

APT先進持續性攻擊趨勢與防  
範對策研習  
敦陽科技



# 講師

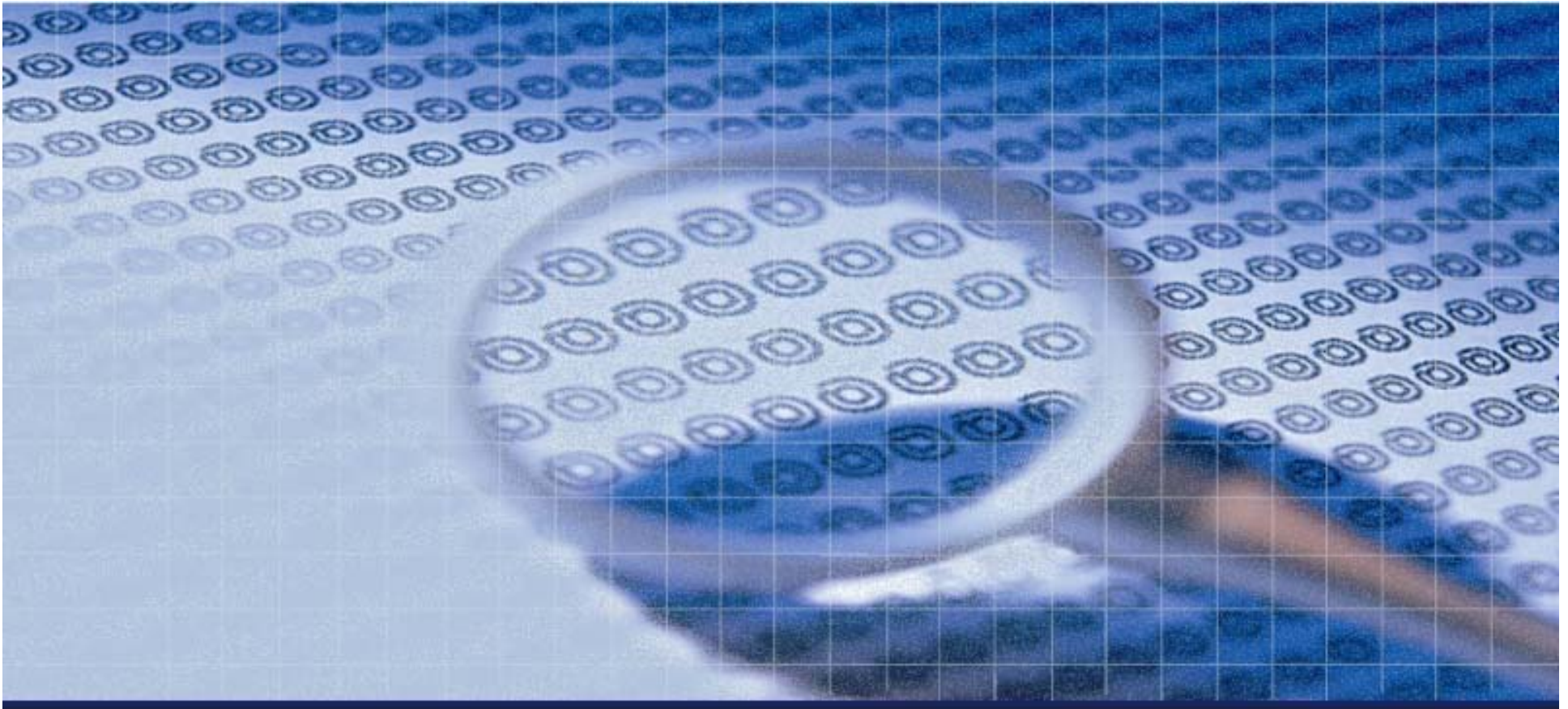


- 楊伯瀚 ( *lucifer.yang@sti.com.tw* )
- 現任: 敦陽科技IT管理技術開發處資安顧問
- 專長
  - ▶ 滲透測試
  - ▶ 網頁應用程式安全
  - ▶ 系統入侵事件分析
  - ▶ 資安事件處理
- 資安認證
  - ▶ CISSP (Certified Information Systems Security Professional )
  - ▶ CEH (Certified Ethical Hacker) /CEI (Instructor)
  - ▶ Cert/CC Advanced Incident Handling 講師

# 大綱



- 資安技術與防駭
- 敏感資料外洩防護
  - ▶ 系統面防護-DRM、DLP、EndPoint
  - ▶ 網路面防護-稽核、資料庫、次世代防火牆



# 資安技術與防駭



# 資安三原則

## ● Confidentiality – 機密性

- ▶ 確保資料傳遞與存取的私密性
- ▶ 避免未經授權的存取或有意無意的揭露與掠奪

## ● Integrity – 完整性

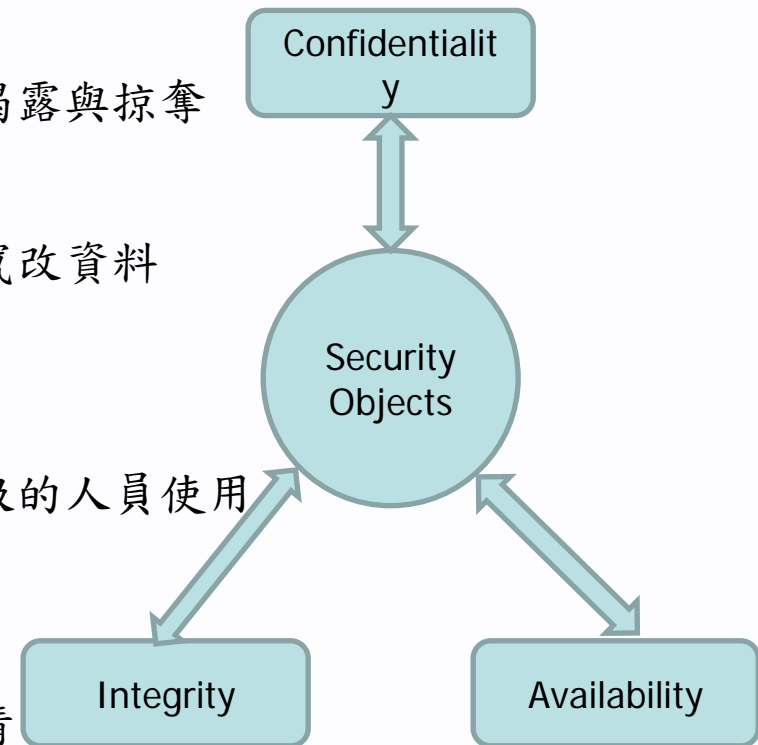
- ▶ 避免非經授權的使用者或處理程序竄改資料

## ● Availability – 可用性

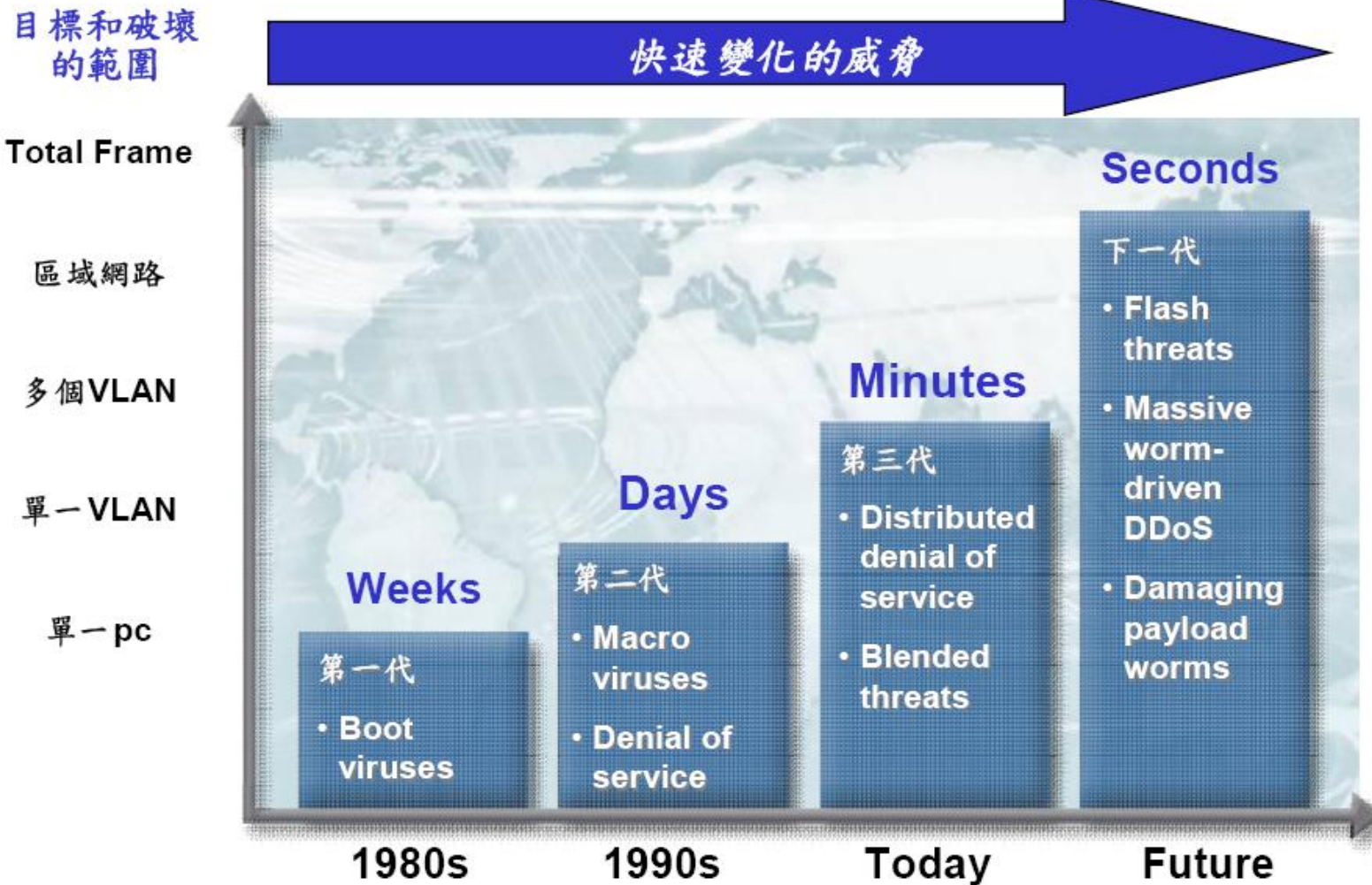
- ▶ 讓資料隨時保持在可用狀態
- ▶ 讓資料即時而且可靠的提供給各層級的人員使用
- ▶ 確保該服務的品質與永不中斷

## ● Non-repudiation – 不可否認性

- ▶ 防止存心不良者否認其所做過的事情



# 攻擊範圍和時間變化

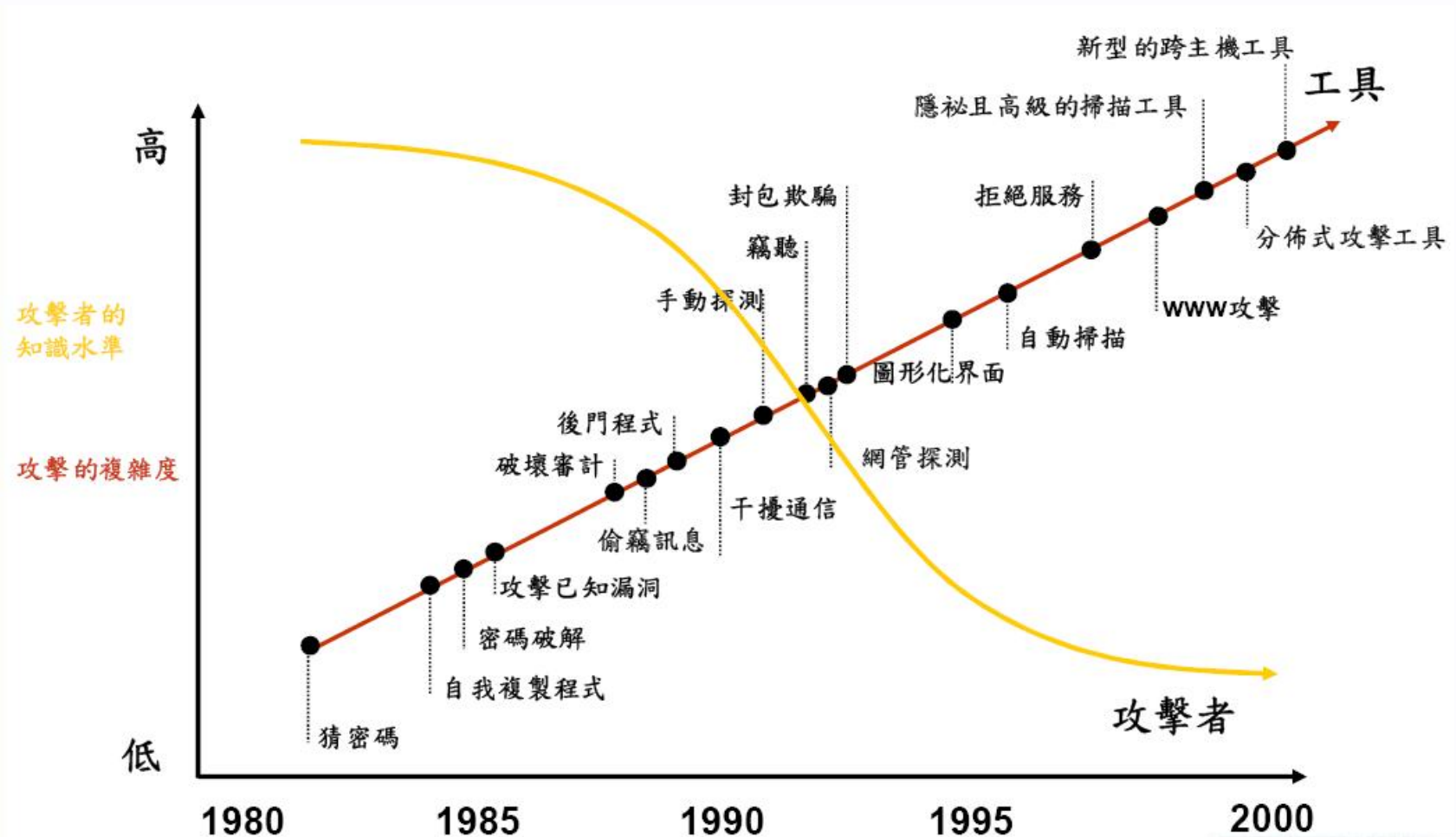


# 零時差攻擊



- **zero-day attack** 已是一個趨勢
- 此種態勢憑藉著被廣泛傳播的攻擊，將會嚴重的威脅到Internet以及其眾多的使用者或機器。
- 雖然供應商(OS、防毒廠商)已然了解此種形式，但他們仍然束手無策。屆時他們將**無法及時**的提供修正檔或是補強措施。

# 攻擊複雜度與攻擊者的技術水準





# 當今威脅情勢分析



- 威脅的複雜性日益增高
  - ▶ 90% 透過email繁殖與散撥，如mass mailing worms
  - ▶ 50%+ 經由Webpage讓使用者在無知的狀況下受感染
  - ▶ 10% 因系統本身的漏洞(弱點)，透過以internet為途徑被攻擊
  - ▶ 77% 擁有多重的散佈管道
  - ▶ 87% 會引發其他的攻擊行為
- 威脅以多重方式與途徑的攻擊傳染能力大增
  - ▶ 現今的攻擊大多具備多種攻擊途徑
  - ▶ 單一的防禦措施或防禦點，已無法滿足企業面對攻擊的需求
  - ▶ 資訊安全須以系統的角度來思考部署企業安全防護網

# 資料販售



排名		商品	比例		價格範圍
2009	2008		2009	2008	
1	1	信用卡	19%	32%	\$0.85 - \$30
2	2	銀行帳戶密碼	19%	19%	\$15 - \$850
3	3	電子郵件帳號及密碼	7%	5%	\$1 - \$20
4	4	電子郵件位址	7%	5%	\$1.70/MB - \$15/MB
5	9	自動程式	6%	3%	\$2 - \$5
6	6	完整身份	5%	4%	\$0.70 - \$20
7	13	信用卡轉錄	5%	2%	\$4 - \$150
8	7	寄信程式	4%	3%	\$4 - \$10
9	8	洗錢服務	4%	3%	\$0-\$600 加 50%-60%
10	12	網站管理權	4%	3%	\$2 - \$30

地下經濟伺服器上販售的商品與服務

資料來源：Symantec網路安全威脅就研究報告 第15期

# 惡意程式散佈途徑與管道



入侵途徑及管道	說明
電子郵件	電子郵件本身夾帶隱藏惡意程式的WORD的或其他類型檔案，利用OFFICE程式的漏洞，開啟後便連帶安裝後門或木馬程式。
系統本身漏洞	對目標系統或網路之漏洞進行攻擊，進而取得控制權，常見的方式包含：網芳相關、RPC-DCOM、IIS、IE弱點攻擊等等。
網站注入攻擊	使用特殊字元，使網頁應用程式略過安全性檢查，或輸入錯誤資料，得到錯誤訊息進而推敲資料庫的格式及內容。
惡意網頁	駭客先攻陷某一網站，並在網頁上加入一些惡意程式碼，使瀏覽用戶不自覺就被植入木馬程式。或是網路釣魚方式。
系統不當權限設定	防火牆規則不嚴謹、防毒軟體未更新，讓駭客利用掃描工具直接獲得帳號密碼。

# 前、後期駭客手法比較



項目	早期駭客手法	新型駭客手法
掃描方式	<ul style="list-style-type: none"><li>• 大規模</li><li>• 從不同的網段</li><li>• 單一掃描來源</li></ul>	<ul style="list-style-type: none"><li>• 小規模隨機</li><li>• 在相同網段或信任網段</li><li>• 分散掃描來源</li></ul>
攻擊方式	<ul style="list-style-type: none"><li>• 單純</li><li>• 漏洞攻擊</li></ul>	<ul style="list-style-type: none"><li>• 未知形態</li><li>• 社交工程</li><li>• 網站漏洞攻擊</li></ul>
後門及木馬運用模式	<ul style="list-style-type: none"><li>• 植入後馬上使用</li><li>• 本機開啟 Listen Port</li></ul>	<ul style="list-style-type: none"><li>• 潛伏等待</li><li>• 主動向外連線、匿蹤</li></ul>
駭客工具	<ul style="list-style-type: none"><li>• 一般網路上常見工具</li></ul>	<ul style="list-style-type: none"><li>• 自製工具、Rootkit</li><li>• 惡意網站、網頁、電子郵件</li></ul>
目的	<ul style="list-style-type: none"><li>• 竊取資料檔案</li><li>• 偷取密碼</li><li>• 炫耀</li></ul>	<ul style="list-style-type: none"><li>• 竊取資料檔案</li><li>• 偷取密碼</li><li>• 生財工具</li></ul>

# 內部網路的潛在危機



## ● 網路瀏覽的安全風險

- ▶ 間諜軟體(Spyware)
- ▶ 惡意網站病毒(Malicious Mobile Code)
- ▶ 釣魚詐欺(Phishing Attack)
- ▶ 鍵盤側錄攻擊(Key-logger)

## ● 網路資源的誤用

- ▶ 濫用網路存取(Internet Access)
- ▶ 頻寬的誤用：
  - 串流媒體使用(Streaming Media)
  - 網路收音機(Internet radio)

## ● 欲禁止與管理的使用

- ▶ 即時通訊(Instant Messaging)
- ▶ P2P傳輸(Peer-to-peer file sharing)

## ● 惡意的意圖

- ▶ 透過網路闖道的機密資料外洩
- ▶ 內部網路的駭客行為(Employee Hacking)

# 資訊發展的趨勢



## ● 更貼近生活的應用

- ▶ 手機網路化
- ▶ 食衣住行電子化
- ▶ 醫療生化晶片化
- ▶ 網路依存度過高

## ● 更強大的計算能力

- ▶ 雲端運算
- ▶ 虛擬化環境

# 駭客能打開監獄牢房門



駭客能打開監獄牢房門 - 數位生活 - 美國中文網論壇 - Powered by Discuz! - Windows Internet Explorer

http://gate.sinovision.net/82/gate/big5/www.sinovision.net/bbs/rec

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 我的最愛 駭客能打開監獄牢房門 - 數位生活 - 美國中文...

## 駭客能打開監獄牢房門

《連線》報導，研究人員發現，控制監獄牢門的PLC（可編程式控制器）中的安全漏洞可讓駭客釋放出囚犯。破壞伊朗核電站離心機的Stuxnet蠕蟲是利用了工業控制系統中PLC的漏洞，而控制牢門的PLC存在類似的漏洞。安全顧問和工程師John Strauchs將在本週舉行的DefCon 駭客會議上討論和演示他的發現。

Strauchs稱，監獄使用PLC控制牢門和其他設施上的鎖和門。他指出，許多人並不知道監獄是如何設計的，因此這個問題以前很少有人關注，他們不知道監獄使用了與離心機相同的PLC。PLC並不連接到網際網路上，但控制PLC的電腦則可能聯網。因此駭客可以通過感染病毒的U盤或對監獄工作人員的郵箱發送釣魚攻擊，控制電腦並進而控制PLC。

Strauchs說，監獄的電子安全系統不僅僅控制門，還控制著對講機、燈光控制、視頻監控、水和淋浴，等等。一旦控制了PLC(PDF)後駭客可以為所欲為，他們可以破壞整個系統。

收藏 分享

完成 網際網路 100%

# RSA遭遇APT攻擊 SecureID被偷





# RSA遭遇APT攻擊 SecureID被偷

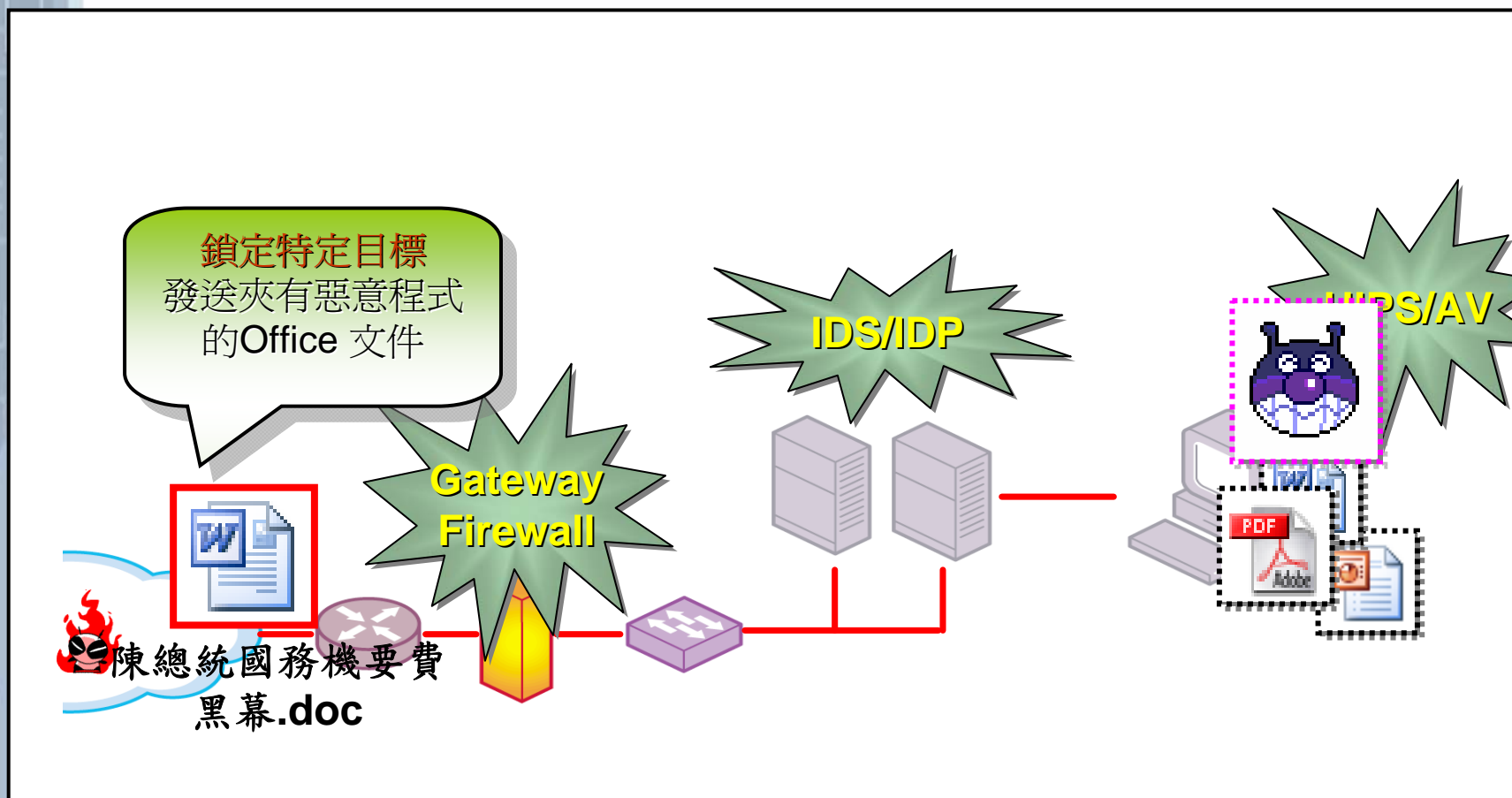
- Advanced Persistent Threat – 特定組織，針對特定目標，利用最新技術有規模地長期進行攻擊
- 資安界習慣發明新名詞，受害者聲稱被新名詞攻擊感覺比較沒有責任:P

# APT攻擊現象



- 採被動為主動，鎖定具有高價值目標的攻擊行為
- 駭客比組織還要了解組織
- 目標明確精準，範圍小樣本少，不易警覺，攻擊內容量身訂做，以假亂真
- 相關的子公司、合作廠商、下包商、物流業者都是可能被攻擊的對象
- 經常拌隨針對性的社交工程攻擊（原名魚叉式攻擊）
- 長期、低調、不易發現

# 魚叉式路徑示意圖



# 網軍



中共對台用兵，國防部之最新評估

檔案(F) 編輯(E) 檢視(V) 工具(T) 郵件(M) 說明(H)

