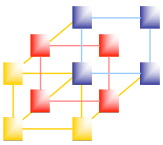
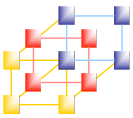
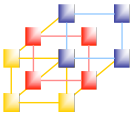


Unit 8
Intrusion Detection



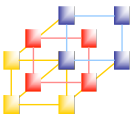
學習目的

- 網路的普及率逐年升高，網路服務的增加以及網路生活化，讓網路安全成為近年來熱門的研究主題之一。對於尚未被入侵的系統而言，防火牆是一道防線；然而，一旦系統遭到入侵，內部資源便無任何隱蔽性可言。因此入侵偵測系統(intrusion detection systems, IDS)成為系統的另外一項保障，寄望達到事前預防、增加網路安全層級。
- 入侵偵測系統的基本工作原理是從TCP/IP網路上偵測到入侵行為的特徵模式(signatures)，建立入侵偵測資料庫，利用模式比對方式，判別是否具有攻擊的意圖，並偵測出使用何種方法來入侵主機。



入侵偵測及入侵防禦系統概念

- 何謂入侵偵測系統
- 入侵偵測系統的種類
- 入侵偵測系統的限制
- 何謂入侵防禦系統
- 入侵防禦系統的種類
- 入侵偵測系統及入侵防禦系統之差異
- 集中式威脅管理簡介



何謂入侵偵測系統

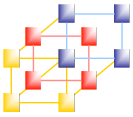
- Intrusion Detection System
- 入侵偵測(Intrusion Detection)就是對電腦網路和電腦系統的關鍵結點的資訊進行收集分析，偵測其中是否有違反安全策略的事件發生或攻擊跡象，並通知系統安全管理員。
- 一般把用於入侵偵測的軟體，硬體合稱為入侵偵測系統。

IDS能做些什麼

- 監控網路(NIDS)和系統(HIDS)
- 發現入侵企圖或異常現象
- 主動告警，通知系統管理者現在網路狀況
- 將網路封包紀錄下來以為未來辨識或作為證據之用

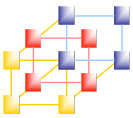
為什麼需要IDS

- 防火牆功能不足
  - 無法阻擋合法網路連結
  - 自身可以被攻破
  - 對於某些攻擊的保護很弱
  - 不是所有的威脅均來自防火牆外部
- 入侵很容易
  - 入侵教學隨處可見
  - 各種駭客工具垂手可得



防火牆防不到的攻擊

- 緩衝區溢位攻擊(Buffer Overflows)
- 通訊埠掃瞄攻擊(Port Scans)
- 木馬程式攻擊(Trojan Horses)
- 碎片封包攻擊(IP Fragmentation)
- 蠕蟲攻擊(Worms)
- 系統與應用程式漏洞攻擊(System & Application Vulnerabilities)



