Module 12 ： 網路安全架構

學習目的

1. 在新的商業型態、降低銷售成本、提升客戶服務方面，Internet具有極大的潛力，但在企業組織的資訊和系統方面，也可能會增加極大的風險。然而只要具有適當的安全架構，也可以賦予Internet極大的效用，且可用來管理資訊和系統的風險。
2. 在逐步規劃組織Internet連線的通訊架構時，最重要的就是流量處理能力和可用性問題。在某些情況下，必須和組織的ISP討論流量處理能力的問題，以建構適當的網路通訊架構，以確保安全的網路環境，提供穩定的網路服務

3. 本課程模組將教導學生設計規劃DMZ系統以落實組織的安全政策，同時做好NAT服務的規劃建置，提供部分安全的功能。
4. 本模組共有三個小節包括(1)網路通訊架構(2)設計DMZ (3)網路轉址NAT服務(4)專案實作，共須三個鐘點。

Module 12 ： 網路安全架構

Module 12-1：網路通訊架構(*)

Module 12-2：設計DMZ(*)

Module 12-3：網路轉址NAT服務(**)

Module 12-4：專案實作(*)

* 初級(basic):基礎性教材內容
**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
***高級(advanced):適用於深入研究的內容

Module 12-1：網路通訊架構(*)

網路通訊架構

- 企業/組織/學校希望從網際網路獲得什麼資訊？
- 企業/組織/學校希望提供什麼服務？
- 企業/組織/學校服務的對象是誰？

網路通訊架構

- 企業/組織/學校最常提供的服務為
  - mail、web、dns…
- 服務對象除了內部網路存取外，也提供外部網路存取相關資源

網路通訊架構

- 郵件伺服主機
  - 至少一台郵件主機作為收發信件之用
  - 可建置接收內送郵件伺服器與外寄郵件伺服器
  - 提供郵件加密

網路通訊架構

- 網頁伺服主機
  - 對外網頁服務，讓任何人瀏覽
  - 加密或認證機制

網路通訊架構

- 內部網路存取
  - 允許/不允許的服務
  - 特定的網站瀏覽
  - 監控/規範/原則

網路通訊架構

- 內部網路存取
  - HTTP(80、443)
  - FTP(20、21)
  - telnet(23)、ssh(22)
  - Pop3(110)、smtp(25)

網路通訊架構

- 外部網路存取
  - 允許/不允許的服務
  - DMZ原則
  - 防火牆規範
  - 外部網路/DMZ/內部網路存取控制

網路通訊架構

- 外部網路存取
  - 僅開放公眾服務，如http
  - 如要從外部存取至內部網路，需透過VPN或其他撥號方式

Module 12-2：設計DMZ(*)

什麼是DMZ？

- DMZ-Demilitarized Zone
  - 中文翻譯：隔離區、非軍事化區…
  - 意指不能完全信任的網段
- DMZ泛指內部網路和外部網路之間的緩衝地帶

DMZ定義

- 一般而言，只要外部使用者可以直接接觸到的系統，都應該架設在DMZ內
  - 對外的服務，如web、ftp等接須建置在DMZ內，避免受到入侵時受到嚴重的威脅
  - 這類放置在DMZ內的對外服務，若要存取內部網路則必須限定存取能力以及其他安全規則(例如只允許內部網域存取DMZ)

架設DMZ

- 架設DMZ前須有下列前置動作
  - 災難復原與備份
  - 建置在DMZ內的服務
  - 內部網路與DMZ之間的網路架構、規則政策

架設DMZ(續)

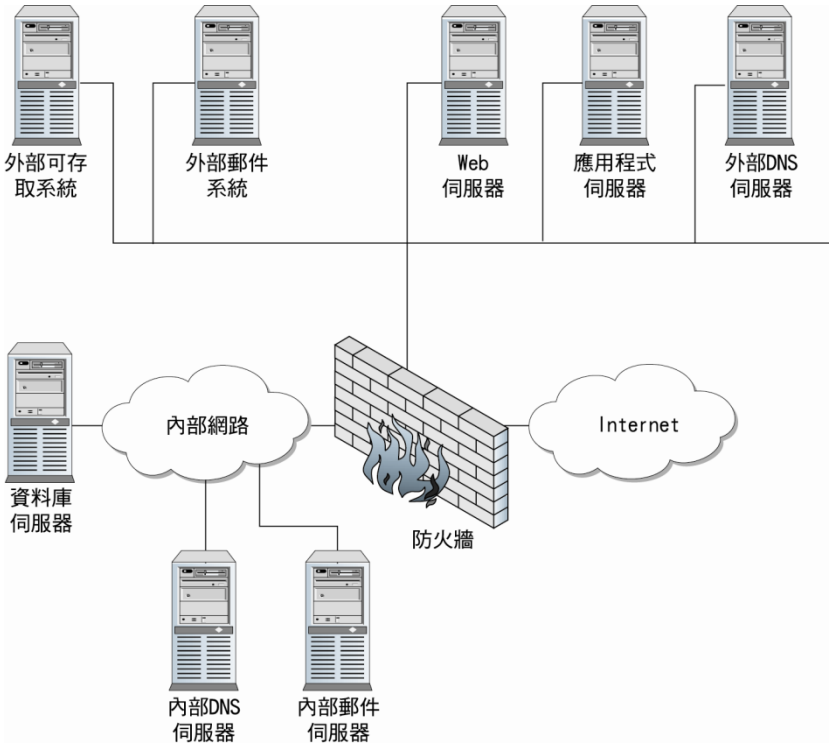
- 架設DMZ前須有下列前置動作
  - 災難復原與備份
    - 異地備援機制
    - 稽核系統運作
    - 風險與攻擊
      - 潛在弱點與潛在風險，包含人為疏失、天然災害...
  - 建置在DMZ內的服務
  - 內部網路與DMZ之間的網路架構、規則政策

架設DMZ(續)

- 架設DMZ前須有下列前置動作
  - 災難復原與備份
  - 建置在DMZ內的服務
    - 允許公眾存取的服務
      - web、mail、ftp、dns、ntp應用程式、外部可存取的系統…
      - 存取原則：外部存取DMZ的服務，DMZ服務也僅能被動的從內部網路接受資料，而非主動要求
      - 嚴禁外部使用者存取內部系統
  - 內部網路與DMZ之間的網路架構、規則政策

架設DMZ(續)

- 架設DMZ前須有下列前置動作
  - 災難復原與備份
  - 建置在DMZ內的服務
  - 內部網路與DMZ之間的網路架構、規則政策
    - 定義內部網路、外部網路與DMZ服務
    - 定義規則與防火牆策略



DMZ系統和內部網路系統的規劃圖
(來源：資訊安全[學貫行銷股份有限公司])

DMZ架構

- DMZ架構應視環境需求與狀況加以設計並判斷，不一定每一類型架構適合
- 建立DMZ首重建置防火牆，利用防火牆的特性隔離內外網路，提供DMZ區域和保護能力

DMZ架構(續)

- 談DMZ架構前，先了解防火牆特性
  - 為什麼需要防火牆？
  - DMZ與防火牆之間的關係？
  - 網路流量、架構與服務的增加
  - 資料安全性考量
  - 安全無慮的網路環境
  - 造成駭客的興起

DMZ架構(續)

- 防火牆的功能?!
  - 在不同網路之間，實作安全政策
  - 具有強制功能，僅允許符合規則的連線
  - 架設在網路的主要出入口，集中風險，提高監控的便利與安全性
  - 搭配入侵偵測系統，阻擋惡意及非法的使用者
  - 能完整實作DMZ

DMZ架構(續)

- 防火牆的考量?
  - 降低威脅
  - 對外的服務
  - 對內的服務
  - 分辨服務的使用者
  - 管理防火牆
  - 未來發展與網路規劃

DMZ架構(續)

