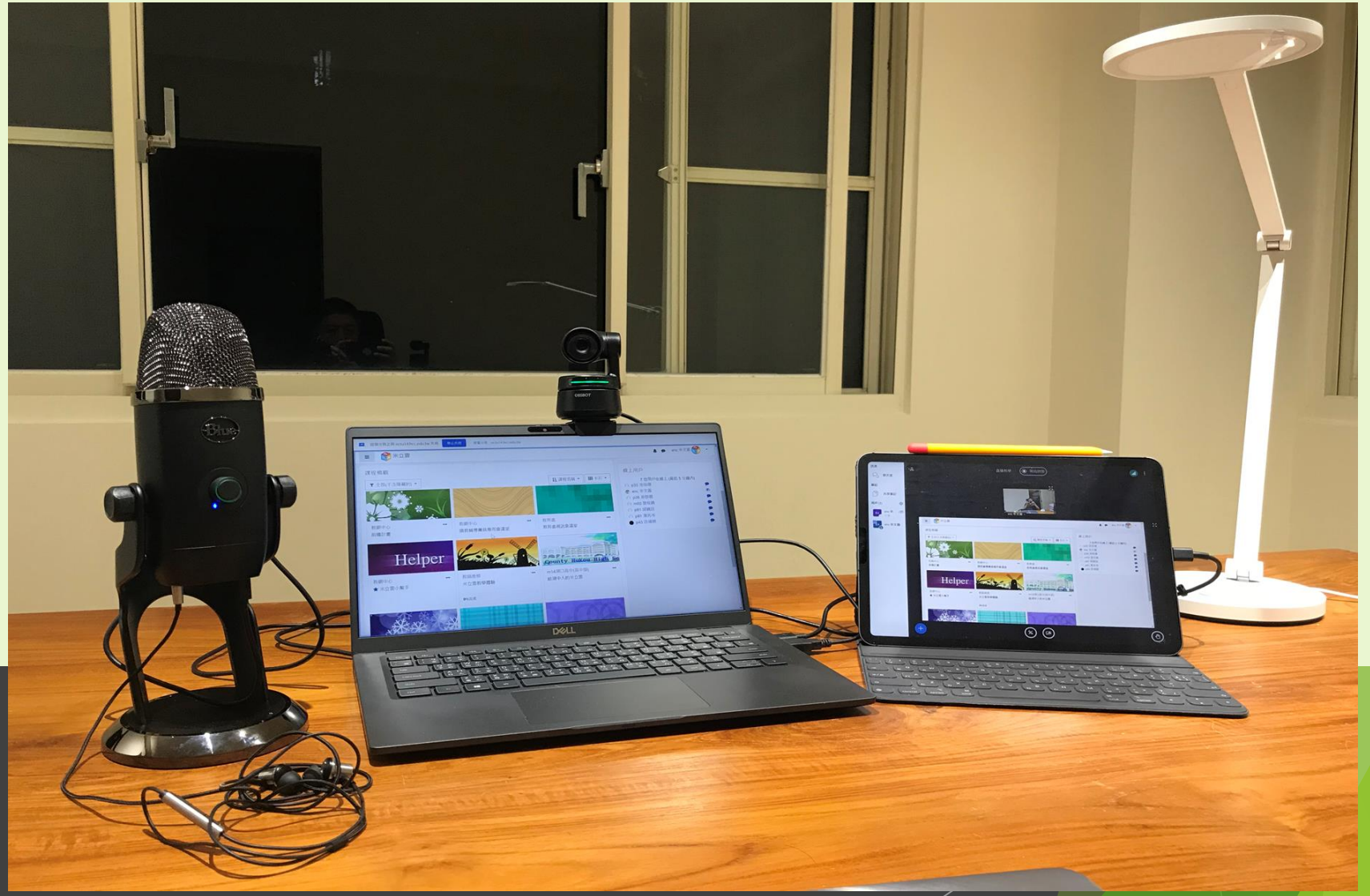
Windows 及 Linux 主機架設安全防護

辛文義 Eric Hsin @2021
eric.hsin@gmail.com

歡迎
Start



1


您想如何加入音訊？
麥克風
僅聆聽

2

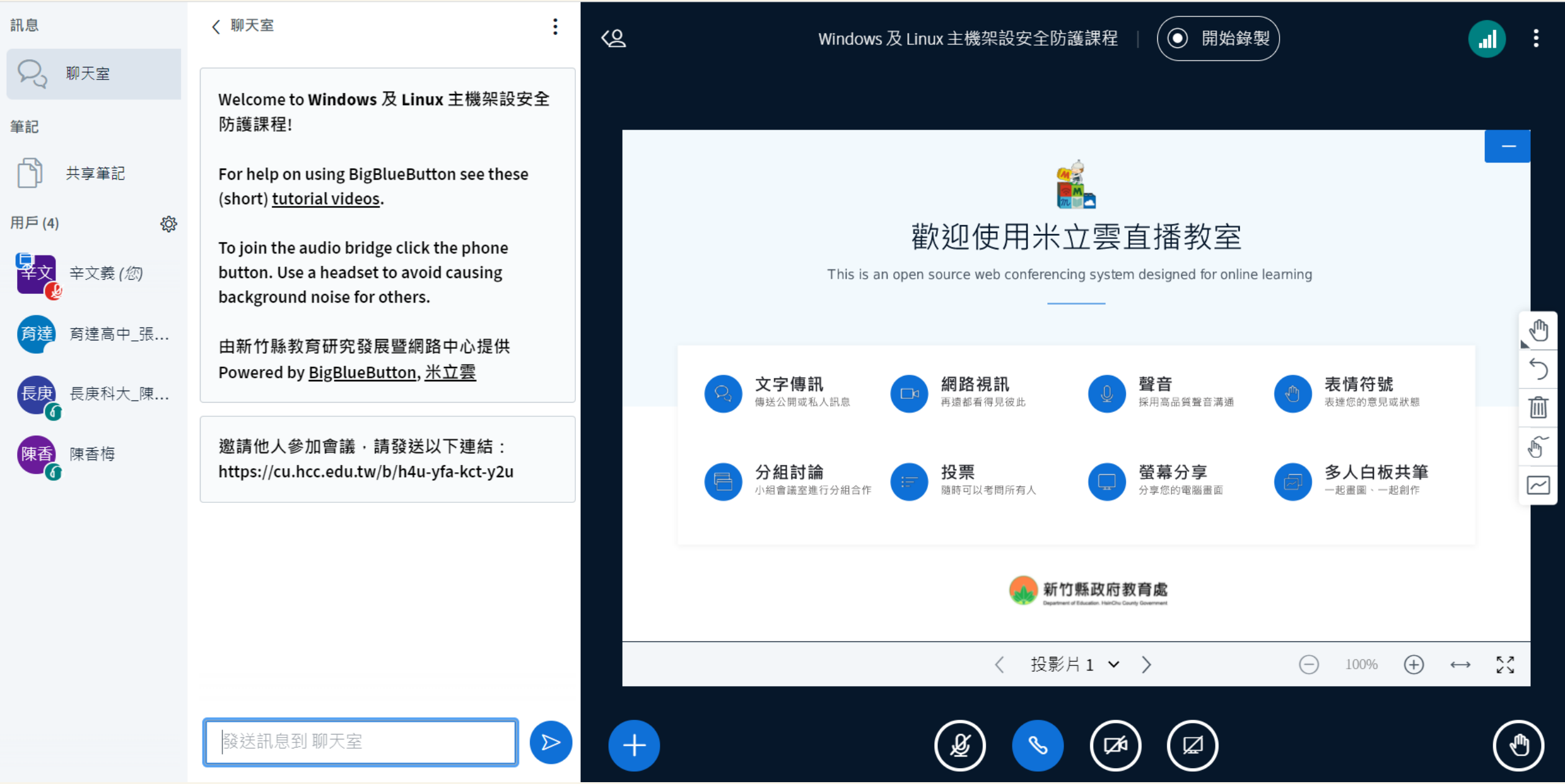

這是私人的回音測試，說幾句話。您能聽到聲音嗎？
是
否

4


字傳訊
網路視訊
再遠都看得見彼此
聲音
採用高品質聲音溝通
表情符號
表達您的意見或狀態
分組討論
小組會議室進行分組合作
投票
隨時可以考問所有人
螢幕分享
分享您的電腦畫面
多人白板共筆
一起畫圖、一起創作
新竹縣政府教育處
投影片 1
100%
取消靜音

3


變更您的聲音設定
請注意，瀏覽器彈出對話框，您必需允許分享您的麥克風。
麥克風來源
預設 - 麥克風 (Yeti X) (046d:0aaf)
揚聲器來源
預設 - 喇叭 (Realtek(R) Audio)
Test your speaker volume
播放聲音
返回
重試


訊息
聊天室
筆記
共享筆記
用戶 (4)
辛文義 (您)
育達高中_張...
長庚科大_陳...
陳香梅
聊天室
Welcome to Windows 及 Linux 主機架設安全防護課程!
For help on using BigBlueButton see these (short) tutorial videos.
To join the audio bridge click the phone button. Use a headset to avoid causing background noise for others.
由新竹縣教育研究發展暨網路中心提供
Powered by BigBlueButton, 米立雲
邀請他人參加會議，請發送以下連結：
https://cu.hcc.edu.tw/b/h4u-yfa-kct-y2u
發送訊息到 聊天室
Windows 及 Linux 主機架設安全防護課程
開始錄製
歡迎使用米立雲直播教室
This is an open source web conferencing system designed for online learning
文字傳訊
傳送公開或私人訊息
網路視訊
再遠都看得見彼此
聲音
採用高品質聲音溝通
表情符號
表達您的意見或狀態
分組討論
小組會議室進行分組合作
投票
隨時可以考問所有人
螢幕分享
分享您的電腦畫面
多人白板共筆
一起畫圖、一起創作
新竹縣政府教育處
投影片 1
100%

辛文義 Eric Hsin eric.hsin@gmail.com

1. 是一位中學老師並以教育為終身志業，兼任網路管理與資安防護工作資歷超過20年。
2. 現於新竹縣教育研究發展暨網路中心擔任資訊教育專任輔導員兼任網路管理組組長、中學資訊教師。在社會服務志業中，曾膺任軟體自由協會常務理監事、多所大專院校及醫院數位教學平台導入的協助與諮詢、多個自由軟體專案開發與推廣志工。
3. 交大電資學院工學碩士/淡大資訊40學分班/師大物理系理學士
4. 擁有CSA的CCSK/VMware的VCP/MikroTik的MTCRE和MTCTCE證照

自我介紹
Profile

本課程將介紹校園常用的作業系統Windows及Linux在主機架設安全防護應該注意的地方，內容包含作業系統基本安全設定、網路基本安全防護、虛擬化環境應用，以及導入開放的資安解決方案。分享講師多年工作經驗，希望與您一起檢驗資安攻防的脈絡，累積能力建立穩固安全的堡壘。

摘要
Abstract

1. Windows Security基礎
2. Linux Security基礎
3. 網路通訊的安全
4. 防火牆知多少(Microsoft Defender /Linux iptables/Mikrotik Firewall)
5. 積極防護的解決方案(虛擬IP與NAT活用/VPN建置與應用)
6. 積極備援的解決方案(虛擬化應用Proxmox)

大綱
Outline

Windows Security基礎

statcounter
GlobalStats

Press Releases FAQ About Feedback

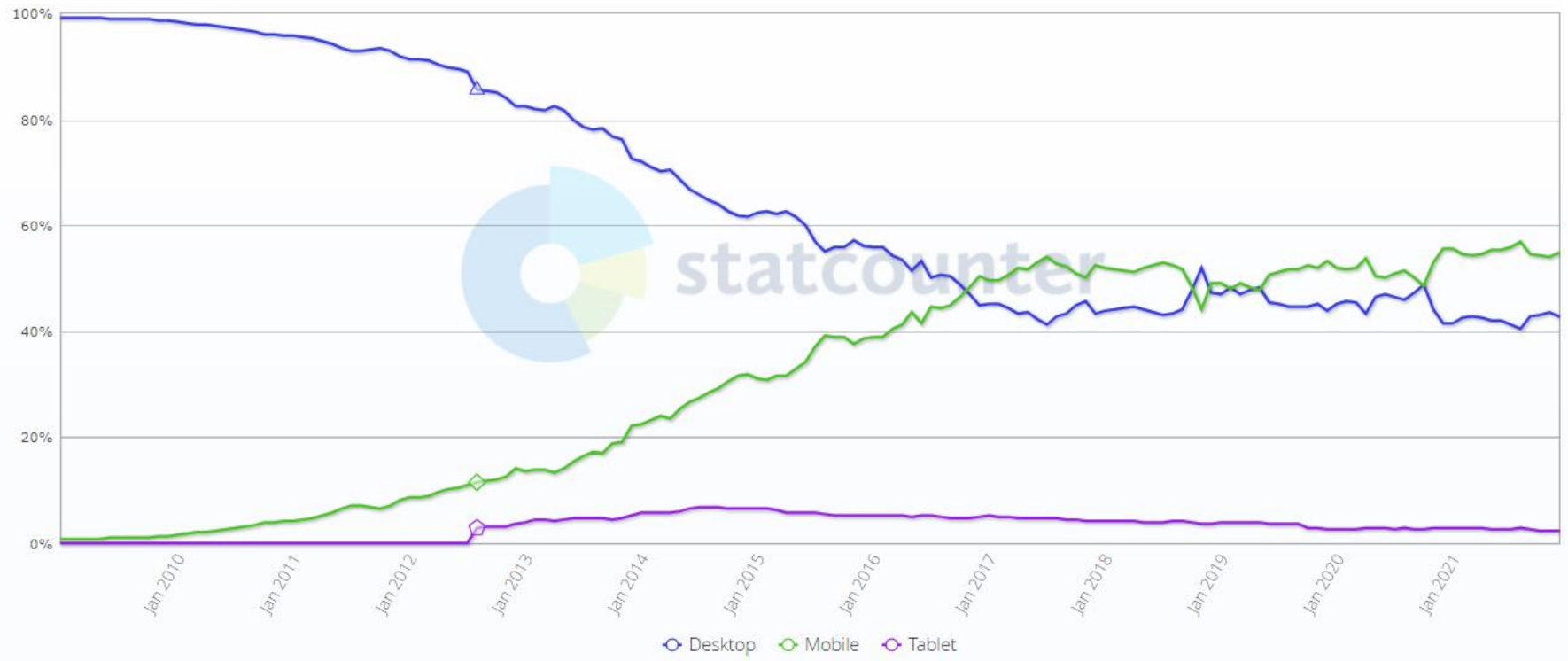
Mobile	Desktop	Tablet
53.98%	43.55%	2.48%