回覆 全部回覆 轉寄 列印 刪除 上一個 下一個 通訊錄

寄件者: ly10717b@ly.gov.tw  
日期: 2006年3月31日 下午 10:25  
收件者: amis@appledaily.com.tw; amu390@ms22.hinet.net; astrid\_tsai@hotmail.com; aug@mail2000.com.tw; av0885@hotmail.com; betty09883@hotmail.com; bresson\_lee@it.chinatimes.com; bressonlee@yahoo.com.tw; busoni@ms37.hinet.net; c1101585@ms26.hinet.net; cashwa@ms75.hinet.net; chihping.chen@udngroup.com; chinghui@mail.bcc.com.tw; chrislee6382@yahoo.com.tw; cindy.chen@ettoday.com; ck030700@yahoo.com.tw; cld@dtm.com.tw; cmf92@ms77.hinet.net; cschena@ms35.hinet.net; cyw@mail.bcc.com.tw; d27@mail.cna.com.tw; dylu@ms15.url.com.tw; dylu@pchome.com.tw; east.chai777@msa.hinet.net; ellen.wu@msa.hinet.net; ellien88@yahoo.com.tw; fang59845984@yahoo.com.tw;  
主旨: 中共對台用兵，國防部之最新評估  
附加檔案: 950331國防委員會新聞參考.doc (93.6 KB)

中共對台用兵，國防部之最新評估見副檔。

寄予各位朋友.rar - WinRAR (evaluation copy)

File Commands Favorites Options Help

Add Extract To Test View

寄予各位朋友.rar - RAR archive, u

Name

寄予各位朋友.doc

建立我國通資訊基礎建設安全機制計畫.rar - WinRAR (evaluation copy)

File Commands Favorites Options Help

Add Extract To Test View Delete Find Wizard

建立我國通資訊基礎建設安全機制計畫.rar - RAR archive, u

Name	Size	Packed
建立我國通資訊基礎建設安全機制計畫.exe	1,052,672	1,009,418

# 被狠狠羞辱的資安大神



▲ 社交工程偽冒信件內容，資料來源：<http://krebsonsecurity.com>

簡單摘要如下，駭客先冒充Greg Hoggund寄給他們公司的IT manager說：「我現在人在歐洲出差，我想連回進公司Server，情況很急，等一下就要用，可以幫我改一下Firewall的設定，以及把Root密碼改成changeme123嗎？」

IT Manager說：「OK！」

呃...之後，我就不用說了，反正是很歡樂... XD

### 有防火牆就不會資料外洩？

這些外洩的E-mail十分精彩，八卦內幕都有，包含HB Gary跟CIA、NSA、FBI、軍方、參議院還有各家資安公司往來信件都被公佈在網路上（據聞某朋友熬夜看了兩天，看到欲罷不能！）。原來HBGary也幫美國政府單位研究很多網軍的活動，據說也做了一些阿里不達的事情，而且對大陸駭客也著墨不少，由此可知各國對於資訊戰爭已經是提升到國防等級問題。反觀我們政府的資安態度，每次都是那句老話「本單位設置有XX道防火牆，沒有資料外洩情況發生」。

### 結論

這個故事告訴我們，花再多錢買了再多道防火牆、防水牆、防毒牆、防釣蝦牆、防釣魚牆都沒有，上了再多的教育訓練也沒用。

你看，一家國際級的資安公司三兩下就被幹掉，連大師也殞落了。

史記資安篇有記載，正所謂「樹大有枯枝，人多有白癡，雞排加辣最好吃」，駭客隨時都在虎

# 惡意附件檢查

● <http://scan.xecure-lab.com/>

XecScan - Xecure Lab - Windows Internet Explorer

<http://scan.xecure-lab.com/>

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

☆ 我的最愛 ☆ 自訂連結 Plurk

XecScan - Xecure Lab

**XecScan**  
Rapid APT Identification Service

Upload Query

**History**

Date	Result	File Name	MD5	State
2011/11/28	Malicious	meeting.xls...	fce668ba548d3a29ffc76bef...	★

Page 1 of 7 173, 1 - 25

**Report**

完成 網際網路 105%

# 資訊人員的取捨



安全  
Security

效能  
Performance

便利  
Convenient

管理/實作能力  
Administration

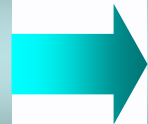
成本  
Cost



# 資安規劃大架構



高層支持  
政策宣示



瞭解需求  
訂立範圍



持續稽核與改進

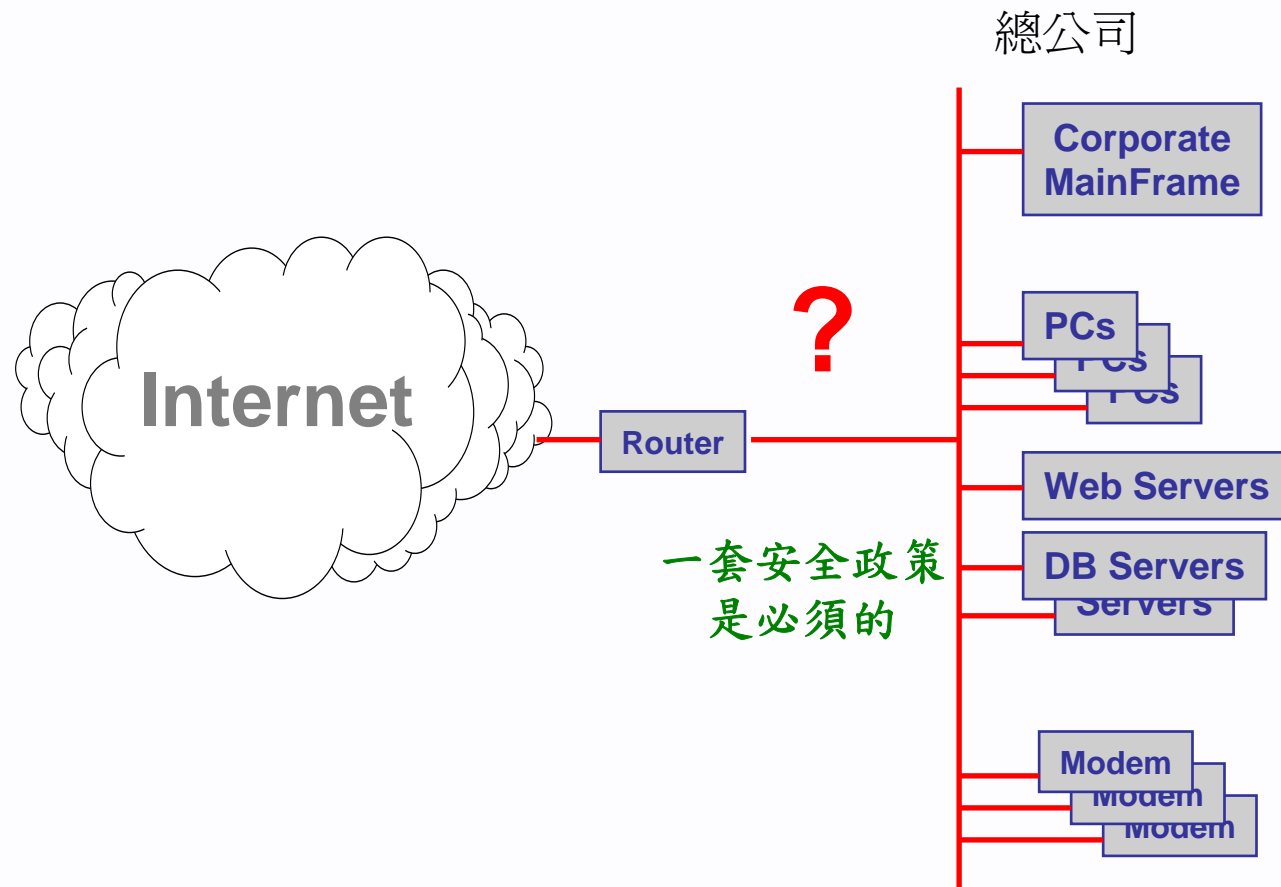
資安教育訓練

部署資安設備 執行專業服務

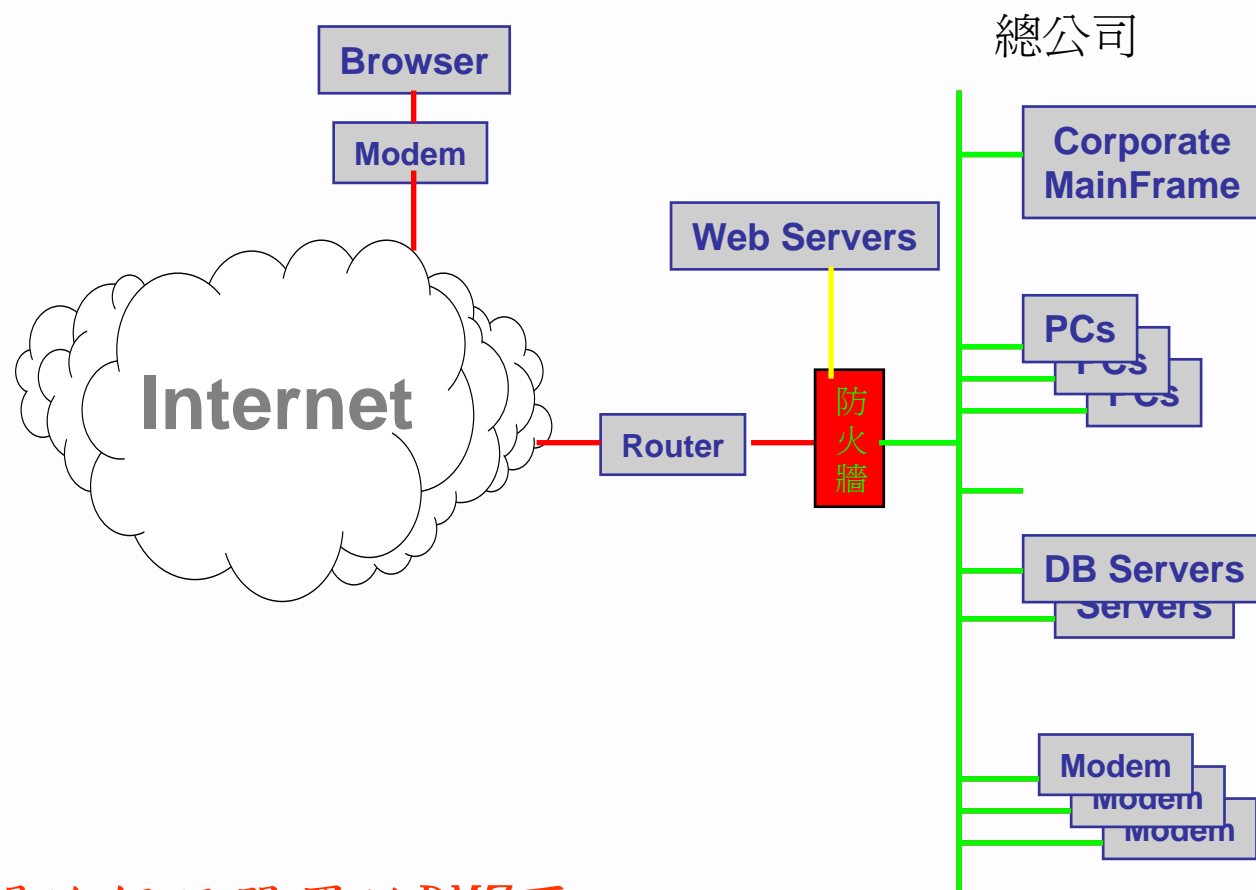
Security Step by Step



# 連接到網際網路隱藏的安全問題



# 建置防火牆區隔網路



並將公開的伺服器置於DMZ區

# 封包過濾



## ● 靜態過濾(Static Packet Filtering)

- ▶ 來源位址(Source IP) 、
- ▶ 來源埠號(Source Port) 、
- ▶ 目標位址(Destination IP) 、
- ▶ 來源埠號(Destination Port) 、
- ▶ 允許活動(Action allow/deny)

## ● 動態過濾(Dynamic Packet Filtering)

- ▶ 除檢查上述參數外，還需記錄並檢查連線狀態

# 防火牆的優、缺點



## ● 優點

- ▶ 保護系統免於遭受易被攻擊服務的威脅
- ▶ 控制存取權
- ▶ 集中安全管理
- ▶ 隱密性 – 利用 proxy
- ▶ 統計資料的蒐集

## ● 缺點

- ▶ 無法限制所有的流量；**僅可管控**流經設備之流量
- ▶ 無法抵抗後門的攻擊 – 如經由位於內部網路的攻擊行為
- ▶ 無法防止病毒的入侵
- ▶ 防火牆形成流量的瓶頸
- ▶ 集中管理 VS. 分散管理

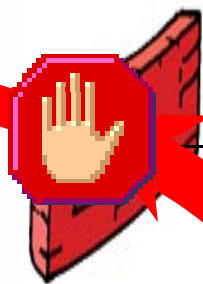
# 迴避防火牆



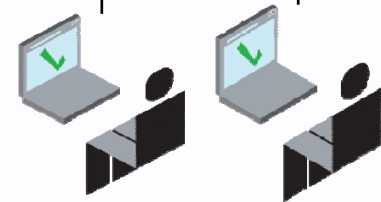
網際網路

防火牆只允許WWW常用埠  
80/TCP

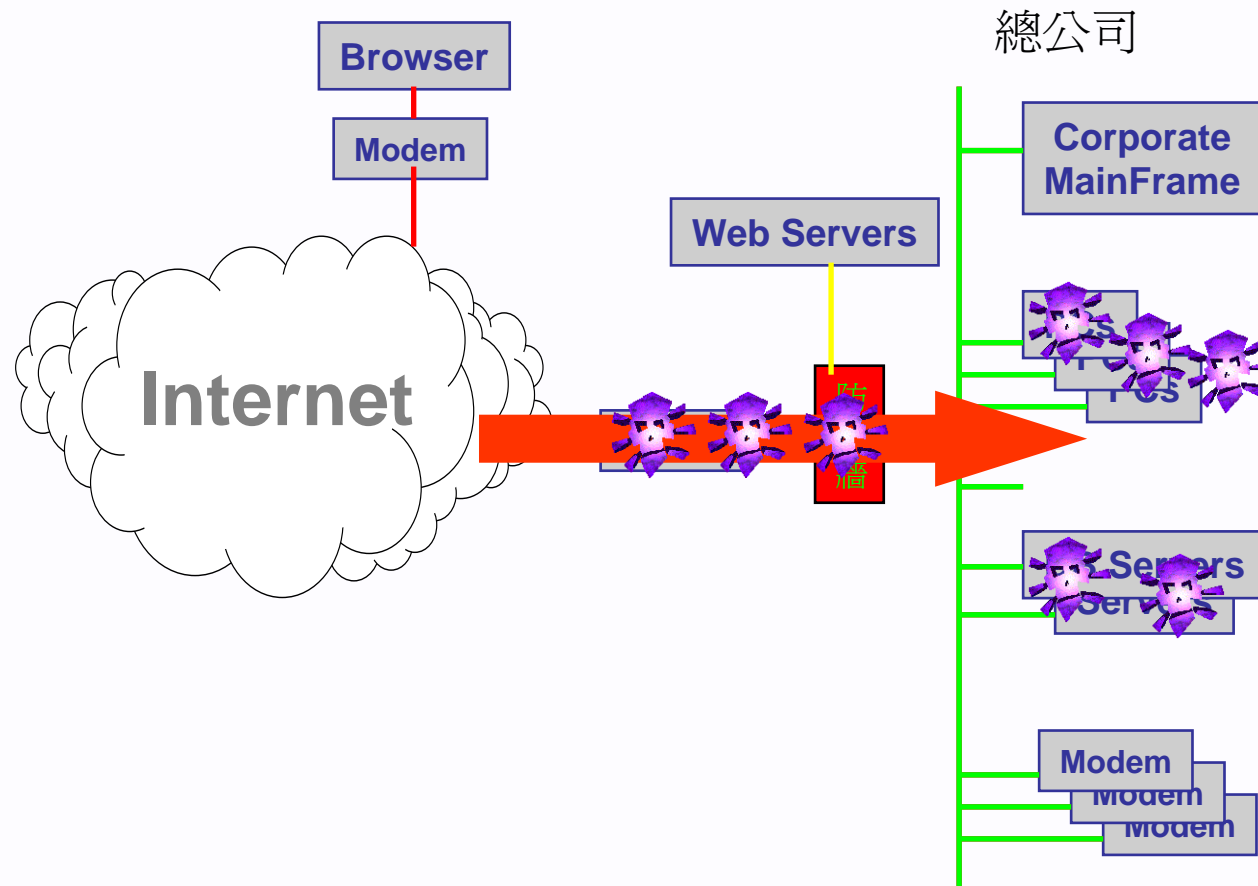
WWW網拍購物  
FTP檔案上傳  
P2P檔案分享  
IM即時通分享  
80/TCP反向式木馬  
P2P使用80/tcp  
IM使用80/tcp  
無界瀏覽



內部使用者

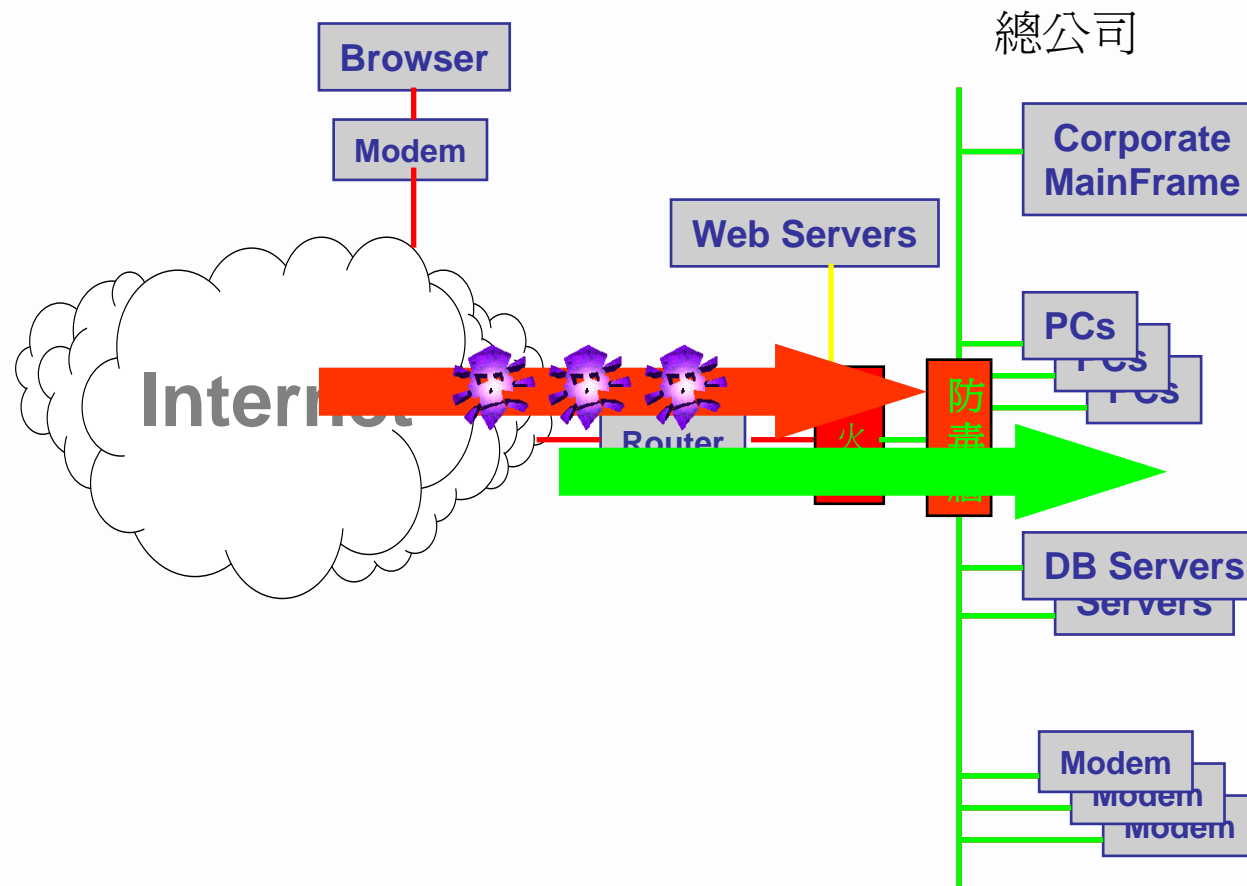


# 網際網路變成病毒主要來源

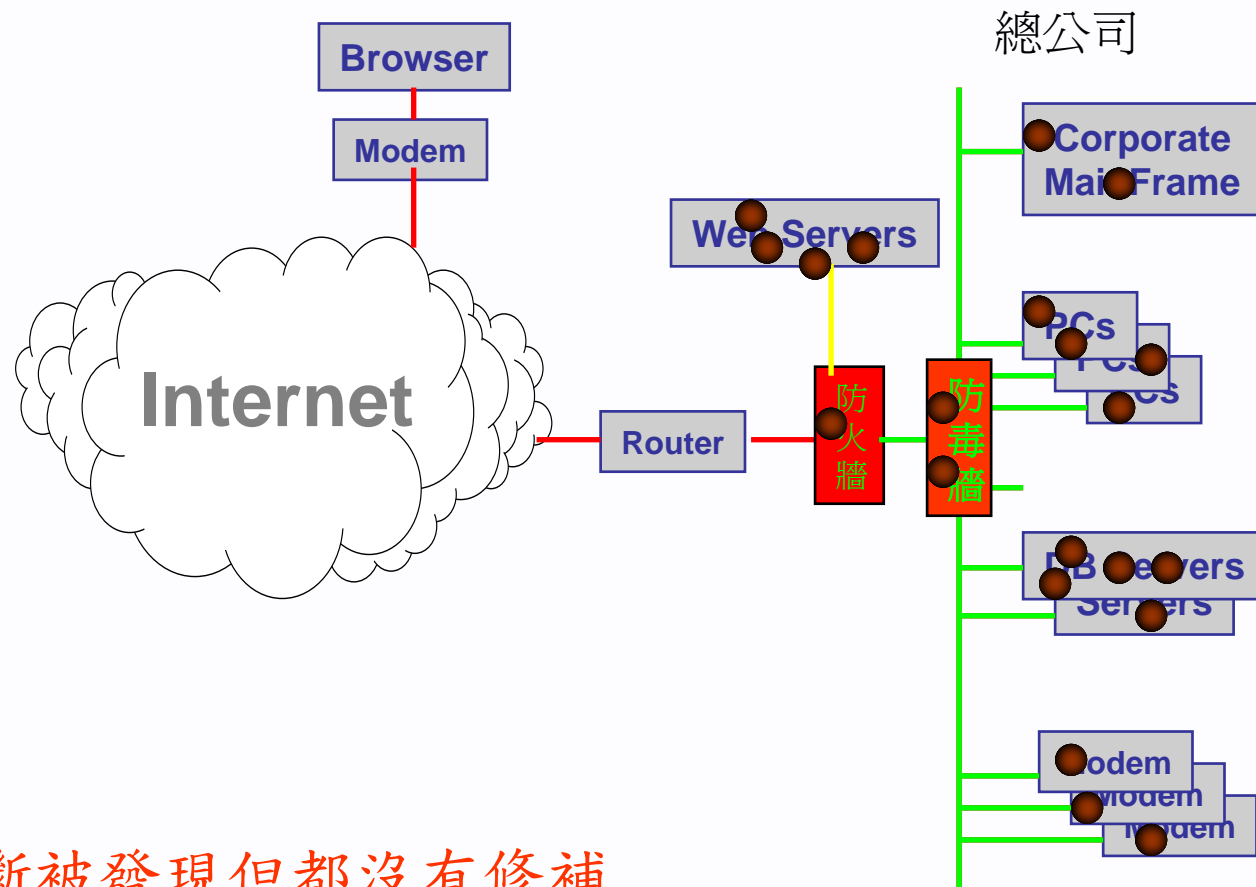


在Mail, HTTP, FTP的檔案中藏有病毒

# 建置防毒牆過濾病毒



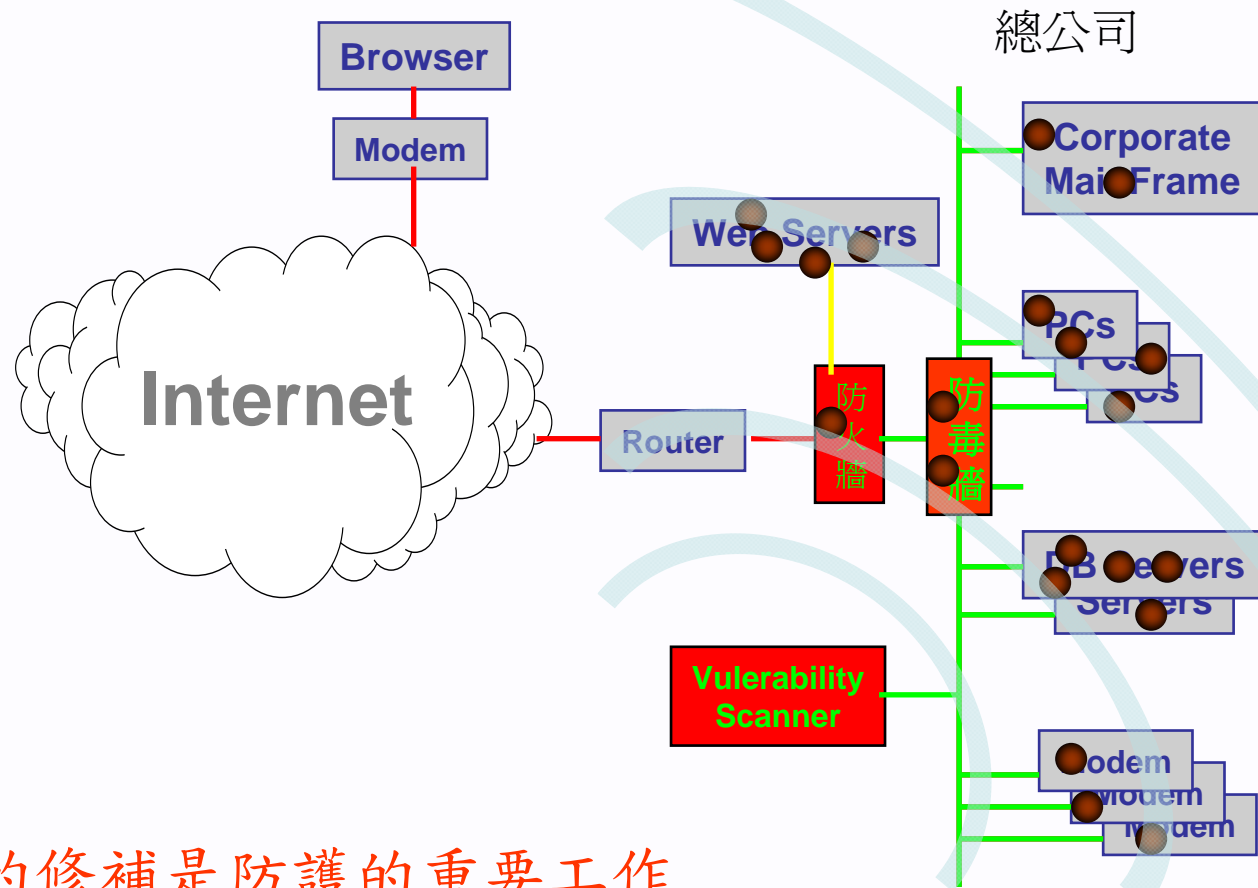
# 系統中有那些漏洞?