- 防火牆的優點?
  - 集中風險
  - 搭配入侵偵測系統(IDS)

DMZ架構(續)

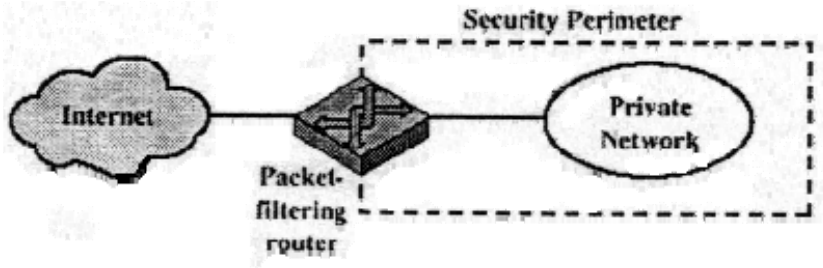
- 防火牆的限制?
  - 無法保護bypass的攻擊
  - 無法防止內部攻擊
  - 防火牆管不到不經過他的連線
  - 防火牆無法防範病毒爆發

DMZ架構(續)

- 防火牆種類
  - 封包過濾防火牆 (Packet Filtering)
  - 應用層閘道式防火牆 (Application-Level Gateway)
  - 電路層(環繞)閘道式防火牆 (Circuit-Level Gateway)

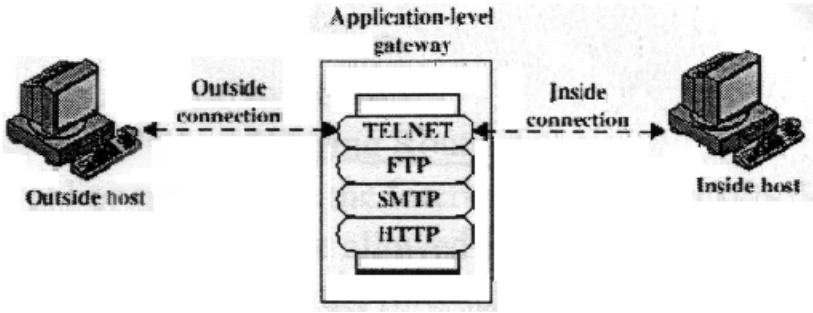
DMZ架構(續)

- 防火牆種類-Packet Filtering
  - It applies a set of ***filtering rules*** to each incoming IP packet and then forwards or discards the packets
  - **Filtering rules** are based on fields in the IP and Transport headers
    - Source IP address
    - Destination IP address
    - Transport port number
  - Advantages: simplicity
  - Disadvantages:
    - Difficulty of setting up filtering rules correctly
    - Lack of authentication



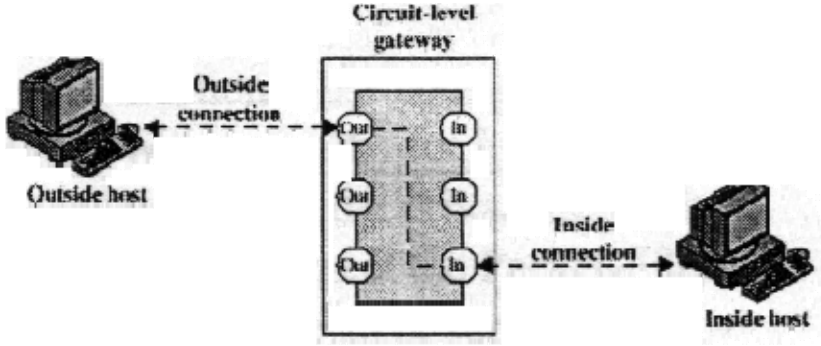
DMZ架構(續)

- 防火牆種類-Application-level Gateway
  - The user contacts it using a TCP/IP application and it asks the user for the name of the remote host to be accessed.
  - When the user is authenticated, it contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
  - If it does not implement the proxy code for a specific application, the service is not supported and cannot be forward across it.
  - Advantages: more secure than packet-filtering router
  - Disadvantages: Additional processing overhead on each connection.



DMZ架構(續)

- 防火牆種類-Circuit-Level Gateway
  - It sets up two TCP connections
  - It ←→inner TCP user
  - It ←→outside TCP user
  - It acts as a relay of TCP segment from one connection to the other
  - Advantages: flexibility
  - Disadvantages: less secure

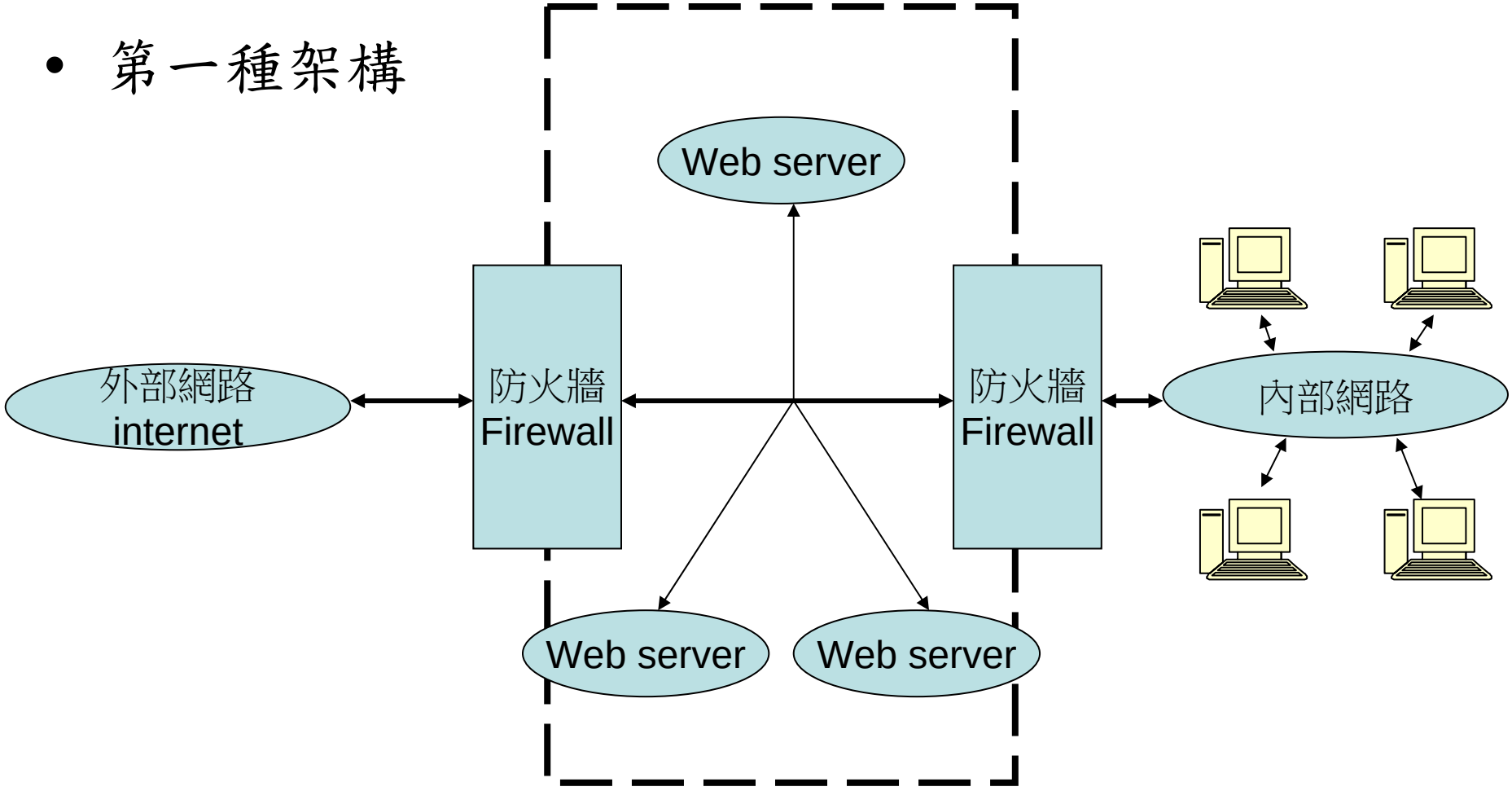


DMZ架構(續)