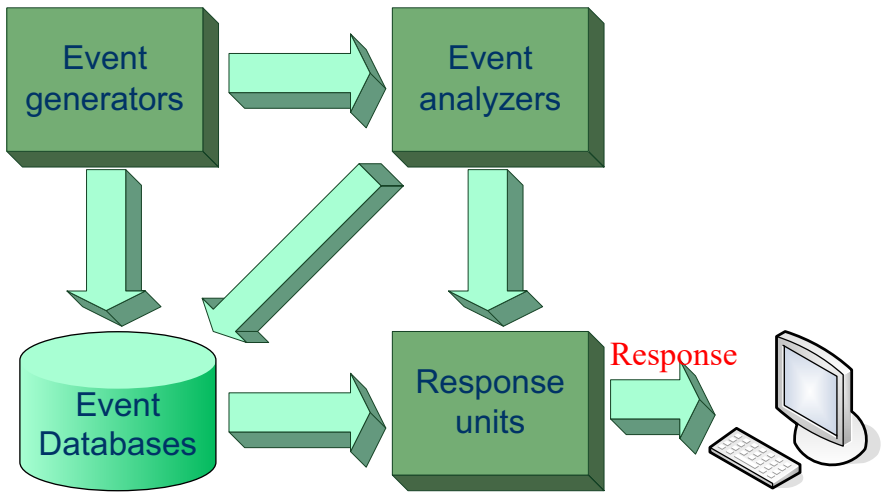
防毒軟體防不了的攻擊

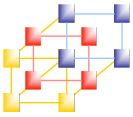
- 緩衝區溢位攻擊(Buffer Overflows)
- 通訊埠掃瞄攻擊(Port Scans)
- 系統與應用程式漏洞攻擊(System & Application Vulnerabilities)
- 阻斷服務與分散式阻斷服務攻擊(DoS/DDoS)

CIDF模型

- 為了提高IDS產品、組件及與其他安全產品之間的相互溝通，Common Intrusion Detection Frame闡述了一個入侵偵測系統（IDS）的通用模型。
- 元件：
  - 事件產生器（Event generators）
  - 事件分析器（Event analyzers）
  - 回應元件（Response units）
  - 事件資料庫（Event databases）

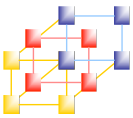
CIDF模型架構





入侵偵測系統之種類

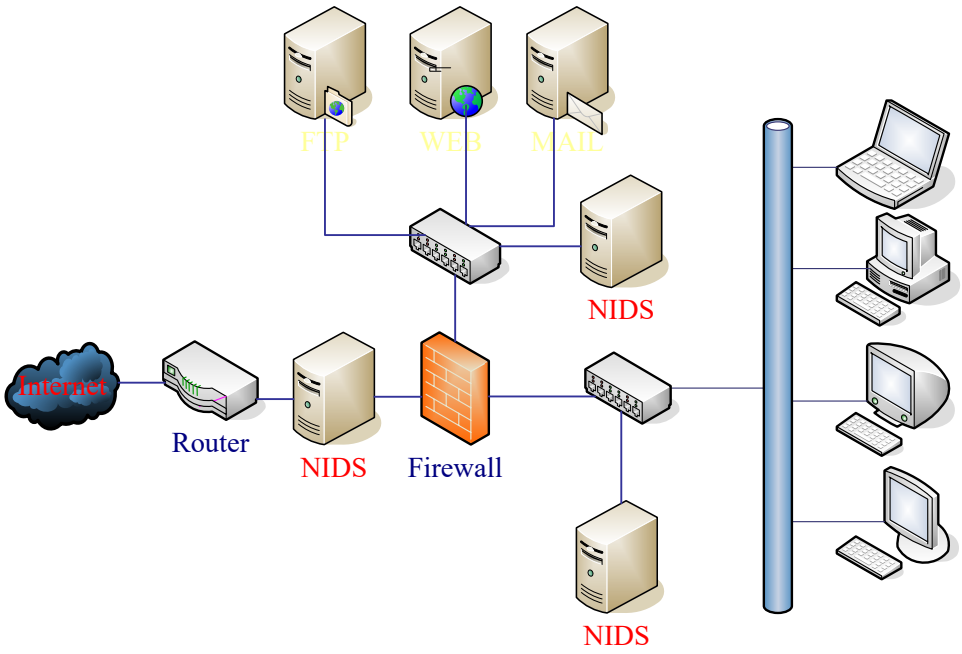
- 網路型入侵偵測系統Network-based IDS,簡稱NIDS
- 主機型入侵偵測系統Host-based IDS,簡稱HIDS
- 網路節點入侵偵測系統Network Node IDS,簡稱NNIDS



NIDS

- 安裝於被保護的網段中
- 雜亂模式監聽
- 分析經過這網段的所有封包
- 不會增加網段中主機的負載
- 產品：eTrust、Snort

NIDS範例



NIDS放置的位置

- 放在防火牆外：優點是IDS能夠看到所有來自Internet的攻擊者對系統的各種攻擊手段；缺點就是IDS的負荷會加重。
- 放在防火牆內：也有人認為應該把偵測器放在防火牆內，這樣可以用設置良好的防火牆把大部分的“幼稚腳本”阻止在防火牆外，而讓IDS把注意力集中在高水準的攻擊上。而且這樣可以把IDS保護在防火牆內，免於遭受攻擊。

