

PFSENSE

無線網路管理與驗證

育達高中 張以勤

yaichin@yuda.tyc.edu.tw

PFSENSE軟體防火牆簡介

- OPEN SOURCE
- Based on FreeBSD
- 簡單易用
- 外掛軟體眾多
- 硬體需求低

- 硬體相容性清單

<http://www.freebsd.org/releases/10.1R/hardware.html>

Hardware Requirements

The following outlines the minimum hardware requirements for pfSense 2.x. Note the minimum requirements are not suitable for all environments. You may be able to get by with less than the minimum, but with less memory you may start swapping to disk, which will dramatically slow down your system.

General Requirements:

Minimum

- CPU - 500 Mhz
- RAM - 256 MB

Recommended

- CPU - 1 Ghz
- RAM - 1 GB

Requirements Specific to Individual Platforms:

Live CD/USB

- CD-ROM or USB drive
- USB flash drive to hold configuration file

Hard Drive

- CD-ROM or USB for initial installation
- 1 GB hard drive

Embedded

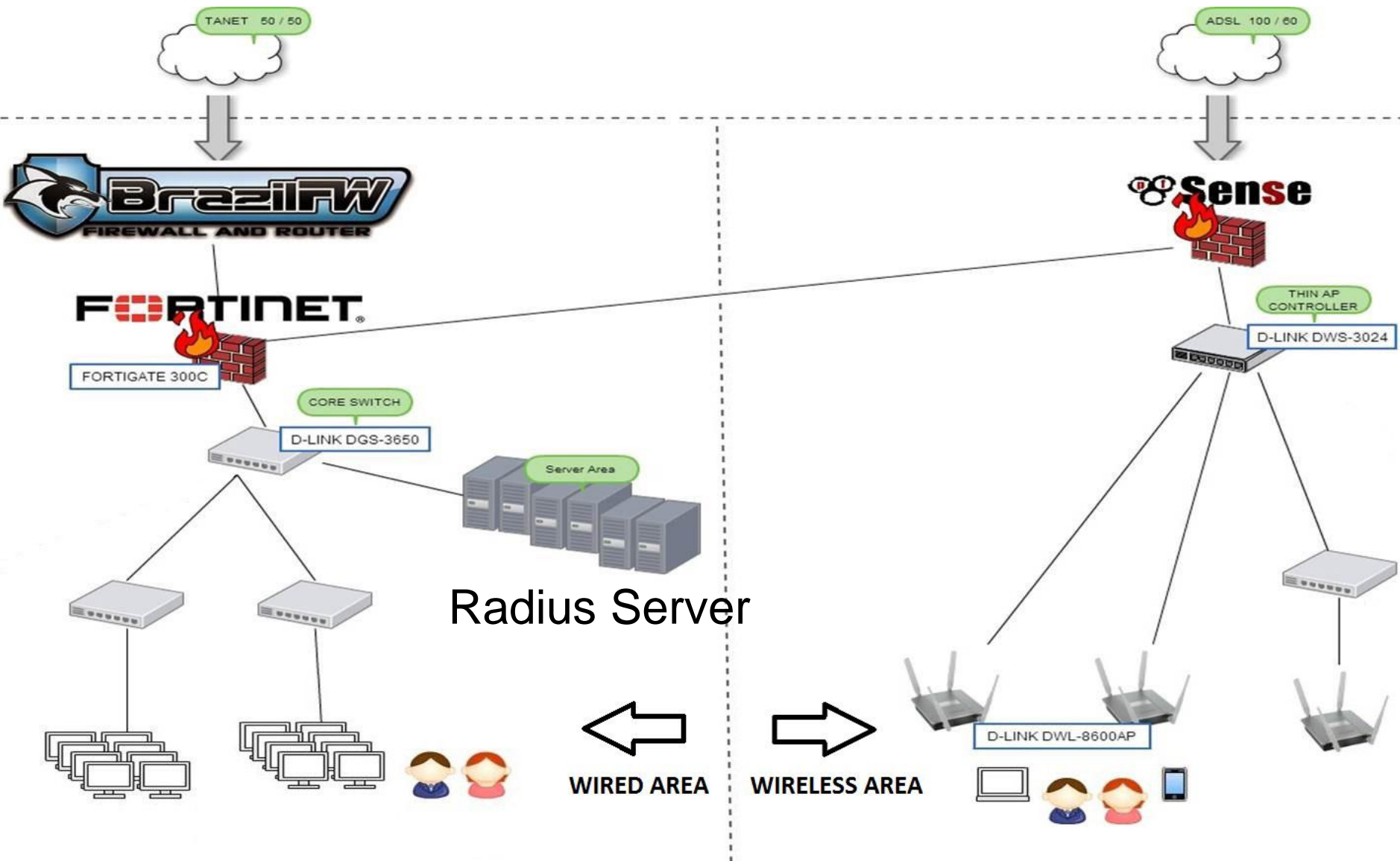
- 1 GB Compact Flash card
- Serial port for console

