        | protocols
        | reference
        | reference_system
        | schema
        | sensor
        | services
        | sig_class
        | sig_reference
        | signature
        | tcphdr
        | udphdr
        +-----------------+
        19 rows in set (0.00 sec)

        exit
```

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

安裝JPGraph

```
cd /var/www
tar -xvzf /root/tmp/jpgraph-1.16.tar.gz
cd jpgraph-1.16
rm -rf README
rm -rf QPL.txt
```

安裝ADODB

```
cd /var/www
tar -xvzf ~/snortisntall/adodb453.tgz
```

安裝ACID

```
cd /var/www/html
tar -xvzf ~/snortisntall/acid-0.9.6b23.tar.gz
cd acid
```

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

設定ACID

vi acid_conf.php　　更改以下藍色文字

```
$DBlib_path = "/var/www/adodb";

$DBtype = "mysql";

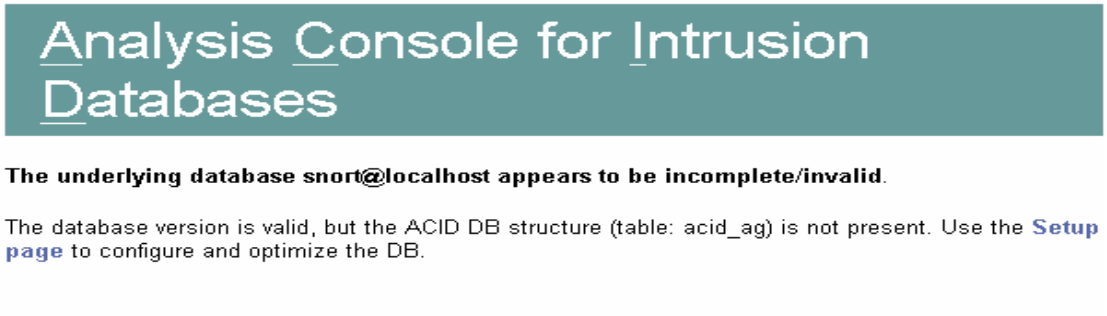
/* Alert DB connection parameters
* - $alert_dbname : MySQL database name of Snort alert DB
* - $alert_host : host on which the DB is stored
* - $alert_port : port on which to access the DB
* - $alert_user : login to the database with this user
* - $alert_password : password of the DB user
*
* This information can be gleaned from the Snort database
* output plugin configuration.
*/

