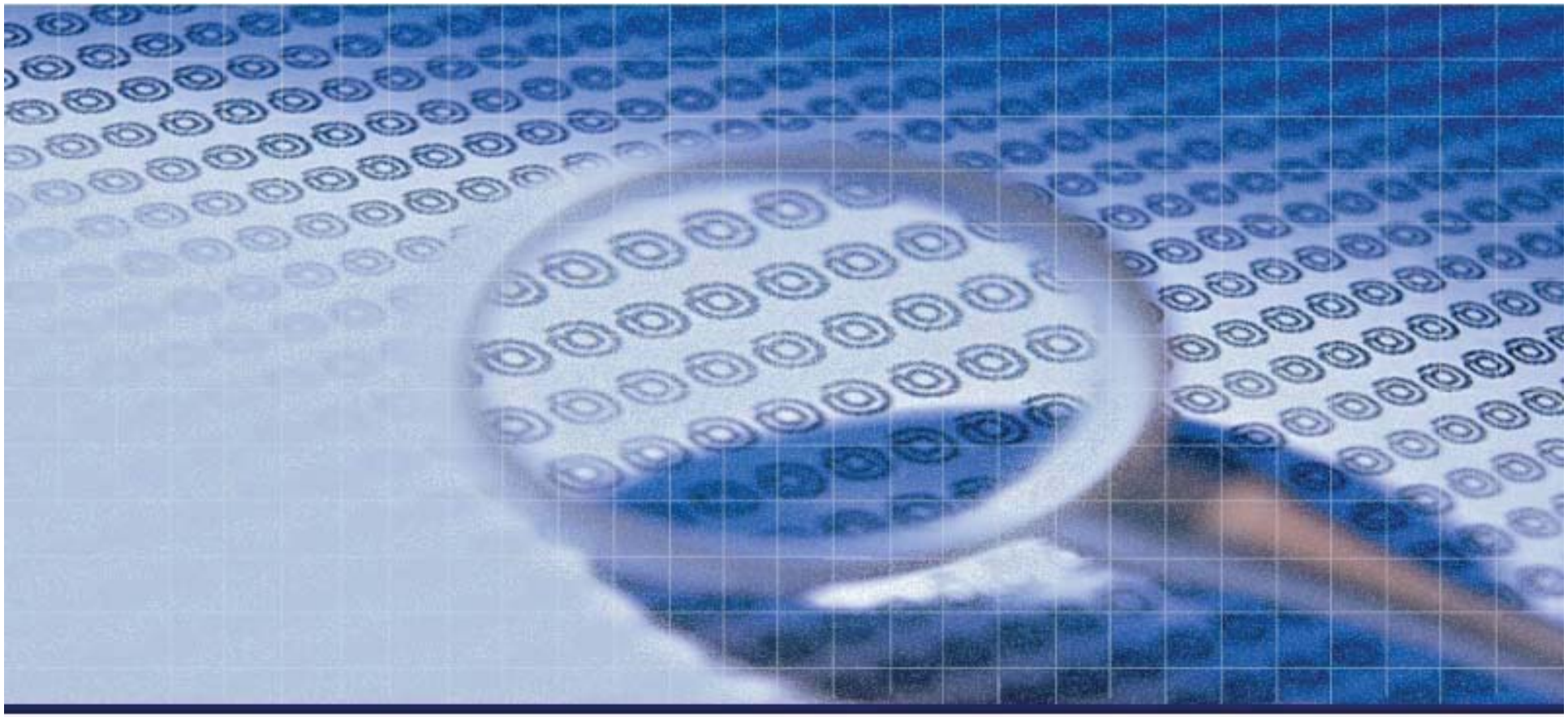
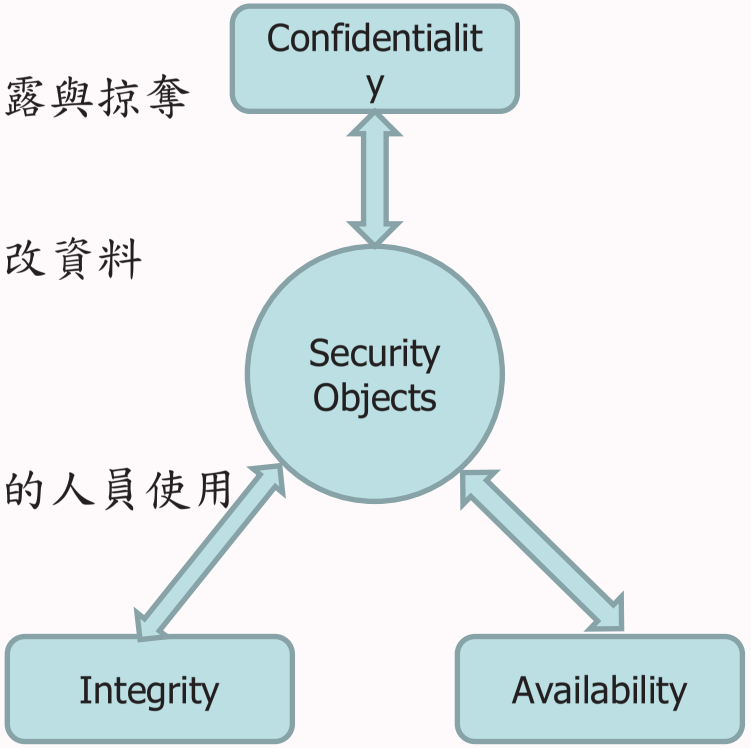


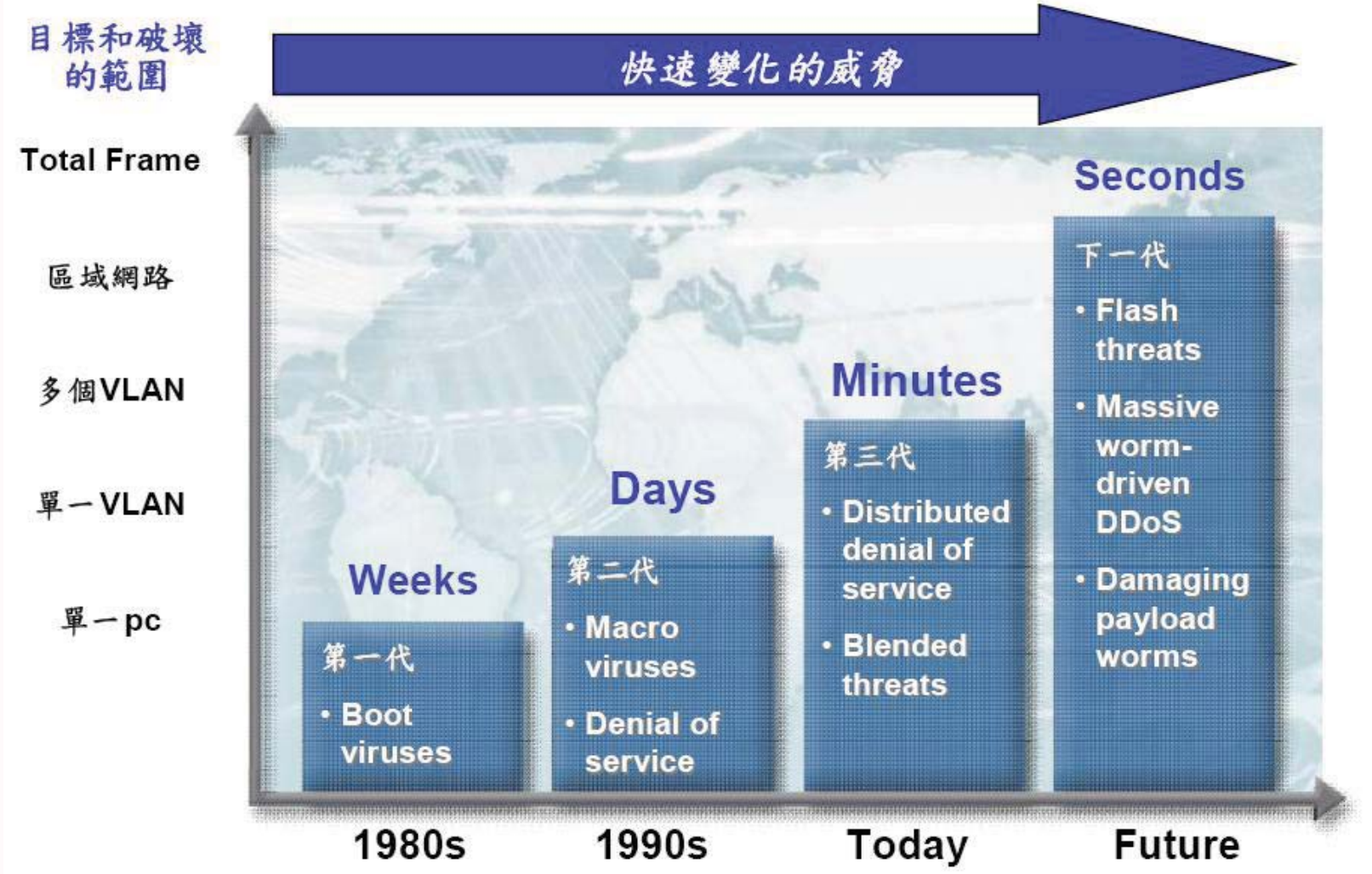
資安技術與防駭

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



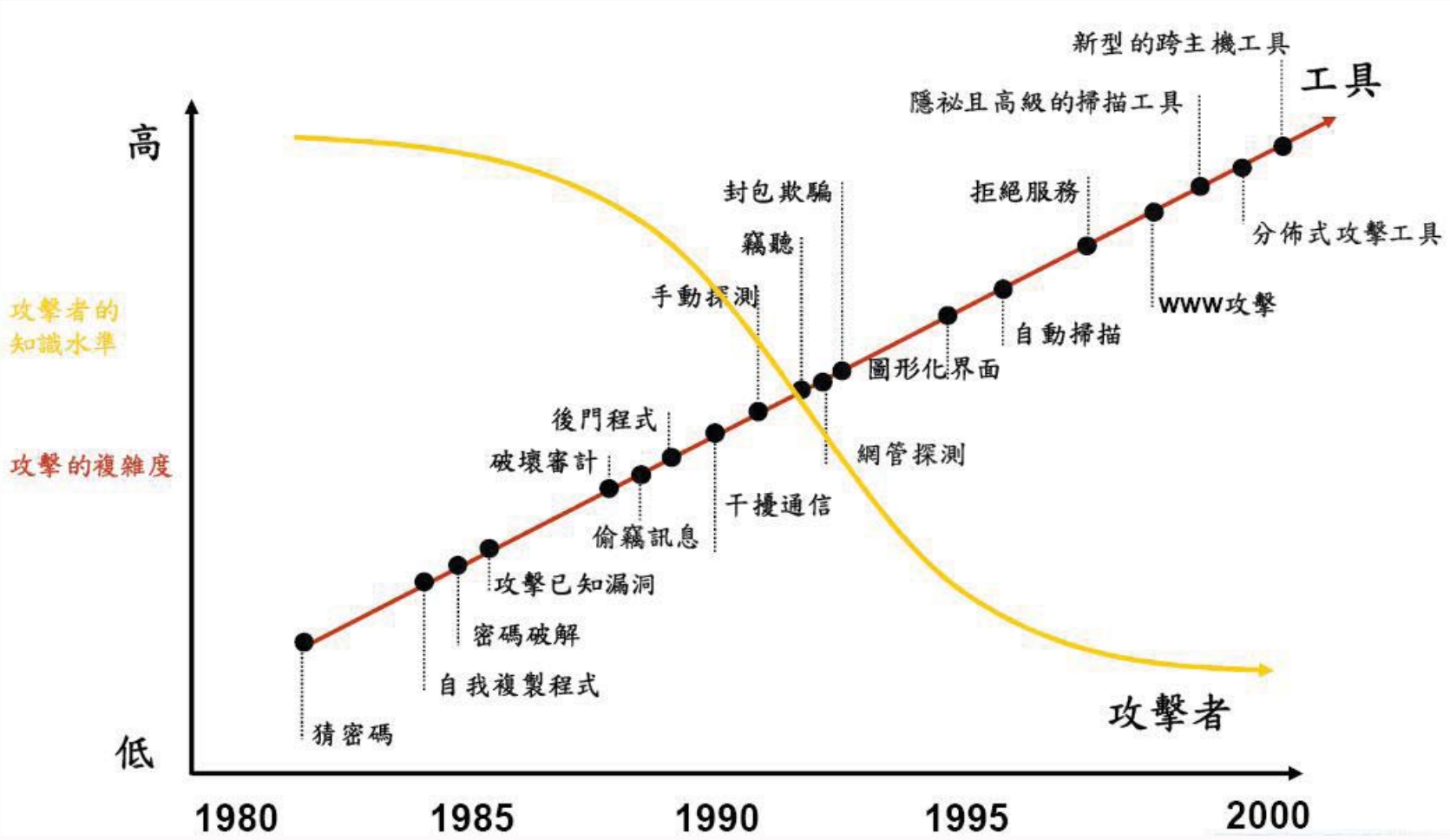
攻擊範圍和時間變化



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	• 大規模 • 從不同的網段 • 單一掃描來源	• 小規模隨機 • 在相同網段或信任網段 • 分散掃描來源
攻擊方式	• 單純 • 漏洞攻擊	• 未知形態 • 社交工程 • 網站漏洞攻擊
後門及木馬運用模式	• 植入後馬上使用 • 本機開啟 Listen Port	• 潛伏等待 • 主動向外連線、匿蹤
駭客工具	• 一般網路上常見工具	• 自製工具、Rootkit • 惡意網站、網頁、電子郵件
目的	• 竊取資料檔案 • 偷取密碼 • 炫耀	• 竊取資料檔案 • 偷取密碼 • 生財工具