Desktop vs Mobile vs Tablet Market Share Worldwide - November 2021

Desktop vs Mobile vs Tablet Market Share Worldwide

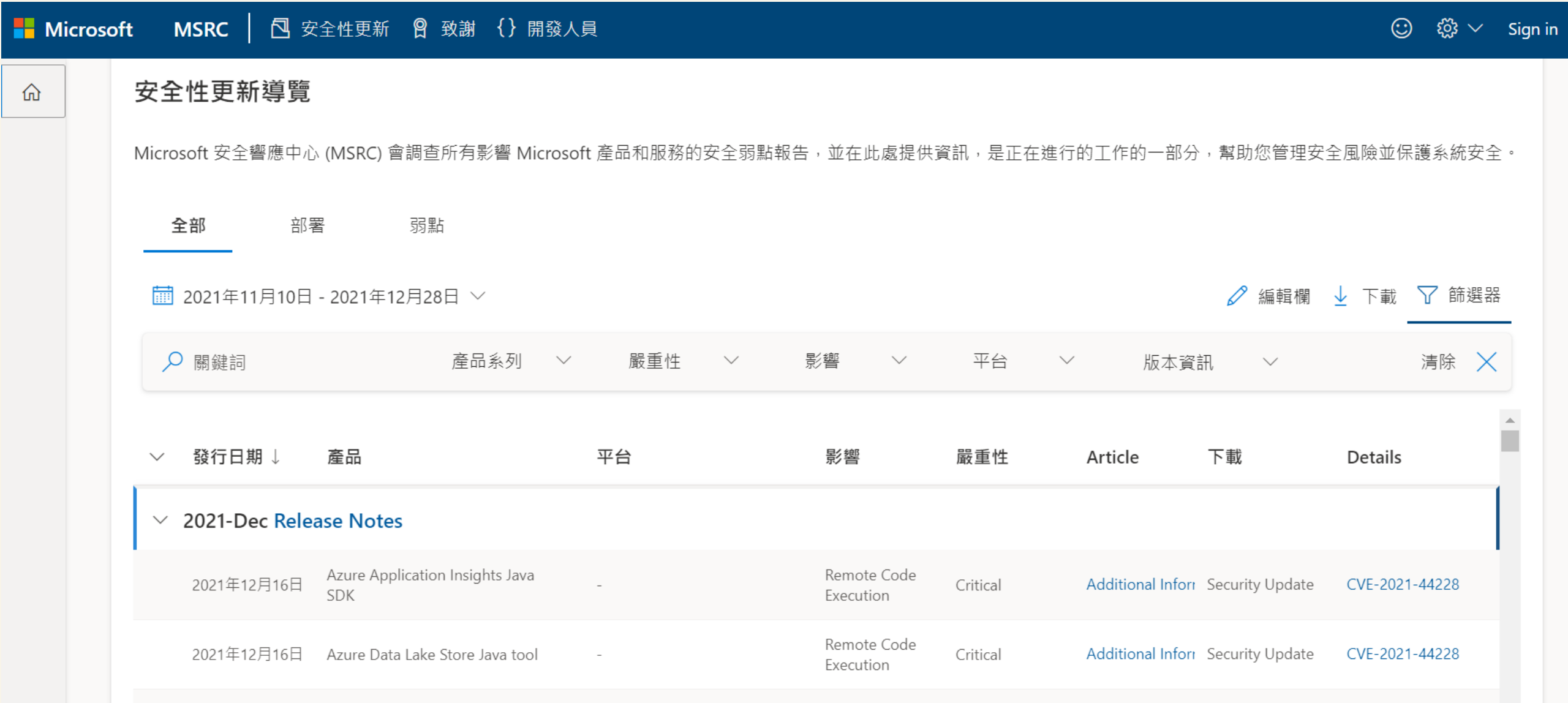
Jan 2009 - Dec 2021

Edit Chart Data



微軟安全性更新導覽

https://msrc.microsoft.com/update-guide/



https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Windows

Search Results

There are **9534** CVE Records that match your search.

Name	Description
CVE-2021-45459	lib/cmd.js in the node-windows package before 1.0.0-beta.6 for Node.js allows command injection via the PID parameter.
CVE-2021-45100	The ksmbd server through 3.4.2, as used in the Linux kernel through 5.15.8, sometimes communicates in cleartext even though encryption has been enabled. This occurs because it sets the SMB2_GLOBAL_CAP_ENCRYPTION flag when using the SMB 3.1.1 protocol, which is a violation of the SMB protocol specification. When Windows 10 detects this protocol violation, it disables encryption.
CVE-2021-44554	Thinfinity VirtualUI before 3.0 allows a malicious actor to enumerate users registered in the OS (Windows) through the /changePassword URI. By accessing the vector, an attacker can determine if a username exists thanks to the message returned; it can be presented in different languages according to the configuration of VirtualUI. Common users are administrator, admin, guest and krgtbt.
CVE-2021-44548	An Improper Input Validation vulnerability in DataImportHandler of Apache Solr allows an attacker to provide a Windows UNC path resulting in an SMB network call being made from the Solr host to another host on the network. If the attacker has wider access to the network, this may lead to SMB attacks, which may result in: * The exfiltration of sensitive data such as OS user hashes (NTLM/LM hashes), * In case of misconfigured systems, SMB Relay Attacks which can lead to user impersonation on SMB Shares or, in a worse-case scenario, Remote Code Execution This issue affects all Apache Solr versions prior to 8.11.1. This issue only affects Windows.
CVE-2021-44230	PortSwigger Burp Suite Enterprise Edition before 2021.11 on Windows has weak file permissions for the embedded H2 database, which might lead to privilege escalation. This issue can be exploited by an adversary who has already compromised a valid Windows account on the server via separate means. In this scenario, the compromised account may have inherited read access to sensitive configuration, database, and log files.
CVE-2021-44203	Stored cross-site scripting (XSS) was possible in protection plan details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035
CVE-2021-44202	Stored cross-site scripting (XSS) was possible in activity details. The following products are affected: Acronis Cyber Protect 15 (Windows, Linux) before build 28035

Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): Windows
- Search Type: Search All
- CPE Name Search: false

There are **9,970** matching records.
Displaying matches **1** through **20**.

1 2 3 4 5 6 7 8 9 10 > >>

Vuln ID	Summary	CVSS Severity
CVE-2021-3622	A flaw was found in the hivex library. This flaw allows an attacker to input a specially crafted Windows Registry (hive) file, which would cause hivex to recursively call the _get_children() function, leading to a stack overflow. The highest threat from this vulnerability is to system availability. **Published:** 十二月 23, 2021; 4:15:08 下午 -0500	*V3.x:*(not available) *V2.0:*(not available)

OWASP Top 10:2021

首頁

注意事項

OWASP 2021 介紹

如何正確使用 OWASP Top 10 為標準

如何使用 OWASP Top 10 啟動 AppSec

OWASP 相關

Top 10:2021 名單

A01 權限控制失效

A02 加密機制失效

A03 注入式攻擊

A04 不安全設計

A05 安全設定缺陷

A06 危險或過舊的元件

A07 認證及驗證機制失效

A08 軟體及資料完整性失效

A09 資安記錄及監控失效

A10 伺服端請求偽造

下一步

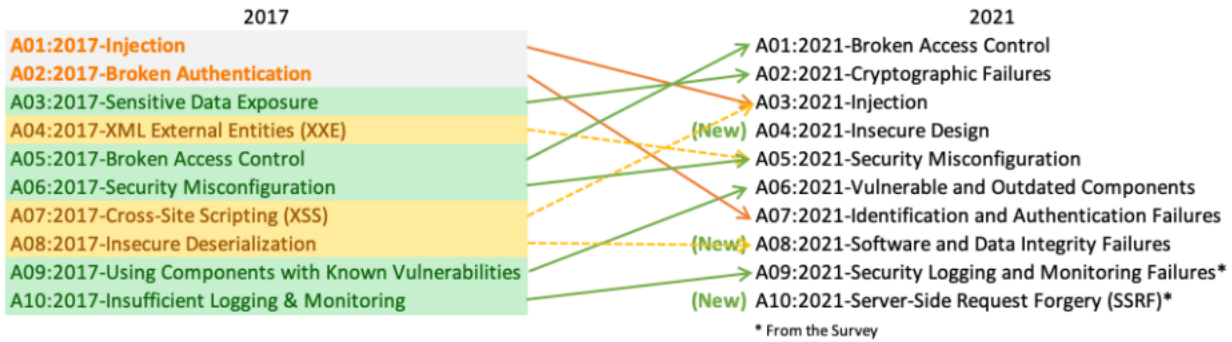
OWASP Top 10 2021 介紹

歡迎來到最新版本的 OWASP Top 10！！OWASP Top 10 2021 是一個全新的名單，包含了你可以列印下來的新圖示說明，若有需要的話，你可以從我們的網頁上面下載。

在此我們想對所有貢獻了他們時間和資料的人給予一個極大的感謝。沒有你們，這一個新版本是不會出現的。**謝謝**。

Top 10 for 2021 有什麼新的變化？

這次在 OWASP Top 10 for 2021 有三個全新的分類，有四個分類有做名稱和範圍的修正，並有將一些類別做合併。



A01:2021-權限控制失效 從第五名移上來; 94% 被測試的應用程式都有驗測到某種類別權限控制失效的問題。在權限控制失效這個類別中被對應到的 34 個 CWEs 在驗測資料中出現的次數都高於其他的弱點類別。

A02:2021-加密機制失效 提升一名到第二名，在之前為 *敏感資料外曝*，在此定義下比較類似於一

Table of contents

Top 10 for 2021 有什麼新的變化？

分析方法

如何建構風險類別

選擇類別時資料的使用方式

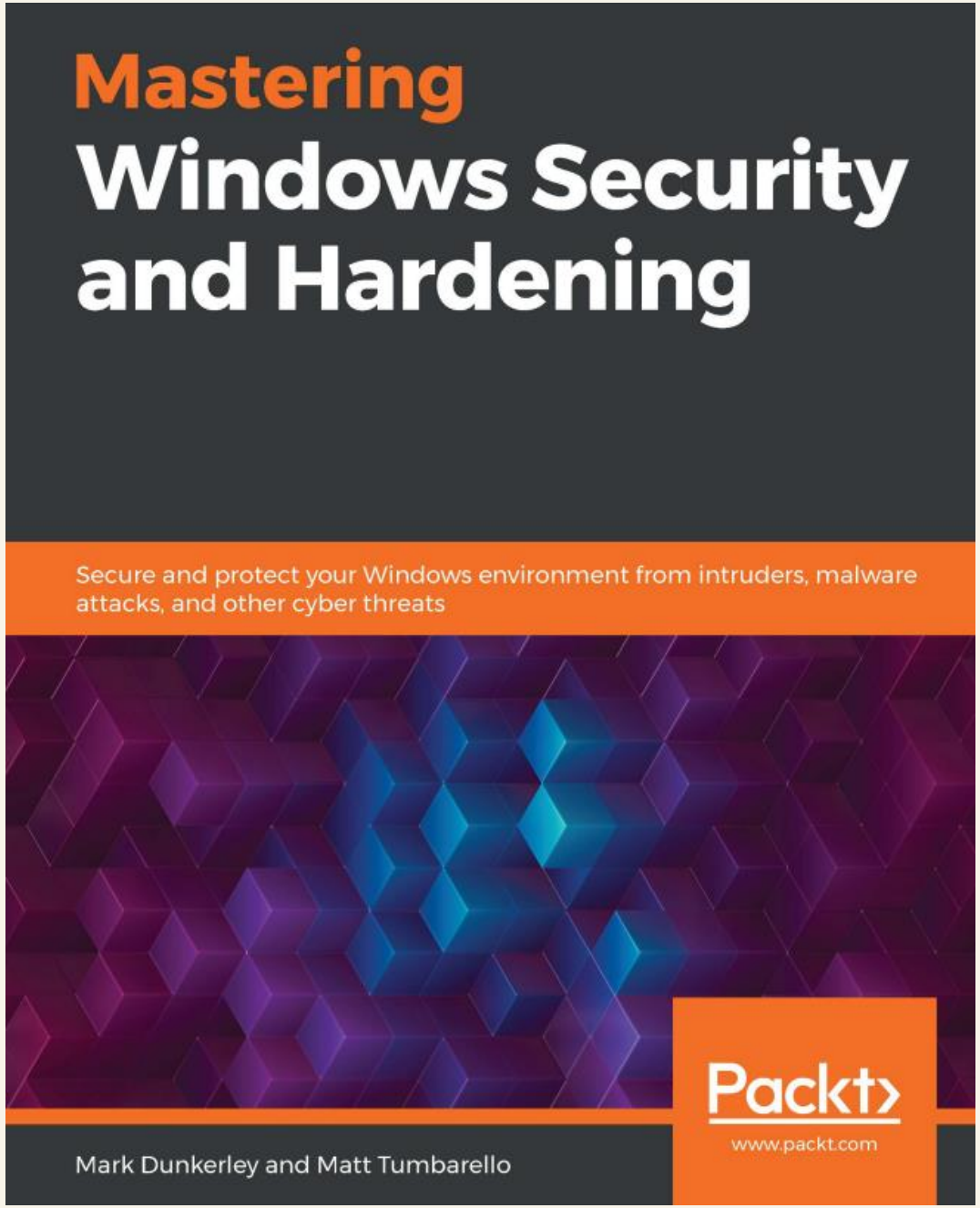
為什麼就不純粹做統計分析？

為什麼用事故率而不是用發生次數

What is your data collection and analysis process?