本校使用的硬體
CPU E5800
8GB RAM

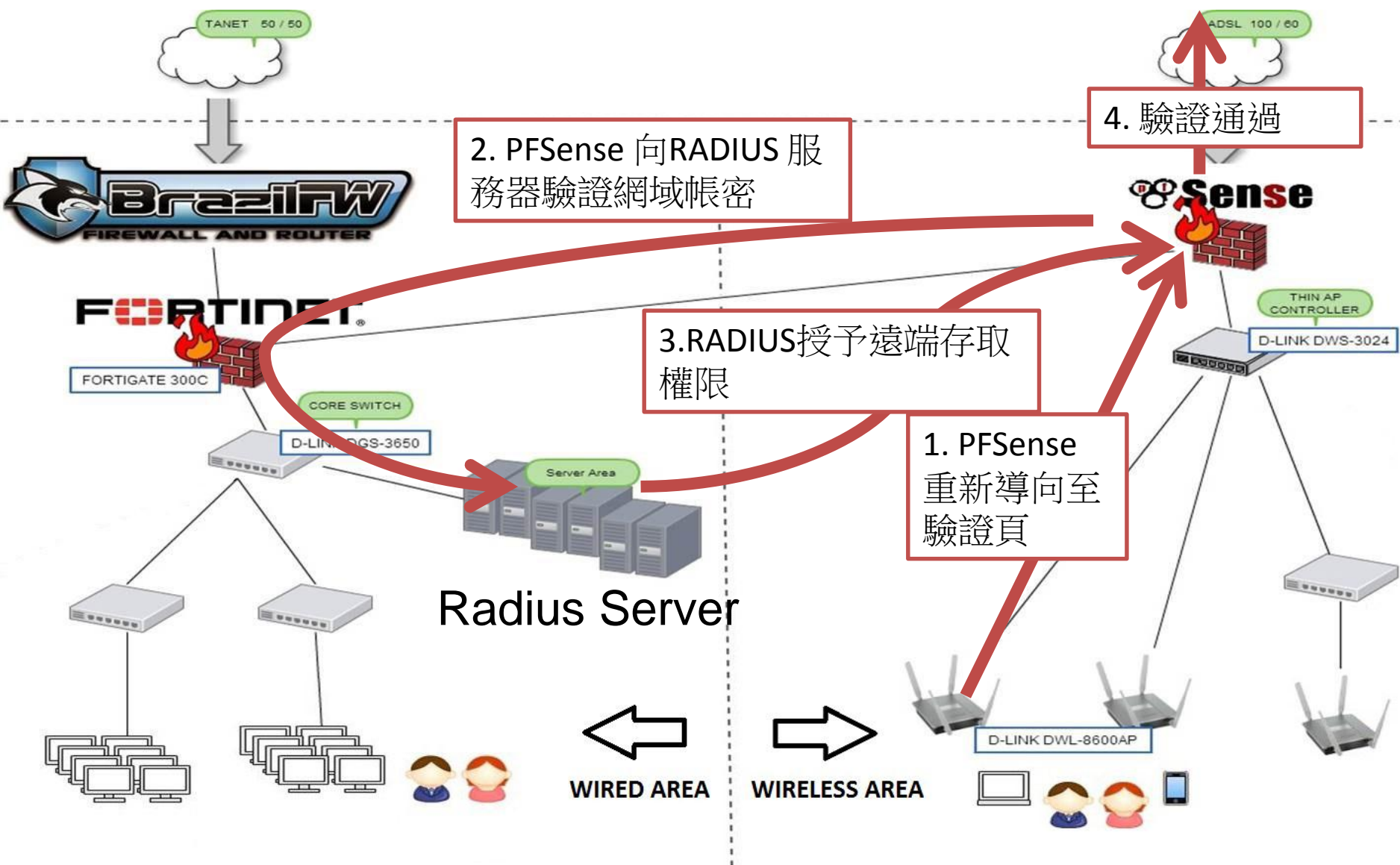
WHY PFSENSE

- FREE
- 資源再利用
- 安裝容易
- 備份方便
- 回復快速

有線與無線網路架構



WIFI AD 驗證流程



PFSense 驗證頁- Captive portal

連上AP後打開 browser 會自動導向到驗證畫面



The screenshot shows a captive portal login page for YUDA Wireless. The page has a blue and white background with a circuit-like pattern. At the top right, it says "YUDA Wireless" with a plus sign and some cube icons. Below that, the text "internet in everywhere" is displayed. The main title is "育達高級中學-無線網路驗證系統". There are three input fields: "帳號" (Username), "密碼" (Password), and "驗證碼" (Verification Code) with a note "(外賓用)" (For guests). A "Continue" button is below the fields. At the bottom, there is a notice: "請使用育達網域帳號登入" (Please use YUDA domain account to log in), "網路使用由資訊中心監管中" (Network usage is supervised by the Information Center), and "非公務用途佔用大量頻寬者停權處理" (Users who occupy a large amount of bandwidth for non-official purposes will be suspended). There is also a small text "啟用 W" and "移至 [管理]" in the bottom right corner.

YUDA Wireless
+
internet in everywhere
育達高級中學-無線網路驗證系統

帳號

密碼

驗證碼 (外賓用)

