[iptables]

*封包 > INPUT > FORWARD > OUTPUT

```
# -P (policy) ACEEPT/DROP   [!= -p 大小寫有別]
# -A (append) / -I (insert)
# -j LOG/ACCEPT/REJECT/DROP
# -i eth0 (input interface) / -o eth0 (output interface)
# -s (source)  *e.g. –s 192.168.0.0/24 –j ACCEPT
# -p tcp/udp/icmp (protocol)
# -t nat  (type)
    *packet > PREROUTING > FORWARD > POSTROUTING
              (source)DNAT          (destination)SNAT
```

*轉送 layer
*指定轉送介面
[DNAT] (針對進 NAT 的封包目標修改) > 對外服務, DMZs
(對外服務) NAT 轉發 80 給內網機器*

```
-t nat –A PREROUTING –i eth0 –p tcp --dport 80 –j DNAT –-to-destination 192.168.1.1:80
                                                          (--to)
```

(Proxy)port 轉發

```
-t nat –A PREROUTING –i eth0 –p tcp –dport 80 –j REDIRECT –-to-ports 8080
-A FORWARD -i eth0 -p tcp --dport 80 -d 172.31.0.23 -j ACCEPT
```

[SNAT] (針對進 NAT 的封包來源修改) > Router, NAT

```
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j MASQUERADE
-A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT --to-source 192.168.0.77
```

* **echo 1 > /proc/sys/net/ipv4/ip_forward**
sysctl –w net.ipv4.ip_forward=1 (/etc/sysctl.conf)
sysctl –p /etc/sysctl.conf **(重新開機也套用規則)**

[Configure sample.]

```
-P INPUT DROP
-t nat -P PREROUTING ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
  *(-A INPUT -p tcp -m multiport --dports 80,53 -j ACCEPT)
-A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT

(clear) iptables –t nat –F
        iptables –t nat –D POSTROUTING 1
```

[DNS]

```
    apt-get install bind9

    NS      (@ IN NS dns.twnic.net.tw.)
    A       (server IN A 140.123.102.10)
    AAAA    (twnic.net.tw. 86400 IN AAAA 3ffe: :bbb:93:5)
    CNAME   (www IN CNAME mix)
    MX      (server IN MX 10 mail.twnic.net.tw.)

/etc/bind/named.conf.default-zones
  zone "." {
        type forward;
        forwarders{
              192.168.1.1;
        };
  };
  zone "len.tw" {
        type master;
        file "/etc/bind/len.tw";
  };

/etc/bind/len.tw
    @      IN     SOA    len.tw. root.len.tw (
                             1        ; Serial
                        604800        ; Refresh
                         86400        ; Retry
                       2419200        ; Expire
                        604800 )      ; Negative Cache TTL
    ;
    @      IN     NS     len.tw.
    @      IN     A      192.168.0.77
    dns    IN     A      192.168.0.77
    web    IN     A      192.168.0.77
    ad     IN     A      192.168.0.100
    (active directory)
    _ldap._tcp.len.tw.     IN SRV 0 0 389 ad.len.tw.
    _kerberos._tcp.len.tw. IN SRV 0 0 88  ad.len.tw.

    _ldap._tcp.dc._msdcs.len.tw.     IN SRV 0 0 389 ad.len.tw.
    _kerberos._tcp.dc._msdcs.len.tw.  IN SRV 0 0 88  ad.len.tw.

    [AD 設定完成其 dns 紀錄會在 C:\Windows\System32\config\netlogon.dns]
```

[dhcp]

```
    apt-get install dhcp3-server

~$ dhcpd
~$ named-checkconf -z
~$/etc/init.d/isc-dhcp-server {start|stop|restart|force-reload|status}

/etc/dhcp/dhcpd.conf
    default-lease-time 600;
    max-lease-time 7200;

    subnet 192.168.0.0 netmask 255.255.255.0 {
       range 192.168.0.100 192.168.0.200;
       option broadcast-address 192.168.0.255;
       option domain-name "len.tw";
       option domain-name-servers 192.168.0.77;
       option routers 192.168.0.77;
    }
    #host fantasia {
    #  hardware ethernet 08:00:07:26:c0:a5;
    #  fixed-address fantasia.fugue.com;
    #}
```

[smb]

```
    apt-get install samba smbfs & testparm (做檢查)
~$ /etc/init.d/samba  {start|stop|reload|restart|force-reload|status}

/etc/samba/smb.conf
   workgroup = WORKGROUP
   netbios name = Len@Pwn
   security = share      # "security = user" This will require a Unix account

  # By default, read-only. Change to 'no' if you want to be able to write to them.
   read only = yes

  #(分享資料夾名稱)
  [smb]
     read only = yes                 # (writable = no)
     guest ok  = yes
     path     = /usr/share/smbshare  #(777 主要寫入 permission)
    (guest account = nobody # 來存取的人都用 nobody user 進來)
```

