檔案格式: PDF 編寫: 陳昇佑 2006/04/05

專案一:Linux 解決方案實作比較

1.專案環境:

- (1) 512/8M 固接 ADSL 網路。
- (2) 5部 Windows Client 端。
- (3) 1000MB的區域網路,内部無任何公開站台。
- (4) 有兩部多餘的主機可以運用。

```
2.功能要求:
```

(1) IP 分享。

```
(2) WEB Mail °
```

- (3) 色情網站存取控制。
- (4) 檔案分享。

```
3.測試環境:
```

- (1) Hostname: server012.tqc.seed 192.168.0.12/24 Red Hat Linux 9 開放 NAT 分享,製造 模擬的區域網路環境。
- (2) Hostname: server202.tqc.seed 192.168.0.202/24 Fedora Core 4 起 DNS 服務,用於區 域網路環境解析,同時也是各項方案驗證的機器。
- (3) Hostname: mswin110.tqc.seed 192.168.0.110/24 MS-Windows 98 驗證 Client 端。DNS 設定為 server202.tqc.seed, Gateway 設定為: server012.tqc.seed。

5.測試環境設定:

(1) server012 事前重要設定:

```
a.)编寫 /usr/local/ipt.rul, 内容如下:
```

#!/bin/bash

EXTIF="ppp0" #對外利用 PPPoE 方式上網

INIF="eth0"

```
INNET="192.168.0.0/24"
```

/sbin/iptables -F

/sbin/iptables -t nat -F

/sbin/iptables -A INPUT -i \$INIF -j ACCEPT

/sbin/iptables -t nat -A POSTROUTING -s \$INNET -o \$EXTIF -j MASQUERADE

b.)執行/usr/local/ipt.rul,產生 NAT 效果。

c.)DNS 指定為 server202, Gateway 不指定

(2) server202 事前重要設定:

a.) DNS 指定為自己(server202.tqc.seed), Gateway 設定為 192.168.0.12

b.)DNS(/var/named/chroot/etc/named.conf)重要設定段落:

options {

directory "/var/named"; dump-file "/var/named/data/cache_dump.db"; statistics-file "/var/named/data/named_stats.txt";

// query-source address * port 53;
forwarders{ 168.95.1.1; };

};

zone "tqc.seed" IN {

type master;

file "tqc.seed.zone";

};

zone "0.168.192.in-addr.arpa" IN {
 type master;
 file "192.168.0.rev";
};

c.)DNS 正解檔案(/var/named/chroot/var/named/tqc.seed.zone)設定:

\$TTL 86400 server202.tqc.seed. samchen.server202.tqc.seed. (tqc.seed. IN SOA 20060404 ;SN 21600 ;RE 3600 ;RT 604800 ;EX 3600 ;MIN) NS server202.tqc.seed. tqc.seed. IN server202.tqc.seed. IN А 192.168.0.202 server012.tqc.seed. IN А 192.168.0.12 **\$GENERATE 101-110** mswin\$ A 192.168.0.\$ d.)DNS 反解檔案(/var/named/chroot/var/named/192.168.0.rev)設定: \$TTL 86400 0.168.192.in-addr.arpa. IN server202.tqc.seed. samchen.server202.tqc.seed. SOA (20060404 ;SN 21600 ;RE 3600 ;RT 604800 ;EX 3600 ;MIN) 0.168.192.in-addr.arpa. IN NS server202.tqc.seed. 202.0.168.192.in-addr.arpa. IN PTR server202.tqc.seed. 12.0.168.192.in-addr.arpa. IN PTR server012.tqc.seed. **\$GENERATE 101-110** mswin\$.tqc.seed. \$ PTR

6.IP 分享方案比較(NAT V.S. Proxy)