- 關於防火牆的基本安全政策
  - 管理防火牆的風險
  - 從你所保護的網路中,對不信任網域所開啟服務
  - 從你要保護的網路中,對不信任網域所要求的服務
  - 實體上所有進出網路的連線,都一定要經過防火牆

DMZ架構(續)

- 第一種架構



DMZ架構(續)

- 第一種架構
  - 架構中，左方為網際網路(外部區域)，直接連結至DMZ
  - DMZ中提供公開服務，如web、mail…
  - DMZ後方也是連結防火牆，分隔內部網路與DMZ中的網域
  - DMZ中的服務有獨立的防火牆保護
  - 左方防火牆規則為DMZ和內部網路流量存取保護
  - 右方防火牆規則為僅允許內部網路對外存取

DMZ架構(續)

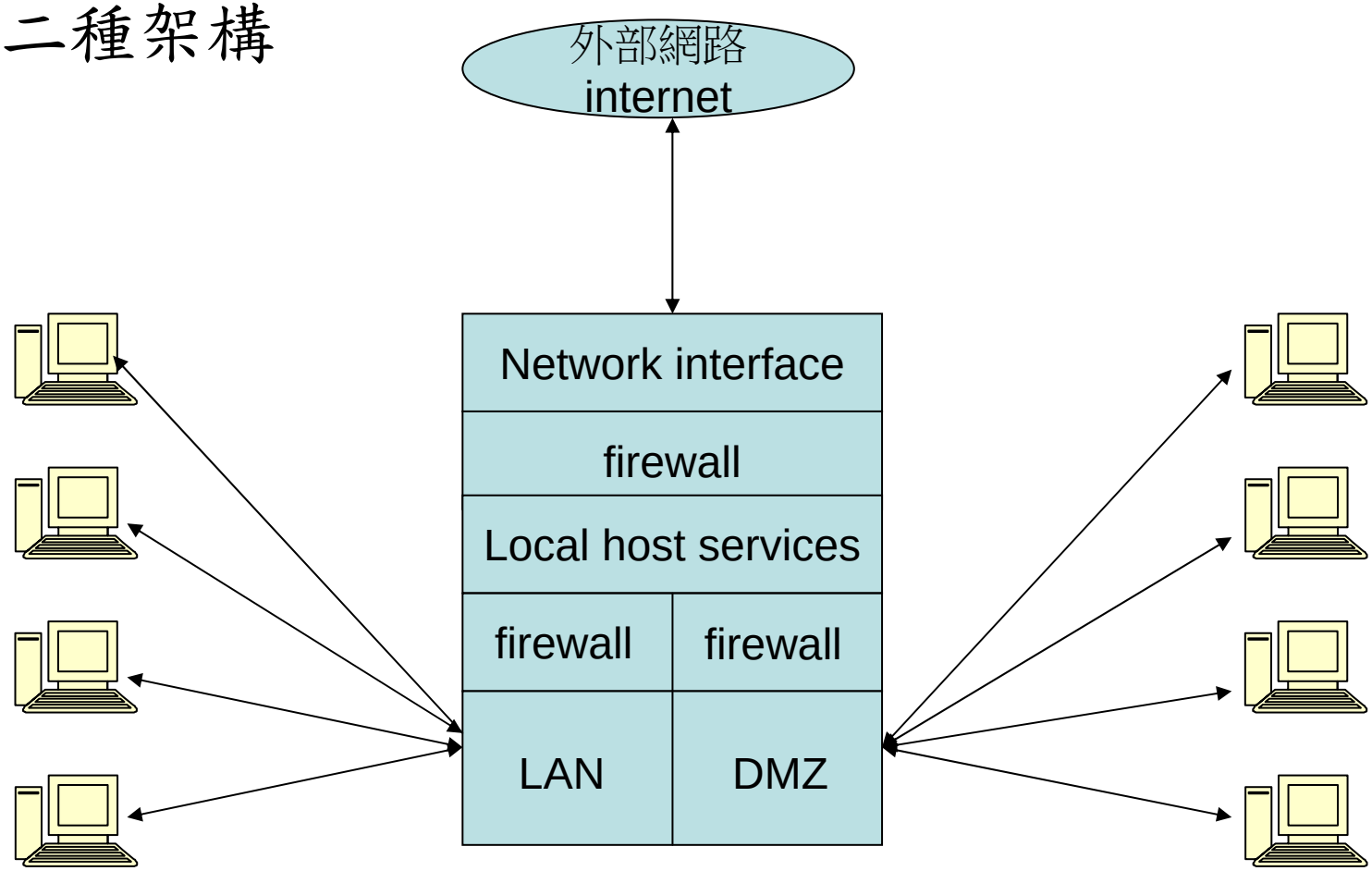
- 第一種架構優點
  - 外層防火牆或其中一台伺服器淪陷時，至少還有一層內部防火牆保護，其餘伺服器也有各自防火牆阻擋
  - 防火牆管理複雜度低
  - 二個防火牆可以是不同類型的防火牆
  - 增進整體架構的安全性

DMZ架構(續)

- 第一種架構缺點
  - 如有大量的頻寬需求，外部防火牆須有處理大量資料的能力
  - 建置成本較高
  - 內部網路與網際網路之間的傳輸會通過DMZ
  - 內部網路對外需經過二層防火牆

DMZ架構(續)

- 第二種架構



DMZ架構(續)

- 第二種架構
  - 架構中，一個連接外部網路，另一個連接DMZ，最後一個連接內部網路
  - DMZ中提供公開服務，如web、mail…
  - LAN和DMZ各自 單獨對外部網路傳輸

DMZ架構(續)