$alert_dbname = "snort";
$alert_host = "localhost";
$alert_port = "";
$alert_user = "snort";
$alert_password = "password";
/* Archive DB connection parameters */
$archive_dbname = "snort";
$archive_host = "localhost";
$archive_port = "";
$archive_user = "snort";
$archive_password = "password ";
```

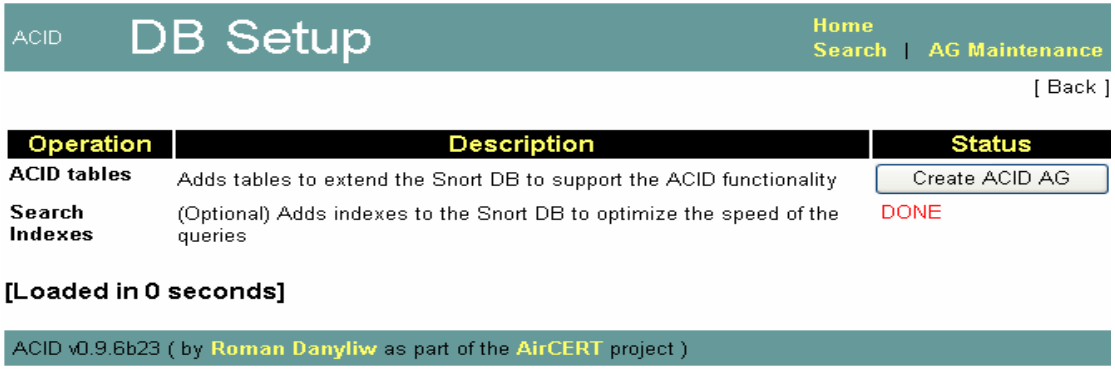
和$ChartLib_path = "/var/www/jpgraph-1.16/src";　　在檔案尾

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

到http://你的ip/acid/acid_main.php去，會顯以下資訊

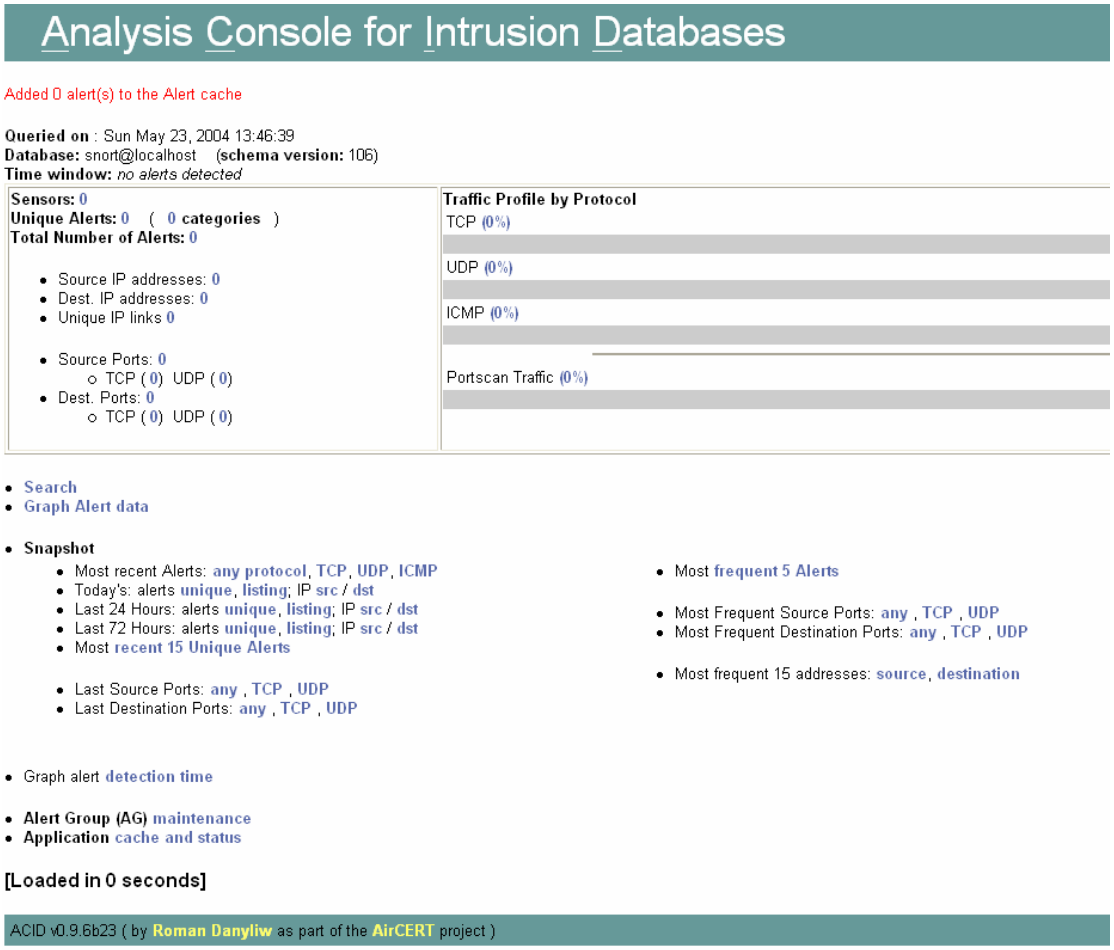


按下Setup page按鈕後，會看到



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

按下**Create ACID AG**按鈕，接著到**http://你的ip/acid**，會看到以下畫面



完成**Snort**安裝

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

iptables 設定

●觀察目前的設定