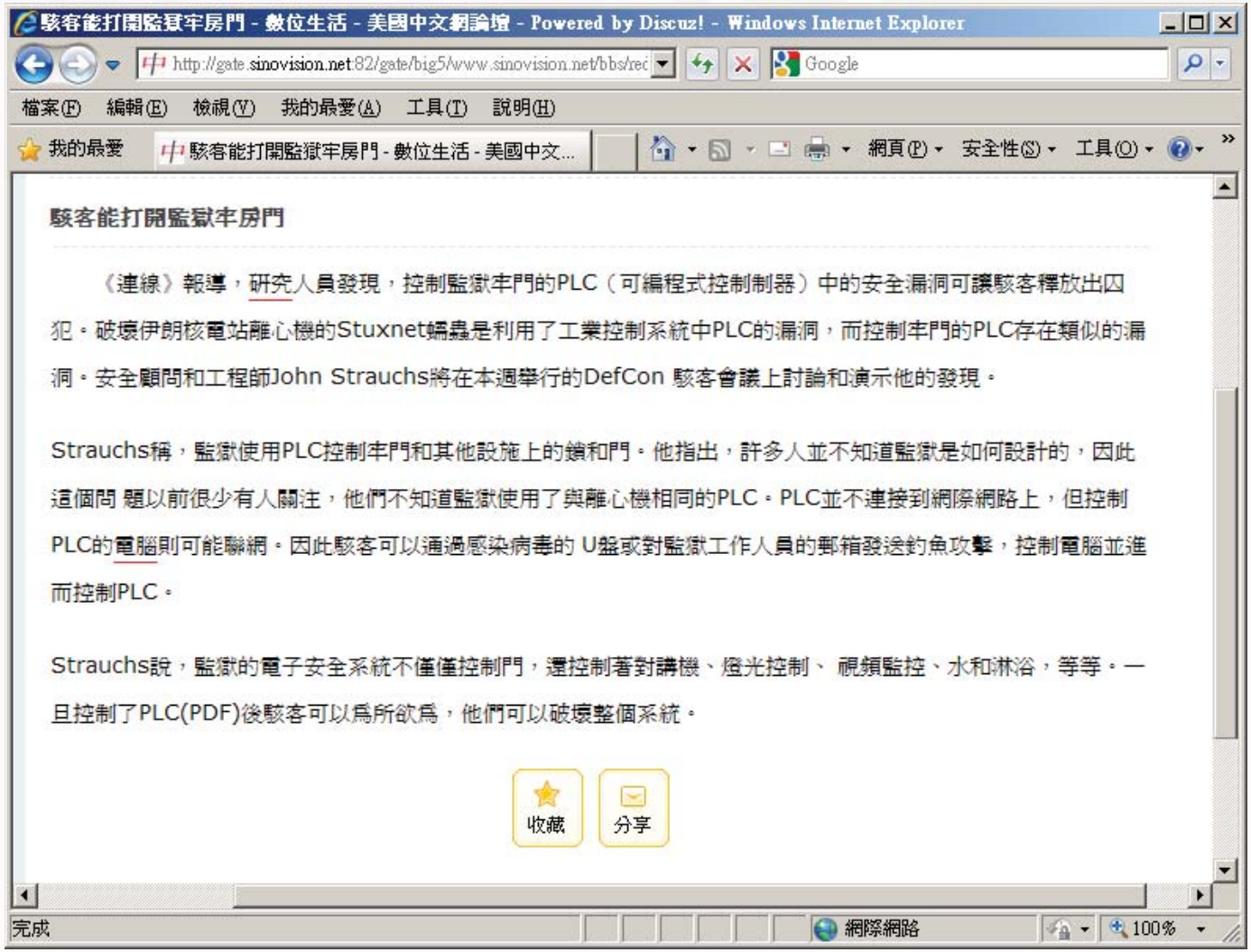
內部網路的潛在危機

- 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
  - 透過網路閘道的機密資料外洩
  - 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