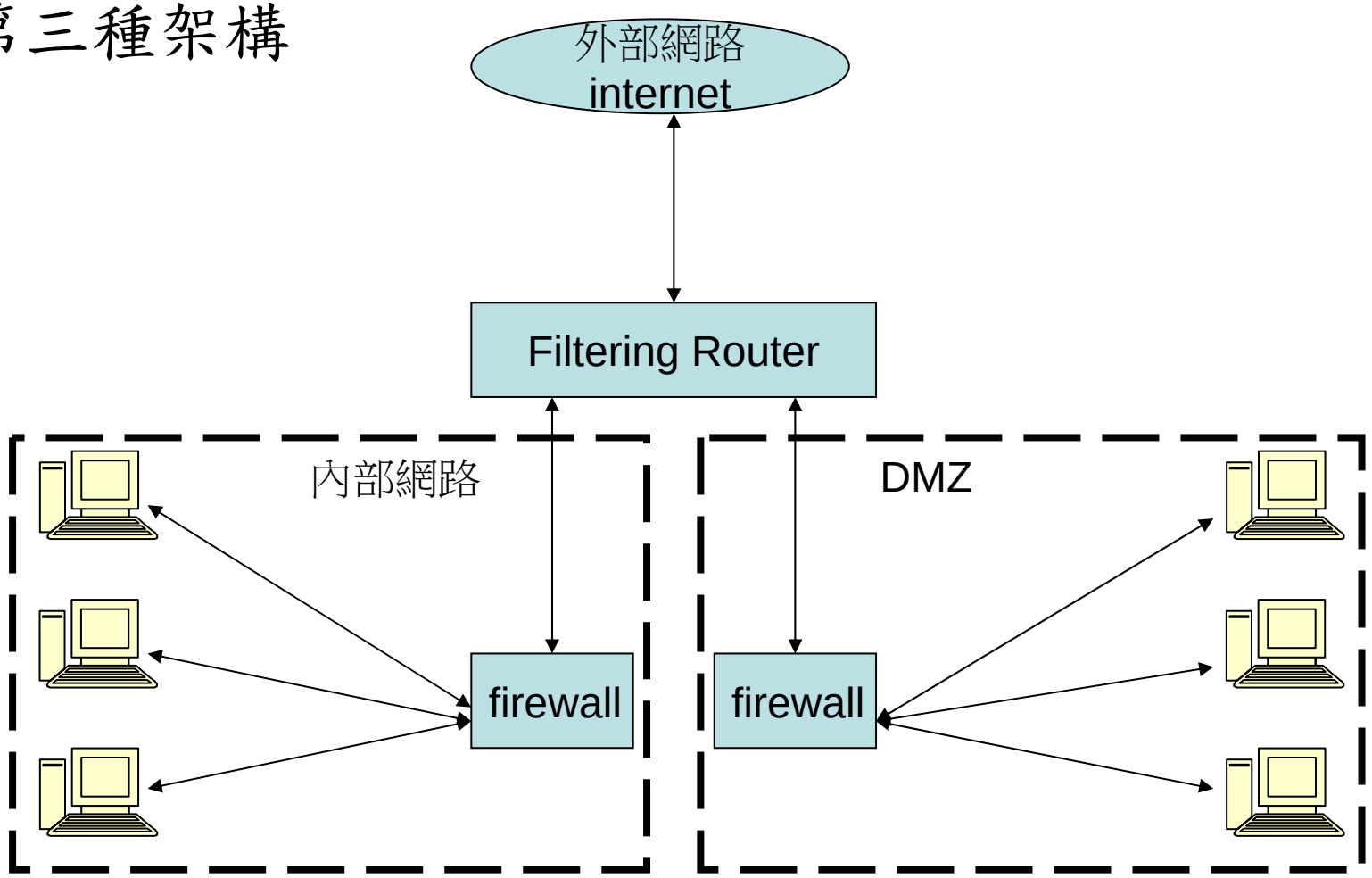
- 第二種架構優點
  - 建置便宜
  - DMZ和內部網路不會佔用彼此頻寬
  - 區別容易

DMZ架構(續)

- 第二種架構缺點
  - 對外層防火牆來說，內部網路與DMZ對外流量將是一個瓶頸
  - 為符合安全需求，內部網路與DMZ設定將會更複雜
  - 後續維護不易

DMZ架構(續)

- 第三種架構



DMZ架構(續)

- 第三種架構
  - 在內部網路與DMZ之上增加filtering router
  - Filtering router為內部網路和DMZ執行基本過濾功能

DMZ架構(續)

- 第三種架構優點
  - 任一防火牆如有問題，將不影響另一端防火牆
  - DMZ和內部網路不會佔用彼此頻寬
  - Filtering router可提供基本過濾功能，減輕防火牆負擔

DMZ架構(續)

- 第三種架構缺點
  - 建置成本較高
  - 為安全需求，雙防火牆以及filtering router設定將比前二者複雜

DMZ架構(續)

- 架構考量
  - 效能
  - 可靠度
  - 安全性
  - 花費
  - 維護設定
  - 功能

DMZ!?

- DMZ設計是否優良，主因在於DMZ與內部網路之間網路流向的控管，理想上DMZ只能被動從內部網路接受資料，不能主動向內部網路要求資料，如此一來DMZ被入侵之後也不會波及內部網路
- 設計考量及在於風險與威脅之間的配置，給外界internet存取的資料機密性低，威脅卻高，內部網路的資料機密性高，所以要提高提安全性，降低風險
- DMZ設計和運作比較複雜,但是提供較多樣化和較高的安全性

Module 12-3：網路轉址(NAT)服務(*)

網路轉址NAT服務(續)

- 什麼是NAT？
  - NAT=network address translation
  - 簡而言之，NAT是讓多台電腦可以共用一個IP上網的一種技術
  - NAT一般配合虛擬IP一同使用
  - 目前作業系統，如windows 2000、windows 2003、linux、freebsd等皆支援NAT
  - 大型router、switch(layer3以上)皆支援NAT
  - 市售產品如IP分享器接支援NAT

網路轉址NAT服務(續)

- NAT優點
  - 由於只使用少數IP對應後端電腦，因此大幅減少實體IP的使用量
  - 內部網路IP可重複在不同環境下使用
  - 只有實體IP才會被外部存取，因此在內部虛擬IP網段內安全度大為提升

網路轉址NAT服務(續)

- NAT缺點
  - NAT如節點失效，將影響全部環節
  - 應用程式服務有可能無法執行
  - NAT效能與流量將考驗機器的存活度
  - NAT無法提供完整的攻擊防護
  - NAT不能與點對點安全的傳輸模式IPSec共存

網路轉址NAT服務(續)

- 為什麼需要NAT？
  - Ipv4的位址幾乎不夠用，在此情形下，ip的配給將越來越少
  - 需要大量IP需求的單位，如企業或學校將在有限的IP中提供管理IP位址
  - 安全防護考量下，NAT可提供簡易的防護措施

網路轉址NAT服務(續)

- NAT帶來什麼好處？
  - 一旦設定完成，由外部探勘也僅能探查到防火牆的資訊或IP位址
  - 外界無法直接存取NAT之後的網路
  - 大部分防火牆或router皆可設定NAT，無須另外購置設備

網路轉址NAT服務(續)

- 私人網域空間

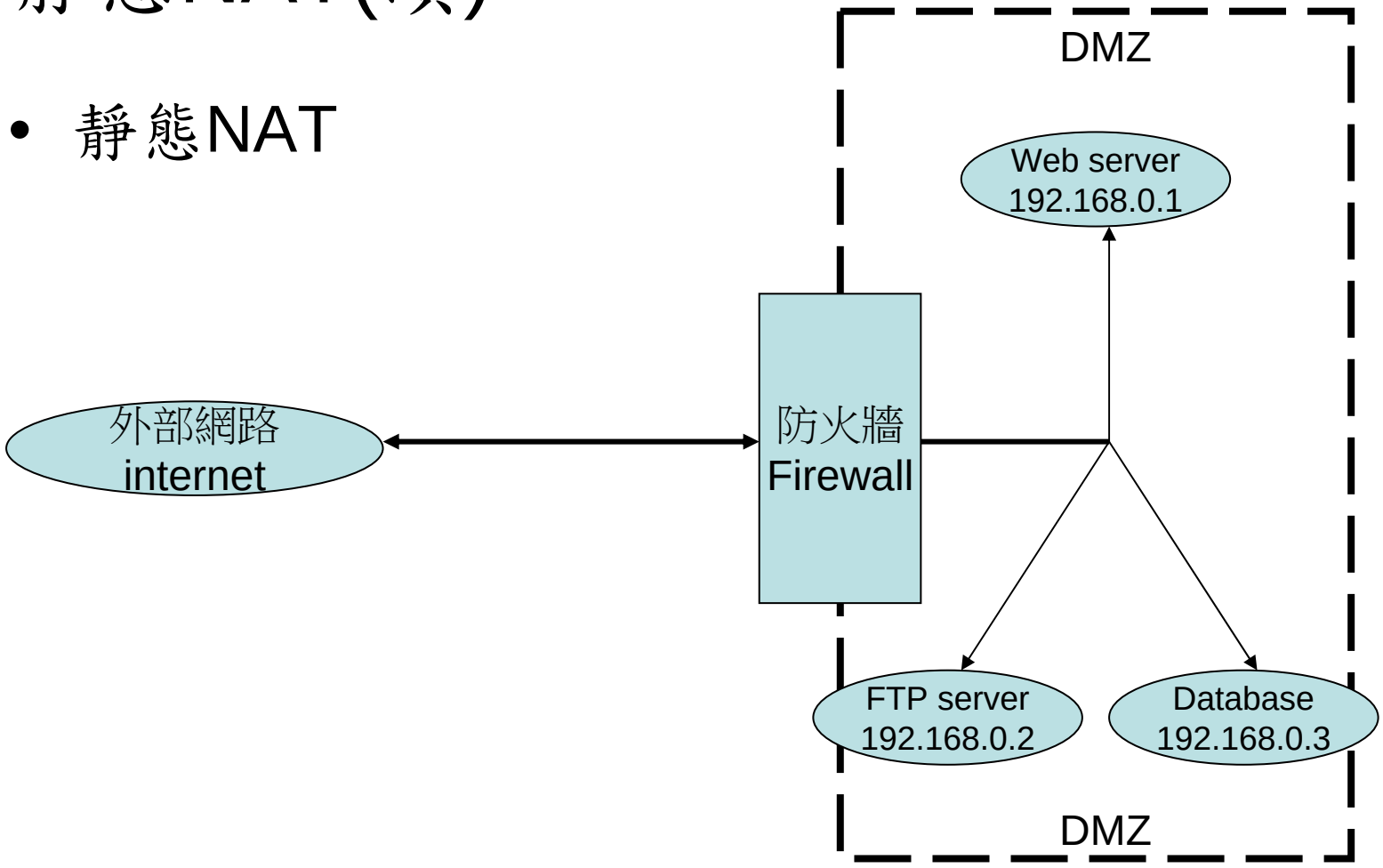
Range / Class	Start IP	End IP
Class A	10.0.0.0	10.255.255.255
Class B	172.16.0.0	172.31.255.255
Class C	192.168.0.0	192.168.255.255