Data Factors

Category Relationships from 2017



Mobile Application Management 132
Windows enrollment methods 133
Introducing Microsoft Endpoint Manager 134
Summary 138

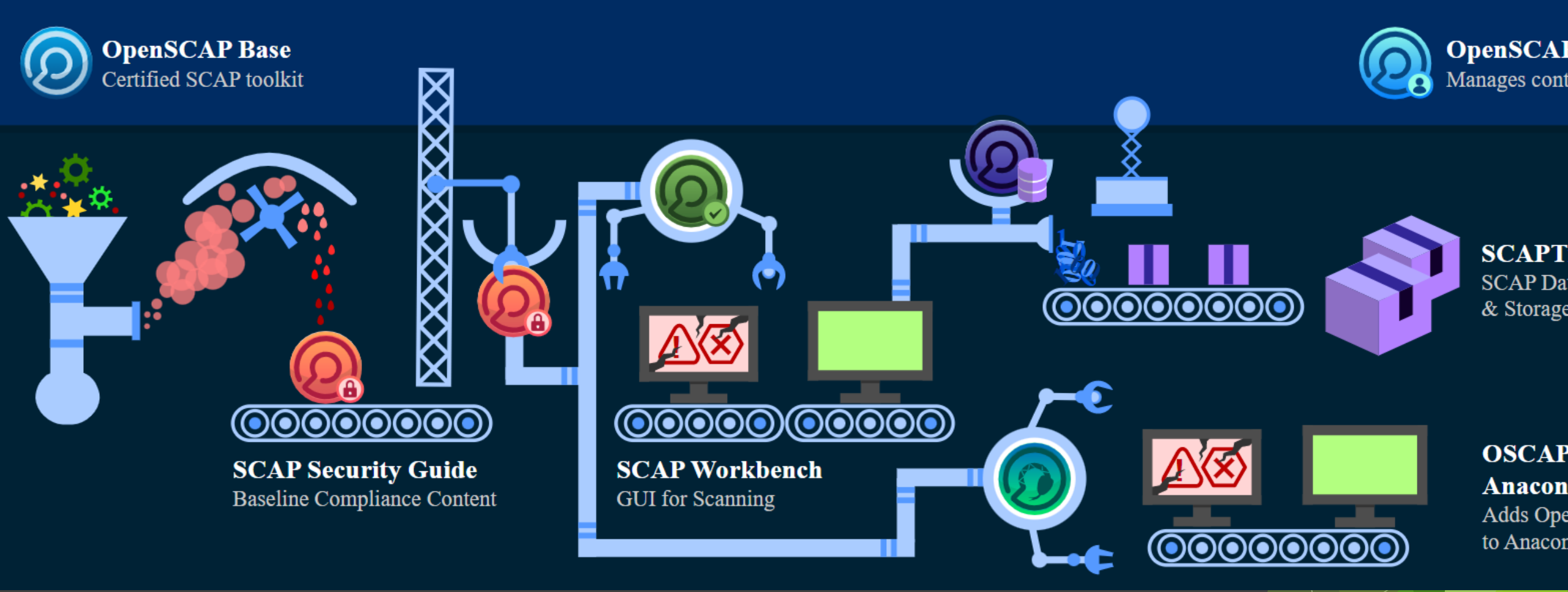
Section 2: Applying Security and Hardening

5
Hardware and Virtualization

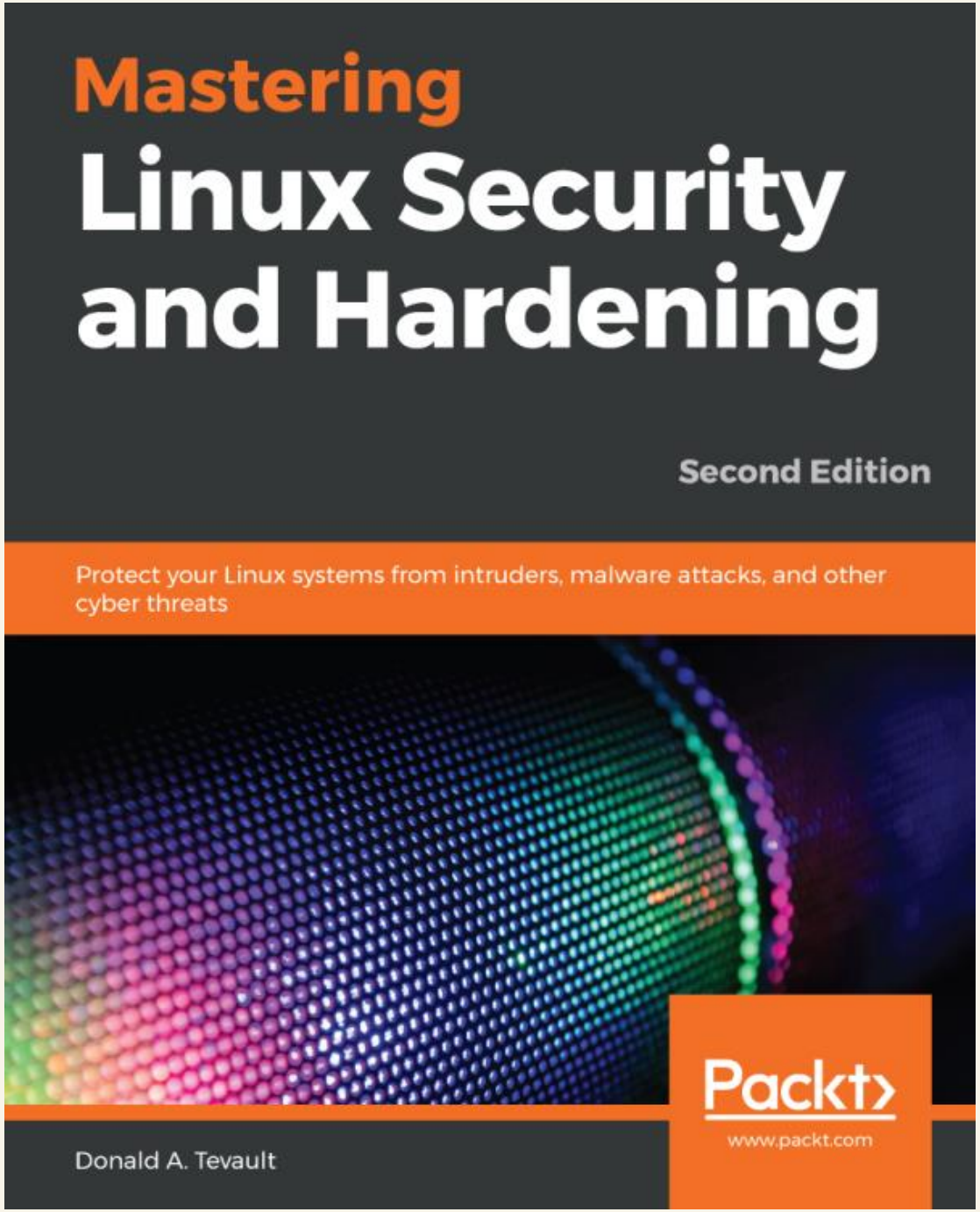
Technical requirements 142
Physical servers and virtualization 143
Microsoft virtualization 144
Hardware security concerns 151
Virtualization security concerns 153
Cloud hardware and virtualization 154
Introduction to hardware certification 154
BIOS and UEFI, TPM 2.0, and Secure Boot 158
Unified Extensible Firmware Interface 159
UEFI Secure Boot 160
Trusted Platform Module (TPM 2.0) 162
Advanced protection with VBS 164
Credential Guard 166
Device Guard 171
Windows Defender Application Guard 175
Hypervisor-Protected Code Integrity 177
Windows Defender System Guard 180
Hardware security recommendations and best practices 182
Summary 182

6
Network Fundamentals for Hardening Windows

Technical requirements 186
Network security fundamentals 187
Understanding Windows Network Security 191
Network baselining 192
Windows 10 193
Windows Server 198
Networking and Hyper-V 201
Network troubleshooting 202
Windows Defender Firewall and Advanced Security 202
Configuring a firewall rule with Group Policy 204
Windows Defender Exploit Guard Network Protection 207
Introducing Azure network security 211
Network Security Groups (NSGs) 211
Summary 218



Linux Security基礎



Scanning the system 487
Remediating the system 489
Using SCAP Workbench 491
Using the OpenSCAP daemon on Ubuntu 18.04 495
Choosing an OpenSCAP profile 499
Applying an OpenSCAP profile during system installation 500
Summary 503
Questions 503
Further reading 505

Chapter 12: Logging and Log Security 506
Understanding the Linux system log files 507
The system log and the authentication log 508
The utmp, wtmp, btmp, and lastlog files 511
Understanding rsyslog 513
Understanding rsyslog logging rules 514
Understanding journald 516
Making things easier with Logwatch 519
Hands-on lab – installing Logwatch 519
Setting up a remote log server 521
Hands-on lab – setting up a basic log server 521
Creating an encrypted connection to the log server 523
Creating a stunnel connection on CentOS 8 – server side 523
Creating an stunnel connection on CentOS 8 – client side 525
Creating a stunnel connection on Ubuntu – server side 526
Creating a stunnel connection on Ubuntu – client side 527
Separating client messages into their own files 528
Summary 529
Questions 530
Further reading 531

Chapter 13: Vulnerability Scanning and Intrusion Detection 533
Introduction to Snort and Security Onion 534
Obtaining and installing Snort 534
Hands-on lab – installing Snort on CentOS 7 535
Graphical interfaces for Snort 537
Using Security Onion 538
Hands-on lab – installing Security Onion 539
IPFire and its built-in Intrusion Prevention System (IPS) 546
Hands-on lab – creating an IPFire virtual machine 547
Scanning and hardening with Lynis 553
Installing Lynis on Red Hat/CentOS 553
Installing Lynis on Ubuntu 553
Scanning with Lynis 554
Finding vulnerabilities with OpenVAS 559
Web server scanning with Nikto 568

防禦工具

ClamAV

- Open Source 防毒軟體，也有Windows版本

LMD

- Linux Malware Detect (LMD/maldet)惡意軟體偵測
- 可與ClamAV並肩作戰

VirusTotal

- 提供可疑檔案分析的網站服務

Rootkit Hunter

檢核系統服務(Auditing system services)

systemctl

```
sudo systemctl -t service --state=active
```

此命令顯示系統上運行的每個服務的狀態

```
UNIT                                    LOAD   ACTIVE SUB     DESCRIPTION
accounts-daemon.service                 loaded active running Accounts Service
apparmor.service                        loaded active exited  Load AppArmor profiles
apport.service                          loaded active exited  LSB: automatic crash report generation
atd.service                             loaded active running Deferred execution scheduler
blk-availability.service                loaded active exited  Availability of block devices
cloud-config.service                    loaded active exited  Apply the settings specified in cloud-config
cloud-final.service                     loaded active exited  Execute cloud user/final scripts
cloud-init-local.service                loaded active exited  Initial cloud-init job (pre-networking)
cloud-init.service                      loaded active exited  Initial cloud-init job (metadata service crawler)
console-setup.service                   loaded active exited  Set console font and keymap
cron.service                            loaded active running Regular background program processing daemon
dbus.service                            loaded active running D-Bus System Message Bus
finalrd.service                         loaded active exited  Create final runtime dir for shutdown pivot root
getty@tty1.service                      loaded active running Getty on tty1
getty@tty6.service                      loaded active running Getty on tty6
irqbalance.service                      loaded active running irqbalance daemon
keyboard-setup.service                  loaded active exited  Set the console keyboard layout
```

檢核系統服務–netstat

追蹤系統上執行的網路服務目的

1. 確認不需要的服務沒有在運行
2. 確認沒有任何正在偵聽網路連線的惡意程式

```
sudo netstat -lp -A inet
```

-l 正在傾聽的網路埠 display listening server sockets
-p display PID/Program name for sockets
-A inet 只看 inet 家族協定的資訊 (raw,tcp,udp)
List of possible address families
inet (DARPA Internet) inet6 (IPv6)...

```
sudo netstat -lp -A inet6
```

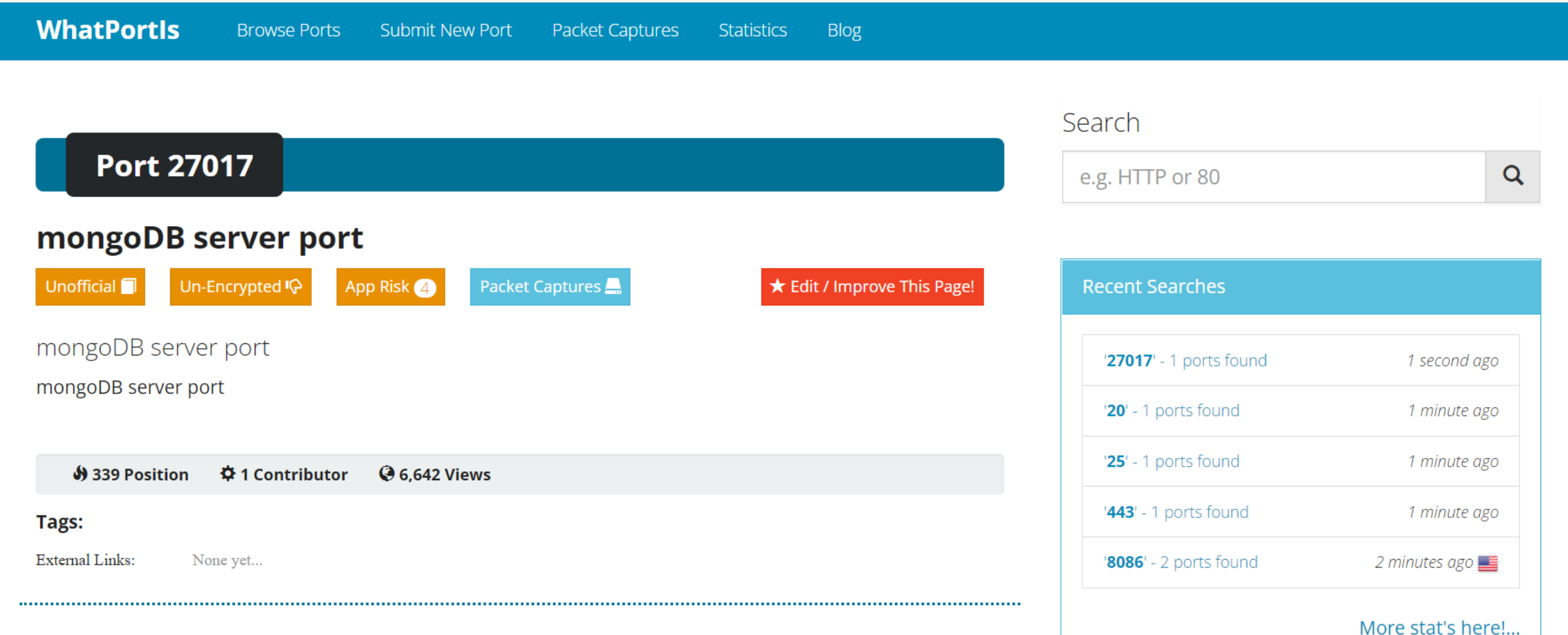
```
eric@rocketchat:~$
eric@rocketchat:~$ netstat -lp -A inet
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program nam
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3000            0.0.0.0:*               LISTEN      -
tcp        0      0 localhost:27017         0.0.0.0:*               LISTEN      -
udp        0      0 localhost:domain        0.0.0.0:*                           -
```

```
eric@rocketchat:~$ sudo netstat -lp -A inet
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      680/systemd-resolve
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      758/sshd: /usr/sbin
tcp        0      0 0.0.0.0:3000            0.0.0.0:*               LISTEN      1280/node
tcp        0      0 localhost:27017         0.0.0.0:*               LISTEN      894/mongod
udp        0      0 localhost:domain        0.0.0.0:*                           680/systemd-resolve
```

```
eric@rocketchat:~$ sudo netstat -lp -A inet6
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp6       0      0 [::]:http               [::]:*                  LISTEN      706/caddy
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      758/sshd: /usr/sbin
tcp6       0      0 [::]:https              [::]:*                  LISTEN      706/caddy
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7           678/systemd-network
eric@rocketchat:~$
```

