

---

# Monowall 防火牆簡介與實作

---

---

# 什麼是 Monowall

- 以FreeBSD 為平台開發出 Embedded 的 Firewall 韌體，大小只有 5M（真是厲害）。
  - 目前官網上的正式版 **generic-pc-1.11.img** 版本，這個版本是用 FreeBSD 4.10-Release 為 base + ipfilter 所開發出來的嵌入式防火牆。
  - 最新的**generic-pc-1.2b7.img** 則是 FreeBSD 5.3 + Packet Filter (PF) + ipfilter 為開發 Base
  - 支援的網路卡及硬體 → FreeBSD有支援的幾乎都有
  - hardware support: bge, em, gx, nge, ti, txp ,dc, fxp, sis, ste, tl, tx, xl (most)
  - 到網站去看 <http://m0n0.ch/wall/hardware.php>
-

m0n0wall - Hardware - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H) Google

# m0n0wall

Search

**Information**

- Background
- Facts
- Hardware
- Features
- Screenshots
- Change log

**Getting m0n0wall**

- Quick start guide
- Downloads
- Installation
- Upgrading
- Old versions
- Beta versions

**Support**

- FAQ
- Getting help
- Documentation
- Security
- Mailing lists

**Miscellaneous**

- Quotes
- Gallery
- To do/Wishlist
- Notes/Bugs/Caveats
- Survey results
- Donations
- Software used
- License

## Hardware

m0n0wall is targeted at embedded x86-based PCs. The net45xx/net48xx range from Soekris Engineering ([www.soekris.com](http://www.soekris.com)) and the WRAP platform from PC Engines ([www.pcengines.ch](http://www.pcengines.ch)) are officially supported. All it takes to get m0n0wall up and running on one of these systems is to download the relevant image and write it to a CF card (8 MB or larger). See [Installation](#) for more information.


It is also possible to run m0n0wall on most standard PCs, either by writing the *generic-pc* image to a small IDE hard disk or CF card, or by using the CD-ROM + floppy disk version. Since m0n0wall is based on FreeBSD 4, most hardware that works with FreeBSD also works with m0n0wall. See the [FreeBSD/i386 Hardware Notes](#) for a detailed listing of supported hardware.

**The recommended amount of RAM for m0n0wall is 64 MB.** It might work with less, especially if you don't use a lot of features/services, but there are no guarantees about that - watch out for failing firmware uploads (m0n0wall does not use swap space, so it can't do anything about running out of memory).


**VLAN tagging**

The following drivers/NICs either support VLAN tagging in hardware or handle long frames properly. All other drivers/NICs use software emulation that causes a reduced MTU (which may lead to problems).

- hardware support: bge, em, gx, nge, ti, txp
- long frame support: dc, fxp, sis, ste, tl, tx, xl (most)



WRAP board from [PC Engines](http://www.pcengines.ch)



WRAP-BOX outdoor enclosure from [mini-box.com](http://www.mini-box.com)

Ads by Goooooogle

**x86 Embedded Controllers**  
ADC/DAC, motion, LCD, I/O, Ethernet Low-Cost, Flexible, C/C++ Program  
[www.tern.com](http://www.tern.com)

**\$98 Embedded Controller**  
Low-cost single board computer w/ Ethernet, DOS & I/O - Dev Kit \$129!  
[www.jkmicro.com](http://www.jkmicro.com)

Last update: 03/20/2005  
Current version: 1.11  
Latest beta version: 1.2b7

網際網路

- 造福窮人家的小孩
- 麻雀雖小卻是五臟俱全

System

- General setup
- Static routes
- Firmware
- Advanced

Interfaces (assign)

- LAN
- WAN

Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

VPN

- IPsec
- PPTP
- OpenVPN

Status

- System
- Interfaces
- Traffic graph
- Wireless
- Diagnostics

No.	Bandwidth	Delay	PLR	Queue	Mask	Description
1	96000 Kbit/s					
2	64000 Kbit/s					
3	5000 Kbit/s					
4	40000 Kbit/s					
5	30000 Kbit/s					
6	20000 Kbit/s					
7	10000 Kbit/s					
8	5000 Kbit/s					
9	2500 Kbit/s					
10	1250 Kbit/s					
11	960 Kbit/s					
12	640 Kbit/s					
13	384 Kbit/s					
14	256 Kbit/s					
15	128 Kbit/s					
16	96 Kbit/s					
17	64 Kbit/s					
18	32 Kbit/s					
19	16 Kbit/s					

Note: a pipe can only be deleted if it is not referenced by any rules or queues.

System information

Name	m0n0wall.local
Version	1.2b7 built on Sun Mar 20 18:45:04 CET 2005
Platform	generic-pc
Uptime	20:42
Last config change	Tue Apr 19 18:06:19 UTC 2005
CPU usage	view graph
Memory usage	<input type="text" value="8%"/>

class3router.jsjhs.ntct.edu.tw - Firewall: Rules - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜索 我的最愛 Google

**m0n0wall** webGUI Configuration class3router.jsjhs.ntct.edu.tw

System  
 General setup  
 Static routes  
 Firmware  
 Advanced

Interfaces (assign)  
 LAN  
 WAN

Firewall  
 Rules  
 NAT  
 Traffic shaper  
 Aliases

Services  
 DNS forwarder  
 Dynamic DNS  
 DHCP server  
 DHCP relay  
 SNMP  
 Proxy ARP  
 Captive portal  
 Wake on LAN

VPN  
 IPsec  
 PPTP  
 OpenVPN

Status  
 System  
 Interfaces  
 Traffic graph  
 Wireless  
 ▶ Diagnostics

**Firewall: Rules**

LAN WAN

	Proto	Source	Port	Destination	Port
<input type="checkbox"/>	TCP	172.22.0.0/16	*	WAN address	10000
<input type="checkbox"/>	TCP	LAN net	*	172.22.0.0/16	*
<input type="checkbox"/>	TCP	172.22.0.0/16	*	LAN net	*

pass     block     reject     log  
 pass (disabled)     block (disabled)     reject (disabled)     log (disabled)

**Hint:**  
 Rules are evaluated on a first-match basis (i.e. the action of the first rule to match means that if you use block rules, you'll have to pay attention to the rule order. If a rule is blocked by default.

m0n0wall is © 2002-2005 by Manuel Kasper. All rights reserved. [view license]

完成

http://172.22.49.241 - m0n0wall.local - Services: Captive portal - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜索 我的最愛 Google

**m0n0wall** webGUI Configuration m0n0wall.local

System  
 General setup  
 Static routes  
 Firmware  
 Advanced

Interfaces (assign)  
 LAN  
 WAN  
 DMZ

Firewall  
 Rules  
 NAT  
 Traffic shaper  
 Aliases

Services  
 DNS forwarder  
 Dynamic DNS  
 DHCP server  
 DHCP relay  
 SNMP  
 Proxy ARP  
 Captive portal  
 Wake on LAN

VPN  
 IPsec  
 PPTP  
 OpenVPN

Status  
 System  
 Interfaces  
 Traffic graph  
 Wireless  
 ▶ Diagnostics

**Services: Captive portal**

Captive portal Pass-through MAC Allowed IP addresses Users

Enable captive portal

Interface: LAN  
 Choose which interface to run the captive portal on.

Idle timeout: [ ] minutes  
 Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout: 60 minutes  
 Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Logout popup window:  Enable logout popup window  
 If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs. When RADIUS accounting is enabled, this option is implied.

Redirection URL: [ ]  
 If you provide a URL here, clients will be redirected to that URL instead of the one they initially tried to access after they've authenticated.

MAC filtering:  Disable MAC filtering  
 If this option is set, no attempts will be made to ensure that the MAC address of clients stays the same while they're logged in. This is required when the MAC address cannot be determined (usually because there are routers between m0n0wall and the clients).

Per-user bandwidth restriction:  Enable per-user bandwidth restriction  
 Pass-through MAC download: [ ] Kbit/s  
 Pass-through MAC upload: [ ] Kbit/s

網際網路

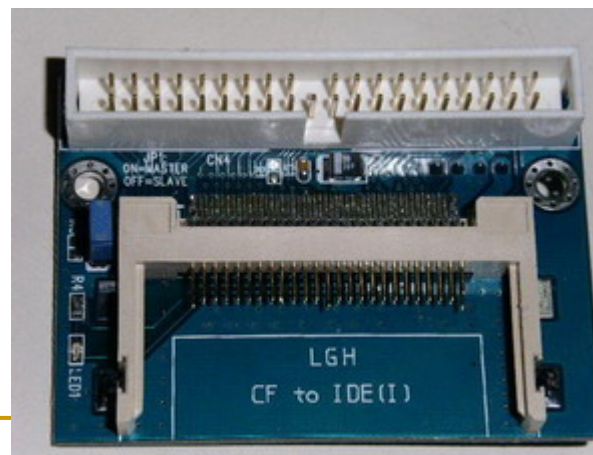
---

# monowall 防火牆實作

- 先確認你的網路卡是否有支援，我是用三片 intel 網卡，是有支援的( fxp0,fxp1,fxp2)。RealTak亦有支援，但拿來玩玩可以不建議作為Server用，要做Server用建議用3Com，Intel等這些大廠的晶片組。
  - 接著下載最新的韌體 **generic-pc-1.2b7.img** 版本 及 for Windows 的安裝程式 **physdiskwrite.exe** (下載點官網的 [Installation on a standard PC \(CF/IDE version\)](#) )
  - 或是你想要用光碟開機的ISO版，需要在A槽軟磁碟機中放1.44磁片，以記錄資料
-