漏洞不斷被發現但都沒有修補  
不知道那些系統有那些漏洞

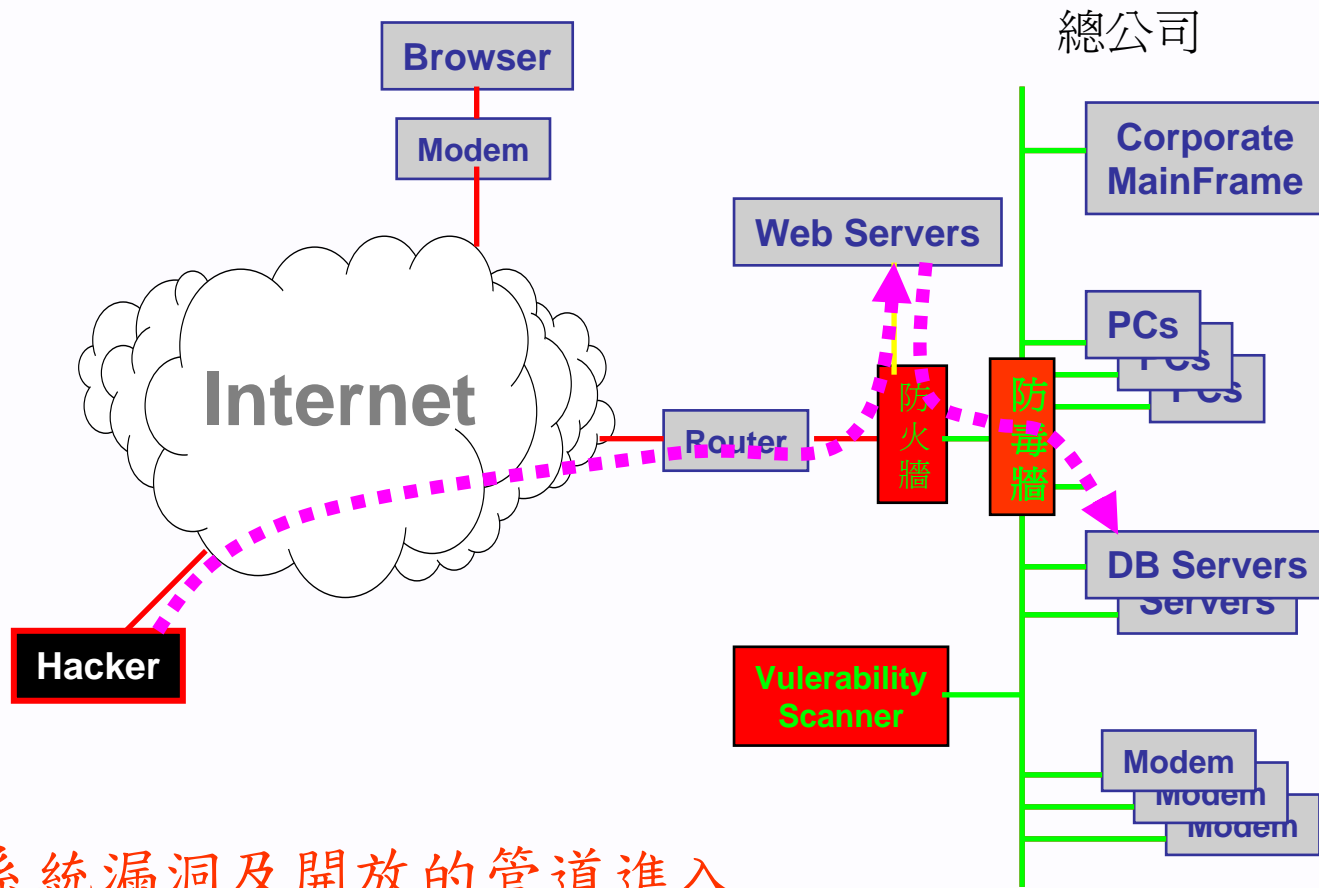


# 定期弱點掃描協助弱點的修補



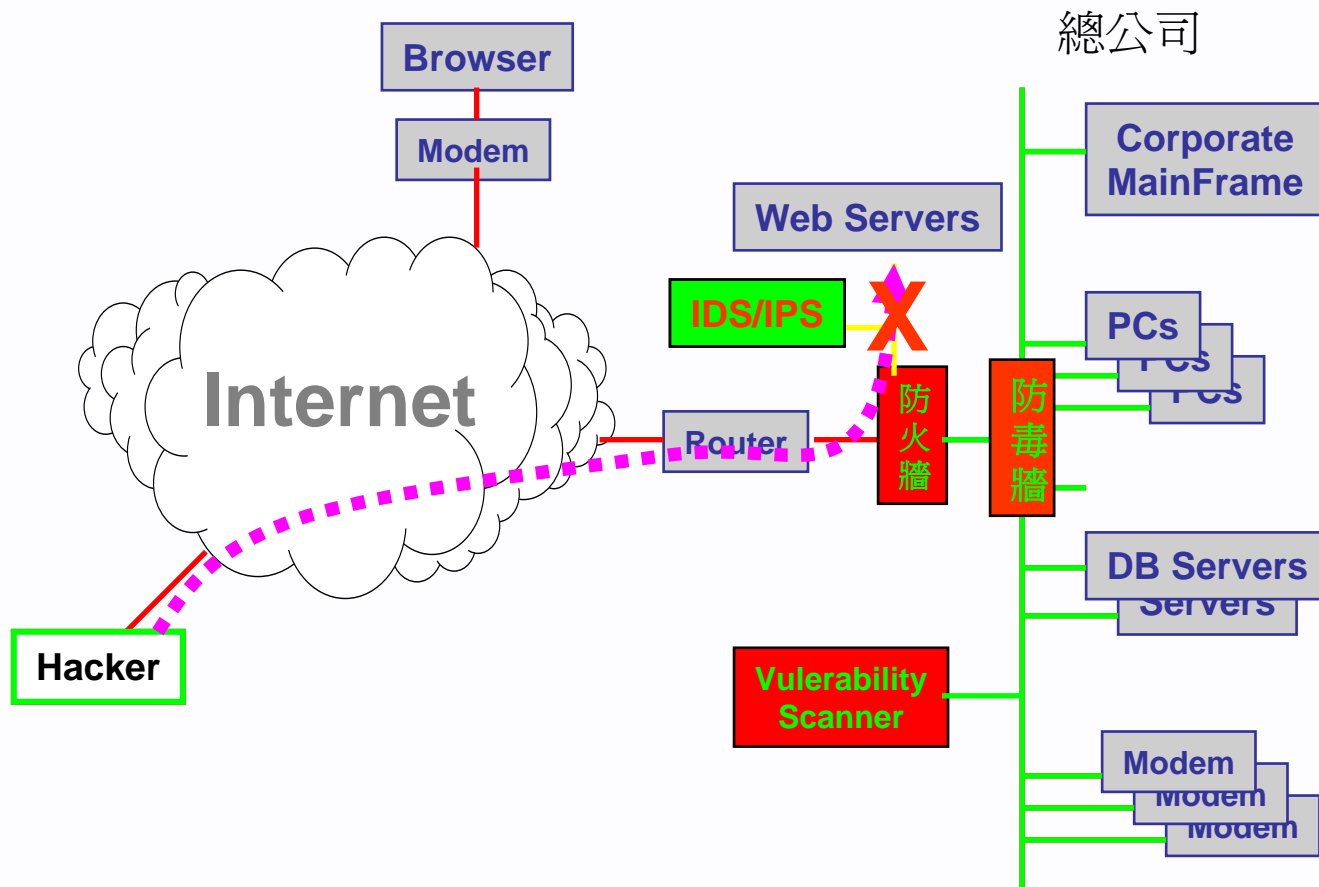
持續性的修補是防護的重要工作

# 駭客的行為無法被測知



透過系統漏洞及開放的管道進入

# 建置IDS/IPS系統讓駭客現形



# 什麼是入侵偵測？



- 監控在電腦或網路上所發生之事件，再分析事件資料以辨別是否為入侵行為，這種動作即稱為**入侵偵測**。
- 入侵偵測系統
  - ▶ Intrusion Detection Systems, IDS
  - ▶ 為負責偵測入侵的自動軟體或硬體設備。
- 入侵防禦系統
  - ▶ Intrusion Prevention Systems, IPS
  - ▶ 又稱IDP, Intrusion Detection and Prevention
  - ▶ 閘道式，除偵測外，可直接進行阻擋
  - ▶ Virtual Patch

# 入侵偵測系統與防火牆的差異



- 防火牆被視為網路的守門員，但是它們能提供的防護卻十分有限。它們最大的問題在於，**防火牆只能檢查少數的封包內容**
- 要檢查封包的內容，企業必須在安全部署中加入入侵偵測的機制。入侵偵測系統可以協助在**早期階段辨識攻擊**，提供企業組織**快速的資安事端分析與更多的回應時間**，並部署防禦機制以防範進一步的攻擊事件。

# Network-Based(NIDS)



- 網路型式的入侵偵測系統以原始網路封包作為資料來源，它通常運用網路卡於“**promiscuous mode**”來偵測及分析所有過往的網路流量，進行**即時分析**
- 當偵測到有惡意行為時，可採多種反應方式應對，各包括通知管理者、切斷連線或記錄入侵資料等
- 優點
  - ▶ 可以同時監控多台主機的網路活動
  - ▶ 駭客消除入侵證據較困難
  - ▶ 可偵測到未成功或惡意的入侵攻擊
  - ▶ NIDS本身不怕攻擊
- 缺點
  - ▶ 可能會Lost Packet，無法完全監控
  - ▶ 無法分析加密過後的封包
  - ▶ 無法得知攻擊是否成功

# NIDS原理-Sniffing側錄



- Sniffing –側錄同網段的網路封包。
- Sniffers – 側錄網路資料的工具，兩面刃
- 只進行側錄，不攔截或改變封包內容，難以發覺
  - ▶ 流量竊聽
  - ▶ 封包竊聽
  - ▶ 內容竊聽
  - ▶ 密碼竊聽

使用IDS/IPS前，確定你的網路是否可側錄？

# 分析引擎



## ● 特徵偵測(Signature-Based)

- ▶ 使用模式比對法(Pattern Matching)，將收集到的資訊與特徵資料庫進行比對

## ● 異常偵測(Anomaly-Based)

- ▶ 利用統計工具觀察並列明正常與異常行為，



# 特徵偵測法



- 採負面表列
- 累積已知攻擊行為特徵 (attack pattern)
- 亦會因為正常之行為中有攻擊行為特徵而被誤解為有攻擊行為
- 只可偵測已知的攻擊行為

# 異常偵測法



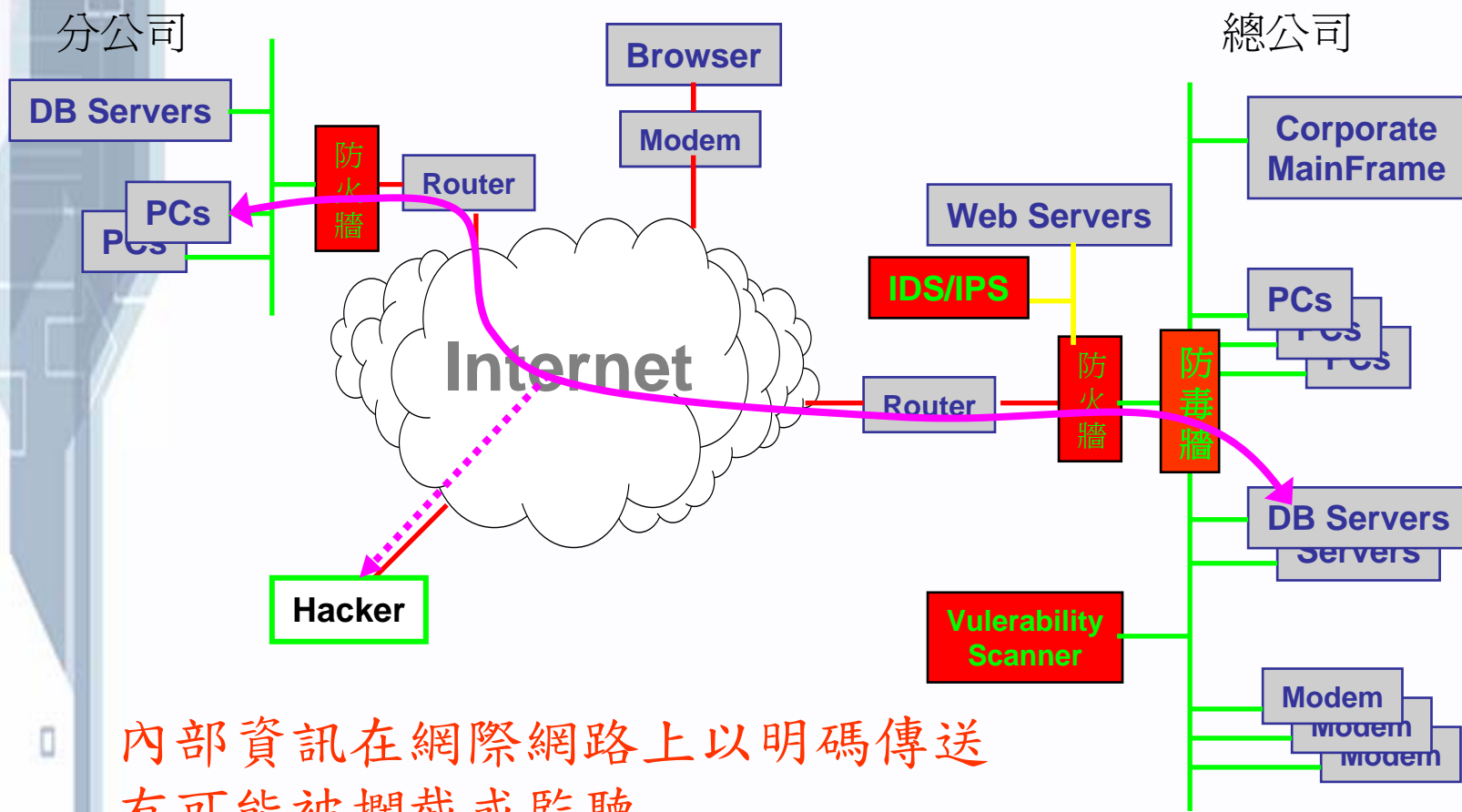
- 採正面表列
- 正面表列規範網路正常行為(Normal Activity)，凡不在此正常行為範圍者都視為異常
- 常造成誤判而拒絕正常網路連線
  - ▶ 難以定義"Normal Activity"
- 可偵測**未知**的攻擊行為

# 網路攻擊側錄分析



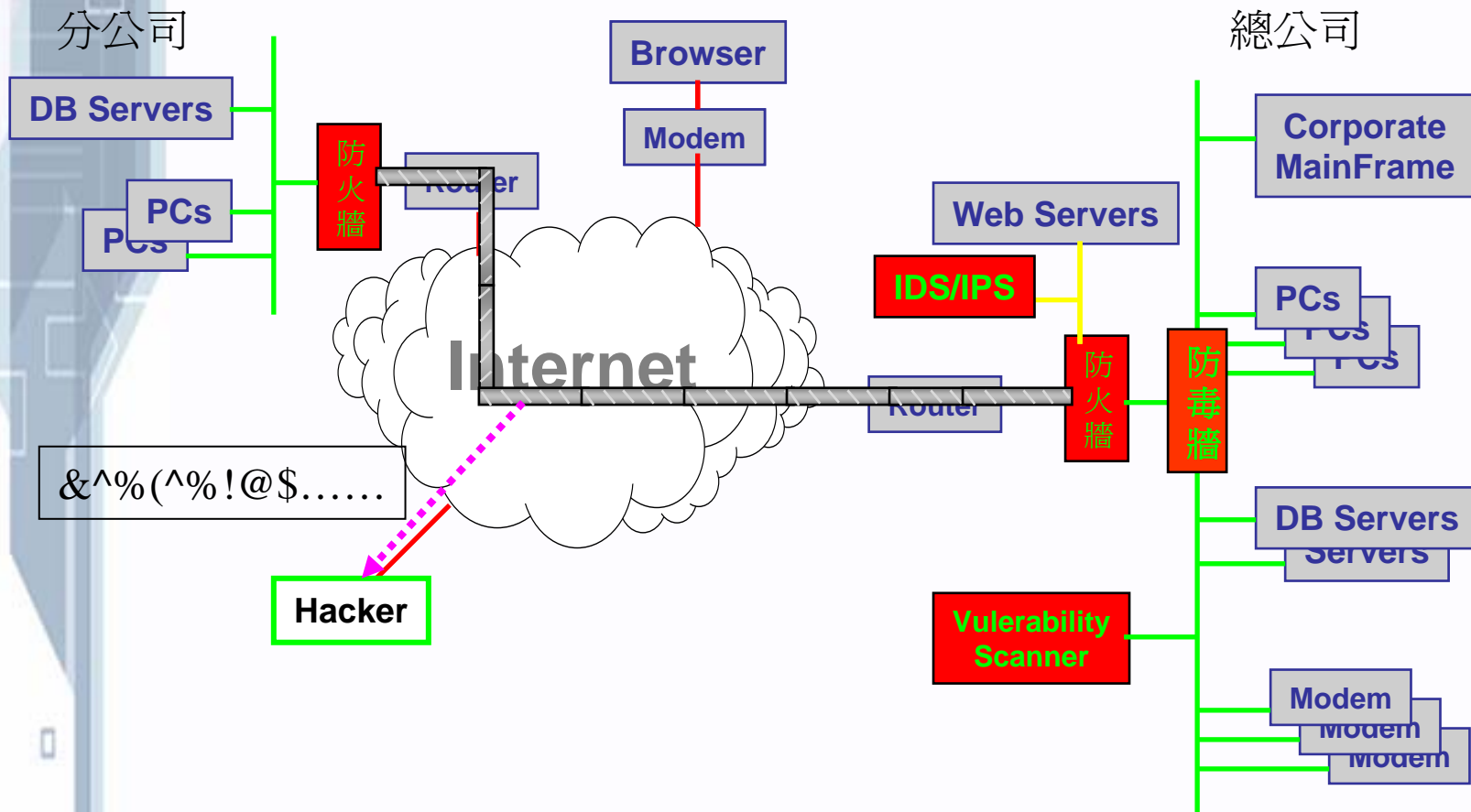
- Network Scan: 針對單一內部主機、大量服務
- Network Sweep: 針對大量內部主機、單一服務
- Worm: 針對隨機內外主機、單一服務
- Backdoor: 非常用埠號的活動
- DoS: 針對單一內部主機、單一服務、大量封包、隨機來源
- Exploit: 特定資料內容與行為(cmd.exe等)
- 其他內容解析：P2P、MSN測錄、ftp測錄...

# 當分公司要透過網際網路傳遞資料時



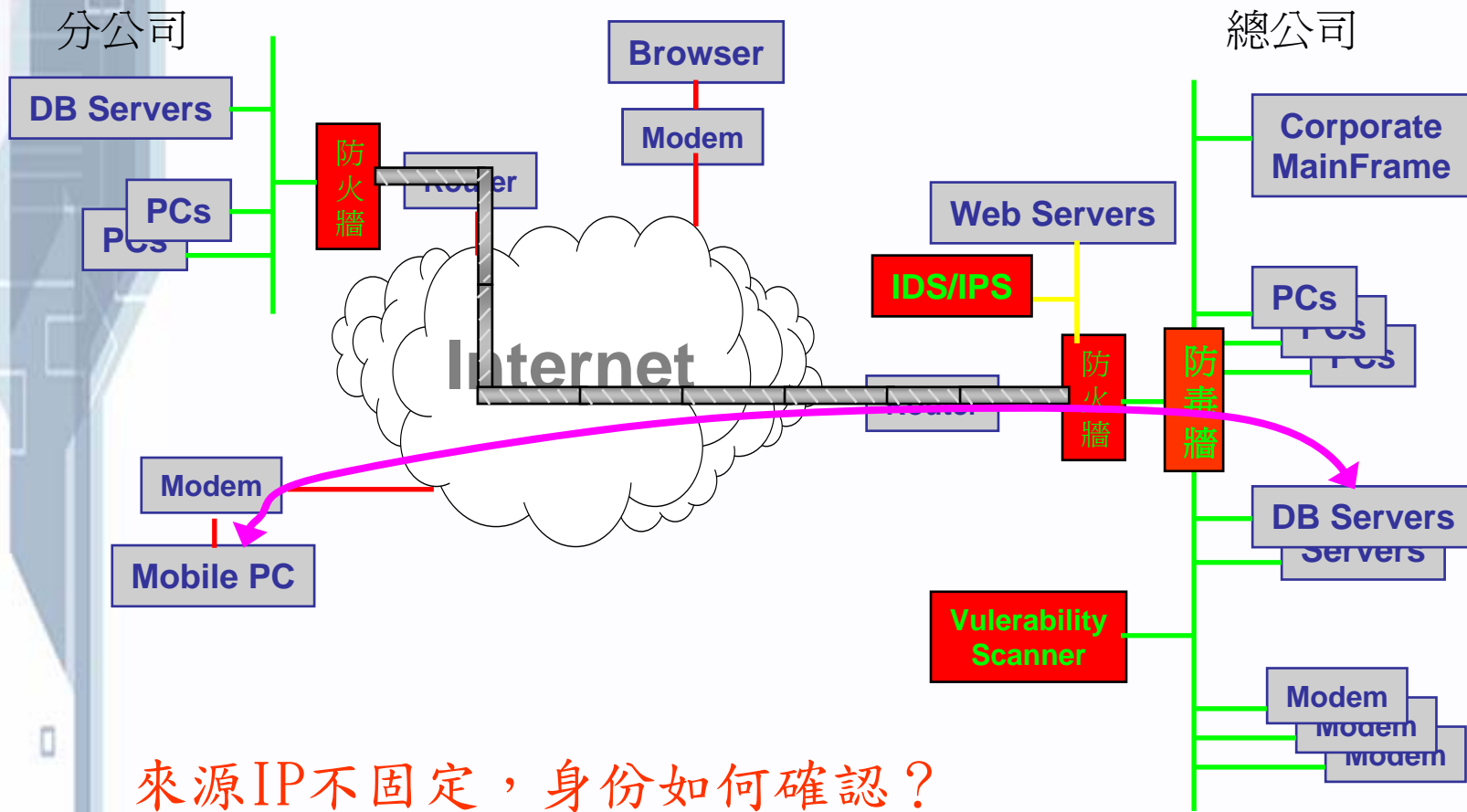
內部資訊在網際網路上以明碼傳送  
有可能被攔截或監聽

# 建置VPN通道確保資料傳輸安全



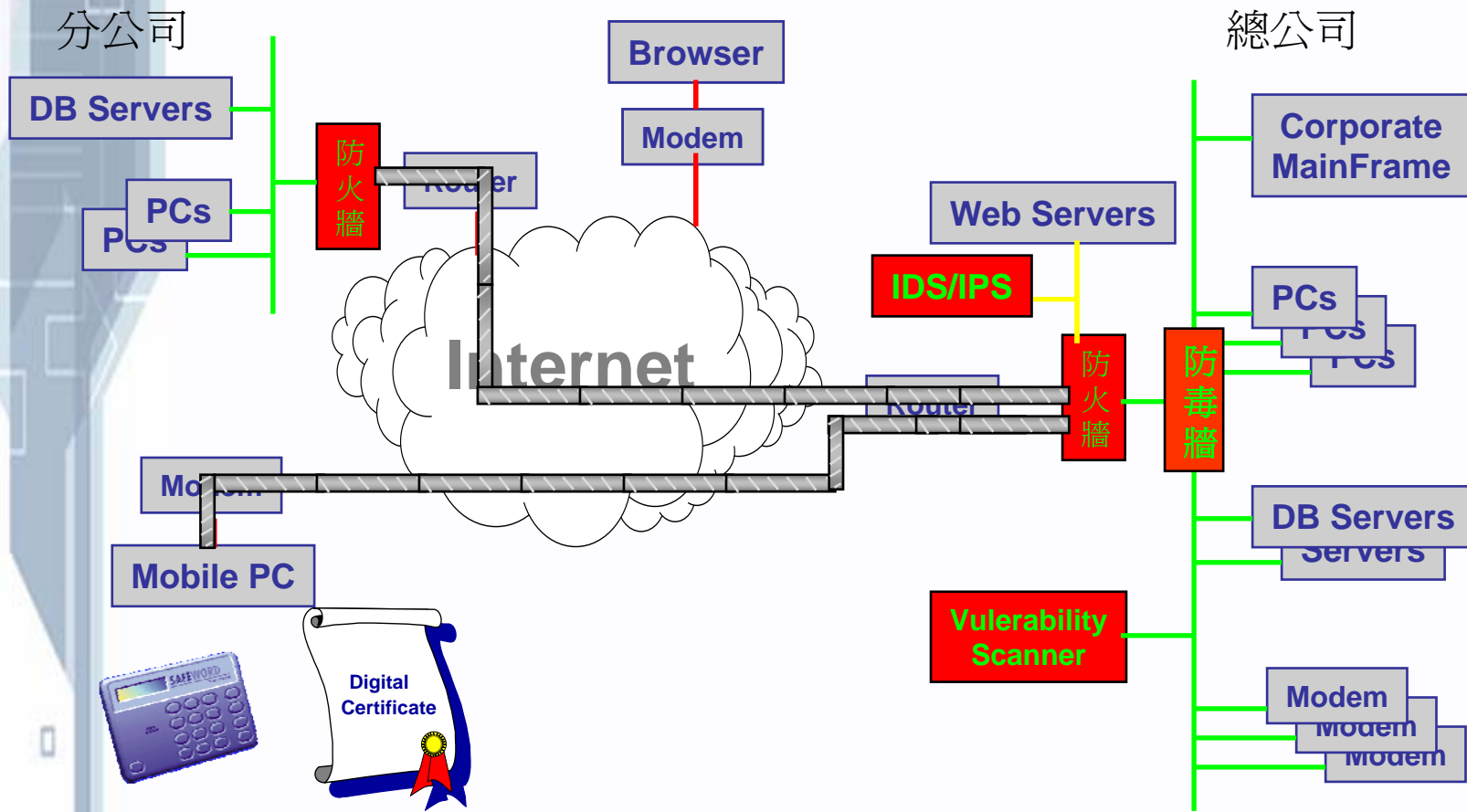
即使被監聽了也是加密資料

# 外勤人員的存取如何確保安全?



來源IP不固定，身份如何確認？  
機密資料傳輸如何保護？

# 採用SSL或Client VPN確保 外勤人員存取安全



身份認證可採用數位憑證或動態密碼

# SSL VPN的掘起



- 不希望因為[無法管理]的設備，而造成helpdesk額外的負擔
  - ▶ 透過瀏覽器存取，無需安裝其他軟體
  - ▶ 無法管理的設備
    - 在家中的使用者(加班、加班...)
    - 上游/下游廠商(對伺服器、應用程式、硬體設備的存取)
    - 合作夥伴(特定的軟體、資料存取結構)
- IPSec有頻繁的穿越網路(防火牆)的問題
  - ▶ SSL使用標準TCP ports
  - ▶ 許多地方，如旅館，會封鎖IPSec protocol
- 薄弱的應用程式存取控制
  - ▶ IPSec使用第三層的"network access"
  - ▶ SSL使用第七層的"application access"