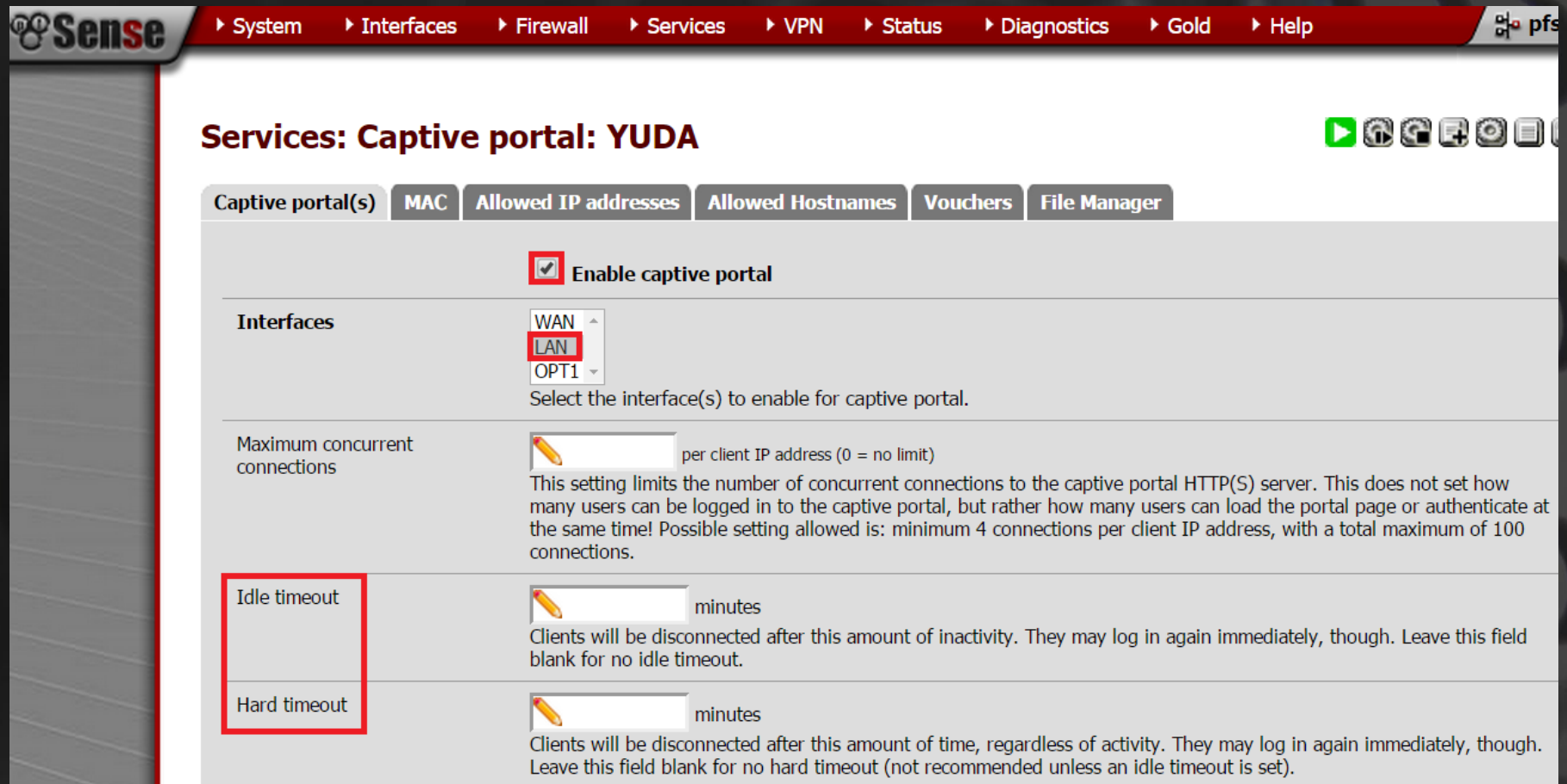
Continue

請使用育達網域帳號登入
網路使用由資訊中心監管中
非公務用途佔用大量頻寬者停權處理

啟用 W
移至 [管理]

(驗證頁可自行客製化)

PFSense Captive portal 1



The screenshot shows the pfsense web interface. The top navigation bar is red with the pfsense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled "Services: Captive portal: YUDA" with a green play button icon. Below the title is a tabbed interface with tabs for "Captive portal(s)", "MAC", "Allowed IP addresses", "Allowed Hostnames", "Vouchers", and "File Manager". The "Captive portal(s)" tab is active. It contains a checkbox labeled "Enable captive portal" which is checked. Below this is a section for "Interfaces" with a dropdown menu showing "WAN", "LAN", and "OPT1". The "LAN" option is selected and highlighted with a red box. Below the dropdown is the text "Select the interface(s) to enable for captive portal." There are three more settings: "Maximum concurrent connections" with a text input field and a description; "Idle timeout" with a text input field and a description; and "Hard timeout" with a text input field and a description. The "Idle timeout" and "Hard timeout" labels are highlighted with red boxes.

Services: Captive portal: YUDA

Captive portal(s) | MAC | Allowed IP addresses | Allowed Hostnames | Vouchers | File Manager

☒ **Enable captive portal**

Interfaces

WAN
LAN
OPT1

Select the interface(s) to enable for captive portal.

Maximum concurrent connections

per client IP address (0 = no limit)

This setting limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many users can load the portal page or authenticate at the same time! Possible setting allowed is: minimum 4 connections per client IP address, with a total maximum of 100 connections.

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

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).

PFSense Captive portal 2

Per-user bandwidth restriction	<input checked="" type="checkbox"/> Enable per-user bandwidth restriction
	Default download <input type="text"/> Kbit/s
	Default upload <input type="text"/> Kbit/s
<p>If this option is set, the captive portal will restrict each user who logs in to the specified default bandwidth. RADIUS can override the default settings. Leave empty or set to 0 for no limit.</p>	
<hr/>	
Authentication	<input type="radio"/> No Authentication
	<input type="radio"/> Local User Manager / Vouchers
	<input checked="" type="checkbox"/> Allow only users/groups with 'Captive portal login' privilege set
	<input checked="" type="radio"/> RADIUS Authentication
	RADIUS Protocol
	<input type="radio"/> PAP
	<input type="radio"/> CHAP_MD5
	<input type="radio"/> MSCHAPv1
	<input checked="" type="radio"/> MSCHAPv2
<hr/>	
Primary Authentication Source	
Primary RADIUS server	
IP address	<input type="text"/> Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.
Port	<input type="text"/> Leave this field blank to use the default port (1812).
Shared secret	<input type="text"/> Leave this field blank to not use a RADIUS shared secret (not recommended).