WhatPortIs https://whatportis.com

例如我們查詢上圖中 netstat 所列出port 27017

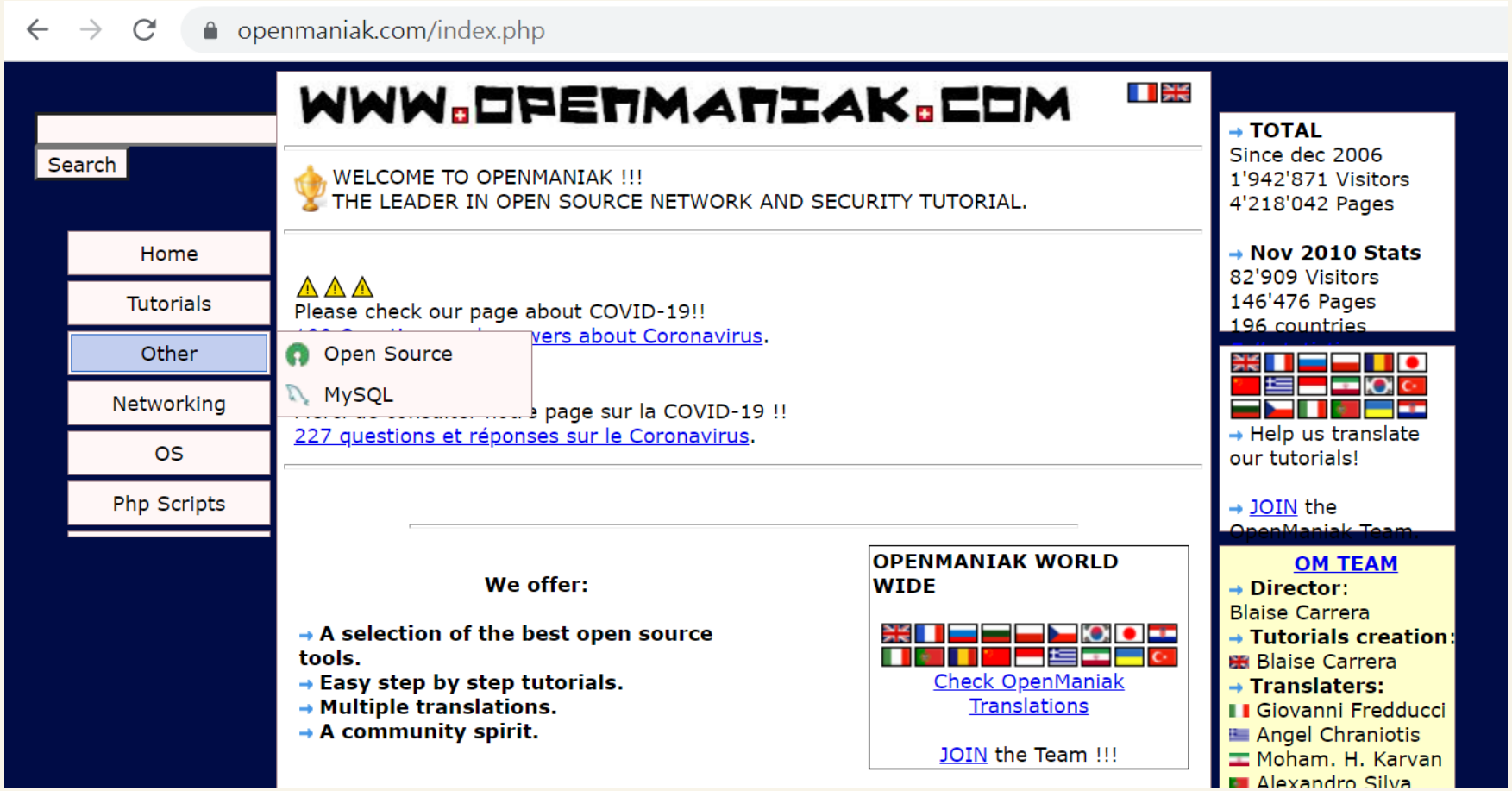


檢核系統服務–netstat

[延伸練習]

netstat -p -A inet

netstat -np -A inet



[學習資源]

https://openmaniak.com/netstat.php

THE LEADER IN OPEN SOURCE NETWORK AND SECURITY TUTORIAL.

檢核系統服務–Nmap

netstat 非常好，但是有個小缺點是您必須登入您網路上每一台主機才能使用
如果您想要遠端檢核您網路上每台主機正在運行哪些服務，但是不想登入主機，那麼 Nmap就是您需要的工具

[安裝]

```
sudo apt install nmap
```

[範例]

```
nmap -v -A scanme.nmap.org
nmap -v -sn 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -Pn -p 80
```

-v:Increase verbosity level (use -vv or more for greater effect)

-A: Enable OS detection, version detection, script scanning, and traceroute

-sn: TCP Null, FIN, and Xmas scans

-iR <num hosts>: Choose random targets

-Pn: Treat all hosts as online -- skip host discovery

-p <port ranges>: Only scan specified ports

檢核系統服務–Nmap

[練習]

sudo nmap -v -A 127.0.0.1

[參考]

Nmap 官網

https://nmap.org

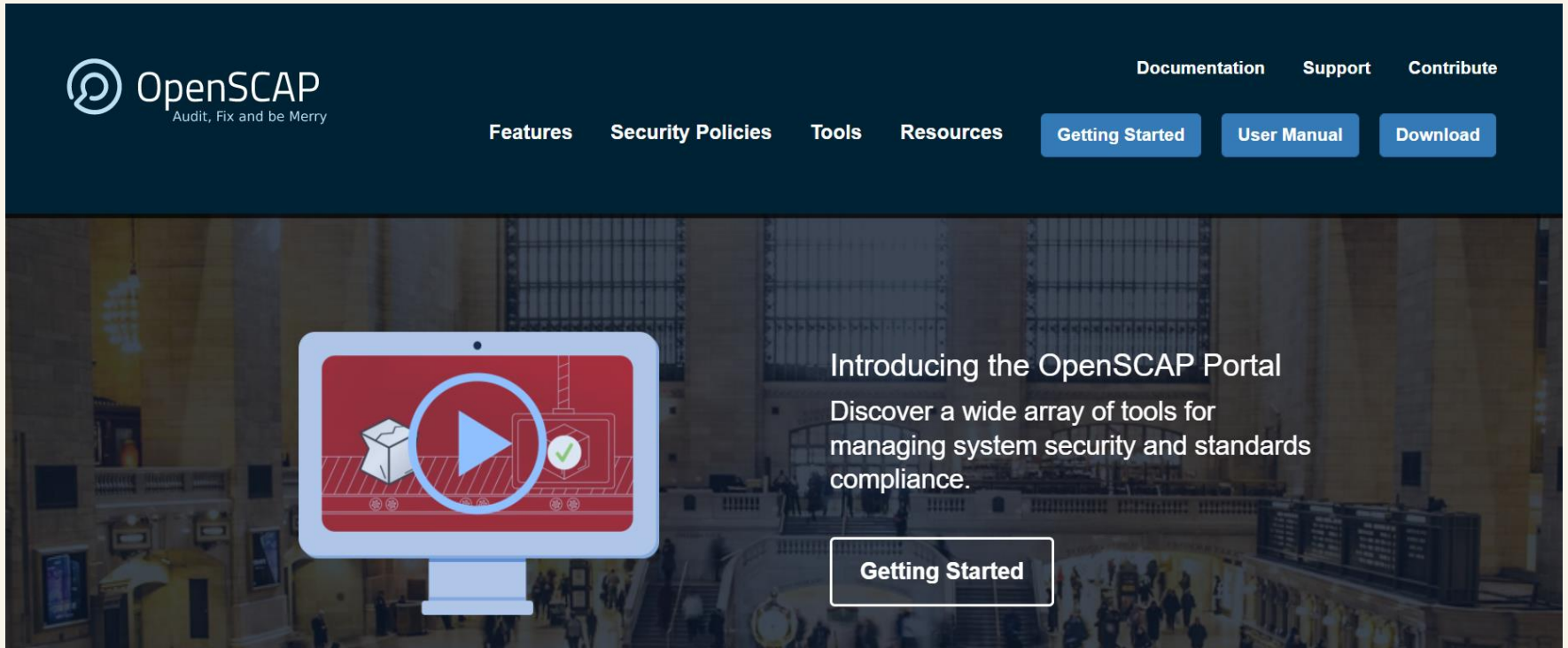
```
eric@rocketchat:~$ sudo nmap -v -A 127.0.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2021-12-27 15:02
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating NSE at 15:02
Completed NSE at 15:02, 0.00s elapsed
Initiating SYN Stealth Scan at 15:02
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 443/tcp on 127.0.0.1
Discovered open port 3000/tcp on 127.0.0.1
Completed SYN Stealth Scan at 15:02, 0.07s elapsed (1000 to
Initiating Service scan at 15:02
Scanning 4 services on localhost (127.0.0.1)
Completed Service scan at 15:02, 14.00s elapsed (4 services
Initiating OS detection (try #1) against localhost (127.0.0
NSE: Script scanning 127.0.0.1.
Initiating NSE at 15:02
```

檢核系統服務–OpenSCAP

Security Content Automation Protocol(SCAP) 由美國國家標準與技術研究院(NIST)制定，包含用於設置安全系統的強化指南、強化模板和基線配置指南
而OpenSCAP就是開源的實作SCAP工具，具備

Security profiles /Security guides/Security templates/SCAP workbench

https://www.open-scap.org/



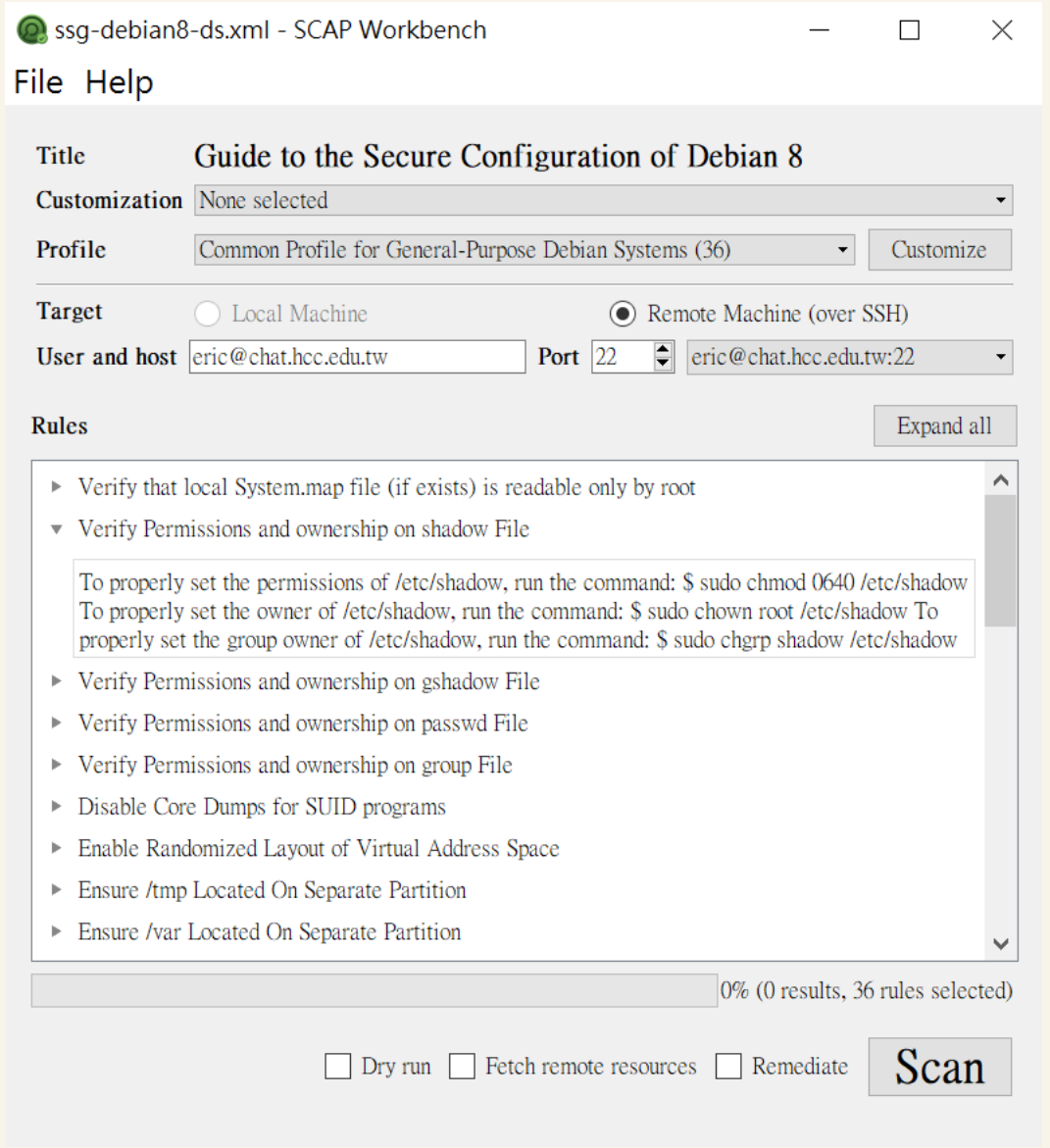
檢核系統服務–OpenSCAP

[Ubuntu 安裝]

sudo apt install openscap-daemon ssg-applications ssg-base ssg-debian ssg-debderived ssg-nondebian

[Windows安裝　SCAP Workbench]

https://www.open-scap.org/tools/scap-workbench/#download



檢核系統服務–Security Checklist

HHS.gov
Health Information Privacy

HIPAA checklist
https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

PCI Security Standards Council

PCI-DSS checklist
https://www.pcisecuritystandards.org/

電腦硬體安全

BIOS/UEFI的安全性---加強電腦硬體安全

每台電腦都有BIOS或是UEFI晶片，儲存著硬體設置和開機後啟動程序指令。UEFI簡單來說就是改良版的BIOS，它比舊式的BIOS具有更多安全功能。所以使用較新的 UEFI 模式安裝 OS才是好選擇。

[作為]

1. 檢查開機順序
2. 停用不必要的裝置(SATA2,Rear USB等)
3. CPU的安全功能
4. BIOS/UEFI的設定密碼

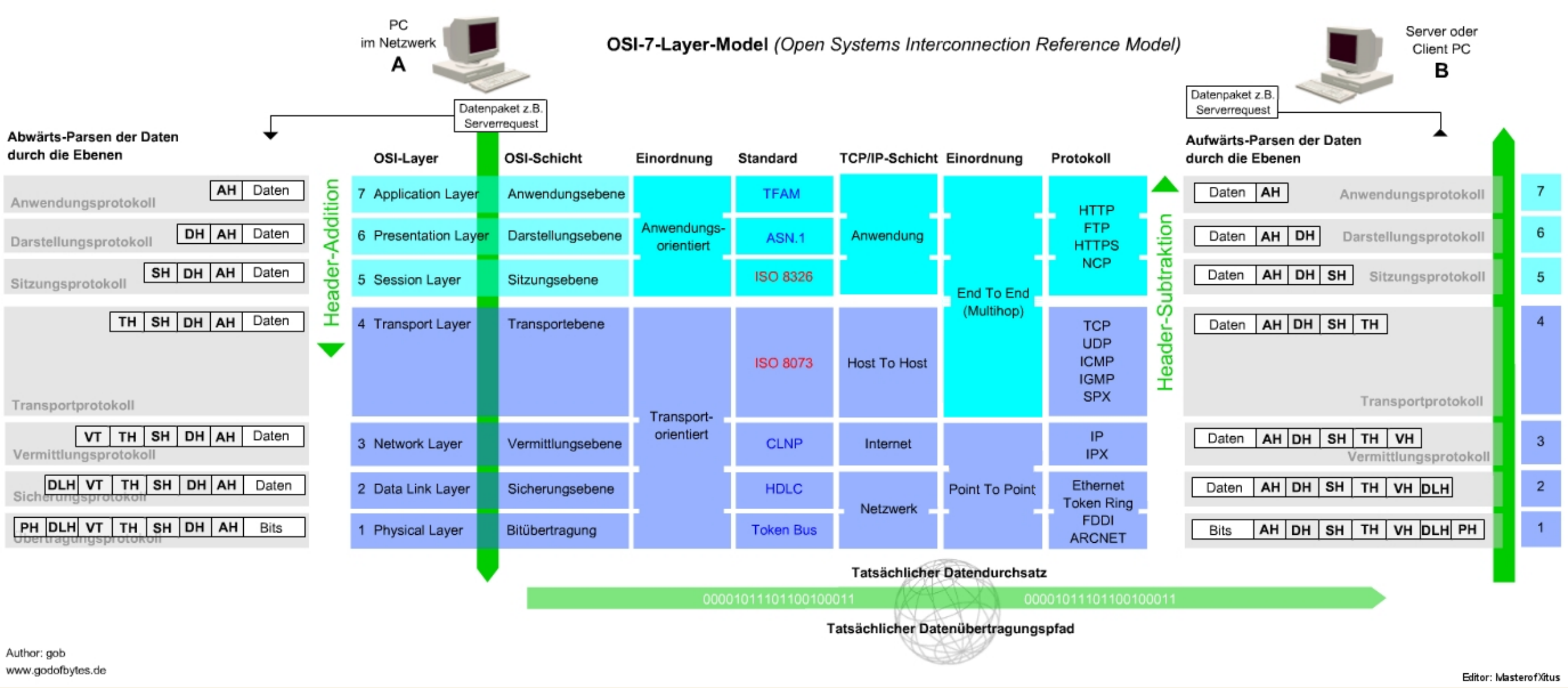
[UEFI]

