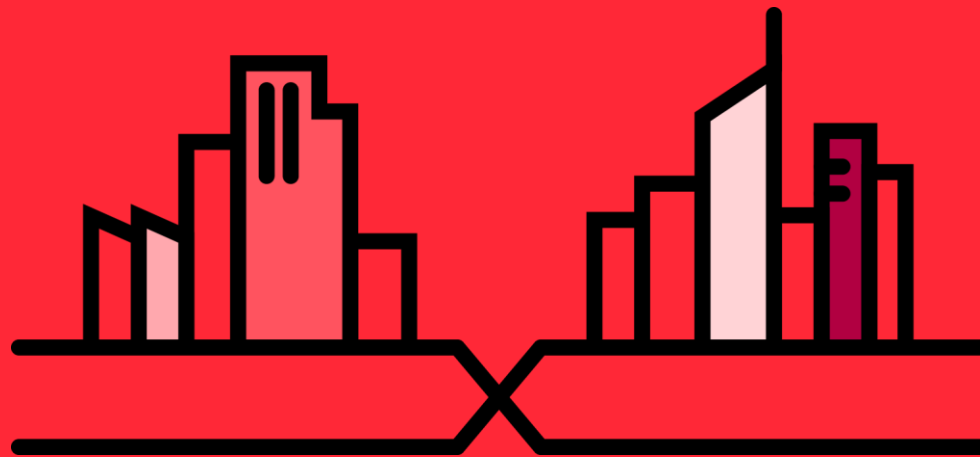


# ZYXEL Security 進階課程



# Outline

---

01

**ZyWALL Security**  
介紹&防護

---

02

功能介紹

---

03

**Security**  
**Services**

---

04

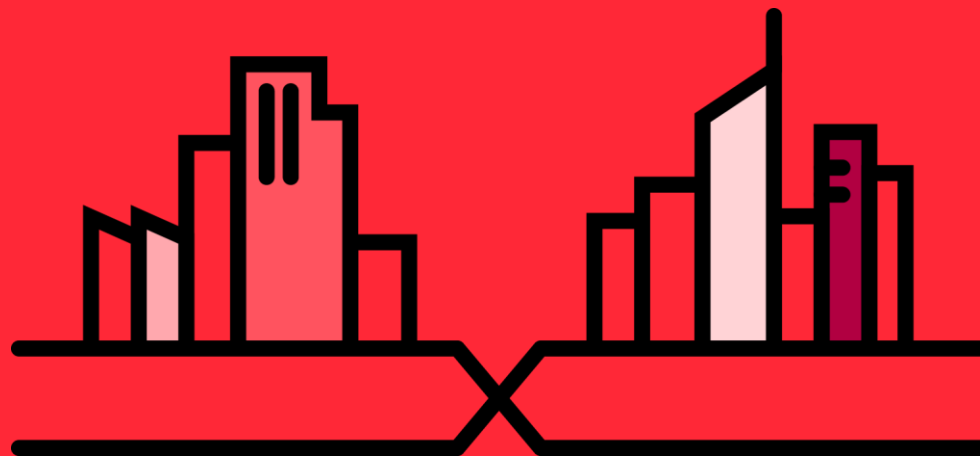
**SecuReporter**

---

05

**Appendix**

# ZYXEL Security 介紹 & 防護



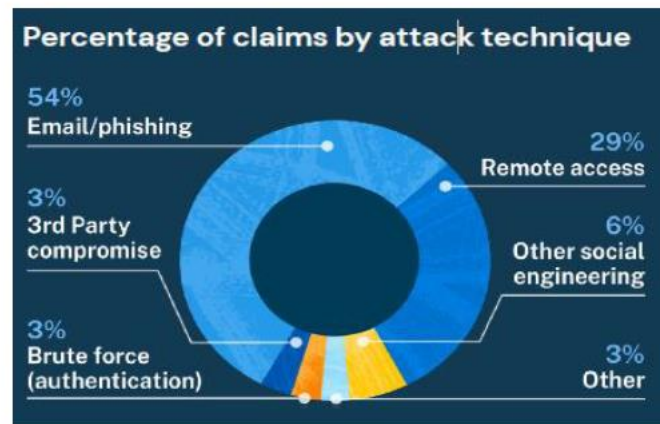
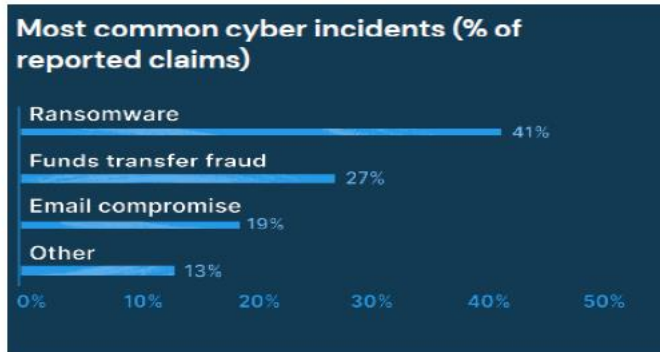
# 最新資訊安全威脅趨勢統計

## ● 資安事件分類

- 勒索軟體攻擊(41%)
- 資金移轉詐騙(27%)
- 電子郵件入侵(19%)

## ● 攻擊技術

- 郵件釣魚(54%)
- 遠端存取(29%)
- 除郵件外社交工程(6%)
- 第三方工具(3%)
- 暴力破解(3%)
- 其他(3%)



# 惡意程式入侵途徑及管道

入侵途徑及管道	說明
電子郵件	<ol style="list-style-type: none"><li>1. 電子郵件本身夾帶隱藏惡意程式的檔案，利用Office程式的漏洞，在收件者開啟後連帶安裝後門或木馬程式</li><li>2. 電子郵件附加仿冒知名網站的惡意連結</li></ol>
系統本身漏洞	對目標系統或網路之漏洞進行攻擊，進而取得控制權，常見方式包含：網芳、IIS、IE弱點攻擊等等
惡意網頁	駭客先攻陷某一網站，並在網頁上加入一些惡意程式碼，使瀏覽用戶不自覺被植入木馬程式。
網站注入攻擊	使用特殊字元，使網頁應用程式略過安全檢查，或輸入錯誤資料，得到錯誤訊息進而推敲資料庫的格式及內容
系統不當權限設定	防火牆規則不嚴謹、防毒軟體未更新，讓駭客利用掃描工具漸進式的獲得帳號密碼

# 惡意程式入侵途徑及管道-電子郵件釣魚

- 電子郵件釣魚手法層出不窮，最後目的多為營利性質，騙取金錢財物。從受害目標鎖定之精準程度，大致分為「亂槍打鳥型」釣魚郵件、「針對型」釣魚郵件
  - 亂槍打鳥型釣魚電郵：利用好康資訊誘使收信者點選連結或開啟附件，例如中獎通知或投資獲利機會。各種通知信件，例如快遞、送貨、銀行通知等，通常會騙取開啟信件附件。宣稱已取得密碼及駭入電腦，威脅將公開不堪的網站瀏覽記錄，並勒索高額比特幣
  - 針對型釣魚電郵：偽造成系統升級、帳號/信箱停用、容量擴充等通知信件，假造信件會附上該系統logo，以騙取信任，例如Yahoo、Google、Hinet，或銀行等logo

# 惡意程式入侵途徑及管道-電子郵件釣魚

智邦生活館 網路郵局

資料夾 (重整資料夾清單)

收件夾  
草稿  
寄信備份  
回收筒

雙主機  
即時備援  
24小時  
真人客服

主旨: 您的包裹無法在2021年03月02日送達 | Fwd: Your package could not be delivered on 02.03.2021 ID51009[RAND][RAND]  
寄件者: Chungwa Post | 中華郵政  
日期: (五), 3月 5日, 2021 7:20 am  
收件者: charny@vot.url.com.tw  
重要性: 普通  
環境設定: [顯示完整標頭](#) | [顯示友善列印模式](#) | [讀取郵件](#) | [新增至通訊錄](#) | [加入黑\(白\)名單](#)

 中華郵政全球資訊網  
Chungwa Post Co., Ltd.

Hello ,

**Last Reminder:** This Email informs you that your shipment is still pending.

Your package could not be delivered on **02.03.2021** because no customs duty was paid ( **369 NT Dollars**)

**Merchant** : Chungwa Post  
**Order Number** : 00275029  
**Purchase Amount** : 369 NT Dollars  
**Delivery scheduled between** : 03.03.2021 - 04.03.2021

- To confirm the shipment of your package [Click here](#).

You will receive an email or SMS when you arrive in your home address. You will have 8 days, from the date of availability, to withdraw the package. Upon withdrawal, you will be asked for ID.

- For more services, find the follow-up of your shipment by [Clicking here](#).

Thank you for your trust,

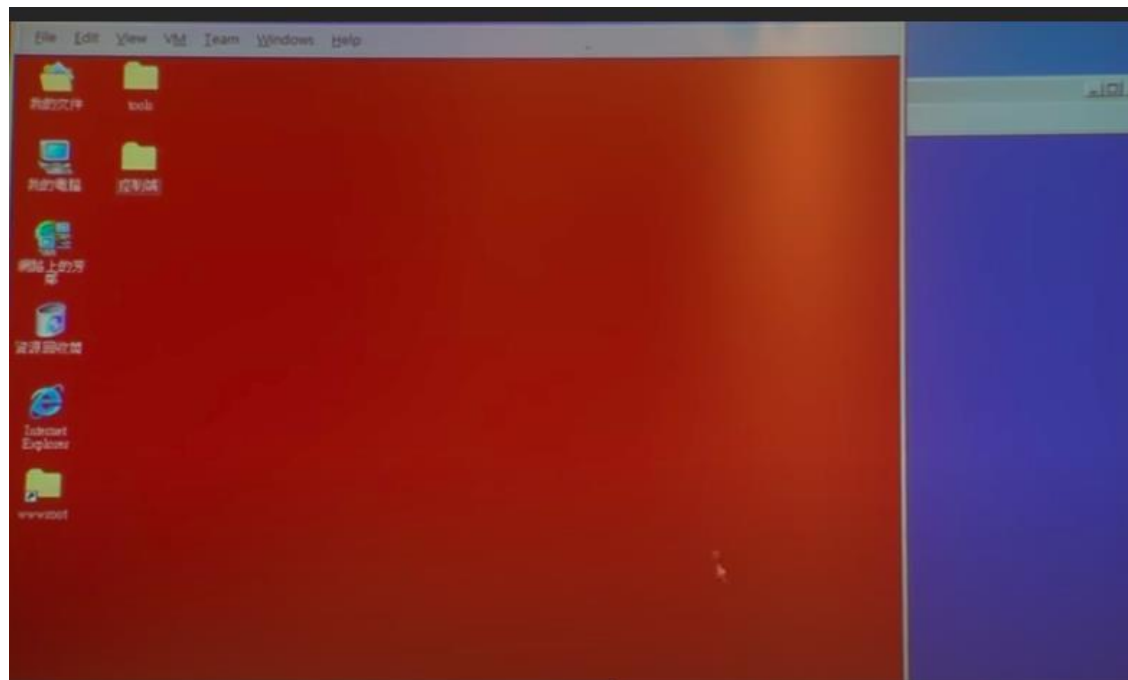
Sincerely,  
Your **Chungwa Post** customer service.

# 惡意程式入侵途徑及管道-電子郵件釣魚





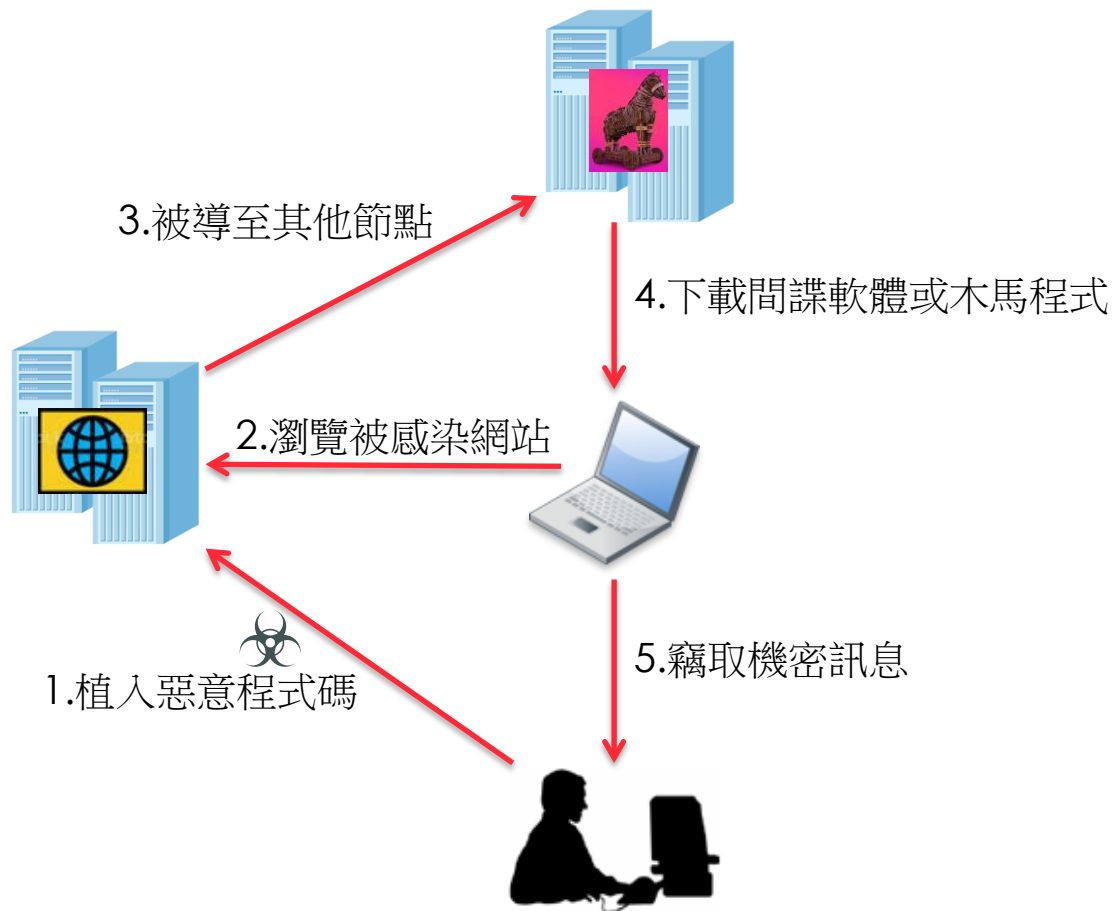
# 《駭客攻擊手法模擬-電子郵件釣魚》 原來駭客就是這樣跟我一起上班的!!



<https://www.youtube.com/watch?v=8DqE21SBHI0&t=5s>



# 惡意程式入侵途徑及管道-惡意網頁



# 惡意程式入侵途徑及管道-惡意網頁

ETtoday新聞雲 > 生活

2014年01月06日 23:55

生活

生活焦點

教育

氣象

健康

藝文 / 運勢 / 交通

雅虎廣告藏病毒！點擊就載惡意程式 每小時  
3萬人中鏢

【清倉】寵物雲毛毛商城換季5折起

0

讚

The screenshot shows the Yahoo! UK homepage. At the top, there is a navigation bar with links for Home, Mail, News, Sport, Finance, Lifestyle, omg!, Weather, Answers, Flickr, and More. Below this is the Yahoo! UK logo and a search bar. On the left side, there is a vertical menu with icons for Mail, News, Sport, Finance, Lifestyle, omg!, Cars, and Movies. The main content area features a large article titled "City's worst drivers shamed in online gallery" with a sub-headline "A social media page has been highlighting some of the most disastrous parking attempts in Edinburgh. 'Hardcore idiots'". Below the article are several smaller thumbnails with titles like "Student's kiss from Cheryl", "Bad parkers shamed online", "Why United must sack Moyes", "United crash out of FA Cup", and "Why Shia didn't shower". On the right side, there is a list of links for "Lost and found", "Debt advice", and "Prison incident".