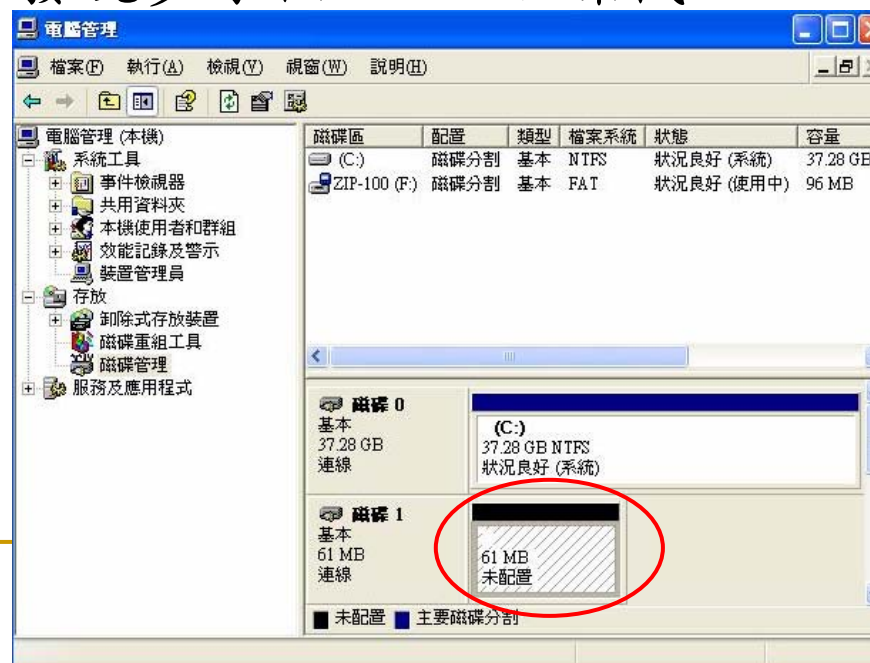
## monowall 防火牆實作 (以CF卡安裝為例)

- 手邊剛好有一塊 32 MB 不用的 CF 卡，在加買一片 **CF轉IDE卡** 即可當成一顆32 MB磁碟機用
- 把兩個下載軟體放置在 windowsXP 的 C:\ 槽目根錄下，接著關機把 **CF轉IDE卡** 插入 IDE 插槽(或排線)，並注意跳線(Master 或 Slave)，並插入轉卡的電源插頭，這個電源是吃跟軟碟機一樣的電源插頭，一切就緒後就可再次開機進入 Windows XP，進入 Windows 桌面後會發現多了個 CF 卡的 32 M(或64MB DOM)磁碟機，一切就緒後即可開始安裝。



## monowall 防火牆實作 (以DOM安裝為例)

- 跟創建訂購一塊64 MB的DOM(Disk On chip Memory)，即可當成一顆64 MB磁碟機用
- 把兩個下載軟體放置在 windowsXP 的 C:\ 槽目根錄下，接著關機把 DOM插入 IDE 插槽，並注意跳線( Master 或 Slave )，並DOM的電源插頭插上電源，一切就緒後就可再次開機進入 Windows XP，進入 Windows 管理程式後，在磁碟管理的地方會發現多了個64MB磁碟機，一切就緒後即可開始安裝。







# monowall 防火牆實作 (以DOM安裝為例)

- 在Windows XP的cmd 模式下輸入
  - `physdiskwrite.exe generic-pc-1.2b7.img` ←
- 這時會將你的系統中所有的磁碟機顯示出，並問你要將影像檔寫入哪個磁碟，不要選錯喔！不然會把你的系統給毀了。

```
C:\WINDOWS\system32\cmd.exe - physdiskwrite generic-pc-1.2b7
Information for \\.\PhysicalDrive0:
  Windows:      cyl: 4866
                tpc: 255
                spt: 63
  C/H/S:        16383/16/63
  Model:         MAXTOR 6L040L2
  Serial number: 662214729088
  Firmware rev.: A93.0500
Information for \\.\PhysicalDrive1:
  Windows:      cyl: 62
                tpc: 32
                spt: 63
  C/H/S:        978/4/32
  Model:         TRANSCEND DOM064M
  Serial number: SSSI064M05408T18402P
  Firmware rev.: 1.1
Information for \\.\PhysicalDrive2:
  Windows:      cyl: 12
                tpc: 255
                spt: 63
Which disk do you want to write? (0..2) 1

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\RegisUser>cd\

C:\>dir
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號:  ACA9-B815

C:\> 的目錄

2005/02/24 上午 12:50           0 AUTOEXEC.BAT
2005/02/24 上午 12:50           0 CONFIG.SYS
2005/04/13 下午 10:06          <DIR>      Documents and Settings
2005/04/11 下午 12:11          7,074,445 generic-pc-1.2b7.img
2004/08/22 上午 10:55           90,112 physdiskwrite.exe
2005/04/24 下午 03:41          <DIR>      Program Files
2005/04/24 下午 03:47          <DIR>      Temp
2005/04/17 下午 06:12          <DIR>      WINDOWS
                4 個檔案          7,164,557 位元組
                4 個目錄          35,536,965,632 位元組可用

C:\>physdiskwrite generic-pc-1.2b7.img_
```

■ 不要選錯喔

# monowall 防火牆實作 (以DOM安裝為例)

■ 再確認一次

■ 開始寫入

```
C:\WINDOWS\system32\cmd.exe - physdiskwrite generic-pc-1.2b7

Information for \\.\PhysicalDrive0:
  Windows:      cyl: 4866
                tpc: 255
                spt: 63
  C/H/S:       16383/16/63
  Model:        MAXTOR 6L040L2
  Serial number: 662214729088
  Firmware rev.: A93.0500

Information for \\.\PhysicalDrive1:
  Windows:      cyl: 62
                tpc: 32
                spt: 63
  C/H/S:       978/4/32
  Model:        TRANSCEND DOM064M
  Serial number: SSSI064M05408T18402P
  Firmware rev.: 1.1

Information for \\.\PhysicalDrive2:
  Windows:      cyl: 12
                tpc: 255
                spt: 63

Which disk do you want to write? (0..2) 1
About to overwrite the contents of disk 1 with new data. Proceed? (y/n) y
```

```
Information for \\.\PhysicalDrive2:
  Windows:      cyl: 12
                tpc: 255
                spt: 63
```

```
Which disk do you want to write? (0..2) 1
About to overwrite the contents of disk 1 with new data. Proceed? (y/n) y
Found signed compressed image file
450560 bytes written
```

```
Which disk do you want to write? (0..2) 1
About to overwrite the contents of disk 1 with new data. Proceed? (y/n) y
Found signed compressed image file
7995392/7995392 bytes written in total
```

```
C:\>
```

■ 完成後回到C:\

## monowall 防火牆實作 (以DOM安裝為例)

- 再來將DOM插入你想要作防火牆的電腦IDE 插槽後，重新開機即可進入系統做初步設定。

```
*** This is m0n0wall, version 1.2b7
built on Sun Mar 20 18:45:04 CET 2005 for generic-pc
Copyright (C) 2002-2005 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1

Port configuration:

LAN   -> sis0
WAN   -> sis1

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 1
```

- 第一次開機，設定畫面
- 請選第一項，設定Interfaces

# monowall 防火牆實作 (以DOM安裝為例)

```
n8n8wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

fxp0  00:d0:b7:4d:ec:25  (up)
fxp1  00:d0:b7:4d:e9:ec
fxp2  00:d0:b7:4d:e9:f0

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces, you
should say no here and use the webGUI to configure VLANs later, if required.

Do you want to set up VLANs now? (y/n) █
```

■ 請選第一項,設定 Interfaces後,系統會告訴你,目前有幾張網卡?型號是  
多少的?還有目前哪張網卡已經接上HUB

■ 設定前會先問你  
要不要做VLANs  
設定

# monowall 防火牆實作 (以DOM安裝為例)

```
Valid interfaces are:

fxp0  00:d0:b7:4d:ec:25  (up)
fxp1  00:d0:b7:4d:e9:ee
fxp2  00:d0:b7:4d:e9:f0

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces, you
should say no here and use the webGUI to configure VLANs later, if required.
Do you want to set up VLANs now? (y/n) n

If you don't know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces before you begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection: fxp0
Enter the WAN interface name or 'a' for auto-detection: fxp1
Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): fxp2
Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):
```

■ 因為VLANs 設定都需搭配網管型交換器,這裡我們就先不設定

■ 依次在各項網路位置設定中,輸入你想要的網卡名稱

■ 不要輸入任何字來結束設定

# monowall 防火牆實作 (以DOM安裝為例)

```
Do you want to set up VLANs now? (y/n) n

If you don't know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces before you begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection: fxp0

Enter the WAN interface name or 'a' for auto-detection: fxp1

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): fxp2

Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:
LAN -> fxp0
WAN -> fxp1
OPT1 -> fxp2

The firewall will reboot after saving the changes.

Do you want to proceed? (y/n) y
```