靜態NAT

- 靜態NAT
  - 採用靜態NAT，則外部網路可存取NAT內特定系統
  - 可將真實IP對應至DMZ的設備或服務

靜態NAT(續)

- 靜態NAT



由外部存取一真實IP → 防火牆將位址轉換成伺服器內部網址，例如192.168.0.1

靜態NAT(續)

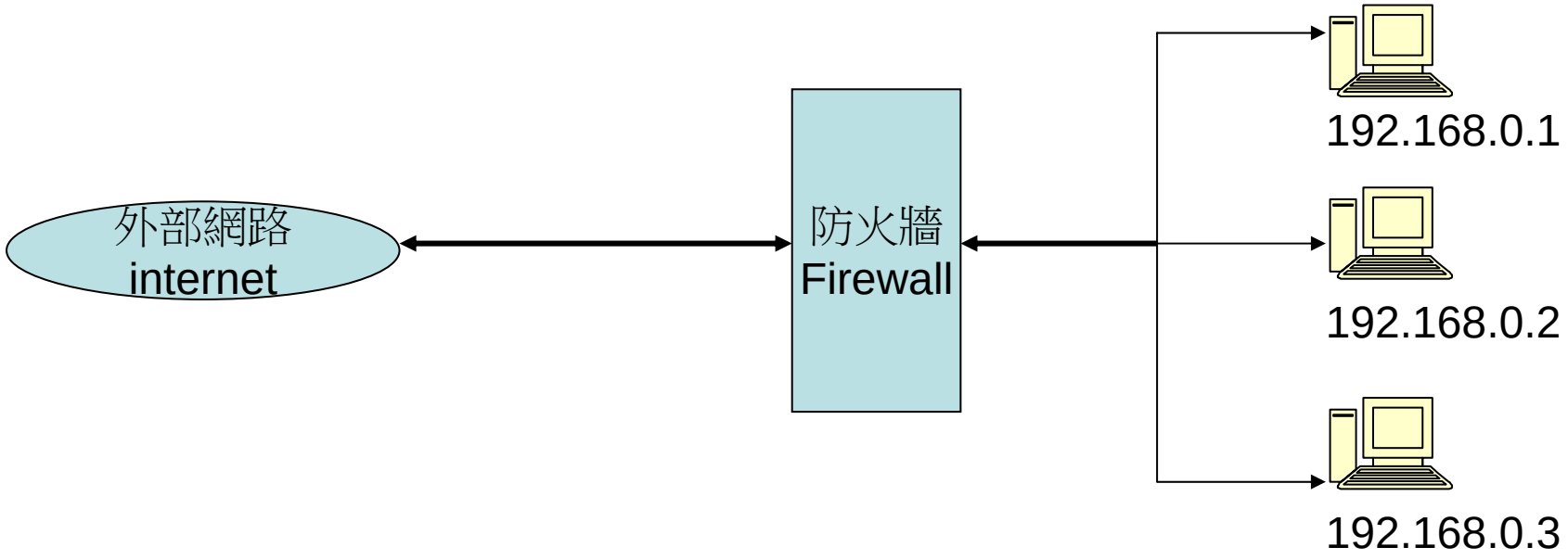
- 靜態NAT
  - 靜態NAT是採用一對一單一組態設定，針對外部網路來說，也只需要一個位址
  - 以上張投影片來說，應用伺服器(database)並不需要外部網路存取，其所在的DMZ位址僅提供給web server互動

動態NAT

- 動態NAT
  - 將多個私有IP位址，可轉譯為相同一個合法IP位址
  - 防火牆會為每一個連線開起一個連接埠
  - 在轉譯的過程中會動態產生一組NAT mapping table，其目的除了讓後續的封包依循一致的轉譯方式外，並用於解析返回的IP封包，做為判讀反轉置換邏輯之依據

動態NAT(續)

- 動態NAT



防火牆接到此流量
將虛擬IP轉換成外部網路位址
連接埠將由防火牆指派在送到外部網路

內部網路以虛擬IP對外連線

動態NAT(續)

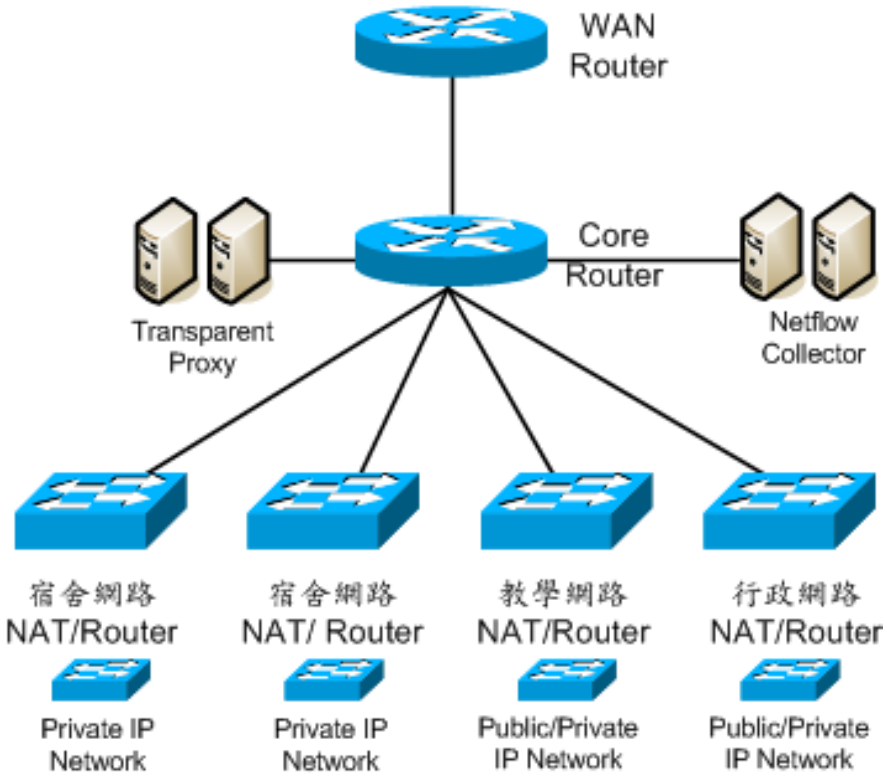
- 動態NAT
  - 實務上動態NAT最多只能同時允許大約64000個連線需求
  - 若採行DHCP分發IP，則動態NAT將十分符合此環境