PFsense Captive portal 3

Radius Server部分

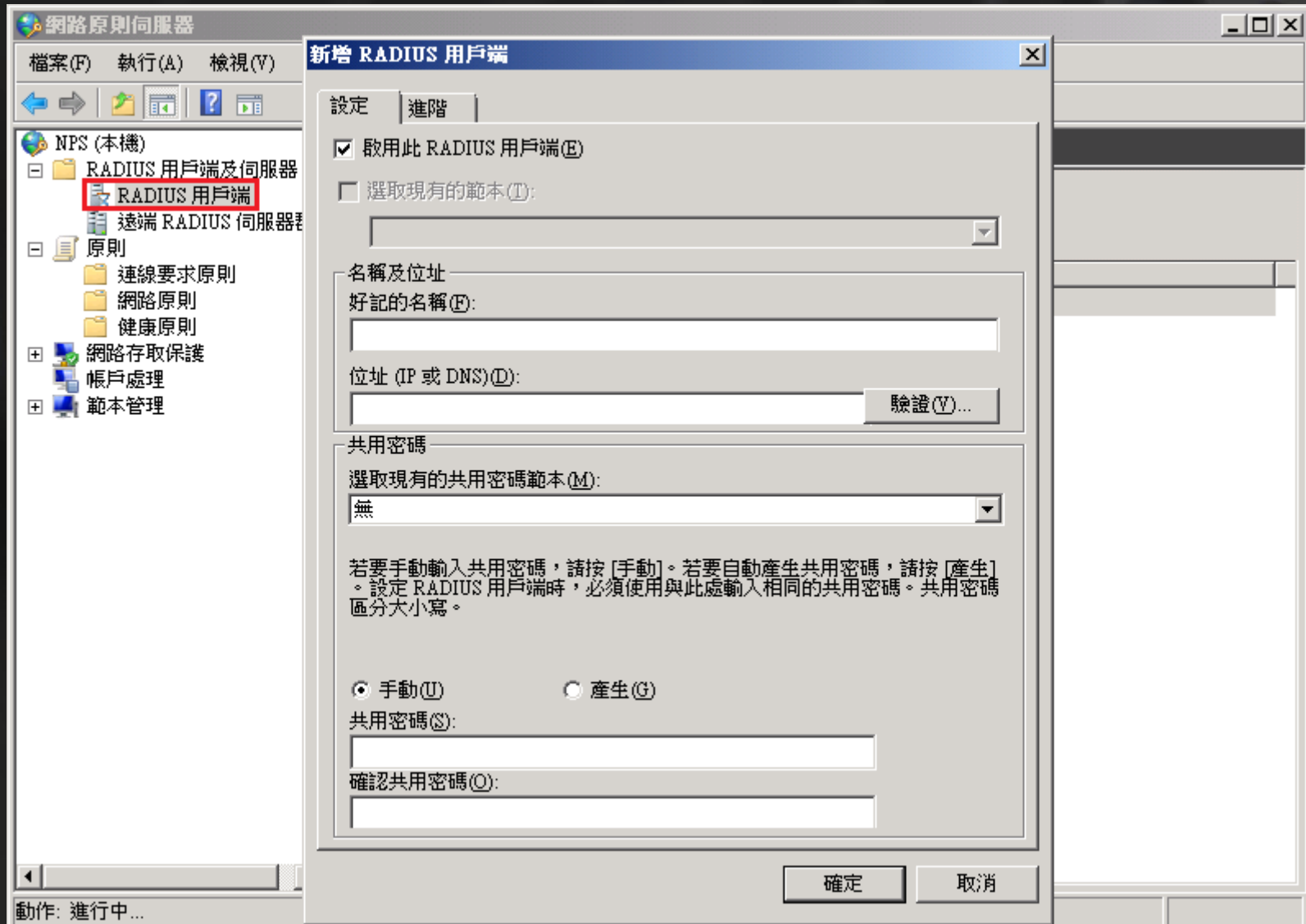
於MS Server2008或2012

新增角色

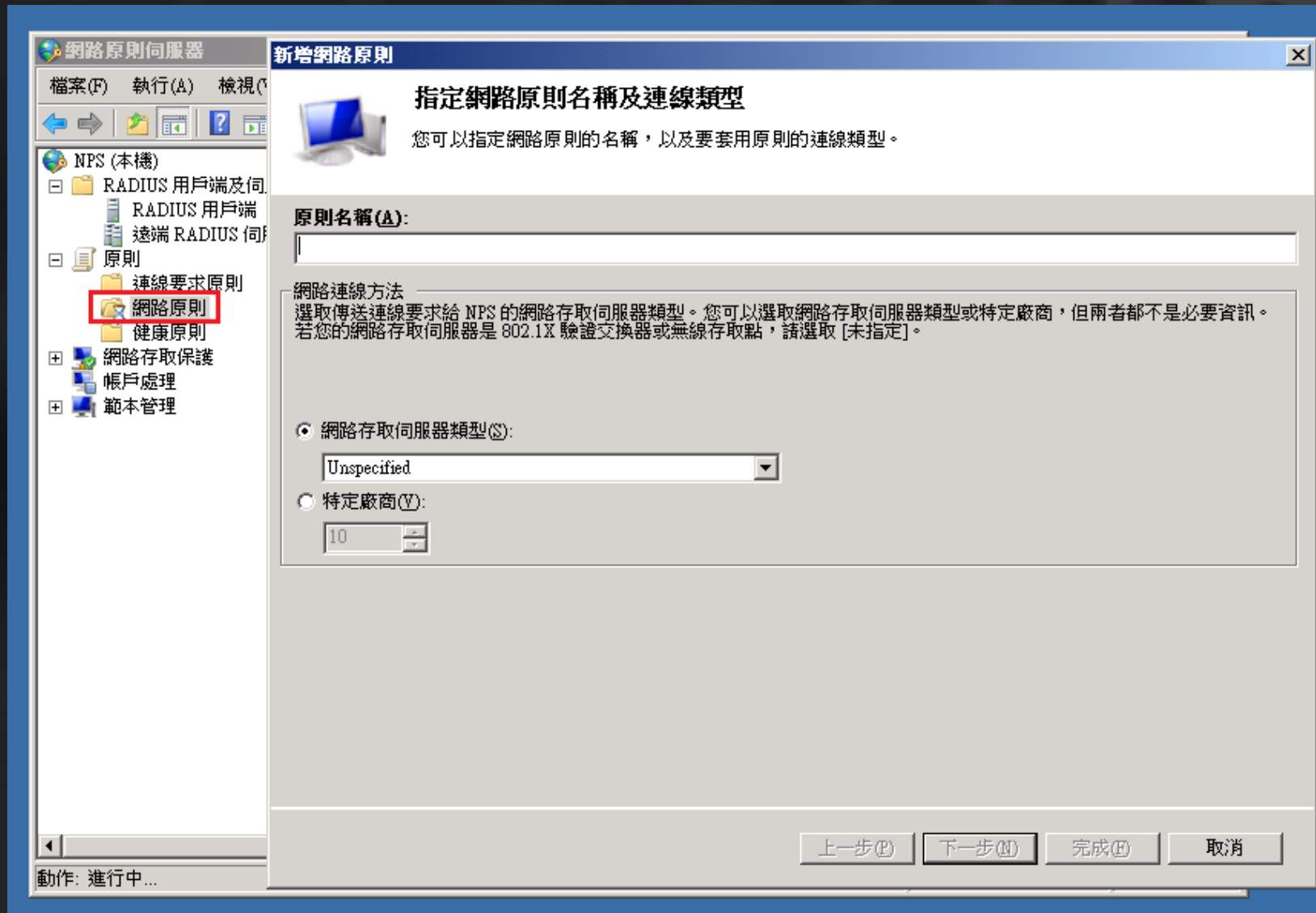
[網路原則與存取服務]中之

[網路原則伺服器]