NIDS放置的位置

- 防火牆內外都放IDS：如果組織的經費充足的話，可以在防火牆的內外都放IDS，這樣就可以得到以上兩種方法的優點。
- 這種情況下，一般放在防火牆內部的IDS是用來作為緊急告警的裝置。

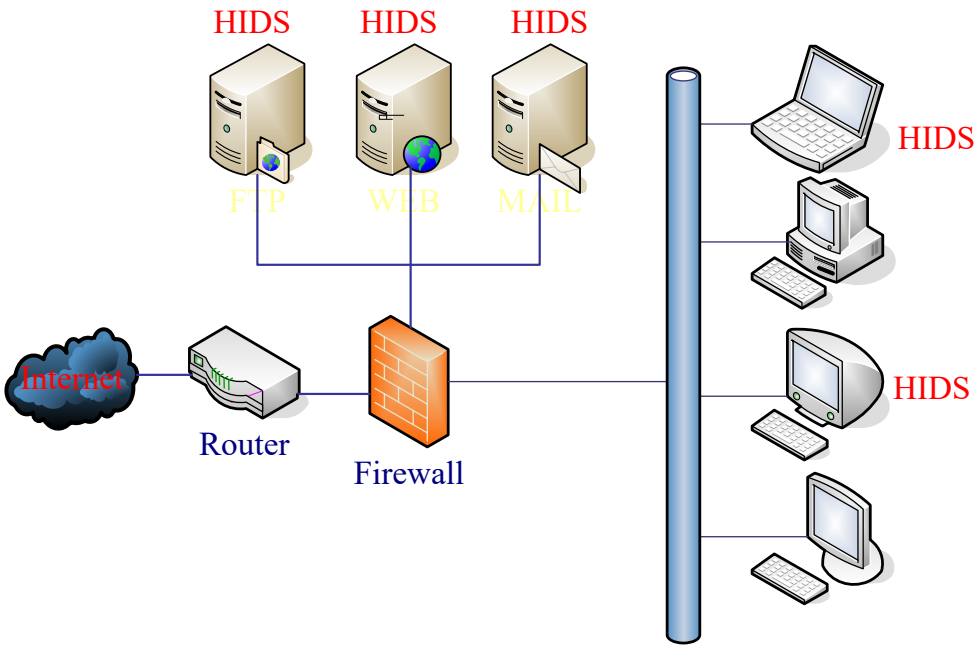
NIDS的優勢

- 花費較少
- 可分析封包
- 防止入侵的證據被移除
- 即時偵測和回應
- 不良意圖的偵測
- 不受作業系統影響

HIDS

- 安裝於被保護的主機中
- 主要分析主機內部活動
  - 系統LOG
  - 系統Process
  - 文件完整性檢查
- 佔用一定的系統資源
- 產品：Enterasys Dragon Host Sensor 、Tripwire