NAT架構規劃

- NAT架構大部分有下列二種方式
  - 分散式架構
  - 集中式架構

NAT架構規劃(續)

- 分散式架構



NAT架構規劃(續)

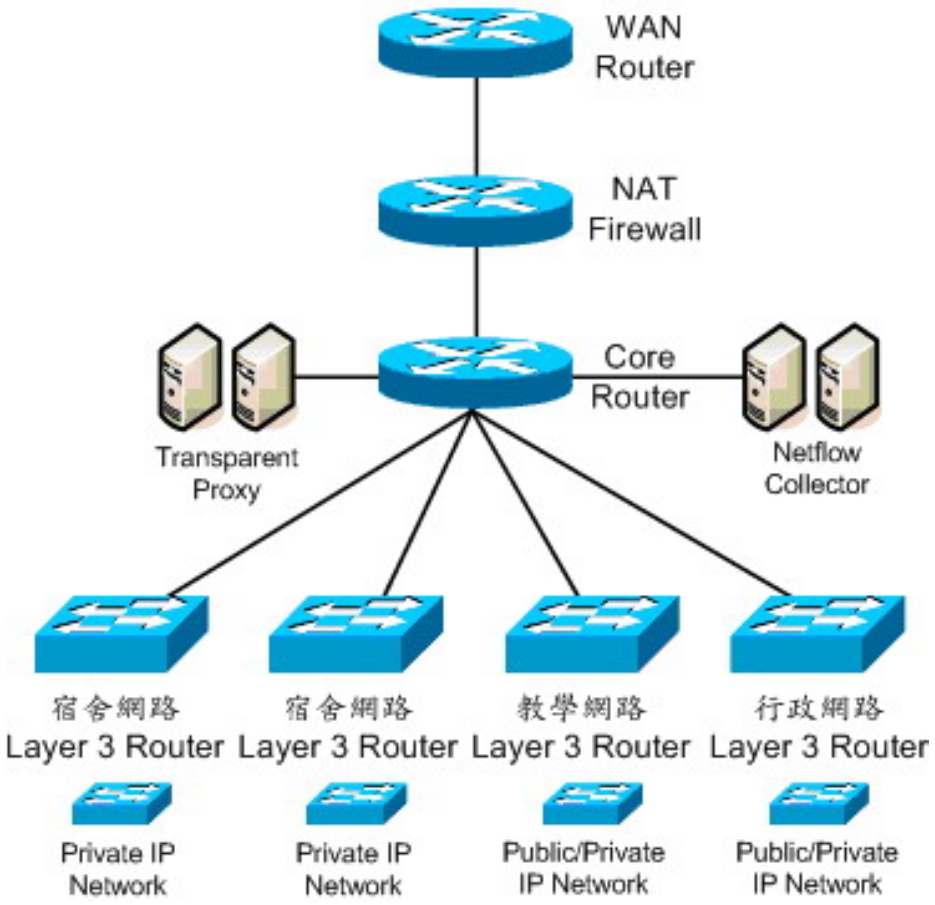
- 分散式架構優點
  - 有效將NAT分散至各層做轉換
  - 減輕單一NAT的負載

NAT架構規劃(續)

- 分散式架構缺點
  - 端點設備必須為layer 3
  - 無法掌握Edge端的Netflow、IP記錄
  - NAT轉址浪費

NAT架構規劃(續)

- 集中式架構



NAT架構規劃(續)

- 集中式架構優點
  - 最能有效管理NAT環境，合法IP與私有IP皆能互通
  - 對原始網路環境影響較少
  - Log紀錄與分析容易
    - Transparent Proxy Server及Netflow Collector放置於Core Router上則能收到正確的Source IP與Destination IP的記錄，更能利用這些完整的資料加以分析整理

NAT架構規劃(續)

- 集中式架構缺點
  - 設備昂貴
    - NAT設備需要有夠大的Throughput與Sessions數，目前多數為企業式、電信等級的硬體式(ASIC base)防火牆才擁有如此完整功能

軟體式(Software base) NAT

- 經費考量下，軟體式NAT為最佳選擇方案
  - 便宜、紀錄容易
  - 擁有與硬體式NAT相同功能(效率部份依環境不同而有差異，越大型的環境相對的也須越有power的機器)

軟體式(Software base) NAT(續)

- Server以上的作業系統大部分都有防火牆功能，也能作NAT
- 建議採用freebsd
  - freebsd內建三種防火牆，分別為IPFW2(IPFW)、IPFilter(ipf)及Packet Filter(pf)
  - 本例IPFW及IPFilter來做為NAT的轉換功能

軟體式(Software base) NAT(續)

- Freebsd 功能
  - IPFW2(IPFW)
    - 擁有過濾第二層MAC address、MAC type及VLAN功能。
    - 為TCP、UDP、ICMP保留封包狀態資訊(keep state)。
    - 提供重新導向(divert)功能。
    - 擁有頻寬控制(dummynet)功能。
    - NAT轉址功能(natd)。

軟體式(Software base) NAT(續)

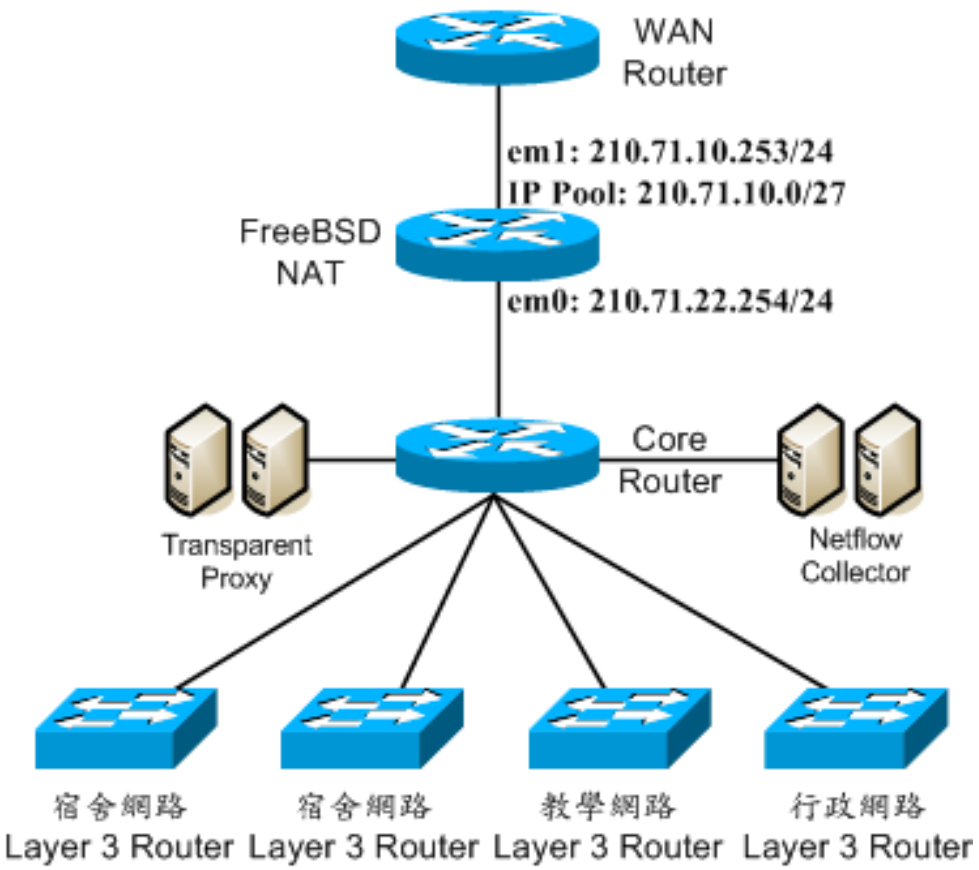
- Freebsd 功能
  - IPFilter
    - 為TCP、UDP、ICMP保留封包狀態資訊(packet state)。
    - 為IP 封包保存分段資訊(fragment state)，用同樣的規則套用到所有的分段封包上。
    - 提供重新導向(redirection)。
    - 提供封包表頭(packet header)給使用者指定的程式做認證用。
    - 擁有Large NAT轉址功能(ipnat)。