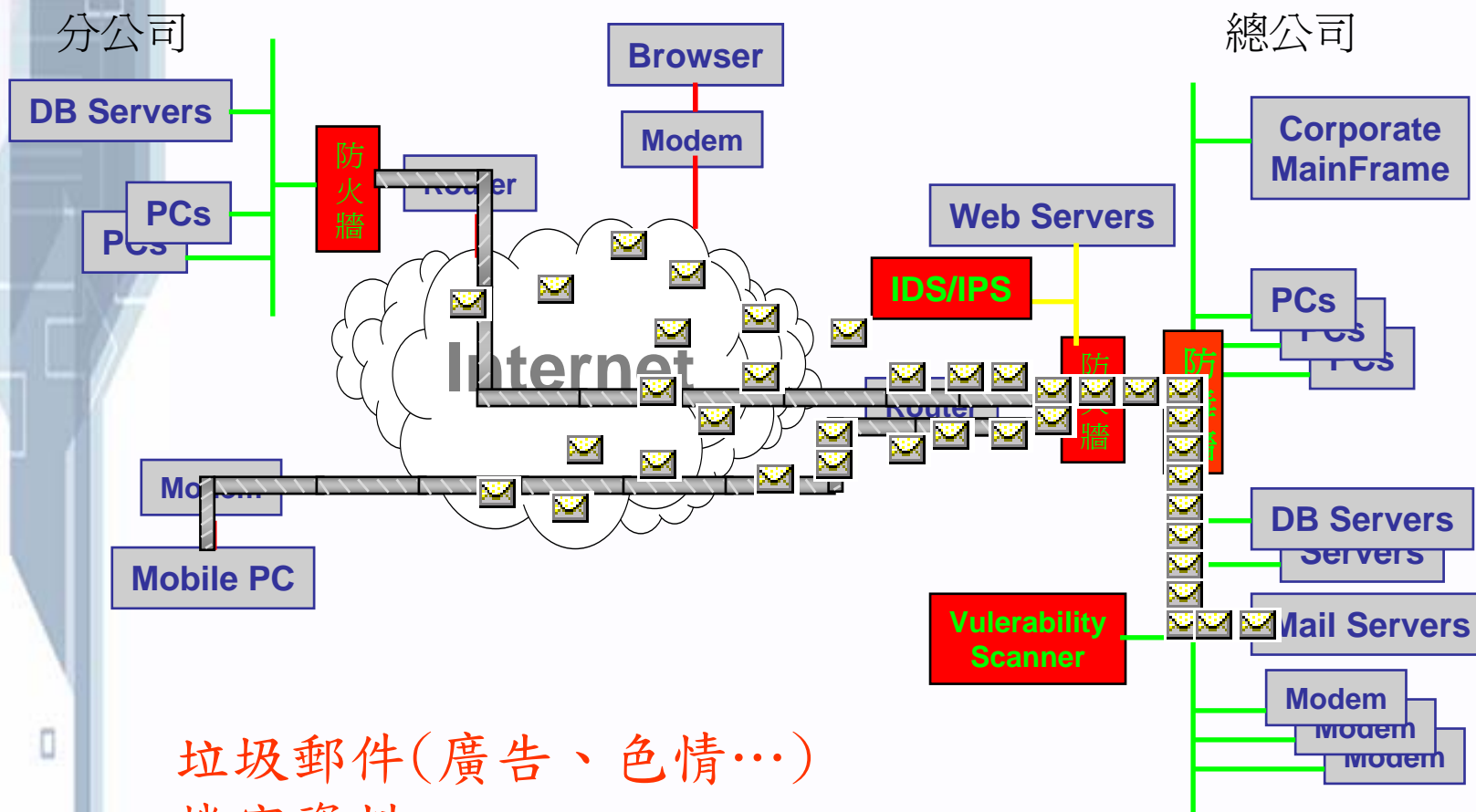


# SSL VPN



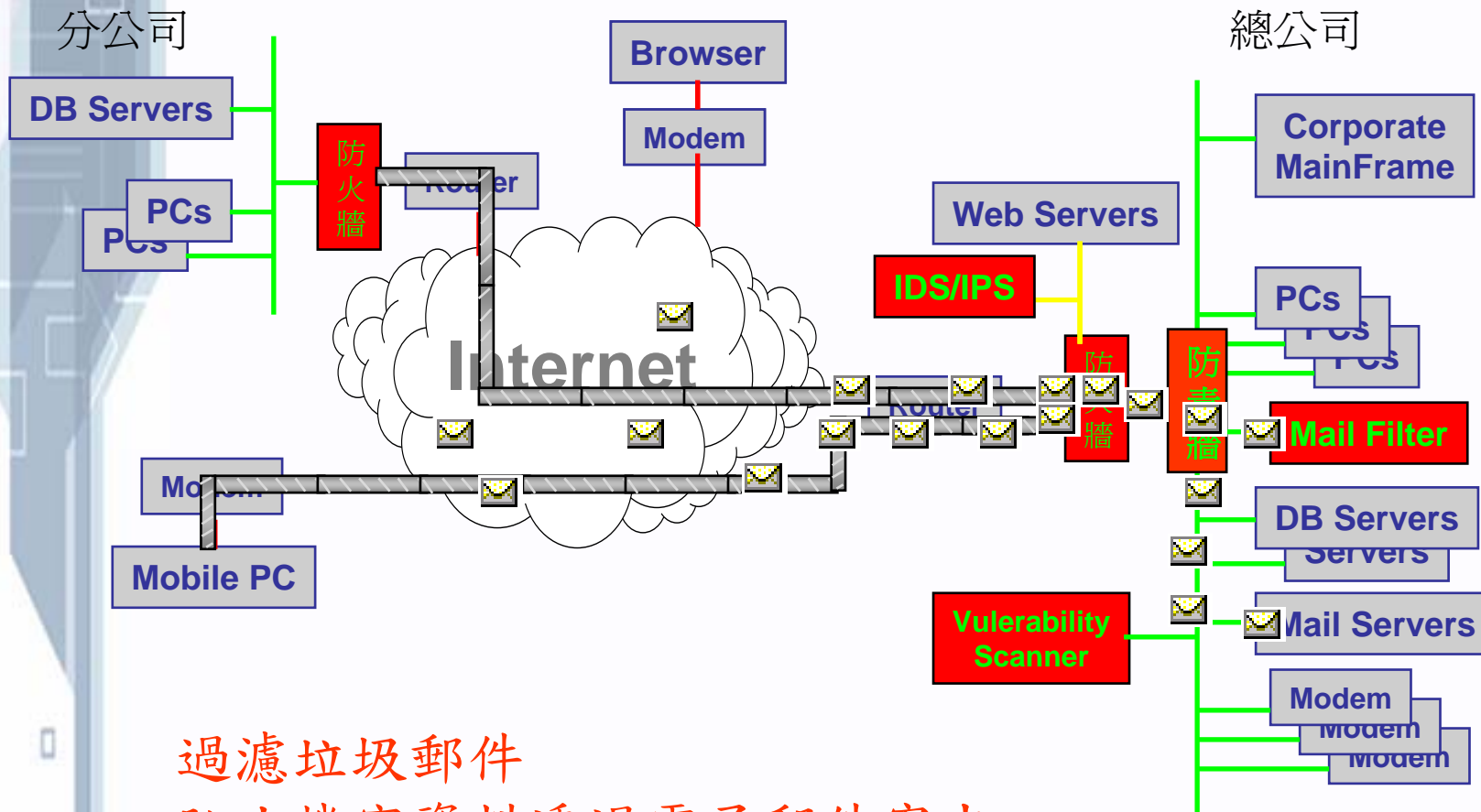
- 透過瀏覽器即可使用(HTTP/HTTPS)
- 電子郵件存取
  - ▶ Outlook (MAPI), OWA, POP, IMAP,SMTP, Notes, iNotes
- 檔案伺服器的使用
  - ▶ Windows CIFS file shares via Web Interface
- 埠號轉送
  - ▶ Access to thick client TCP-based applications
- 可與其他用戶認證系統結合
  - ▶ Group based access control
  - ▶ Support for all enterprise authentication mechanisms