# 惡意程式入侵途徑及管道-系統本身的漏洞

- 零時差漏洞：是指軟體、韌體或硬體設計當中已被公開揭露但廠商卻仍未修補的缺失、弱點或錯誤。
- 零時差攻擊：就是利用尚未修補的漏洞進行攻擊

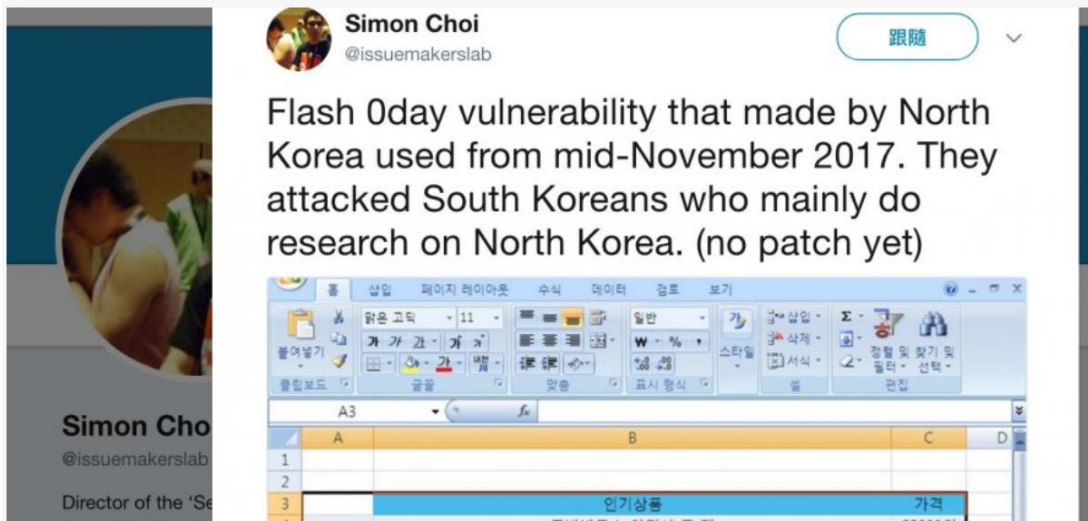
南韓KS-CERT警告，駭客利用Flash零時差漏洞進行攻擊

文/ 陳曉利 | 2018-02-02 發表

讚 6.4 萬

按讚加入iThome粉絲團

讚 89



南韓資安公司Hauri的研究人員Simon Choi在推特上直指北韓利用Flash零時差漏洞對南韓展開攻擊。

# 惡意程式入侵途徑及管道- SQL Injection

- SQL Injection 的本質就是把「輸入的惡意資料」變成「程式的一部分」意思是駭客可在輸入資料時，用一些奇怪的方式（惡意字串）竄改 SQL 語法，以偷取、假冒別人資料或刪除資料庫，

[ 正常輸入 ]

- 帳號：123
- 密碼：456

```
// 接收輸入的 SQL
```

```
SELECT * FROM users WHERE user='123' AND pwd='456';
```

[ SQL Injection ]

- 帳號：' or 1=1 -
- 密碼：(甚至不用輸入)

```
// 接收輸入的 SQL
```

```
SELECT * FROM users HWERE user=' ' or 1=1 --' AND pwd = ''; // => 永遠成立
```

# 入侵案例探討-中油勒索案(2020.5)

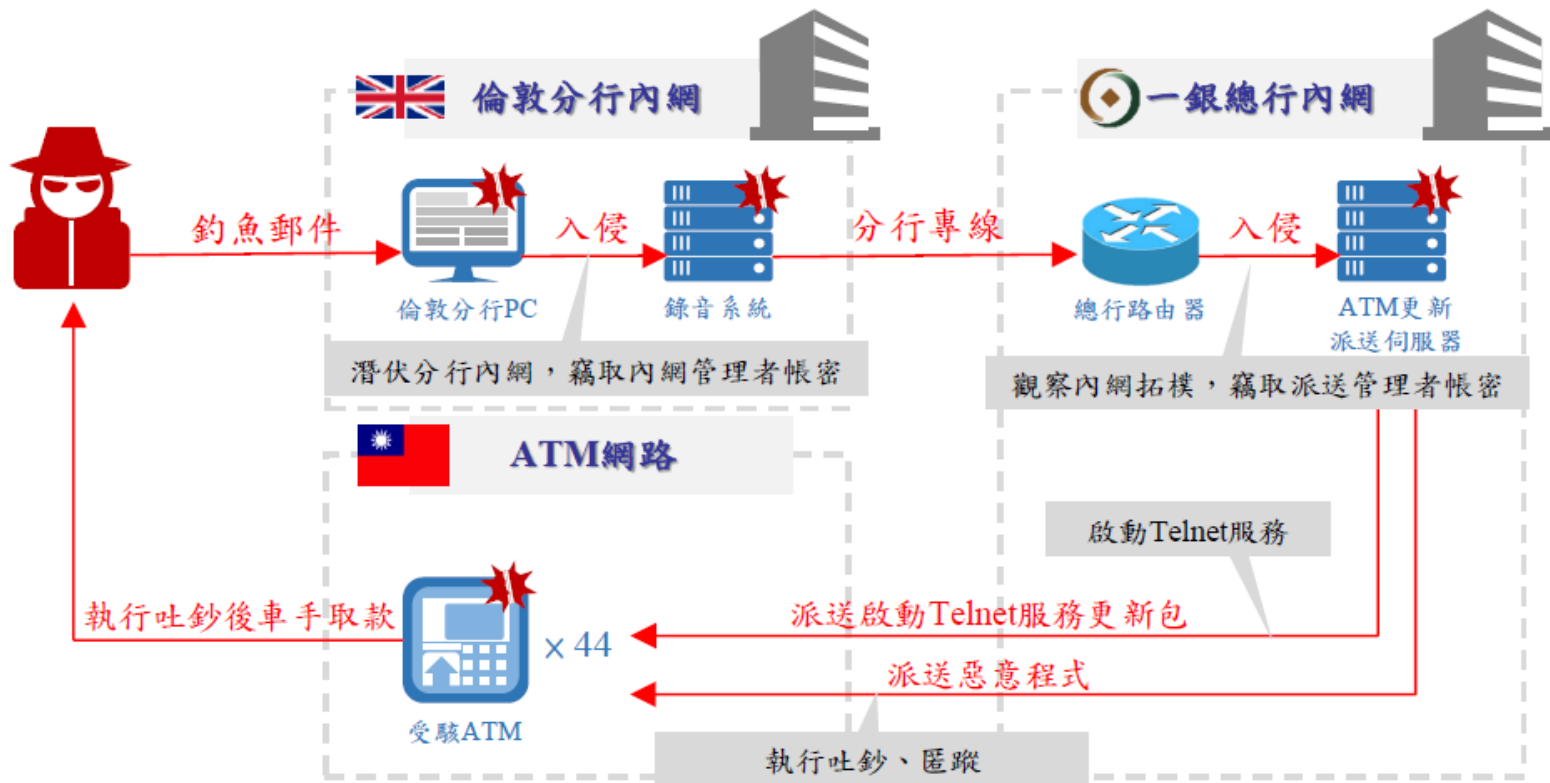
臺灣中油公司在5月4日遭到勒索軟體威脅，但中油公司主要油品生產和製造系統並沒有受到勒索軟體的危害，因有部分資料庫和電腦主機受駭，中油立即透過斷網進行災害控管，受到勒索軟體影響的包括捷利卡、中油Pay系統，但加油站的油品銷售系統不受影響，仍可以使用現金和信用卡進行交易。



## 中油感染病毒 全新特殊設計

據透露，中油感染的勒索軟體具高度目標性，是全新特殊設計的病毒，現有病毒資料庫比對無資料，且僅針對中油員工帳號攻擊，疑為較高層級電腦遭帶毒隨身碟入侵。台塑感染的目前看來並非勒索病毒，與中油具加密電腦檔案的特徵不同，是否為同一攻擊來源，待進一步分析。

# 入侵案例探討-一銀盜領案(2016.7)



# 什麼是APT？

- APT ( Advanced Persistent Threat ) 進階漸進式威脅
  - 進階：綜合各種技術、非技術手段 ( 包括釣魚、木馬、殭屍、注入、DDoS、滲透、0day.....等等 ) ，裏應外合
  - 漸進：極強的隱藏能力，當發現漏洞時，並不會立刻發動攻擊，而是非常有耐心地藉由這個漏洞滲透目標組織，潛伏在裡面伺機而動
  - 威脅：竊取甚至大量破壞核心數據