Stark Technology Inc.
敦陽科技股份有限公司

資訊人員的取捨

安全
Security

效能
Performance

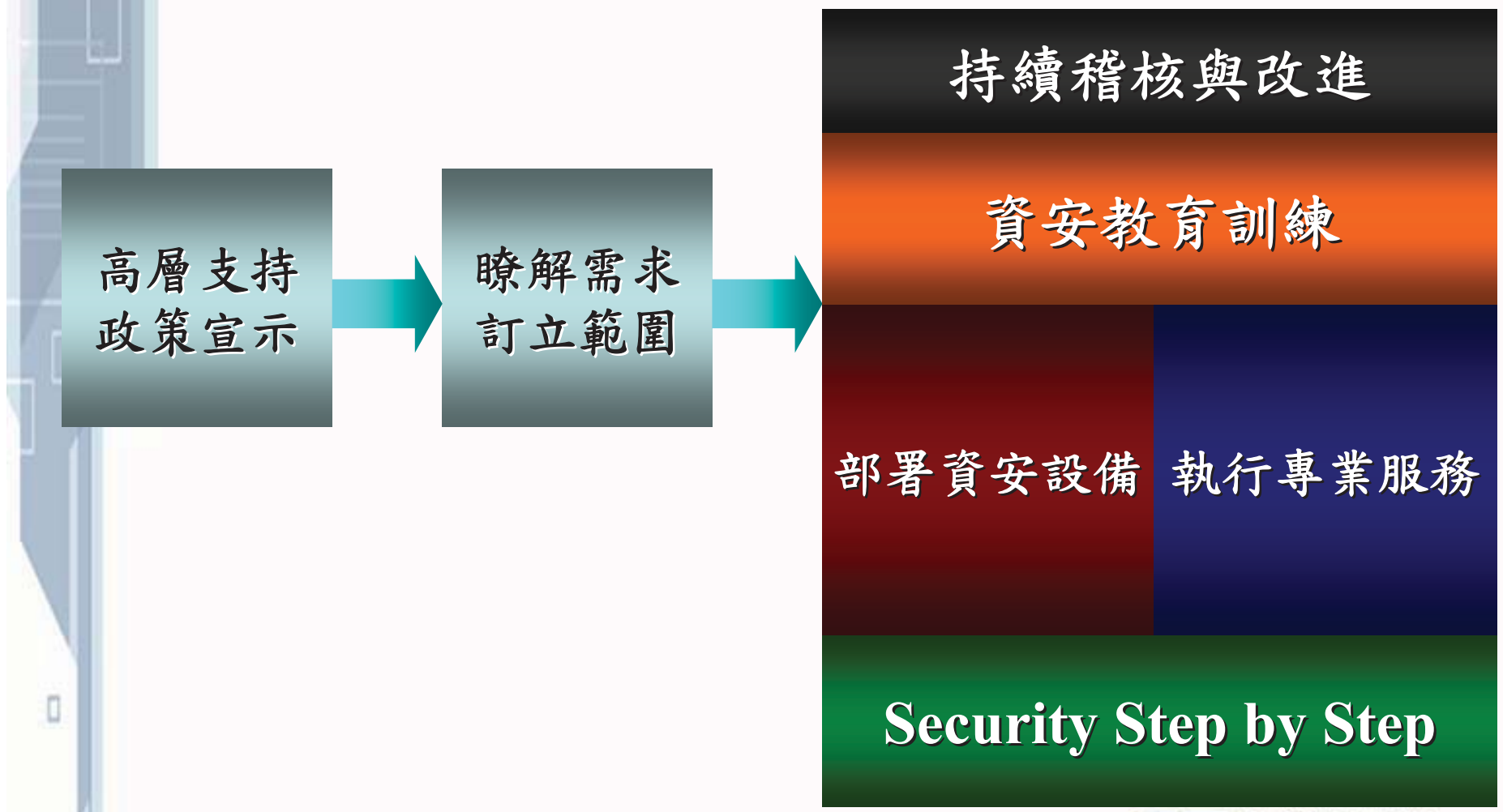
便利
Convenient

管理/實作能力
Administration

成本
Cost

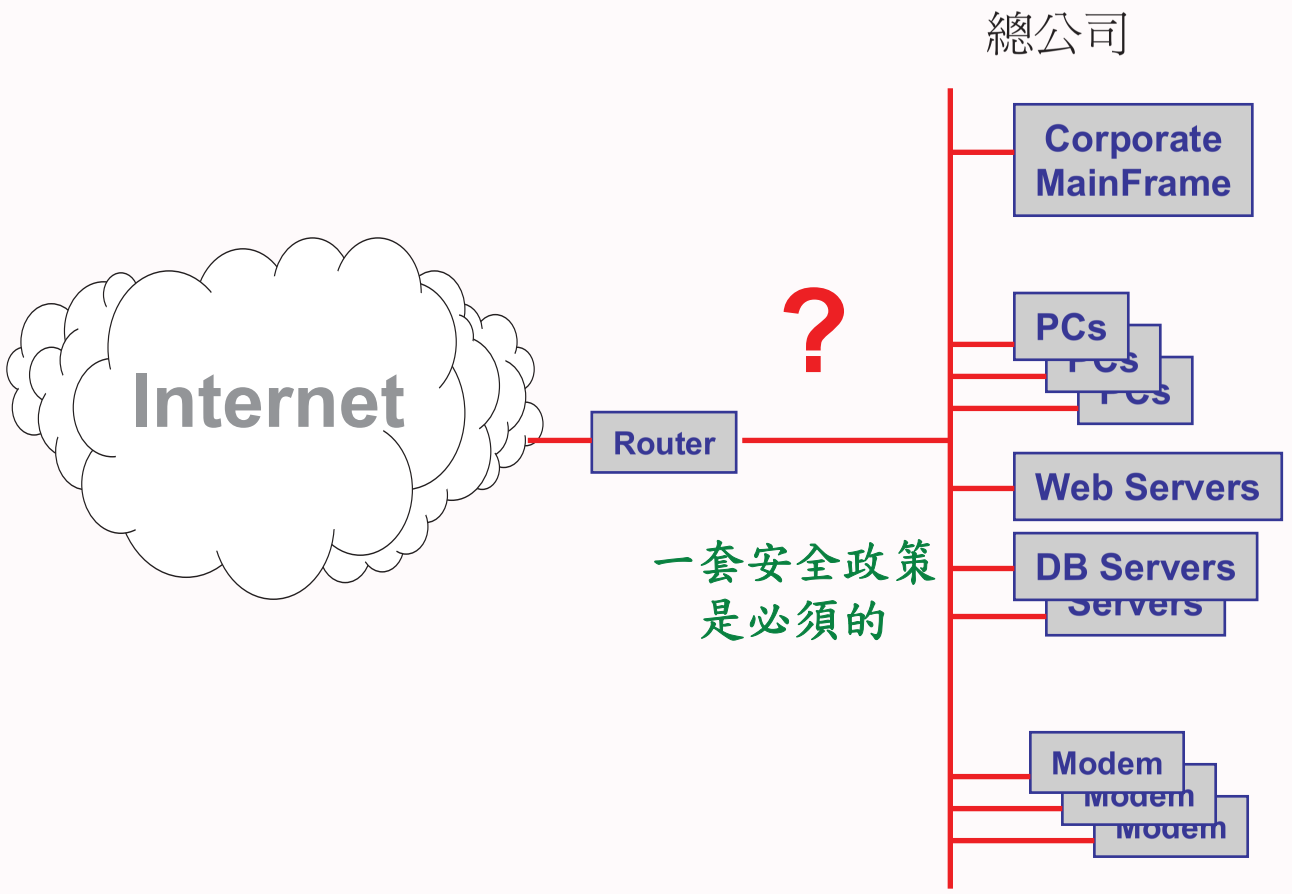
Stark Technology Inc.
敦陽科技股份有限公司

資安規劃大架構



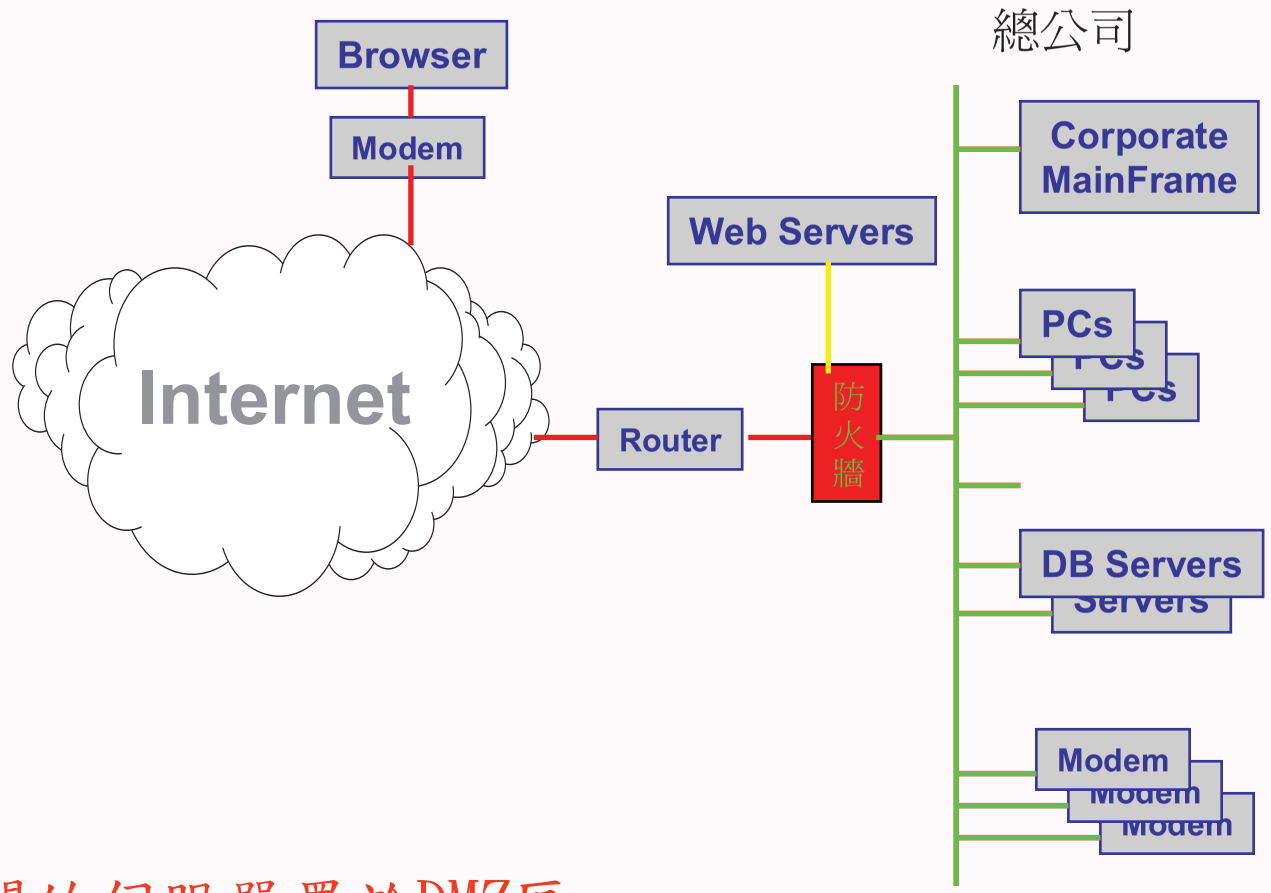
Stark Technology Inc.
敦陽科技股份有限公司

連接到網際網路隱藏的安全問題



Stark Technology Inc.
敦陽科技股份有限公司

建置防火牆區隔網路



並將公開的伺服器置於DMZ區