- 結束設定後,會先顯示你剛剛所設的網路設定及網卡名稱。
- 並問你是否要啟動剛才的網路設定。
- 你按下 y 後電腦會重新開機。

# monowall 防火牆實作 (以DOM安裝為例)

```
*** This is n0n0wall, version 1.2b7
built on Sun Mar 28 18:45:04 CET 2005 for generic-pc
Copyright (C) 2002-2005 by Manuel Kasper. All rights reserved.
Visit http://n0n0.ch/wall for updates.

LAN IP address: 192.168.1.1

Port configuration:

LAN   -> fxp0
WAN   -> fxp1
OPT1  -> fxp2 (OPT1)

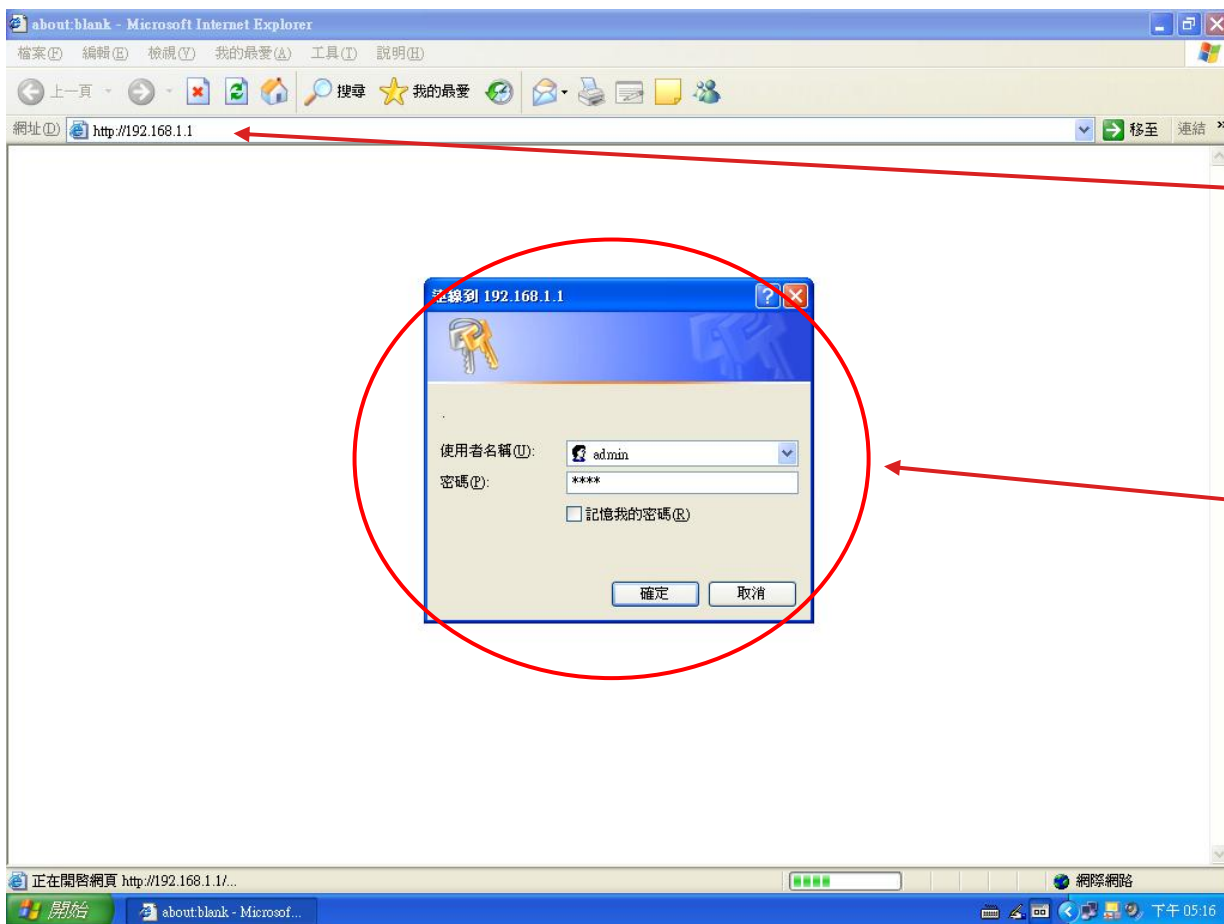
n0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: █
```

- 電腦重新開機後告訴你目前的網路設定及LAN的IP位址。
- 我們可以用系統所告知的IP,利用瀏覽器連上至該位址作更進一步的設定



# monowall 防火牆實作 (以DOM安裝為例)



- 利用系統所告知的 IP -192.168.1.1, 以瀏覽器連至該位址作更進一步的設定
- 設定時系統會問你的登錄帳號及密碼
- 系統內定  
登錄帳號：admin  
密碼：mono

# monowall 防火牆實作 (以DOM安裝為例)

System information	
Name	m0n0wall.local
Version	1.2b7 built on Sun Mar 20 18:45:04 CET 2005
Platform	generic-pc
Uptime	05:35
Last config change	Sun Apr 24 9:21:07 UTC 2005
CPU usage	view graph
Memory usage	<input type="text" value="9%"/>

- 好了,終於可以登錄進去看看了
- Monowall 系統就像一般市面上常見的嵌入式防火牆系統一樣,控制介面應有盡有

# m0n0wall 防火牆實作 (系統設定)

The screenshot shows the 'System: General setup' page in a Microsoft Internet Explorer browser. The page contains several configuration fields and a 'Save' button. Red arrows point from the Chinese text on the right to specific fields in the form:

- Hostname:** 'firewall' (points to the text box)
- Domain:** 'jsjhs.ntct.edu.tw' (points to the text box)
- DNS servers:** '163.22.54.1' and '163.22.168.1' (points to the list of IP addresses)
- Allow DNS server list to be overridden by DHCP/PPP on WAN:** Checked checkbox (points to the checkbox)
- Username:** 'admin' (points to the text box)
- Password:** '.....' (points to the password field)
- webGUI protocol:** 'HTTPS' selected (points to the radio button)
- webGUI port:** '9999' (points to the text box)
- Time zone:** 'Etc/UTC' (points to the dropdown menu)
- Time update interval:** '300' (points to the text box)
- NTP time server:** 'time.stdtime.gov.tw' (points to the text box)
- Save button:** (points to the 'Save' button)

System: General setup

Hostname: firewall  
name of the firewall host, without domain part  
e.g. *firewall*

Domain: jsjhs.ntct.edu.tw  
e.g. *mycorp.com*

DNS servers: 163.22.54.1  
163.22.168.1  
IP addresses; these are also used for the DHCP service, DNS forwarder and for PPTP VPN clients

Allow DNS server list to be overridden by DHCP/PPP on WAN  
If this option is set, m0n0wall will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS forwarder). They will not be assigned to DHCP and PPTP VPN clients, though.

Username: admin  
If you want to change the username for accessing the webGUI, enter it here.

Password: .....  
..... (confirmation)  
If you want to change the password for accessing the webGUI, enter it here twice.

webGUI protocol:  HTTP  HTTPS

webGUI port: 9999  
Enter a custom port number for the webGUI above if you want to override the default (80 for HTTP, 443 for HTTPS).

Time zone: Etc/UTC  
Select the location closest to you

Time update interval: 300  
Minutes between network time sync.; 300 recommended, or 0 to disable

NTP time server: time.stdtime.gov.tw  
Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if you enter a host name here!

Save

系統名稱

你學校的Domain

你想要的DNS主機IP

勾取此選項,則會覆蓋你在DHCP設定中的DNS選項

管理者帳號

管理者密碼

管理的登入協定(最好選HTTPS)

管理登入port(為了安全一定要作設定)

系統的工作時區(要選Asia/Taipei)

網路對時的時間間隔

網路校時主機(改設為time.stdtime.gov.tw)

記得按下儲存設定值

# monowall 防火牆實作 (系統設定)



webGUI Configuration

m0n0wall.local

## System

- General setup
- Static routes
- Firmware
- Advanced

## Interfaces (assign)

- LAN
- WAN
- OPT1

## Firewall

- Rules
- NAT
- Traffic shaper
- Aliases

## Services

- DNS forwarder
- Dynamic DNS
- DHCP server
- DHCP relay
- SNMP
- Proxy ARP
- Captive portal
- Wake on LAN

## VPN

- IPsec
- PPTP
- OpenVPN

## Status

- System
- Interfaces
- Traffic graph
- Wireless

## ▶ Diagnostics

### System: Static routes

Interface	Network	Gateway	Description
-----------	---------	---------	-------------



按下 + 號後  
會出現下列  
的對話欄位

一般學校對該項設定可以忽略，除非你像我一樣在內部規劃了很多子網段

### System: Static routes: Edit

#### Interface

LAN

Choose which interface this route applies to.

#### Destination network

/ 32

Destination network for this static route

#### Gateway

Gateway to be used to reach the destination network

#### Description

You may enter a description here for your reference (not parsed).