```
[root@test root]# iptables -L -n

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

仔細看到上面，因爲沒有加上 -t 的參數，所以預設就是 filter 這個表格， 在這個表格當中有三條鏈，分別是 INPUT, OUTPUT 與 FORWARD ，而且因爲 沒有規則，所以規則裡面都是空的！同時注意一下，在每個 chain 的後面 () 裡面，會發現有 policy 對吧！那就是『預設動作(政策)』咯！以上面來看， 雖然我們啓動了 iptables ，但是我們沒有設定規則，然後政策又是 ACCEPT， 所以『任何封包都會接受』

```
[root@test root]# iptables -t nat -L -n
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

與 filter 類似的， nat 這個表格裡面有的則是 PREROUTING, POSTROUTING 以及 OUTPUT 三條鏈！

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

- **清除所有的規則**

```
[root@test root]# /sbin/iptables –F
[root@test root]# /sbin/iptables –X
[root@test root]# /sbin/iptables -Z
[root@test root]# /sbin/iptables -t nat -F
```

請注意，如果在遠端連線的時候，『這三個指令必須要用 scripts 來連續執行』，
不然肯定『會讓您自己被主機擋在門外！』

參數說明：
-F ：清除所有的已訂定的規則；
-X ：殺掉所有使用者建立的 tables ；
-Z ：將所有的 chain 的計數與流量統計都歸零

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

●設定預設的政策

[root@test root]# /sbin/iptables [-t tables] [-P] [INPUT,OUTPUT,FORWARD| PREROUTING,OUTPUT,POSTROUTING] [ACCEPT,DROP]

參數說明：
-P　　：定義政策(Policy)。注意，這個 P 爲大寫啊！
INPUT　：封包爲輸入主機的方向；
OUTPUT ：封包爲輸出主機的方向；
FORWARD：封包爲不進入主機而向外再傳輸出去的方向；
PREROUTING ：在進入路由之前進行的工作；