Stark Technology Inc.
敦陽科技股份有限公司

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

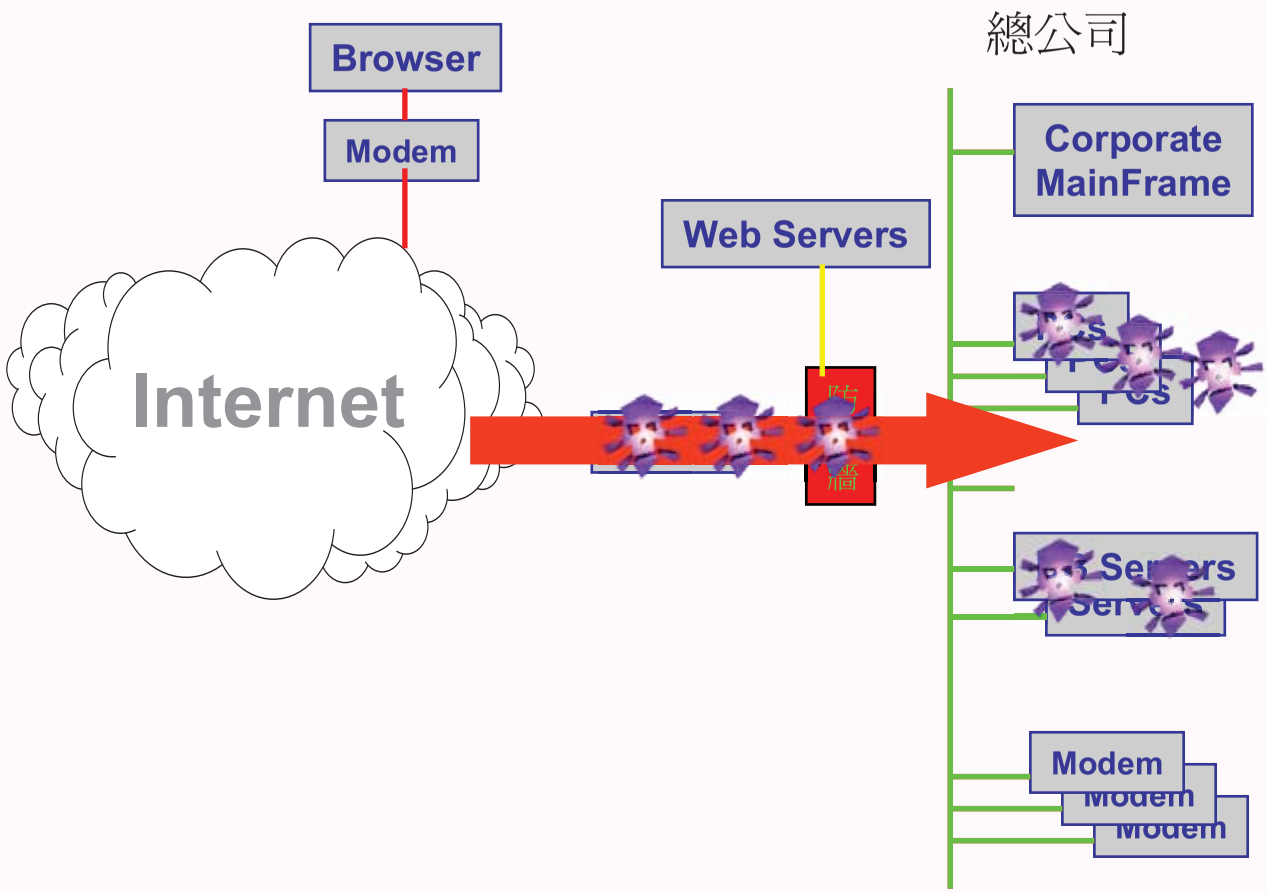
缺點

- 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

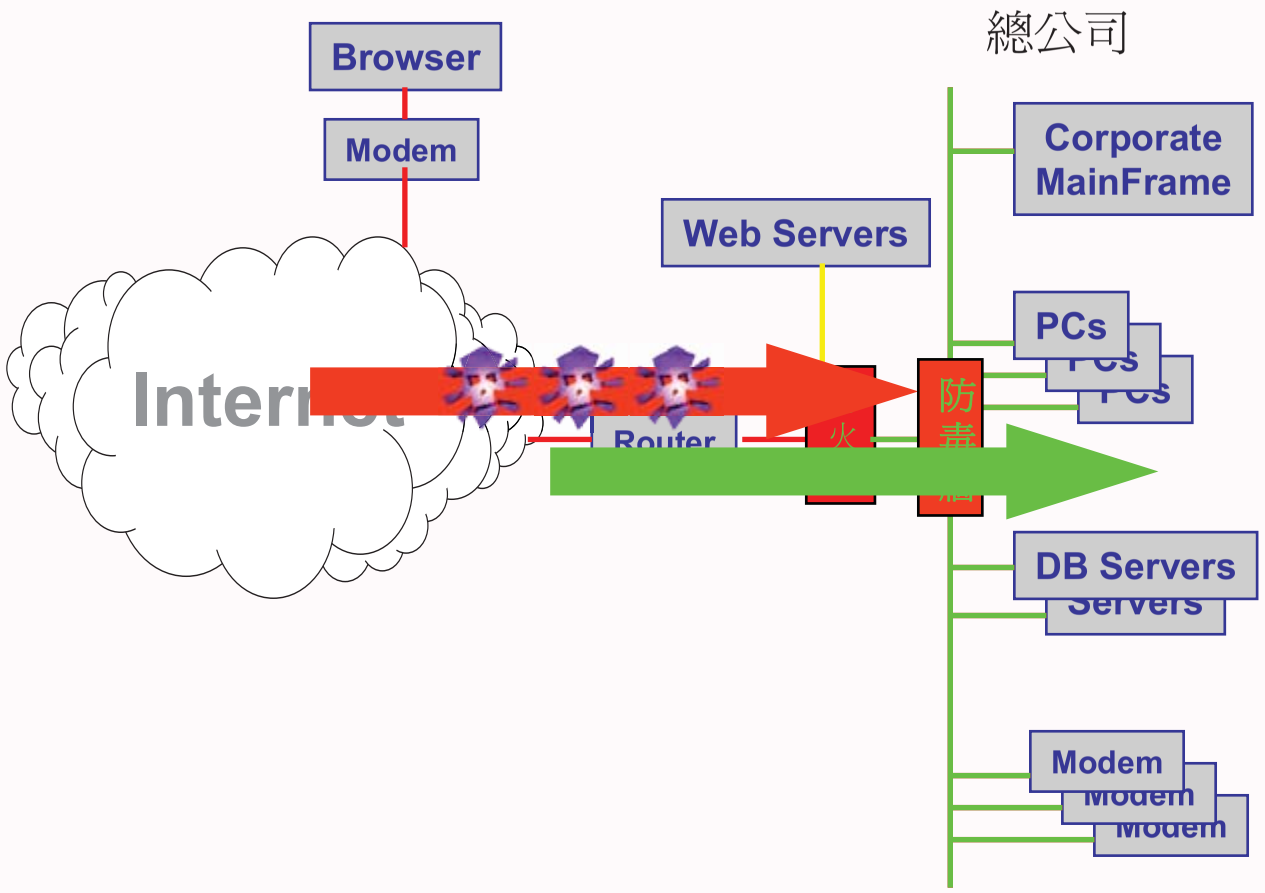
Stark Technology Inc.
敦陽科技股份有限公司

網際網路變成病毒主要來源

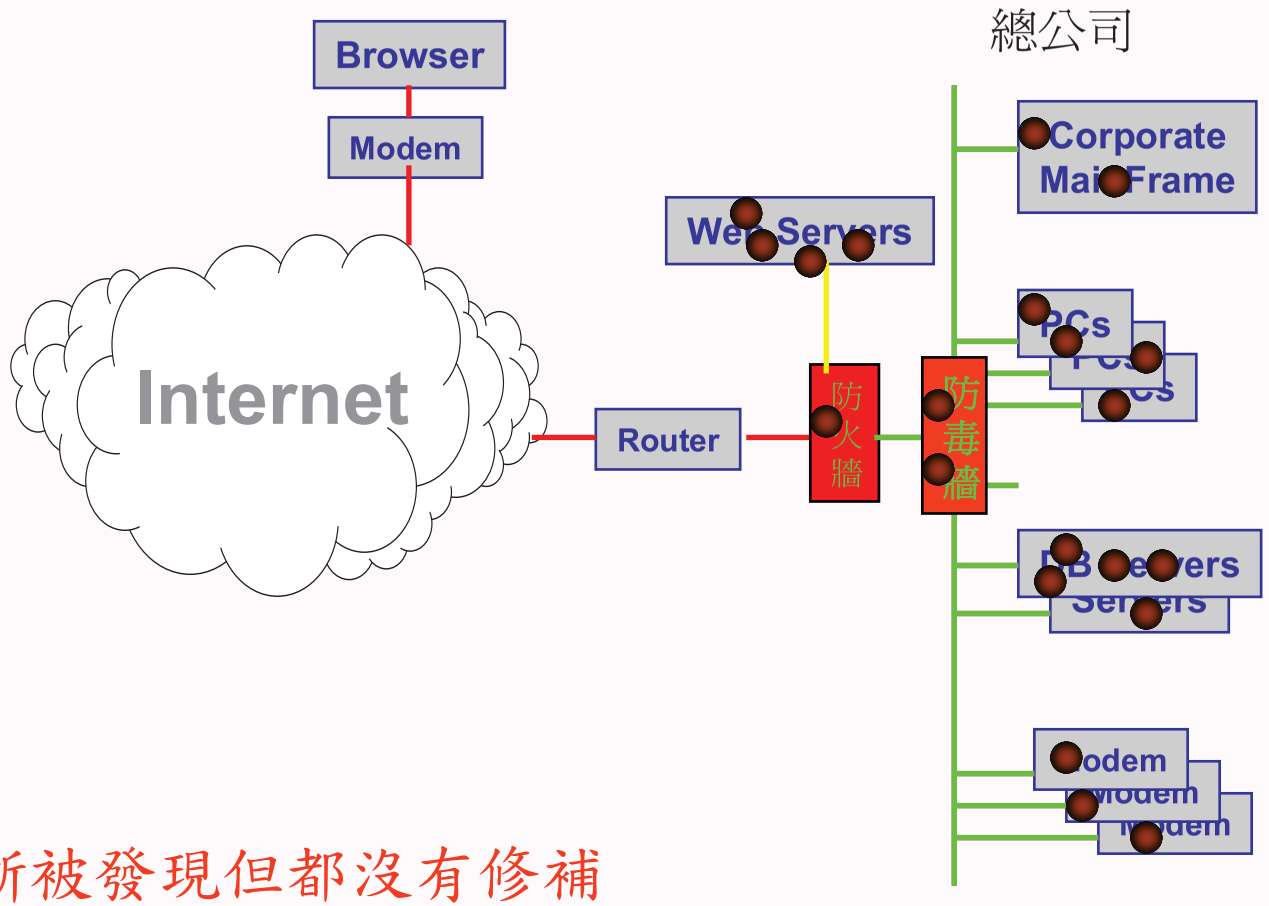


在Mail, HTTP, FTP的檔案中藏有病毒

建置防毒牆過濾病毒



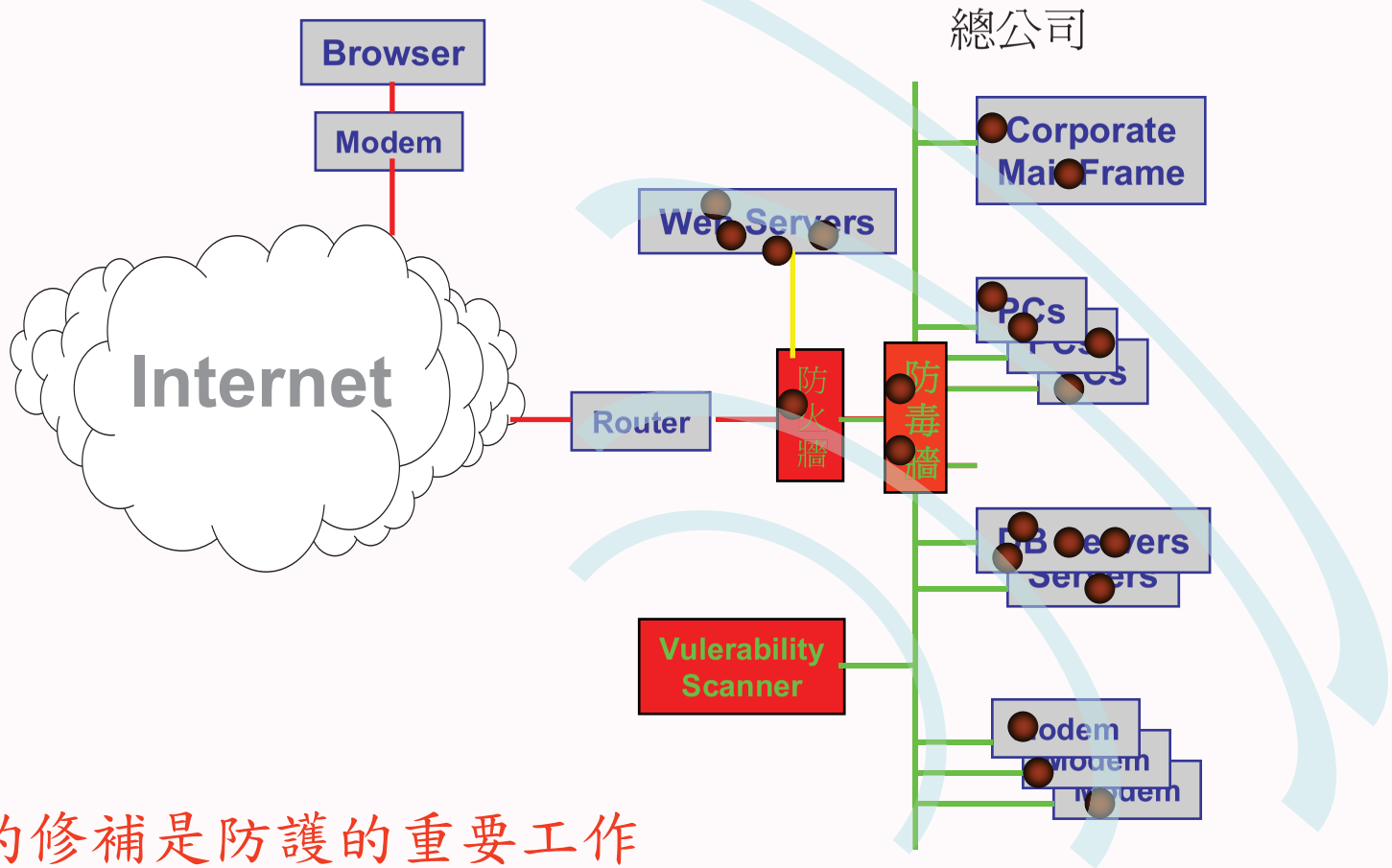
系統中有那些漏洞?