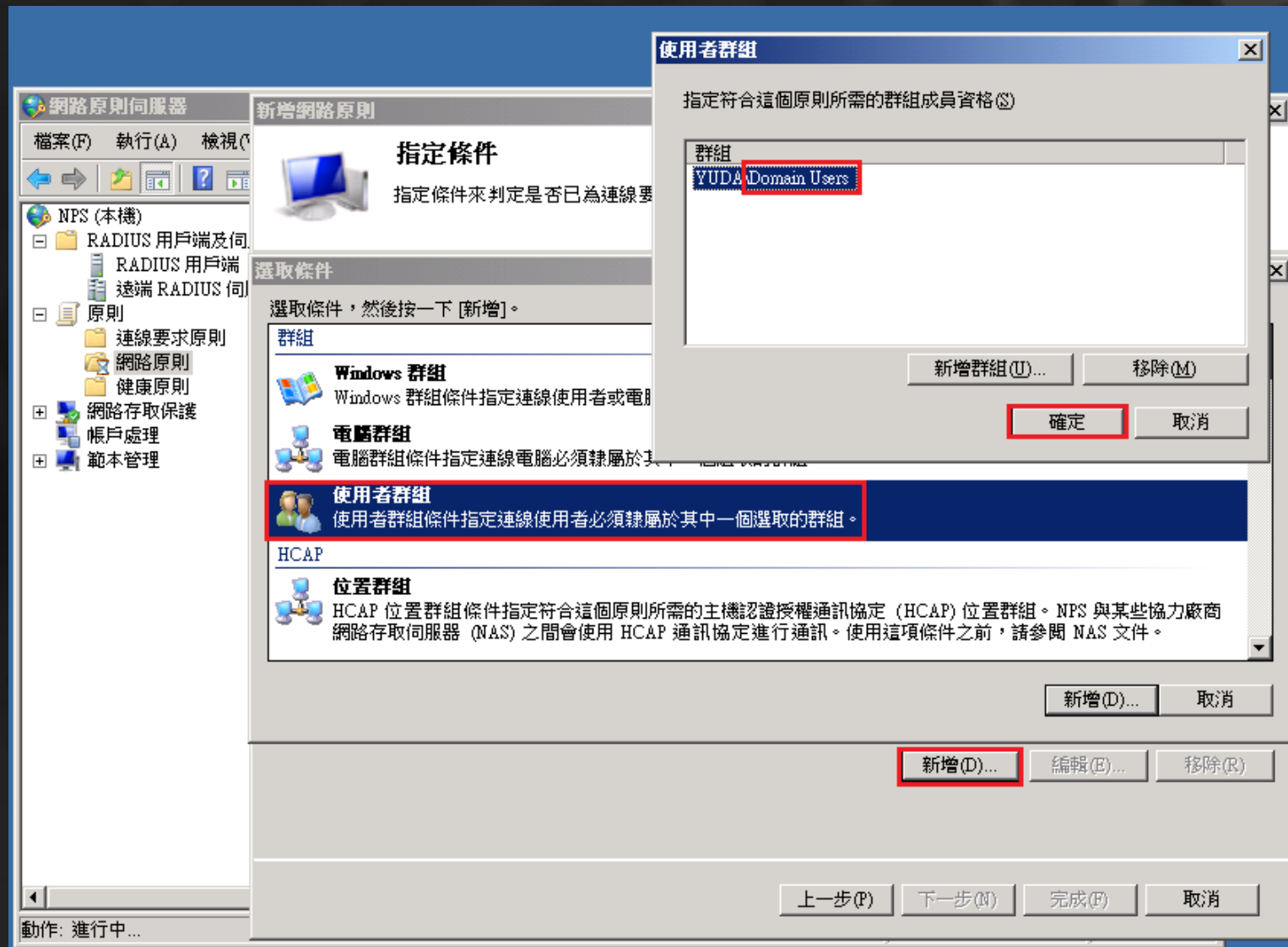
PFSense Captive portal 4



PFSense Captive portal 5




PFSense Captive portal 6



PFSense Captive portal 7

新增網路原則

 **指定存取權限**

設定連線要求符合這個原則時，應該授與或是拒絕網路存取。

☒ 授與存取權(A)
如果用戶端連線嘗試符合此原則的條件，便授與存取權。

☐ 拒絕存取(D)
如果用戶端連線嘗試符合此原則的條件，便拒絕存取。

☐ 存取權是由使用者撥入內容 (會覆寫 NPS 原則) 決定(S)
如果用戶端連線嘗試符合此原則的條件，便根據使用者撥入內容授與或拒絕存取。

上一步(B) 下一步(N) 完成(F) 取消

PFSense Captive portal 8

新增網路原則

設定驗證方法

設定所需的一或多種驗證方法，讓連線要求符合這個原則。對於 EAP 驗證，您必須設定 EAP 類型。如果部署 802.1X 或 VPN 的 NAP，您必須在連線要求原則中設定受保護的 EAP，該原則會覆寫網路原則驗證設定。

EAP 類型是以列出的順序，依序在 NPS 和用戶端之間交涉。

EAP 類型(T):

新增(D)...

編輯(E)...

移除(R)

較不安全的驗證方法:

- ☒ Microsoft 加密驗證版本 2 (MS-CHAP-v2)(V)
 - ☒ 使用者在密碼到期後可以變更密碼(H)
- ☒ Microsoft 加密驗證 (MS-CHAP)(Y)
 - ☒ 使用者在密碼到期後可以變更密碼(X)
- ☐ 加密驗證 (CHAP)(C)
- ☐ 未加密驗證 (PAP, SPAP)(S)
- ☐ 允許用戶端沒有交涉驗證方法仍然可以連線(L)
- ☐ 僅執行電腦健康情況檢查(M)

上移(U)

下移(W)

新增 EAP

驗證方法(A):

- Microsoft: 智慧卡或其他憑證
- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)**

確定

取消

上一步(B)

下一步(N)

完成(F)

取消

PFSense Captive portal 9






新增網路原則

設定限制

限制是比對連線要求所需的其他網路原則參數。如果連線要求和限制不相符，NPS 就會自動拒絕該要求。限制是選用項目，如果您不想要設定限制，請按 [下一步]。

設定這個網路原則的限制。
如果連線要求不符合所有限制，便會拒絕網路存取。

限制(S):

限制
 閒置逾時
 工作階段逾時
 被呼叫的工作站識別碼
 日期和時間限制
 NAS 連接埠類型

指定在中斷連線前可閒置伺服器的最長時間 (分鐘)


☐ 超過最長閒置時間後中斷連線(D)

1

上一步(B) **下一步(N)** 完成(F) 取消

PFSense Captive portal 10

新增網路原則



設定設定值

如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。

設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

RADIUS 屬性

- 標準
- 特定廠商

網路存取保護

- NAP 強制
- 擴充狀態

路由及遠端存取