統一可延伸韌體介面（英語：Unified Extensible Firmware Interface，縮寫UEFI）是一種個人電腦系統規格，用來定義作業系統與系統韌體之間的軟體介面，作為BIOS的替代方案[1]。可延伸韌體介面負責加電自檢（POST）、聯絡作業系統以及提供連接作業系統與硬體的介面。

UEFI在概念上類似於一個低階的作業系統，並且具有操控所有硬體資源的能力。不少人感覺它的不斷發展將有可能代替現代的作業系統。

網路通訊的安全

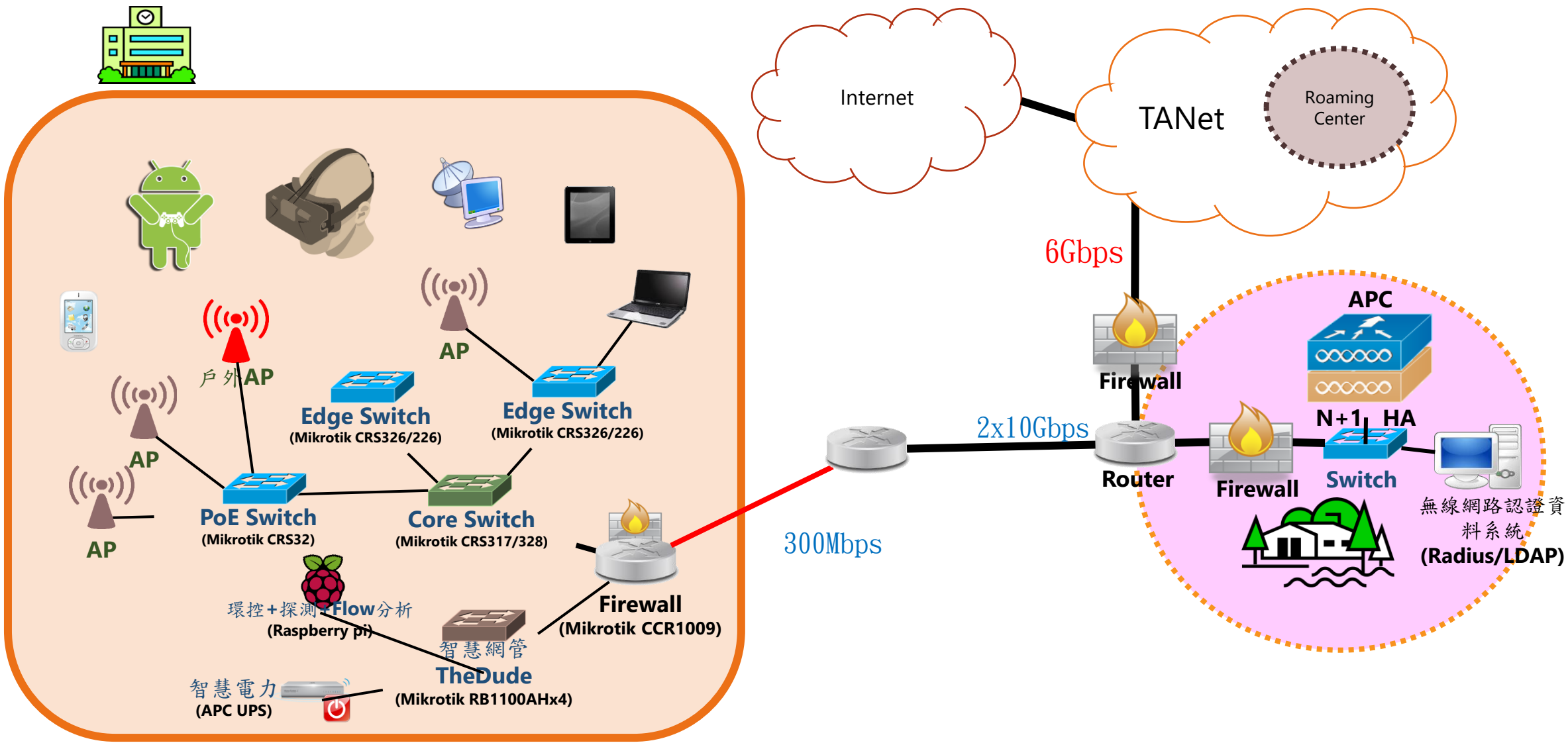
七層架構觀–Divide & Conquer



Author: gob
www.godofbytes.de

Editor: MasterofXitus

縱深防禦


Internet
TANet
Roaming Center
6Gbps
Firewall
APC
N+1
HA
2x10Gbps
Router
Firewall
Switch
無線網路認證資料系統
(Radius/LDAP)
300Mbps
AP
戶外AP
AP
Edge Switch
(Mikrotik CRS326/226)
Edge Switch
(Mikrotik CRS326/226)
AP
AP
PoE Switch
(Mikrotik CRS32)
Core Switch
(Mikrotik CRS317/328)
Firewall
(Mikrotik CCR1009)
環控+探測+Flow分析
(Raspberry pi)
智慧網管
TheDude
(Mikrotik RB1100AHx4)
智慧電力
(APC UPS)

防火牆知多少

忠實的警衛

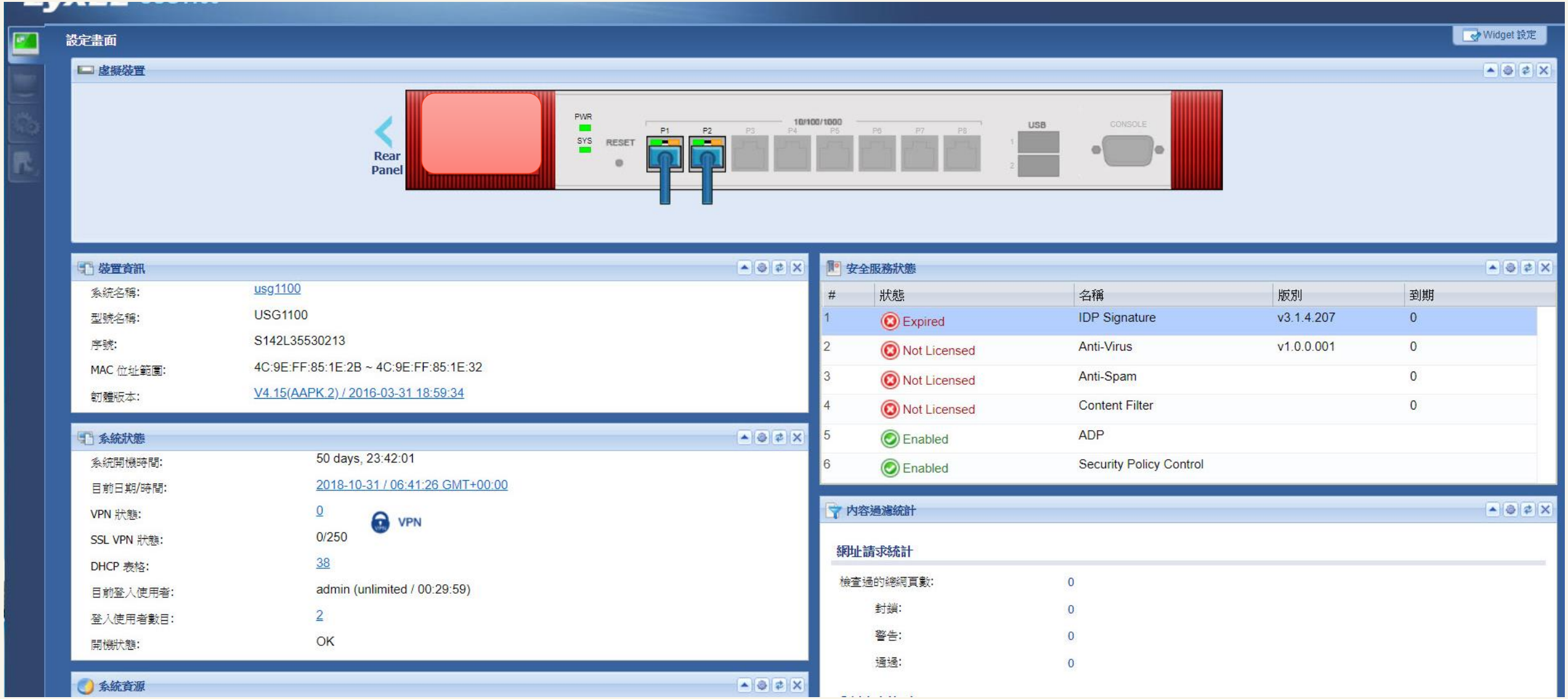
Host

- Microsoft Defender Firewall
- Linux iptables

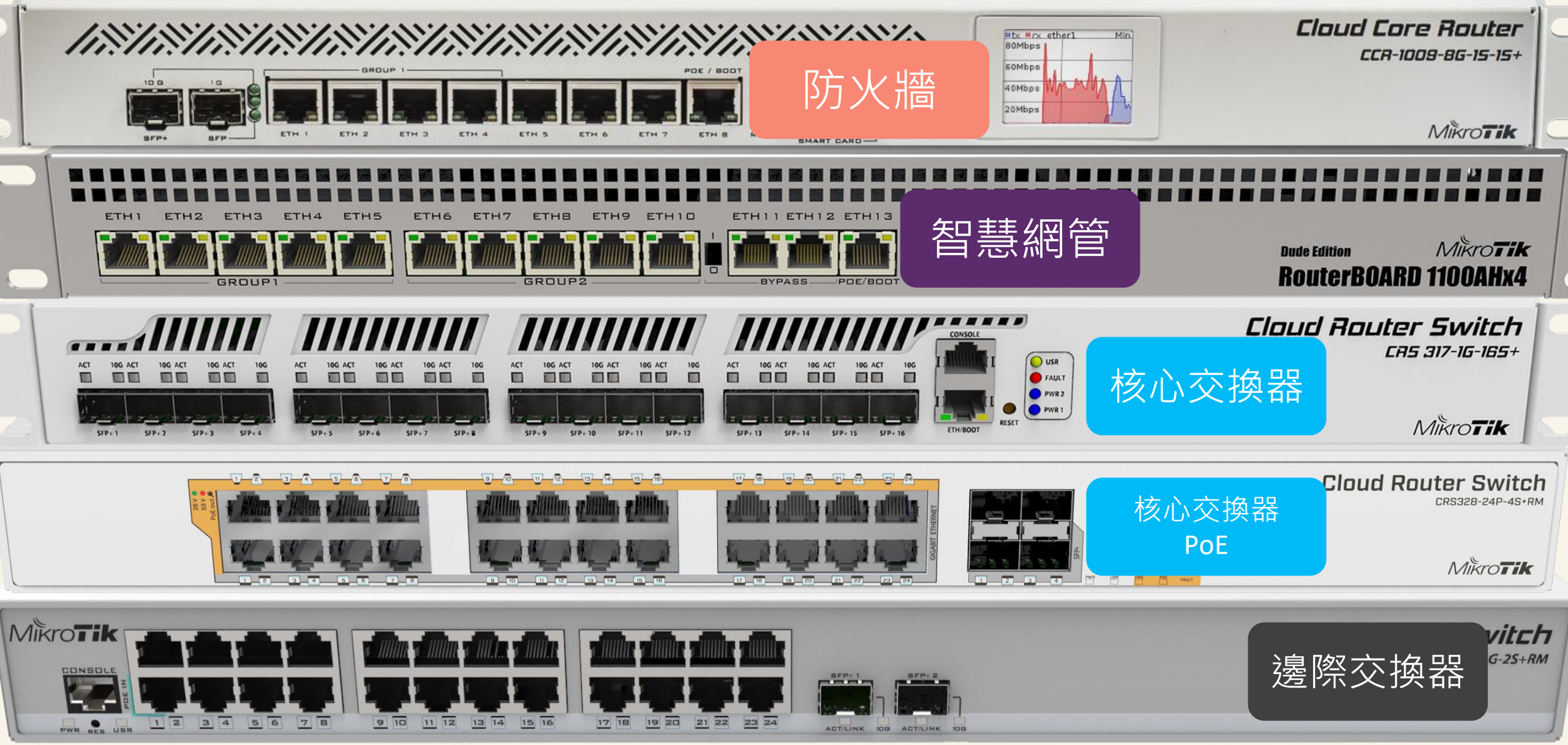
Network

- MikroTik Firewall

某廠牌防火牆授權到期


設定畫面
Widget 設定
虛擬裝置
Rear Panel
PWR
SYS
RESET
P1
P2
10/100/1000
USB
CONSOLE
裝置資訊
系統名稱: usg1100
型號名稱: USG1100
序號: S142L35530213
MAC 位址範圍: 4C:9E:FF:85:1E:2B ~ 4C:9E:FF:85:1E:32
韌體版本: V4.15(AAPK.2) / 2016-03-31 18:59:34
安全服務狀態
狀態 名稱 版別 到期
1 Expired IDP Signature v3.1.4.207 0
2 Not Licensed Anti-Virus v1.0.0.001 0
3 Not Licensed Anti-Spam 0
4 Not Licensed Content Filter 0
5 Enabled ADP
6 Enabled Security Policy Control
系統狀態
系統開機時間: 50 days, 23:42:01
目前日期/時間: 2018-10-31 / 06:41:26 GMT+00:00
VPN 狀態: 0
SSL VPN 狀態: 0/250
VPN
DHCP 表格: 38
目前登入使用者: admin (unlimited / 00:29:59)
登入使用者數目: 2
開機狀態: OK
內容過濾統計
網址請求統計
檢查過的總網頁數: 0
封鎖: 0
警告: 0
通過: 0
系統資源