# 電子郵件被濫用



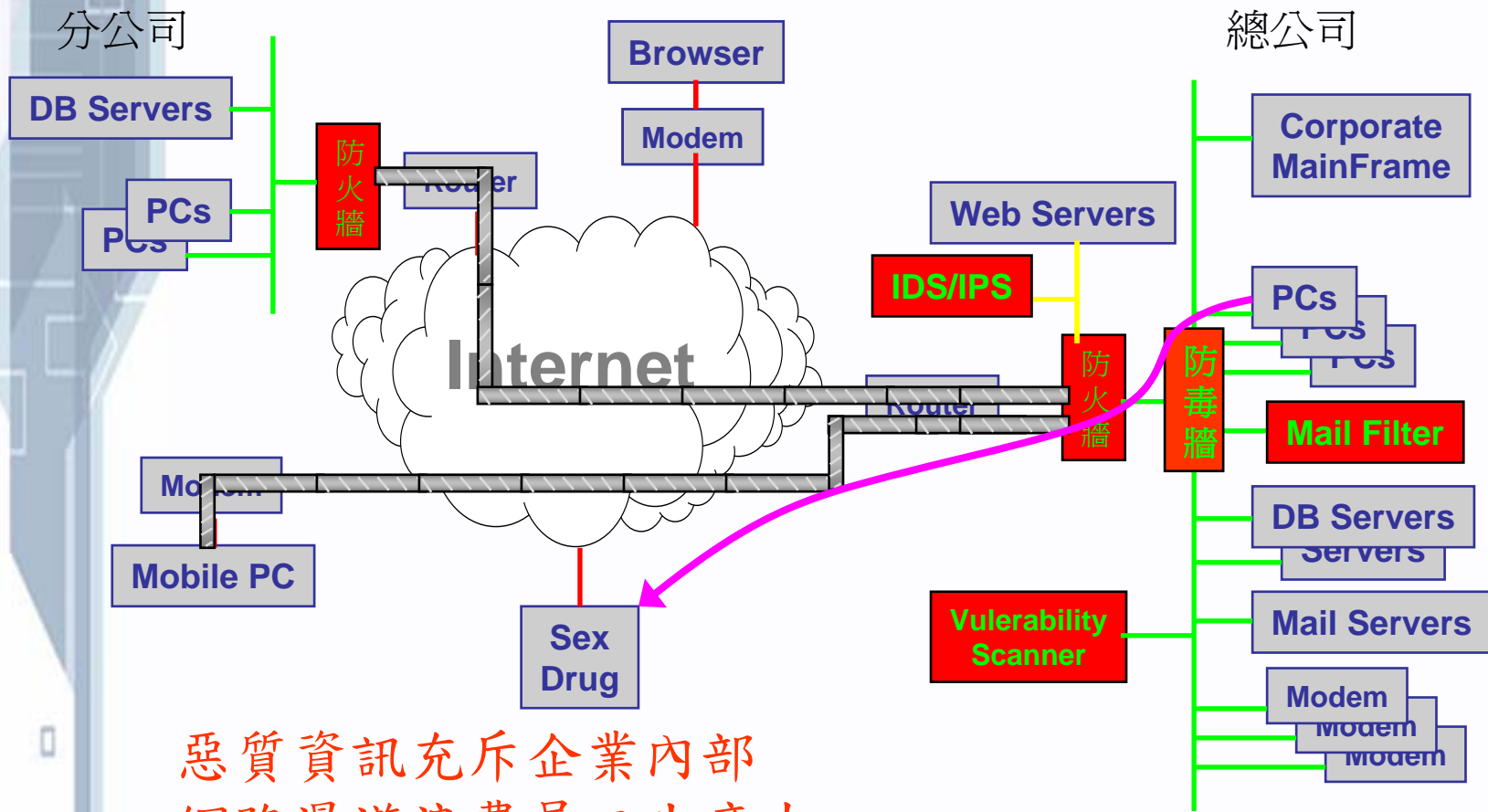
垃圾郵件(廣告、色情...)  
機密資料

# 建置電子郵件過濾匣道 保護機密資料不外洩



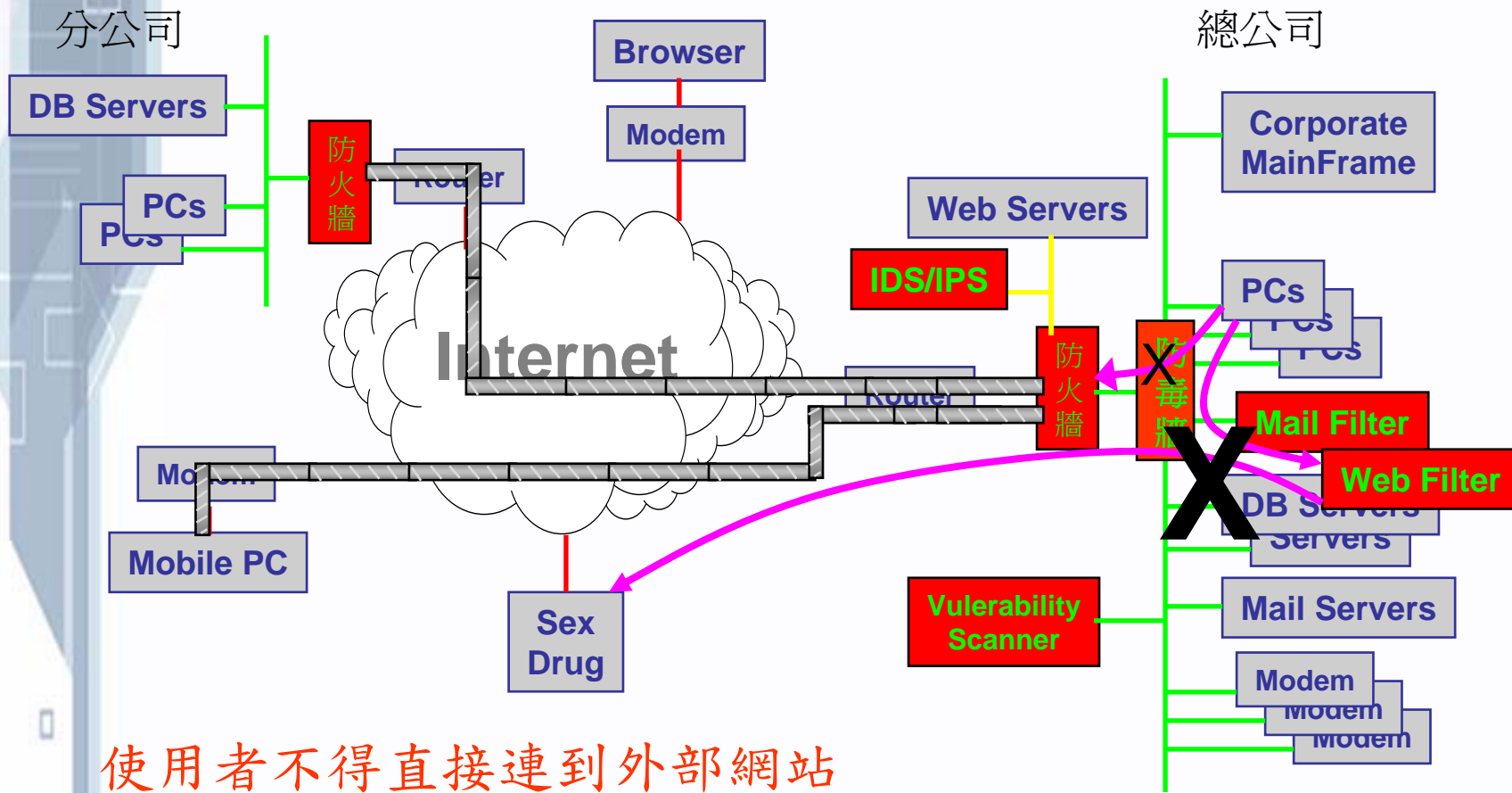
過濾垃圾郵件  
防止機密資料透過電子郵件寄出

# 不良網站充斥網際網路



惡質資訊充斥企業內部  
網路漫遊浪費員工生產力

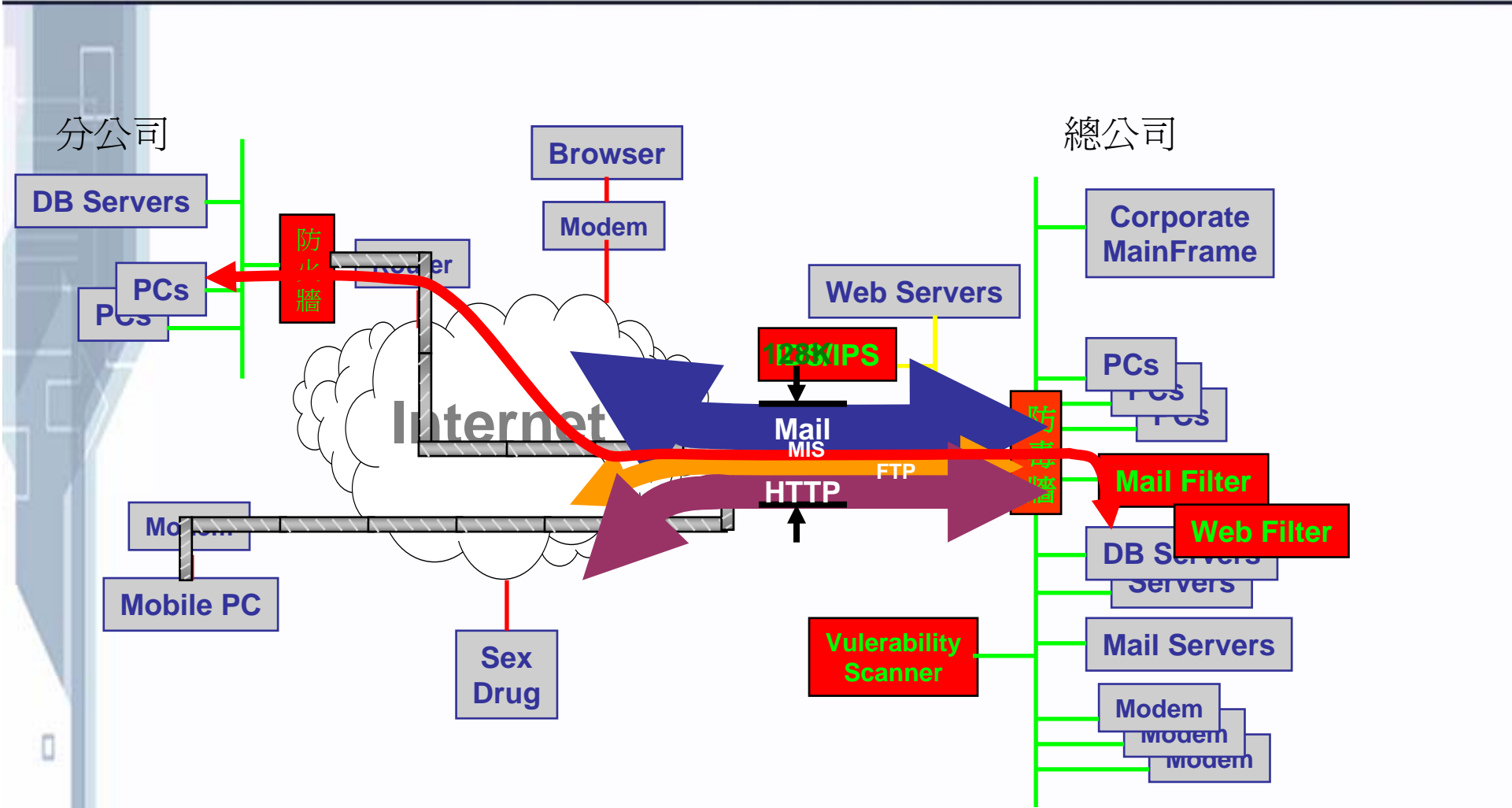
# 建置Web過濾系統確保員工生產力



使用者不得直接連到外部網站

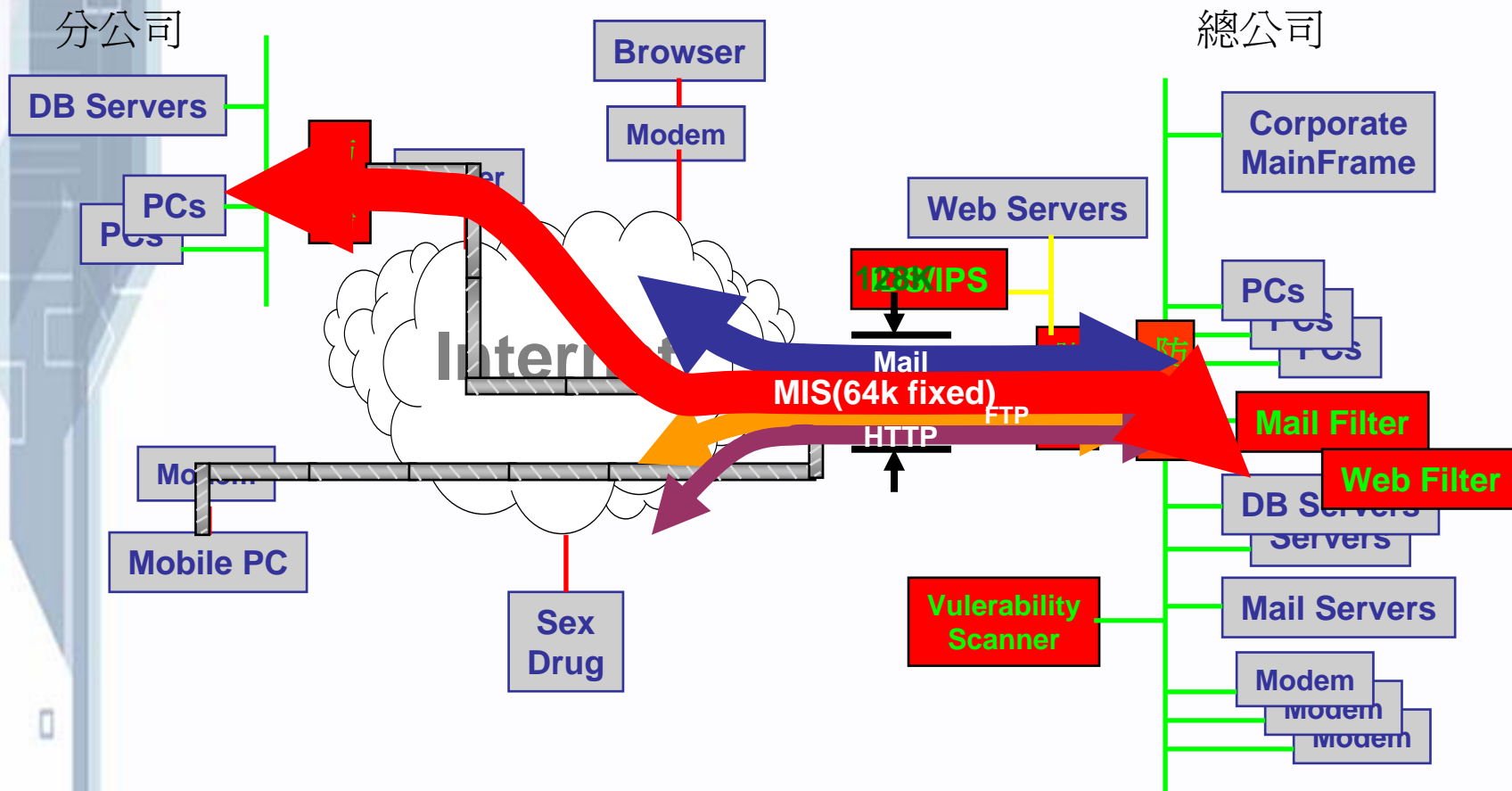
Web Filter拒絕不良網址

# 重要的MIS通訊無法順利傳送



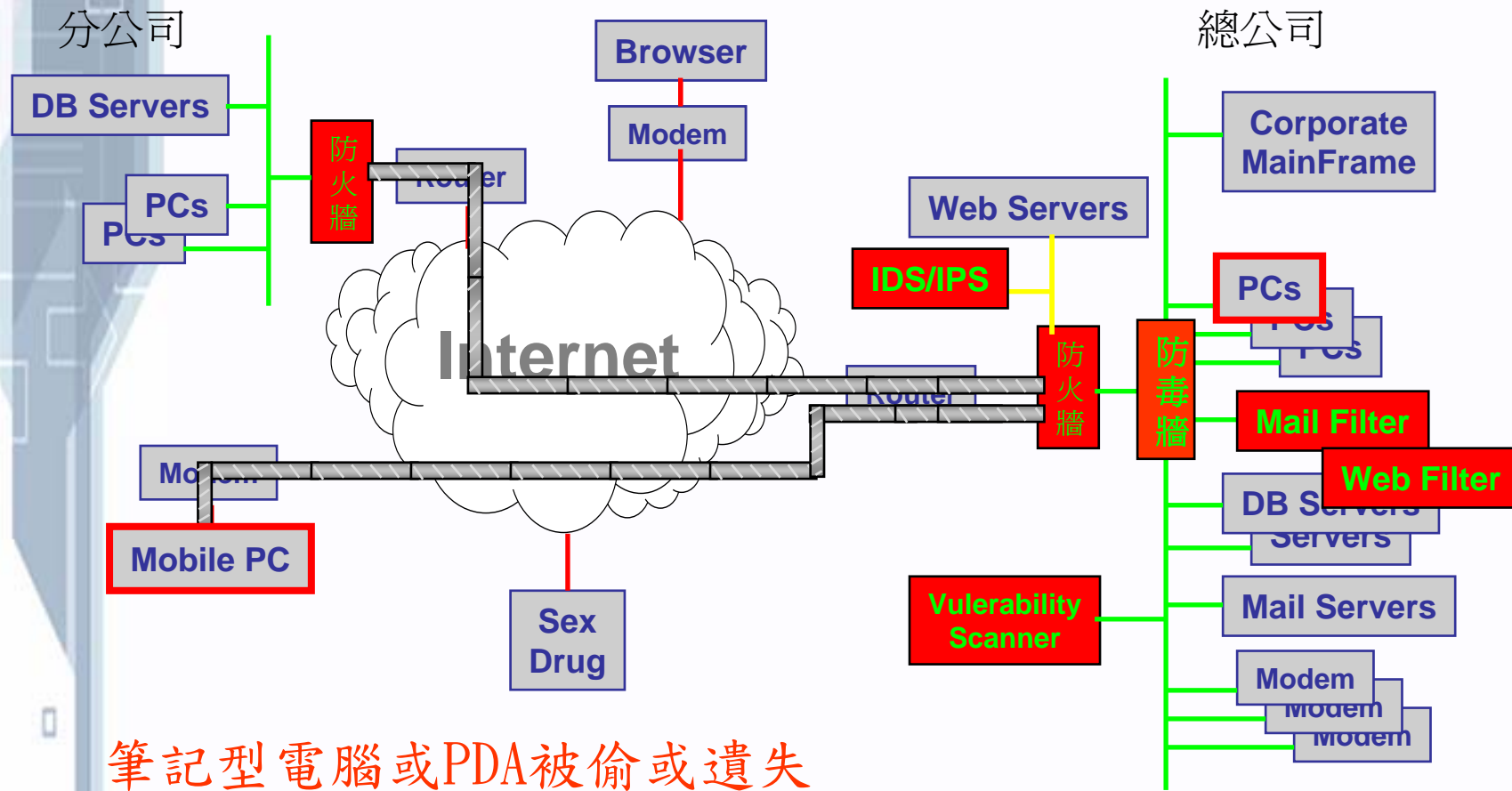
佔據頻寬的竟然都是Mail, HTTP, FTP等不急迫的通訊

# 採用頻寬管理設備保障頻寬可用性



讓最重要的通訊最優先，最有保障

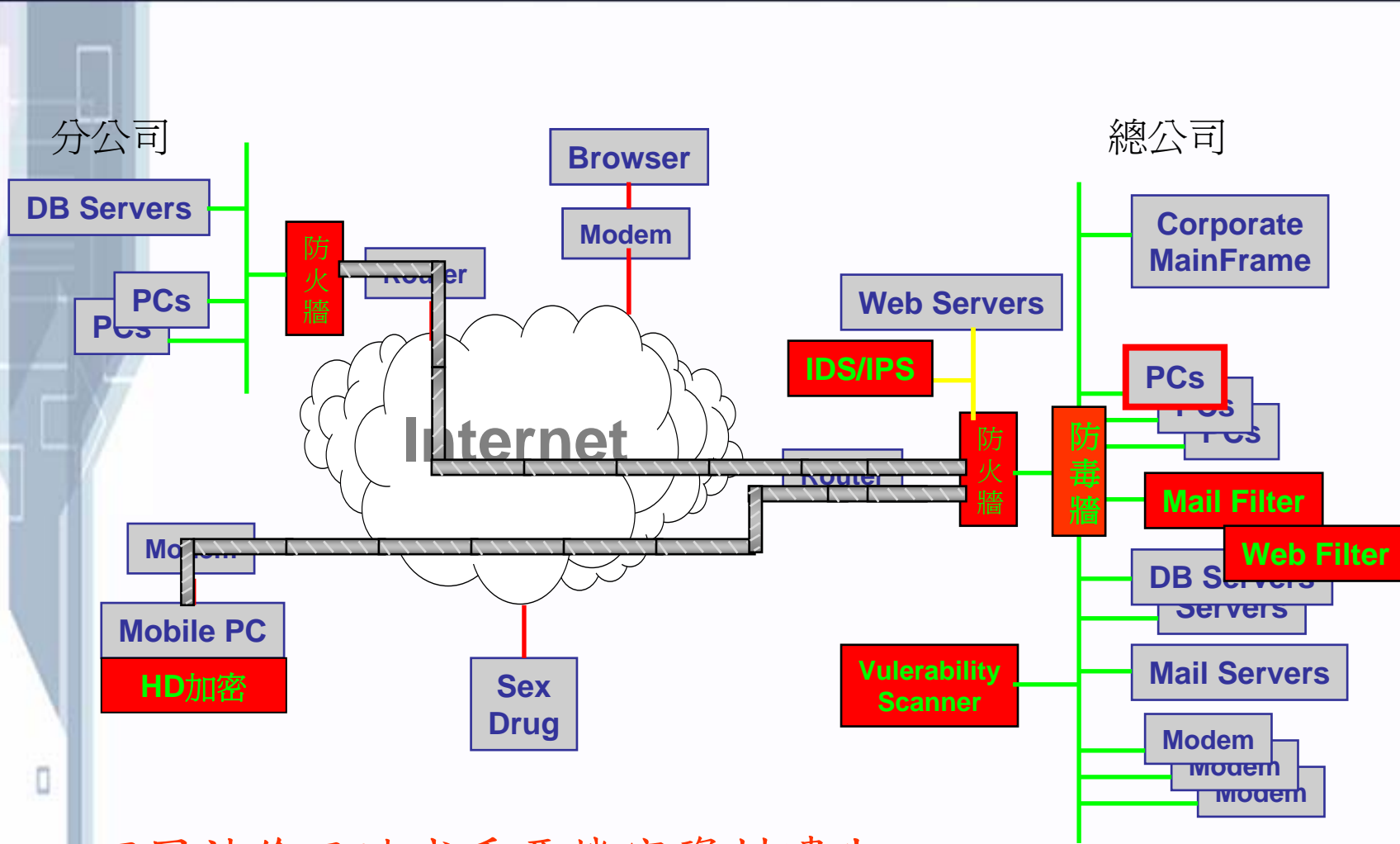
# 個人電腦的安全？



筆記型電腦或PDA被偷或遺失  
PC成為駭客入侵的最佳跳板

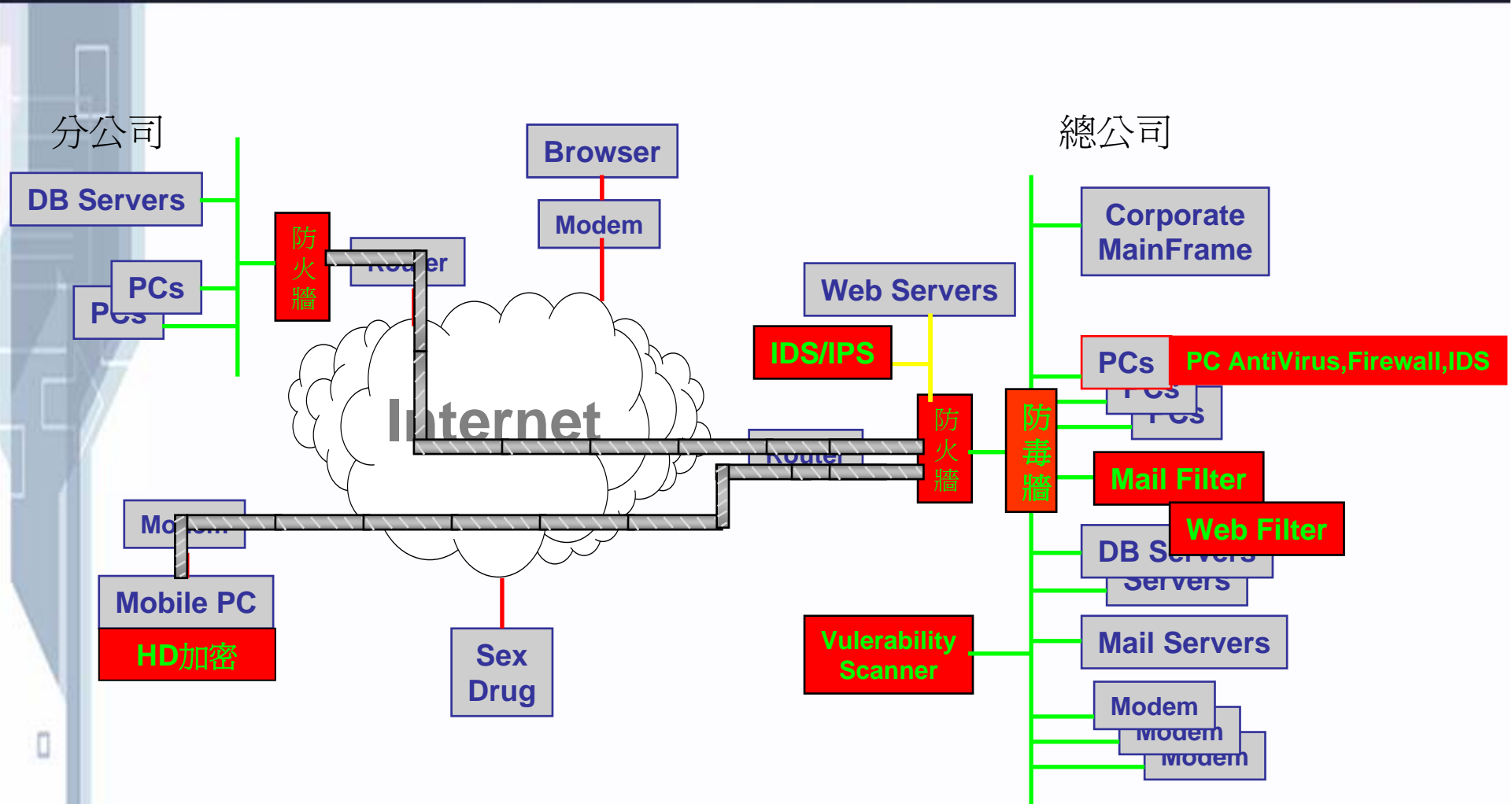


# 硬碟加解密系統保障可攜式媒體安全

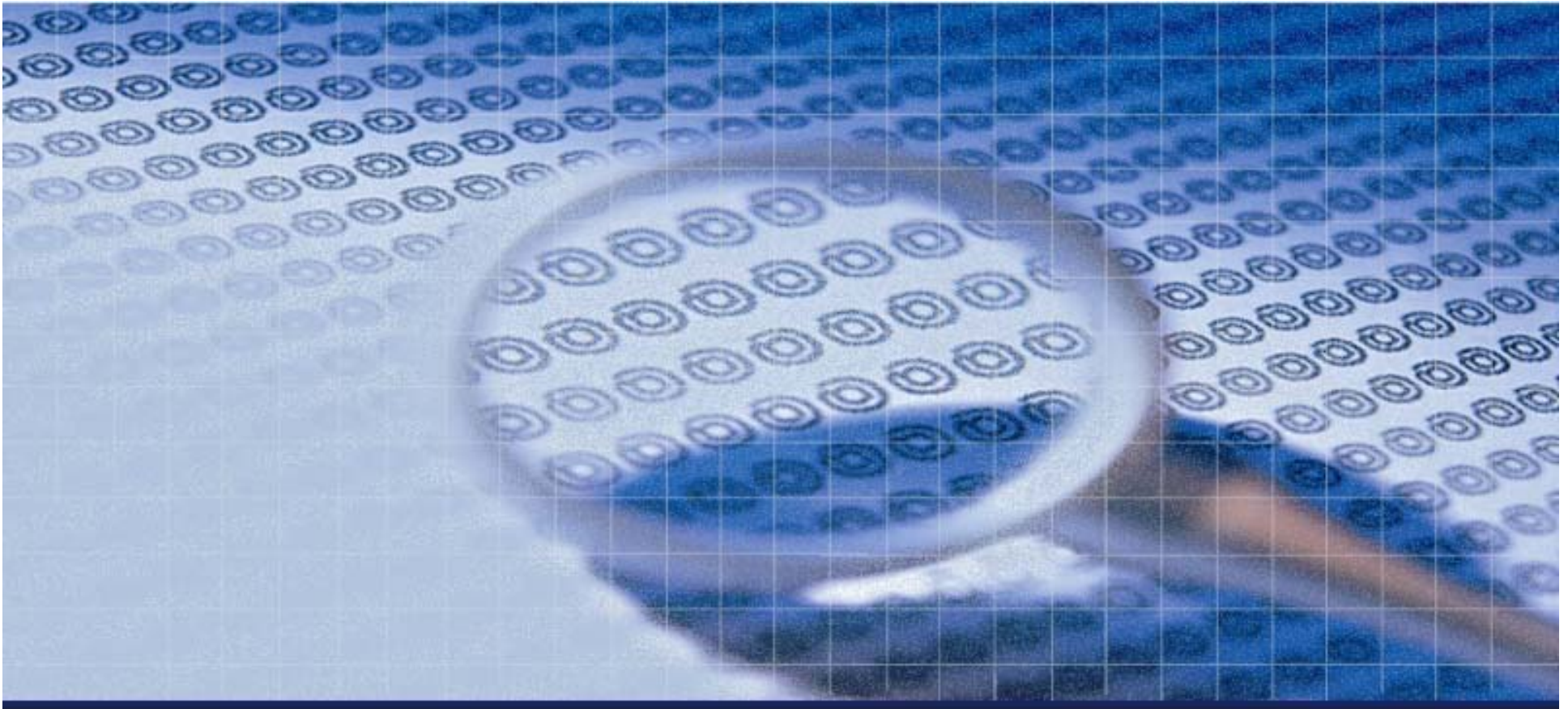


不因被偷而造成重要機密資料遺失

# 個人電腦防毒、防火牆及IDS 加強深度防護



防止內/外部入侵及使用的控管



# 敏感資料外洩防護





**75%的企業用戶不知道自己的機密資料已經外洩。**

**Verizon Business 2008調查報告**

# 高頻率外洩



## 機密資料 的類型

### 客戶資料

身份證號碼  
信用卡卡號  
個人健康醫療資訊

### 企業資料

財務資訊  
合併與併購計畫  
員工資料

### 智慧財產

原始碼  
設計文件  
定價資訊

## 風險事件統計



每**400** 封訊息中，就有 **1** 封包含了機密資料



每 **50** 個網路檔案中，就有 **1** 個不當曝露在外



每**5** 家公司，就有 **4** 家曾遺失筆記型電腦上的資料

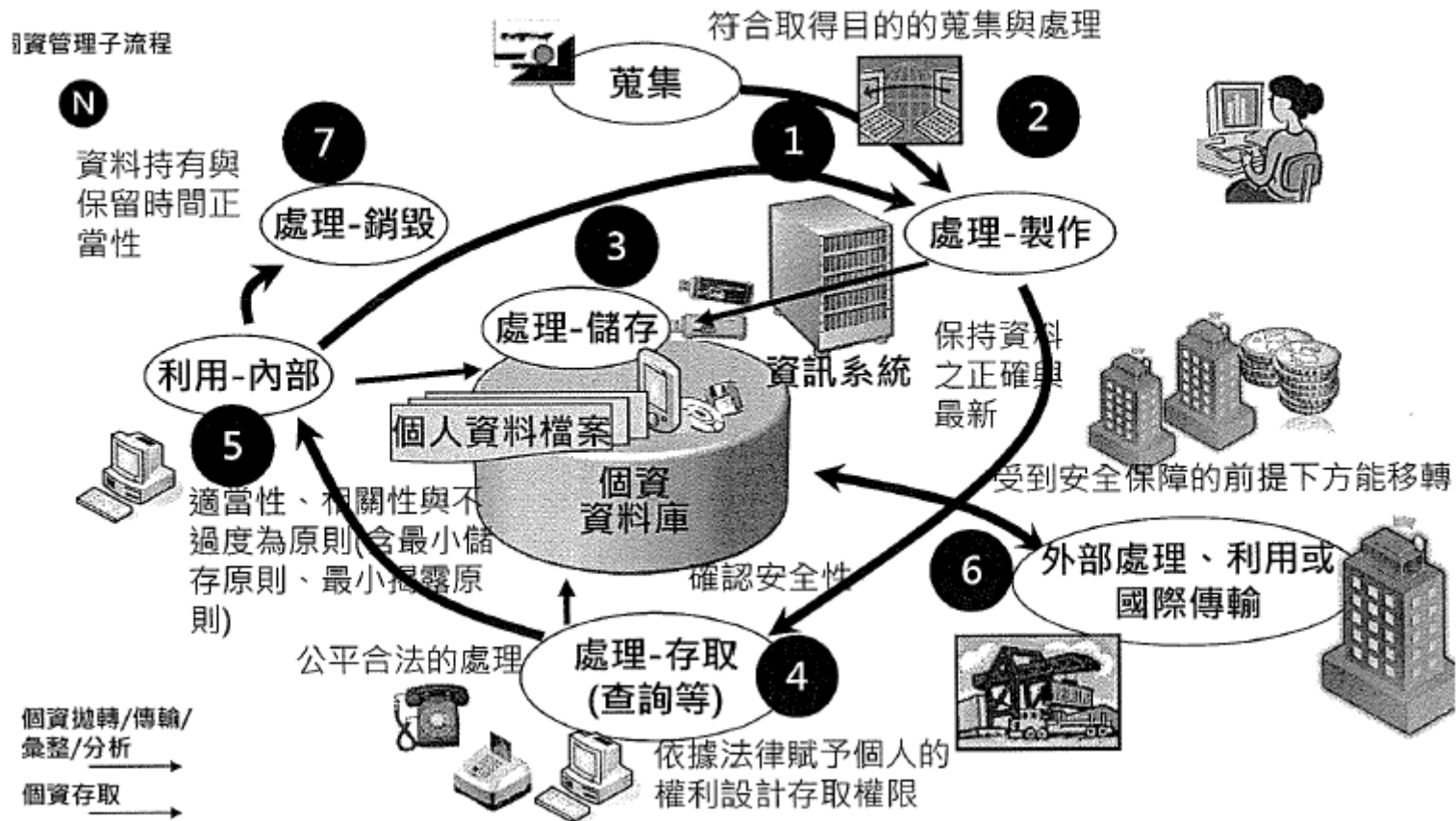


每**2** 家公司，就有 **1** 家曾遺失 **USB 硬碟** 上的資料

Source: Symantec統計

# 個資生命週期

## 個資生命週期與國際隱私保護原則



# 個人資料保護法



參考JIS Q 15001:2006制定，共六章 56條

- ▶ 第一章 總則
- ▶ 第二章 公務機關對個人資料之蒐集、處理、利用
- ▶ 第三章 非公務機關對個人資料之蒐集、處理、利用
- ▶ 第四章 損害賠償及團體訴訟
- ▶ 第五章 罰則
  - 罰款：個人500~2萬；企業上限2億
  - 坐牢：圖利個人可罰5年以下有期徒刑；修改資料造成他人損害。
- ▶ 第六章 附則

# 實施時程

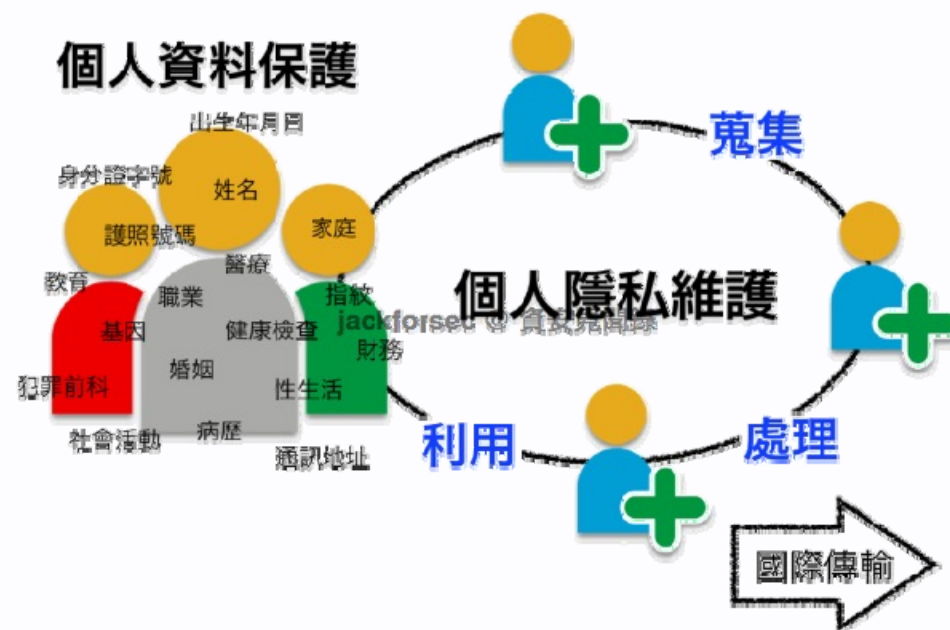


- §56：施行日期由行政院定之。
- §55：施行細則由法務部定之。
- 預計進度：
- 法務部計畫於2011/06完成施行細則並呈報行政院審核，預計11/25審核完。
- 行政院將視情況召開會議決定爭議處，而後才公告施行細則正式版本，並同時公布法案正式施行日期。



## §2：管轄行為

- 蒐集：以任何方式取得個人資料。
- 處理：為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送
- 利用：將蒐集之個人資料為處理以外之使用



# 個人資料定義



個人的姓名

出生年月日

身分證統一編號

護照號碼

特徵

指紋

婚姻

家庭

教育

職業

病歷

醫療

基因

性生活


健康檢查

犯罪前科

聯絡方式

財務情況

社會活動

姓名: 父母取的	性别: 天生的	年龄: 不大
身高: 不高	体重: 不肥	生日: 还没到
居住地: 家里	电子邮箱: 朋友帮申请的	
联系方式: 喊我	电话: 摩托罗拉的	
兴趣: 广泛		
曾经受过何种形式的嘉奖: 大家都说我像奥特曼。		
个人经历: 刚才上了厕所		
父母姓名: 爸爸妈妈		
父母联系方式: 打电话 		

不愿透露详细资料的学生 [www.sina.com.cn/lengxiaohua](http://www.sina.com.cn/lengxiaohua)