Save

下表為設定完成後的情形

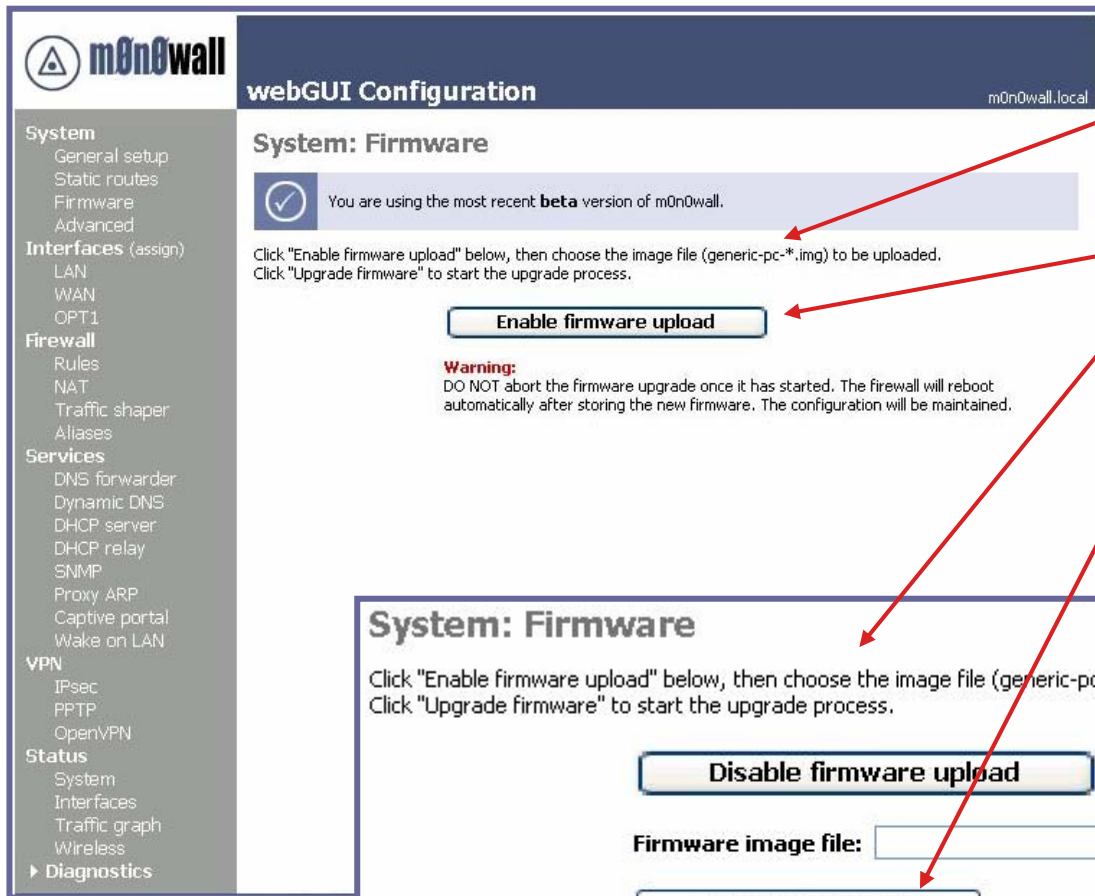
### System: Static routes

Interface	Network	Gateway	Description
WAN	172.22.1.0/24	172.22.0.240	
WAN	172.22.2.0/24	172.22.0.240	
WAN	172.22.3.0/24	172.22.0.3	
WAN	172.22.4.0/24	172.22.4.254	
WAN	172.22.5.0/24	172.22.5.254	
WAN	172.22.6.0/24	172.22.6.254	
WAN	172.22.7.0/24	172.22.0.240	



按下 x  
號後會  
刪除設  
定

# m0n0wall 防火牆實作 (系統設定)



- 韌體更新
- 首先確認你的韌體版本是否符合這個原則
- 按下啟動鈕後會出現下列選項
- 按瀏覽找到你的韌體檔案後，按 Upgrade 按鈕即可更新

取消更新

※系統內定是會檢查上載更新的韌體版本，是否比目前線上執行的新

※除非你在進階設定中勾選關閉韌體版本檢查

# monowall 防火牆實作 (系統設定)

**System: Advanced setup**

**Note:** the options on this page are intended for use by advanced users only, and there's **NO** support for them.

**IPv6 tunneling**

NAT encapsulated IPv6 packets (IP protocol 41/RFC2893) to:  
[ ] (IP address)  
Don't forget to add a firewall rule to permit IPv6 packets!

**Save**

**Filtering bridge**

Enable filtering bridge  
This will cause bridged packets to pass through the packet filter in the same way as routed packets do (by default bridged packets are always passed). If you enable this option, you'll have to add filter rules to selectively permit traffic from bridged interfaces.

**Save**

**webGUI SSL certificate/key**

Certificate  
[ ]  
Paste a signed certificate in X.509 PEM format here.

Key  
[ ]  
Paste an RSA private key in PEM format here.

**Save**

**Miscellaneous**

■ 進階設定(一)

■ 啟動IPv6 to IPv4 NAT

■ 啟動防火牆的 bridge功能

■ 進入管理介面時所需的自訂公鑰 (一般可忽略)

# m0n0wall 防火牆實作 (系統設定)

Miscellaneous	
Console menu	<input type="checkbox"/> <b>Disable console menu</b> Changes to this option will take effect after a reboot.
Firmware version check	<input type="checkbox"/> <b>Disable firmware version check</b> This will cause m0n0wall not to check for newer firmware versions when the <a href="#">System: Firmware</a> page is viewed.
TCP idle timeout	<input type="text" value="2.5"/> seconds Idle TCP connections will be removed from the state table after no packets have been received for the specified number of seconds. Don't set this too high or your state table could become full of connections that have been improperly shut down. The default is 2.5 hours.
Hard disk standby time	<input type="text" value="Always on"/> Puts the hard disk into standby mode when the selected amount of time after the last access has elapsed. <i>Do not set this for CF cards.</i>
Navigation	<input type="checkbox"/> <b>Keep diagnostics in navigation expanded</b>
Static route filtering	<input type="checkbox"/> <b>Bypass firewall rules for traffic on the same interface</b> This option only applies if you have defined one or more static routes. If it is enabled, traffic that enters and leaves through the same interface will not be checked by the firewall. This may be desirable in some situations where multiple subnets are connected to the same interface.
webGUI anti-lockout	<input type="checkbox"/> <b>Disable webGUI anti-lockout rule</b> By default, access to the webGUI on the LAN interface is always permitted, regardless of the user-defined filter rule set. Enable this feature to control webGUI access (make sure to have a filter rule in place that allows you in, or you will lock yourself out!). Hint: the "set LAN IP address" option in the console menu resets this setting as well.

## 進階設定(二)

關閉主機console端的選項(啟動這選項後連主機端都無法更改設定值)

關閉韌體版本檢查

移除閑置的連線程序之時間值(內定是2.5小時)

硬碟進入待機時間

啟動防火牆不檢查在同一網路介面中作路由傳送的封包

啟動管理介面鎖定。(除非在防火牆規則中有設定,否則你將無法由瀏覽器及基本設定中指定的port進入管理介面,建議先不要勾選)