- (1) NAT 在本測試環境中,只要將 server012 NAT 設定稍加修改,即可運用到專案環境。 也就是說,在 NAT 的運用上,我們可以採用 iptables 去實作,同時,也可以順便利用 iptables 的封包過濾的功能,讓 NAT 主機擔任閘道上防火牆的功能。
- (2) 採用 Proxy 的方案時,可以直接利用 FC4 内建的 squid 套件達到這樣的功能。如果利用 squid,則 Client 端必須進行設定(除非利用反向 proxy)才能正常上網。在設定上可能較為麻煩。不過,就目前的專案環境而言, Client 端的設定麻煩的狀況還在容允範圍內。
- (3) 分析1:使用NAT時,相容性會比較高,將來如果要在區域網路內擴充其他對外功 能時(Ex.對外公開的web站台),也可以將其放入iptables防禦的範圍內。缺點是在主 機的設定思考上,較為麻煩,同時須熟練iptables的語法規則,才不會在設定上出錯。
- (4)分析2:使用Proxy時,可以簡單製造IP分享的環境,同時可以配合公司政策利用一些簡單的方式去封鎖特定站台。只不過,Proxy相容性較差,且不同於NAT是在系統層級的設定,而是在應用程式層的地方處理,會在將來對外服務的擴充上造成麻煩。
- (5) 建議:如果機器效能許可,可以在 NAT 機器上同時加進 Proxy 服務,且讓 NAT 服務 只對某些機器有效(如只對 192.168.1.0/24 開放 NAT,包含 Proxy 自己等需要對外服務 的機器放入該網段,其他 Client 端使用另外的網段透過 Proxy 連出)。長期規劃上,可 以將 NAT 機器擺到 Proxy 之前,就可以結合兩者的優點了。
- 7.WEB Mail 方案比較(WAM V.S. Squirrelmail)
 - (1) 事前準備工作: FC4 的 postfix(smtp) + dovecot (pop3)實作:
 - a.)先利用「 service sendmail stop 」和「 chkconfig sendmail off 」指令關閉 sendmail Server
 - b.) 編輯 postfix 設定檔案(/etc/postfix/main.cf),重要設定段落為:

```
myhostname = server202.tqc.seed
```

mydomain = tqc.seed

myorigin = \$myhostname

myorigin = \$mydomain

inet_interfaces = all

mynetworks = 192.168.0.0/24, 127.0.0.0/8

relay_domains = tqc.seed

alias_maps = hash:/etc/postfix/aliases

alias_database = hash:/etc/postfix/aliases

- c.)下指令「cp /etc/aliases /etc/postfix/aliases」,將FC4預設該檔案位置調整一下。
- d.)下指令「postmap hash:/etc/postfix/access」,建立 access 資料庫。
- e.)下指令「postalias hast:/etc/postfix/aliases」,建立 aliases 資料庫。

- f.)下指令「service postfix restart」和「chkconfig postfix on」 啓動 postfix。
- g.)編輯 dovecot 設定檔案(/etc/dovecot.conf)開放 pop3 和 imap 服務,重要設定如下: protocols = imap imaps pop3 pop3s
 - imap_listen = [::]
 - pop3_listen = [::]
 - imaps_listen = [::]
 - pop3s_listen = [::]
- h.)下指令「service dovecot restart」和「chkconfig dovecot on」 啓動 dovecot。
- i.)到 Windows 底下利用 Outlook 測試可否利用 server202.tqc.seed 機器去正常收發信。
- (2) WAM 的實作:
 - a.) 到網址: <u>http://webmail.ysps.tp.edu.tw/~wam/download.html</u> 去下載 WAM 檔案,該 檔案為一個 ZIP 檔案,目前最新的版本到 1.631225,全新安裝的話,建議下載 wam-1.631225full.zip 檔案解壓縮後安裝之。
 - b.)解壓縮後,可以看到一個「install」的安裝 scripts 檔案,可以利用指令「sh install」 後照其敘述安裝之即可(由於編寫者在寫 scripts 時可能沒考慮到編碼問題,所以, 安裝過程中可能會看到亂碼)。
 - c.)安裝完成後,應該可以在 client 端看到 WAM 的畫面。方法是將瀏覽器開啓後,可 以在網址列上 Key「 http://(mail server IP/Hostname):12000 」看到 WAM 的畫面。 預設只能在區域網路範圍內用 WAM。