可直接或間接識別人的資料

# 12點施行細則的制定方向



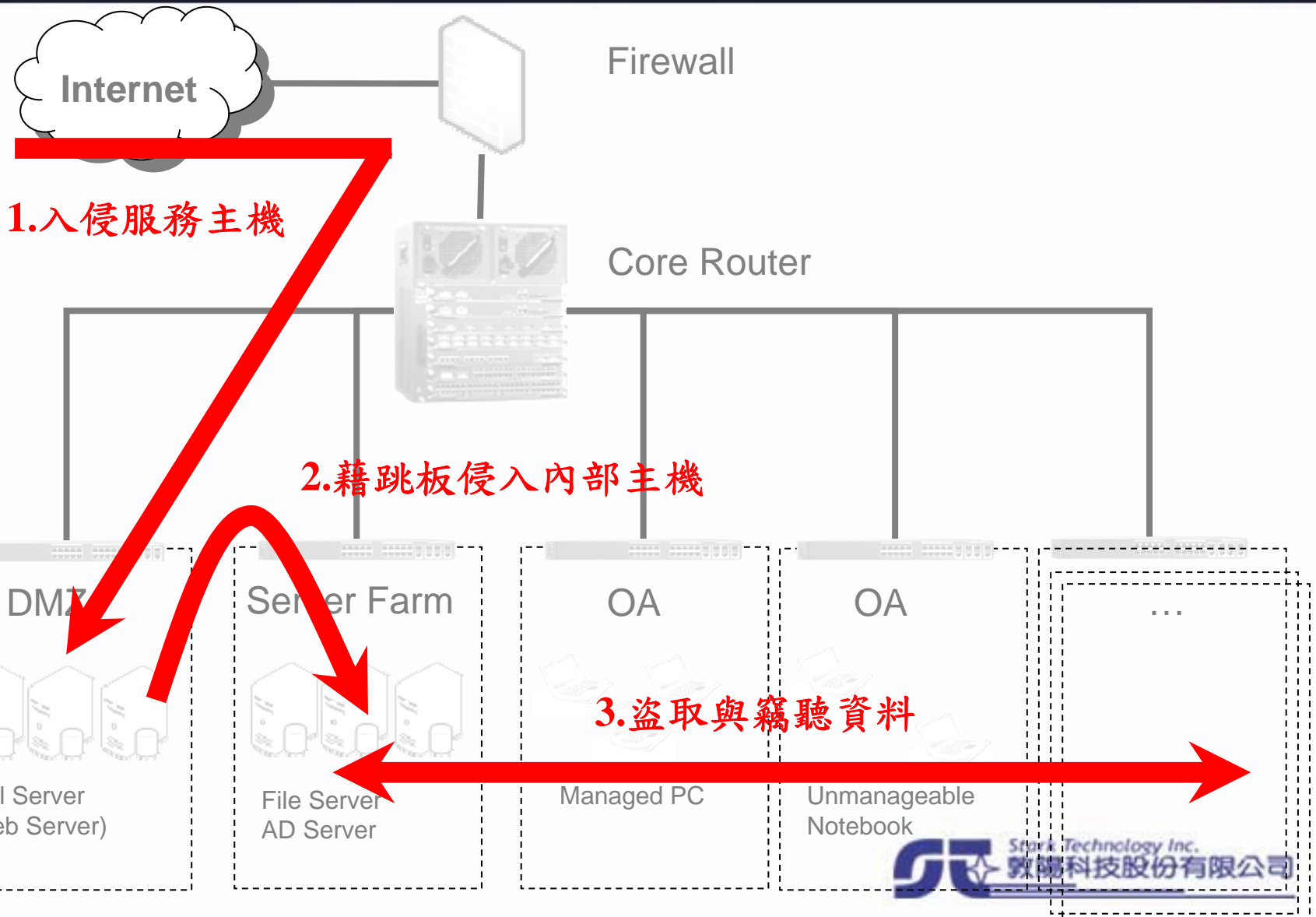
- (1) 必要之組織
- (2) 界定個人資料範圍
  
- (3) 個人資料蒐集、處理或利用之程序
- (4) 當事人行使權利之處理程序
  
- (5) 資料安全
- (6) 資料稽核
- (7) 人員管理及教育訓練
- (8) 記錄與證據之保存
- (9) 設備管理
  
- (10) 緊急應變措施及通報
- (11) 改善建議措施
- (12) 其他安全維護事項

# 因應方案



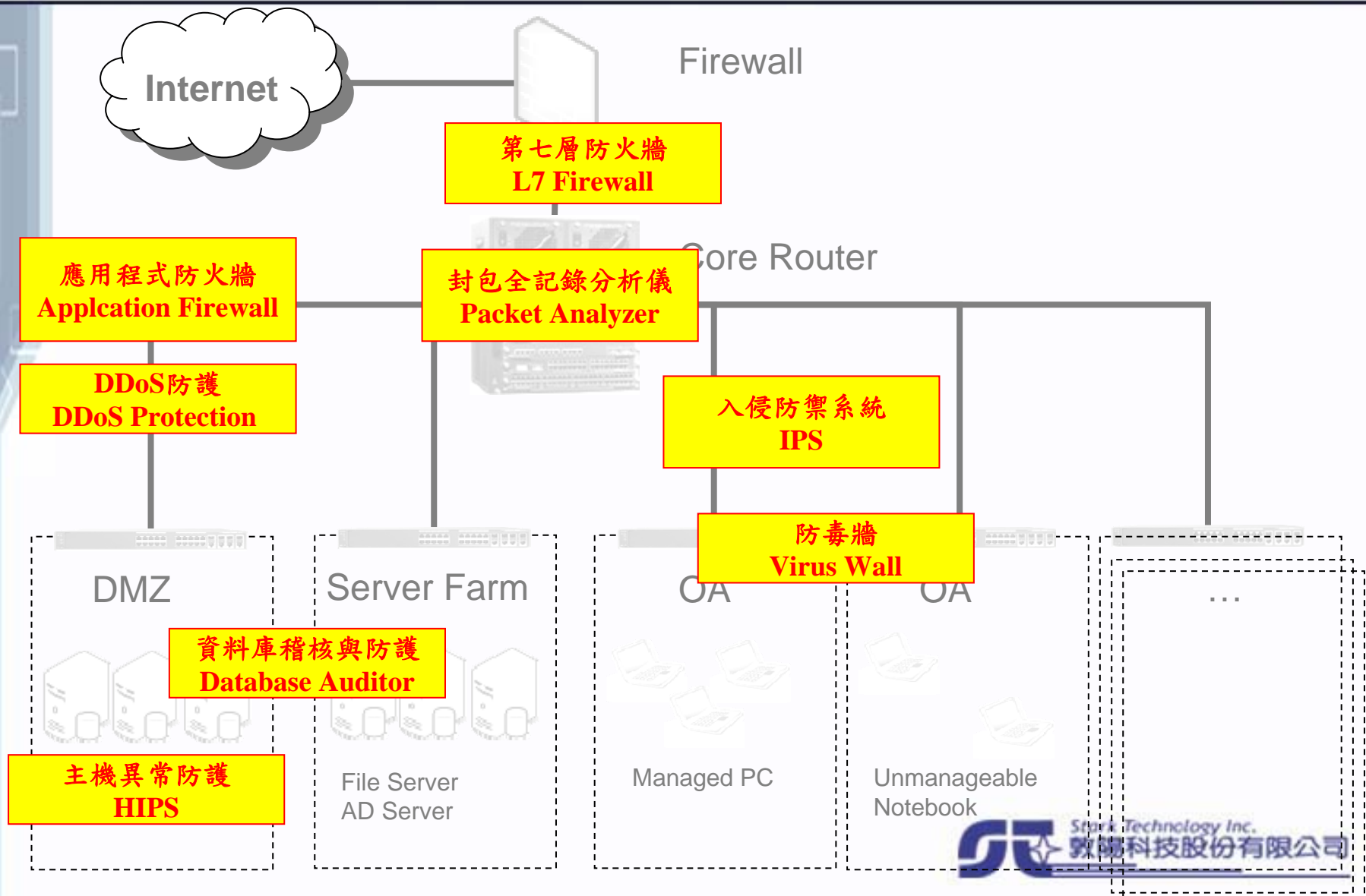
- 決定專人小組
- 決定公務上需要的個資種類與用途
- 盤點現有的個資數量及必要性
  - ▶ 員工資料
  - ▶ 民眾資料/客戶資料
  - ▶ 單位機密
  
- 制定蒐集、處理與利用政策
- 制定保管與銷毀政策
- 制定變更要求處理政策
- 制定稽核與監控機制
  
- 環境建置
- 政策執行

# 資訊外洩管道(1) - 駭客攻擊

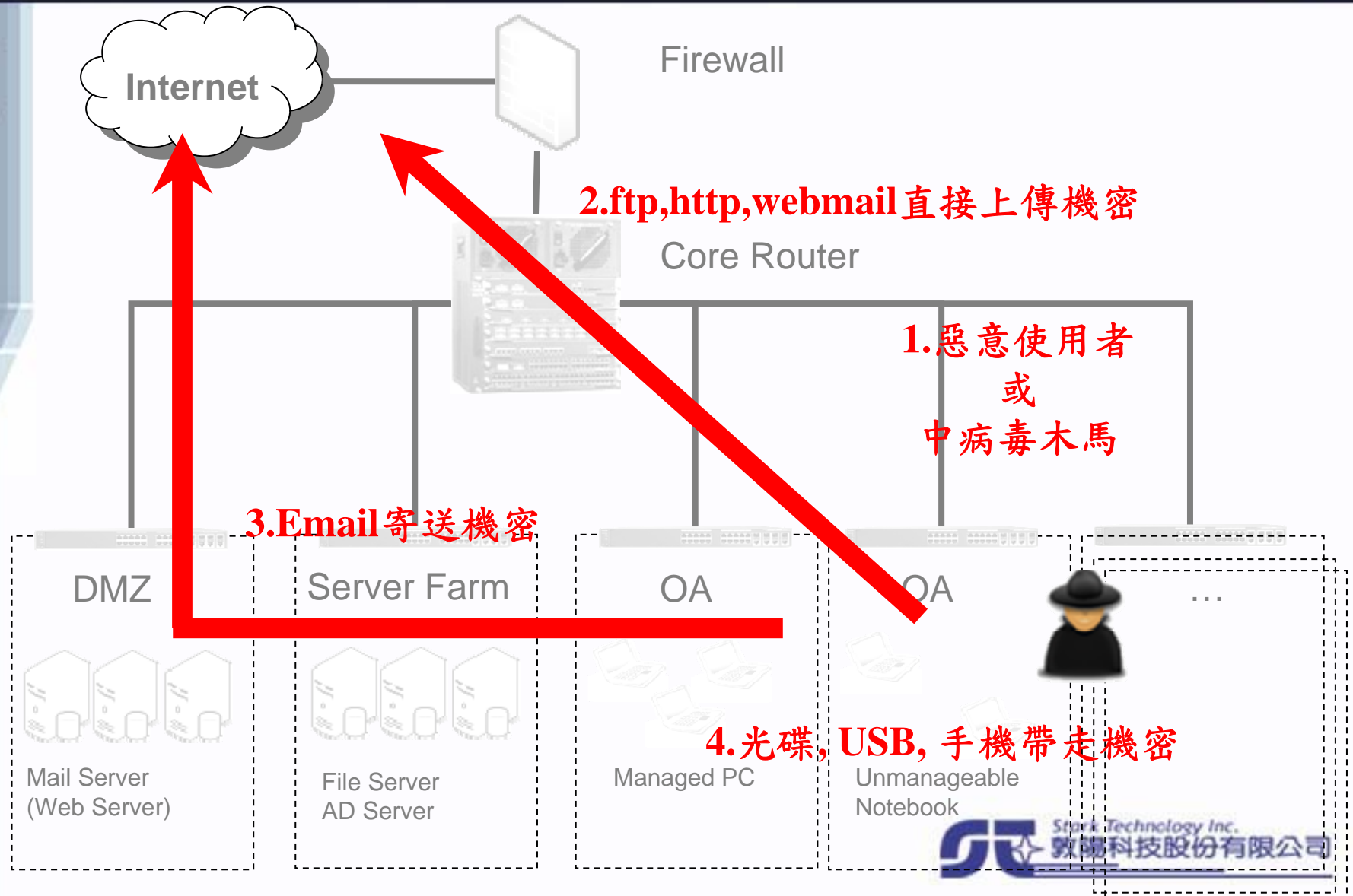


# 駭客攻擊—各種不同防護方式

視組織架構與作業需求選擇



# 資訊外洩管道(2) - 內部上傳



# 遠端偷渡管道



- FTP
- 網路硬碟空間
- 網路芳鄰
- 遠端操作
  - ▶ Windows 遠端桌面, PCAnywhere, VNC
- 即時通訊
  - ▶ MSN, Skype, QQ
- P2P
  - ▶ FOXY、BitComet、eDonkey



# Web MSN



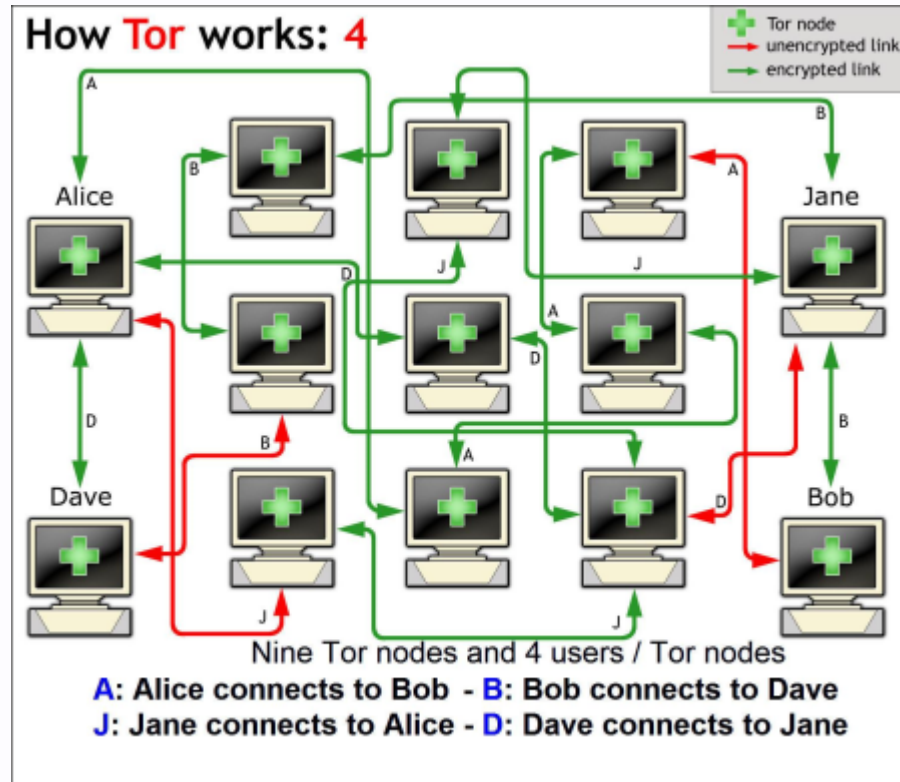
The screenshot displays the MSN Messenger web interface in a browser window. The main chat area shows a conversation with 'Robbie在Linux下工作'. The contact list on the right includes 'Guo Yu with prying eyes', 'Jasper(超魅)', 'Jeffrey', 'Keren Tan', 'Susy:凤凰台上凤凰游, 凤去台空江自流', 'zhangdf\_ya@yahoo.com.cn', '刘子行 (离开)', '啥也不想 (忙碌)', '坚--Rain Stops (离开)', and '有组织,无纪律..'. The system tray at the bottom shows the time as 18:07 on 2005-07-12.

# 無界瀏覽 UltraSurf



幫助IE自動尋找美國的代理伺服器(Proxy)

# 洋蔥路由 - 剝掉一個又一個

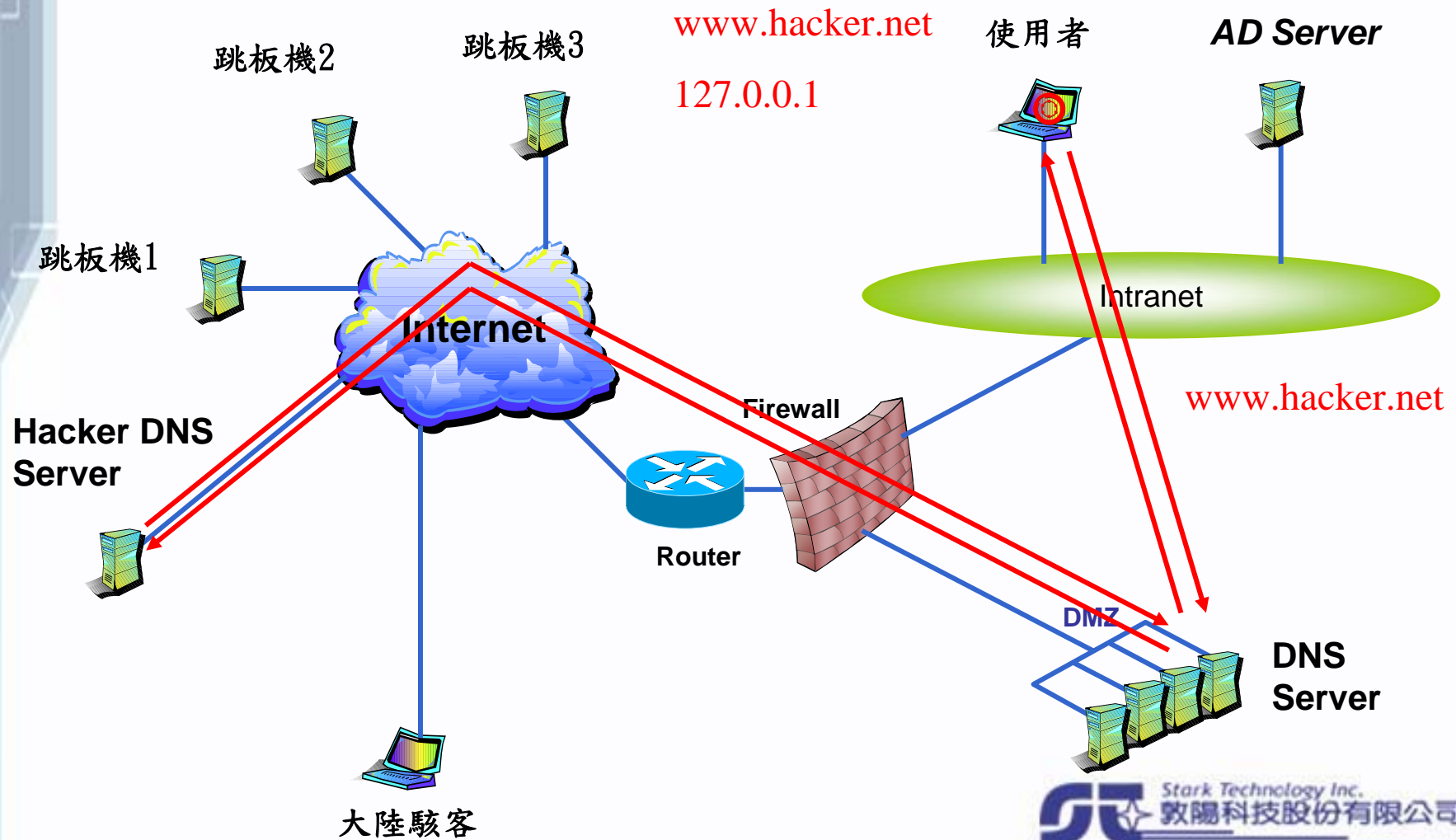


- 利用P2P概念傳遞
- 2010年6月，中國長城終於成功封鎖

# 反向式木馬案例

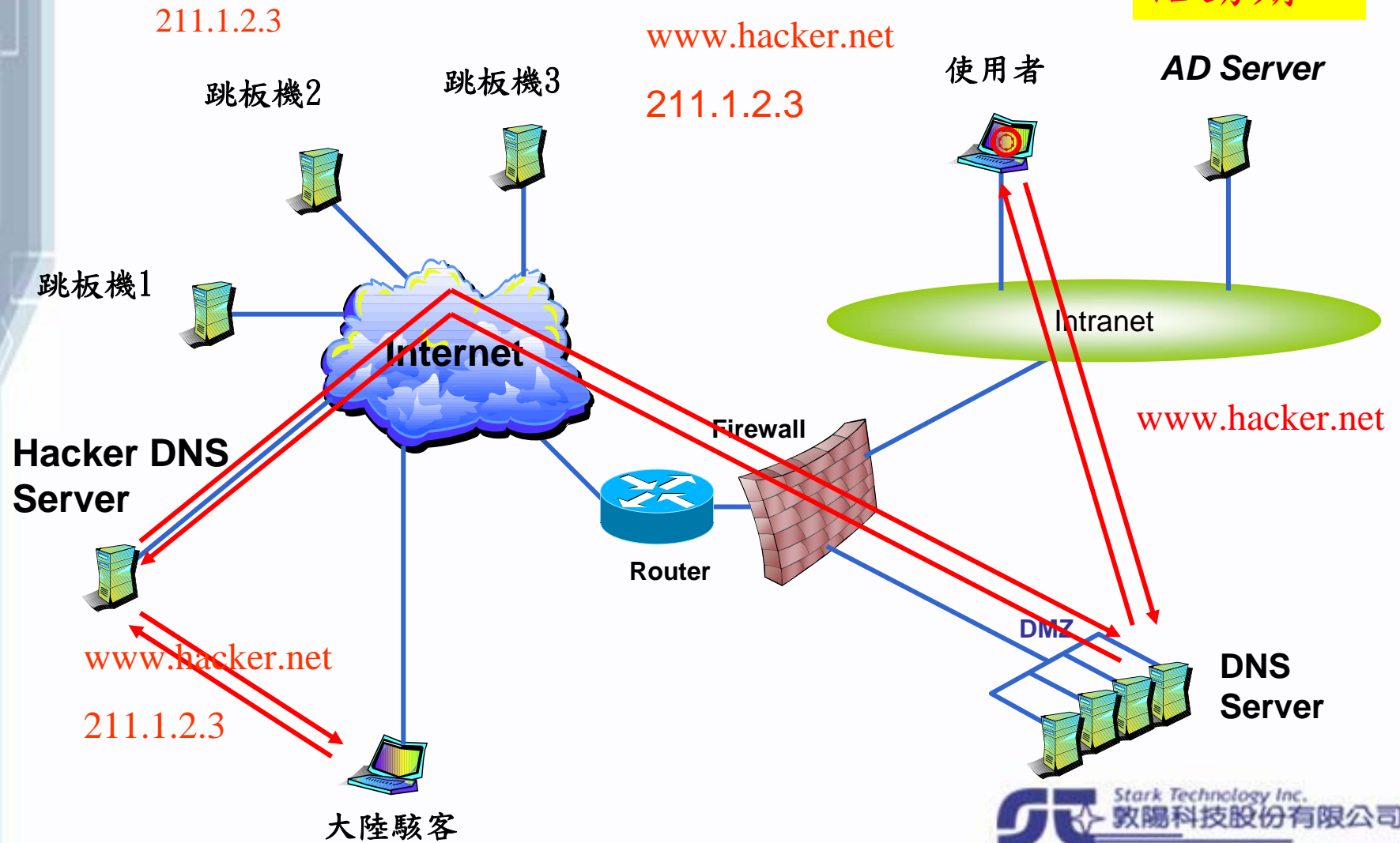


潛伏期



# 反向式木馬案例(續)

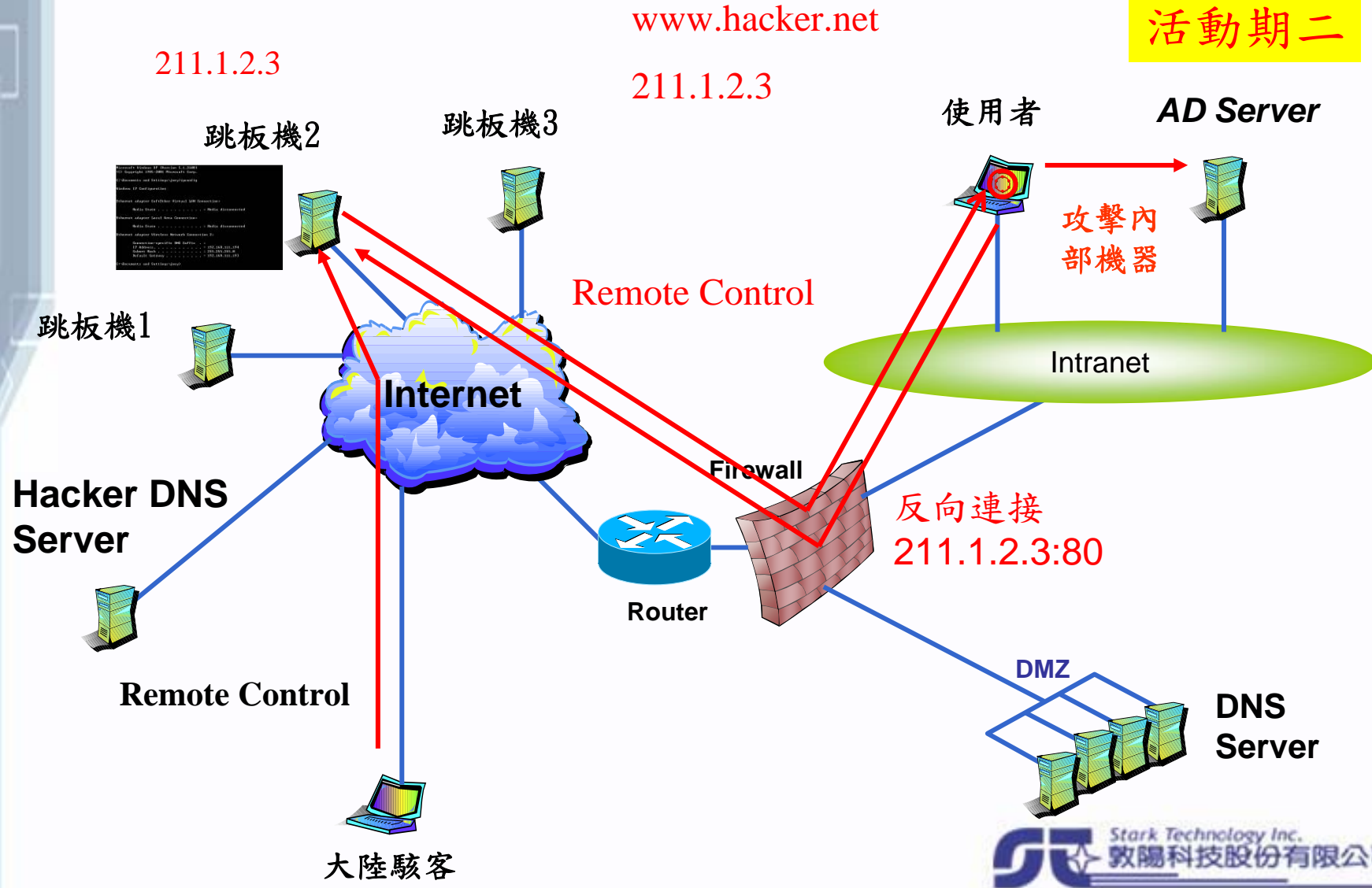
活動期一



# 反向式木馬案例(續)



活動期二



# 系統面強化



- 帳號密碼政策
- 使用者權限設定
- 服務狀態設定
- 本機安全性規則
- 本機稽核規則 - 物件稽核
- 外接式設備管制
- 安全修補程式
- 主機端安全防護軟體
- 第三方軟體管制/資產管理

# 系統面防護



- 本機稽核
- DRM
  - ▶ 以文件為主的存取控管
- DLP
  - ▶ 以內容為主的偵測
- EndPoint
  - ▶ 以行為為主的限制



# DRM數位版權管理解決方案



文件管理者/政策制定者

- 編輯文件
- 制定文件
- 加密



上傳使用政策



- 1.身份確認
- 2.下載金鑰



文件可儲存在網站伺服器、檔案伺服器、光碟、磁片，或者以e-mail方式傳送

# DRM保護目標



- 針對MS Office、PDF、AutoCAD、Pro/E等格式文件達到：
  - ▶ 受保護的文件不影響原本應用軟體的操作功能  
(依據權限政策來限制行為)
  - ▶ 控制文件的存取對像
  - ▶ 防止文件被不當散佈給未授權人員
  - ▶ 禁止文件或部份內容被任意列印
  - ▶ 無法透過複製/貼上或者螢幕截取功能取得內容
  - ▶ 授權列印功能時加註浮水印證明來源(法律追究依據)
  - ▶ 隨時可以撤回文件或變更有效時間
  - ▶ 完整追蹤稽核文件的活動歷程

# DRM政策



- 線上閱讀
- 鎖定特定電腦才能閱讀
- 強制設定有效閱讀期限
- 浮水印
- 限制可採取的動作
  - ▶ 複製
  - ▶ 列印
  - ▶ 修改
  - ▶ ...
- 記錄完整動作流程並回傳
  - ▶ 違規複製

# DRM-3A原則驗證



- 認證 Authentication ( Access Control )
  - ▶ 加密保護文件標準(RSA,AES,...)
  - ▶ 結合 Microsoft AD、PKI、指紋辨識..等系統加強認證
- 授權 Authorization
  - ▶ 複製、列印、修改
  - ▶ 閱讀有效期間
  - ▶ 防 PrintScreen、ScreenCapture
  - ▶ 鎖定在特定電腦才能閱讀
  - ▶ \* 照相較難預防
- 稽核 Auditing
  - ▶ 管理者行為, 使用者行為
  - ▶ 連線閱讀, 離線閱讀

# DLP



- 資料防洩(Data Leakage Protection)
  - ▶ 著重資安三原則中的機密性原則
  - ▶ 預防與稽核機密資料洩露
  - ▶ 偏向資訊安全類產品
- 資料防失(Data Loss Prevention)
  - ▶ 著重資安三原則中的完整性原則
  - ▶ 預警及避免資料損毀
  - ▶ 偏向備援儲存類產品
- 市場趨勢：
  - ▶ 採用後者為品牌名，實作前者功能

# DLP – 管理目標



## 防護上網安全風險

- 間諜軟體 (Spyware)
- 惡意網站病毒 (Malicious Mobile Code)
- 釣魚詐欺 (Phishing Attack)
- 鍵盤側錄攻擊(Key-logger)

## 控管網路資源濫用

- 與工作無關的網頁瀏覽
- 頻寬的誤用：
  - 網路影音傳媒 (Web TV, Youtube)
  - 網路收音機 (Internet radio)
  - 網路磁碟(Web HDD)
  - 網路相簿(無名小站, Myspace)

## 非法的資料傳遞管制

- 即時通訊 (Instant Messaging)
- P2P傳輸 (Peer-to-peer file sharing)
- Tunnel 通道

## 資訊外洩管道的管制

- 透過網路閘道的機密資料外洩
- 不當的網路行為
- Web Mail、Web 2.0 資料外洩

# DLP – 文件內容指定

製作內容特徵

研發部門機密文件:



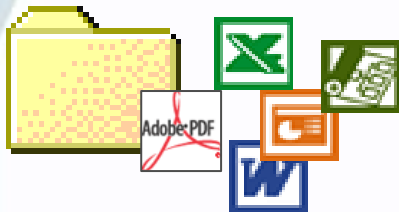
```
01011100
11010011
00001011
00 100100
1000111
01110101
01101011
0110011
0111101
```

```
0xB6751
0xB61C1
0x37CB2
0x5BD41
0x190C1
0x93005
0x590A9
0xA0001
```

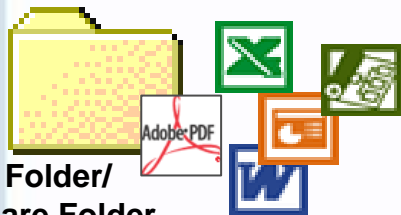
萃取本文  
轉換為特徵

儲存為指紋  
與索引

行銷計畫:



人資紀錄:



Folder/  
Share Folder  
with Documents

Properties Forensics History

Details: FW: Here is the spec(WS規格)

Source: @ms1.hinet.net Incidents by this Source

Destination: @ms1.hinet.net

Violated Policies

- Confidential/WS\_規格機密文件 (PreciseID File Fingerprints) 100% Detection  
\\CPSMANAGER\c\$\temp\test\_docu\LearnSource\WS\_Spec\_3.doc

Email / SMTP 信  
件內容偵測

# DLP – 資料庫內容指定



PreciseID Record Fingerprints Policy Properties

Sample Data | Policy Rules | Schedule | Channels | Authorization | Actions

General | Database | Table Name | Incremental Fingerprinting | Validation Script

From Table/View: "CrystalDIY"."dbo"."C\_Member"

Select:  All Fields  
 Specific fields:

Display Name	Database Field Name
<input type="checkbox"/> member_id	"member_id"
<input checked="" type="checkbox"/> email	"email"
<input checked="" type="checkbox"/> password	"password"
<input checked="" type="checkbox"/> name	"name"
<input checked="" type="checkbox"/> name_alias	"name_alias"

Where:

SQL Query:

1. 選擇哪些欄位要  
納入特徵中。

PreciseID Record Fingerprints Policy Properties

General | Database | Table Name | Incremental Fingerprinting | Validation Script

Sample Data | Policy Rules | Schedule | Channels | Authorization | Actions

Rule	Dictionary	Dictionary Fi...	Threshold
"gift_id"			20
"email" and "password"			3
"email" and "name"			5
"name" and "name_alias" an...			7
"name" and "tel_home" and "..."			4

Add... Edit... Delete

Note: The policy will be triggered if at least one of the rules is matched.