OUTPUT　　：封包爲輸出主機的方向；
POSTROUTING：在進入路由之後進行的工作。

範例：
[root@test root]# /sbin/iptables -P　INPUT DROP
[root@test root]# /sbin/iptables -P　OUTPUT ACCEPT
[root@test root]# /sbin/iptables -P FORWARD ACCEPT
[root@test root]# /sbin/iptables -t nat -P　PREROUTING ACCEPT
[root@test root]# /sbin/iptables -t nat -P　　OUTPUT ACCEPT
[root@test root]# /sbin/iptables -t nat -P POSTROUTING ACCEPT

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

●增加與插入規則

例一：所有的來自 lo 這個介面的封包，都予以接受

[root@test root]# iptables -A INPUT -i lo -j ACCEPT

注意一下，因爲 -d, --dport, -s, --sport 等等參數都沒有設定，這表示：
不論封包來自何處或去到哪裡，只要是來自 lo 這個介面，就予以接受！
這個觀念挺重要的，就是『沒有設定的規定，則表示該規定完全接受』的意思！
例如這個案例當中，關於 -s, -d...等等的參數沒有規定時！

例二：來自 **192.168.0.1** 這個 **IP** 的封包都予以接受：

[root@test root]# iptables -A INPUT -i eth0 -p tcp -s 192.168.0.1 -j ACCEPT

新增一條規則，只要是來自於 192.168.0.1 的封包，不論他要去哪裡，
使用的是那個協定 (port) 主機都會予以接受的意思～

例三：來自 **192.168.1.0** 這個 **C Class** 的網域的任何一部電腦，就予以接受！

[root@test root]# iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 -j ACCEPT

這個是網域的寫法喔！稍微注意一下的是，在範例二當中我們僅針對一個 IP ，
至於這個範例當中，則是針對整個網域來開放吶！而網域的寫法可以是：
192.168.1.0/24 也可以是 192.168.1.0/255.255.255.0 都能夠接受喔！

例四：來自 **192.168.1.25** 的封包都給他丟棄去！