# 典型的APT過程



社交分析



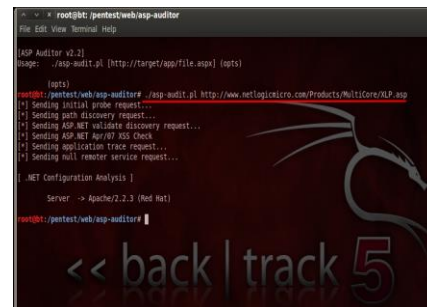
網路釣魚



0day攻擊



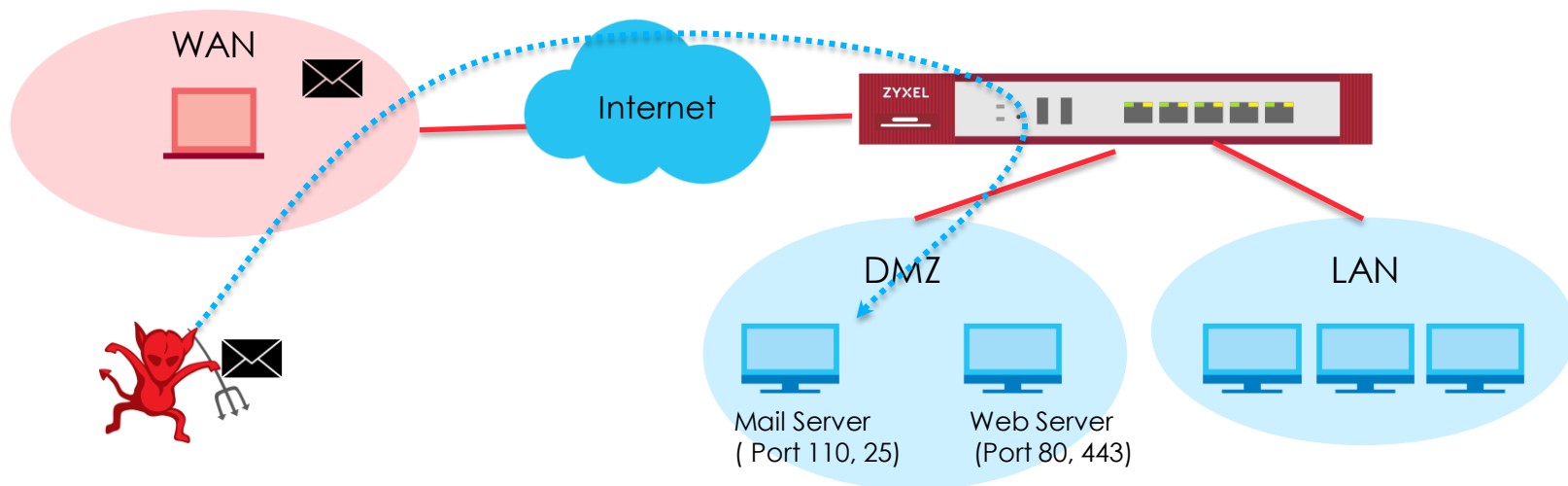
數據竊取



入侵滲透 © 2016 ZYXEL | 17

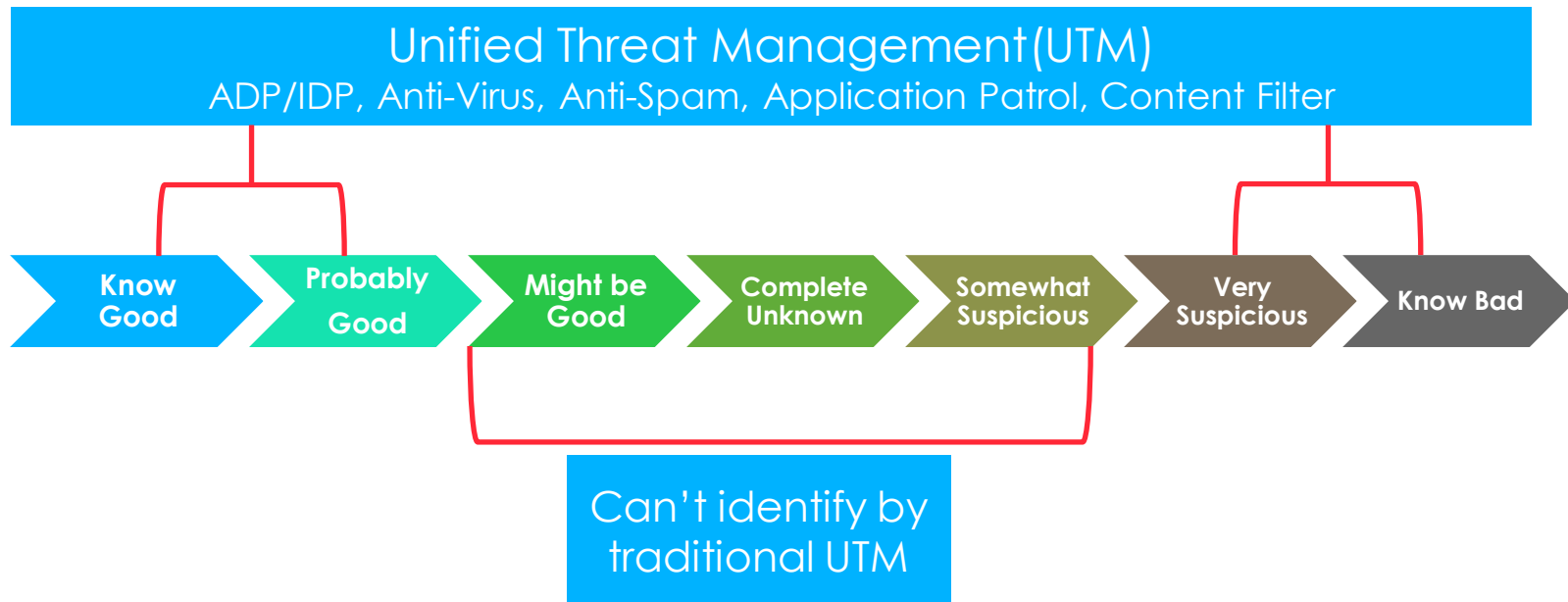
# 傳統 Firewall 提供的-Policy 防護限制

- 限制可用服務 (Security Policy)
  - 非允許服務、IP 無法存取
- 但如果是合法的途徑呢？



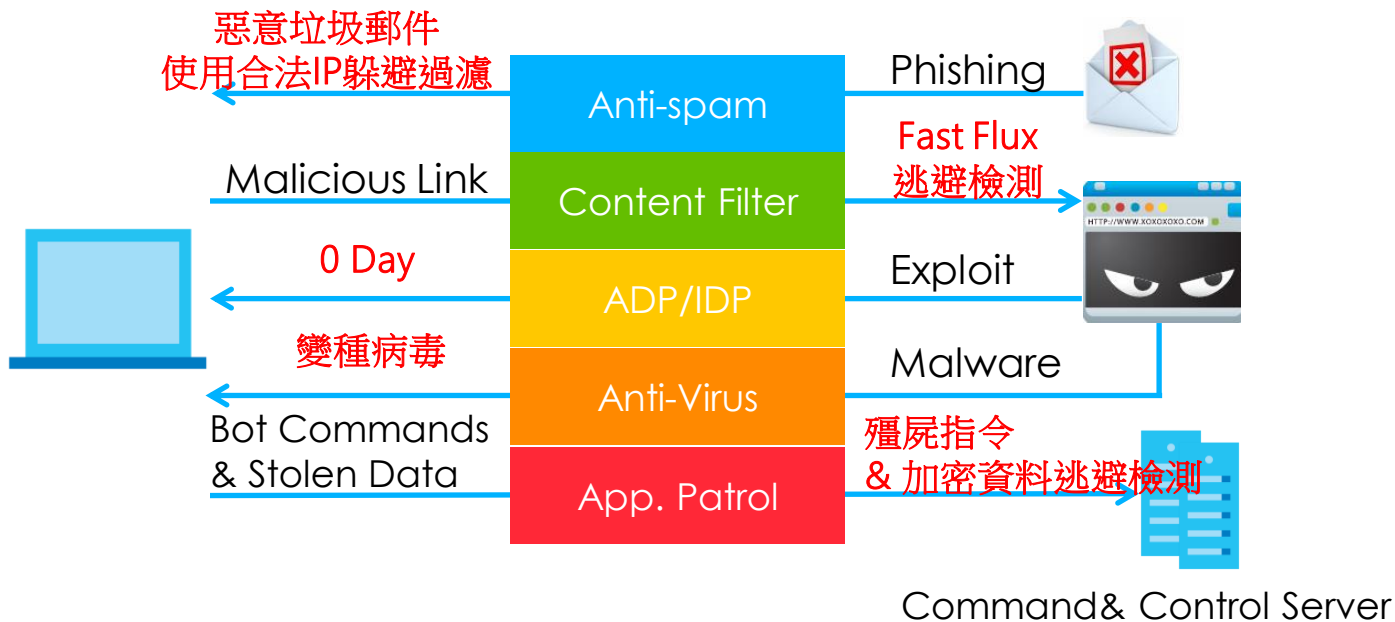
# 傳統 Firewall 提供的-UTM 防護限制

- 傳統UTM 可以阻擋已知的攻擊，但是無法阻擋**未知的攻擊**



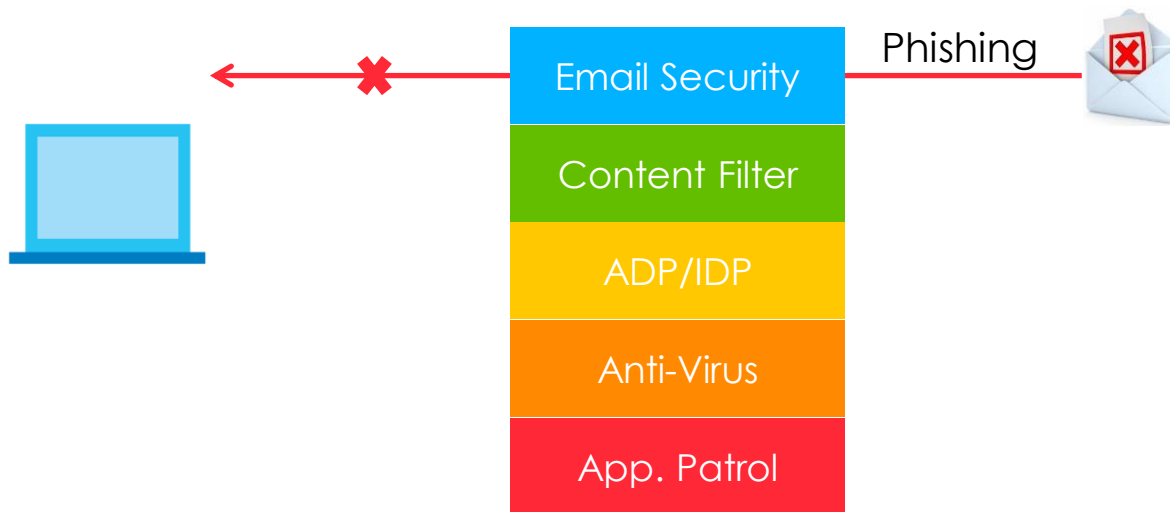
# 傳統 Firewall 提供的 UTM 防護限制

- 傳統UTM的防禦風險



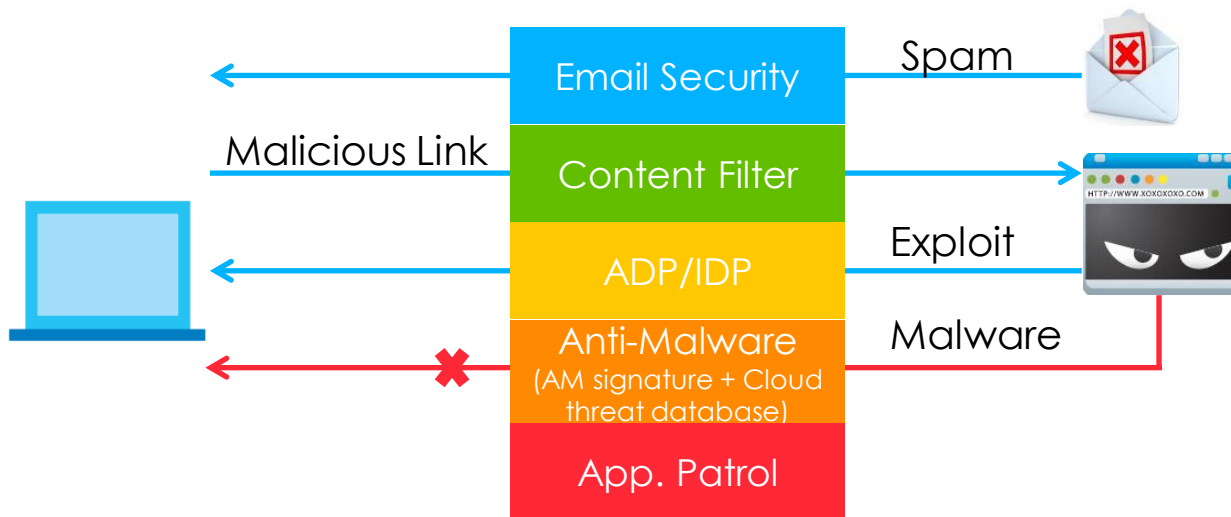
# 如何保護使用者免於進階式威脅？

- Email Security with anti-phishing enhancement can detect phishing attacks targeting users



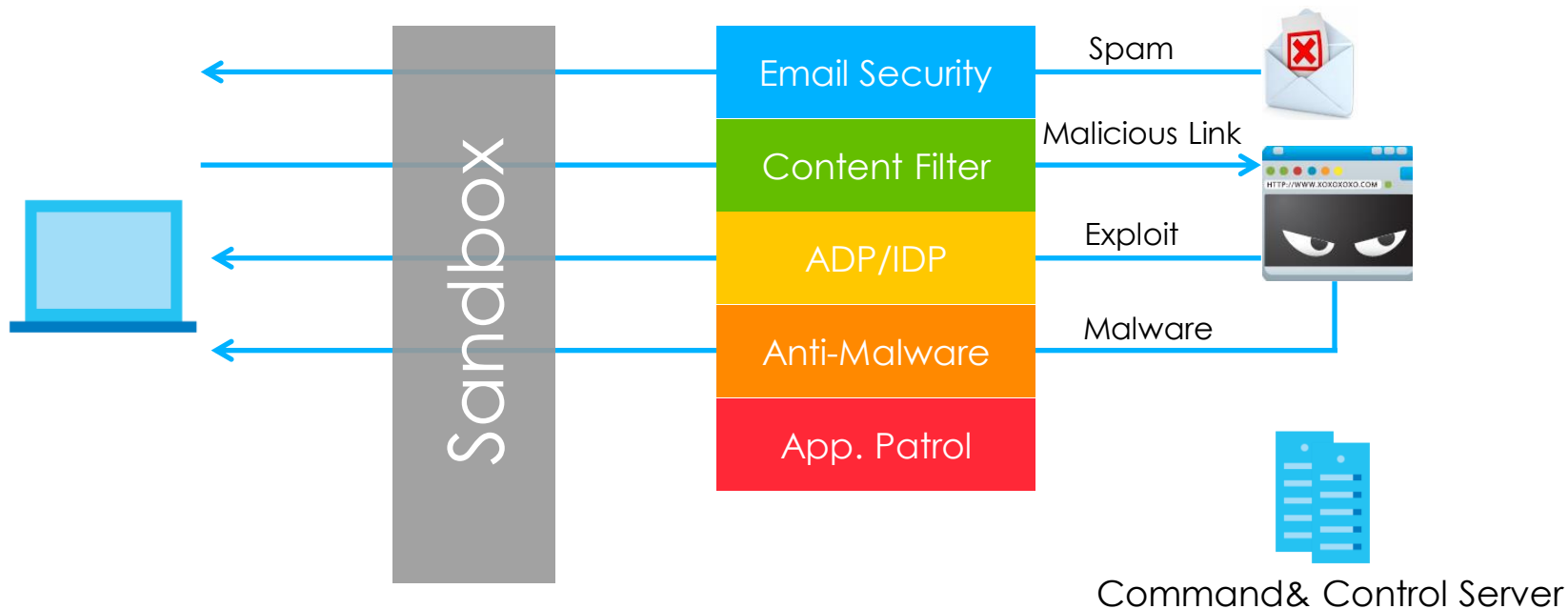
# 如何保護使用者免於進階式威脅？

- Anti-Malware with multiple database environments can fully protect your network



# 如何保護使用者免於進階式威脅？

- Sandbox performs deeper inspection to detect new or evasive threat designed to hide from traditional prevention measures



# Zywall ATP/USG Flex/VPN 安全服務一覽

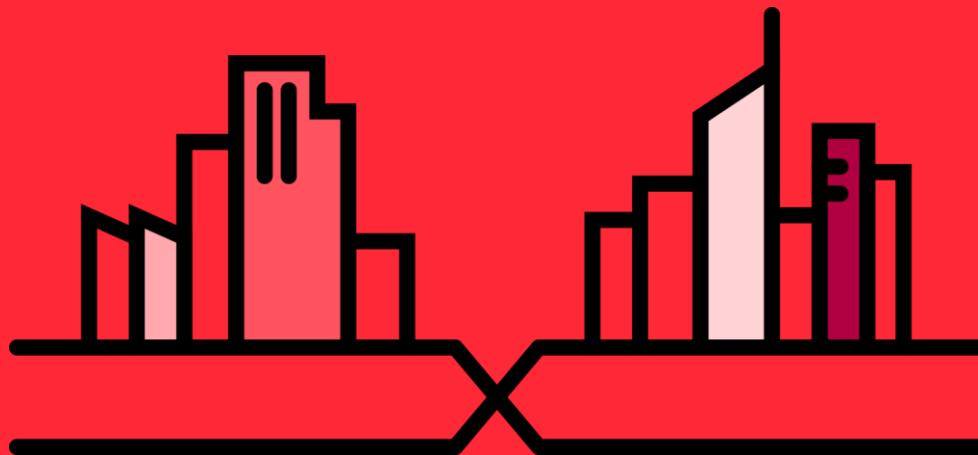
	Features	ZyWALL VPN	ZyWALL USG Flex	ZyWALL ATP	
Security Service	Sandboxing 沙箱			✓	
	Content Filter 內容過濾	✓	✓	✓	
	App Patrol 應用程式巡查		✓	✓	
	Anti-Malware (Anti-Virus)	Anti-Malware Signature		✓	✓
		Cloud Threat Database		✓	✓
	IDP 入侵偵測與防護		✓	✓	
	Email Security (Anti-Spam)	Anti-Spam		✓	✓
	SSL Inspection		✓	✓	✓
	SecuReporter		✓	✓	✓



# 標準資通安全系統建置與持續防禦機制建議方案

- 安全網路架構
  - VLAN, Switch ACL, IP Security, Firewall Zone/ACL, VPN ... 等
- 多層次防禦軟、硬體
  - UTM、ATP Sandbox 進階安全防護 Gateway ... 等
- 終端設備防毒
  - 防毒軟體
- 儲體加密與備份
  - 定時資料 snapshot/backup, 異地備份.. 等
- 資通安全設定檢測
  - 關閉不必要 open port, 帳號、限縮帳戶權限... 等 (可參考 GCB 標準或透過弱點掃描軟體 ex: Nessus 做全面性的檢測)
- 持續系統監控
  - 網路管理、Report 系統... 等網路、系統活動監測
- 立即反應與補強
  - Firmware update、system security patch... 等弱點修補

# 功能介紹



ZYXEL

Your Networking Ally

# 基本配置

# ZYXEL 次世代防火牆

- Online Demo 連結
  - <https://atp500demo.zyxel.com/>
  - <https://flex500.zyxel.com/>

Note: Limited Administrator

# Outline

---

01  
裝置管理

02  
GUI Overview

# 裝置管理



# Agenda

---

01  
總覽

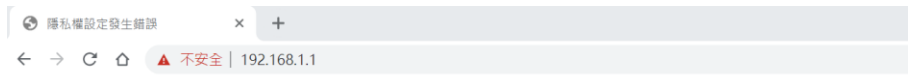
02  
註冊

03  
指令操作頁面

# 總覽(1/3)

## • Web 設定

- Step 1: 開啟瀏覽器, 輸入 URL **https://192.168.1.1**
- Step 2: ZyWALL/USG/VPN/ATP 會跳出告警訊息, 請點選 "繼續前往網站"



你的連線不是私人連線

攻擊者可能會試圖從 **192.168.1.1** 竊取你的資訊 (例如密碼、郵件或信用卡資料)。 [瞭解詳情](#)

NET::ERR\_CERT\_COMMON\_NAME\_INVALID

💡 要獲得 Chrome 最高等級的安全防護，請啟用強化防護功能

隱藏詳細資料

返回安全性瀏覽

這個伺服器無法證明所屬網域為 **192.168.1.1**；其安全性憑證未指定主體別名。這可能是因為設定錯誤，或是有攻擊者攔截你的連線所致。

[繼續前往 192.168.1.1 網站 \(不安全\)](#)

因為 HTTPS 連結會檢查設備本身的憑證，設備本身的憑證為 self-signed 故會出現告警，並非真的有安全問題



# 總覽(2/3)

- **Web 設定**

- Step 3: 預設帳號 **admin** ，密碼 **1234**

**ZYXEL**

**VPN100**

Enter User Name/Password and click to login.

**Login**

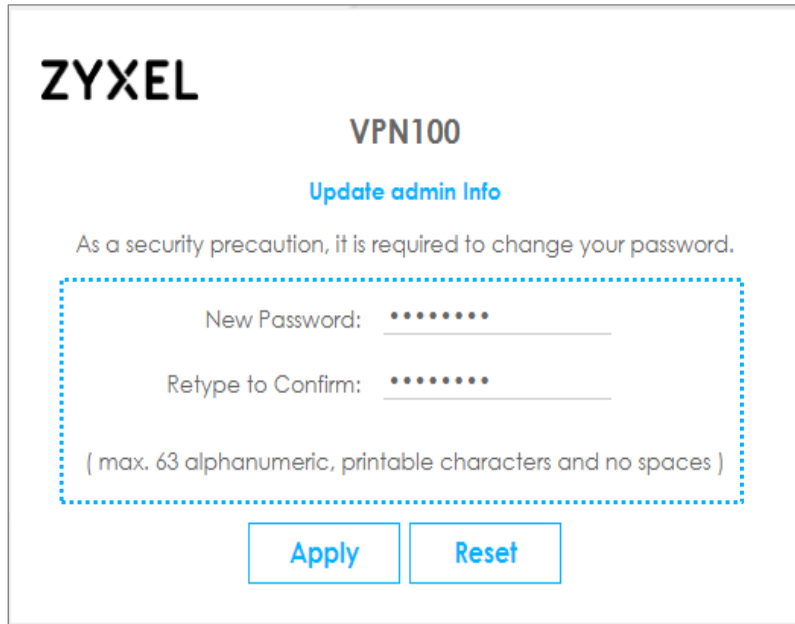
**Note:**

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.
5. Turn off Compatibility View settings in IE10 is recommended, or upgrade to IE11 for better user experience.

# 總覽 (3/3)

- **Web 設定**

- Step 4: 第一次登入 ZyWALL/USG/VPN/ATP, 設備會要求輸入新的密碼，更改後 **Apply** 即可.



**ZYXEL**

**VPN100**

[Update admin Info](#)

As a security precaution, it is required to change your password.