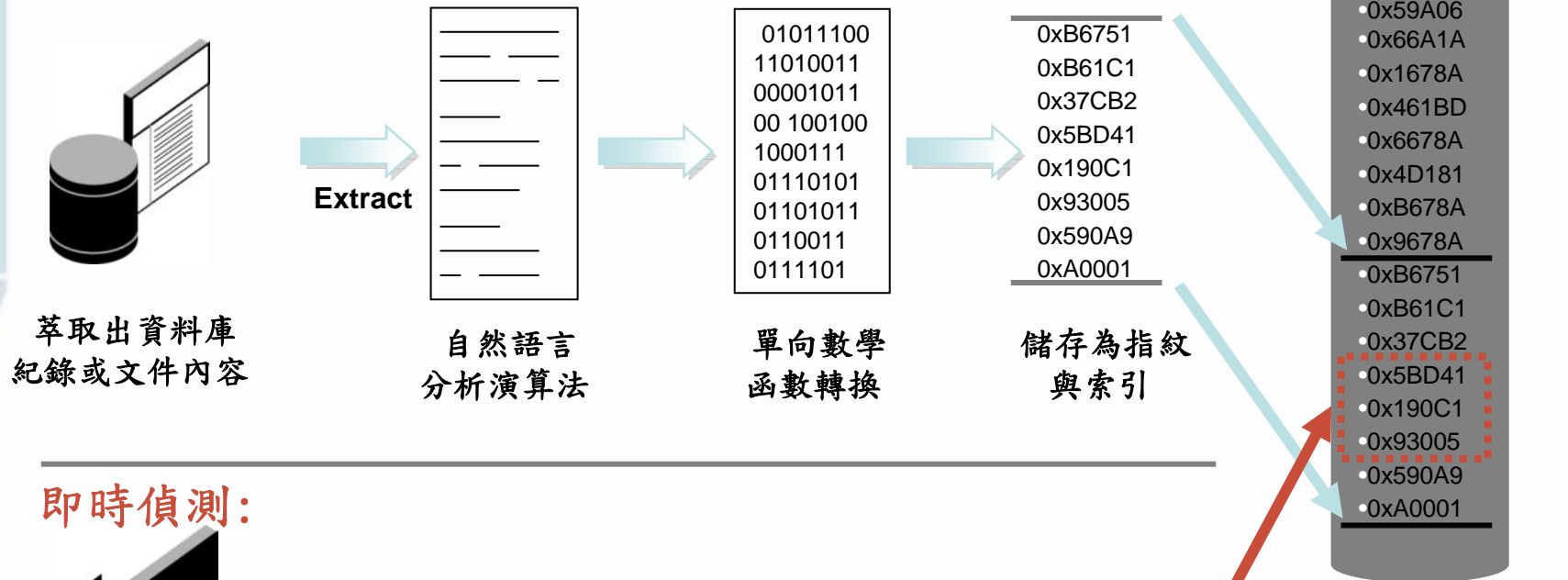
2. 制定比對規則。



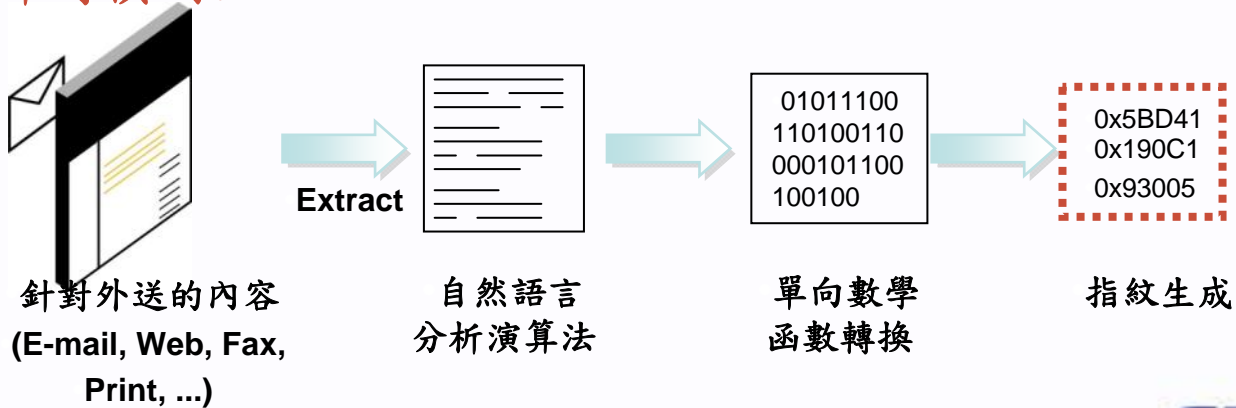
# DLP – 指紋製作與比對



## 指紋建立作業:



## 即時偵測:



# DLP – 上網內容偵測



Gmail - 撰寫郵件 - lambert.lin@gmail.com - Windows Internet Explorer

http://mail.google.com/mail/?shva=1#compose

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

Gmail 撰寫郵件 - lambert.lin@gmail.com

搜尋郵件 搜尋網頁 顯示搜尋選項 建立篩選器

撰寫郵件

傳送 立即儲存 捨棄 草稿自動儲存於 下午1:58 (1分鐘以前)

收件者: test@docutek.com.tw

新增副本 | 新增密件副本

主旨: 客戶個資於內容與附件

附加檔案

B I U F T T « 純文字 檢查拼字 »

林 彰化市 -2號  
曾 復興北  
陳 桃園市 2-1號13樓之一  
鄭 內湖區  
傅 內湖區  
李 林森北  
蔡 楊梅鎮  
邱 中山區 樓  
白 大里市  
金 健康路  
呂 台南市 59號

1. 依據內容進行研判
2. 敏感資料於郵件內容區，可被偵測
3. HTTP / HTTPS / FTP

# DLP – 上網內容偵測



張貼到部落格、網路  
硬碟與討論區，均  
可檢查內容

Network & Endpoint

Assign... Release... More Actions Filter Favorites

Filter: Default Filter Number of Filtered Incidents: 174

ID	Date & Time	Source	Policy Categories	Channel	Destination	Severity	Action	Count	Size
135348	17 Mar. 2009, 02:31:03 PM		電話號碼測試	HTTP	na...	Moderate	Audited	1	103 B
135342	17 Mar. 2009, 02:28:35 PM	...@docutek.com.tw	電話號碼測試	SMTP	3!	Moderate	Notified, Audited	2	
135331	17 Mar. 2009, 02:28:21 PM		電話號碼測試	HTTP	mail.google.com	Serious	Notified, Audited	3	10 KB
135320	17 Mar. 2009, 02:28:08 PM		電話號碼測試	HTTP	mail.google.com	Serious	Notified, Audited	3	10 KB
135203	17 Mar. 2009, 02:27:25 PM		Credit Cards; FCRA; ...	HTTP	mail.google.com	Critical	Notified, Audited	34	38 KB
135198	17 Mar. 2009, 02:21:10 PM	maggie@docutek.com.tw	Aaron Lab Test	SMTP	cch...	Moderate	Notified, Audited	1	558 KB

Properties Forensics History

Attachments

Customer Records.xls

檔案以真實格式識別  
，避免使用者改檔  
規避偵測

Gmail by Google BETA

搜尋郵件 搜尋網頁

撰寫郵件

傳送 立即儲存 捨棄 草稿自動儲存於 下午2:01 (26分鐘以前)

收件者: test@docutek.com.tw

新增副本 | 新增密件副本

主旨: 客戶個資於內容與附件

Customer Records.xls 38.00K  
Customer Records2.xls 38.00K 取消

附加其他檔案

B I U F rT T

# DLP – 隨身碟複製機密文件



Assign... Release... More Actions

20966

**Properties** Forensics History

**Details:** File copied: "C:\temp\WS\_Spec\_2.doc" to removable device

**Source:** LAMBERT-NB\ Lambert

**Destination:** USB 2.0 Flash Disk

**敏感內容 / 產品管理部門\_機密文件 (PreciseID Document Fingerprints)**

Run As User:	LAMBERT-NB\ Lambert
<b>File Details</b>	
File Name:	C:\temp\WS_Spec_2.doc - 26 KB
Attachment Size:	26 KB in total
<b>Endpoint Details</b>	
Endpoint Type:	Desktop
Application Name:	EXPLORER.EXE
Device Name:	USB 2.0 Flash Disk
Device Type:	Removable Device
Policy Version:	42

# DLP – 剪貼簿偵測



Assign... Release... More Actions... Filter... Favorites...

Filter: Brian

ID	Date & Time	Source
10000	12 Aug. 2008, 08:42:49 AM	DSS-Client
10049	12 Aug. 2008, 08:58:02 AM	DSS-Client
10092	12 Aug. 2008, 09:30:22 AM	DSS-Client
10145	12 Aug. 2008, 09:31:05 AM	DSS-Client
10152	12 Aug. 2008, 09:37:03 AM	DSS-Client
10470	12 Aug. 2008, 04:52:47 PM	DSS-Client
10181	12 Aug. 2008, 11:15:56 AM	jlondon@ilpdemo.co
10185	12 Aug. 2008, 11:17:06 AM	jlondon@ilpdemo.co
10191	12 Aug. 2008, 11:17:55 AM	jlondon@ilpdemo.co
10197	12 Aug. 2008, 11:17:56 AM	jlondon@ilpdemo.co
10203	12 Aug. 2008, 11:17:56 AM	jlondon@ilpdemo.co
10209	12 Aug. 2008, 11:17:56 AM	jlondon@ilpdemo.co

**Incident Details** ID: 10000

Status: New  
Urgency: Moderate  
Detected by: Endpoint Agent  
Local Date Detected: 12 Aug. 2008, 08:42:52 AM GMT-0700  
Analyzed by: Endpoint Server DSSManager  
Action: Audited  
Assigned to: Unassigned  
Channel: Endpoint Applications ( Paste )  
Protocol: File  
Incident Tag: N/A  
Date & Time: 12 Aug. 2008, 8:42:49 AM

**Source Details**

Full Name: DSS-CLIENT\Administrator  
Username: DSS-CLIENT\Administrator  
Hostname: DSS-Client  
Run As User: DSS-CLIENT\Administrator

**File Details**

File Name: EndpointData.txt - 794 B

**Properties** Forensics

**Details:** Content pasted from applicati  
**Source:** DSS-Client Incidents by

**Violated Policies**

- PCI/PCI: Credit-Card Numbers ...** (P  
3023xxxxxx7549, 5231xxxxxxx4309,
- FCRA/FCRA: CCN: All Credit Car...** (P  
6011xxxxxxx7529, 3670xxxxxx7456,

# Endpoint - 對應用程式的存取控制



**Applications > Add Application**

Define a new application, select an existing one or select a group of applications from the list:

**Application Selection**

Application Group IM **支援應用程式分類**

Single Application --- Select File ---

**Operation Selection**

Apply the following settings:

Print	Allow Operation	<b>印表 剪下、複製 貼上 檔案存取 畫面抓圖</b>
Cut/Copy	Allow Operation	
Paste	Apply Content Policies	
File Access	Apply Content Policies	
Screen Capture	Allow Operation	

**Application Group** --- Select Group ---

**Operation Selection**

Apply the following settings:

Print	Block
Cut/Copy	Allow
Paste	Apply
File Access	Apply
Screen Capture	Allow

Collaboration  
**Instant Messaging**  
P2P File Sharing  
Telephony, Conferencing, ...  
Web Browsers  
CRM  
Data Warehousing, Analyti..  
Contact Managers  
ERP, SCM  
Word Processing  
Spreadsheets  
Project Managers  
Email  
Database  
Presentation

Name	Location Based Enforcem
<input type="checkbox"/> IM	Always
<input type="checkbox"/> Email	Always
<input type="checkbox"/> Default NOT Connected	NOT Connected
<input type="checkbox"/> Default Connected	Connected

# Endpoint - 資產盤點清單與狀態



The screenshot displays the Endpoint Manager interface. On the left, a table lists endpoints. The main area shows detailed information for the selected endpoint 'template-ab', categorized into Data Discovery, Host Details, Profile & Policy, and System Summary.

Hostname	IP Address	Location
<input type="checkbox"/> DSS-Client	192.168.88.130	Address
<input checked="" type="checkbox"/> template-ab	192.168.88.130	Address

**Data Discovery**

- Last Discovery Start Time:
- Last Discovery End Time:
- Discovery Scanned Files: 0
- Discovery Status: Idle
- Next Discovery Scan:

**Host Details**

- Hostname: template-ab
- IP Address: 192.168.88.130
- Logged-in Users: a
- Client Installation Version: 7.0.0.42
- Endpoint Server: DSSManager

**Profile & Policy**

- Synced: ✗
- Profile Name: Default
- Client Status: ✔ Enabled
- Last Profile Update: 19 Aug. 2008, 11:32:59 PM GMT+0700
- Last Policy Update: 19 Aug. 2008, 11:32:53 PM GMT+0700
- Profile Version: 2
- Policy Version: 0
- Active Profile Services:

**System Summary**

- OS Name: Windows XP
- OS Version: 5.1
- CPU: Intel(R) Core(TM)2 Duo CPU T7700 @ 2
- Total Physical Memory: 539 MB
- Type: WorkStation
- MAC Address: 00-0C-29-F9-9B-7D

# Endpoint – 硬碟文件探勘與盤點



Configuration > Endpoint Profiles > Endpoint Profile Properties

### Endpoint Profile: Default Profile

**General** | **Services** | **Servers** | **Properties**

The Services are the various applications, removable media and discovery tasks that can be restricted in the endpoint profile. For each Service to be restricted, select the service in the Services list and then configure the service properties in the right pane.

#### Services

- Applications
- Removable Media
- Discovery

#### Discovery

Enabled

**File Filter** | **Scheduler**

**Filter by Type**  
\* and ? can be used as wildcards

Include File Types:  
\*.xls; \*.potx; \*.xlsx; \*.xlsm;  
\*.ppam; \*.docm; \*.vbs; \*.ppt;  
\*.ppsm; \*.c; \*.rtf; \*.h; \*.pdf;  
\*.pptm; \*.dotm; \*.eps

Except:  
\*.jpg; \*.ima; \*.raw; \*.med;  
\*.png; \*.acr; \*.ico; \*.iw44;  
\*.pgm; \*.tcl; \*.avi; \*.window;  
\*.drv; \*.inx; \*.nlm; \*.mof; \*.erw;  
\*.aw; \*.hdr; \*.ani; \*

**Filter by Age**  
 Search only for files that are older than

**Filter by Size**  
 Discover All Files  
 Discover Specific Files  
 Only files larger than  
 Only files smaller than

#### Discovery

Enabled

**File Filter** | **Scheduler**

**Schedule Period**  
Start: 08/07/2008 at: 1:00 AM client time  
 Duration Limit: 60 Minutes

**Recurrence Pattern**

<input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly	<b>Options</b> Recur every day
---	-----------------------------------

No end date  
 End by: [calendar icon]

**Scan Type**  
 Differential Scan  
 Full scan every 10 scheduled scans  
 Full Scan



# Endpoint – 行為紀錄

## ● 員工行為紀錄

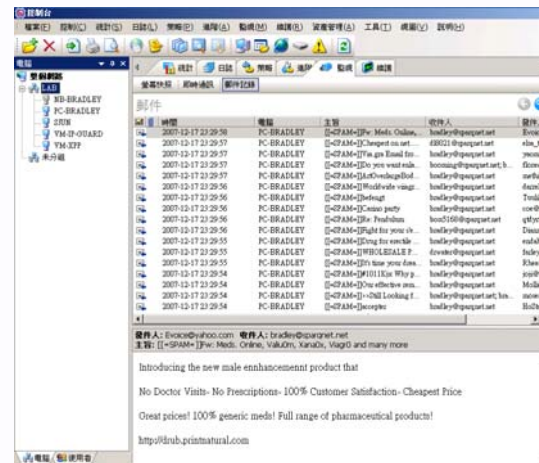
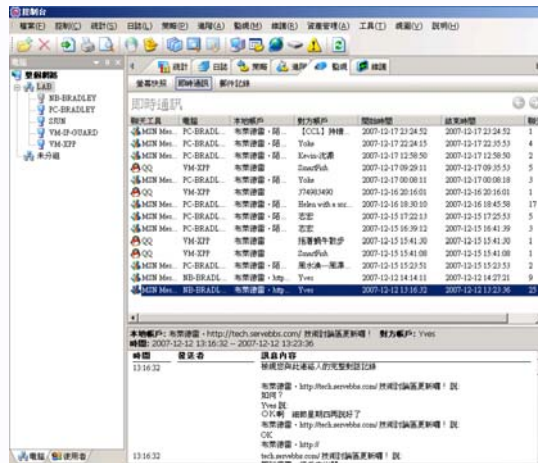
記錄員工在電腦上的各項操作，用於跟蹤及分析員工的工作行為。

## ● 郵件內容監控 (MS Exchange、Lotus Domino、一般郵件及 WebMail)

記錄員工收發的所有郵件內容及附件資料。

## ● 即時通訊監控 (MSN、Yahoo、Skype、QQ、ICQ、Popo、RTX、Sametime、TM、UC、阿里巴巴)

監控各類即時通訊軟體的聊天內容，及接收的文件檔案。



# Endpoint – 行為防止

## ● 防止透過隨身碟及網路芳鄰洩密

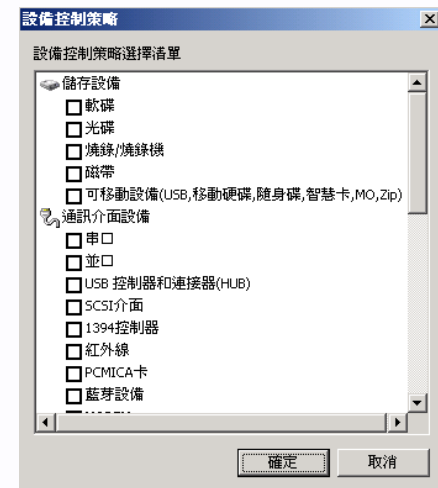
限定文件的讀寫權限，防止重要文件複製至隨身碟或共用資料夾內。

## ● 防止透過外接裝置洩密

禁用各種外接裝置 (如軟碟機、燒錄器、隨身碟、數據機(卡)、藍芽、紅外線...等裝置)，防止非法複製和傳送資料。

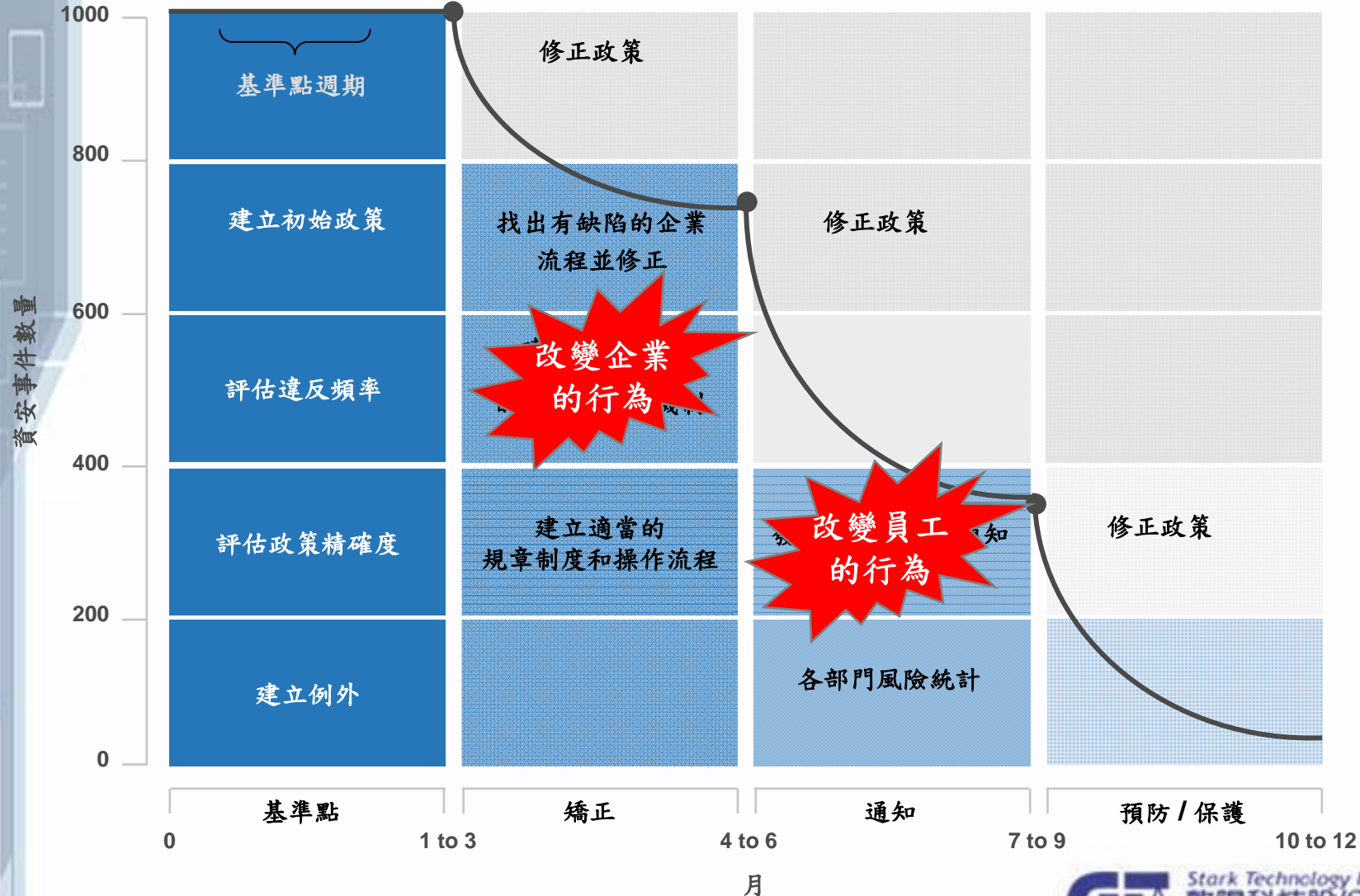
## ● 禁止外部電腦非法竊取企業機密

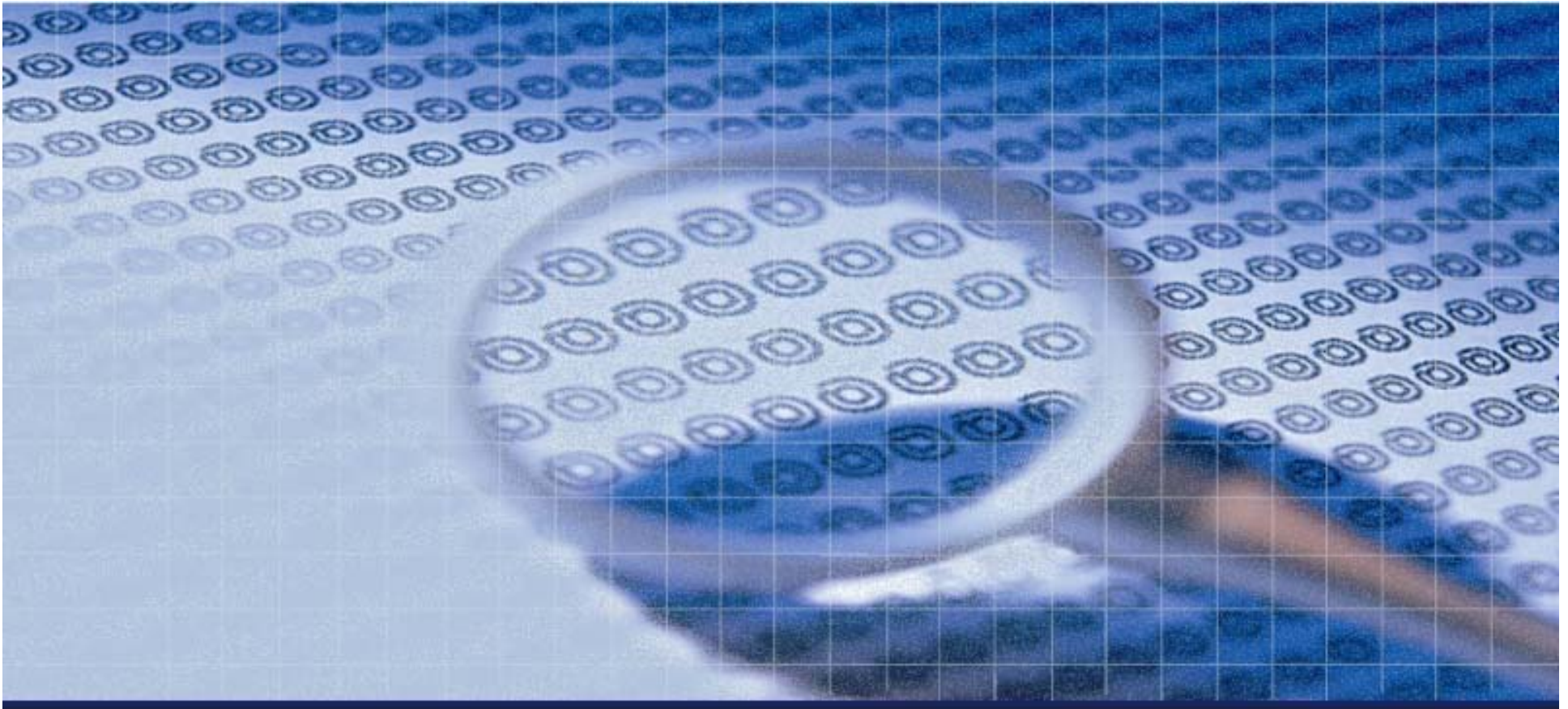
針對未經授權的外來電腦，即使接上內網，仍可禁止存取內部文件及各項服務，有效的杜絕外部電腦設備非法存取、複製企業重要資訊文件的可能性。