(WAM的首頁,由於這個東西是國人研發的,所以看到的介面是全中文喔)



(一般使用者登入後會看到的畫面,第一次登入可能要點選「網路郵局」去設定一下,才 能使用 webmail,同時,可以發現 WAM 不止 webmail 的功能)



(簡潔的 webmail 畫面)

- d.) WAM 如果完全照其安裝的 scripts 安裝時,會自動把自己的 web server 編譯安裝起來,所以,要啓動 WAM 的指令為「/usr/libexec/apache_wam/bin/apachectl start」。 安裝過程中,會自動把這個啓動的指令寫到/etc/rc.d/rc.local 内,方便重新開機時啓動之。
- (3) Squirrelmail 的實作:
 - a.)於安裝 FC4 過程中,如果有勾選「Mail Server」選項時,應該會把這個套件順便安 裝進去。可以利用「rpm -qa | grep squirrelmail」指令看看有無安裝。若沒有,可以 透過 FC4 更新機制(yum/rpm 或 GNOME 桌面的新增移除程式)安裝之。這個套件在 FC4 的第三片光碟内。
 - b.)如果要 squirrelmail 能正常運作,又不想碰觸 SELinux 設定問題時,請將 SELinux 關閉(如果沒設定好,會遇到 ICMP 服務存取被拒絕的狀況)。

要關閉 SELinux,須先編輯/etc/selinux/config,修正内容為:

SELINUX=disabled

SELINUXTYPE=targeted

設定好之後請重新啓動!

- c.)下指令「 ln -s /usr/share/squirrelmail/ /var/www/html/mail 」,將可愛的松鼠 (squirrelmail)畫面連接到 Apache 的預設 web root 目錄下。
- d.)修正設定檔案/etc/squirrelmail/config.php 内容如下:

\$squirrelmail_default_language = 'zh_TW';

\$default_charset = 'Big5';

此修正的目的在於讓松鼠可以用中文顯示它的畫面。

- e.) 啓動 Apache,利用指令「service httpd restart」 啓動之。如果要讓重開機還有效果, 可以利用指令「chkconfig httpd on」。
- f.) 啓動 httpd 後,就可以在網址列上 Key「http://(mail server IP/Hostname)/mail」後 看到松鼠的畫面。如下圖就是本機可以看到的登入畫面。



🎒 Squirrel	Mail - 登入	- Microsof	't Internet Explore	ſ									_ 8 ×
檔案E	編輯(E)	檢視(♡)	我的最愛(A)	工具(T)	說明(<u>H</u>)								
~ 上一頁	• → 下一頁	· (●	公前	② 捜尋	▲ 我的最愛	⑦ 媒體	③ 記錄	▶ 郵件	到印	編輯		
網址①	🕘 http://ser	ver202.tqc	.seed/mail/src/logi	n.php							-	∂移至	連結 »
				W powere 由校 帳職 密研	ed by Fe 松鼠電子郵 Squi 記:	edora an 部件管理系統 irrelMail	的 (統 1.4.4- (研發小維 登入	ail rrrelMail 設計			*39/92	8697.4	X
5 7G.BX											😻 भाषाः 😪	19UB	

(在 client 端看到的登入畫面)

🚈 SquirrelMail 1.4.4-2 - Micros	ft Internet Explorer				_ 8 ×
檔案 (E) 編輯 (E) 檢視 (♥)	我的最愛(A) 工具(I) 說明	(H)			10
◆ • ● • (上一頁 • 下一頁 • 例	● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	2000 1000 1000 1000 1000 1000 1000 1000	⑦	■ 日 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	編輯 討論
網址D) 🕘 http://server202.tq	.seed/mail/src/webmail.php				▼ 於務至 連結 ※
資料夾 最後更新時間: Wed, 4:10 (<u>Check mail</u>)	目前的資料夾: 收件夾 編寫郵件 通訊錄 資料	<u> 夾</u> 環境設定	2 搜尋 求助		<mark>登出</mark> SquirrelMail
收件夾	選擇全部				the state of the state of the state
Drafts Sent Trash	搬移已選取項目至:: 「收件夾 」 機移 ■ 轉寄 ■ 主題串列			린	轉移已選取項目: 遭取 未讀取 删除
	寄件者 □ 日	期▲ 主旨 🗉			
		本資	料夾中沒有郵	8件	
					🥑 網際網路

