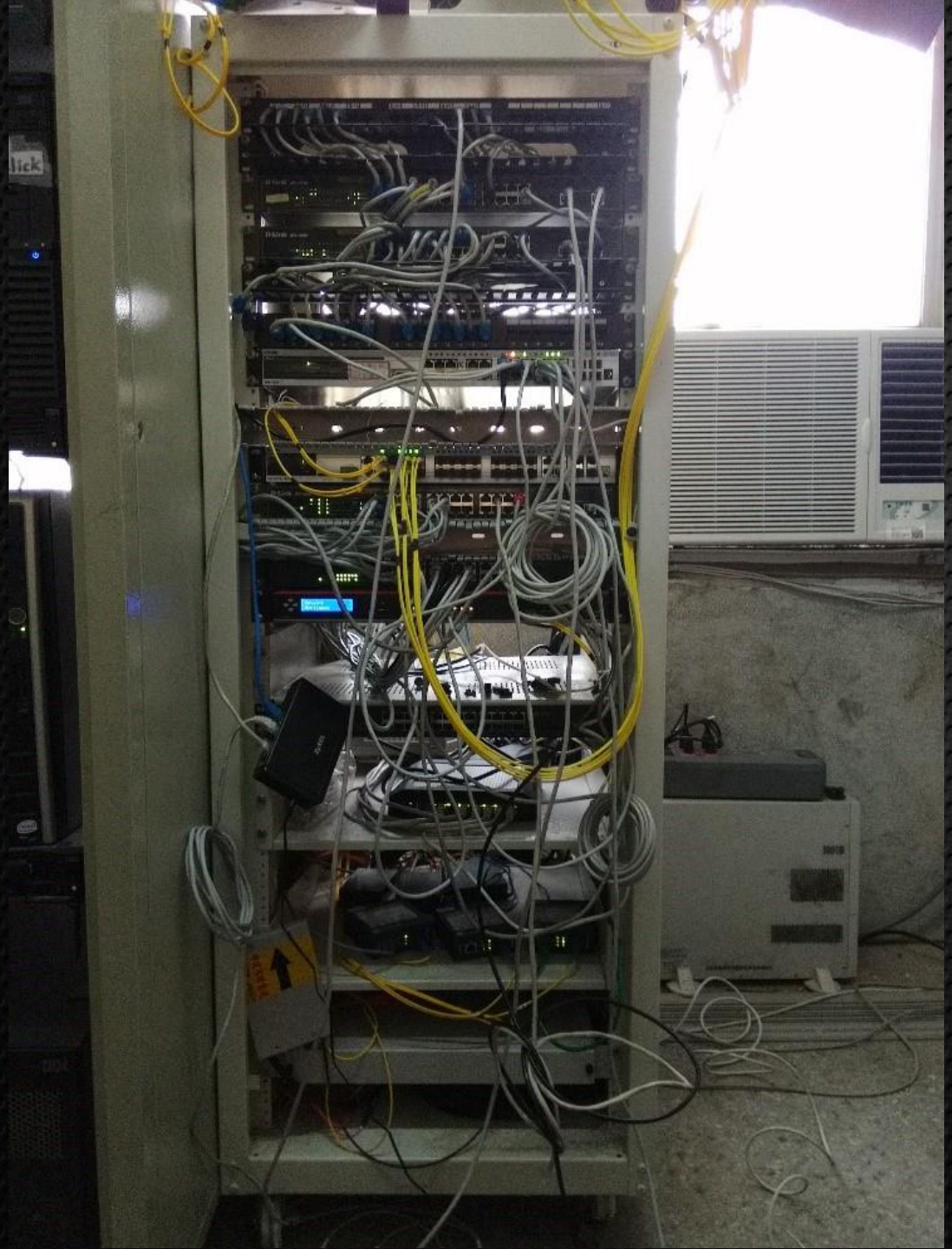
用pfSense翻轉校園資訊科技應用環境

2015/5/6

南投教網 / Ming-Chang Cheng
everfree@ntct.edu.tw

故事的起源是這樣的



愛恨交織

藕斷絲連....