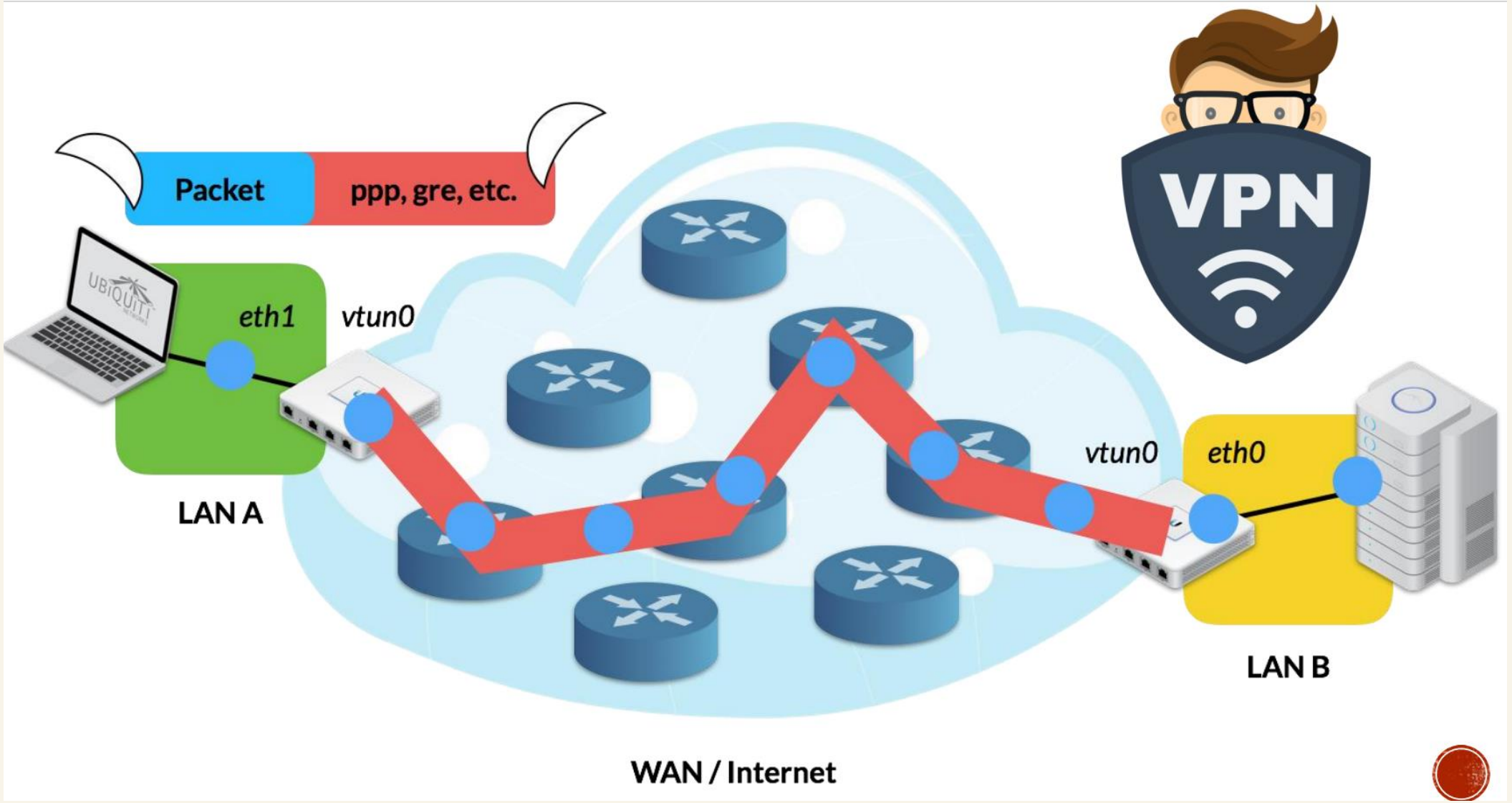
MikroTik 網路設備



積極防護的解決方案

虛擬IP與NAT活用/VPN建置與應用/Log戰情蒐集

VPN


Packet
ppp, gre, etc.
eth1
vtun0
LAN A
VPN
vtun0
eth0
LAN B
WAN / Internet

建構VPN服務 L2TP over IPSec VPN Server

- 建構VPN服務 L2TP over IPSec VPN Server

1.建立 VPN 網段 (也可以用現有的DHCP網段)

/ip pool add name=vpn_pool ranges=10.0.0.1-10.0.0.100

2.建立給 L2TP 使用的 profile

/ppp profile add local-address=192.168.88.1 name=l2tp_profile remote-address=vpn_pool use-encryption=required

- [註] local-address 可改用其他 Local IP

3.建立 L2TP 連線用的帳號密碼

/ppp secret add name=帳號 password=密碼 profile=l2tp_profile service=l2tp

4.啟動 L2TP Server

/interface l2tp-server server set default-profile=l2tp_profile enabled=yes ipsec-secret=秘鑰 use-ipsec=yes

5.開防火牆

/ip firewall filter add chain=input action=accept protocol=17 dst-port=500,1701,4500

校園網路智慧管理系統

視覺化、人工智慧(AI)應用、大數據(Big Data)分析、資安聯防、雲服務(Cloud Computing)與霧運算

視覺化異質設備管理

導入智慧化視覺式網路品質、物聯裝置監測管理系統
對異質網路設備進行監測及控制、行動載具管控

異常警訊與設備管控

資訊具體明白、資產盤點、狀態即時掌握、隔離封鎖
網路異常時簡訊即時通知管理人員

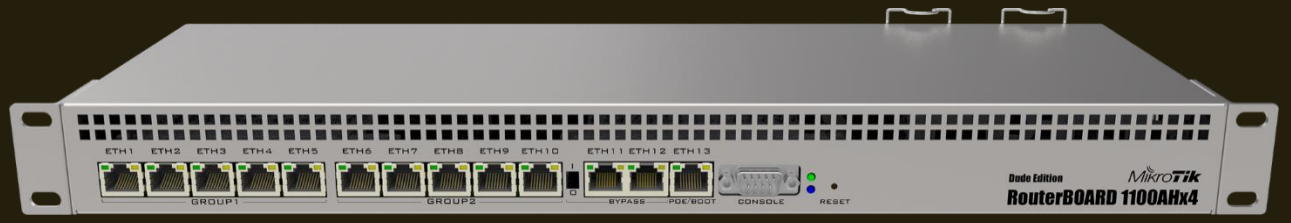
數據分析與資產管理

提供網路拓樸自動產出、監控資訊面板、資產清單、
效能使用率、統計報表等功能

流量與日誌倉儲

SNMP蒐集統計、Netflow流量使用分析、Syslog日誌事件匯聚
資安聯防與稽核

智慧網管運算與倉儲中心



邊際運算資料存取（edge computing）設備#1

- ✓ 可安裝四顆固態硬碟，做為 FTP與Syslog Server儲存用。
- ✓ 自動偵測、辨識介接設備的能力，提供介接連線設備之型號、韌體版本、MAC位址、系統名稱等資訊，並支援單鍵連線至該設備的管理介面。支援SNMP v1/v2c/v3。
- ✓ 具有API Service，透過API 蒐集設備資訊、調整設定和管理設備，並提供Python、PHP或C# 的API函式庫。
- ✓ Traffice Flow 支援NetFlow v9或 sFlow，可傳送至流量分析伺服器(例如 ntopng)進行封包 蒐集與分析。
- ✓ 支援Syslog協定，可接收儲存設備系統訊息，提供Syslog倉儲功能。
- ✓ 內建管理系統，具備視覺化網路拓樸、設備狀態查詢、流量統計、事件通知等功能。
- ✓ 將學校現有支援SNMP協定的設備，以及本計畫網路設備與不斷電系統，完成相關設定納入監管

遠端遙控與環境感測設備

- ✓ 採用樹莓派Raspberry Pi 3 Model B+建構
- ✓ DHT22數位溫溼度感測器，以及I2C 16x2 LCD顯示器。
- ✓ 本中心建置乙個供各校使用之雲端平台。功能包含：各校機房溫溼度數據統計、各校機房UPS電力狀況。
- ✓ 各校裝置的遠端控制，可以從雲端伺服器存取遠端裝置的 SSH、RS232、RDP，並提供雲端帳號密碼的控管功能。
- ✓ NTOP 流量分析(接收NetFlow資料)

邊際運算資料存取（ edge computing ）設備#2
High-Speed Web-based Traffic Analysis and Flow Collection

Settings

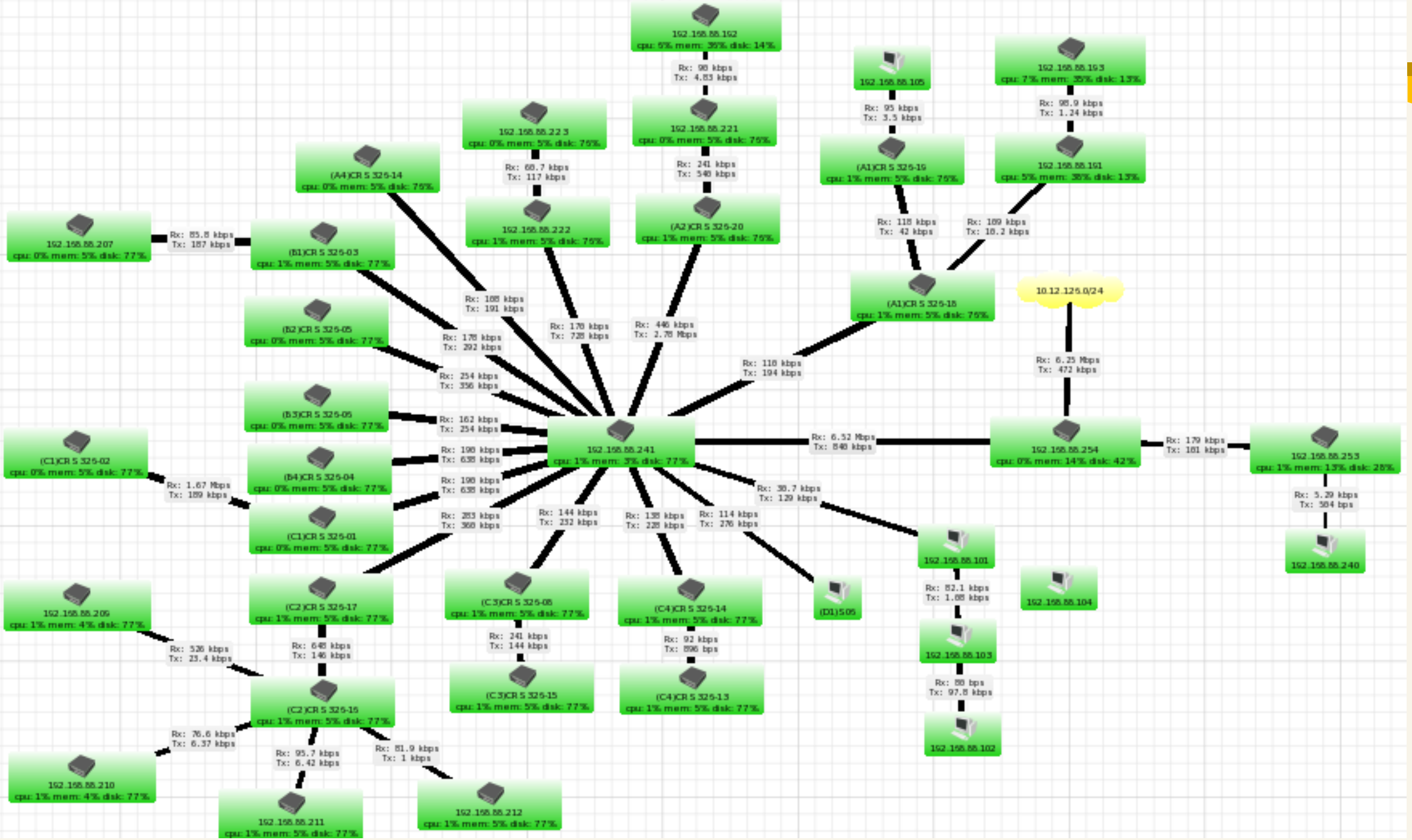
Contents

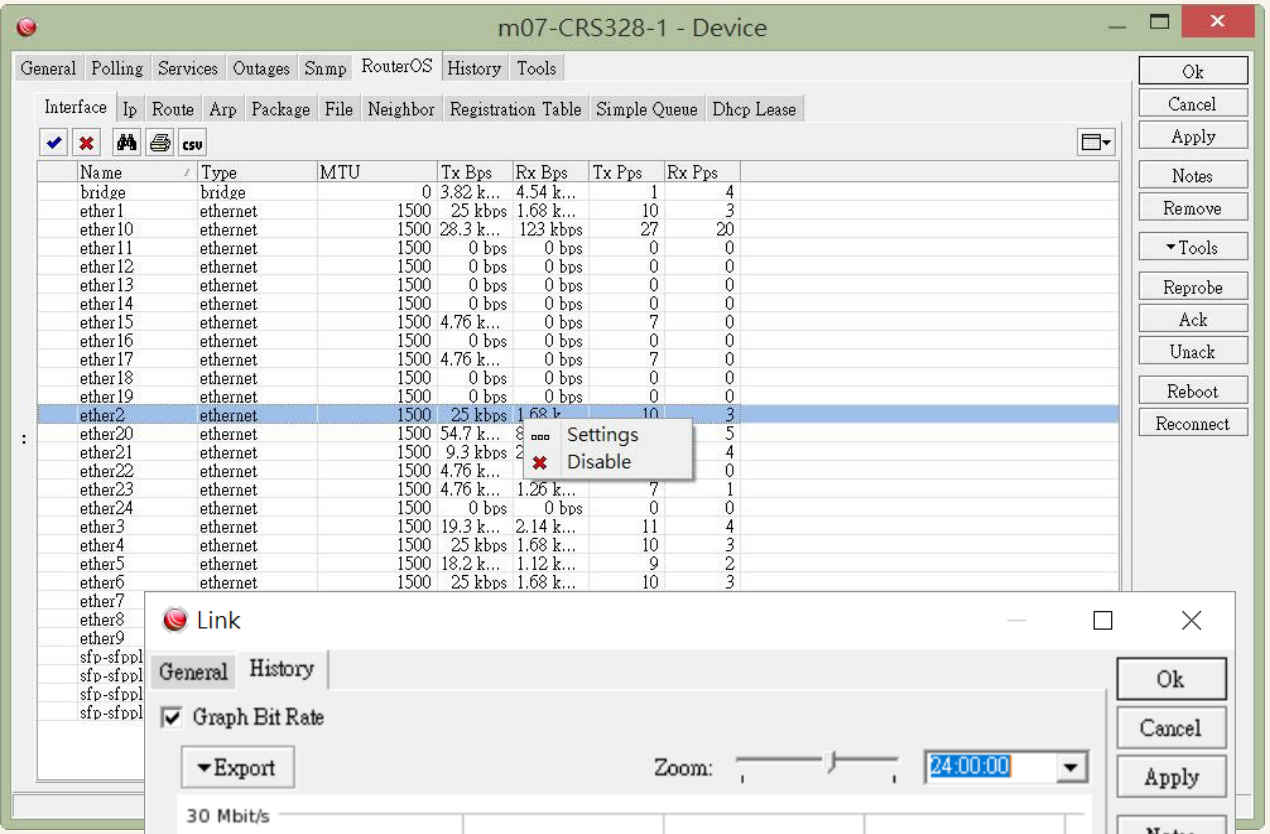
- Charts
  - CPU
  - Chart
  - Flow Map
- Devices
- Files
- Functions
- History Actions
- Links
- Log
- Mib Nodes
- Network Maps
  - 五峰
  - 北埔
  - 寶山
  - 尖石
  - 峨嵋
  - 新埔
  - 新竹縣全境
  - 新豐
  - 橫山
  - 湖口
  - 竹北
  - 竹東
  - 芎林
  - 關西
  - 高中職及私立...