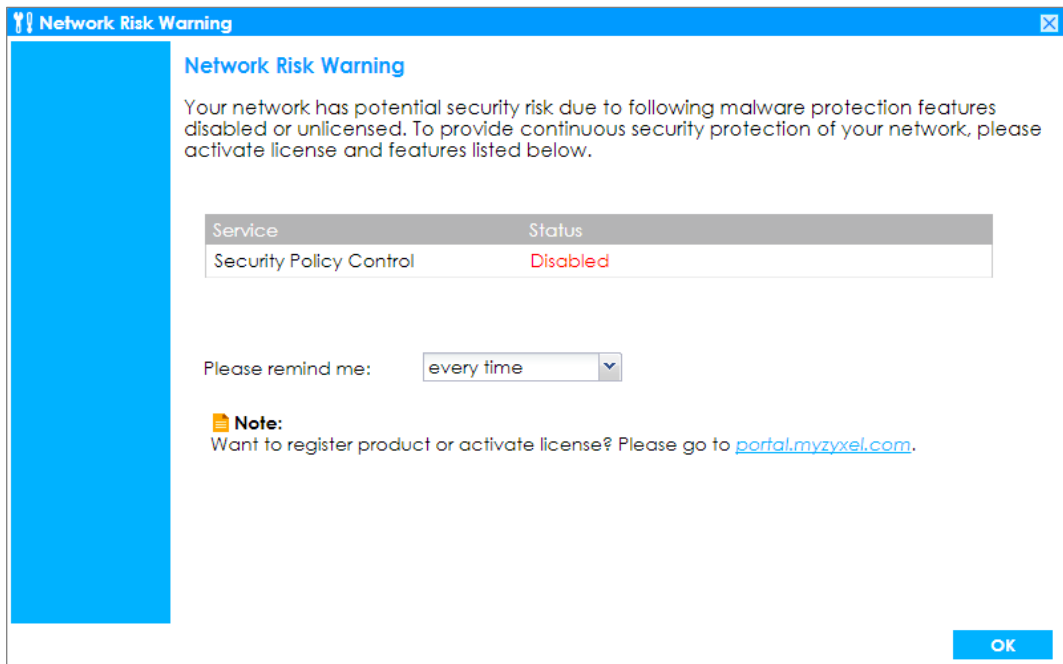
New Password:

Retype to Confirm:

( max. 63 alphanumeric, printable characters and no spaces )

[Apply](#) [Reset](#)

# Network Risk Warning Screen

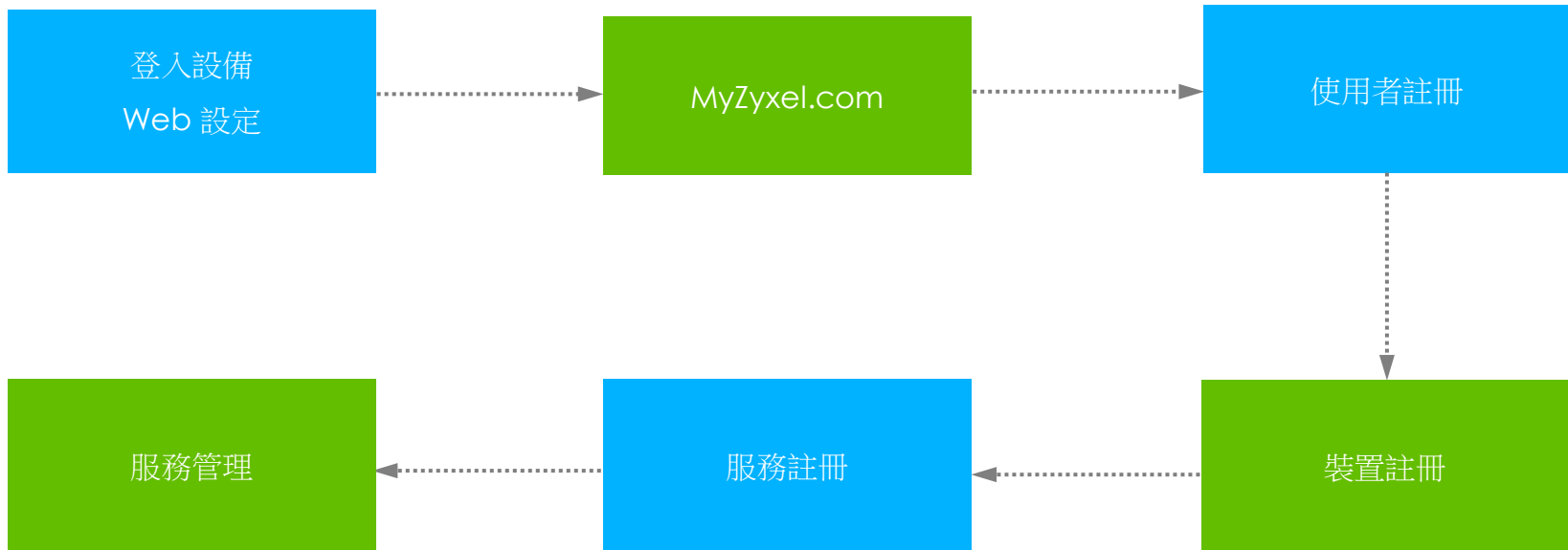


\* 如果登入後有新韌體更新的提醒，建議應參考 **release** 資訊並做更新

# 註冊

- 到 **myZyxel.com** 註冊你的 **ZyWALL/USG/VPN/ATP** 並啟用服務，例如：內容過濾等服務
- 請務必把設備註冊到 **MyZyxel.com**
- 註冊後才能獲得以下資訊：
  - 1.最新韌體更新
  - 2.服務更新
  - 3.最新資安資訊

# 註冊流程



操作影片：<https://www.youtube.com/watch?v=CyYbIU2yNc>

# Web 管理建議

- 螢幕解析度：**1024\*768**
- 支援瀏覽器（建議）
  - IE 8~10 或以上版本
  - Google Chrome v31 或以上版本
  - Firefox v25 或以上版本
- 啟用瀏覽器 **JavaScript** 及 **Cookie** 設定（預設為開啟）。
- 允許彈出視窗(**Pop-out Window**)

# 主畫面 (Dashboard)

- 管理 ZyWALL/USG/VPN/ATP: Web 設定

The screenshot displays the ZyXEL VPN100 Web Management Dashboard. The top navigation bar includes links for Logout, Help, About, Site Map, Object Reference, and CLI. The main content area is divided into several sections:

- General** (selected) and **VPN** tabs.
- System Health**: CPU Usage (7%), Memory Usage (18%), Flash Usage (9%), and USB Storage Usage (0/0 MB).
- Active Sessions**: 6/800000.
- DHCP Table**: 1 Host(s).
- Device HA**: 0 Switch Counter.
- Number of Login Users**: 1.
- Current Login User**: admin unlimited / 00:29:58.
- VPN Status**: 0.
- SSL VPN Status**: 0/10.
- Virtual Device**: A diagram of the device showing ports (USB, WAN1, WAN2, LAN/DMZ) and a highlighted Port 4.
- Device Information**: System Name (vpn100), Serial Number (S142L44290052), MAC Address Range (B8:EC:A3:12:C1:29 ~ B8:EC:A3:12:C1:2F), and Firmware Version (V4.30(A8FV.0) / 2017-11-23 21:16:34).
- System Status**: Boot Status (System default configuration), System Uptime (01:02:18), and Current Date/Time (2018-01-02 / 17:16:53 UTC+00:00).
- Tx/Rx Statistics**: A line graph showing traffic in Mbps over time (16:15 to 17:15). Port Selection is set to P1.
- The Latest Logs**: A table of system events.

#	Time	Priority	Category	Message	Source	Destination
1	2018-01-02 16:15:16	alert	system	Device starts up.		
2	2018-01-02 16:15:10	alert	system	Port 4 is up!		
3	2018-01-02 16:14:54	alert	policy-route	Trunk SYSTEM_DEFAULT_WAN_TRUNK deac		
4	2018-01-02 16:14:54	alert	file-manage	WARNING: #configure terminal account		
5	2018-01-02 16:14:54	alert	file-manage	WARNING: #configure terminal account		

# CLI 存取

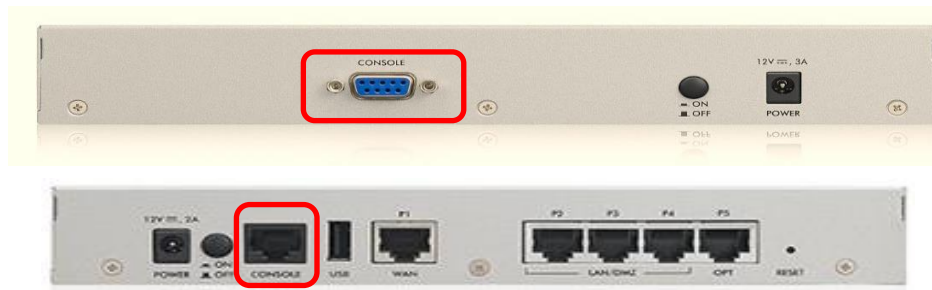
- Console Port
- SSH
- Telnet
- Web Console



# Console Port

- 可透過 **Console Port** 管理設備或進行一些修復動作（例如：忘記密碼）
- 僅能以指令方式進行操作
- 預設參數
  - Speed: 115,200 bps
  - Data Bits: 8
  - Parity: None
  - Stop Bit: 1
  - Flow Control: Off

\* 電腦須具備 Com Port 或 USB to RS-232 Cable  
\* 終端機軟體，putty、teraterm ...等



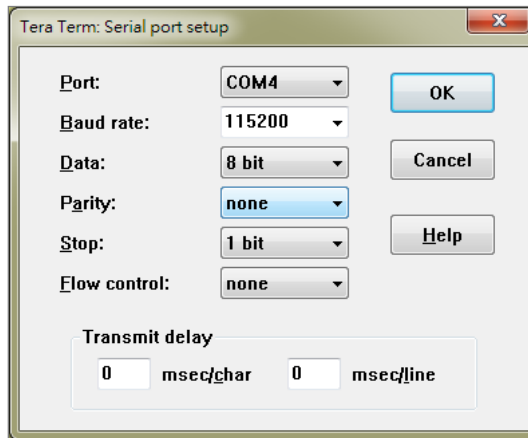
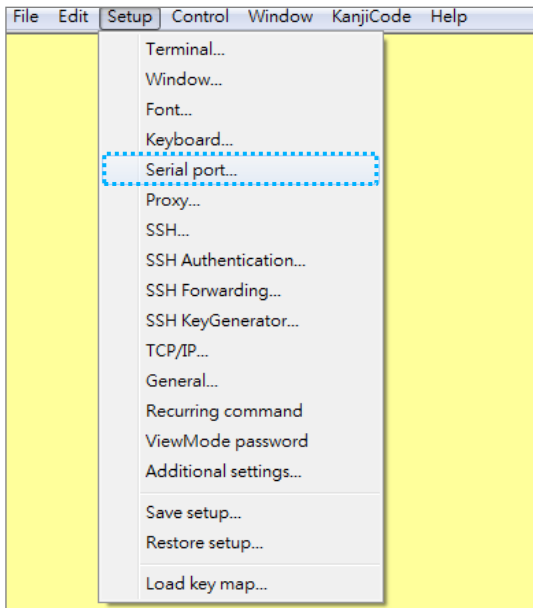
USB to  
RS-232 DB-9



RS-45 to  
DB-9

# Tera Term

- TeraTerm Terminal 設定



# Initialization Information

U-Boot 2013.07 (Development build, svnversion: u-boot:501M, exec:)-svn501 (Build time: Nov 21 2016 - 14:23:05)

BootModule Version: V1.16 | Nov 21 2016 14:23:05  
DRAM: Size = 2048 Mbytes

Press any key to enter debug mode within 3 seconds.

.....  
Allocating memory for ELF segment: addr: 0xfffffff80800000 (adjusted to: 0x800000), size 0xc69a20  
Start to check file system...  
/dev/mmcblk0p6: 495/61440 files (0.4% non-contiguous), 74161/245760 blocks  
/dev/mmcblk0p7: 168/131072 files (7.1% non-contiguous), 27243/524288 blocks  
Done  
Kernel Version: V3.10.87 | 2017-11-23 06:21:30  
ZLD Version: V4.30(ABFV.0) | 2017-11-23 21:16:36

INIT: version 2.86 booting  
Initializing Debug Account Authentication Seed (DAAS)... done.  
Setting the System Clock using the Hardware Clock as reference...System Clock set. Local time: Fri Jan 5 23:03:45 UTC 2018

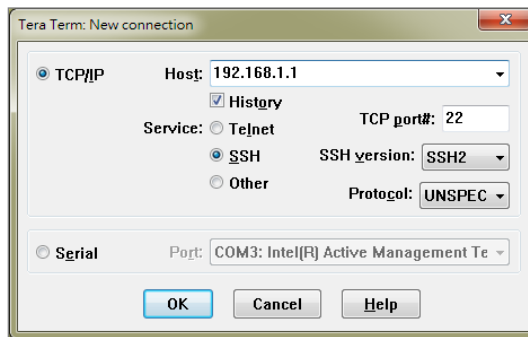
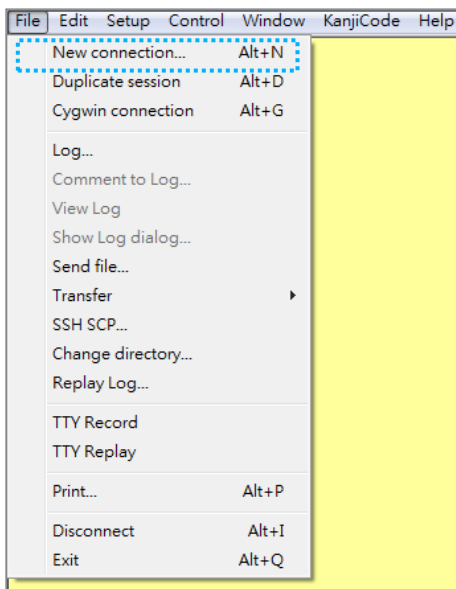
INIT: Entering runlevel: 3  
Insmod ZYKLOG Module. Starting zylog daemon: zylogd zylog starts.  
Starting syslog-ng secu-reporter.  
Starting ZLD Wrapper Daemon....  
Starting uam daemon.  
Starting myzyxel daemon.  
Starting periodic command scheduler: cron.  
Start ZyWALL system daemon....  
Starting link\_updown daemon.  
[zy\_adp]load ZyADP Ver1.0.0 OK  
.....Applying system configuration file, please wait...  
.....ZyWALL system is configured successfully with startup-config.conf

Welcome to VPN100

Username:

# SSH (1/2)

- 以 SSH 管理 ZyWALL/USG/VPN/ATP



\*無法如 Console Port 做一些修復動作

# SSH (2/2)

- 設定 > 系統 > SSH

SSH

設定

- BWM
- Web 認證
- + 安全性策略
- + 安全服務
- + 物件
- + Cloud CNM
- 系統
- 主機名稱
- USB 儲存
- 日期/時間
- Console 速度
- DNS
- WWW
- **SSH**
- TELNET
- FTP

一般設定

啟用

伺服器埠: 22

伺服器憑證: default

服務控制

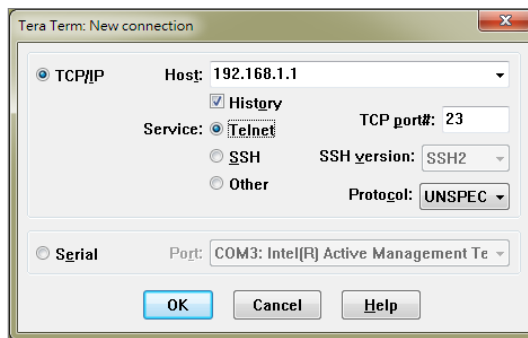
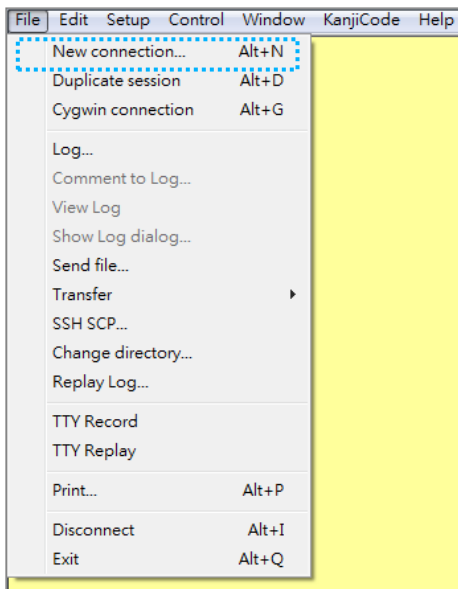
+ 新增   編輯   刪除   移動

#	區域	位址	動作
-	ALL	ALL	Accept

第 1 頁, 共 1 頁   每頁顯示 50 行   顯示 1 - 1 之 1

# Telnet (1/2)

- 以 Telnet 管理 ZyWALL/USG/VPN/ATP



\*無法如 Console Port 做一些修復動作

# Telnet (2/2)

- 設定 > 系統 > TELNET

TELNET

設定

- BWM
- Web 認證
- + 安全性策略
- + 安全服務
- + 物件
- + Cloud CNM
- 系統
- 主機名稱
- USB 儲存
- 日期/時間
- Console 速度
- DNS
- WWW
- SSH
- **TELNET**
- FTP

一般設定

啟用

伺服器埠:

服務控制

+ 新增   編輯   移除   移動

#	區域	位址	動作
-	ALL	ALL	Accept

第 1 頁, 共 1 頁   每頁顯示 50 行   顯示 1 - 1 之 1

# Web Console (1/2)

- 在 Web 界面使用 CLI

The screenshot displays the Zyxel ATP200 Web Console interface. The top navigation bar includes a '一般' (General) tab and a '進階威脅防護' (Advanced Threat Protection) tab. On the right side of the navigation bar, there is a row of icons, with the first icon (representing a terminal or CLI) highlighted by a dashed blue circle and a blue arrow pointing to a terminal window.

