增加 Windows 遠端桌面連線的安全性
--使用 Redhat Linux NAT

呂紹勳

若是您身爲 **Windows Server System** 的系統管理者，相信您對於 **Windows** 遠端桌面連線的使用，一定不會感到陌生。因爲該項工具對於管理者而言，可說是一項相當便利的工具。

因爲自從這項工具誕生後，**Windows** 系統管理者便不需要再安裝任何 **third-party** 的遠端管理產品。可以直接使用微軟所提供的遠端桌面管理工具，就能夠及時地管理並修改 **Windows Server** 伺服器的設定，間接也省卻了來回往返機房的時間。

不過愈是方便，代表愈有可能存在著潛藏的安全性問題（只要輸入正確的帳號及密碼，便能使用該台 **Windows Server** 的桌面環境），其風險也愈高，筆者曾經瀏覽網頁時，無意間發現有份資料顯示**(**網址位於 **http://lcr.old-castle.org/?p=76)**，有一些駭客已經注意到『遠端桌面連線』的方便性，並伺機蠢蠢欲動。

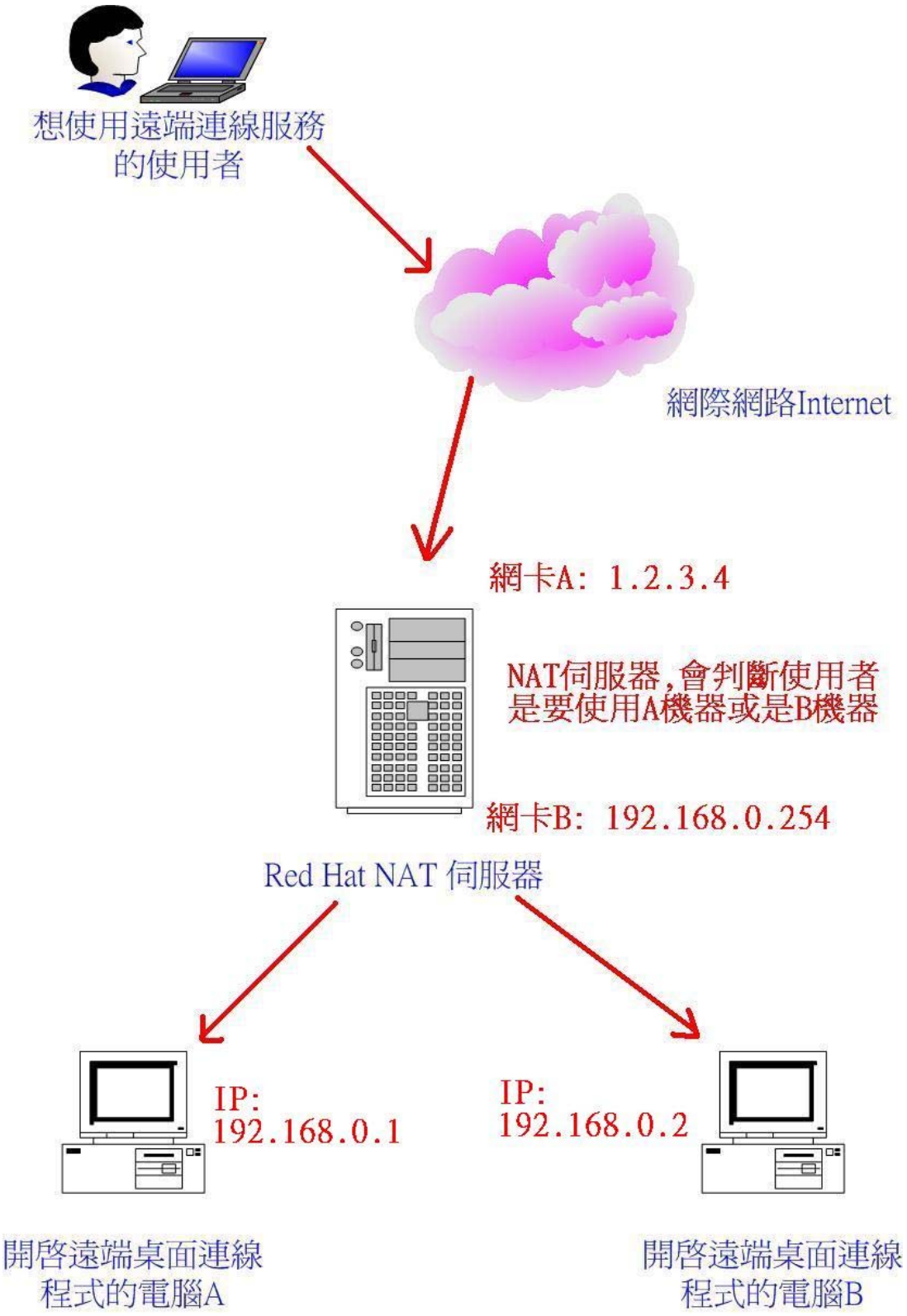
筆者曾經天真的以爲，可以利用 **Windows Firewall** 來增加遠端桌面連線的安全性。不過，當開啓了 **Windows Firewall** 後，才發現它所能設定的項目，真是少的可憐，完全無法達到筆者的要求，也因此筆者最後只得放棄這個念頭，另謀他途。