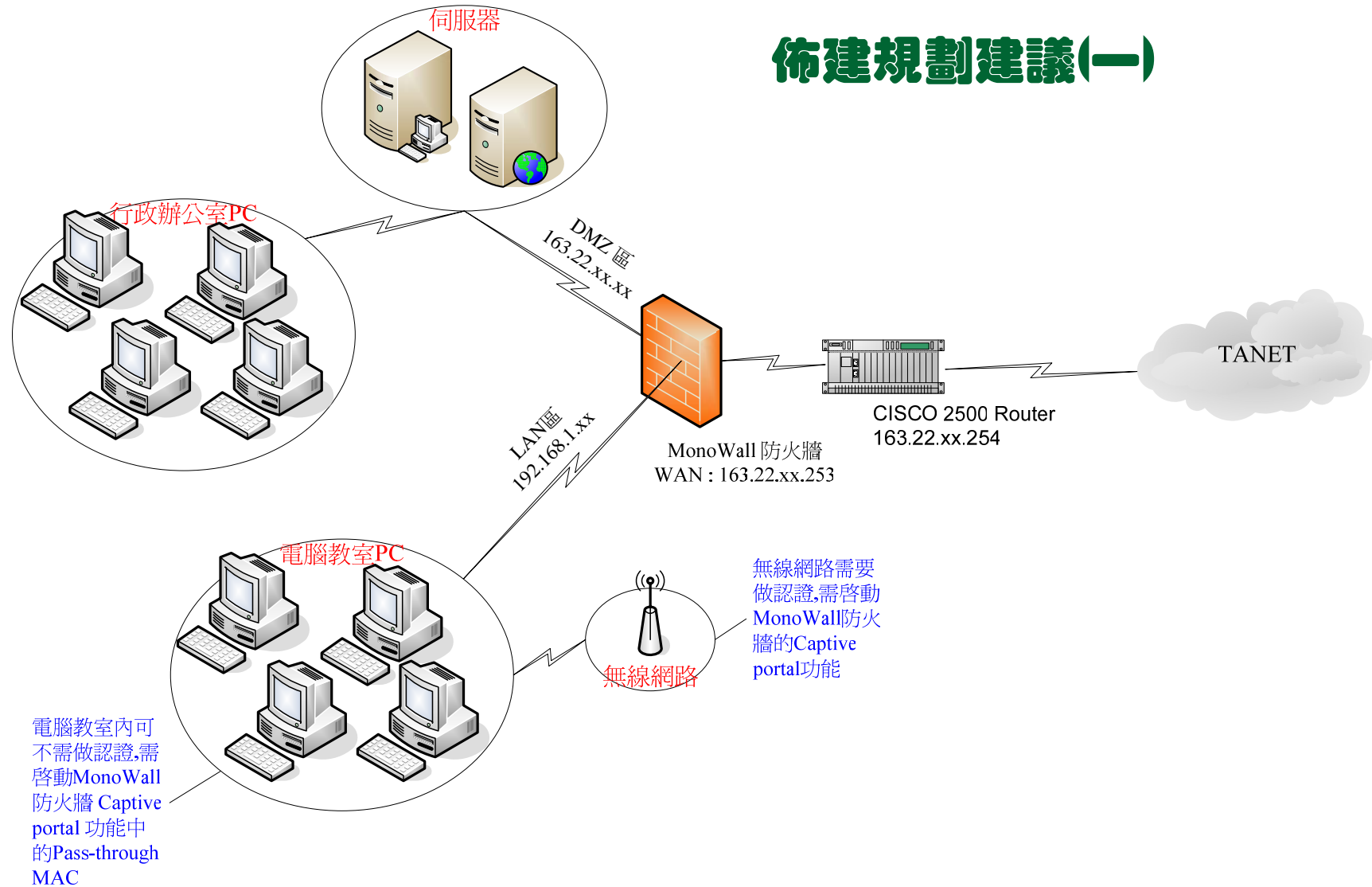
---

**使用monowall防火牆但  
不取代CISCO Router**

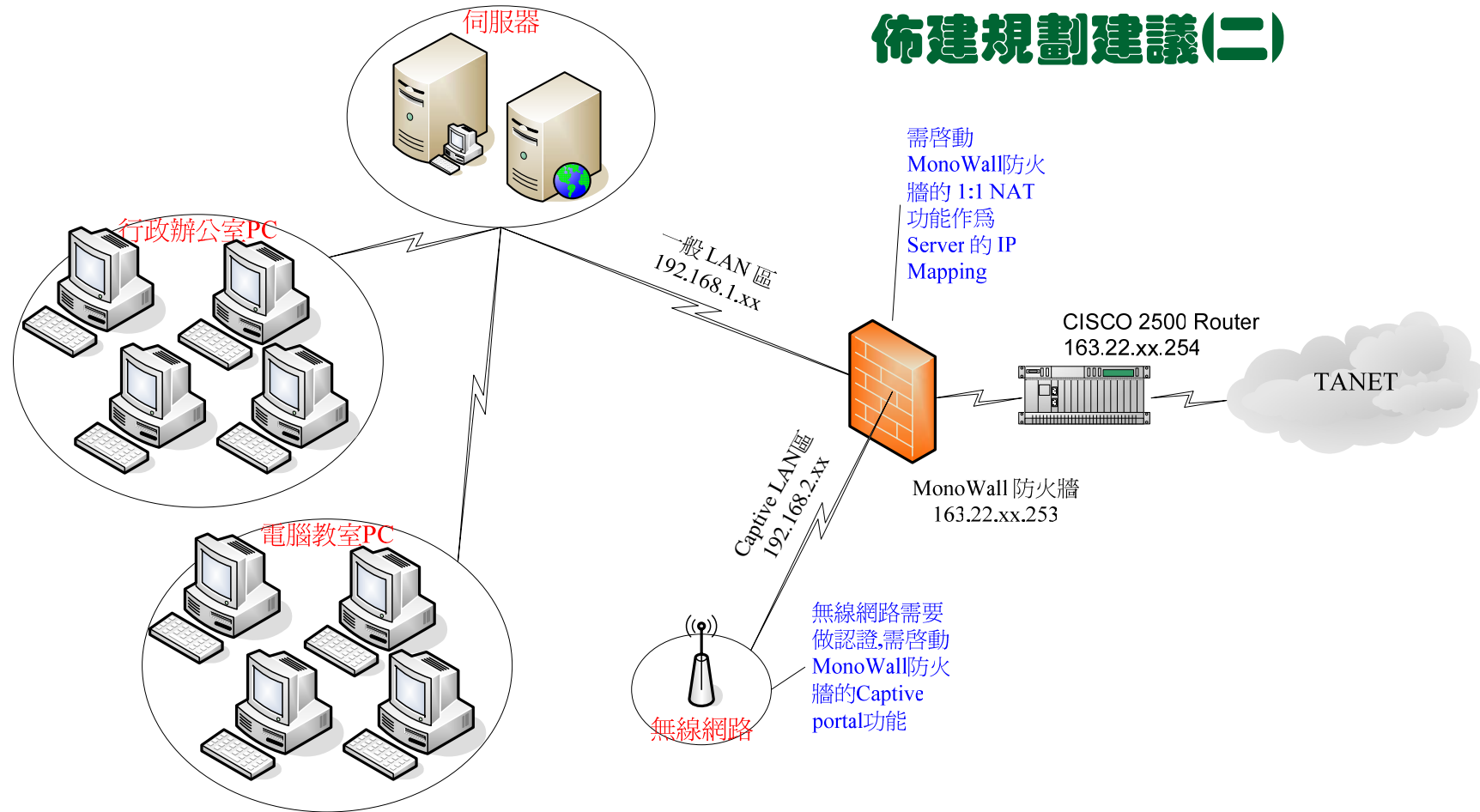
---



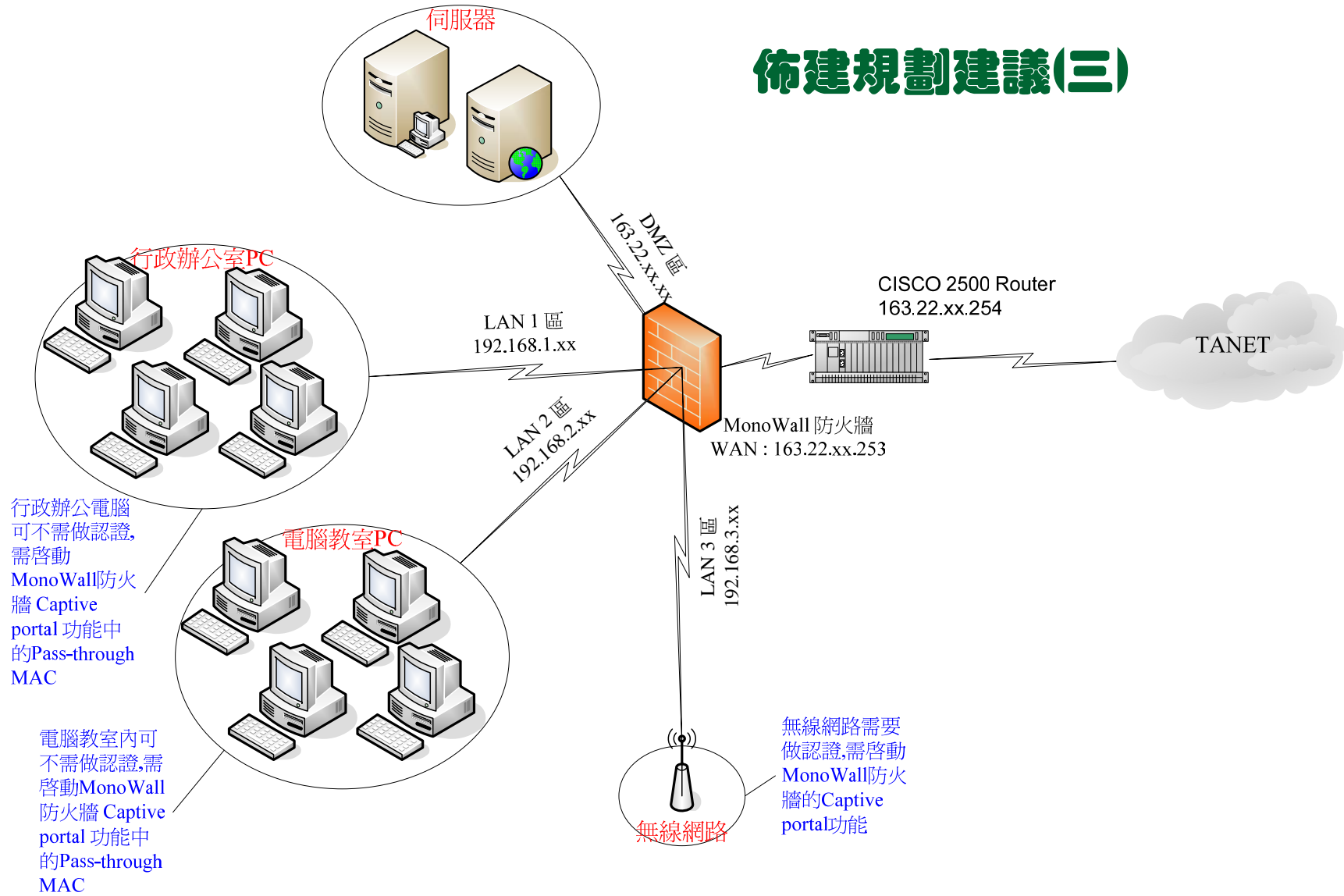
# 佈建規劃建議(一)