The terminal window, titled 'web-console-login (atp500)', shows the following content:

```
web-console-login (atp500) x +
Not secure | https://10.214.48.31/webconsole/
Username: admin
Password:
Router# show interface all
```

No.	Name	Status	IP Address	Mask	IP Assignment
1	ge1	Down	0.0.0.0	0.0.0.0	DHCP client
2	ge2	100M/Full	10.214.48.31	255.255.255.0	DHCP client
3	ge3	Down	0.0.0.0	0.0.0.0	DHCP client
4	ge4	Down	192.168.1.1	255.255.255.0	Static
5	ge5	Down	192.168.2.1	255.255.255.0	Static
6	ge6	Down	192.168.3.1	255.255.255.0	Static
7	ge7	Down	0.0.0.0	0.0.0.0	Static
8	ge8	Down	0.0.0.0	0.0.0.0	Static

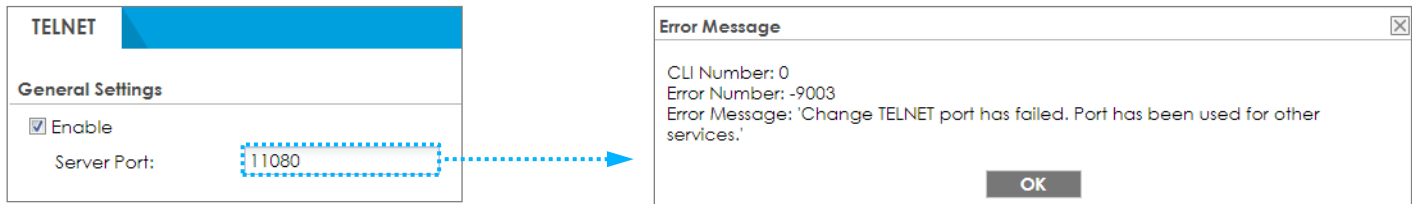
```
Router#
```

The interface also shows system information on the left, including CPU usage (2%), Memory usage (43%), Flash usage (13%), and USB storage usage (0/0 MB). The system name is 'atp200' and the serial number is 'S192L11200120'. The MAC address range is 'BC:CF:4F:E8:44 ~ BC:C...'. The firmware version is 'V4.62(ABFW.0) / 2021-01-19 11:08:39'. The connection port is set to 'P2'.



# Web Console (2/2)

- 直接在 **Web** 設定頁面使用（本機未安裝 **SSH, Telnet** 等用戶端軟體下的替代方案）
- **Debug messages** 不會在此顯示
- 使用 **port 11080** 故此 **port** 號為保留 **port**
  - Web GUI setting



```
Router(config)# ip telnet server port 11080
% Change TELNET port has failed. Port has been used for other services.
retval = -9003
ERROR: Change TELNET port has failed. Port has been used for other services.
```

# 回復出廠預設值- 方式 1

1. 確認 **SYS** 燈恆亮綠燈
2. 按住 **Reset** 按鈕 **30** 秒不放直到 **SYS** 燈開始閃爍
3. 放開 **Reset** 按鈕



\* 在無法登入設備，或不想登入設備後做 **Reset** 的選項

# 回復出廠預設值- 方式 2

- 維護 > 檔案管理程式 > 設定檔 > 設定

設定檔 韌體管理 Shell 指令碼

設定 備份排程

▷ 套用設定檔 [?] [X]

套用設定檔

檔案名稱: system-default.conf

套用設定檔時遭遇錯誤：

- 立即停止套用設定檔
- 立即停止套用設定檔，並返回上一個設定
- 忽略錯誤並結束套用設定檔
- 忽略錯誤並結束套用設定檔，接著返回上一個設定

OK Cancel

第 1 頁，共 1 頁 每頁顯示 50 行 顯示 1 - 8 行，共有 8 行

# 回復出廠預設值- 方式 3

- CLI

```
Router# configure terminal
Router(config)# apply /conf/system-default.conf
Set SW_WDT timeout: 60 secs
WTP System-log suppression: enable
WTP mail server '1' log_category(all) is:all
WTP mail server '2' log_category(all) is:all
USB Storage: off
WTP System-log suppression: enable
System-log suppression: enable
server category 'forward-web-sites' is : disable
server category 'ssl-inspection-traffic' is : disable
mail server '1' log_category(all) is:all
mail server '2' log_category(all) is:all
Router(config)#
```

# 忘記密碼如何備份設定檔

- 使用Console直連設備，並於開機過程輸入以下指令

```
COM3 - PuTTY
U-Boot 2013.07 (Development build, svnversion: u-boot:501M, exec:)-svn501 (Build time: Feb 13 2017 - 17:04:56)

BootModule Version: V1.17 | Feb 13 2017 17:04:56
DRAM: Size = 2048 Mbytes

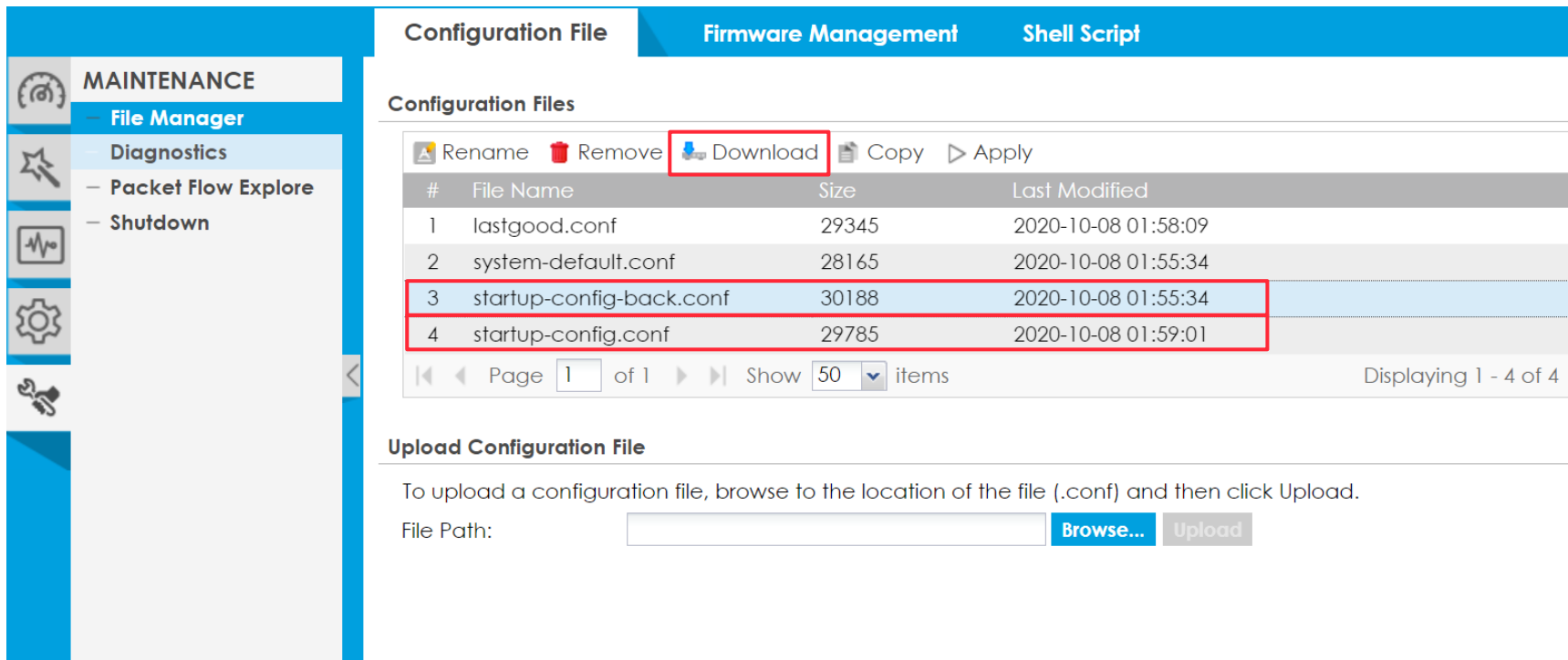
Press any key to enter debug mode within 3 seconds.
.....
Enter Debug Mode
ATP200> atkz -b

-b
OK
ATP200> atgo

Booting...
Allocating memory for ELF segment: addr: 0xfffffffff8080000 (adjusted to: 0x800000), size 0xc5a0a0
```

# 忘記密碼如何備份設定檔

- 重新登入後，下載「startup-config-back.conf」及「startup-config.conf」



The screenshot shows the 'Configuration File' tab in a network device's web interface. The left sidebar contains navigation options: MAINTENANCE, File Manager, Diagnostics, Packet Flow Explore, Shutdown, and a gear icon. The main content area has three tabs: Configuration File (selected), Firmware Management, and Shell Script. Below the tabs is a 'Configuration Files' section with a table of files. The 'Download' button in the toolbar is highlighted with a red box. The table lists four files, with the last two highlighted in red: 'startup-config-back.conf' and 'startup-config.conf'. Below the table is a pagination control showing 'Page 1 of 1' and 'Show 50 items'. At the bottom, there is an 'Upload Configuration File' section with a text input for 'File Path', a 'Browse...' button, and an 'Upload' button.

Configuration File    Firmware Management    Shell Script

Configuration Files

Rename Remove Download Copy Apply

#	File Name	Size	Last Modified
1	lastgood.conf	29345	2020-10-08 01:58:09
2	system-default.conf	28165	2020-10-08 01:55:34
3	startup-config-back.conf	30188	2020-10-08 01:55:34
4	startup-config.conf	29785	2020-10-08 01:59:01