軟體式(Software base) NAT(續)

- IPFW、IPFilter皆提供NAT轉址的功能
- IPFW是把封包丟給另一隻natd這支Uerland的程式去執行，而IPFilter則是直接在Kernel Space裡面完成(速度上面是IPFilter略佔優勢)
- IPFilter在設計時就有考慮到大型的NAT環境，只要稍加修改IPFilter的原始程式碼再重新編譯，即可建置出大型NAT網路環境

軟體式(Software base) NAT(續)

- 系統規劃架構



測試網路架構圖

軟體式(Software base) NAT(續)

- 系統規劃架構
  - NAT部分由IPFilter來處理，防火牆部分因IPFilter並沒有連線數限制及頻寬控管功能，所以改用IPFW來處理
- 主機配備

OS	FreeBSD 5.4-RELEASE-p4
CPU	Intel Xeon 3.2G *1(disable HTT/SMP)
RAM	3G ECC DDR
BUS	PCI-X 133 *2
NIC	Intel 1000MF(1000base-SX) *2

軟體式(Software base) NAT(續)

- 作業系統核心調整

```
options CPU_ENABLE_SSE
options TCP_DROP_SYNFIN
options ZERO_COPY_SOCKETS
options IPFIREWALL #使用IPFW2
options IPFIREWALL_VERBOSE
options IPFIREWALL_DEFAULT_TO_ACCEPT
options IPFIREWALL_FORWARD
options IPFIREWALL_FORWARD_EXTENDED
options IPFILTER #使用IPFilter
options IPFILTER_LOG
options IPSTEALTH
```

FreeBSD Kernel設定

軟體式(Software base) NAT(續)

- 作業系統核心調整
  - 原始的IPFilter中，sessions最多只能到3萬條
  - 將NAT_TABLE_MAX及NAT_TABLE_SZ的參數放大，使原有處理有3萬條sessions的NAT能處理至18萬條sessions

修改/usr/src/sys/contrib/ipfilter/netinet/ip_nat.h
define NAT_TABLE_MAX 180000
define NAT_TABLE_SZ 16383

軟體式(Software base) NAT(續)

- 作業系統核心調整(最佳化)

```
kern.ipc.nsfbufs=13312
kern.ipc.maxsockets=32768
```

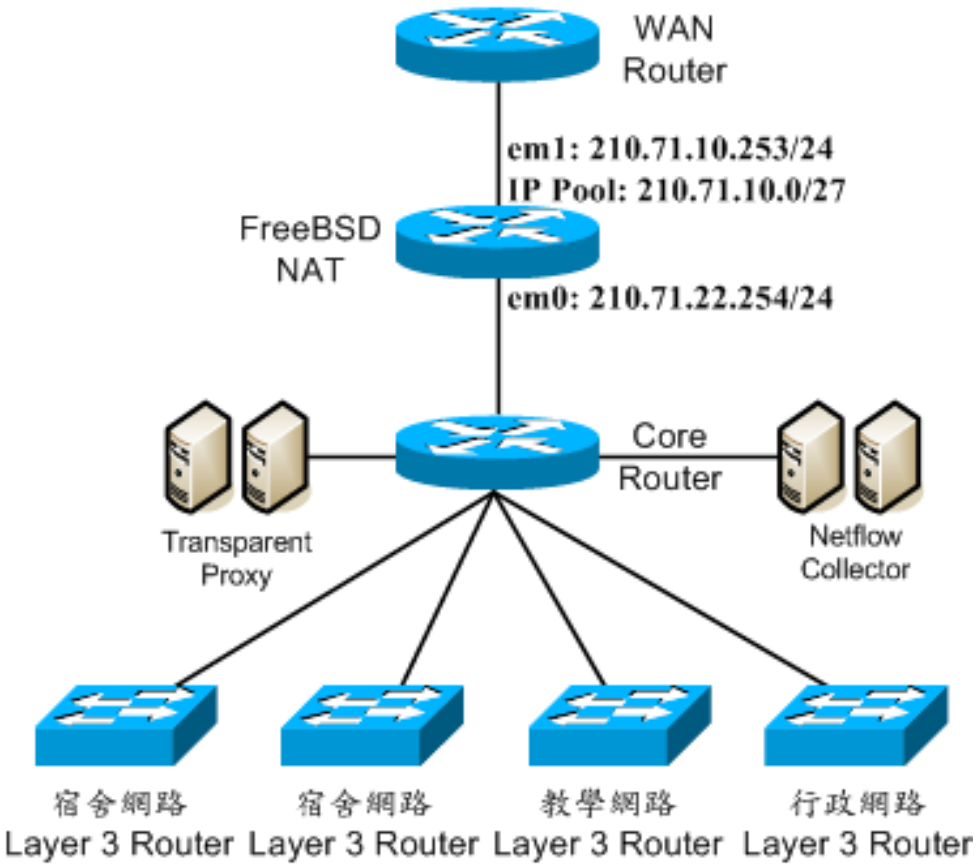
/boot/loader.conf設定

```
#系統核心調整
kern.ipc.nmbclusters=81920
kern.ipc.somaxconn=32767
kern.maxfiles=131070
kern.maxfilesperproc=32767
      #網路參數調整
net.inet.tcp.delayed_ack=0
net.inet.tcp.sendspace=65535
net.inet.tcp.recvspace=65535
net.inet.udp.recvspace=65535
net.inet.udp.maxdgram=57344
net.local.stream.recvspace=65535
net.local.stream.sendspace=65535
net.inet.ip.forwarding=1
      #IPFilter參數調整
net.inet.ipf.fr_tcpidletimeout=600
net.inet.ipf.fr_tcpclosed=1
#ipfw參數調整
net.inet.ip.fw.dyn_buckets=65535
```

/etc/sysctl.conf設定

軟體式(Software base) NAT(續)

- **Dynamic NAT設定**



em0是內部的網段
em1為對外網段

利用ARP Proxy建立IP Pool Address，ARP Proxy的網卡號碼為em1本身的網卡號碼。ARP Proxy建立完成後，再建立IPFilter的NAT規則，即完成建立Dynamic NAT的動作。

軟體式(Software base) NAT(續)

- 防火牆及連線數設限
  - 此架構NAT是放置在最外層出口，同時也需處理合法IP網段的封包及各式常見的網路攻擊
  - P2p軟體的流行會造成NAT mapping table快速暴漲或是過載

軟體式(Software base) NAT(續)