後來筆者想到，何不利用 **Redhat Linux NAT** 來防護 **Windows** 遠端桌面連線呢？因爲很多數據資料都已經顯示並證明 **Linux** 的防火牆功能，已經可以媲美許多業界商用防火牆了，因此我們若能使用以高穩定性聞名的 **Linux** 來增進使用 **Windows** 遠端桌面連線的安全性，不但可以節省大筆的經費支出，更可讓 **Windows** 遠端桌面連線，擁有銅牆鐵壁般的防護。

在筆者的 **Lab** 環境中，係以 **Redhat Linux 9** 並搭配著 **iptables** 架設成 **NAT**。該部 NAT 伺服器上具備有兩張網卡，網卡 A 爲對外的介面，IP 位址爲『1.2.3.4』（請依據現實環境狀況自行更改）。網卡 B 則爲對內部網路的介面，IP 位址爲『192.168.0.254』。筆者並將 NAT 伺

服器上的 IP Forward 的功能開啓，俾便網卡 A 與網卡 B 能夠互通。要啓用 IP Forward 的功能相當簡單，只須利用編輯軟體（例如 vi）編輯『/etc/sysctl.conf』這個檔案，將其中『net.ipv4.ip_forward=0』改成『net.ipv4.ip_forward=1』即可，而後利用指令『sysctl -p』，讓其立即生效，完全無需重新開機。

除此之外，筆者並將電腦 A 及電腦 B 的遠端桌面連線程式開啓，亦即是允許外面的使用者，利用 Windows 內附的遠端桌面連線程式，通過網際網路，連線至電腦 A 或電腦 B 來使用該機器的桌面，如【圖一】所示：



【圖一、利用 NAT 防護 Windows 遠端桌面】

以下筆者所舉的例子，是想讓 Internet 的使用者（前提是他知道電腦 A 有開啓遠端桌面程式，並允許連線，且知道帳號及密碼）。該位外部使用者，只需要在使用遠端桌面連線程式的時候，額外指定要連線到 NAT 伺服器外面 IP 位址的 7878 port，如【圖二】所示。此時 NAT 伺服器便會自動將此一連線需求，轉送到電腦 A 的遠端桌面程式（port number 3389）。

爲了達成讓電腦 A 及電腦 B 不須更改預設的連線 port number 3389，並且讓 NAT 伺服器自動轉送連線需求到特定的位址，筆者必須在 NAT 伺服器上做些設定。

由於筆者的 NAT 係以 Redhat linux 的 iptables 達成，因此筆者以一個簡單的 shell script，讓其滿足上述的需求，該 shell script 如下，文字前帶有#符號的是筆者的說明，shell script 在執行時，會忽略該行。若是有需求的讀者，可依據筆者所撰寫的 shell script，加以修改，相信便可立即在您的真實環境中執行。

以下是筆者所撰寫的 shell script：

```
#!/bin/bash
######define internal network#########
INTERNAL_NET="192.168.0.0/24"
INTERNAL_NIC="eth1"
INTERNAL_ADDRESS="192.168.0.254"
```

```
######define External network#########
EXTERNAL_NET="1.2.3.0/24"
EXTERNAL_NIC="eth0"
EXTERNAL_ADDRESS="1.2.3.4"

######load modules####################
modprobe ip_conntrack
modprobe ip_conntrack_ftp
modprobe ipt_state

######clean default rules#############
iptables -t filter -F
iptables -t nat -F
iptables -t mangle -F

######deny all traffic#################
iptables -t filter -P INPUT DROP
iptables -t filter -P OUTPUT DROP
iptables -t filter -P FORWARD DROP

######Allow lo traffic#################
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT


######Allow eth0 to anywhere############
iptables -t filter -A OUTPUT -o $EXTERNAL_NIC -s
$EXTERNAL_ADDRESS -j ACCEPT
iptables -t filter -A INPUT -m state --state
ESTABLISHED,RELATED -j ACCEPT

######Allow INTRANET to eth0#########
iptables -t filter -A OUTPUT -o $INTERNAL_NIC -s
$INTERNAL_ADDRESS -j ACCEPT
```

```
#######Allow Remote Control for Windows Desktop ####
iptables -t nat -A PREROUTING -i $EXTERNAL_NIC -p tcp --dport
7878 -j DNAT --to 192.168.0.1:3389
iptables -t filter -A FORWARD -i $EXTERNAL_NIC -p tcp --dport
3389 -j ACCEPT

######Allow Internal NAT user to Internet###
iptables -t nat -A POSTROUTING -o $EXTERNAL_NIC -s
$INTERNAL_NET -j SNAT --to $EXTERNAL_ADDRESS
iptables -t filter -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT


######Allow port################################
iptables -t filter -A INPUT -p tcp --dport 7878 -j ACCEPT
```

相信以此簡易的方法，來對 Windows 遠端桌面進行防護，應該是相當足夠的。原因有三：

1. 以駭客攻擊的角度來看，他並不知道究竟是哪台伺服器提供了『Windows 遠端桌面』？因爲真正提供遠端桌面的機器，藏在 NAT 後面。
2. 就算駭客知道了 A 電腦提供了遠端桌面，他也不知道應該如何連線至該台機器，因爲他不知道 NAT 伺服器上究竟允許哪個 port number 可以將連線需求，轉送到電腦 A。
3. 我們還可以在 NAT 上面，進行 IP 的管控。意即允許某個特定的 IP(例如 5.6.7.8)才可以連線到 NAT 伺服器上的 7878 port。

Linux iptables 的功能相當強大，筆者只是使用其簡單的功能，並應用在防護『Windows 遠端桌面連線』上。感謝 Open Source 社群，由於有他們的默默貢獻，才讓我們有如此方便又免費的工具可以使用。