實驗日期:2020/6/11

實驗名稱:

* ITS Exp. 21: FTP
* ITS Exp. 22: NAT
* ITS Exp. 23: Firewall

實驗相關技術資訊:

* FTP uses out-of-band control. What does out-of-band mean?

out-of-band control是網絡協議的一個特徵，用於控制數據，out-of-band control將控制數據傳遞到與主數據不同的連接上。FTP在一個連接上發送其控制信息，包括用戶標識，密碼和put / get命令，並在單獨的並行連接上發送數據文件。因為它使用單獨的連接來控制信息，所以FTP使用out-of-band control。

out-of-band是指在定義的電信頻段之外的活動，或者在某種其他類型的活動之外，防止偽造是其目的之一。

* **What is the difference between active and passive FTP?**

Active FTP

如果數據連接由服務器啟動，則FTP連接處於活動狀態服務器和客戶端都需要打開端口以監聽傳入流量。如果在防火牆/ NAT路由器後面，這可能會導致發生問題。

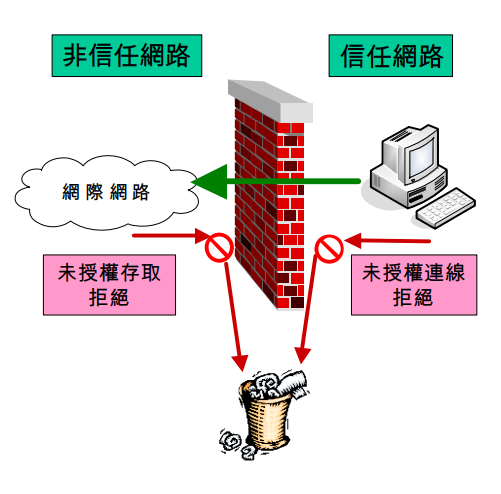
Passive FTP

如果客戶端啟動數據連接，則FTP連接是被動的，只需服務器即可為傳入流量打開端口。由於安全問題，大多數FTP服務器以Passive FTP連接，一般情況下，所有瀏覽器都配置為FTP客戶端時處於被動模式。

兩種模式各有優缺點，主動模式對伺服器來說比較安全，但對用戶端來說可能帶來危險，因此很可能被用戶端的防火牆所阻擋了。使用被動模式雖然解決了用戶端的問題，但相對的伺服器必須開啟一定範圍的通訊埠供用戶端連線，目前絕大部分的 FTP 伺服器軟體，皆可以由管理者決定開啟哪些範圍的通訊埠。

* **What is a firewall? How does it work?**

一種安全機制用來隔離兩個安全信任度不同的網路。可由軟體或硬體

來實作，利用系統所建立的安全性規則，有效的控制對內與對外流量。 

**防火牆的定義**

在私有網路（內部網路）與網際網路（外部網路）之間建立一個安全的通訊閘道稱為「防火牆（Firewall）」，類似軍隊的檢查哨，可以控制並且管制所有進出私有網路與網際網路的資料封包，防火牆最重要的成員是「封包過濾器（Packet filter）」與「應用閘道器（Application gateway）」，但是必須配合其他伺服器軟體的合作才能真正達到網路安全的目的，使用防火牆的優點包括：