- 多重連結與頻寬配置通訊協定 (BAP)
- IP 篩選器
- 加密**
- IP 設定

執行 Microsoft 路由及遠端存取服務的電腦支援加密設定。

如果您使用其他網路存取伺服器進行撥號或 VPN 連線，請確定您的伺服器支援所選取的加密設定。

如果只選取 [不加密] 選項，從存取用戶端前往網路存取伺服器的流量便不會受到加密保護。不建議使用這個設定。

☒ 基本加密 (MPPE 40 位元)(B)

☒ 增強式加密 (MPPE 56 位元)(I)

☒ 最強加密 (MPPE 128 位元)(G)

☐ 不加密(O)

上一步(B)


下一步(N)

完成(F)

取消

PFSense Captive portal 11

新增網路原則

 **正在完成新增網路原則**

您已成功建立下列網路原則:

TEST

原則條件:

條件	值
使用者群組	YUDA\Domain Users

原則設定:

條件	值
驗證方法	EAP 或 MS-CHAP v1 或 MS-CHAP v1 (使用者可在密碼到期後變更密碼) 或 MS-CHAP v2 ...
存取權限	授與存取權
更新不合格的用戶端	True
NAP 強制	允許完整的網路存取權
Framed-Protocol	PPP
Service-Type	Framed

要關閉這個精靈，請按一下 [完成]。

上一步(B) 下一步(N) **完成(F)** 取消

PFsense Captive portal 12



MAC : [來源端]免驗證 MAC Address

Allowed IP addresses : [目的端]免驗證IP

Allowed Hostnames : [目的端]免驗證Hostnames

Vouchers : 憑單系統

FileManager : 客製化檔案上傳

PFSense Captive portal 13

Services: Captive portal: Vouchers: YUDA Vouchers : 憑單系統

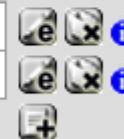


Captive portal(s) MAC Allowed IP addresses Allowed Hostnames Vouchers File Manager

☒ Enable Vouchers

Voucher Rolls

Roll #	Minutes/Ticket	# of Tickets	Comment
1	600	15	10HR
2	120	15	2hr



Create, generate and activate Rolls with Vouchers that allow access through the captive portal for the configured time. Once a voucher is activated, its clock is started and runs uninterrupted until it expires. During that time, the voucher can be re-used from the same or a different computer. If the voucher is used again from another computer, the previous session is stopped.