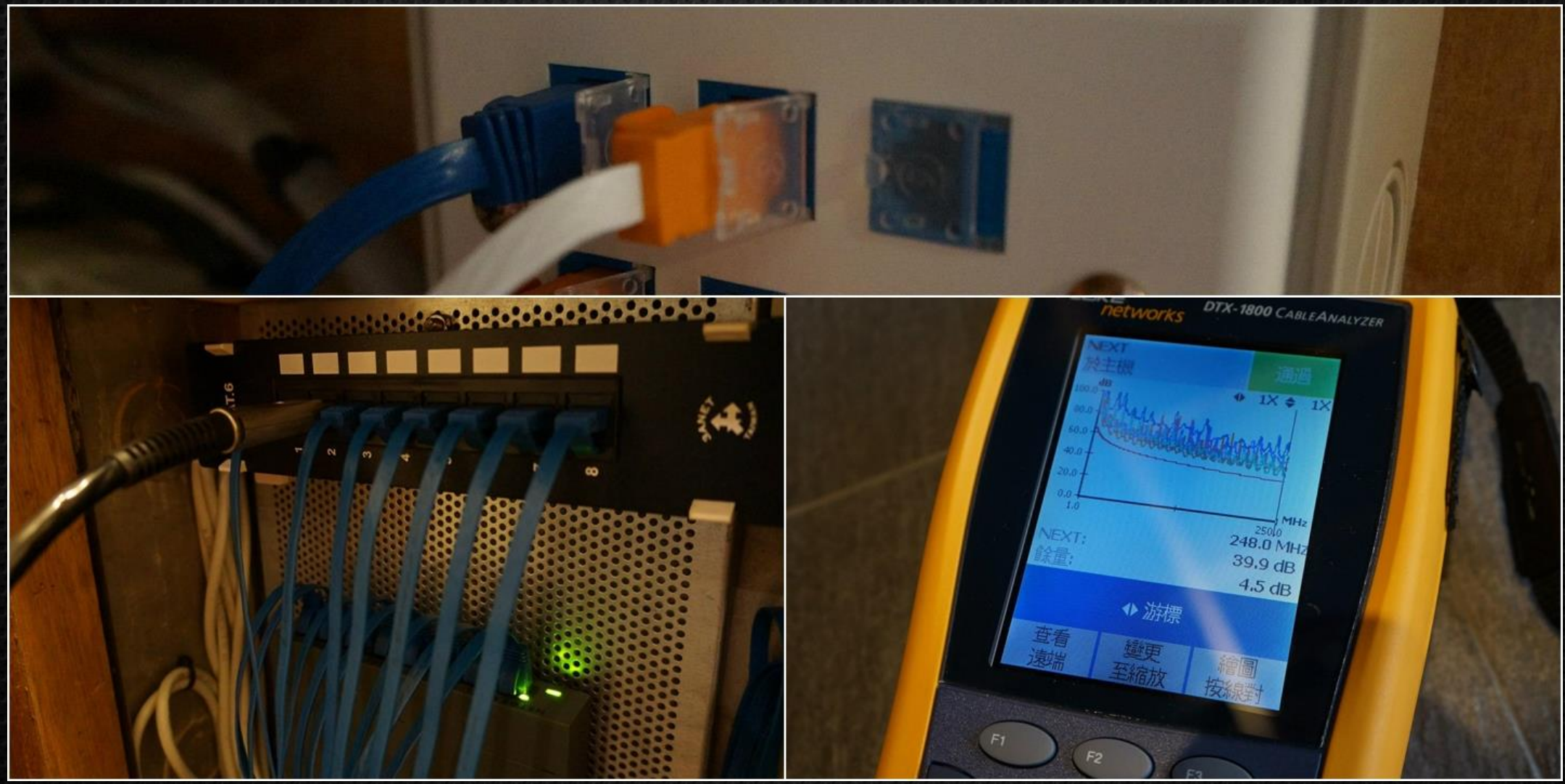
好的架構上天堂

差的架構還有套房嗎？

老師又來啦！！！

- 交換器與網路線
- 資訊座與跳線面板
- 防火牆與網段規劃

很多網路的問題來自於「架構」