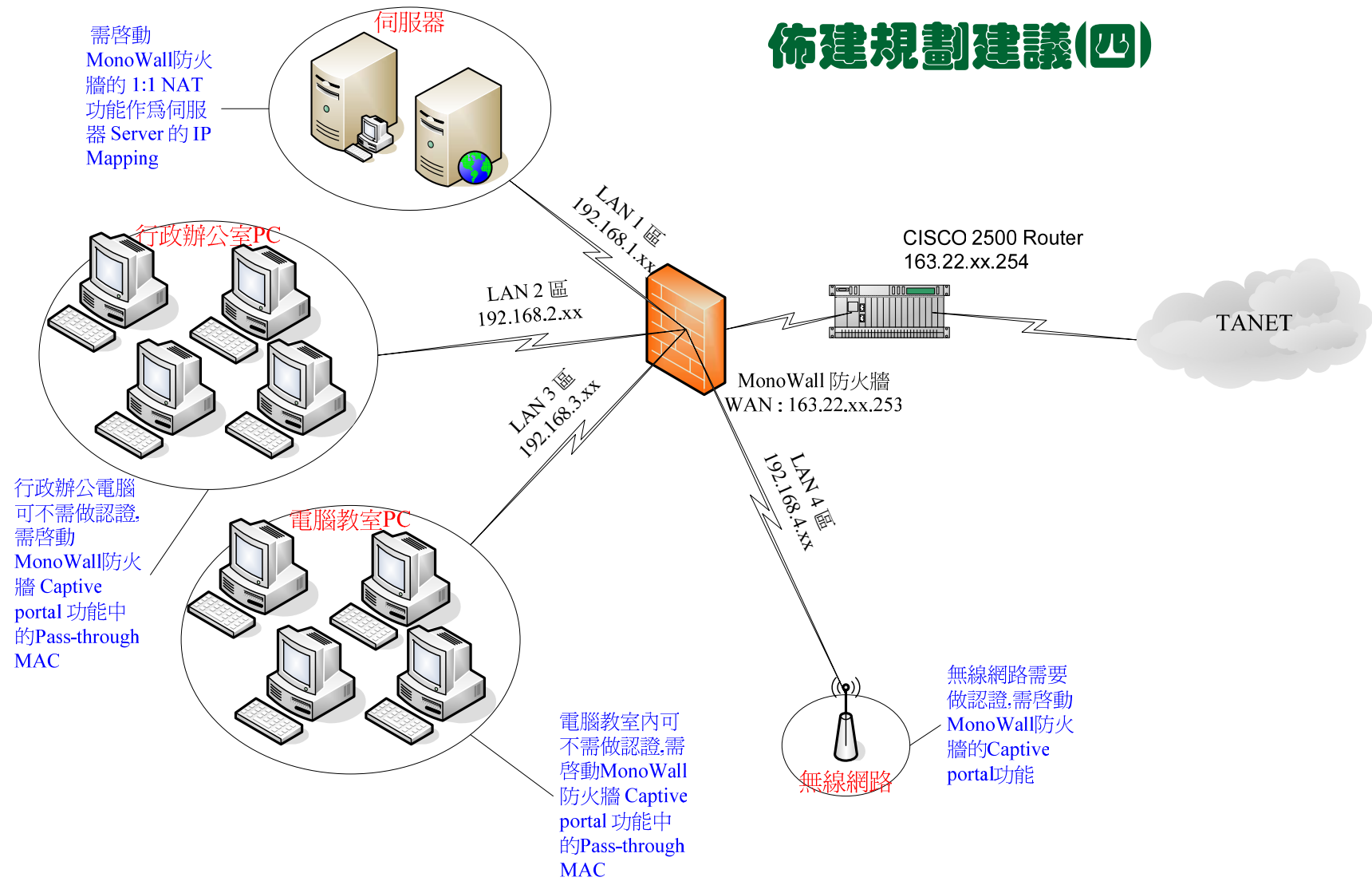
## 佈建規劃建議(二)