Voucher public key

```
-----BEGIN PUBLIC KEY-----  
  
-----END PUBLIC KEY-----
```

Paste an RSA public key (64 Bit or smaller) in PEM format here. This key is used to decrypt vouchers. [Generate new key.](#)

Voucher private key

```
-----BEGIN RSA PRIVATE KEY-----  
  
-----END RSA PRIVATE KEY-----
```

Paste an RSA private key (64 Bit or smaller) in PEM format here. This key is only used to generate encrypted vouchers and doesn't need to be available if the vouchers have been generated offline. [Generate new key.](#)

Character set

2345678abcdefghijklmnopqrstuvwxyz








Tickets are generated with the specified character set. It should contain printable characters (numbers, lower case and upper case letters) that are hard to confuse with others. Avoid e.g. 0/O and l/1.

PFSense Captive portal 14

	A	B	C	D	E
1	# Voucher Tickets 1..15 for Roll 1				
2	# Nr of Roll Bits	4			
3	# Nr of Ticket Bits	4			
4	# Nr of Checksum Bits	4			
5	# magic initializer	1 (19 Bits used)			
6	# Character Set used	2345678abcdefghijklmnopqrstuvwxyz			
7	#				
8	xvjxbt3				
9	wtct8r7				
10	xkswn24				
11	583vi7				
12	6psr7y				
13	5tzzvn7				
14	6h47vr7				
15	s7p2km8				
16	tnk7zu4				
17	hj4pns3				
18	kvach67				
19	de72r45				
20	e3xzdb7				
21	wk82ub7				
22	6mfcz83				

PFSense Captive portal 15

PFSense System Interfaces Firewall Services VPN Status **Diagnostics**

Status: Captive portal       

Active Users Active Vouchers Voucher Rolls Test Vouchers Expire Vouchers

Captive Portal Zone YUDA

Captive Portal status					
IP address		MAC address		Username	Session start
17	5.131	ac:	ab:de	/	05/05/2015 08:59:09
17	6.175	88	0:27:79	32183	05/05/2015 09:00:32
17	5.165	08	4:6d:c4	l285	05/05/2015 09:07:00
17	4.30	00	6:47:6f	:	05/05/2015 09:09:29
17	5.168	00	c:4c:ee	ng619	05/05/2015 09:20:27
17	5.170	c0:	1:e0:1d	la	05/05/2015 09:53:27
17	6.127	ac:	3:21:d1	iao	05/05/2015 09:55:36
17	5.235	3c:	9:75:ff	liachang	05/05/2015 10:07:32
17	5.146	44	3:3d:c2	420	05/05/2015 10:10:03
17	6.106	2c:	f:96:a6	8899	05/05/2015 10:16:54
17	6.113	78	7:94:b3	i	05/05/2015 10:35:37
17	4.124	00	6:1e:2f	446@yuda.tyc.edu.tw	05/05/2015 10:49:09
17	4.119	00	6:2c:f4	k	05/05/2015 10:50:07
17	4.34	00	6:25:71	y	05/05/2015 10:53:09
17	6.118	1c:	4:cc:1a	0505	05/05/2015 10:59:33
17	5.130	84	5:50:f6	alee	05/05/2015 11:05:22

PFSense Captive portal 16



▸ System ▸ Interfaces ▸ Firewall ▸ Services ▸ VPN ▸ Status ▸ Diagnostics

Status: RRD Graphs

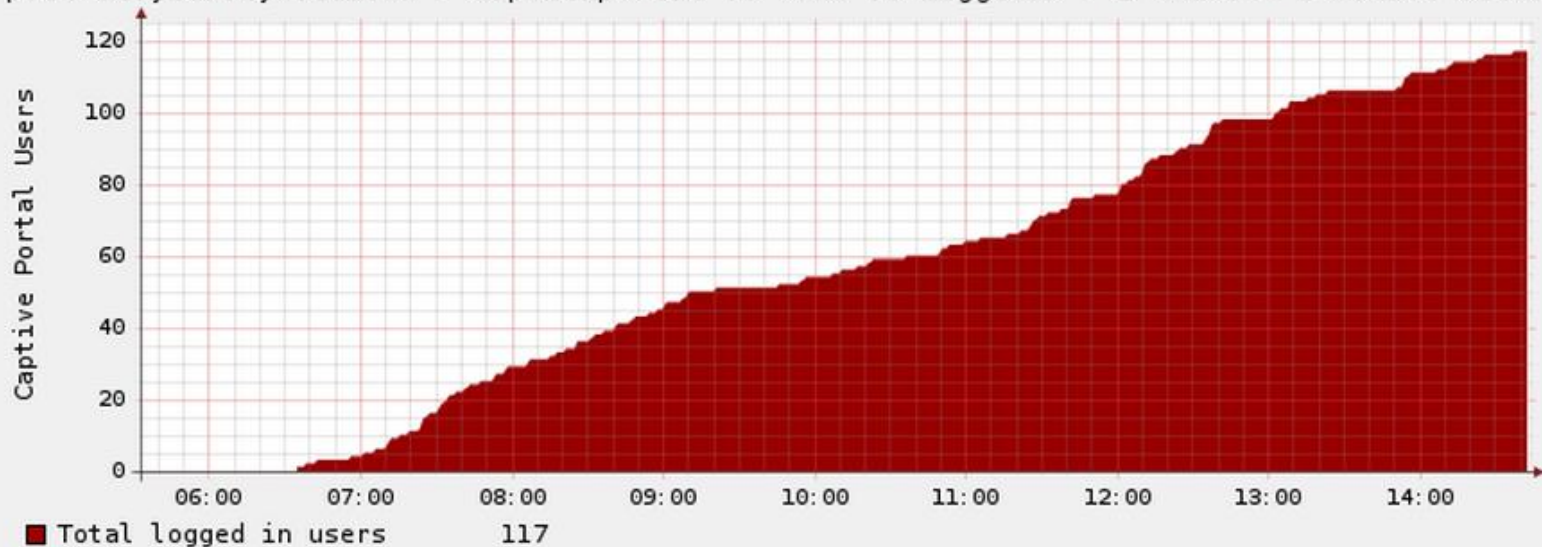
System Traffic Packets Quality Captive Portal Custom Settings

YUDA

Note: Change of color and/or style may not take effect until the next refresh

Graphs: Loggedin ▾ Style: Inverse ▾ Period: Absolute Timespans ▾

pfsense.yuda.tyc.edu.tw - Captiveportal :: Yuda :: Loggedin - 9 hours - 1 minute average



May 05 14:43:28 2015

備份 與 還原



System Interfaces Firewall Services VPN Status Diagnostics

Diagnostics: Backup/restore

Config History

Backup/Restore

Backup configuration

Click this button to download the system configuration in XML format.