Page 1 of 1 Show 50 items Displaying 1 - 4 of 4

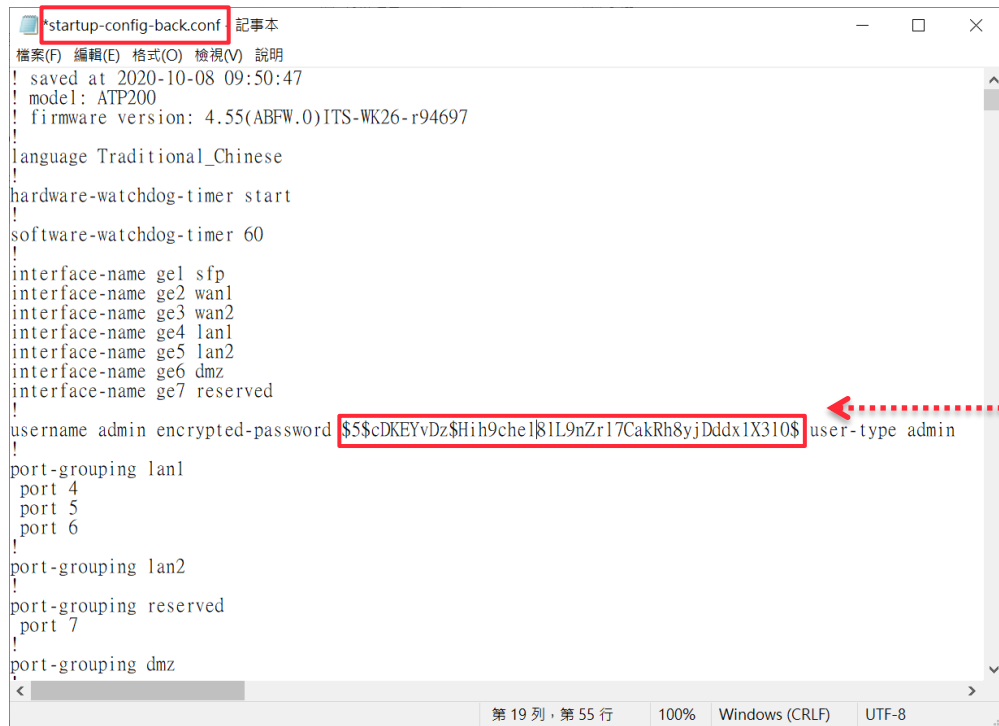
Upload Configuration File

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

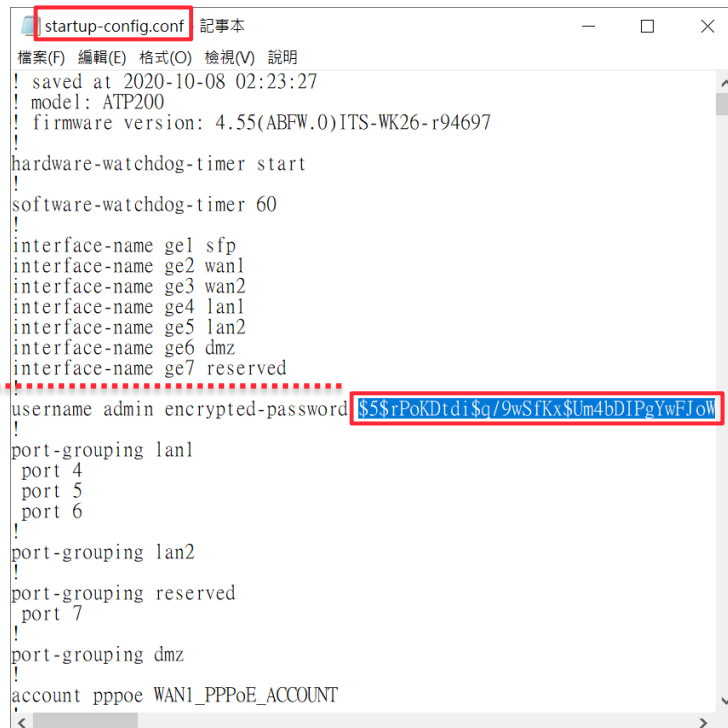
File Path:  Browse... Upload

# 忘記密碼如何備份設定檔

- Copy 「startup-config.conf」 的password取代 「startup-config-back.conf」 的password



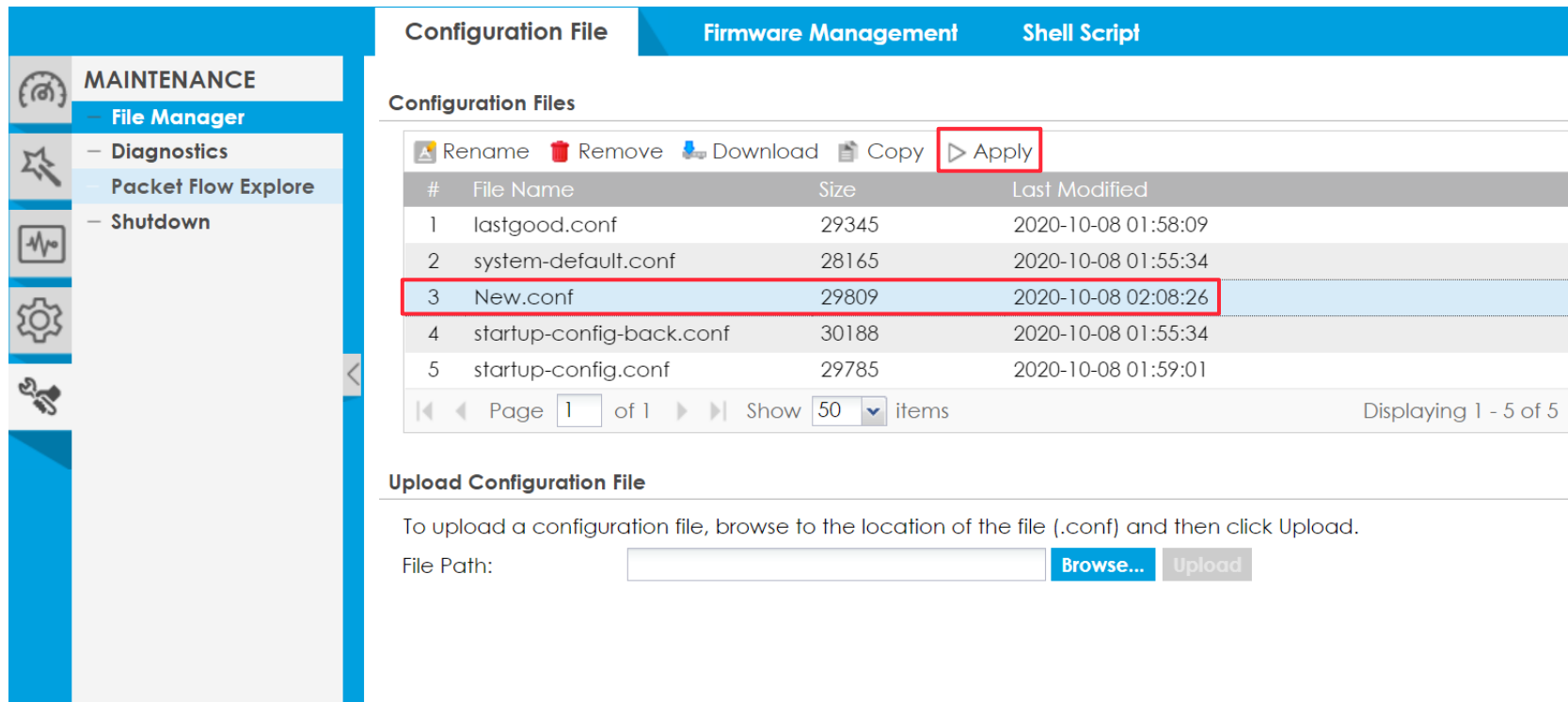
```
*startup-config-back.conf 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
! saved at 2020-10-08 09:50:47
! model: ATP200
! firmware version: 4.55(ABFW.0)ITS-WK26-r94697
!
! language Traditional_Chinese
!
! hardware-watchdog-timer start
!
! software-watchdog-timer 60
!
! interface-name ge1 sfp
! interface-name ge2 wan1
! interface-name ge3 wan2
! interface-name ge4 lan1
! interface-name ge5 lan2
! interface-name ge6 dmz
! interface-name ge7 reserved
!
! username admin encrypted-password $5$cDKEYvDz$Hih9che1$1L9nZr17CakRh8yjDddx1X310$ user-type admin
!
! port-grouping lan1
!   port 4
!   port 5
!   port 6
!
! port-grouping lan2
!
! port-grouping reserved
!   port 7
!
! port-grouping dmz
!
<
第 19 列, 第 55 行 100% Windows (CRLF) UTF-8
```



```
startup-config.conf 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明
! saved at 2020-10-08 02:23:27
! model: ATP200
! firmware version: 4.55(ABFW.0)ITS-WK26-r94697
!
! hardware-watchdog-timer start
!
! software-watchdog-timer 60
!
! interface-name ge1 sfp
! interface-name ge2 wan1
! interface-name ge3 wan2
! interface-name ge4 lan1
! interface-name ge5 lan2
! interface-name ge6 dmz
! interface-name ge7 reserved
!
! username admin encrypted-password $5$rPoKDtdi$g/9wSfKx$Um4bD1PqYwFJoW
!
! port-grouping lan1
!   port 4
!   port 5
!   port 6
!
! port-grouping lan2
!
! port-grouping reserved
!   port 7
!
! port-grouping dmz
!
! account pppoe WANI_PPPoE_ACCOUNT
<
```

# 忘記密碼如何備份設定檔

- 將「startup-config-back.conf」變更新檔名後上傳並Apply



The screenshot displays the ZyXEL configuration management interface. The left sidebar contains navigation options: MAINTENANCE, File Manager, Diagnostics, Packet Flow Explore, and Shutdown. The main content area is titled 'Configuration File' and includes tabs for 'Configuration File', 'Firmware Management', and 'Shell Script'. Below the tabs, there is a 'Configuration Files' section with a table of files. The table has columns for '#', 'File Name', 'Size', and 'Last Modified'. The file 'New.conf' is highlighted in blue, and the 'Apply' button is also highlighted in red. Below the table, there is an 'Upload Configuration File' section with a text input field for 'File Path', a 'Browse...' button, and an 'Upload' button.

#	File Name	Size	Last Modified
1	lastgood.conf	29345	2020-10-08 01:58:09
2	system-default.conf	28165	2020-10-08 01:55:34
3	New.conf	29809	2020-10-08 02:08:26
4	startup-config-back.conf	30188	2020-10-08 01:55:34
5	startup-config.conf	29785	2020-10-08 01:59:01

Page 1 of 1 Show 50 items Displaying 1 - 5 of 5

**Upload Configuration File**

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path:  **Browse...** **Upload**



# GUI Overview



# Agenda

---

01

**Navigation  
Panel**

02

**Dashboard**

# 主畫面

- FLEX200 主畫面

**ZYXEL USG FLEX 200**

General | **Advanced Threat Protection**

**System Status**  
CPU Usage: 2%  
Memory Usage: 35%  
Flash Usage: 15%  
USB Storage Usage: 0/0 MB  
Active Sessions: 405/600000  
DHCP Table: 1 Host(s)  
Number of Login Users: 1  
Current Login User: [redacted]

**Virtual Device**

ZYXEL USG FLEX ZYWALL Security

Ports: P1, P2, P3, P4, P5, P6, P7  
WAN1, WAN2, LAN/DMZ

**Device Information**  
System Name: [usgflex200](#)  
Serial Number: S202L12200632  
MAC Address Range: BC:CF:4F:B8:71:44 ~ BC:CF:4F:B8:71:4A  
Firmware Version: [V4.60\(ABUI.0\) / 2020-10-17 04:17:25](#)

**System Status**  
Boot Status: System default configuration  
System Uptime: 01:23:31  
Current Date/Time: [2020-11-17 / 13:07:56 UTC+08:00](#)

**Tx/Rx Statistics**

Port Selection: P2

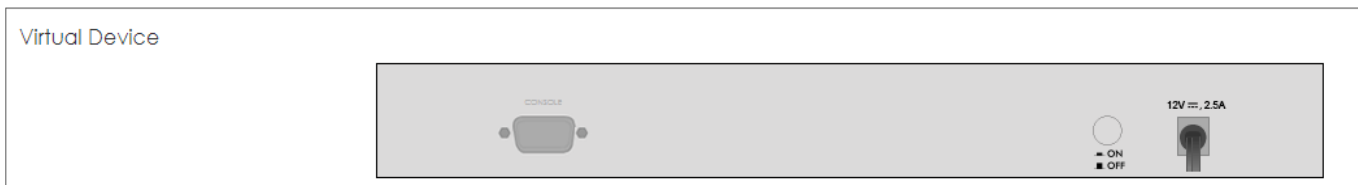
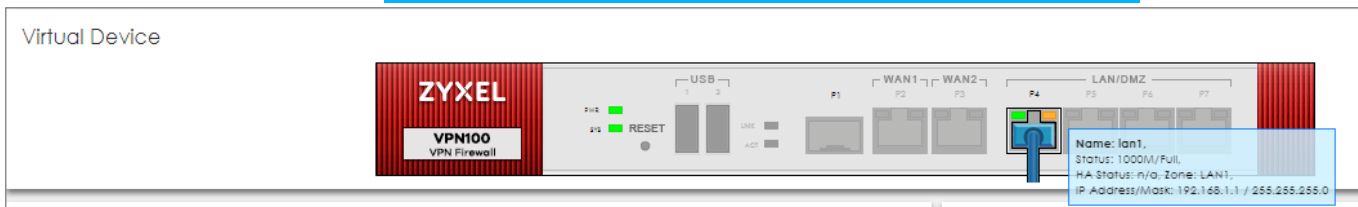
1.100  
0.800  
Tx

# 主畫面

- Virtual Device 可自行切換

- Example : VPN100、ATP100

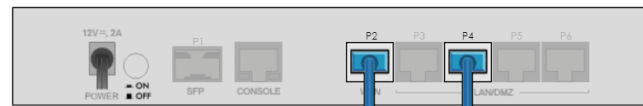
Different models have different virtual device panels



虛擬裝置



虛擬裝置



# Navigation Panel

- Main Dashboard Screens

工具列

The screenshot shows the Zyxel gateway dashboard. On the left is a vertical navigation panel (工具列) with icons for Home, Settings, System, and Tools. The main dashboard area is titled "Dashboard - show status information about the gateway" and has two tabs: "General" (selected) and "Advanced Threat Protection".

**General Tab Content:**

- CPU Usage:** 2%
- Memory Usage:** 35%
- Flash Usage:** 15%
- USB Storage Usage:** 0/0 MB
- Active Sessions:** 405/600000
- DHCP Table:** 1 Host[s]
- Number of Login Users:** 1
- Current Login User:** (empty)

**Virtual Device:** A diagram of the ZYXEL USB FLEX ZWALL Security gateway showing ports: USB 1, 2; P1; WAN1, WAN2; P2, P3; F4; LAN/DMZ P4, P5, P6, P7. A blue arrow points to port P2.

**Device Information:**

- System Name: [usgflex200](#)
- Serial Number: S202L12200632
- MAC Address Range: BC:CF:4F:8B:71:44 ~ BC:CF:4F:8B:71:4A
- Firmware Version: [V4.60\(ABUI.0\) / 2020-10-17 04:17:25](#)

**System Status:**

- Boot Status: System default configuration
- System Uptime: 01:23:31
- Current Date/Time: [2020-11-17 / 13:07:56 UTC+08:00](#)

**Tx/Rx Statistics:** Port Selection: P2

# Navigation Panel (1/2)

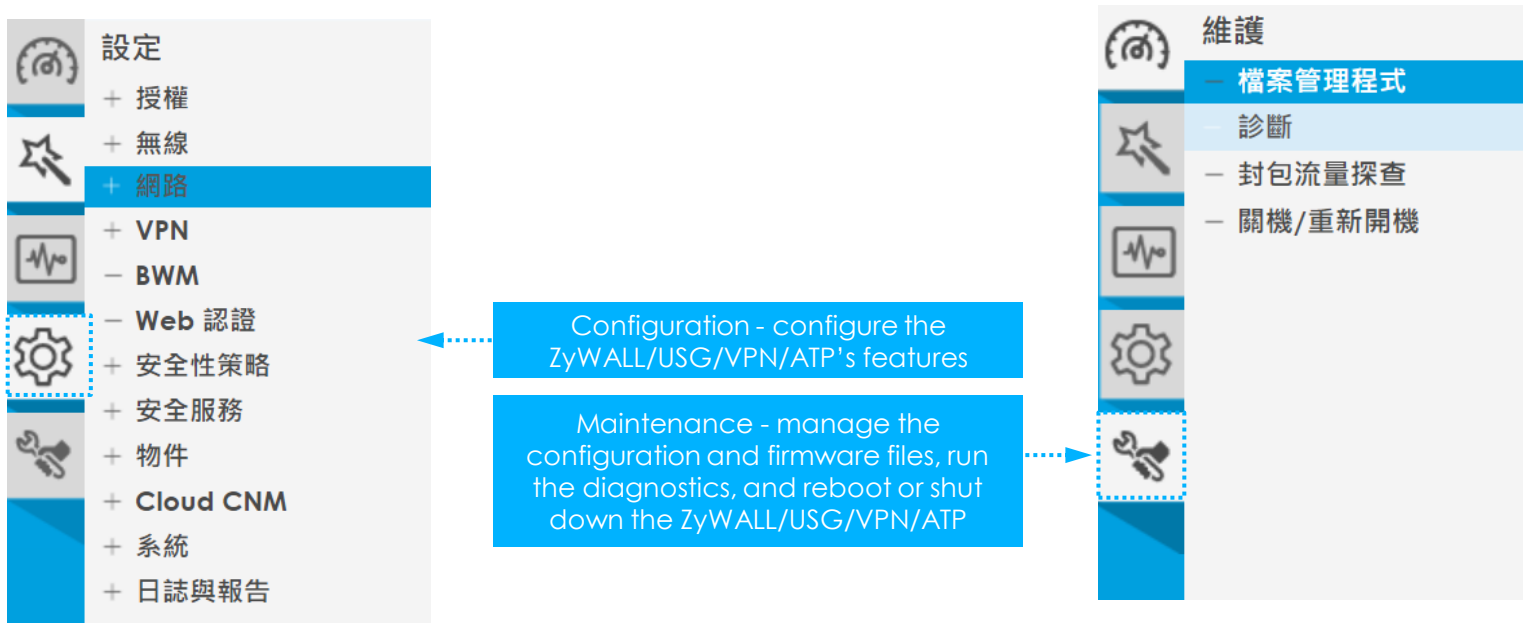
- **Monitor Screen**

Monitor - display status and statistics information



# Navigation Panel (2/2)

- Configuration Screen and Maintenance Screen



# Interface & Port





# Agenda

---

01

什麼是介面 &  
**Port**

02

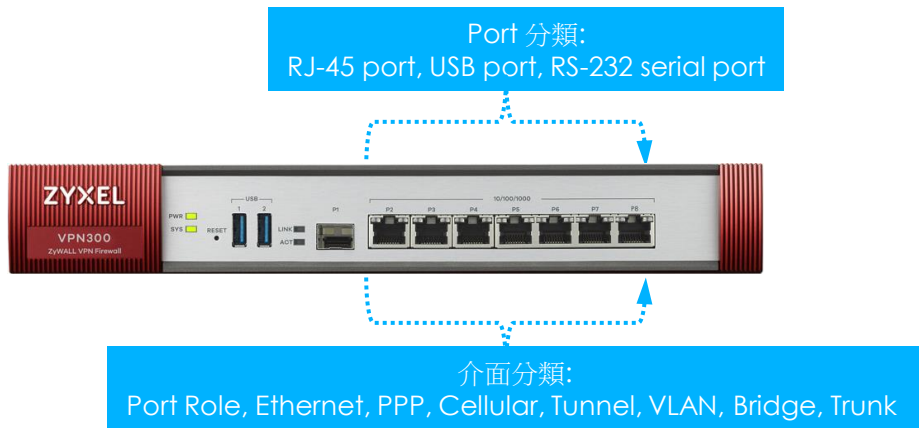
介面設定 **GUI**

03

介面的類型

# 什麼是介面 & Port?

- **Port**
  - 實際接線的孔位
- **介面**
  - 邏輯上連線介面結合實體 Port. EX: Bridge, Vlan... 等等



# 設定 GUI

- 設定頁面
  - 設定 > 網路 > 介面

The management interface category

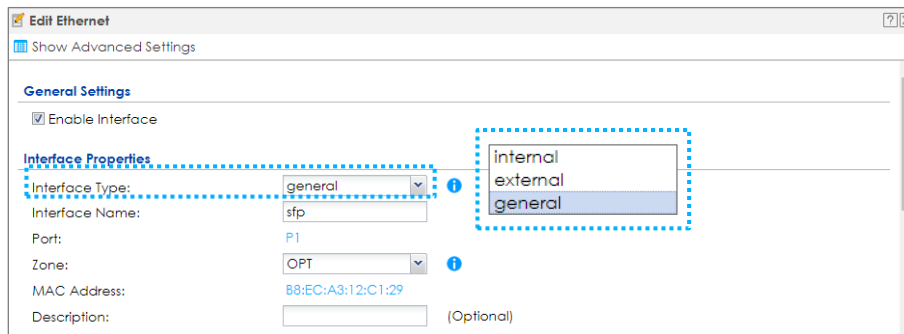
The screenshot shows the management interface for a ZyXEL device. The navigation menu on the left includes '設定' (Settings), '+ 授權' (Authorization), '+ 無線' (Wireless), '- 網路' (Network), '介面' (Interface), '- 路由' (Routing), '- DDNS', '- NAT', '- 重新導向服務' (Port Forwarding), '- ALG', '- UPnP', '- IP/MAC 綁定' (IP/MAC Binding), '- 層級 2 隔離' (Layer 2 Isolation), '- DNS 內送負載' (DNS Load Balancing), '+ VPN', and '- BWM'. The main content area has tabs for '連接埠' (Ports), '乙太網路' (Ethernet), 'PPP', '行動電話' (Mobile Phone), '通道' (Channel), 'VLAN 虛擬區域網路' (VLAN Virtual Local Area Network), '橋接器' (Bridge), 'VPN通道介面' (VPN Channel Interface), and '線路負載平衡策略' (Line Load Balancing Policy). Under '連接埠', there are sub-tabs for '連接埠角色' (Port Role) and '連接埠設定' (Port Configuration). The '連接埠設定' tab is active, showing a diagram of the network ports (P1, P2, P3, P4, P5, P6, P7) and a table of configuration options.