(也是相當簡潔的 webmail 畫面,不過,可以發現有些地方還沒完全中文化)

(4)分析比較:由於WAM已經好一段時間沒有再發展,可以說有一點點可惜。否則,全 中文的Webmail,加上功能强大,安裝的方式也很傻瓜!實在很適合學校去運用。相 較之下,松鼠的資源就不少,加上多人使用,中文的問題應該會慢慢解決。兩者都是 相當輕鬆簡單且免費的webmail解決方案,也建議使用之。 8.色情網站控制存取方案比較(單純的 proxy 過濾設定 V.S. Proxy + Proxy Filter)

- (1) Proxy 過濾設定實作:
 - a.) 編輯/etc/squid/squid.conf 設定檔案 http_port 3128 # 設定 Proxy 的使用 port #Recommended minimum configuration: acl stopfile dst "/usr/lib/squid/hosts.deny" # 設定封鎖的 ACL 名稱 acl localnet src 192.168.0.0/24 # 允許 192.168.0.0/24 網段使用 proxy #Recommended minimum configuration: # # Only allow cachemgr access from localhost # 注意:如果後面有「允許全部」的 ACL 設定時,此規則一定要放於其前 http_access deny stopfile b.) 編輯/usr/lib/squid/hosts.deny # 假設我們要封鎖 MSN 台灣站台不給人進入,就可以在下面 Key 上去。

www.msn.com.tw #實驗效果用,MSN 是已知的合法站台。

(其他想要封鎖的網址)

c.)用指令「service squid restart」和「chkconfig squid on」指令去啓動 Proxy。

d.)將 Client 端設定利用該 Proxy 去上網,同時驗證是否有封鎖掉所設定的站台。



(可以發現這樣設定後,MSN台灣站就進不去了。當然,這是效果示範,和我們真正 在專案中想要封鎖的網站無關。)

- (2) Proxy + Proxy Filter 的設定實作:
 - a.) 由於光靠 Proxy 還是會有些盲點,因此,加上了「DansGuardian」這個 Proxy 過濾 器來强化我們想要的網站存取控制。

Proxy Server 的 IP

- b.)下載套件: <u>http://parent.dansguardian.org/downloads/2/Stable/FedoraCore4/</u>
- c.)下載後,可以直接利用 rpm 指令安裝之。
- d.)编輯/etc/dansguardian/dansguardian.conf 設定檔案内容如下:

```
language = 'chinesebig5' # 改用中文顯示
```

loglevel = 1

filterport = 8080

proxyip= 192.168.0.202

proxyport = 3128

forcequicksearch = 1 # 使用中文的必要設定

- e.) 執行指令「 cd /etc/dansguardian/ 」
- f.) 執行指令「 ./logrotation 」
- g.) 想要定期更新的話,可以設定/etc/crontab 排程檔案加入如下内容:

00 00 * * * root /etc/dansguardian/logrotation

h.) 利用指令「 service dansguardian restart 」和「 chkconfig dansguardian on 」來啓動 dansguardian 服務。

f.)Client端在連線設定的部份需設成如下圖的畫面(網址就是 proxy 的 IP 或 hostname):

自動定。	設定會	取代手	動設定。	要確保	候用手	動設定	,諸停門	用自動設
ΓĒ	自動偵測	- 殿定(A	D)					
匚條	使用自重	加組態指	令碼(5)					
帮	間址(<u>R</u>)						1 ,	
Proxy	y 伺服器	ş		~~~~				
₽損	Ξ您的區 發號或 \	国域網路 VPN 連絡	後年用 Pr 泉)(X)	oxy 伺,	服器(這	些設定	将不會到	∰到
#	周址(E):	server	202.tqc.s	eer 連接	辑(<u>T</u>):	8080	進降	\$C)
Г	- 近端	網址不住	使用 Pro	xy®)				

g.)由於這回真的會封鎖掉一些網站,因此我們利用一些關鍵字來查詢看起來像色情網站者連結看看,結果出現如下圖的畫面:



(真是太好了!這樣一來有問題的網站就可以請這過濾器幫忙檔掉囉!)