HIDS範例



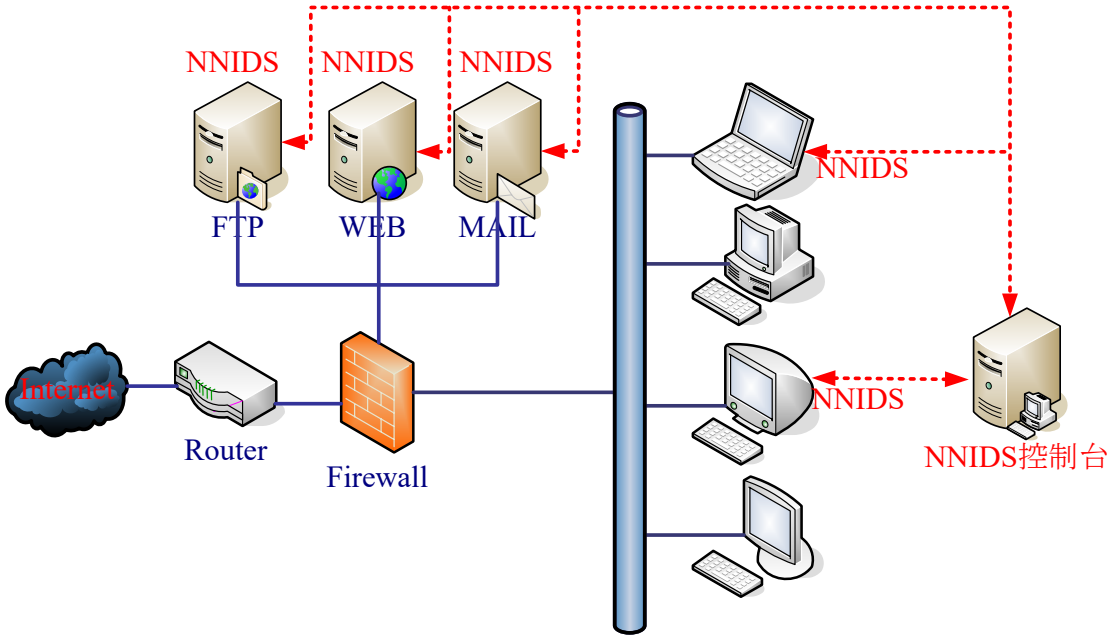
HIDS的優勢

- 可確認攻擊是成功的
- 監控系統特定的活動
- 可偵測加密封包及交換網路環境中的攻擊
- 監控系統關鍵部份
- 不須新增額外硬體

NNIDS

- Network Node IDS也稱作Stack-Based IDS
- 安裝於網路節點的主機中
- 結合了NIDS及HIDS的技術
- 適合於高速網路環境：NIDS因為效能的關係，在高速網路下是不可靠的，因為有很高比例的封包會被丟棄，而且交換型網路經常會妨礙NIDS看到的封包。NNIDS將NIDS的功能委托給單獨的主機，進而解決了高速網路和交換網路的問題。
- 產品：BlackICE Agent 、Tiny personal firewall with CMDS、ISS RealSecure Desktop Protector

NNIDS範例



IDS的偵測技術

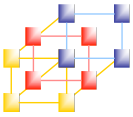
- 基於特徵（Signature-based）
  - 維護一個入侵特徵的資料庫
  - 準確性較高
- 基於異常（Anomaly-based）
  - 統計模型
  - 專家系統
  - 誤報較多

IDS的限制

- 沒有主動防禦的能力：IDS只有告警的能力，無法主動防禦入侵行為。
- 誤報率偏高：目前多數的IDS利用特徵資料庫以判斷是否為入侵行為，但有些正常封包的特徵和入侵行為的特徵十分類似，但修改特徵資料庫之後又造成漏報。
- 漏報率偏高：目前的IDS系統還無法有效的識別出未知的入侵，也就是造成安全假象。

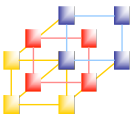
IDS的限制

- 性能普遍不足：現在市場上的IDS產品多依賴單一主機，因現今網路流量十分龐大，這種IDS產品已不能適應交換網路技術和高頻寬環境的發展，一旦資源耗盡，就無法運作了。
- 加密封包無法辨識：越來越多攻擊用加密封包，使得IDS監控網路流量的能力產生盲點，因IDS是擷取網路封包進行分析的，如果封包加密，就無法辨識其內容，也就無法進行分析。



何謂入侵防禦系統

- Intrusion Prevention System
- 可視為IDS功能的延伸，用以彌補IDS功能之不足
- 可主動偵測入侵行為並主動防禦
- 其餘的限制性與IDS相同