Settings | Discover | Tools | Layer: links

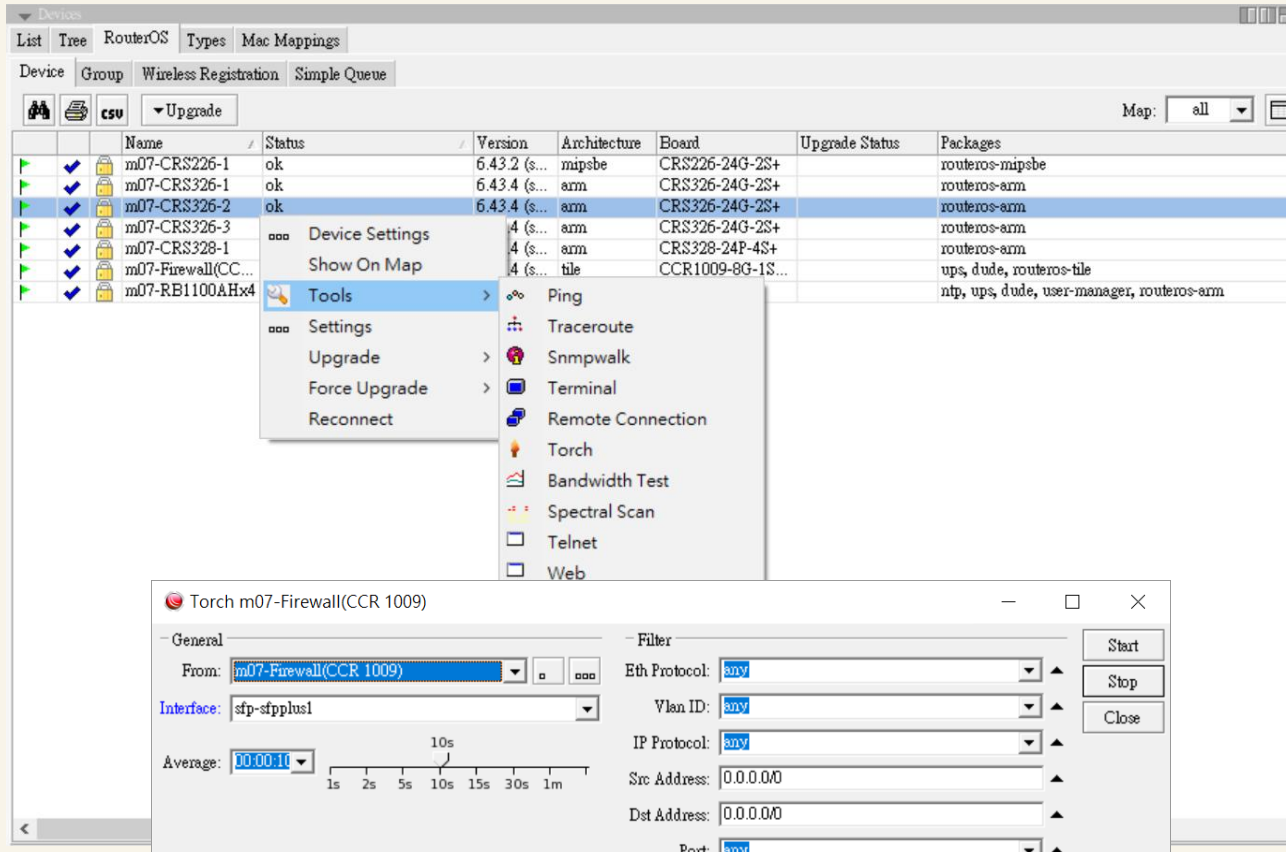
Network Map 尖石
Up: 新光國小, 新光國小-司馬庫斯分班, 秀巒國小, 秀巒國小-田埔分校, 石磊國小, 尖石國小, 嘉興國小, 嘉興分校, 新樂國小, 梅花國小, 錦屏國小, 玉峰國小, 尖石國中
Partially down:
Down:
Acked:
Unknown:
Notes:

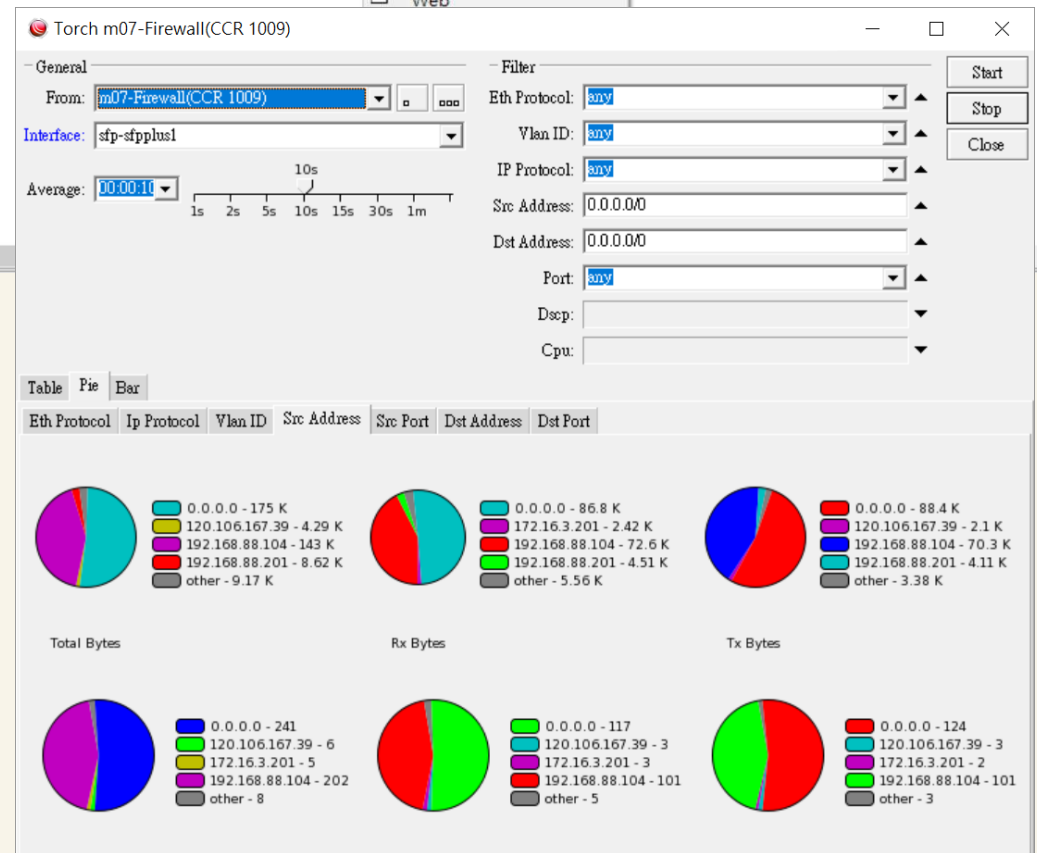
Client: rx 15.6 kbps / tx 351 bps | Server: rx 0 bps / tx 0 bps | connected


192.168.88.192
cpu: 6% mem: 39% disk: 14%
Rx: 90 kbps
Tx: 4.83 kbps
192.168.88.221
cpu: 0% mem: 5% disk: 76%
Rx: 241 kbps
Tx: 540 kbps
192.168.88.223
cpu: 0% mem: 5% disk: 76%
Rx: 60.7 kbps
Tx: 117 kbps
192.168.88.222
cpu: 1% mem: 5% disk: 76%
(A2)CR S 326-20
cpu: 1% mem: 5% disk: 76%
Rx: 446 kbps
Tx: 2.76 Mbps
192.168.88.105
Rx: 95 kbps
Tx: 3.5 kbps
(A1)CR S 326-19
cpu: 1% mem: 5% disk: 76%
192.168.88.193
cpu: 7% mem: 35% disk: 13%
Rx: 98.9 kbps
Tx: 1.24 kbps
192.168.88.191
cpu: 5% mem: 38% disk: 13%
Rx: 118 kbps
Tx: 42 kbps
Rx: 109 kbps
Tx: 10.2 kbps
(A1)CR S 326-18
cpu: 1% mem: 5% disk: 76%
10.12.126.0/24
Rx: 6.25 Mbps
Tx: 472 kbps
(A4)CR S 326-14
cpu: 0% mem: 5% disk: 76%
192.168.88.207
cpu: 0% mem: 5% disk: 77%
Rx: 85.8 kbps
Tx: 187 kbps
(B1)CR S 326-03
cpu: 1% mem: 5% disk: 77%
Rx: 188 kbps
Tx: 191 kbps
Rx: 178 kbps
Tx: 728 kbps
(B2)CR S 326-05
cpu: 0% mem: 5% disk: 77%
Rx: 178 kbps
Tx: 292 kbps
Rx: 254 kbps
Tx: 356 kbps
(B3)CR S 326-06
cpu: 0% mem: 5% disk: 77%
Rx: 162 kbps
Tx: 254 kbps
(B4)CR S 326-04
cpu: 0% mem: 5% disk: 77%
Rx: 190 kbps
Tx: 638 kbps
Rx: 190 kbps
Tx: 638 kbps
(C1)CR S 326-02
cpu: 0% mem: 5% disk: 77%
Rx: 1.67 Mbps
Tx: 189 kbps
(C1)CR S 326-01
cpu: 0% mem: 5% disk: 77%
Rx: 283 kbps
Tx: 360 kbps
192.168.88.241
cpu: 1% mem: 3% disk: 77%
Rx: 6.52 Mbps
Tx: 840 kbps
192.168.88.254
cpu: 0% mem: 14% disk: 42%
Rx: 179 kbps
Tx: 181 kbps
192.168.88.253
cpu: 1% mem: 13% disk: 28%
Rx: 5.29 kbps
Tx: 504 bps
192.168.88.240
Rx: 144 kbps
Tx: 232 kbps
Rx: 138 kbps
Tx: 228 kbps
Rx: 114 kbps
Tx: 276 kbps
Rx: 30.7 kbps
Tx: 129 kbps
(D1)505
192.168.88.101
Rx: 82.1 kbps
Tx: 1.08 kbps
192.168.88.104
192.168.88.103
Rx: 80 bps
Tx: 97.8 kbps
192.168.88.102
192.168.88.209
cpu: 1% mem: 4% disk: 77%
Rx: 526 kbps
Tx: 23.4 kbps
(C2)CR S 326-17
cpu: 1% mem: 5% disk: 77%
Rx: 648 kbps
Tx: 146 kbps
(C2)CR S 326-16
cpu: 1% mem: 5% disk: 77%
Rx: 76.6 kbps
Tx: 6.37 kbps
Rx: 95.7 kbps
Tx: 6.42 kbps
Rx: 81.9 kbps
Tx: 1 kbps
192.168.88.210
cpu: 1% mem: 4% disk: 77%
192.168.88.211
cpu: 1% mem: 5% disk: 77%
192.168.88.212
cpu: 1% mem: 5% disk: 77%
(C3)CR S 326-05
cpu: 1% mem: 5% disk: 77%
Rx: 241 kbps
Tx: 144 kbps
(C3)CR S 326-15
cpu: 1% mem: 5% disk: 77%
(C4)CR S 326-14
cpu: 1% mem: 5% disk: 77%
Rx: 92 kbps
Tx: 896 bps
(C4)CR S 326-13
cpu: 1% mem: 5% disk: 77%

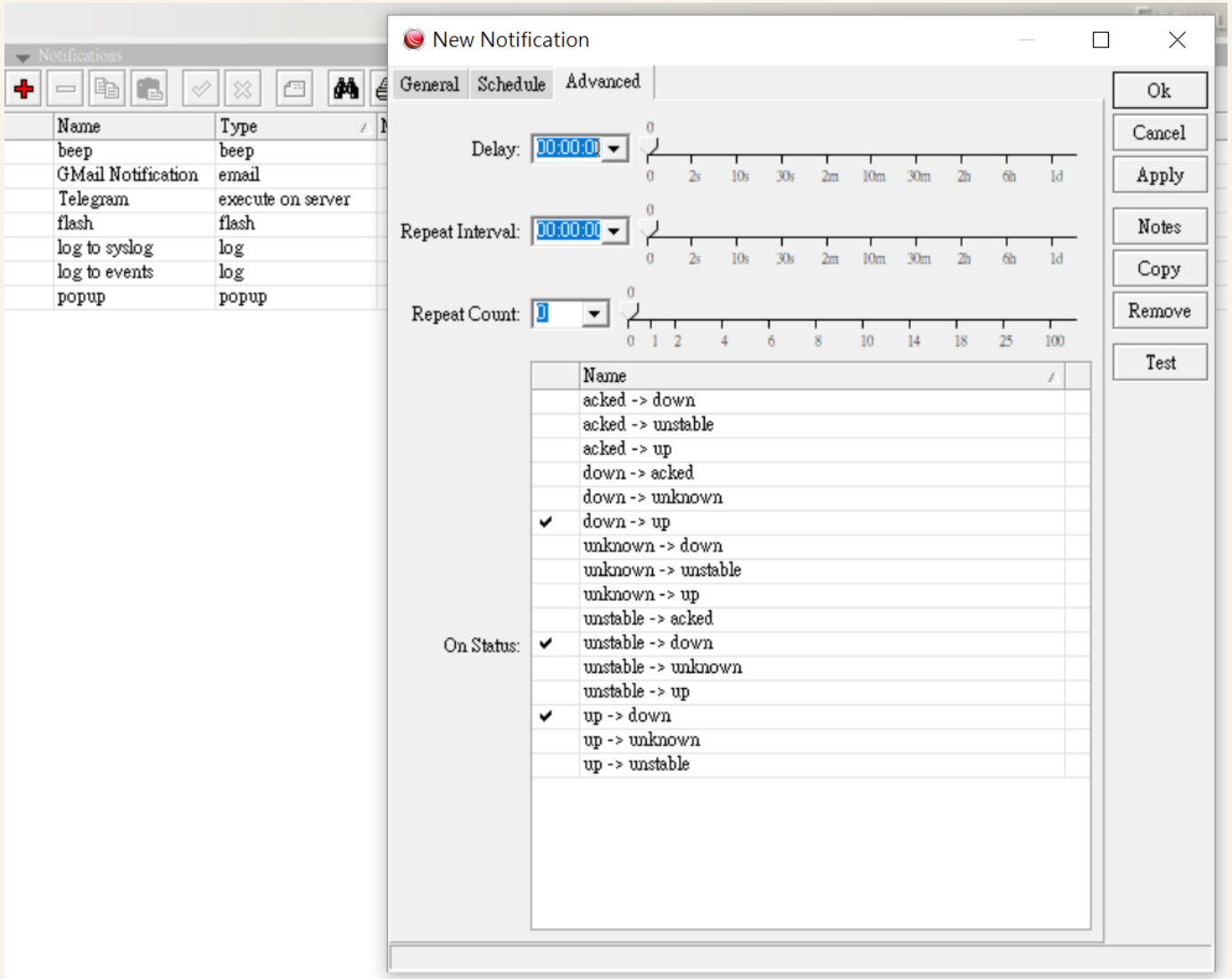

m07-CRS328-1 - Device
General Polling Services Outages Snmp RouterOS History Tools
Interface Ip Route Arp Package File Neighbor Registration Table Simple Queue Dhcp Lease
Name Type MTU Tx Bps Rx Bps Tx Pps Rx Pps
bridge bridge 0 3.82 k... 4.54 k... 1 4
ether1 ethernet 1500 25 kbps 1.68 k... 10 3
ether10 ethernet 1500 28.3 k... 123 kbps 27 20
ether11 ethernet 1500 0 bps 0 bps 0 0
ether12 ethernet 1500 0 bps 0 bps 0 0
ether13 ethernet 1500 0 bps 0 bps 0 0
ether14 ethernet 1500 0 bps 0 bps 0 0
ether15 ethernet 1500 4.76 k... 0 bps 7 0
ether16 ethernet 1500 0 bps 0 bps 0 0
ether17 ethernet 1500 4.76 k... 0 bps 7 0
ether18 ethernet 1500 0 bps 0 bps 0 0
ether19 ethernet 1500 0 bps 0 bps 0 0
ether2 ethernet 1500 25 kbps 1.68 k... 10 3
ether20 ethernet 1500 54.7 k... 8 5
ether21 ethernet 1500 9.3 kbps 2 4
ether22 ethernet 1500 4.76 k... 0
ether23 ethernet 1500 4.76 k... 1.26 k... 7 1
ether24 ethernet 1500 0 bps 0 bps 0 0
ether3 ethernet 1500 19.3 k... 2.14 k... 11 4
ether4 ethernet 1500 25 kbps 1.68 k... 10 3
ether5 ethernet 1500 18.2 k... 1.12 k... 9 2
ether6 ethernet 1500 25 kbps 1.68 k... 10 3
ether7
ether8
ether9
sfp-sfppl
sfp-sfppl
sfp-sfppl
sfp-sfppl
Settings
Disable
Ok
Cancel
Apply
Notes
Remove
Tools
Reprobe
Ack
Unack
Reboot
Reconnect