序號	狀態	電腦	網路位址	網路卡位址	類型	首次出現時間
1		VM-IP-GUARD	192.168.2...	00-0C-29-...	正常	2007-12-18 20:17:37
2		SUPPORT	192.168.2...	00-01-80-...		2007-12-18 20:17:19
3			192.168.2...	00-10-DE...	授權	2007-12-18 20:17:19
4			192.168.2...	00-30-48-...		2007-12-18 20:17:19
5		NB-BRADLEY	192.168.2...	00-16-D3-...	非法	2007-12-18 20:17:19
6			192.168.2...	00-30-48-...		2007-12-18 20:17:19
7			192.168.2...	00-10-DE...	保護	2007-12-18 20:17:19
8			192.168.2...	00-0D-60...		2007-12-18 20:17:19

# 主機控管完整流程





# 網路控制



# 網路封包稽核



- 側錄所有網路封包，以進行網路鑑識分析及效能監控
- 功能
  - ▶ 即時分析，找出異常行為與流量，並提出告警
  - ▶ 重組相關封包，還原事件真相
  - ▶ 找出資料外洩的過程及證據
- 目的
  - ▶ 網路狀況分析
  - ▶ 資安事件鑑識
  - ▶ 追蹤異常事件

# Packet SNIFFER

- >> 原始資料封包
- >> SNMP
- >> NetFlow
- >> Alarms (IDS)

連續性資料  
擷取

網路與資安分散式  
資料倉儲

**目標** > 如同網路攝影機架設於關鍵網路節點  
>> 進行封包擷取與分類並即時分析  
>> 整合性告警機制  
>> 簡而易懂之分析報表  
**效益** > 於事件發生第一時間定位問題根本，縮短問題查找所需時間，迅速恢復服務

資訊安全與內容監控

網路與服務效能分析

告警與  
第三方  
系統整合

- >> 資訊分類
- >> 資訊合法擷取
- >> 入侵偵測
- >> 安全監控
- >> 網路鑑識
- >> 政策遵循
- >> 異常流量偵測

- >> SNMP
- >> Syslogs
- >> 第三方 NMS 系統整合

- 效能優化 <<
- 趨勢分析 <<
- 容量規劃 <<
- 服務保證 <<
- 服務品質分析 <<
- 封包解譯與分析 <<
- RMON, 流量分析與告警 <<
- 整合性分析報表 <<
- VoIP分析(QoS) <<

# 還原網路行為

**Session Reconstruction - Microsoft Internet Explorer**

Address: <https://ext-demo.niksun.com/scratch/tepReassem/ycj72p5711/EMAIL/MAIL1/ichiro.ppt>

**Instant Messaging Reconstruction**

Chat Participants	Instant Message
buddyA	buddyA: test for NetDetector reconstruction
yplum2000	yplum2000: i have confidence that it will work
buddyA	buddyA: OK what are your plans for weekend

**Hotmail**

10.70.0.73<-->10.70.0.93

Date	Start
Aug 18	11
Aug 18	578
Aug 17	46
Aug 17	11
Aug 17	46
Aug 17	38
Aug 16	28
Aug 15	38
Aug 14	11
Aug 13	28
Aug 9	38

GET /cgi-bin/HotMail?combox=F00000001&a=b6148c0b3d52e049662244507652011 HTTP/1.0  
Referenc: http://lw14f4.lw14.betamil.asn.com/cgi-bin/tobase?combox=F00000001&a=b6148c0b3d52e049662244507652011&fri=yres&lang=EN  
Connection: Keep-Alive  
User-Agent: Mozilla/4.720-CCK-MCD Caldera Systems OpenLinux [en] (X11; U; Linux 2.2.14 i686)  
Host: lw14f4.lw14.betamil.asn.com

Attachments: [textfile1](#), [textfile2](#), [ichiro.ppt](#)

Unknown Zone

Stark Technology Inc. 敦陽科技股份有限公司

# 資料庫交易稽核



- 紀錄所有對資料庫的存取行為，以即時阻絕或供後續稽核
- 支援目前所有常見之資料庫系統
- 佈署模式
  - ▶ Mirror – 不影響網路架構下進行被動紀錄
  - ▶ In-Line – 在紀錄的同時亦可即時進行主動控管
- 目標 – 五W
  - ▶ 誰(Who)、透過什麼方式(What)、從哪裡(Where)、什麼時候(When)存取了資料庫，如何(hoW)避免？



# 資料庫稽核系統

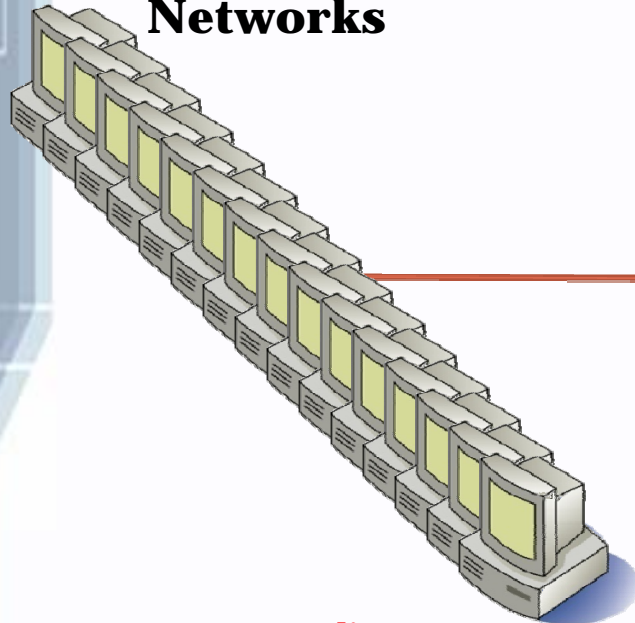


- 自動發現資料
- 漏洞及配置評估
- 加強保護
- 追蹤變化
- 資料庫活動監控
- 稽核
- 身份認證、存取控制和授權管理
- 加密

# 監控目標

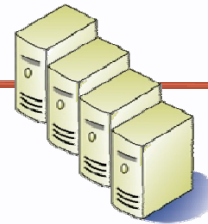
106

## Networks



**Client IP**  
**Client host name**  
OS User  
**MAC**  
TTL  
**Origin**  
Failed logins

## Applications



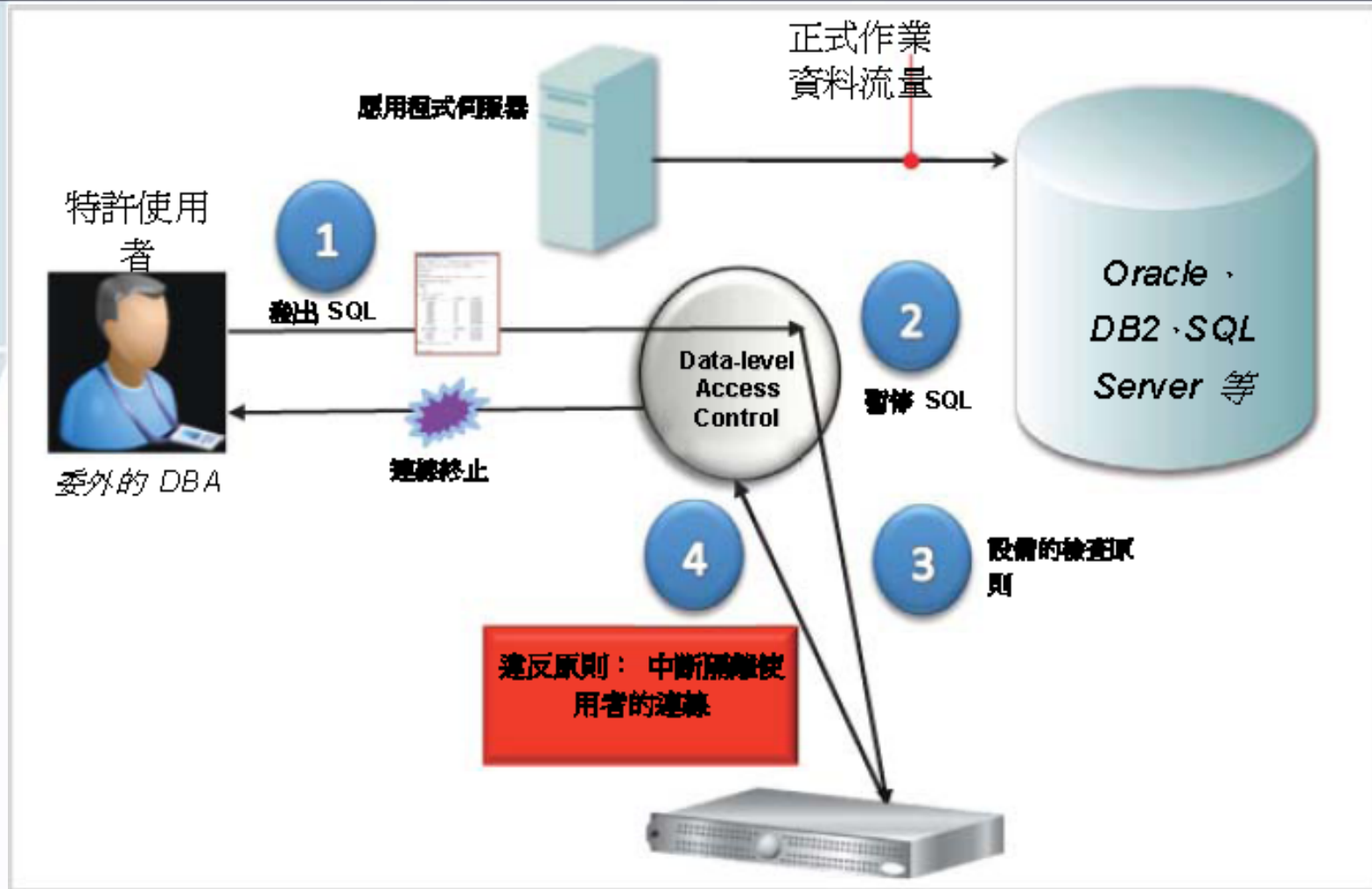
**Server IP**  
**Server port**  
Server name  
**Session**  
SQL patterns  
**Network protocol**  
Application User  
Timestamp  
Source programs

## Databases

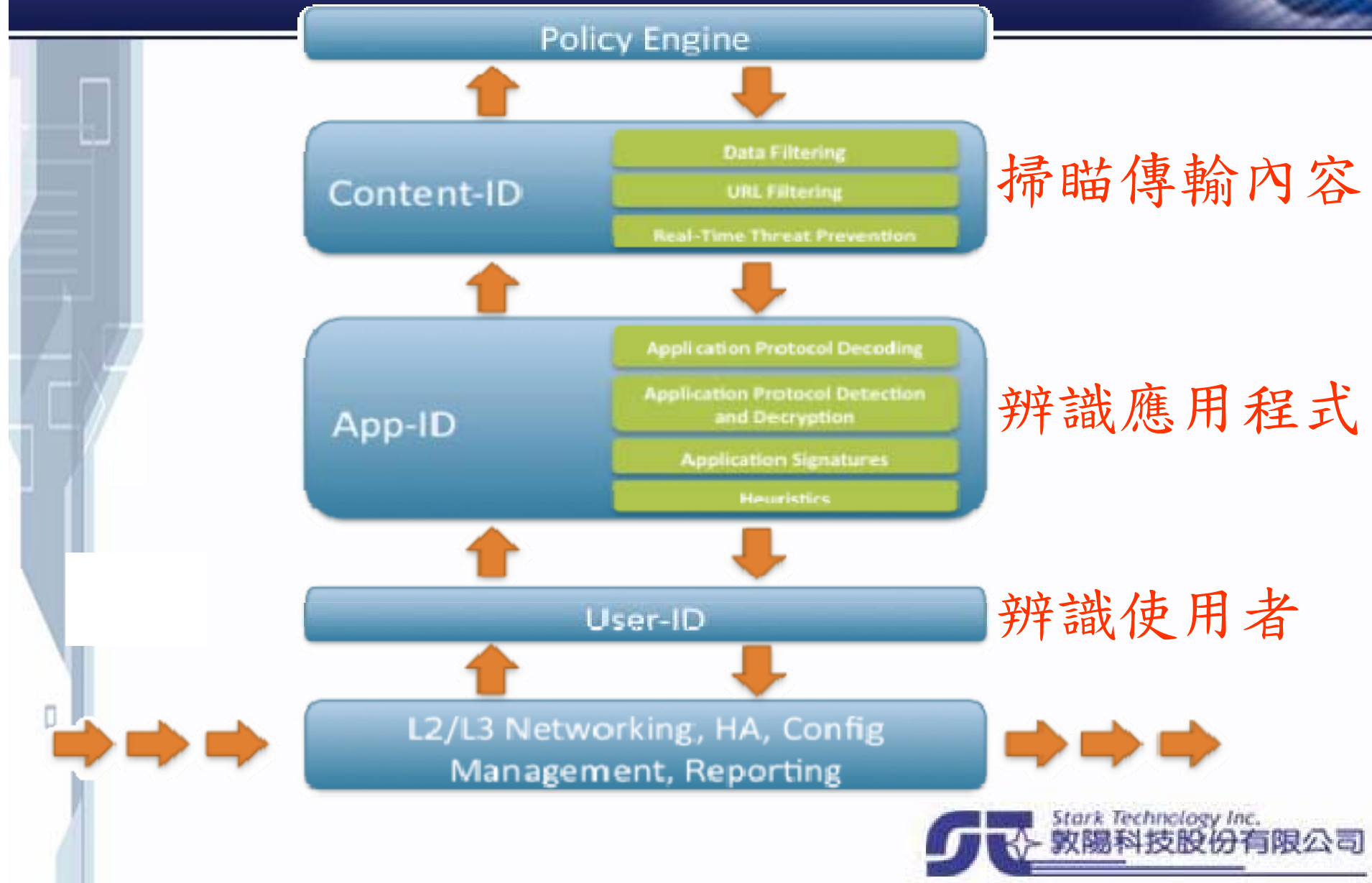


**ALL SQL commands**  
**Actual SQL**  
**Fields**  
**Objects**  
**Verbs**  
**All SELECTS**  
**DDL**  
**DML**  
**DB user name**  
**DB version**  
**DB type**  
**DB protocol**  
**DB User**  
**DB errors**  
etc.

# AP之外的存取行為也要注意!



# 次世代應用程式防火牆



# 辨識應用程式



## Top Applications

	Risk	Application	Sessions	Bytes
1	4	web-browsing	300	2,276,586
2	4	facebook-base	123	698,546
3	3	facebook-chat	46	209,009
4	4	dns	26	10,454
5	4	myspace-base	24	605,456
6	2	ntp	21	3,870
7	3	myspace-mail	12	208,662
8	4	flash	10	368,366
9	3	myspace-im	8	34,896
10	3	photobucket	4	38,730
11	1	myspace-video	4	6,214
12	4	rtmpe	2	10,786
13	4	ssl	2	16,702
14	5	http-audio	2	12,402
15	2	google-analytics	2	2,334

# 辨識使用者



Dashboard

ACC

Monitor

Policies

Objects

Network

Device

Logout

Time Frame Last Hour

Sort By Sessions

Top N 25

Go

Set Filter

Help

Application facebook

## Application Information

Name: facebook

Related: facebook-chat, facebook-mail, facebook-games

Description: all the facebook related apps.

Additional Information: facebook - Google Yahoo!

## Top Applications

	Risk	Application	Sessions	Bytes
1	4	facebook-base	5,042	45,735,093
2	3	facebook-chat	421	4,911,969
3	4	facebook-apps	44	1,946,120
4	2	facebook-mail	11	588,180

## Top Sources

	Source address	Source Host Name	Source User	Bytes	Sessions
1	10.154.2.33	engr33.net2.bigeduo	pancademo\phillip.blumste	1,158,885	180
2	10.154.1.27	engr27.net1.bigeduo	pancademo\ellen.cook	822,648	171
3	10.154.12.89	engr89.net12.bigeduo	pancademo\ginger.poppe	2,360,286	140
4	10.154.14.61	engr61.net14.bigeduo	pancademo\natalie.ullrich	681,430	140
5	10.154.12.21	engr21.net12.bigeduo	pancademo\shawn.skilton	453,449	108

## ● 辨識使用者

- ▶ 老闆可以玩facebook遊戲
- ▶ MIS可以facebook聊天
- ▶ 員工不能上facebook

# 辨識傳輸內容



Edit Custom Data Pattern -- 網頁對話

<https://ca2demo.paloaltonetworks.com/esp/editDlpDataObjectPattern.esp?mode=edit&row=0&origpattern> 憑證錯誤

**Pattern Name**

**Regular Expression**  Max 1024 characters

**Weight**  (0 - 255)

<https://ca2demo.paloaltonetworks.com/esp/editDlpDataObjec>

New Data Pattern -- 網頁對話

<https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&returnTo=editDlp> 憑證錯誤

**Name**

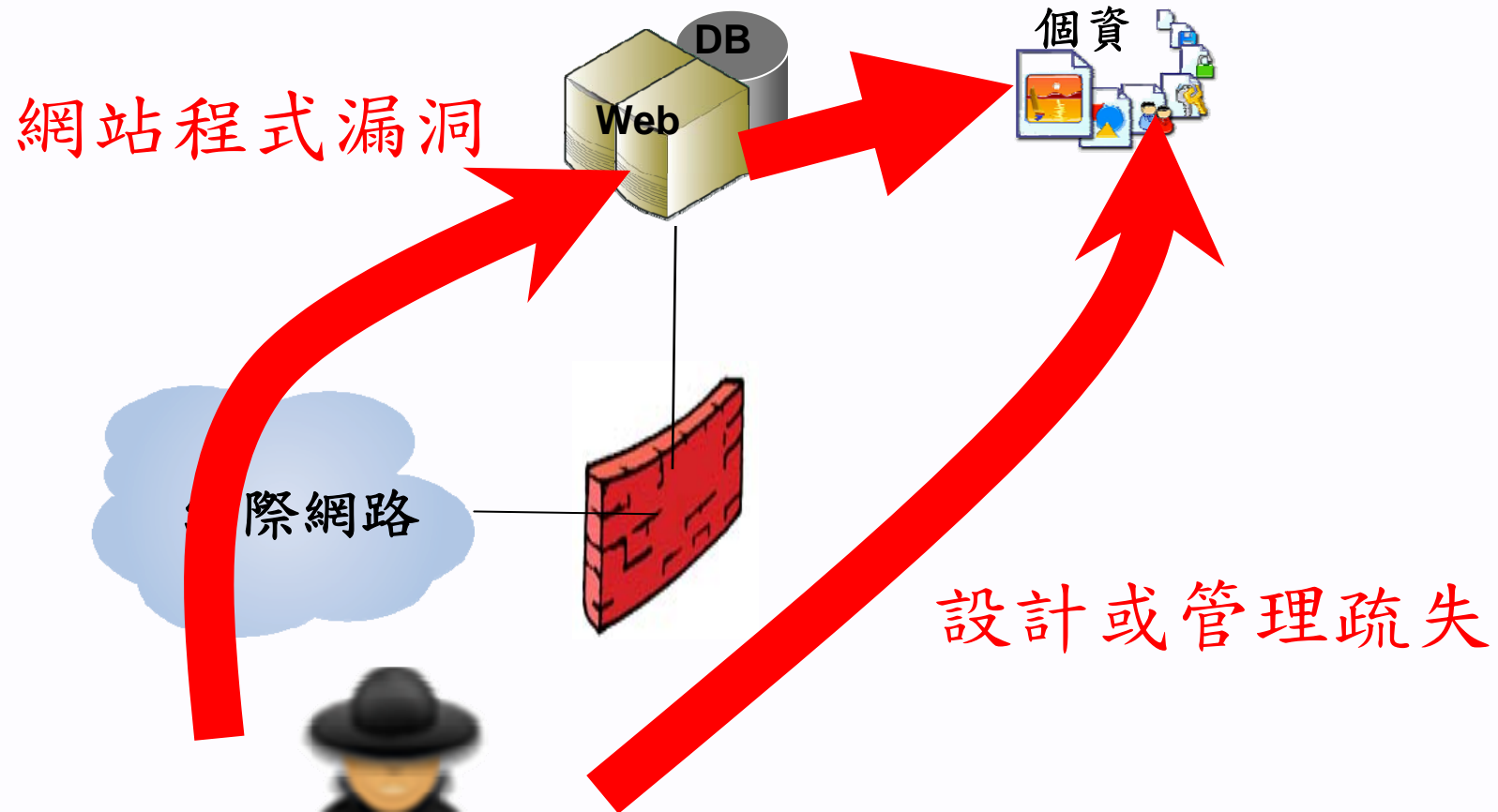
**Description**

**Patterns**

Pattern	Weight	
Credit Card Number	<input type="text"/>	
Social Security Number	<input type="text"/>	
Social Security Number (without dash)	<input type="text"/>	
Confidential Secret Garden	1	<input checked="" type="checkbox"/>
	(0 - 255)	

<https://ca2demo.paloaltonetworks.com/esp/editDlpDataObject.esp?mode=new&retu> 網際網路

# 利用第七層網站漏洞





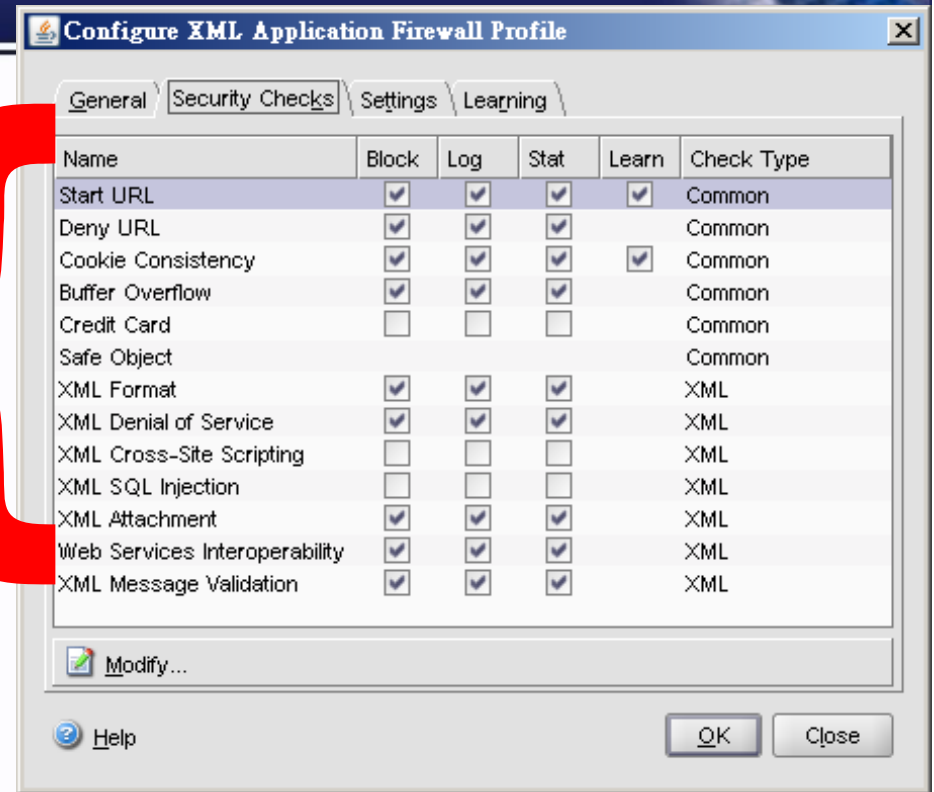
# 網站防火牆

毋須上百條規則  
以「行為」為基準  
毋須更新

正面表列白名單

只開放程式可正常執行的行為

就可防堵零時差攻擊





Q&A