[root@test root]# iptables -A INPUT -i eth0 -p tcp -s 192.168.1.25 -j DROP

例五：來自 **192.168.0.24** 這個 **IP** 的封包，想要到我的 **137,138,139** 埠口時，都接受

[root@test root]# iptables -A INPUT -i eth0 -p tcp -s 192.168.0.24/24 --dport 137:139 -j ACCEPT

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

參數說明：

**[root@test root]# iptables [-t filter] [-AI INPUT,OUTPUT,FORWARD] **
**> [-io interface] [-p tcp,udp,icmp,all] [-s IP/network] [--sport ports] **
> [-d IP/network] [--dport ports] -j [ACCEPT,DROP]

-A ：新增加一條規則，該規則增加在最後面，例如原本已經有四條規則， 使用 -A 就可以加上第五條規則

-I ：插入一條規則，如果沒有設定規則順序，預設是插入變成第一條規則，例如原本有四條規則，
使用 -I 則該規則變成第一條，而原本四條變成 2~5

INPUT ：規則設定爲 filter table 的 INPUT 鏈
OUTPUT ：規則設定爲 filter table 的 OUTPUT 鏈
FORWARD：規則設定爲 filter table 的 FORWARD 鏈

-I ：設定『封包進入』的網路卡介面

-o ：設定『封包流出』的網路卡介面
interface ：網路卡介面，例如 ppp0, eth0, eth1....

-p ：請注意，這是小寫呦！封包的協定啦！
tcp ：封包爲 TCP 協定的封包；
upd ：封包爲 UDP 協定的封包；
Icmp：封包爲 ICMP 協定、
all ：表示爲所有的封包！

-s ：來源封包的 IP 或者是 Network (網域)；

--sport：來源封包的 port 號碼，也可以使用 port1:port2 如 21:23
同時通過 21,22,23 的意思

-d ：目標主機的 IP 或者是 Network (網域)；

--dport：目標主機的 port 號碼；

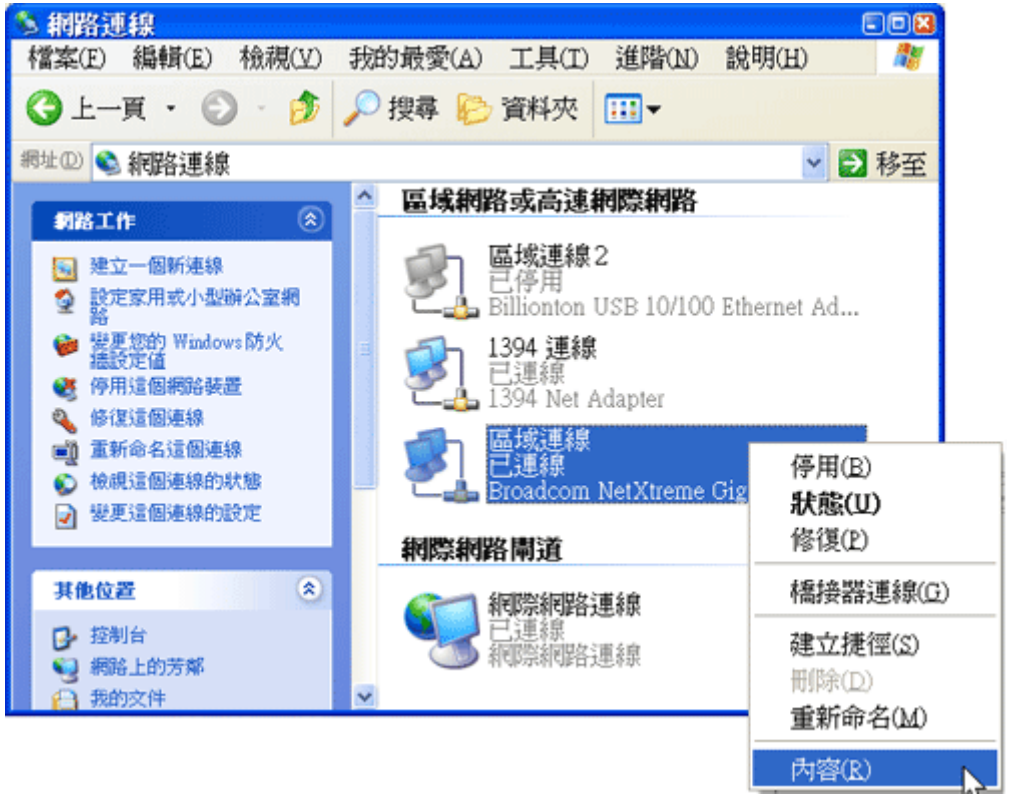
-j ：動作，可以接底下的動作；
ACCEPT ：接受該封包