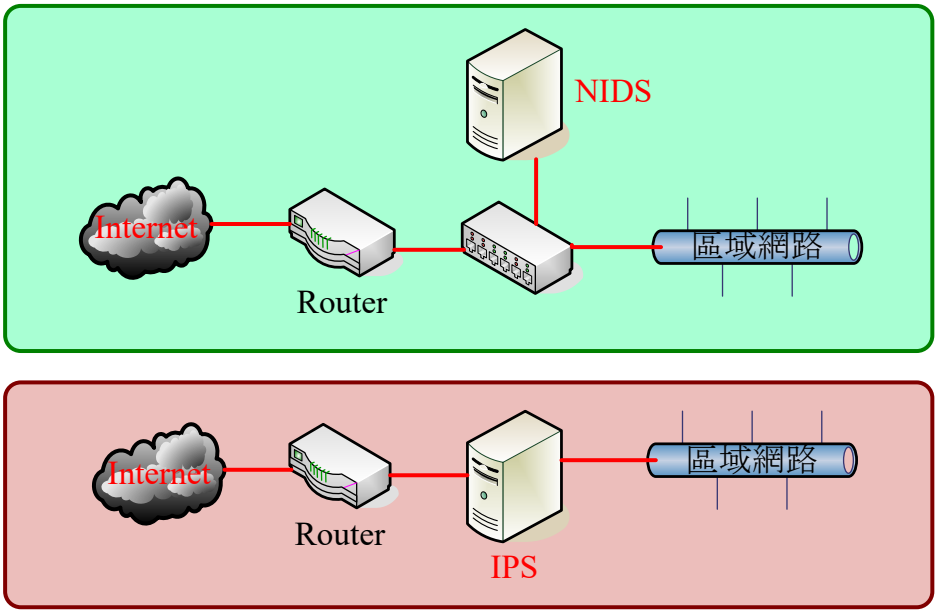
入侵防禦系統之種類

- 主機型入侵防禦（HIPS）：用於保護伺服器和主機系統不受入侵行為的攻擊
- 網路型入侵防禦（NIPS）：透過偵測流經的網路流量，提供對網路的安全保護，一旦辨識出入侵行為，NIPS就阻斷該網路連線
- 應用型入侵防禦（AIPS）：將主機型的入侵防禦擴展成為位於應用伺服器之前的資訊安全設備，主要針對應用程式的攻擊進行防禦。

入侵偵測系統及入侵防禦系統之差異

- 傳統的網路IDS(NIDS)系統用於被動地監測網路，根據規則資料庫和策略來尋找異常行為並提出告警訊息。如果NIDS突然出現故障，業務並不受影響，網路封包依然繼續流動，只是無法針對異常行為告警而已，故障對用戶是透明的。
- IPS系統是主動的在線設備，能丟棄攻擊的網路封包，或者在網路封包到達主機前切斷連線，如果出現故障，將影響到整個網路連線。

NIDS與IPS之差異



UTM簡介

- 集中式威脅管理(Unified Threat Management)
- NSS的定義www.nss.co.uk/utm/introduction.htm，UTM設備必須符合「可支援防火牆、VPN、IPS、內容過濾（Virus、Web、Mail、Spyware）等功能的單一設備」
- IDC（國際數據資訊）的定義，UTM設備至少要具備防火牆、VPN、ID&P和閘道防毒等4種功能

UTM優缺點

- 優點：整合多種功能在一台硬體設備，減少不同建案時期建置之設備所發生的設備衝突或不同廠商技術支援的整合性問題。
- 缺點：UTM設備強調多合一，產品功能之完整度與彈性，比不上單一功能的專屬設備。
- 產品：Fortinet FortiGate、ISS Proventia M10E、SonicWALL Pro4100 、友旺SV2000 、ZyXEL ZyWALL 70 UTM、臨通NS-720

UTM部署模式

- 路由模式(Routing Mode)：替換掉原有網路設備及資安設備
- 透通/橋接模式(Transparent/Bridge Mode)：不更動原有網路架構，保留原有資安設備
- 代理模式(Proxy Mode)：最能完整檢查網路流量，但DNS或員工電腦要配合修改設定值，同時傳輸效能一定會受到影響