# 佈建規劃建議(三)



# 佈建規劃建議(四)

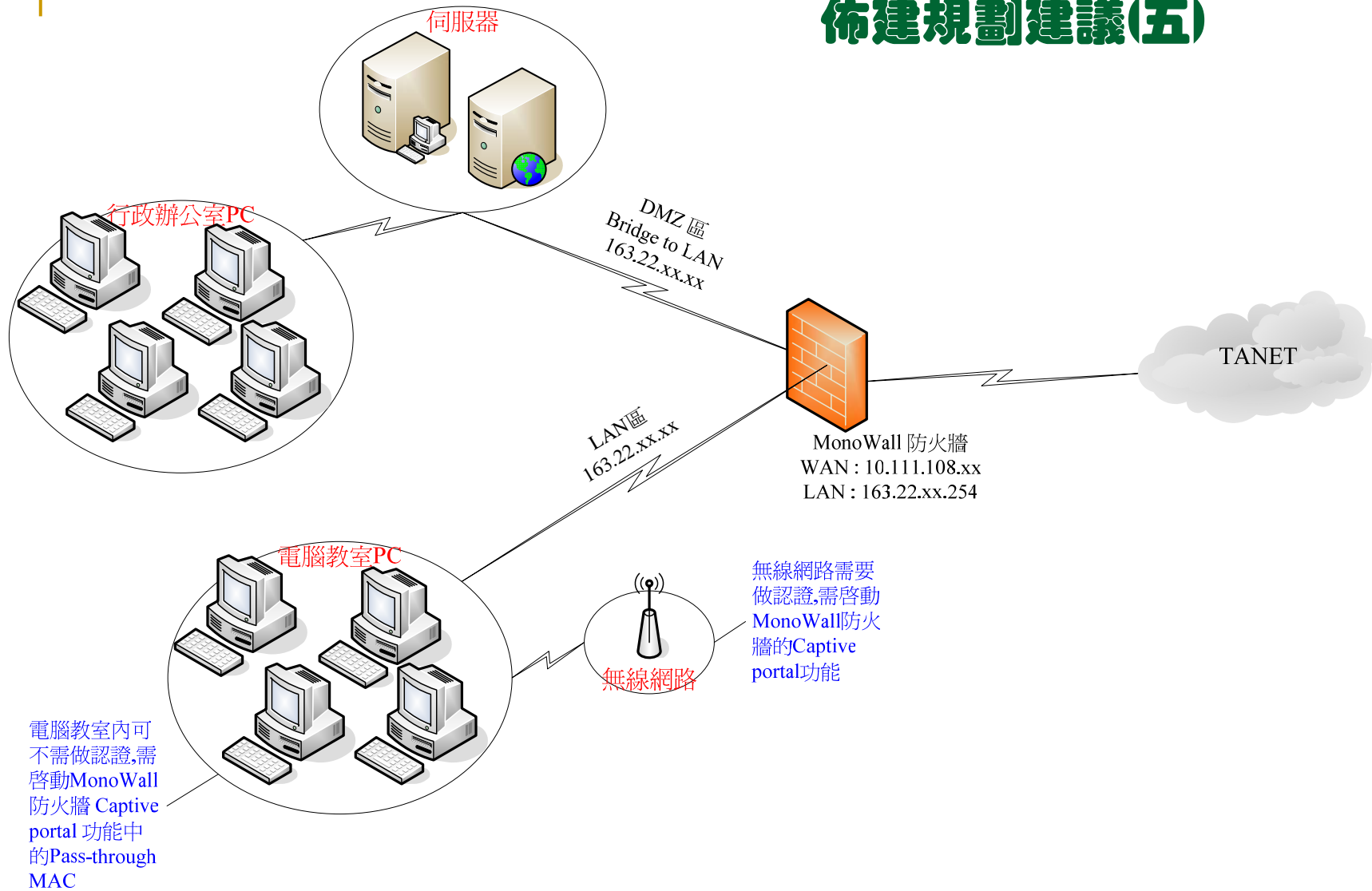


---

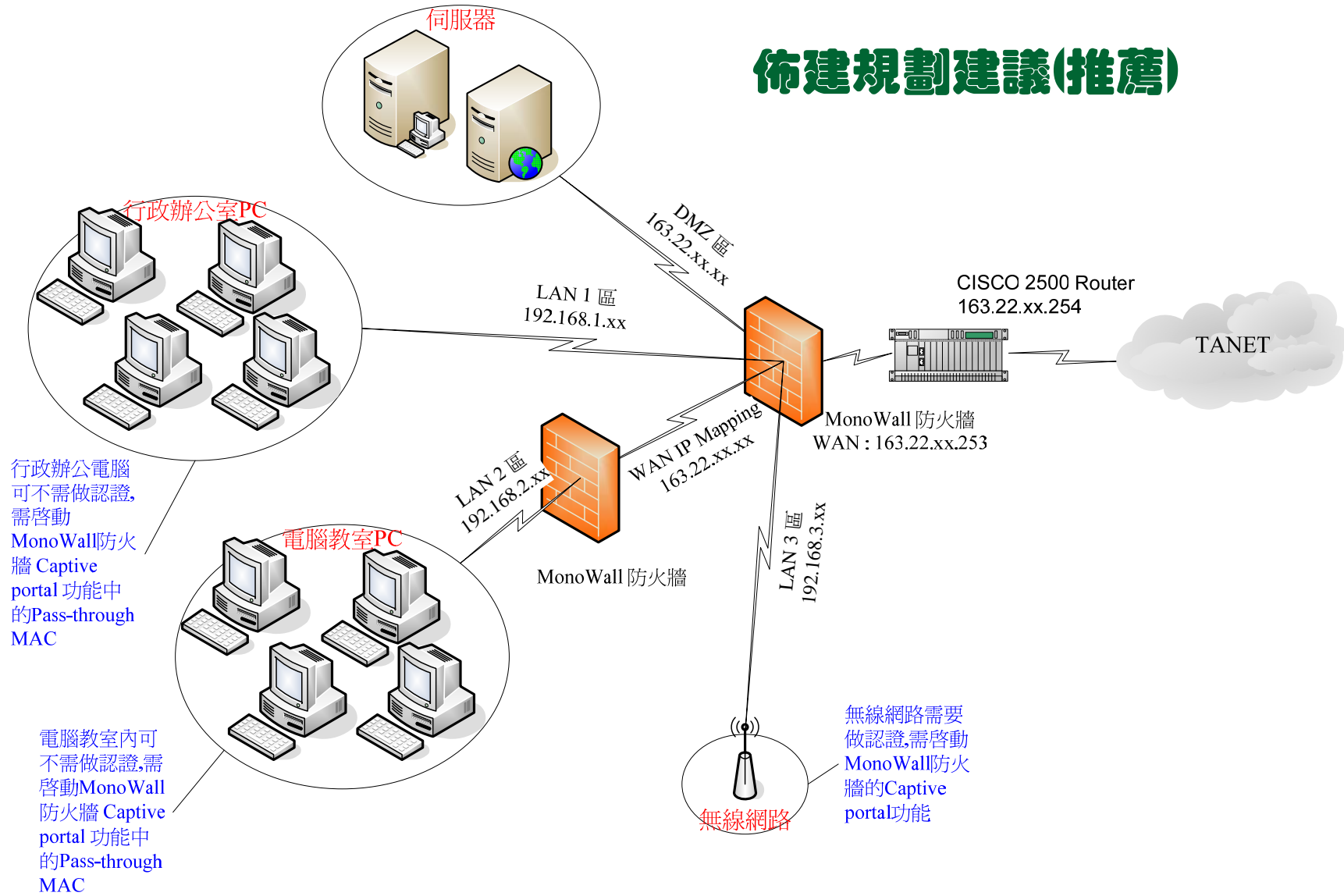
# 利用monowall防火牆取代 CISCO Router

---

## 佈建規劃建議(五)



# 佈建規劃建議(推薦)



---


# 以規劃建議(一)實作設定

---



# monowall 防火牆實作 (WAN設定)

**Interfaces: WAN**

 The changes have been saved. You must reboot your firewall for changes to take effect.

**Type**  ▼

**General configuration**

**MAC address**   
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

**MTU**   
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

**Static IP configuration**

**IP address**  /  ▼

**Gateway**

**DHCP client configuration**

**Hostname**   
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

- WAN的設定共有5種 Static (固定IP式), DHCP (動態取得式), PPPoE (ADSL 撥接式), PPTP (一般撥接式), BigPond Cable (有線電視纜線式)

- 學校請使用Static

- 若有特殊需求可以設定WAN對外的MAC Address

- WAN端的IP及遮罩, 檢查一下學校自己的區段

- WAN端的匝道位址, 一般是設定你的Router的IP

# m0n0wall 防火牆實作 (DMZ設定)

第1步：選擇要設訂的網卡

第2步：勾選要啟動網卡設定

第3步：輸入網卡的描述名稱

System  
General setup  
Static routes  
Firmware  
Advanced

Interfaces (assign)  
LAN  
WAN  
OPT1

Firewall  
Rules  
NAT  
Traffic shaper  
Aliases

Services  
DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP

## webGUI Configuration

m0n0wall,loc

### Interfaces: Optional 1 (OPT1)

Enable Optional 1 interface

Description: DMZ  
Enter a description (name) for the interface here.

Bridge with: WAN

IP address: / 31

Save

**Note:**  
be sure to add firewall rules to permit traffic through the interface. Firewall rules for an interface in bridged mode have no effect on packets to hosts other than m0n0wall itself, unless "Enable filtering bridge" is checked on the System: Advanced Functions page.

System  
General setup  
Static routes  
Firmware  
Advanced

Interfaces (assign)  
LAN  
WAN  
DMZ

Firewall  
Rules  
NAT  
Traffic shaper  
Aliases

會單完 變上變 網網 卡卡 名更 稱後 選

※ bridge 的功能啟動後此項無法再做設定

第4步：選擇要作Bridge的網卡

第5步：記得要在進階設定中啟動 filtering bridge 的功能

---

# Monowall 防火牆 Rules 設定

(使學生的電腦僅能連到學術網路或被允許的網站)

---

# monowall 防火牆實作 (Rule設定)

The image shows three screenshots of the monowall Firewall: Rules configuration interface, stacked vertically. Each screenshot shows a different interface: LAN, WAN, and DMZ.

**LAN Screenshot:** Shows a table with one rule. The rule is enabled (checkbox checked) and has a green up arrow. The rule details are: Proto: \*, Source: LAN net, Port: \*, Destination: \*, Port: \*, Description: Default LAN -> any.

Proto	Source	Port	Destination	Port	Description
*	LAN net	*	*	*	Default LAN -> any

**WAN Screenshot:** Shows a message: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the + button to add a new rule."

**DMZ Screenshot:** Shows a message: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until you add pass rules. Click the + button to add a new rule."

**Legend:**

- ↑ pass
- ↑ pass (disabled)
- ✗ block
- ✗ block (disabled)
- ✗ reject
- ✗ reject (disabled)
- 📄 log
- 📄 log (disabled)

- LAN的Rules內定是設成any to any,可以進入管理畫面
- WAN的Rules內定是不作管制,但無法由WAN進入管理畫面
- DMZ的Rules同樣是不作管制,且與WAN相同是無法進入管理畫面的

# monowall 防火牆實作 (Rule設定)

Firewall: Rules

LAN WAN DMZ

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> ↑	*	LAN net	*	*	*	Default LAN -> any

↑ pass     block     reject     log  
 ↑ pass (disabled)     block (disabled)     reject (disabled)     log (disabled)

- 按+新增Rule設定
- 按這+是加在這一條Rule的後面
- 按這+是加在所有Rule的後面

按 + 新加一個Rule後會出現這個編輯視窗。

Firewall: Rules: Edit

**Action** Block   
 Choose what to do with packets that match the criteria specified below.  
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.

**Disabled**  Disable this rule  
 Set this option to disable this rule without removing it from the list.

**Interface** LAN   
 Choose on which interface packets must come in to match this rule.

**Protocol** any   
 Choose which IP protocol this rule should match.  
 Hint: in most cases, you should specify TCP here.

**ICMP type** any   
 If you selected ICMP for the protocol above, you may specify an ICMP type here.

- 選擇Block,因為我們要先將所有對外的封包給擋掉
- 選擇網路介面
- 選擇通訊協定
- 此選項僅在通訊協定選擇ICMP時才有作用

# monowall 防火牆實作 (Rule設定)

<b>Source</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: LAN subnet Address: /
<b>Source port range</b>	from: any to: any Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the %o' field empty if you only want to filter a single port
<b>Destination</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: any Address: /
<b>Destination port range</b>	from: any to: any

封包來源選擇LAN的子網段

目的地選擇any表示全部

<b>Fragments</b>	<input type="checkbox"/> <b>Allow fragmented packets</b> Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.
<b>Log</b>	<input type="checkbox"/> <b>Log packets that are handled by this rule</b> Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the <a href="#">Diagnostics: System logs: Settings</a> page).
<b>Description</b>	Set Blok LAN -> any You may enter a description here for your reference (not parsed).


**Save**

若檢查有符合規則的封包就做紀錄

規則描述說明

# monowall 防火牆實作 (Rule設定)

Firewall: Rules

 The firewall rule configuration has been changed.  
You must apply the changes in order for them to take effect.

**Apply changes**

LAN **WAN** DMZ

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> ↑	*	LAN net	*	*	*	Default LAN -> any	← ⊕
<input type="checkbox"/> ×	*	*	*	*	*	Set Blok LAN -> any	← ⊕

↑ pass    × block    × reject    📄 log  
↑ pass (disabled)    × block (disabled)    × reject (disabled)    📄 log (disabled)

■ 完成後可看到多了一條Rule

■ Rule設定原則是先將所有的封包都擋掉,再將想要通的介面打開

■ 再來是要把剛剛設定的Rule移至上方

先選擇要移動的Rule

■ 再選擇要移去的位置點的←

LAN **WAN** DMZ

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> ↑	*	LAN net	*	*	*	Default LAN -> any	← ⊕
<input checked="" type="checkbox"/> ×	*	*	*	*	*	Set Blok LAN -> any	← ⊕

↑ pass    × block    × reject    📄 log  
↑ pass (disabled)    × block (disabled)    × reject (disabled)    📄 log (disabled)

# monowall 防火牆實作 (Rule設定)

Apply changes

LAN WAN DMZ

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> ❌	*	*	*	*	*	Set Blok LAN -> any	← e +
<input type="checkbox"/> ⬆️	*	LAN net	*	*	*	Default LAN -> any	← e +

⬆️ pass    ❌ block    ❌ reject    📄 log  
⬆️ pass (disabled)    ❌ block (disabled)    ❌ reject (disabled)    📄 log (disabled)

- 移動完成後可看到 Rule的位置改變了
- Rule的前後位置影響執行的順序,越上方的規則越後執行
- Rule的規則變更後記得要按才會真正執行, (但現在請不要按,以免你無法登錄管理畫面)