Link
General History
Graph Bit Rate
Export
Zoom:
24:00:00
30 Mbit/s
25 Mbit/s
20 Mbit/s
15 Mbit/s
10 Mbit/s
5 Mbit/s
0bit/s
Nov/20 06:00
Nov/20 12:00
Nov/20 18:00
sfp1 (2) @ m07-Firewall(CCR 1009) tx
sfp1 (2) @ m07-Firewall(CCR 1009) rx
Ok
Cancel
Apply
Notes
Remove


List Tree RouterOS Types Mac Mappings
Device Group Wireless Registration Simple Queue
Upgrade
Map: all
Name Status Version Architecture Board Upgrade Status Packages
m07-CRS226-1 ok 6.43.2 (s... mipsbe CRS226-24G-2S+ routeros-mipsbe
m07-CRS326-1 ok 6.43.4 (s... arm CRS326-24G-2S+ routeros-arm
m07-CRS326-2 ok 6.43.4 (s... arm CRS326-24G-2S+ routeros-arm
m07-CRS326-3 4 (s... arm CRS326-24G-2S+ routeros-arm
m07-CRS328-1 4 (s... arm CRS328-24P-4S+ routeros-arm
m07-Firewall(CC... 4 (s... tile CCR1009-8G-1S... ups, dude, routeros-tile
m07-RB1100AHx4 ntp, ups, dude, user-manager, routeros-arm
Device Settings
Show On Map
Tools
Settings
Upgrade
Force Upgrade
Reconnect
Ping
Traceroute
Snmpwalk
Terminal
Remote Connection
Torch
Bandwidth Test
Spectral Scan
Telnet
Web


Torch m07-Firewall(CCR 1009)
General
From: m07-Firewall(CCR 1009)
Interface: sfp-sfpplus1
Average: 00:00:10
10s
1s 2s 5s 10s 15s 30s 1m
Filter
Eth Protocol: any
Vlan ID: any
IP Protocol: any
Src Address: 0.0.0.0/0
Dst Address: 0.0.0.0/0
Port: any
Dscp:
Cpu:
Start
Stop
Close
Table Pie Bar
Eth Protocol Ip Protocol Vlan ID Src Address Src Port Dst Address Dst Port
0.0.0.0 - 175 K
120.106.167.39 - 4.29 K
192.168.88.104 - 143 K
192.168.88.201 - 8.62 K
other - 9.17 K
0.0.0.0 - 86.8 K
172.16.3.201 - 2.42 K
192.168.88.104 - 72.6 K
192.168.88.201 - 4.51 K
other - 5.56 K
0.0.0.0 - 88.4 K
120.106.167.39 - 2.1 K
192.168.88.104 - 70.3 K
192.168.88.201 - 4.11 K
other - 3.38 K
Total Bytes
Rx Bytes
Tx Bytes
0.0.0.0 - 241
120.106.167.39 - 6
172.16.3.201 - 5
192.168.88.104 - 202
other - 8
0.0.0.0 - 117
120.106.167.39 - 3
172.16.3.201 - 3
192.168.88.104 - 101
other - 5
0.0.0.0 - 124
120.106.167.39 - 3
172.16.3.201 - 2
192.168.88.104 - 101
other - 3

異常訊息通知



Telegram

利用 Telegram Bot 傳遞即時通知

安裝Telegram APP 並驗證啟用，與 @BotFather 對話 建立 Bot
/help
/newbot
取得 Bot 的Token 值 例如 548196238:AAFOrXUsakgZlRmsqsC_LWqfVVTgwS1U65A
點按啟用 Bot 並送一則訊息
利用下列URL 取得 Chat_id 例如 614626675
    https://api.telegram.org/bot[Bot 的Token]/getUpdates
傳遞訊息
https://api.telegram.org/bot[Bot 的Token]/sendMessage?chat_id=[Chat_id]&text='訊息內容' keep-result=no

參數 不留檔案 keep-result=no

[例如]
/tool fetch url="https://api.telegram.org/bot[Bot 的Token]/sendMessage\?chat_id=[Chat_id]&text=時間:[Time] 設備：[Device.Name] 狀態:[Service.Status] keep-result=no"

日誌大數據分析(縣網層)

splunk>enterprise 應用套件: 網路管理 | Administrator | 2 訊息 | 設定 | 活動 | 說明 | 尋找

搜尋 資料集 報告 警示 儀表板 | App 網路管理

[RuterBoard][Critical Error 訊息分析

編輯 匯出 ...

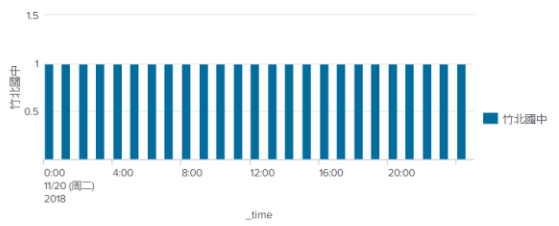
Select School: all

選擇查詢時間: Last 24 hours

竹北國中[RouterBoard][Cirtical_Alarm]

_time	Name	Description
2018/11/21 00:22:02	竹北國中	dhcp,critical,error dhcp alert on bridge1: discovered unknown dhcp server, mac 00:17:16:0E:4F:B4, ip 172.16.0.254
2018/11/20 23:21:39	竹北國中	dhcp,critical,error dhcp alert on bridge1: discovered unknown dhcp server, mac 00:17:16:0E:4F:B4, ip 172.16.0.254
2018/11/20 22:20:51	竹北國中	dhcp,critical,error dhcp alert on bridge1: discovered unknown dhcp server, mac 00:17:16:0E:4F:B4, ip 172.16.0.254
2018/11/20 21:20:14	竹北國中	dhcp,critical,error dhcp alert on bridge1: discovered unknown dhcp server, mac 00:17:16:0E:4F:B4, ip 172.16.0.254
2018/11/20 20:19:31	竹北國中	dhcp,critical,error dhcp alert on bridge1: discovered unknown dhcp server, mac 00:17:16:0E:4F:B4, ip 172.16.0.254

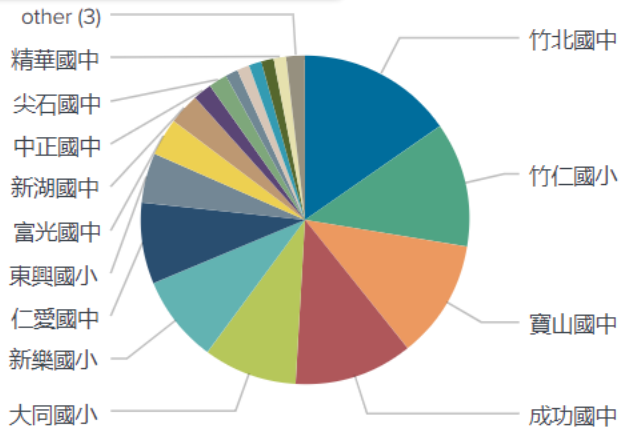
竹北國中[RouterBoard][Critical Error 時間分佈圖]



*[RouterBoard][Critical Error 統計表]

Name	Device_IP	count
竹北國中	163.19.13.254	25
竹仁國小	163.19.76.254	20
寶山國中	163.19.83.254	19
成功國中	163.19.93.254	19
大同國小	163.19.77.254	15
新樂國小	120.106.187.126	14
仁愛國中	163.19.14.254	13
東興國小	163.19.96.254	8

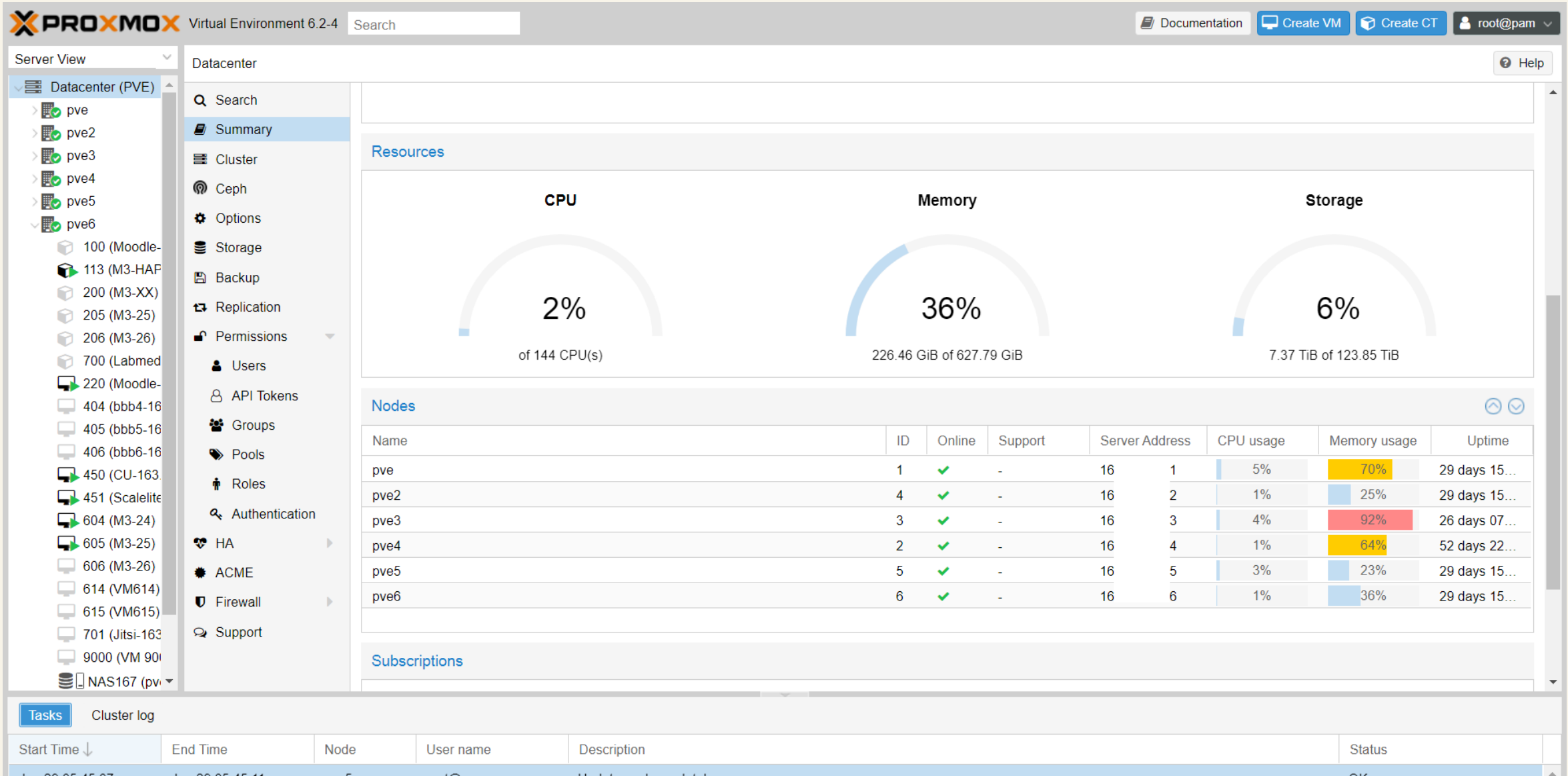
« 上一頁 1 2 3 下一頁 »




中華電信
起始號：3LK201T153002
結束號：3LK201T153990
數　量：100套 2020年03 專案
第054箱／共100箱 10000份
台灣大哥大
4G+
三合一
FAREASTONE

積極備援的解決方案

虛擬化方案：Proxmox



資管藝術

縱深防禦思維、共享夢想之路

Art-1

想掌握網路，先抓住IP

誰盜用IP?私接設備?

ARP(Static Bind)

Hotspot(Account,IP,MAC)

DHCP (Static Lease by MAC、Alert)

Art-2

行動辦公也要安全

誰的電腦不關機?

VPN(L2TP、Radius)

Firewall Rule(by Time Schedule)

Art-3

亂世用重典，多設警衛

電腦教室管理、公用區

NAT(IP 節約)

DNS(Cache)

Web Proxy(網站管制)

Firewall (L7 Rule 過濾不當應用)

Queue (流量管控)

Art-4

瑣事就自動化去跑

如何當一位聰明的網路管理人員?

Scheduler(排程執行Scripts)
WOL(節能、喚醒電腦)
異地備份(backup+ftp or email)
Logging(remote syslog)

Art-5

內賊難防、自動防範破窗

是誰在搗蛋?可不可以自動防範?

Loop Protect(迴路保護)
DHCP Snooping(防止非法DHCP)
Hotspot(上網就要帳號驗證)
Log(長期Log倉儲)

Art-6

號令天下，老闆兼工友

發生甚麼事?遊走內外網路

The Dude(+Syslog Service)

RoMON (Winbox by RoMON Agent)

ROS_command

SNMP

Art-7

一手掌握，On Time

第一手消息

訊息傳遞(+Telegram Bot)

Mikrotik APP

Art-X

同行致遠、大家一起共好

MikroTik (ROS、CP值高)
Open Source (Bigbluebutton、rocket.chat、Proxmox、LibreNMS....)
Community(社群同好....)

把世界帶進教室

新竹縣教育研究發展暨網路中心　辛文義