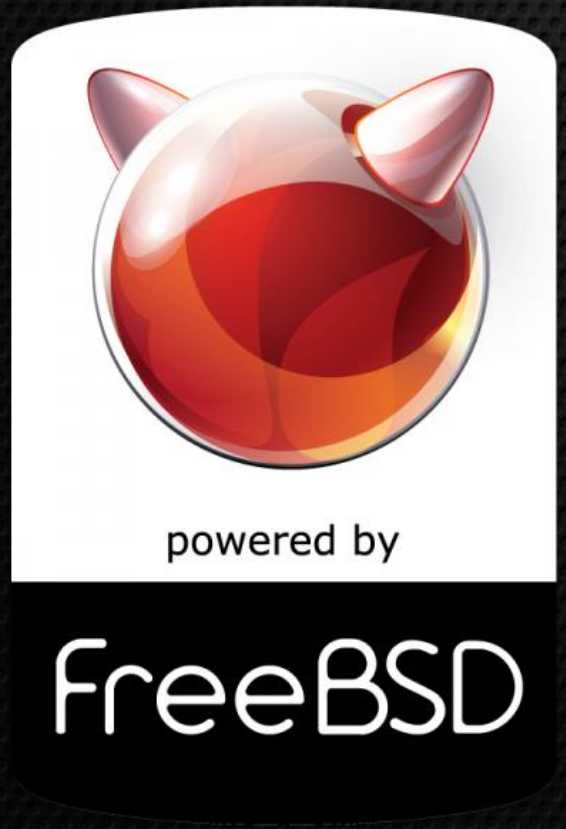

networks
DTX-1800 CableAnalyzer
NEXT
通過
1X
1X
MHz
NEXT:
248.0 MHz
餘量:
39.9 dB
4.5 dB
游標
查看
遠端
變更
至縮放
繪圖
按線對
F1
F2