<input type="checkbox"/> ⬆️	*	LAN net	*	210.243.0.0/17	*	Default LAN -> TANET	← e +
<input type="checkbox"/> ⬆️	*	LAN net	*	163.22.0.0/16	*	Default LAN -> 163.22.0.0/16	← e +
<input type="checkbox"/> ⬆️	*	LAN net	*	172.22.0.0/16	*	Default LAN -> Internal	← e +
<input type="checkbox"/> ❌	*	LAN net	*	*	*	Set Blok LAN -> any	← e +
<input type="checkbox"/> ⬆️	*	LAN net	*	*	*	Default LAN -> any	← e +

⬆️ pass    ❌ block    ❌ reject    📄 log  
⬆️ pass (disabled)    ❌ block (disabled)    ❌ reject (disabled)    📄 log (disabled)

- 請依前面所教授之辦法逐步輸入各TANET的網段是可通行的



# monowall 防火牆實作 (Rule設定)

134.208.0.0/16	192.83.192.0/22
140.109.0.0/16	192.83.196.0/24
140.110.0.0/15	203.64.0.0/16
140.112.0.0/12	203.68.0.0/16
140.128.0.0/13	203.71.0.0/16
140.136.0.0/15	203.72.0.0/16
140.138.0.0/16	210.200.32.0/19
140.92.0.0/16	210.240.0.0/16
140.96.0.0/16	210.243.0.0/17
163.13.0.0/16	210.59.0.0/16
163.14.0.0/15	210.60.0.0/16
163.16.0.0/13	210.62.224.0/20
163.24.0.0/14	210.62.240.0/21
163.28.0.0/16	210.62.64.0/19
192.192.0.0/16	210.70.0.0/16
192.83.166.0/23	210.71.0.0/17
192.83.168.0/21	208.37.27.8
192.83.176.0/20	

- TANET IP 網段

# monowall 防火牆實作 (Rule設定)

Firewall: Rules

The firewall rule configuration has been changed. You must apply the changes in order for them to take effect.

Apply changes

LAN WAN **DMZ**

Proto	Source	Port	Destination	Port	Description
TCP	DMZ net	*	WAN address	9999	DMZ => LOCAL

pass block reject log  
pass (disabled) block (disabled) reject (disabled) log (disabled)

■ 選擇Rule建立區在DMZ

■ 新建一條規則,讓你可以從DMZ區連上系統的管理port位址

■ Rule的規則變更後記得要按才會真正執行, (現在可以按了,因為你已經設定可以登錄的規則了,執行後仍可以登錄管理畫面)

這個port 是你在基本設定中所設定的

---

**Monowall NAT管理設定**

**Monowall 頻寬管理設定**

**Monowall DNS管理設定**

**Monowall DHCP管理設定**

**Monowall 認證管理設定**

**待續**

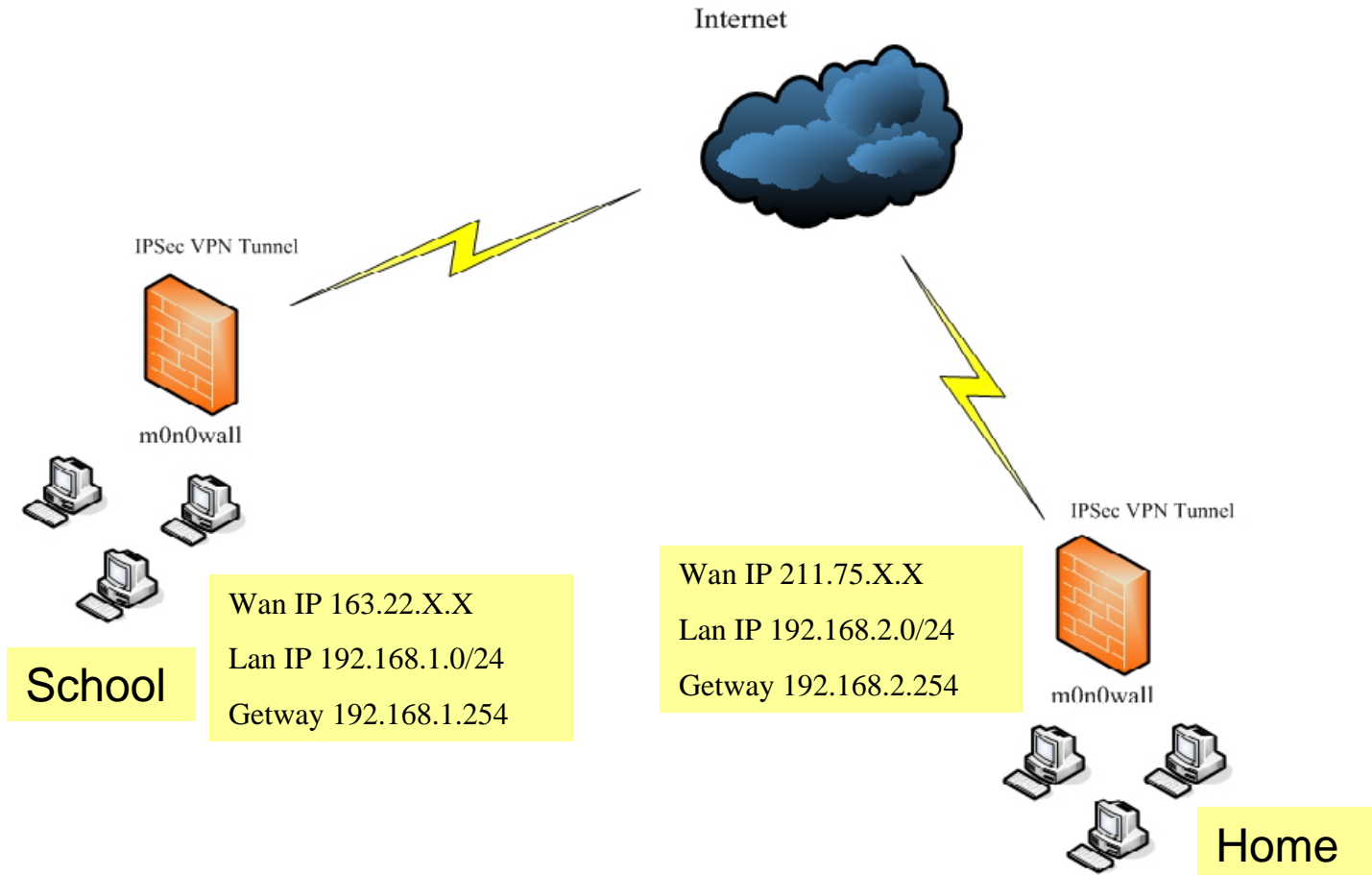
---

---

# 如何利用 monowall 防火牆建構你個人與學校間私人專屬VPN管理通道

---

# monowall 防火牆 VPN 實作



# monowall 防火牆 VPN 實作 (1)

- 首先學校這邊因為要先做測試，所以先將 firewall WAN rule 全開這樣比較方便設定：

## Firewall: Rules

LAN WAN OPT1

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> ↑	*	*	*	*	*		← e + ← x +

↑ pass    ✗ block    ✗ reject    📄 log  
↑ pass (disabled)    ✗ block (disabled)    ✗ reject (disabled)    📄 log (disabled)

- 接下來學校這邊加入 Route rules

## System: Static routes

Interface	Network	Gateway	Description	
WAN	192.168.2.0/24	192.168.1.254	Route to Home	e x +

# monowall 防火牆 VPN 實作 (2)

- 最後學校這邊設定 VPN 的 Tunnels IPsec :

## VPN: IPsec



The changes have been applied successfully.

Tunnels

Mobile clients

Pre-shared keys

Enable IPsec

Save

Local net Remote net	Interface Remote gw	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
LAN 192.168.2. 0 / 24	WAN 163 . 22 . X . X	main	3DES	SHA1	



記得要勾選

# monowall 防火牆 VPN 實作 (3)

- 再來家裡這邊同樣的先將 firewall WAN rule 全開這樣比較方便測試：

## Firewall: Rules

LAN WAN OPT1

	Proto	Source	Port	Destination	Port	Description	
<input type="checkbox"/> ↑	*	*	*	*	*		← e + ← x +

↑ pass    ✗ block    ✗ reject    📄 log  
↑ pass (disabled)    ✗ block (disabled)    ✗ reject (disabled)    📄 log (disabled)

- 接下來家裡這邊加入 Route rules

## System: Static routes

Interface	Network	Gateway	Description	
WAN	192.168.1.0/24	192.168.2.254	Route to School	e x +



# monowall 防火牆 VPN 實作 (2)

- 最後學校這邊設定 VPN 的 Tunnels IPsec :

## VPN: IPsec



The changes have been applied successfully.

Tunnels

Mobile clients

Pre-shared keys

Enable IPsec

Save

Local net Remote net	Interface Remote gw	P1 mode	P1 Enc. Algo	P1 Hash Algo	Description
LAN 192.168.1.0/24	WAN 211.75.X.X	main	3DES	SHA1	



記得要勾選

- 最後學校及家裡已建立 IPsec 的 VPN tunnel 我們可用 **Diagnostics: Ping** 來測試看看可否可以 ping 到對方 gateway

- 使用心得：以 K6-2-350、128MB RAM、2張 Intel 100 pro 網卡、撐電腦教室的 45 部電腦正常上網沒什問題。若機器用高檔一點能支撐的電腦數也會增加，但想一想用一台 P4-3G、512MB RAM、3張 Intel 1000 pro 網卡，這樣值得嗎？
- 不保證反應速度像硬體式的一樣快但它至少對經費困難的學校而言，是一個容易取得的安全防護