- (3)比較分析:其實,由上面的實作可以發現,單單靠 Proxy 就可以達到網路存取控制的目的了!只是,在設定上面,對於禁止網站的存取清單維護可說是件煩人的工作。因此,可以利用 Proxy 過濾器來幫忙過濾,這樣一來,維護工作就可以輕鬆不少。只不過,實際運作發現這樣的網路存取會有等待時間比較久的狀況發生,同時,如果設定好例外清單,再從所允許的例外清單網站去連結可能有問題的網址時,會出現網頁久久沒有反應的現象。因此,這樣的設定應該還有改善的空間。同時,這樣的實作可能就要想辦法避免使用者直接使用 Proxy,一定要讓使用者透過 Proxy 過濾器才能有網路存取控制的效果。
- (4) 建議:如果要求效能,可能直接採用 Proxy 過濾,同時原則禁止,特例開放的設定方式可能較佳。否則,直接採用 Proxy + Proxy 過濾器應該是很好的方法。

9.檔案分享方案比較(SSH+WinSCP V.S. FTP)

(1) SSH + WIN SCP 實作:

- a.)於 server202.tqc.seed 上啓動 SSH Service。
- b.)於所有 Client 端安裝 WinSCP 軟體
- c.)WIN SCP 可以由 http://winscp.net/eng/index.php 網址找到安裝檔下載
- d.)這樣一來, Client 端可以透過 WIN SCP 軟體去上下傳檔案, 達到檔案分享目的。

(2) FTP 實作:

- a.) FTP 設定檔案: /etc/vsftpd/vsftpd.conf
- b.) 啓動:「 service vsftpd restart 」和「 chkconfig vsftpd on 」
- c.)將使用者家目錄權限變更為755
- d.) Client 端驗證:



(剛開始直接在網址列 Key 好後可以匿名登入,不過,這樣無法上傳檔案)

ftp://server202.tqc.seed/ - Microsoft In	ernet Explorer				
檔案 ④ 編輯 ④ 檢視 ♥ 移至	(G) 我的最愛(A) 說	(明任)			
	複製貼上復	の一次です。	<u>Ⅲ</u> 檢視		1 1
網址① 👰 ftp://server202.tqc.seed/			▼ @移至	連結 »	
server202	.tqc.seed				1
伺服器: server202.tqc.seed 使用者名稱: Anonymous	pub				
#		检泪(Ⅵ) ▶	1		
Use 'Copy To Folder' on the File menu to download files and folders to your computer. <u>Click</u> here for other useful bits		排列圖示() ▶			
The for the series and the		重新整理任			
使用其它使用者名種與密碼登入伺服器	₽	貼上企) 貼上捷徑(2)		\$	
Media Play	/er	登入成①…		<u> </u>	
			ſ	Ocli	
ストレンジェン ストレー ストレー ストレース おうしん ひょうしん おうしん ひょうしん ひょう ひょうしん ひょうしん ひょうしん ひょうしん ひょう		<u> </u>			ull'
		h	/		- H
🏨開始 🛛 🥔 🇐 💆 🗍 👰 ftp://serv	er202.tqc.seed/ 🎦	ftp_ano_login - 小畫家		23 (2)	🛃 🧼 🏧 😌 🛛 PM 11:49
(切換一下使用者)					
登入身份				×	
0	諸輸入使用者名	稲 和密碼,以巻り	、ILE FTP 伺服器		
J~					
	FTP 伺服器:	server202.tqc.see	d		
	使用者名稱(U):	samchen		_	
	密碼(P):				
	登入之後,您可 便快速回到此 F.	以將 FTP 伺服器力 TP 伺服器。	加到我的最愛,	IJ.	
	┏ 匿名登入(А)		儲存密碼③		
			登入(1)	取消	