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

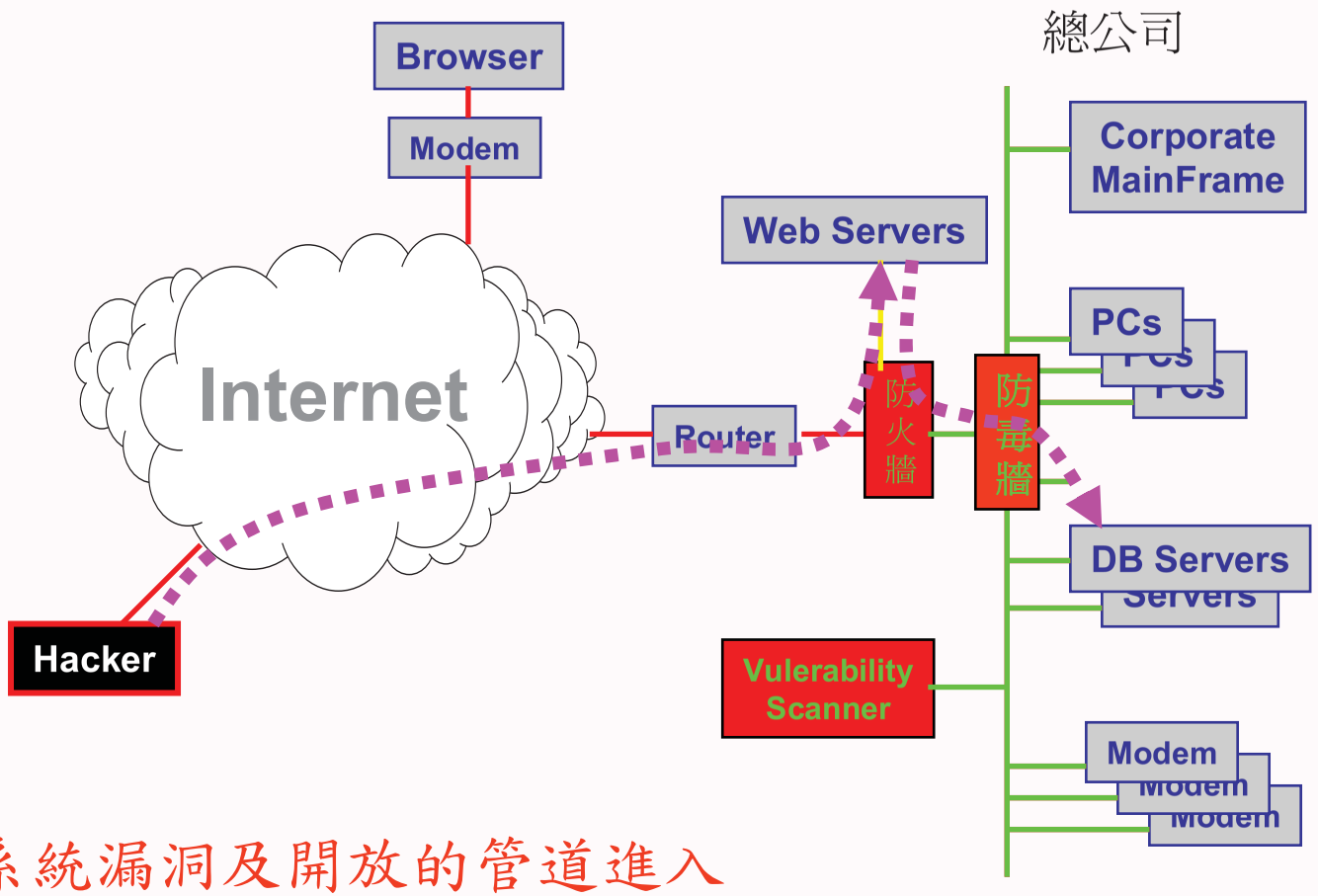
定期弱點掃描協助弱點的修補



持續性的修補是防護的重要工作

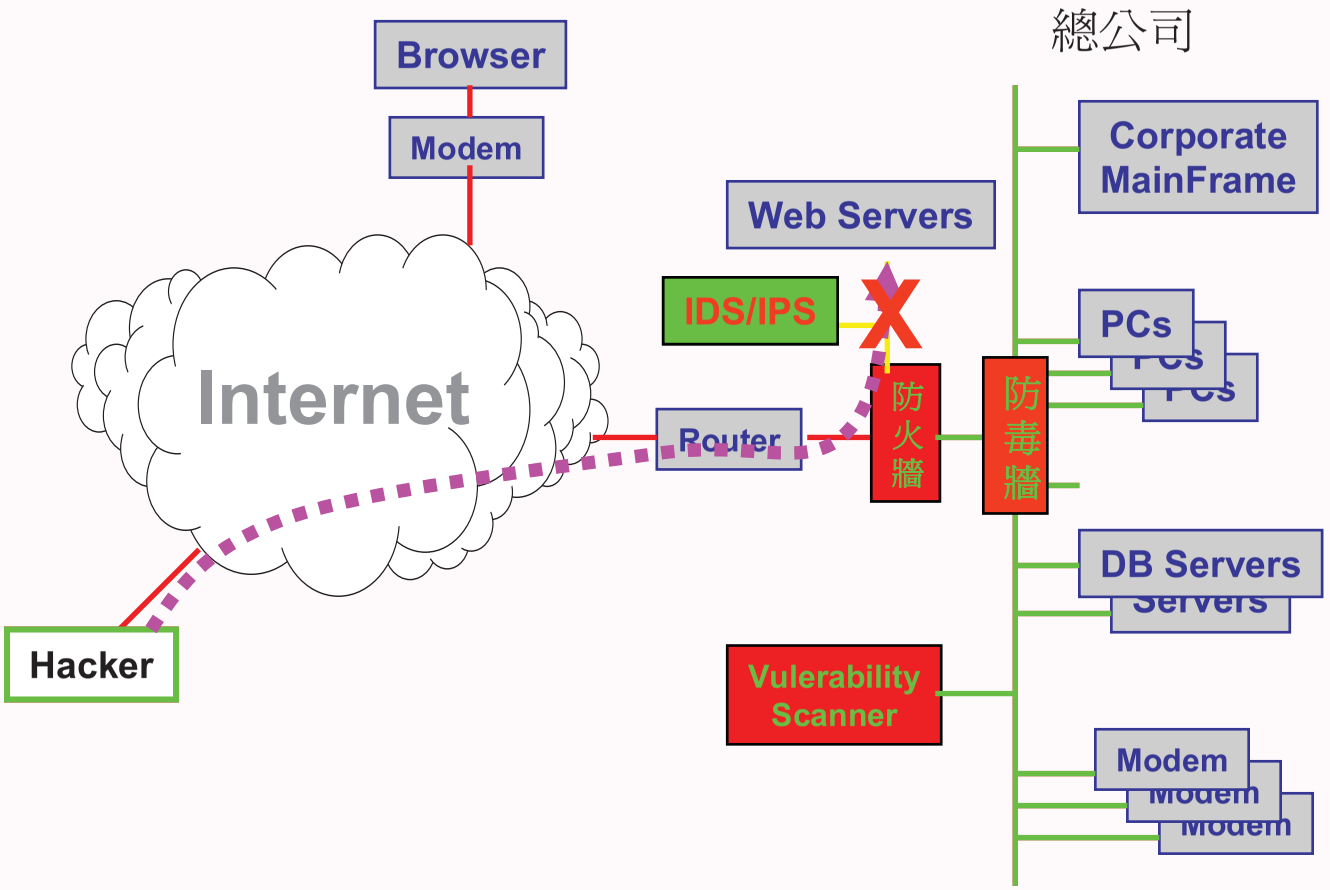
Stark Technology Inc.
敦陽科技股份有限公司

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



Stark Technology Inc.
敦陽科技股份有限公司

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

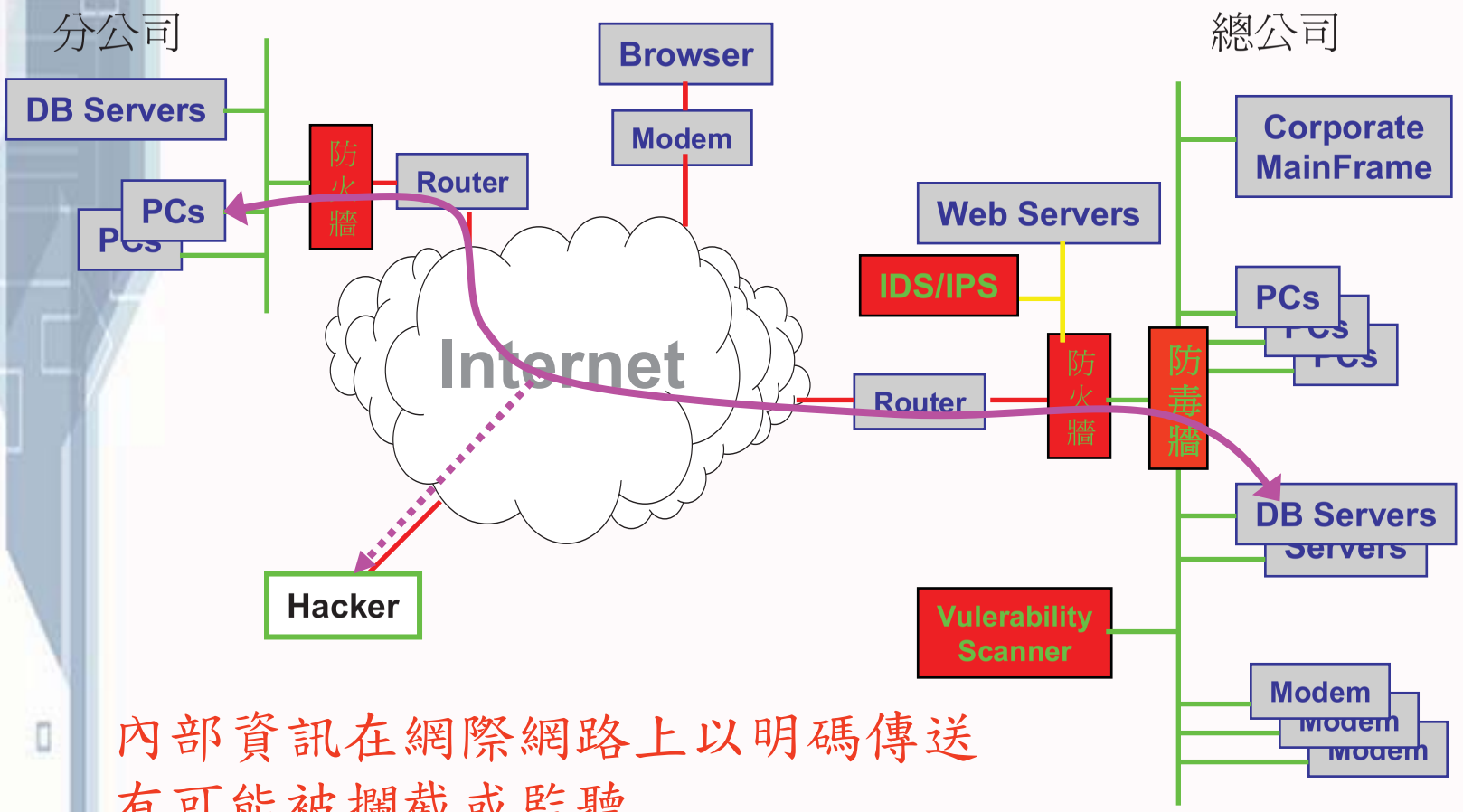
異常偵測法

- 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…

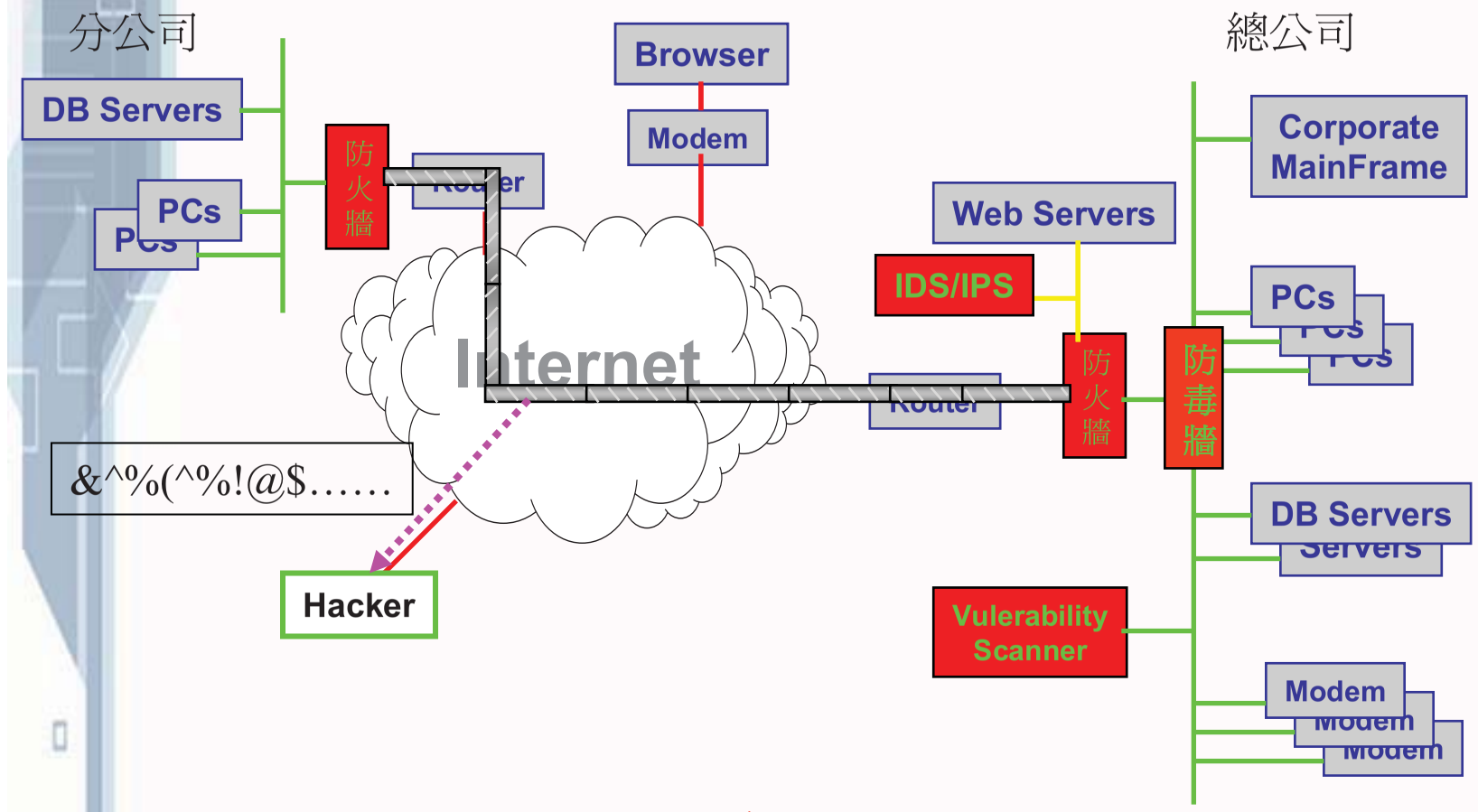
當分公司要透過網際網路傳遞資料時



內部資訊在網際網路上以明碼傳送
有可能被攔截或監聽

Stark Technology Inc.
敦陽科技股份有限公司

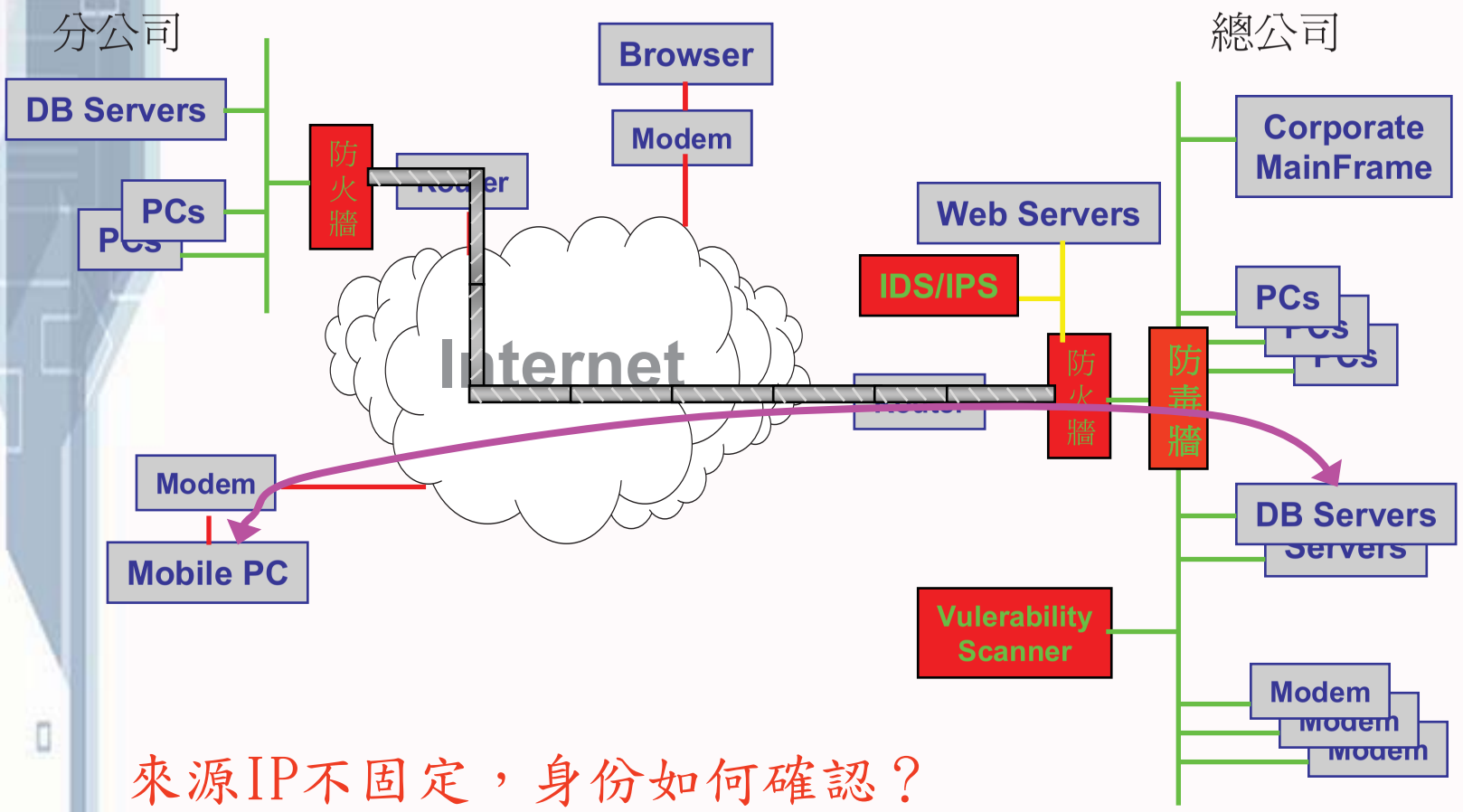
建置VPN通道確保資料傳輸安全



即使被監聽了也是加密資料

Stark Technology Inc.
敦陽科技股份有限公司

外勤人員的存取如何確保安全?