➤保護私有網路：可以保護私有網路（內部網路）的安全，把惡意攻擊的怪客（Cracker）阻擋在外面。

➤管制私有網路：可以管制私有網路（內部網路）與網際網路的存取，避免員工使用公司網路進行違法行為。

➤保存使用記錄：可以保存網路使用的記錄，並且統計內部網路的使用情形。

**防火牆的缺點**

使用防火牆是在私有網路（內部網路）與網際網路（外部網路）之間建立一個安全的通訊閘道，所有的封包進出都必須經過檢查，因此也會產生一些缺點包括：

➤降低傳輸效率：防火牆對網路進出的封包進行檢查的動作會降低網路的傳輸效率。

➤防火牆被入侵：當防火牆被入侵的時候，整個私有網路（內部網路）會完全暴露，因此不可以完全依賴防火牆，私有網路（內部網路）的每一台電腦都必須做好安全管理工作。

➤無法防範內賊：防火牆無法防範內賊，所以人員使用權限的管制也是網路安全重要的項目。

**防火牆的成員**

安全的防火牆架構如＜圖一＞所示，包括下列基本的伺服器軟體：

➤封包過濾器（Packet filter）：例如 NAT 伺服器（NAT server）。

➤應用閘道器（Application gateway）：例如代理伺服器（Proxy server）。

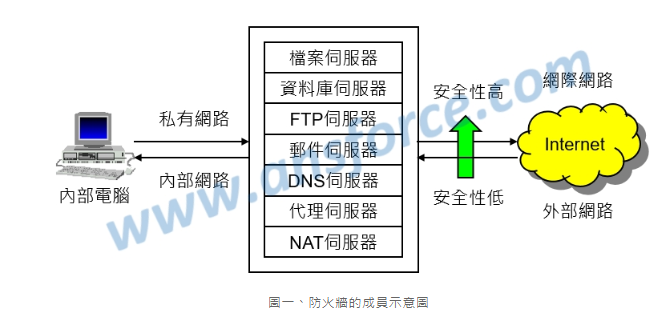
➤網域名稱管理：例如 DNS 伺服器（DNS server）。

➤電子郵件管理：例如郵件伺服器（Mail server）。

➤檔案傳輸管理：例如 FTP 伺服器（FTP server）。

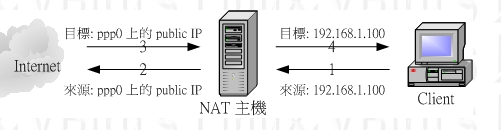
➤檔案資料管理：例如資料庫伺服器（Database server）、檔案伺服器（File server）。

➤安全的作業系統：例如 Unix、Linux 或 Windows 等。



* **What is NAT? How does it work?**

其實是 Network Address Translation 的簡寫，字面上的意思是『網路位址的傳送』，他主要的功能就是在提供內部私有網路的電腦之頻寬分享了。簡單的說，NAT 的功能就是『 IP 分享器』。NAT在保護IP地址，使用未註冊IP地址的專用IP網絡能夠連接到Internet，NAT在路由器上運行，通常將兩個網絡連接在一起，並在將數據包轉發到另一個網絡之前將內部網絡中的私有（非全局唯一）地址轉換為合法地址。作為此功能的一部分，NAT可以配置為僅將整個網絡的一個地址通告給外部世界。這通過有效地隱藏該地址後面的整個內部網絡來提供額外的安全性。NAT提供安全性和地址保護的雙重功能，通常在遠程訪問環境中實現。



這個 client 的 gateway 設定為 NAT 主機，所以當要連上 Internet 的時候，該封包就會被送到 NAT 主機啦，這個時候的封包 Header 之 source IP 為 192.168.1.100 喔；

而透過這個 NAT 主機，她會將 client 的對外連線封包的 source IP ( 192.168.1.100 ) 偽裝成 ppp0 ( 假設為撥接情況 )這個介面所具有的公共 IP 囉，因為是公共 IP 了，所以這個封包就可以連上 Internet 了！同時 NAT 主機並且會記憶這個連線的封包是由哪一個 ( 192.168.1.100 ) client 端傳送來的；

由 Internet 傳送回來的封包，當然由 NAT 主機來接收了，這個時候， NAT 主機會去查詢原本記錄的路由資訊，並將目標 IP 由 ppp0 上面的公共 IP 改回原來的 192.168.1.100 ；

最後則由 NAT 主機將該封包傳送給原先發送封包的 Client

參考資料:

<http://avp.toko.edu.tw/docs/class/3/%E9%98%B2%E7%81%AB%E7%89%86%E5%8E%9F%E7%90%86%E6%9E%B6%E6%A7%8B%E5%92%8C%E7%A8%AE%E9%A1%9E%E4%BB%8B%E7%B4%B9.pdf>

<https://www.stockfeel.com.tw/80872-2/>