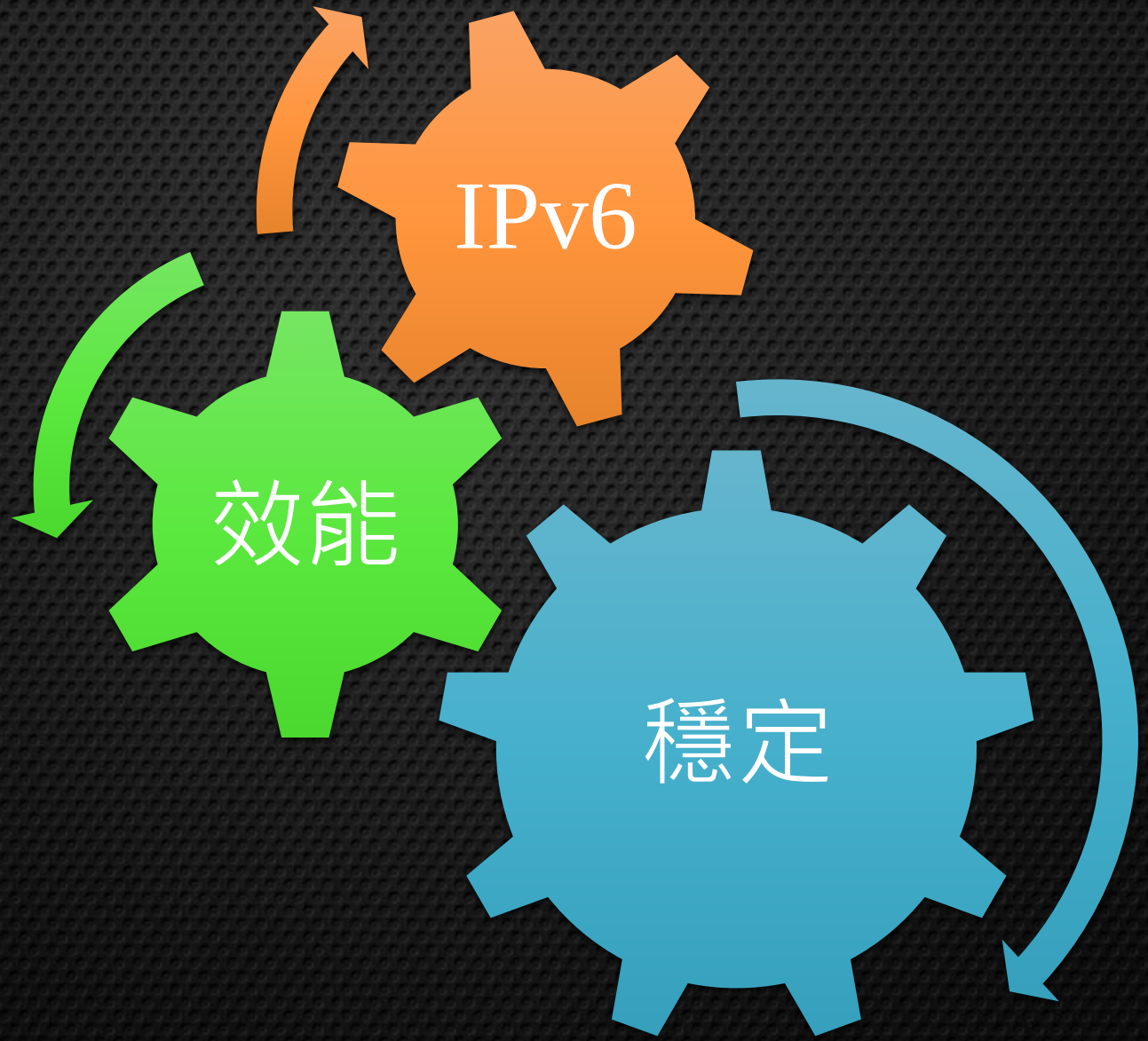
龜毛的代價

高速公路蓋好了，接下來呢？

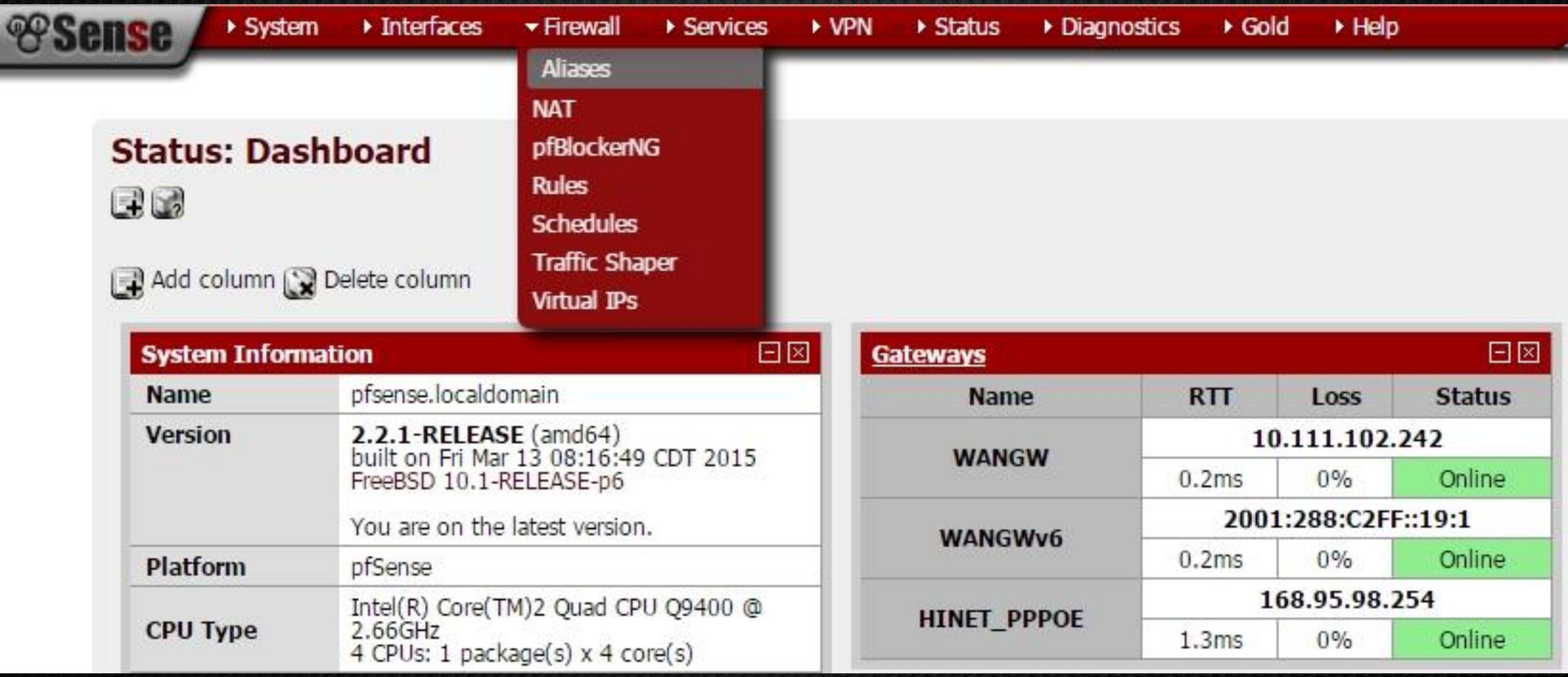
去吧 pfSense 就决定是你啦！

十年磨一劍

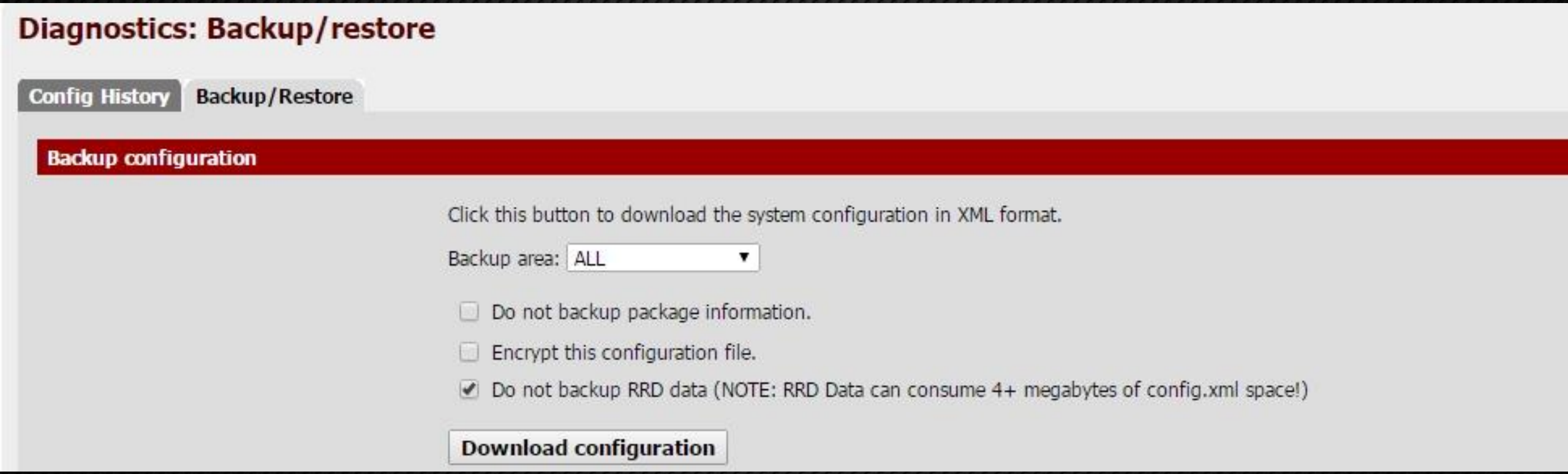




南投縣pfSense導入流程

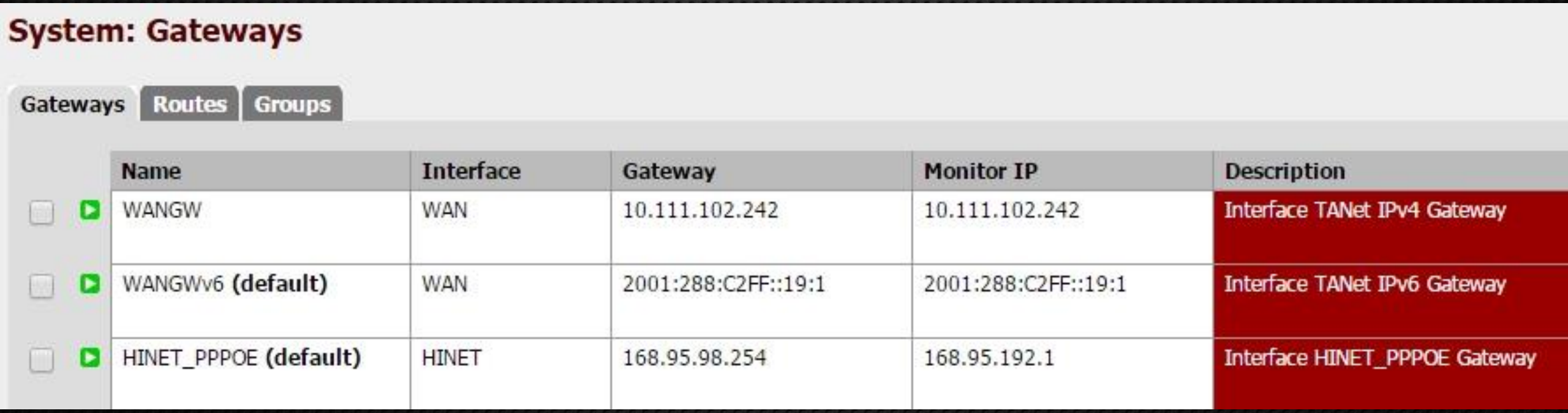

pfSense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Aliases
NAT
pfBlockerNG
Rules
Schedules
Traffic Shaper
Virtual IPs
Status: Dashboard
Add column
Delete column
System Information
Name
pfsense.localdomain
Version
2.2.1-RELEASE (amd64)
built on Fri Mar 13 08:16:49 CDT 2015
FreeBSD 10.1-RELEASE-p6
You are on the latest version.
Platform
pfSense
CPU Type
Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz
4 CPUs: 1 package(s) x 4 core(s)
Gateways
Name
RTT
Loss
Status
WANGW
10.111.102.242
0.2ms
0%
Online
WANGWv6
2001:288:C2FF::19:1
0.2ms
0%
Online
HINET_PPPOE
168.95.98.254
1.3ms
0%
Online