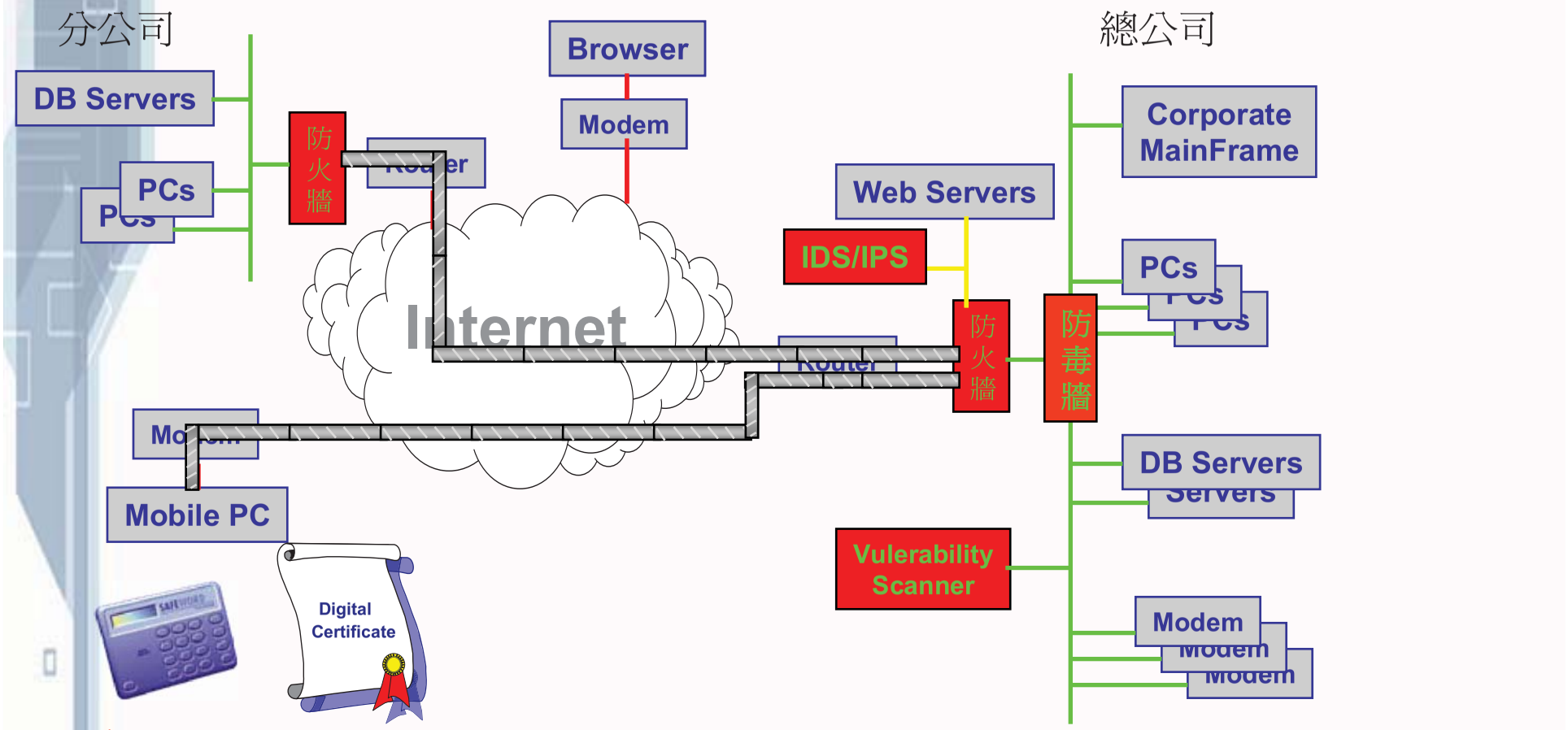


來源IP不固定，身份如何確認？

機密資料傳輸如何保護？

Stark Technology Inc.
敦陽科技股份有限公司

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

Stark Technology Inc.
敦陽科技股份有限公司

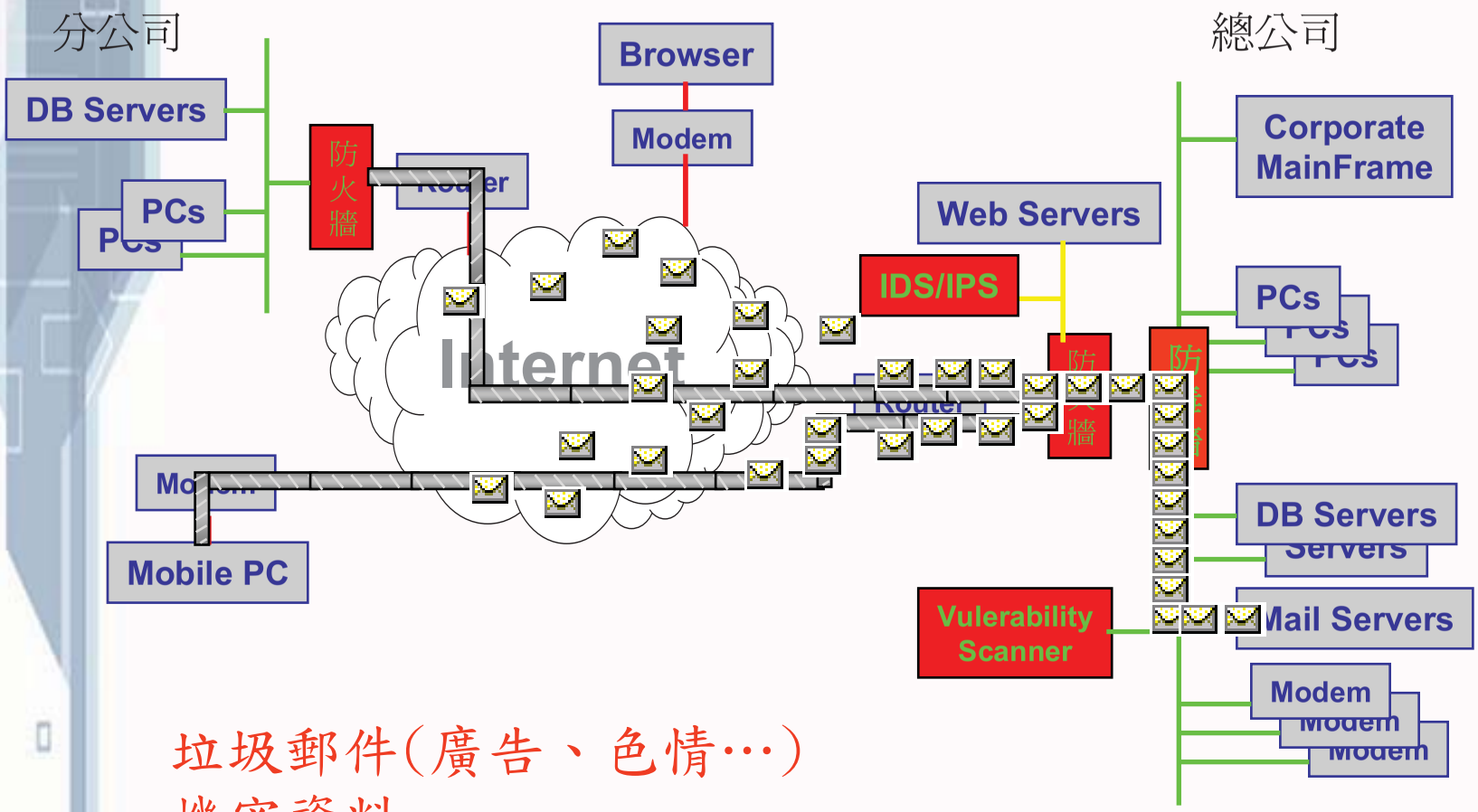
SSL VPN的掘起

- 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

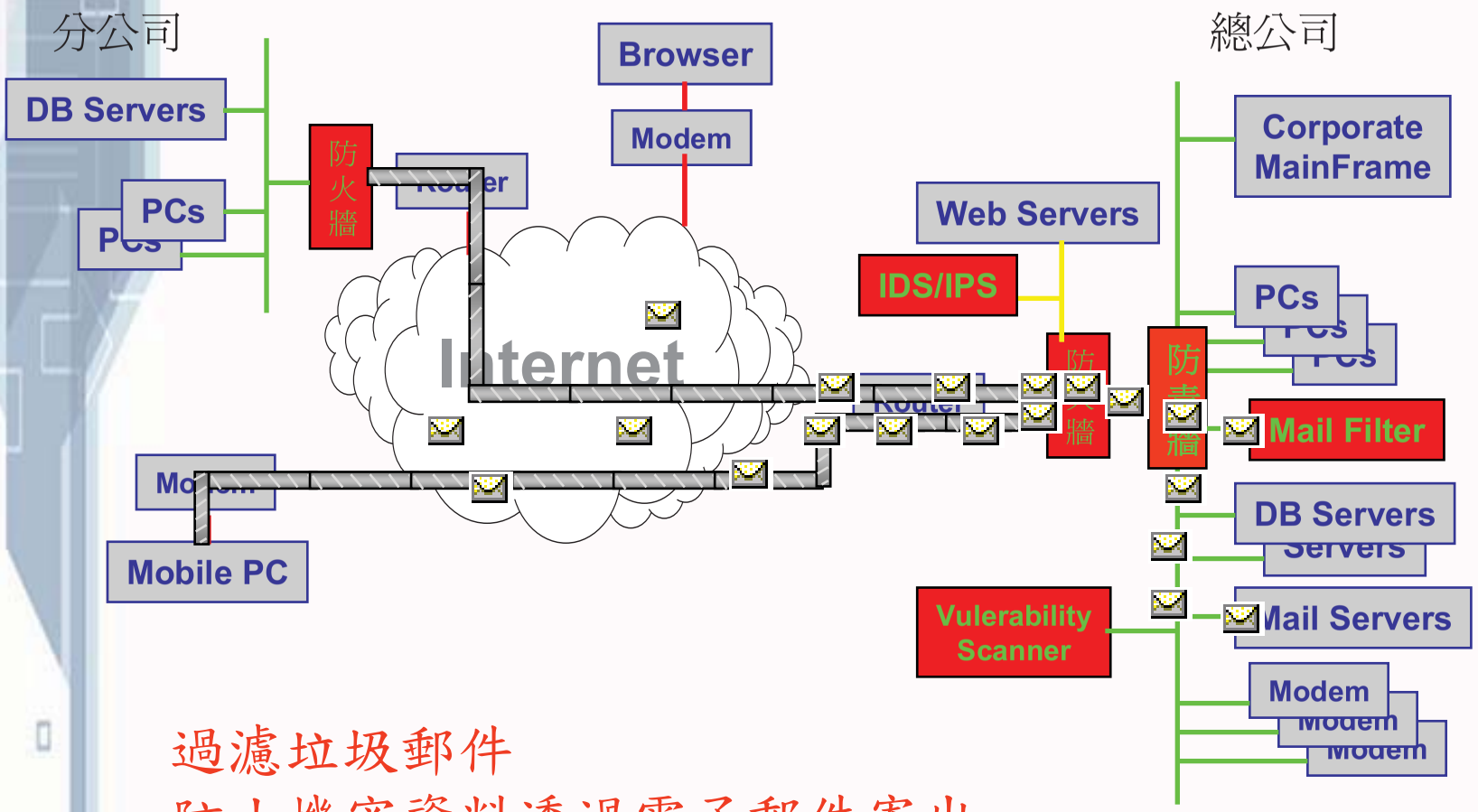


垃圾郵件(廣告、色情…)