設定	P1	WAN1 P2	WAN2 P3	P4	P5	P6	P7
sfp (OPT)	<input checked="" type="radio"/>						
lan1 (LAN1)				<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
lan2 (LAN2)				<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
dmz (DMZ)				<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
reserved				<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

# 介面的種類(1/4)

- 設定 > 網路 > 介面 > 乙太網路
  - Internal interface
    - Connecting to a local network (DHCP Server/Relay, 無 Gateway 設定)
  - External interface
    - Connecting to an external network like the Internet (DHCP Client, 有 Gateway 設定)
  - General interface

預設：  
Internal --> External (NAT)



# 介面的種類 (2/4)

- Internal Interface

Interface Properties	
Interface Type:	internal
Interface Name:	lan1
Port:	P4, P5, P6
Zone:	LAN1
MAC Address:	B8:EC:A3:12:C1:2C
Description:	<input type="text"/> (Optional)

IP Address Assignment	
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
<input type="checkbox"/> Enable IGMP Support	
<input type="radio"/> IGMP Upstream	
<input checked="" type="radio"/> IGMP Downstream	

DHCP Setting			
DHCP:	DHCP Server		
IP Pool Start Address:	192.168.1.33	Pool Size:	200
First DNS Server (Optional):	ZyWALL		
Second DNS Server (Optional):	None		
Third DNS Server (Optional):	None		

# 介面的種類 (3/4)

- External Interface

Interface Properties	
Interface Type:	external
Interface Name:	wan1
Port:	P2
Zone:	WAN
MAC Address:	B8:EC:A3:12:C1:2A
Description:	<input type="text"/> (Optional)
IP Address Assignment	
<input checked="" type="radio"/> Get Automatically	192.168.1.105
<input type="checkbox"/> Advance	
<input type="radio"/> Use Fixed IP Address	
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>
Gateway:	<input type="text"/> (Optional)
Metric:	0 (0-15)

# 介面的種類 (4/4)

- General Interface

**Interface Properties**

Interface Type:  ⓘ

Interface Name:

Port:

Zone:  ⓘ

MAC Address:

Description:  (Optional)

**IP Address Assignment**

Get Automatically

Advance

Use Fixed IP Address

IP Address:

Subnet Mask:

Gateway:  (Optional)

Metric:  (0-15)

**DHCP Setting**

DHCP:  ⓘ

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

When the Interface Type is set to internal or external, the device will add corresponding default route and SNAT settings.

# VLAN

04





# Agenda

---

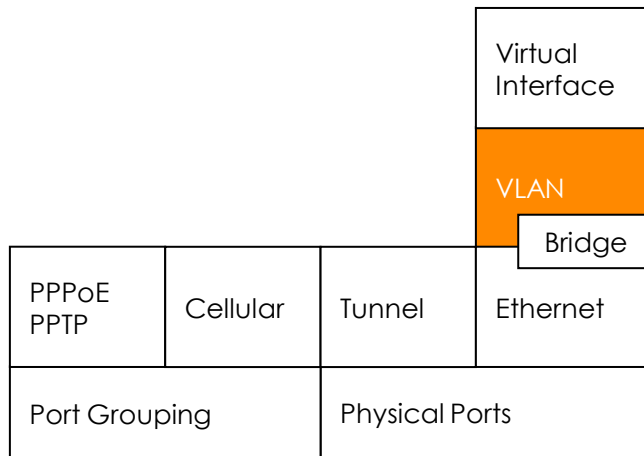
01  
VLAN介紹

02  
VLAN 使用情境

03  
VLAN Web  
設定頁面

# VLAN (1/2)

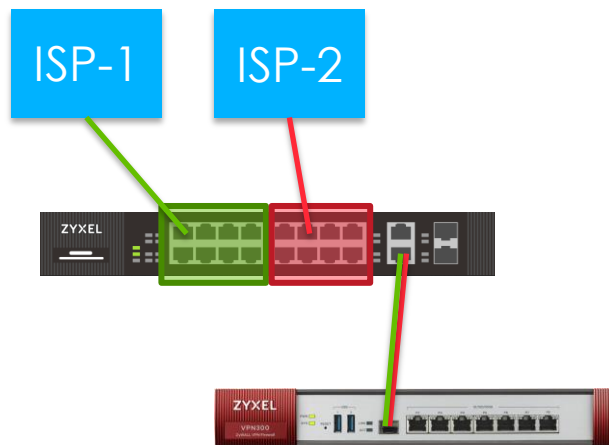
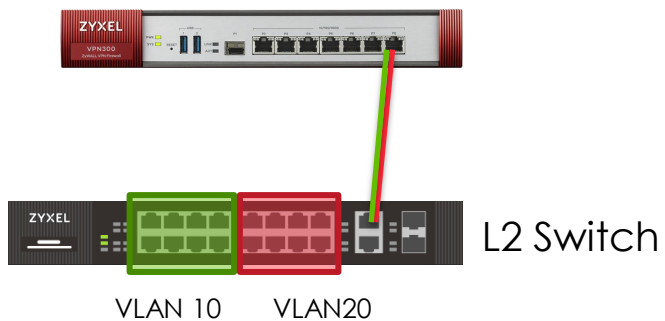
- **USG Flex/VPN/ATP 支援 IEEE 802.1Q VLAN.**
- **VLAN 界面設定存在於實體介面上**
- **Tagged-based VLAN.**





# VLAN 使用情境

- VLAN Routing
- Single Port, Multi-WAN



# VLAN Web設定頁面

- 設定 > 網路 > 介面 > VLAN 虛擬區域網路

**Add VLAN** [?] [X]

Show Advanced Settings

**Interface Properties**

Interface Type: internal [v] ⓘ

Interface Name: vlan20

Zone: LAN1 [v] ⓘ

Base Port: sfp [v]

VLAN ID: 20 (1-4094)

Advance

Description: [ ] (Optional)

**IP Address Assignment**

IP Address: 192.168.20.1

Subnet Mask: 255.255.255.0

Enable IGMP Support

IGMP Upstream

IGMP Downstream

**DHCP Setting**

DHCP: None [v]

Enable IP/MAC Binding

Enable Logs for IP/MAC Binding Violation

None  
DHCP Relay  
DHCP Server

# VLAN 數量的最大值

- 下表為不同 Gateway 支援最大 VLAN 數量
- 最少8個，最多256個

ZLD 4.60	USG20(W)-VPN	USG40(W)	USG60(W)	USG110	USG210	USG310	USG1100	USG1900	USG2200
Maximum of VLAN number	8	8	16	16	32	64	128	128	256

ZLD 4.60	ATP100(W) USG FLEX 100 (W)	ATP200 USG FLEX 200	ATP500 USG FLEX 500	ATP700 USG FLEX 700	ATP800
Maximum of VLAN number	8	16	64	128	128

ZLD4.60	VPN50	VPN100	VPN300	VPN1000
Maximum of VLAN number	8	16	64	128

# Bridge

05



# Agenda

---

01  
**Bridge** 介紹

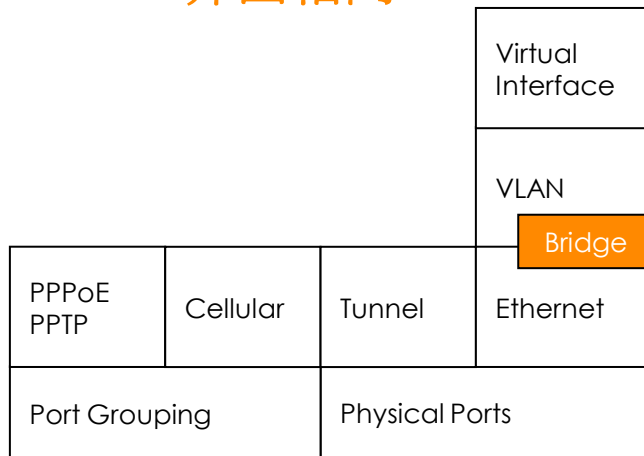
02  
**Bridge** 使用情境

03  
**Bridge**  
**Web** 設定頁面



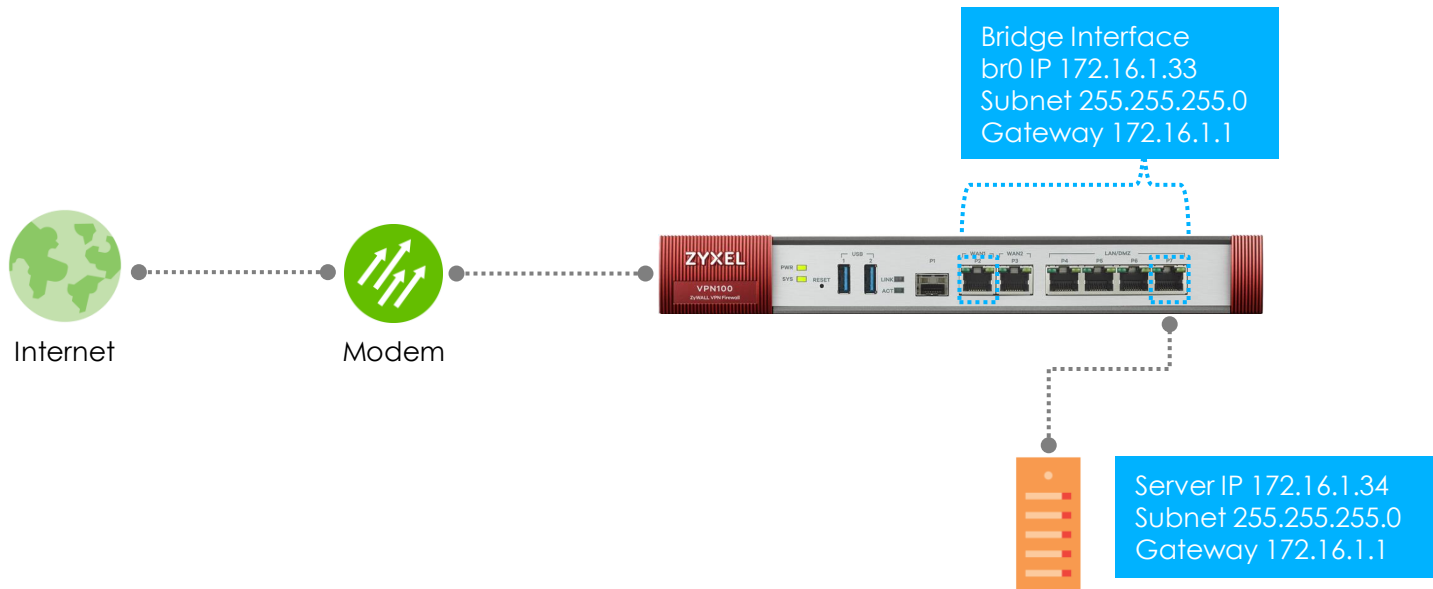
# Bridge

- 又稱為透通模式.
- 由 **Ethernet** 介面及最多一組 **VLAN** 介面組成
- **Ethernet** 介面一旦橋接為 **Bridge**，**Ethernet** 介面上的 **IP** 及 **Routing** 功能就會失效
- **Bridge** 介面的設定內容與 **Ethernet** 介面相同



# Bridge 使用情境

- **Server 使用的 IP 與 Internet 使用相同網段 IP**
- **做 POC 或不異動客戶現有環境架構下可以採用 Bridge mode**



# Bridge 介面設定

- 新增 Bridge 介面
  - 設定 > 網路 > 介面 > 橋接器

The screenshot shows the 'Add Bridge' configuration window with three blue callout boxes pointing to specific fields:

- 設定介面的區域類型**: Points to the 'Zone' dropdown menu, which is currently set to 'DMZ'.
- 選擇要橋接的介面  
ex : [WAN1 and DMZ]**: Points to the 'Member Configuration' section, where 'wan1' and 'dmz' are selected in the 'Member' list.
- 輸入 Bridge 介面的 IP Address**: Points to the 'IP Address Assignment' section, where 'Use Fixed IP Address' is selected and the IP address '172.16.1.33' is entered.

The window also shows the following configuration details:

- Interface Properties**: Interface Type: external, Interface Name: br0, Zone: DMZ, Description: (Optional).
- Member Configuration**: Available: sfp, wan2, lan1, lan2, reserved; Member: wan1, dmz.
- IP Address Assignment**:  Get Automatically,  Advance,  Use Fixed IP Address. IP Address: 172.16.1.33, Subnet Mask: 255.255.255.0, Gateway: 172.16.1.1 (Optional), Metric: 0 (0-15).

# PPPoE

06



# Agenda

---

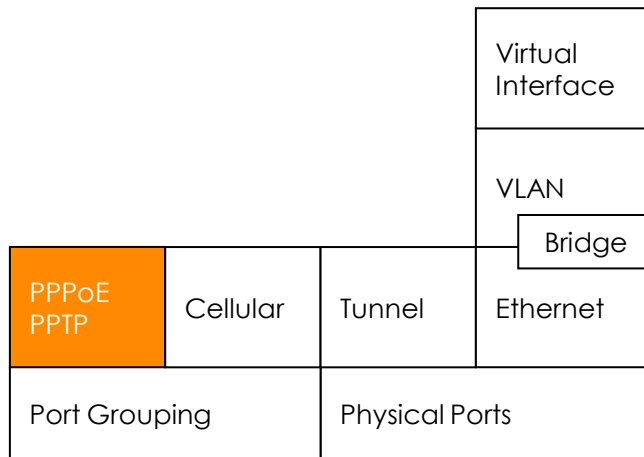
01  
PPP 介紹

02  
PPPoE 使用情境

03  
PPP 連線  
設定模式

# PPP (1/3)

- 設備支援 **PPP-over-Ethernet (PPPoE)**
- **PPPoE** 廣泛的應用在 **xDSL** 環境



# PPP (2/3)

- **USG Flex/VPN/ATP 提供的 PPP 介面數量**
  - ZyWALL/USG series

ZLD 4.60	USG20(W)-VPN	USG40(W)	USG60(W)	USG110	USG210	USG310	USG1100	USG1900	USG2200
System Default	2	2	2	3	3	8	8	8	8
User Create	2	2	4	4	8	16	32	32	32

連接埠 乙太網路 PPP 行動電話 通道 VLAN 虛擬區域網路

使用者配置

新增 編輯 刪除 啟動 停用 連線 中斷連線 物件參考

#	狀態	名稱	描述	基本介面	帳號設定組合
<< 第 0 頁, 共0頁 >>   每頁顯示 50 行 沒有任何資料					

系統預設

編輯 啟動 停用 連線 中斷連線 物件參考

#	狀態	名稱	描述	基本介面	帳號設定組合
1		wan1_ppp		wan1	WAN1_PPPoE_ACCOUNT
2		wan2_ppp		wan2	WAN2_PPPoE_ACCOUNT
3		sfp_ppp		sfp	none

||<< 第 1 頁, 共1頁 >>|| 每頁顯示 50 行 顯示 1 - 3 之 3

# PPP (2/3)

- **USG Flex/VPN/ATP 提供的 PPP 介面數量**
  - ATP/USG FLEX/VPN series

ZLD4.60	ATP100(W) USG FLEX 100(W)	ATP200 USG FLEX 200	ATP500 USG FLEX 500	ATP700 USG FLEX 700	ATP800
System Default	2	3	8	14	14
User Create	2	4	16	32	32

ZLD4.60	VPN50	VPN100	VPN300	VPN1000
System Default	3	3	8	14
User Create	2	4	16	32



# PPP (3/3)

- 2種不同的連線模式
  - Nailed-Up
  - Dial-on-Demand

The screenshot displays the Zyxel Network Manager web interface for configuring PPP. The main navigation bar includes tabs for 連接埠, 乙太網路, PPP, 行動電話, 通道, and VLAN. The left sidebar contains a menu with options like 設定, 授權, 無線, 網路, 介面, 路由, DDNS, NAT, 重新導向服務, ALG, UPnP, IP/MAC 綁定, 層級 2 隔離, DNS 內送負載, VPN, and BWM. The main content area is titled 'Edit PPPoE/PPTP' and includes a sub-menu with '隱藏進階設定' and '建立新物件'. The configuration is divided into sections: '一般設定' with a checked '啟用介面' option; '介面屬性' with fields for '介面名稱' (wan1\_ppp), '基本介面' (wan1), and '區域' (WAN); and '連線' with radio buttons for '固定' (selected) and '隨需撥接'. A red dashed box highlights the '連線' section.