(此時會要求要輸入帳號密碼,由於我們是允許實體帳戶登入,所以可以直接打上實 體帳戶的帳號和密碼)

💽 ftp://ser	ver202.tqc.:	æed/ - Micr	osoft Inter	net Exp	lorer						- 🗆 🗵
檔案E	編輯(E)	檢視(♡)	移至(G) 我的	的最愛(A)	說明(<u>H</u>)				
~ ~ 上一頁 ~	→ 、	▲ 上移	》 剪下	自複製	日 貼上	い) 復原		() 内容	上 職	•	
網址① ② ftp://server202.tqc.ssed/											
Q		server	202.t	qc.s	eed						
伺服器 使用者	: server202 名稱: samc	.tqc.seed hen	De) ktop	dig	rits	help	Ĺ	nages	img	-
Use 'Co menu t folders <u>here</u> fo	opy To Fold o download to your con r other usefu	er' on the Fi files and aputer. <u>Clic</u> al hints.	ile li <u>k</u>	ng	linux_		mail	name	d.setup	neomail	6
) atch			tools	(clinux	wam1 6115	2
			P		piony_	∞ 使用者∷	samchen	ч С	網際網路	*************************************	••••••••••••••••••••••••••••••••••••••

(登入成功後,就可以看到自己家目錄上的資料)



🔯 ftp://server202.tqc.seed/ - Microsoft Internet Explo	er	
檔案(E) 編輯(E) 檢視(V) 移至(G) 我的	最愛(<u>A</u>) 說明(<u>H</u>)	
		 EEE ◆ 検視
網址① 👰 ftp://server202.tqc.seed/		▼
server202.tqc.se	ed	
伺服器: server202.tqc.seed mail.cgi 使用者名稱: samchen	MD5-1.7.tar.gz named.setup Q	uota-1.3.4.t Quota-1.4.tar
Use 'Copy To Folder' on the File menu to download files and folders to your computer. <u>Click</u> here for other useful hints.	squinelmail version	wam.cgi wam.conf
wam-1.6312	ftp_ano_logi ftp_login.jpg in	homedir_f

(這樣就代表 FTP 能作用囉)

- (3)分析比較1:雖然我們只要很單純在Linux上開一個SSH服務,就可以達到檔案分享的目的。可是,這個代價就是犧牲掉Client端的方便性。簡單來說,那樣的方式可能比較適合工程師級的人物使用,對於一般使用者而言,可能還需要花額外的教育訓練時間才能上手。不過,SSH本身就是加密的協定,利用此方式,在安全性上面比FTP還佳。
- (4) 分析比較 2: 從上面的實作就可以發現利用 FTP 應該是一般使用者比較能接受的。同時,對於使用者而言,還是可以利用原本的操作方式來作業。不過,就網管的安全性來說可能比較頭痛些。另外,非必要的話可能拒絕匿名登入會比較好!
- (5) 建議:如果沒有安全上的顧慮,可以採用 FTP 來處理,同時,再利用一些設定技巧 來加强其安全性就是相當好用的檔案分享方式了!
- 10.專案綜合分析建議:
 - (1) IP 分享:可以採用 NAT 和 Proxy 並用的方式處理,同時, Client 端一定透過 Proxy 來 對外連線。
 - (2) WEB Mail:如果考慮中文問題,可以採用 WAM。另外一方面, squirrelmail 也是相 當簡單易用 web mail 解決方案。
 - (3) 色情網站存取控制:如果不太考慮效能問題,在利用 Proxy 對外連線作業時,可以併用 Proxy 過濾器,來達到存取控制的目的。
 - (4) 檔案分享:可以考慮利用 FTP 的方式達到檔案分享的目的,同時,一般使用者可以直接利用 IE 上手,不太需要改變什麼使用習慣。