Web GUI管理介面



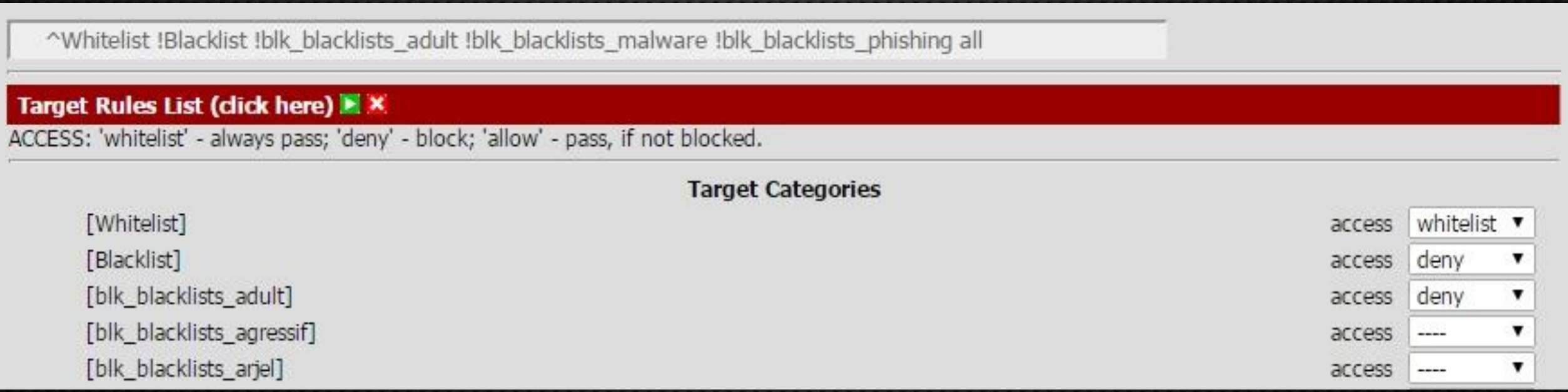
XML格式備份與還原，提供「南投版各校設定檔」

學校可快速導入



搭配內建別名來判斷，使用Multi-WAN分流

Squid 快取伺服器，節省頻寬降低負載


^Whitelist !Blacklist !blk_blacklists_adult !blk_blacklists_malware !blk_blacklists_phishing all
Target Rules List (click here)
ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.
Target Categories
[Whitelist] access whitelist
[Blacklist] access deny
[blk_blacklists_adult] access deny
[blk_blacklists_agressif] access ----
[blk_blacklists_arjel] access ----

URL黑名單過濾機制

搭配 unbound DNS，開啟Google安全搜尋

自動產生安裝程式

client-to-site, site-to-site

Deny - Last 50 Alert Entries. Firewall Rule changes can unsync these Alerts.

Date	IF	Rule	Proto	Source	Destination	CC	List
Apr 13 15:02:46	SERVER	pfB_EmergingThreats (118)	TCP-S	163.22.61.140:53898	146.3.99.136:3389	LU	Shadowserver 146.3.0.0/16
Apr 13 15:02:45	SERVER	pfB_EmergingThreats (118)	TCP-S	163.22.61.140:53894	101.253.0.147:3389	CN	Shadowserver 101.252.0.0/15
Apr 13 15:02:43	SERVER	pfB_EmergingThreats (118)	TCP-S	163.22.61.140:53898	146.3.99.136:3389	LU	Shadowserver 146.3.0.0/16
Apr 13 15:02:42	SERVER	pfB_EmergingThreats (118)	TCP-S	163.22.61.140:53894	101.253.0.147:3389	CN	Shadowserver 101.252.0.0/15
Apr 13 15:02:11	SERVER	pfB_EmergingThreats (118)	TCP-S	163.22.61.140:53698	119.232.165.208:3389	CN	Shadowserver 119.232.0.0/16

IP黑名單與預警機制，十萬筆資料每天更新

http://www.abuse.ch
http://rules.emergingthreats.net

Active Flows

10 ▾ Applications ▾

Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes
Info	HTTP	TCP	192.168.7.154:52572	img7.8comic.com :80	3 min, 11 sec	Server	1.43 Mbit ↑	7.05 MB
Info	SSL_No_Cert	TCP	2001:288:c219:0:f8e5... :50165	2404:6800:4008:3::e :443	59 sec	Server	0 bps –	5.22 MB
Info	SSDP	UDP	192.168.0.70:1900	239.255.255.250:1900	7 h, 31 min, 58 sec	Client	0 bps –	4.6 MB
Info	SSDP	UDP	192.168.0.74:1900	239.255.255.250:1900	1 h, 37 min, 37 sec	Client	0 bps ↓	3.88 MB
Info	ICMPV6	IPv6-ICMP	fe80::260:e0ff:fe5e:...	ff02::1	2 days, 9 h, 15 min, 10 sec	Client	0 bps –	3.06 MB
Info	HTTP	TCP	192.168.0.70:51996	ib.adnxs.com :80	53 min, 33 sec	Client Server	0 bps –	2.34 MB