機密資料

Stark Technology Inc.
敦陽科技股份有限公司

建置電子郵件過濾匣道
保護機密資料不外洩

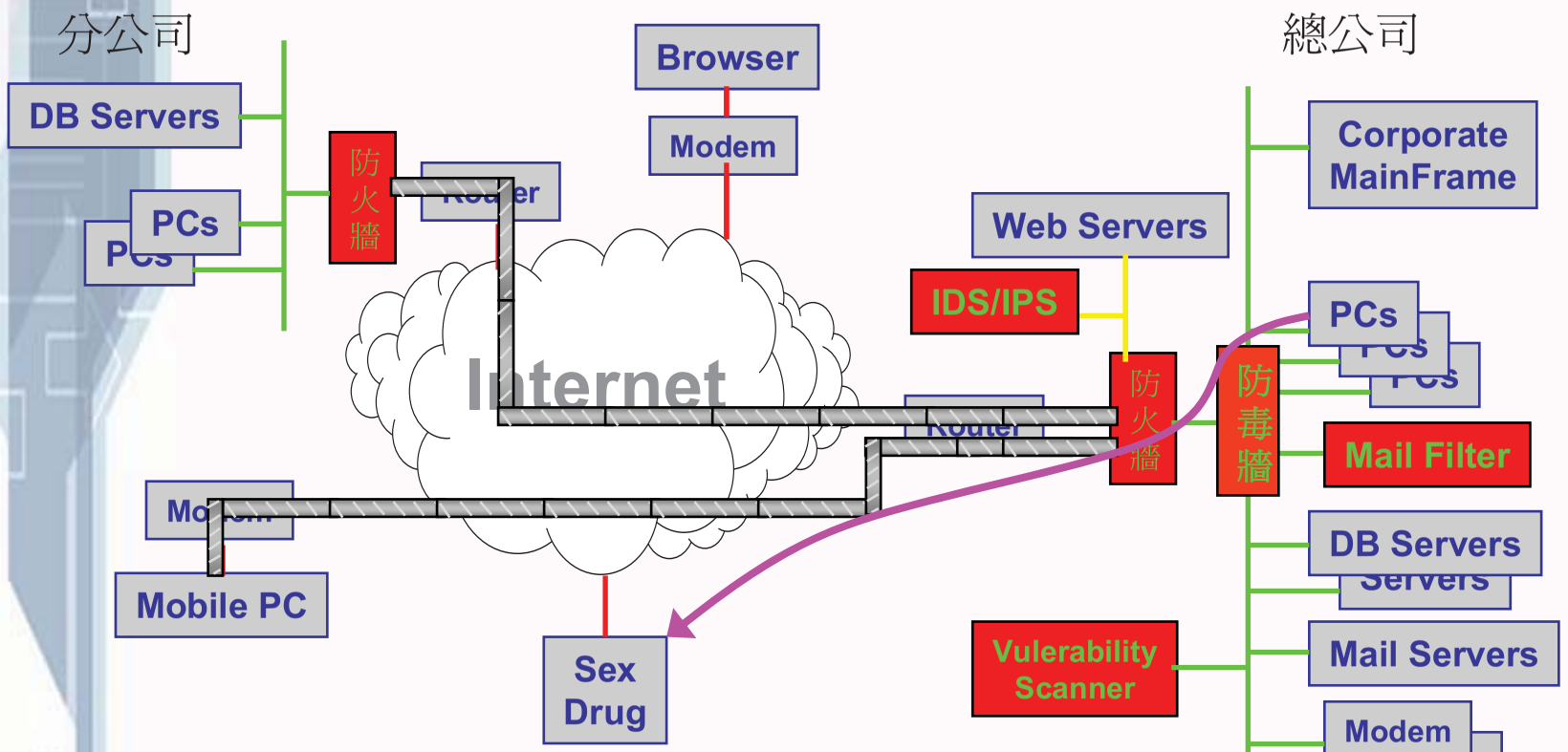


過濾垃圾郵件

防止機密資料透過電子郵件寄出

Stark Technology Inc.
敦陽科技股份有限公司

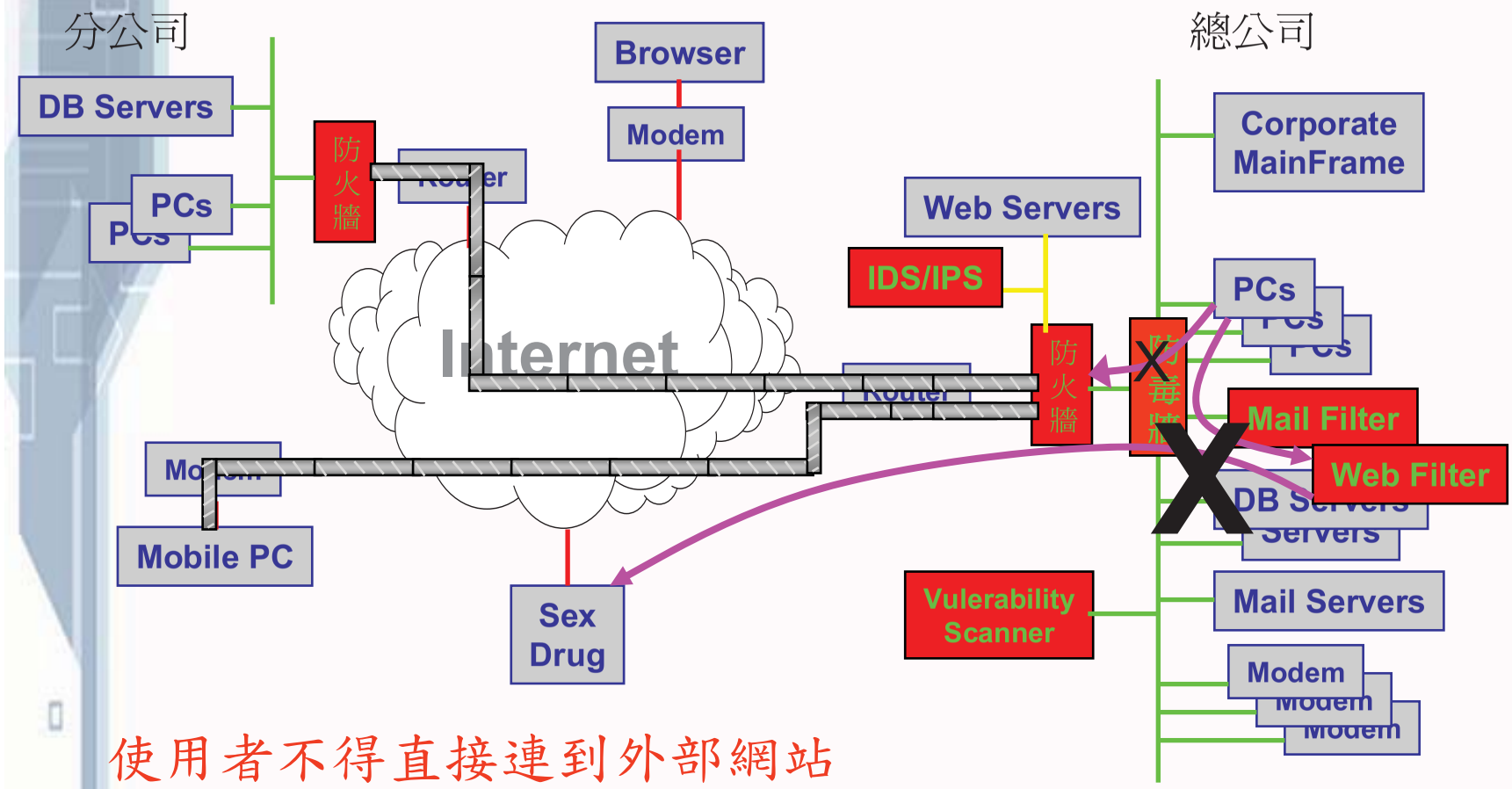
不良網站充斥網際網路



惡質資訊充斥企業內部
網路漫遊浪費員工生產力

Stark Technology Inc.
敦陽科技股份有限公司

建置Web過濾系統確保員工生產力

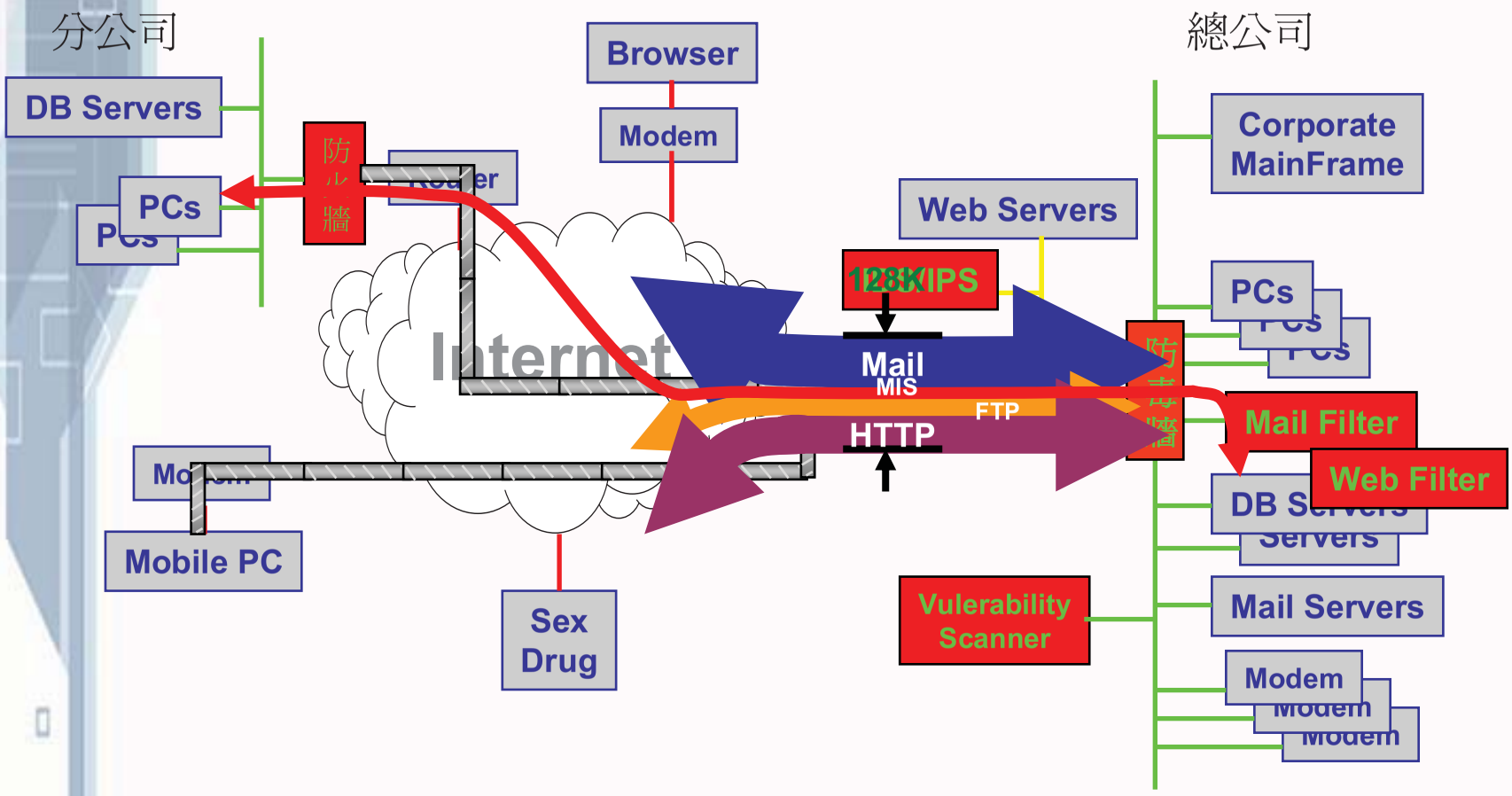


使用者不得直接連到外部網站

Web Filter拒絕不良網址

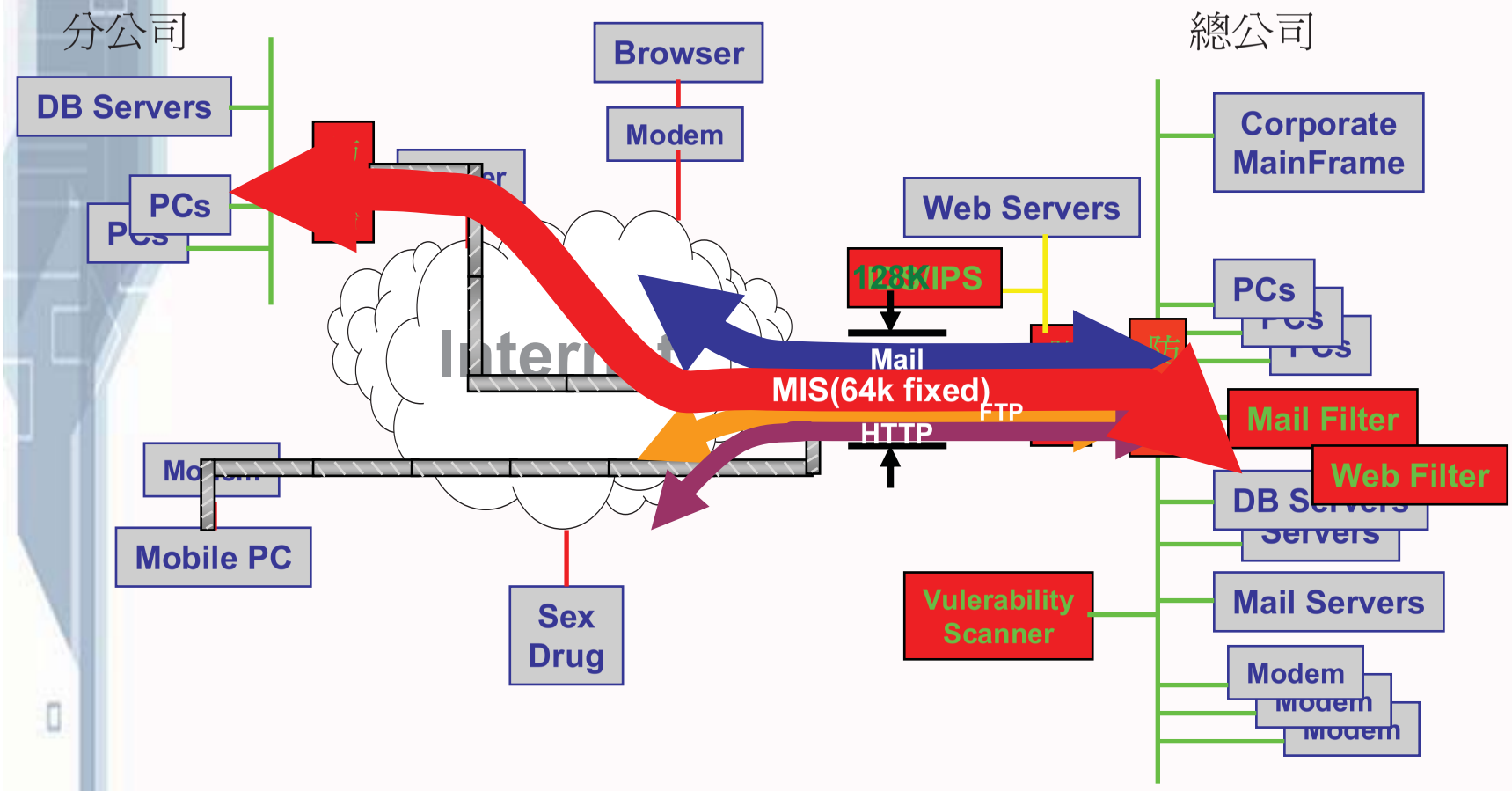
Stark Technology Inc.
敦陽科技股份有限公司