- 防火牆及連線數設限

```
#!/bin/sh
ipfw="/sbin/ipfw"
$ipfw -f flush
$ipfw add 1 permit ip from any to any via lo0
$ipfw add 2 permit ip from 127.0.0.1 to any
$ipfw add 10 deny tcp from any to any in tcpflags syn,fin
$ipfw add 21 check-state
$ipfw add 22 allow tcp from any to any in established
$ipfw add 23 permit tcp from any to any out keep-state
$ipfw add 24 permit udp from any to any out keep-state
$ipfw add 100 deny tcp from any to any 445,139,135,1433,1434,6667,1025,12345
$ipfw add 101 deny udp from any to any 1433,1434,1025,500
#連線數控制
$ipfw add 501 permit tcp from 192.168.0.0/16 to not 192.168.0.0/16 limit src-addr 32
```

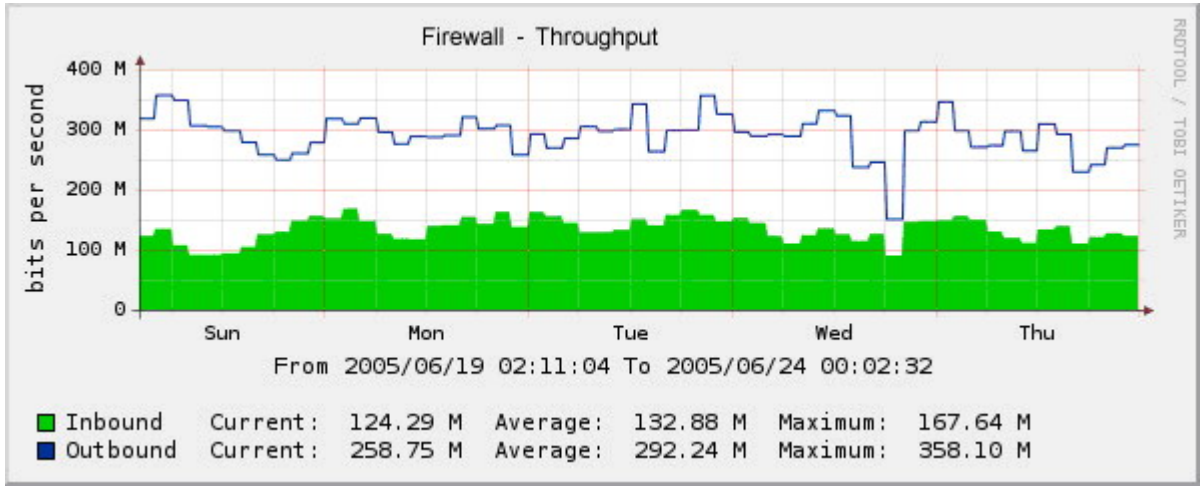
IPFW防火牆設定規則

NAT測試

- 硬體式防火牆VS軟體式防火牆
  - 以樹德科技大學為例，採用硬體式防火牆與軟體式防火牆做評比
  - 硬體式防火牆採用juniper netscreen 5200

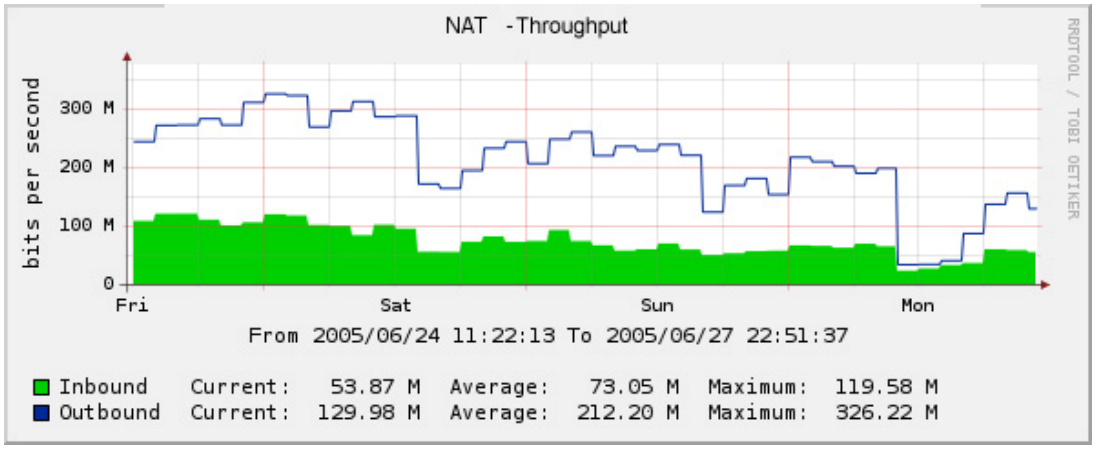
NAT測試(續)

- 硬體式防火牆效能
  - 平均流量約**132Mbps/292Mbps(IN/OUT)**
  - 高尖峰的流量可達到167Mbps/358Mbps(IN/OUT)
  - CPU負載率平均維持在1~2%
  - Sessions平均維持在9萬~11萬條



NAT測試(續)

- 軟體式防火牆效能
  - 平均流量約73Mbps/212Mbps(IN/OUT)
  - 最高尖峰的流量可達到119Mbps/326Mbps(IN/OUT)
  - CPU負載率平均維持在20~30%
  - Sessions平均維持在8萬~10萬條



NAT測試(續)

- 硬體式防火牆VS軟體式防火牆比較
  - 軟體式的NAT最大的缺點在於CPU處理NAT轉址的速度沒有ASIC晶片快
  - PCI-X的匯流排速度還是比硬體式慢了一點
  - 管理者需要花較多的時間去調整作業系統與硬體上的搭配

習 題

習題一

- 請簡單說明DMZ定義以及DMZ帶來的效益。

習題二

- 請簡易說明防火牆種類、優點和限制並說明防火牆與DMZ的關係。

習題三

- 請說明DMZ架構以及各架構的優缺點。

習題四

- 請簡單說明NAT定義以及優缺點。

習題五

- 請說明靜態NAT與動態NAT。

習題六

- 請說明NAT架構以及優缺點。

Module 12-4:專案實作(**)

專案目的

- 建置DMZ及NAT應用環境。
- 利用實際操作的方式讓同學了解DMZ及NAT工作原理。

專案一描述：實作-DMZ架設

- 以公司環境考量，公司對外服務有mail、web等伺服器，而這些公開伺服器需躲在DMZ後端，也必須讓後端使用者作存取更新
  1. 規劃防火牆架構(架構圖)-採用dull firewall
  2. 規劃放置在DMZ內的伺服器
  3. 防火牆政策

專案二描述：實作-NAT架設

- 以上個實作DMZ為主，在接續內部網路的firewall上實作NAT，以便讓內部使用者自動抓取虛擬IP並上網
  1. 規劃NAT網段
  2. 架設DHCP
  3. 規劃NAT政策

參考文獻

1. K. Egevang, P. Francis, "The IP Network Address Translator (NAT)", RFC 1631, May 1994.
2. P. Srisuresh, M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, Aug 1999.
3. T. Hain, "Architectural Implications of NAT", RFC 2993, Nov 2000
4. Y. Rekhter, "Address Allocation for Private Internets:, RFC 1918, Feb 1996.
5. The FreeBSD Project, http://www.freebsd.org/
6. IP Filter - TCP/IP Firewall/NAT Software, http://coombs.anu.edu.au/~avalon/

參考文獻

7. IPFirewall, http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html
8. PF: The OpenBSD Packet Filter, http://www.openbsd.org/faq/pf/
9. Eric Maiwald,資訊安全(Network Security: A Beginner‘s Guide, 2/e),2004,學貫出版社
10. Robert L. Ziegler,實戰Linux防火牆iptables應用全蒐錄,2004,上奇科技
11. The netfilter.org project. Linux 2.4 NAT HOWTO, from the World Wild Web: http://www.netfilter.org/projects/iptables/index.html
12. Craig Hunt, TCP/IP Network Administration, 2006, O’REILLY