DROP ：丟棄封包
LOG ：將該封包的資訊記錄下來 (預設記錄到 /var/log/messages 檔案)

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

如何以設定Personal Firewall確保Windows 安全

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

1. 首先請確定視窗版本為Windows XP/2003或是Vista，兩者皆具備內建防火牆功能。
2. 以Windows XP操作為範例，防火牆設定方式進入控制台>網路連線>(通常為)區域連線>滑鼠右鍵點選(內容)



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

- 點選進階>Windows防火牆畫面點選(設定值)



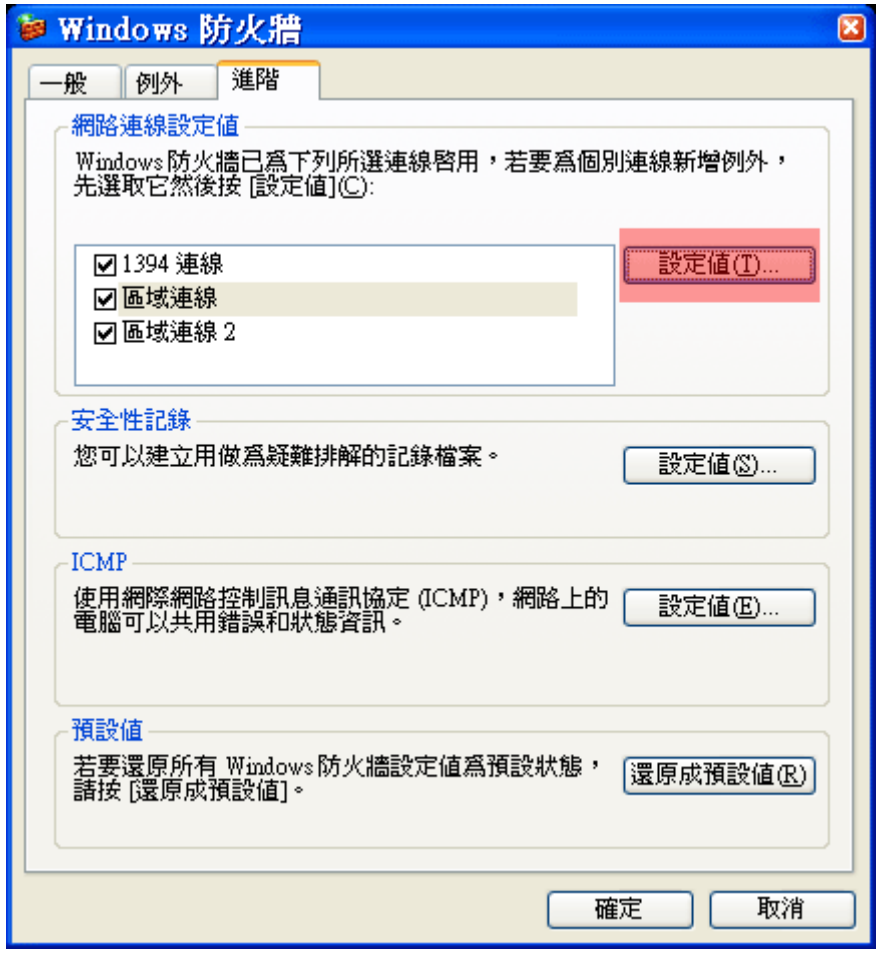
本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

- 點選進階>Windows防火牆畫面點選(設定值)



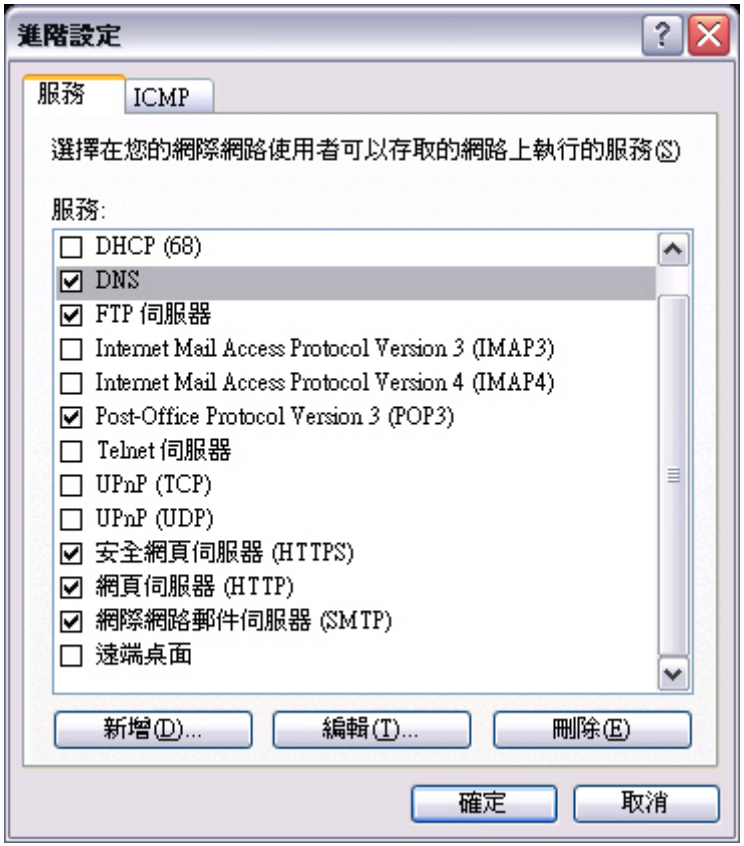
本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

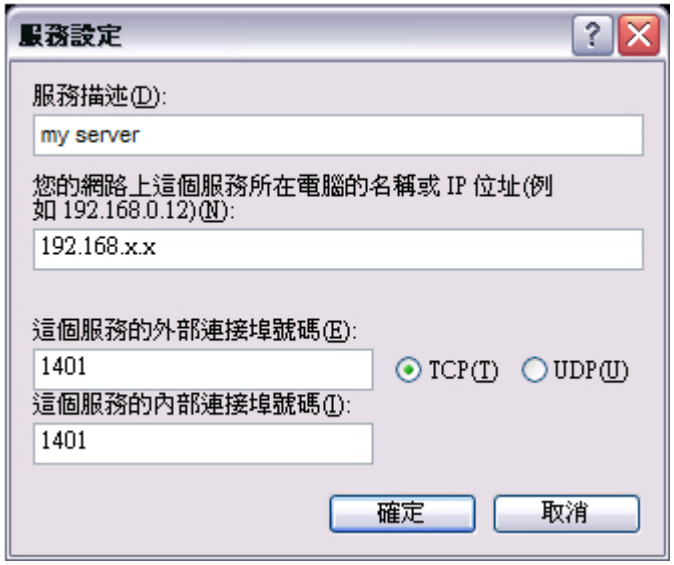
- Windows防火牆設定>進階>點選(通常為)區域連線>按下右方(設定值)按鈕



本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。

- 進入進階設定畫面>**依照需求定義與新增服務項目**





DNS UDP PORT 53 用於**DNS SERVER**
FTP伺服器 TCP PORT 21 用於**FTP SERVER**
Post-Office Protocol Version 3(POP3) TCP PORT 110 用於**MAIL SERVER**
安全網頁伺服器 (HTTPS) TCP PORT 443 用於**WEB SERVER**
網頁伺服器 (HTTP) TCP PORT 80 用於**WEB SERVER**
網際網路郵件伺服器 (SMTP) TCP PORT 25 用於**MAIL SERVER**

本簡報內容著作權為KPMG、NII產業發展協進會、以及精誠資訊所有，
非經正式書面授權同意，不得將全部或部份內容，以任何形式變更、轉載、再製、散佈、出版、展示或傳播。