Backup area: ALL

- ☐ Do not backup package information.
- ☐ Encrypt this configuration file.
- ☒ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Download configuration

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

Restore area: ALL

選擇檔案 未選擇任何檔案

- ☐ Configuration file is encrypted.

Restore configuration

Note:

The firewall will reboot after restoring the configuration.

ALL

Captive Portal
Captive Portal Vouchers
DNS Forwarder
DHCP Server
Firewall Rules
Interfaces
NAT
Package Manager
PPTP Server
RRD Data
Scheduled Tasks
Syslog
System
Static routes
System tunables
SNMP Server

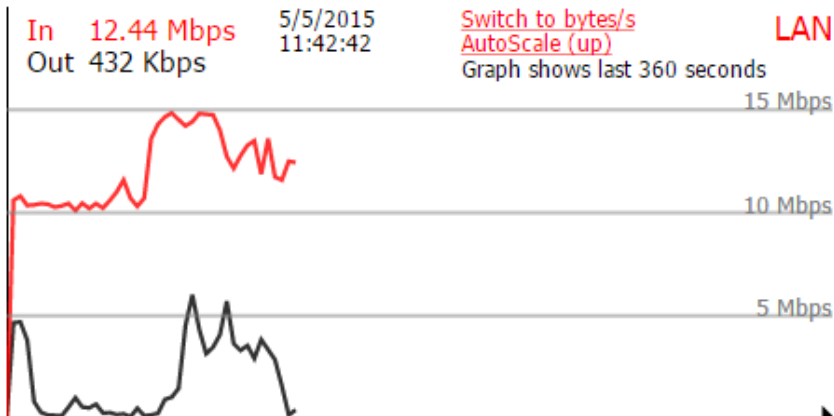
即時流量監控



System Interfaces Firewall Services VPN Status Diagnostics

Status: Traffic Graph

Interface: LAN , Sort by: Bw In , Filter: Local , Display: Host Name



Host Name or IP	Bandwidth In	Bandwidth Out
b_122	2.19M Bits/sec	43.83k Bits/sec
DARREN_NB	80.43k Bits/sec	719.02k Bits/sec
it21	48.75k Bits/sec	47.11k Bits/sec
STU00_PAD	28.59k Bits/sec	636.80k Bits/sec
C883	4.22k Bits/sec	18.28k Bits/sec
spring	0.00 Bits/sec	2.89k Bits/sec
C213	0.00 Bits/sec	2.58k Bits/sec

Note: the Adobe SVG Viewer, Firefox 1.5 or later or other browser supporting SVG is required to view the graph.

PFSense Packet



Programmed by David Hinkle, Commissioned by [DerbyTech](#) wireless networking.

- [Daily](#) -- [Weekly](#) -- [Monthly](#) -- [Yearly](#) -

Pick a Subnet:

- [Top20](#) -- [172.20.112.0](#) -

Top 20 IPs by Traffic - Daily

Ip and Name		Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total		5.9G	5.2G	703.8M	0	661.5M	201.2K	717.2M	5.2G	9.4M
172.20.112.251	.251	3.1G	3.1G	0	0	0	0	0	3.1G	0
172.20.112.251	.251	1.7G	1.7G	0	0	0	0	0	1.7G	0
172.20.112.130	.130	177.8M	3.9M	173.8M	0	177.7M	0	177.7M	58.2K	0
172.20.112.132	.132	166.2M	161.4M	4.9M	0	220.8K	0	226.4K	166.0M	0
172.20.112.241	.241	153.5M	153.5M	0	0	0	0	0	153.5M	0
172.20.112.3	.3	115.4M	7.0M	108.3M	0	36.0M	0	37.6M	77.7M	1.6K
172.20.112.137	.137	54.4M	1.2M	53.1M	0	54.1M	0	54.4M	11.1K	0
172.20.112.114	.114	53.6M	2.5M	51.1M	0	53.5M	0	53.6M	68.6K	0
172.20.112.254	.254	40.0M	34.1M	5.9M	0	15.4M	27.0K	39.7M	355.6K	17.3K
172.20.112.20	.20	34.9M	5.6M	29.2M	0	34.0M	73.2K	34.4M	498.2K	336
172.20.112.162	.162	33.5M	1.9M	31.6M	0	33.2M	0	33.4M	78.4K	0
172.20.112.157	.157	28.8M	2.4M	26.4M	0	28.6M	0	28.7M	61.8K	1.6K
172.20.112.70	.70	28.3M	8.1M	20.3M	0	12.0M	30.3K	26.0M	2.4M	1.1K
172.20.112.1	.1	27.3M	800.2K	26.5M	0	27.3M	0	27.3M	12.5K	0
172.20.112.215	.215	22.4M	8.7M	13.7M	0	22.3M	0	22.3M	107.6K	56

THE END

如對本次分享有任何相關疑問歡迎來信討論

張以勤

yaichin@yuda.tyc.edu.tw