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

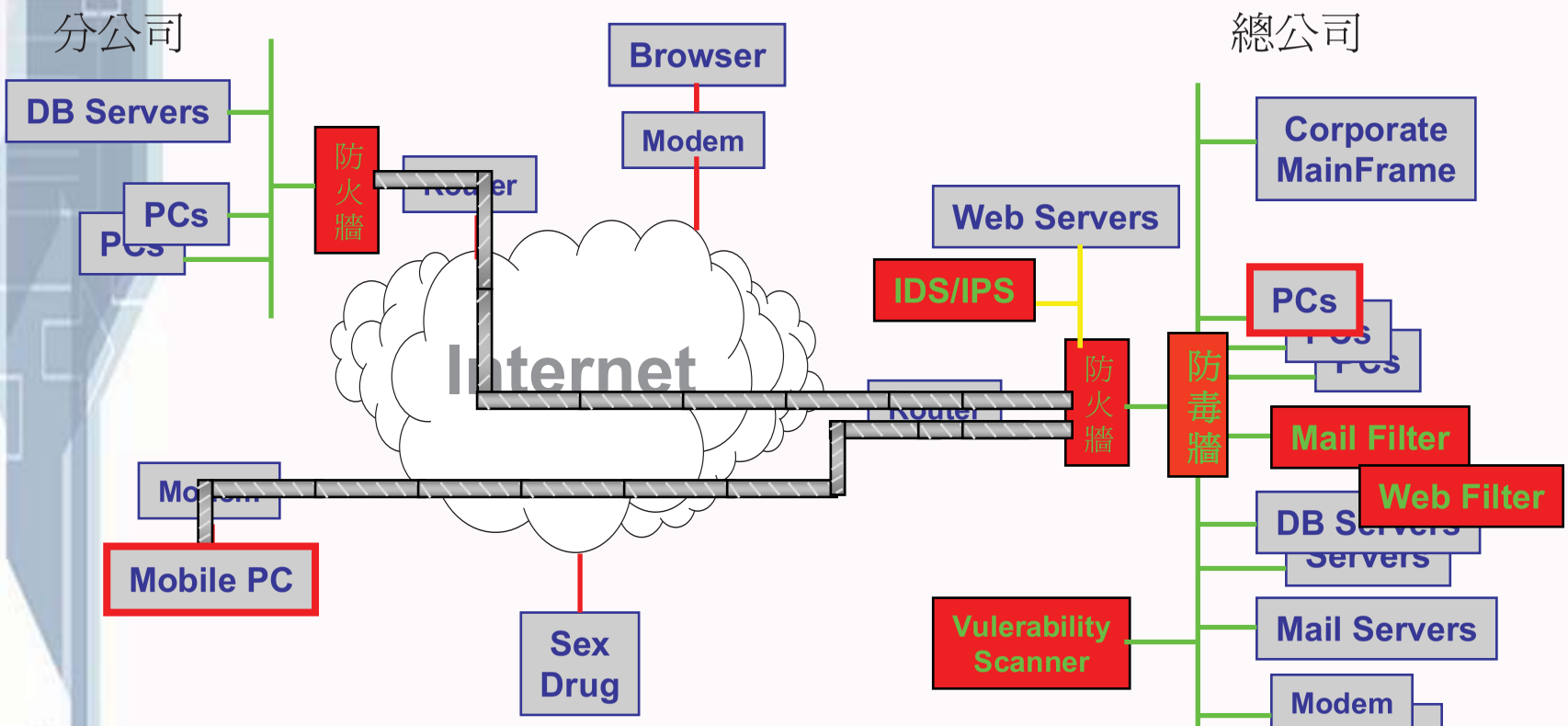
採用頻寬管理設備保障頻寬可用性



讓最重要的通訊最優先，最有保障

Stark Technology Inc.
敦陽科技股份有限公司

個人電腦的安全？

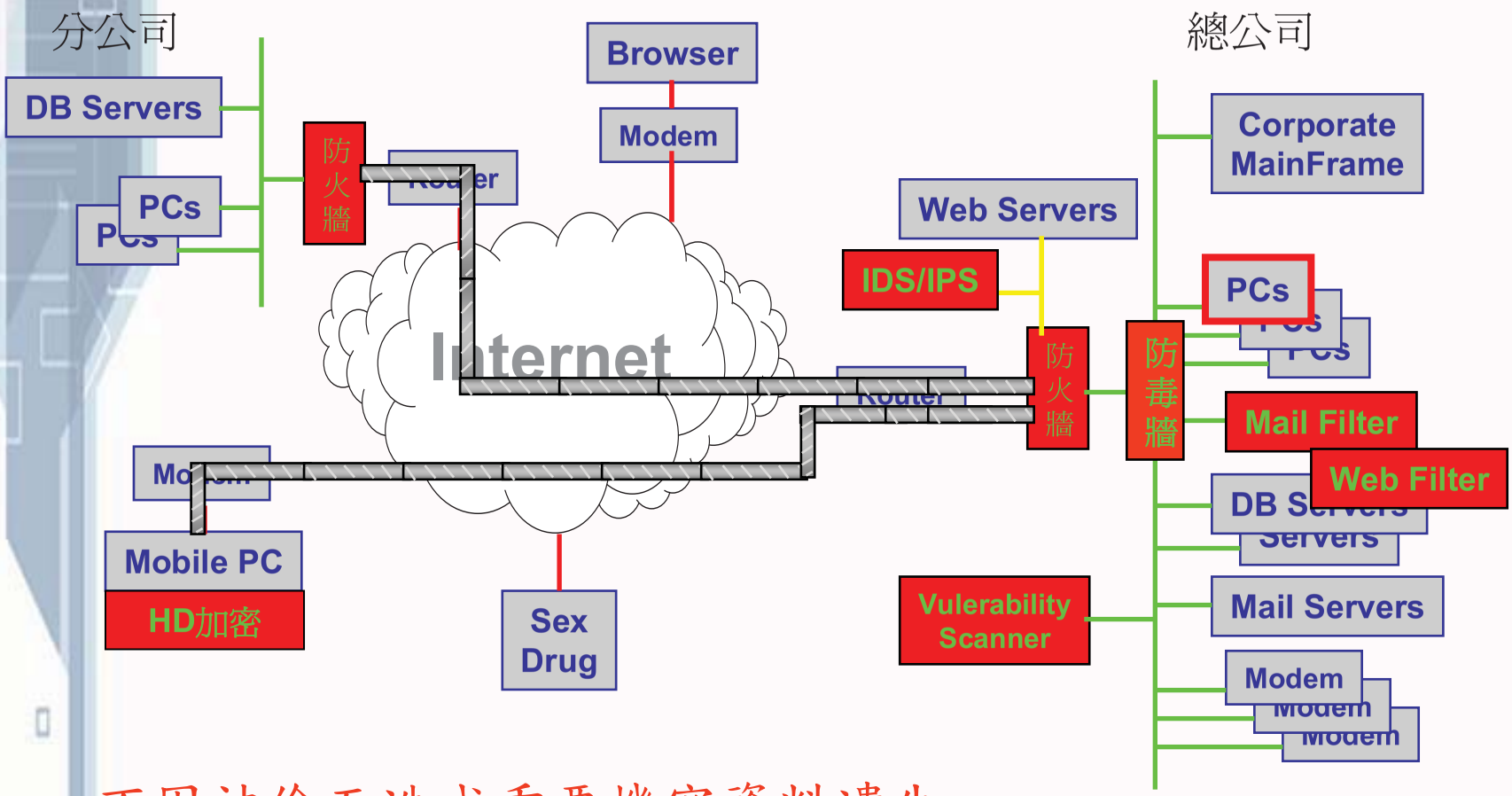


筆記型電腦或PDA被偷或遺失

PC成為駭客入侵的最佳跳板

Stark Technology Inc.
敦陽科技股份有限公司

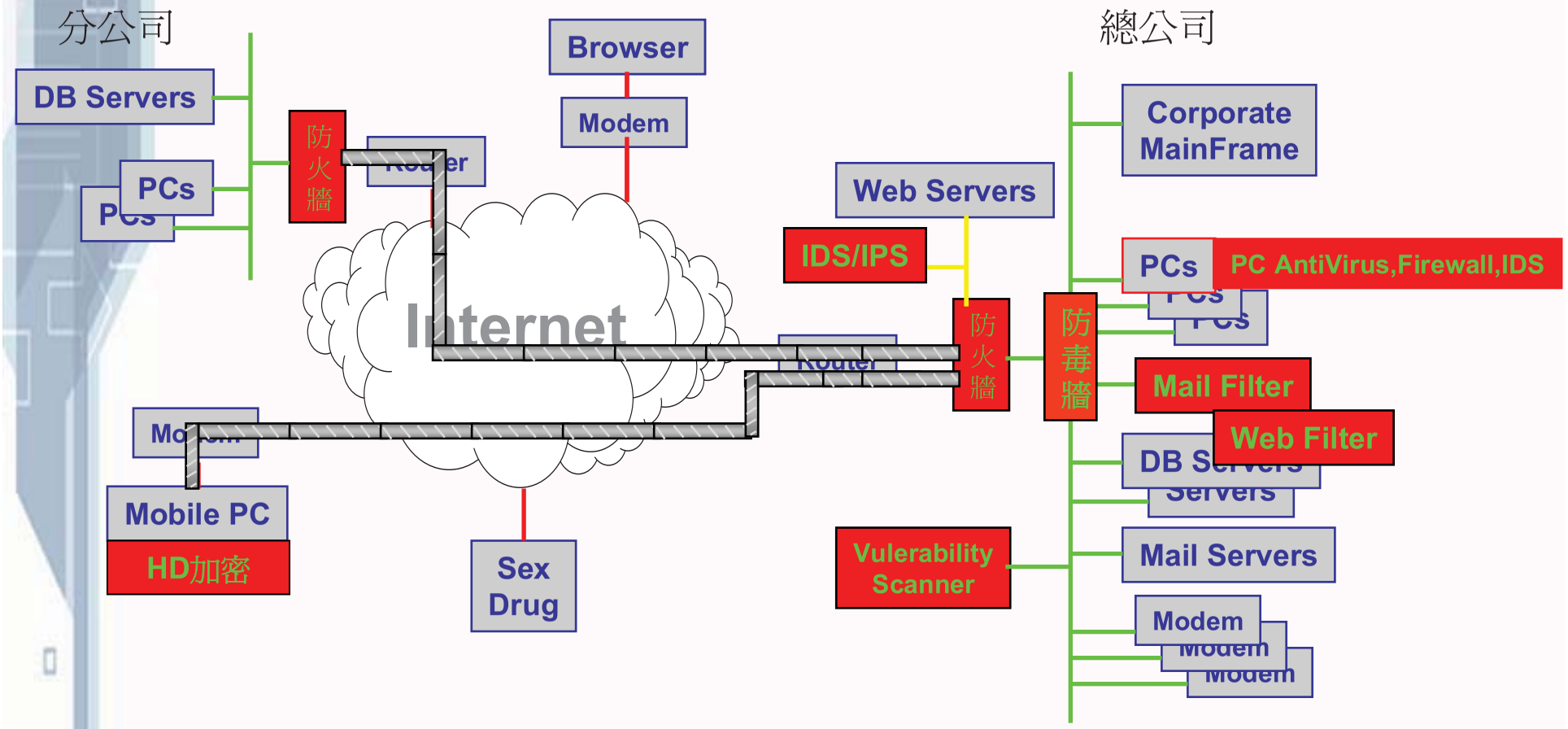
硬碟加解密系統保障可攜式媒體安全



不因被偷而造成重要機密資料遺失

Stark Technology Inc.
敦陽科技股份有限公司

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

Stark Technology Inc.
敦陽科技股份有限公司