- Linux mount

  smbmount -o username="Username",password="Password" //IP/share /mnt/smb

  * mount -t smbfs -o username="Username",password="Password" //IP/share /mnt/smb

  * mount -t cifs -o username="Username",password="Password" //IP/share /mnt/smb

[Apache & SSL]

```
/etc/apache2/mods-enabled/
    ssl.conf -> ../mods-available/ssl.conf
    ssl.load -> ../mods-available/ssl.load

/etc/apache2/sites-available/ -> ../sites-enabled/
    <VirtualHost *:443>
        ServerName len.tw
        DocumentRoot /var/www
         <Directory />
                Options FollowSymLinks
                AllowOverride None
         </Directory>
         SSLEngine on
         SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
         SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
         SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
    </VirtualHost>

<Directory "/usr/share/doc/">
    Options Indexes MultiViews FollowSymLinks
    AllowOverride None
    Order deny,allow
    Deny from all
    Allow from 127.0.0.0/255.0.0.0 ::1/128
</Directory>
```

(mod_rewrite)

```
RewriteEngine On
RewriteCond %{REMOTE_ADDR} ^192\.168\.6\.$
RewriteCond %{REMOTE_ADDR} ^41\.78\.144\. [OR]
RewriteRule .* http://where_you_want_to_redirect.com [R,L]
(整個網站轉移)
RewriteCond %{SERVER_PORT} !^443$
RewriteRule ^(.*)?$ https://%{SERVER_NAME}/$1 [L,R]
```

(目錄做自動轉移)

```
RewriteBase /folder
RewriteCond %{SERVER_PORT} !^443$
#RewriteRule ^(.*)?$ https://%{SERVER_NAME}/$1 [L,R]
RewriteRule ^.*$ https://%{SERVER_NAME}%{REQUEST_URI} [L,R]
```

[Quota]

```
    apt-get install quota
```

設定 /etc/fstab，default 加入 usrquota 和 grpquota，能對使用者和群組做限制

/etc/fstab

```
    UUID=ab0238cf-2859-4522-b0d8-f69985a3066c /home ext3 defaults,usrquota,grpquota 0 2
```

```
~$ sudo mount -o remount /home
    * ~$ umount /home
    這時候很容易遇到 device /home is busy.
        > fuser -m /home (顯示存取/home 的 proccess PID)

~$ quotaoff –av     (*確認已關閉 Quota，才能執行 quotacheck)
~$ quotacheck –avug
    -ug : user & group
    -a  ：掃瞄所有在 /etc/fstab 內，含有 quota 支援的 filesystem，加上此參數後，
     /mount_point 可不必寫，因為掃瞄所有的 filesystem 了嘛！
    -f  ：強制掃瞄檔案系統，並寫入新的 quota 設定檔 (危險)
    -M  ：強制以讀寫的方式掃瞄檔案系統，只有在特殊情況下才會使用。

~$ sudo quotaon –av (*啟動 quota) & (quotaon –auvg)
    -v  ：顯示啟動過程的相關訊息；
    -a  ：根據 /etc/mtab 內的 filesystem 設定啟動有關的 quota ，若不加 -a 的話，
          則後面就需要加上特定的那個 filesystem 喔！

(limit)
    edquota –t (修改寬限時間)

    使用者磁碟限額設定
    sudo edquota -u User1

    群組磁碟限額設定
    sudo edquota -g Group1

    複製使用者 User1 設定至其他使用者
    sudo edquota -p user1 user2 user3
```

- quota [-uvs] [username]
- quota [-gvs] [groupname]

直接使用 quota 去顯示出 myquota1 與 myquota2 的限額
~$ quota -uvs myquota1 myquota2

列出所有使用者的磁碟用量及限制狀況
sudo repquota –auvs

(script)
setquota [-u|-g] 名稱 block(soft) block(hard) inode(soft) inode(hard) 檔案系統

(uid range)
    0 root, 1~499 admin, 500~65535 users.
useradd -u 700 -g group user2
username –u 0 user2
userdel –r User (-r 刪除家目錄)

[AD user]

    for /L %%a in (1,1,100) do @echo %%a

    user.txt
      Sam,Chen,sales00,123456
      Jay,Chou,sales01,123456
      Sam,Wu,sales02,123456
      Jack,Cao,rd00,123456
      Len,Cao,Admin,78965

    for /F "tokens=1,2,3,4 delims=," %%a in (user.txt) do @echo %%a %%b %%c %%d

    @for /L %%i in (1,1,9) do @dsadd user cn=Sales00%%i,ou=Sales,dc=len,dc=tw -samid Sales00%%i
    -upn sales%%i@len.tw -display Sales00%%i -pwd 456789
    @for /L %%i in (10,1,99) do @dsadd user cn=Sales0%%i,ou=Sales,dc=len,dc=tw -samid Sales0%%i
    -upn sales%%i@len.tw -display Sales0%%i -pwd 456789
    @for /L %%i in (100,1,100) do @dsadd user cn=Sales%%i,ou=Sales,dc=len,dc=tw -samid Sales%%i
    -upn sales%%i@len.tw -display Sales%%i -pwd 456789

    @dsquery user ou=Sales,dc=len,dc=tw | dsmod group cn=Sales,ou=Sales,dc=len,dc=tw –addmbr

    -mustchpwd yes (下次登入必須更改密碼)
    gpedit.msc