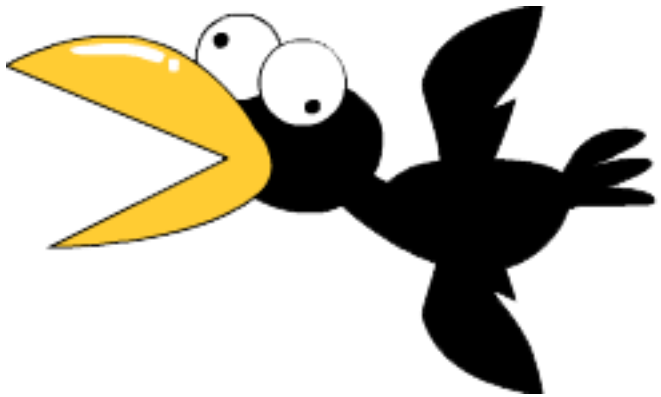
詳細流量監控，便於找出問題

RRD Graphs
Log
Command

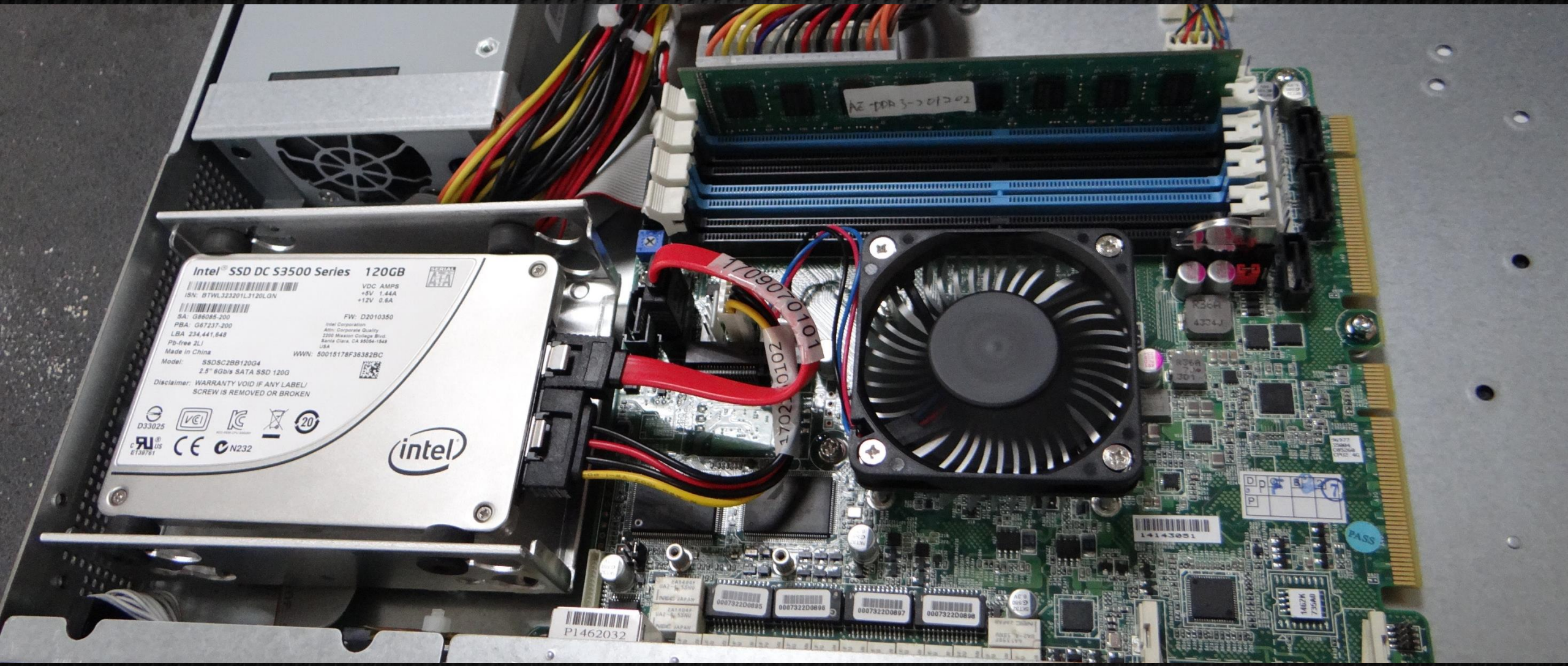
透過Gmail每日寄送報表

And more

那硬體呢？



……



2015最佳選擇，SoC架構工業級主機

中大型學校

- C2558、C2758
- 2.40 GHz
- 四核、八核

800Mbps+

小型學校

- C2358
- 1.70 GHz
- 雙核

500Mbps+


處理器
硬碟
晶片組
記憶體
網路卡

擴充介面的選擇，連10G都有.....

中文語系

第七層限制

臭蟲

帳號授權機制

「教學文件」

「維護人員」

沒缺點豈非太完美

每個環節

都可能影響...

進入「無線」的航道之前

請先把「有線」搞定

Questions?