# PPP (3/3)

## • PPP連線狀態

ZYXEL ATP200



← 連接埠 乙太網路 **PPP** 行動電話 通道 VLAN 虛擬區域網路

設定  
+ 授權  
+ 無線  
- 網路

— 介面  
- 路由  
- DDNS  
- NAT  
- 重新導向服務  
- ALG  
- UPnP  
- IP/MAC 綁定  
- 層級 2 隔離  
- DNS 內送負載

### 使用者配置

新增 編輯 移除 啟動 停用 連線 中斷連線 物件參考

#	狀態	名稱	描述	基本介面	帳號設定組合
第 0 頁，共 0 頁 每頁顯示 50 行 沒有任何資料					

### 系統預設

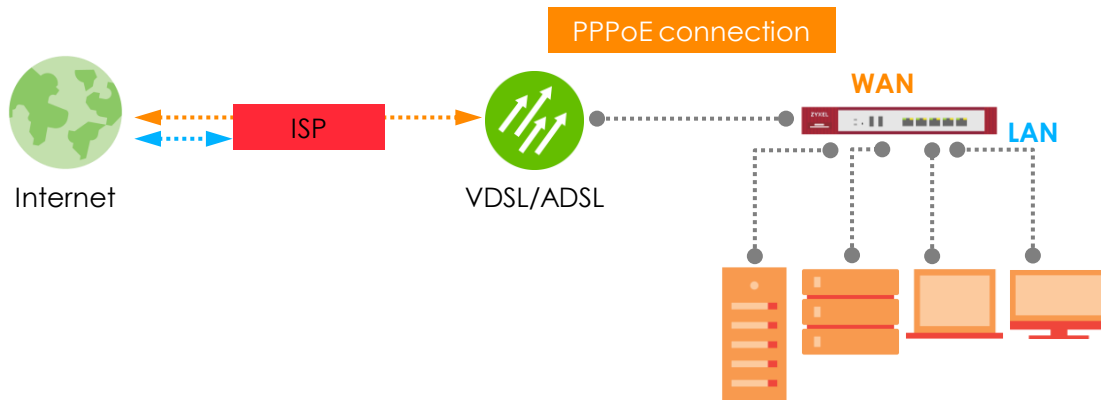
編輯 啟動 停用 連線 中斷連線 物件參考

#	狀態	名稱	描述	基本介面	帳號設定組合
1		wan1_ppp		wan1	WAN1_PPPOE_ACCOUNT
2		wan2_ppp		wan2	WAN2_PPPOE_ACCOUNT
3		sfp_ppp		sfp	none

第 1 頁，共 1 頁 每頁顯示 50 行 顯示 1 - 3 之 3

# PPPoE 使用情境

- PPPoE 通常用於 WAN 的連線



# PPP 連線的設定步驟

- PPP 介面的帳號設定
- 產生 ISP 設定檔，將帳號密碼建立於此
- 相同的帳號可以同時套用到不同的 PPP 介面上

ISP 帳號

設定

新增 編輯 移除 物件參考

#	設定組合名稱	通訊協定	認證方式	使用者名稱
1	SFP_PPPOE_ACCOUNT	pppoe	chap-pap	
2	SFP_PPTP_ACCOUNT	pptp	chap-pap	
3	WAN1_PPPOE_ACCOUNT	pppoe	chap-pap	74102914@hinet.net
4	WAN1_PPTP_ACCOUNT	pptp	chap-pap	
5	WAN2_PPPOE_ACCOUNT	pppoe	chap-pap	
6	WAN2_PPTP_ACCOUNT	pptp	chap-pap	

第 1 頁，共 1 頁 每頁顯示 50 行 顯示 1 - 6 之 6

# 設定 PPP 連線 (1/3)

- 1st Tier : 設定帳號
  - 設定 > 物件 > ISP Account
    - 編輯 ISP account

設定組合名稱: WAN1\_PPPoE\_ACCO

通訊協定: pppoe

認證方式: Chap/PAP

使用者名稱: 74102914@hinet.net

密碼: .....

重新鍵入確認: .....

服務名稱: (選擇性)

壓縮:  On  Off

閒置等候時間: 100 (秒數)

OK Cancel

**Note: Service Name** 在台灣為空白值，請勿填寫以免連線失敗

# 設定 PPP 連線 (2/3)

- 2nd Tier: 設定 PPP 介面
  - 設定 > 網路 > 介面 > PPP
    - 設定 PPP 介面

Edit PPPoE/PPTP

顯示進階設定 建立新物件

一般設定

啟用介面

介面屬性

介面名稱: wan1\_ppp

基本介面: wan1

區域: WAN

描述:  (選擇性)

連線

固定

隨需撥接

ISP 設定

帳號設定組合: WAN1\_PPPoE\_ACC

通訊協定: pppoe

使用者名稱: 74102914@hinet.net

服務名稱:

IP 位址指派

自動取得 36.231.123.147

使用固定 IP 位址

IP 位址:

進階設定

度量資訊: 0 (0-15)

OK Cancel

# 設定 PPP 連線 (3/3)

- 3rd Tier: 撥接 (如果是 Nailed-UP 會自動連線無須手動)
  - 設定 > 網路 > 介面 > PPP
    - 透過 PPP 介面建立 PPPoE 連線

The screenshot displays a network configuration interface with a sidebar on the left and a main content area. The sidebar includes a navigation menu with options like '設定', '+ 授權', '+ 無線', '- 網路', '- 介面', '- 路由', '- DDNS', '- NAT', '- 重新導向服務', '- ALG', '- UPnP', '- IP/MAC 綁定', '- 層級 2 隔離', '- DNS 內送負載平', '+ VPN', '- BWM', and '- Web 認證'. The main content area is titled 'PPP' and shows two sections: '使用者配置' and '系統預設'. The '使用者配置' section has a table with columns for '#', '狀態', '名稱', '描述', '基本介面', and '帳號設定組合'. The '系統預設' section also has a table with similar columns. Both tables show three entries: 'wan1\_ppp', 'wan2\_ppp', and 'sfp\_ppp'.

#	狀態	名稱	描述	基本介面	帳號設定組合
1		wan1_ppp		wan1	WAN1_PPPOE_ACCOUNT
2		wan2_ppp		wan2	WAN2_PPPOE_ACCOUNT
3		sfp_ppp		sfp	none

# Trunk

09





# Agenda

---

01  
**Trunk** 介紹

02  
**Trunk** 使用情境

03  
**Trunk**  
**Web** 設定頁面

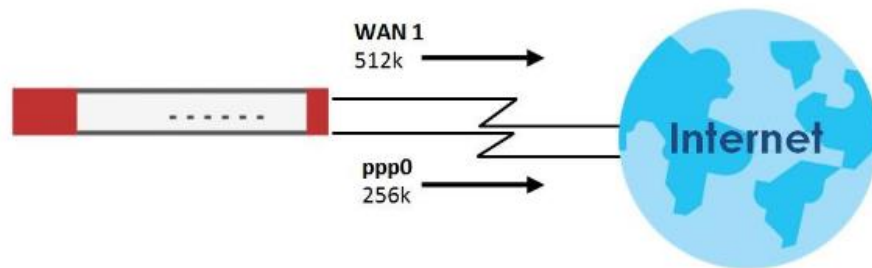
# Trunk 線路負載平衡

- 支援 3 種負載平衡演算法

- Weighted Round Robin (WRR)
- Least Load First (LLF)
- Spillover

- 每一個在 **Trunk** 裡的介面都可以設成

- Active
- Passive (只有在 Active Link 無法使用時才會啟用)



# Trunk 設定畫面(1/3)

- **Trunk 管理頁面**

- 設定 > 網路 > 介面 > 線路負載平衡策略

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes tabs for '連接埠', '乙太網路', 'PPP', '行動電話', '通道', 'VLAN 虛擬區域網路', '橋接器', 'VPN通道介面', and '線路負載平衡策略'. The left sidebar contains a tree view of settings, with '設定' > '網路' > '介面' > '線路負載平衡策略' selected. The main content area is titled '顯示進階設定' and contains the following sections:

- 設定**: Includes a checkbox for '返回前中斷連線'.
- 選取 WAN 線路負載平衡策略**: Includes a '進階設定' dropdown and a selection for '預設線路負載平衡策略'. The selected option is 'SYSTEM\_DEFAULT\_WAN\_TRUNK'.
- 使用者配置**: A table listing user configurations. The table is currently empty, showing '第 0 頁, 共 0 頁' and '每頁顯示 50 行'. A note states '沒有任何資料'.
- 系統預設**: A table listing system defaults. It contains one entry: 'SYSTEM\_DEFAULT\_WAN\_TRUNK' with an algorithm of 'lbf'.

At the bottom right, there are buttons for '套用' and '重設'.

# Trunk 設定畫面 (2/3)

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - 系統預設 (只能調整演算法)

System Default

Edit  Object References

#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TRUNK	lbf

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Edit System Default

Name: SYSTEM\_DEFAULT\_WAN\_TRUNK

Load Balancing Algorithm: Least Load First

- Weighted Round Robin
- Least Load First
- Spillover

#	Member	Mode	Ingress Bandwidth	Egress Bandwidth
1	wan1	Active	1048576 kbps	1048576 kbps
2	wan2	Active	1048576 kbps	1048576 kbps
3	wan1_ppp	Active	1048576 kbps	1048576 kbps
4	wan2_ppp	Active	1048576 kbps	1048576 kbps
5	sfp_ppp	Active	1048576 kbps	1048576 kbps

Page 1 of 1 Show 50 items Displaying 1 - 5 of 5

OK Cancel

# Trunk 設定畫面 (3/3)

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - 使用者配置

**+ Add Trunk** [?] [X]

Name: Custom\_Trunk\_1

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

Weighted Round Robin  
Least Load First  
Spillover  
Outbound  
Inbound  
Outbound + Inbound

+ Add Edit Remove Move

#	Member	Mode	Egress Bandwidth
No data to display			

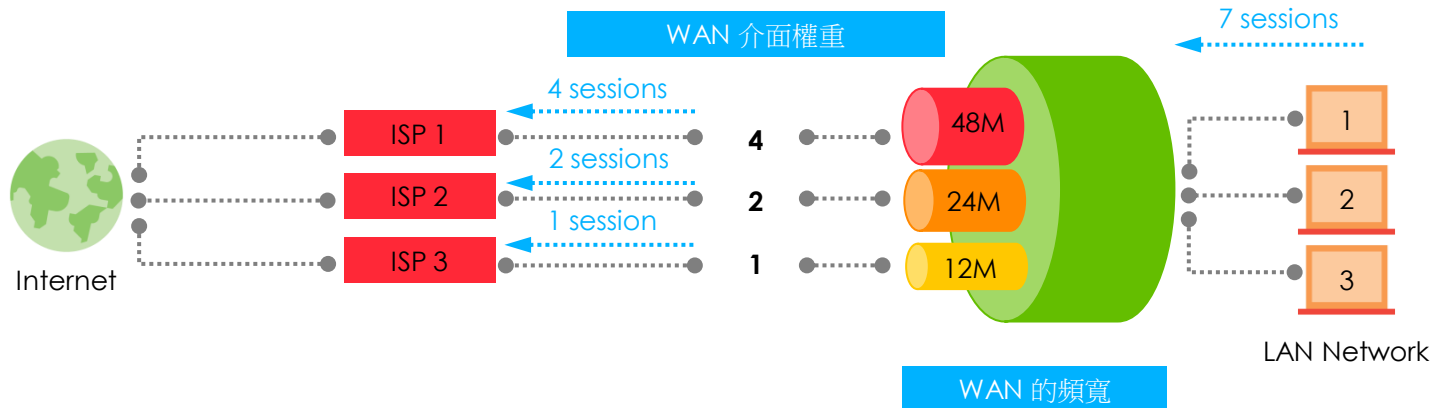
Page 0 of 0 Show 50 items

OK Cancel

# WRR 使用情境

- **Weighted Round Robin (WRR)**

- USG Flex/VPN/ATP 依據 WAN 介面設定的權重進行流量分配 (Session)



# WRR 設定畫面

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - WRR 管理頁面

**Edit WRR**

Name: WRR

Load Balancing Algorithm: Weighted Round R

#	Member	Mode	Weight
1	ISP1	Active	4
2	ISP2	Active	1
3	ISP3	Active	2

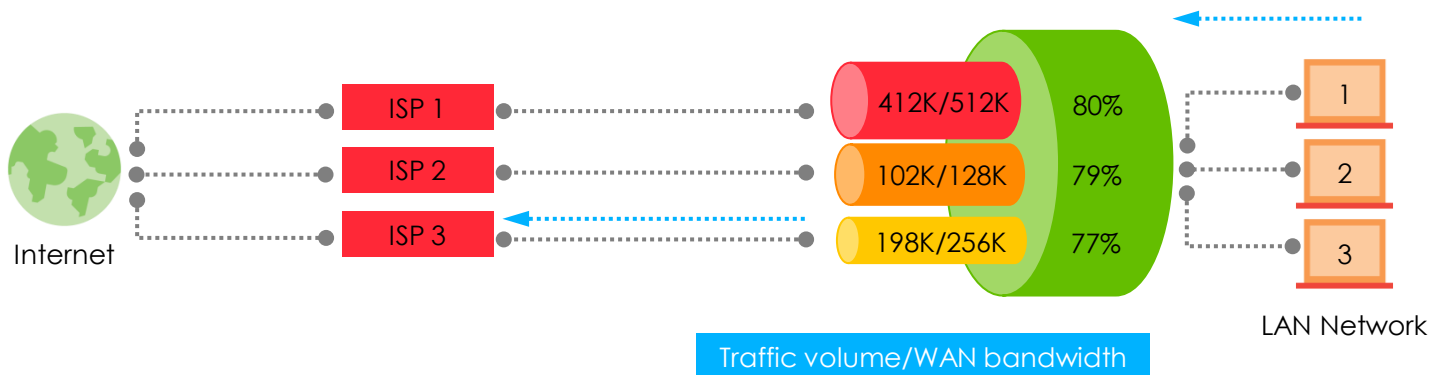
Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

OK Cancel

# LLF 使用情境

- **Least Load First (LLF)**

- USG Flex/VPN/ATP 會計算 WAN 介面的負載狀態 (Session) ，並嘗試使用負載較輕的 WAN 介面傳送資料





# LLF 設定畫面

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - LLF 管理頁面

Edit LLF

Name: LLF

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound + Inbou

#	Member	Mode	Ingress Bandwidth	Egress Bandwidth
1	ISP1	Active	512 kbps	512 kbps
2	ISP2	Active	128 kbps	128 kbps
3	ISP3	Active	256 kbps	256 kbps

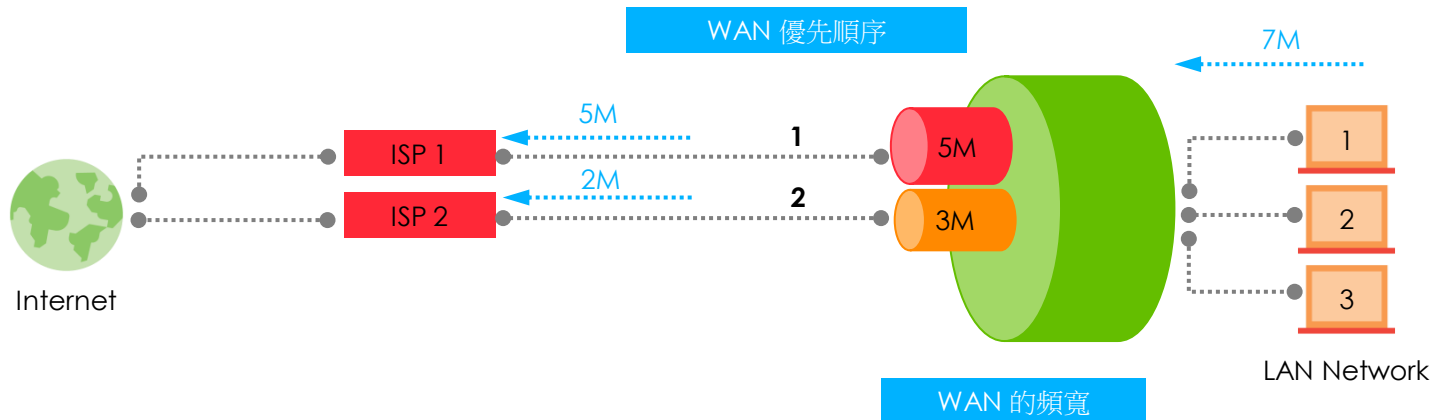
Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

OK Cancel

# Spillover 使用情境

- **Spillover**

- USG Flex/VPN/ATP 會計算 WAN 介面一段時間流量負載，於超過設定門檻時自動切換 Session 至另一 WAN 介面



# Spillover 設定畫面

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - Spillover 的管理頁面

**Edit Spillover**

Name: Spillover

Load Balancing Algorithm: Spillover

Load Balancing Index(es): Outbound + Inbou

#	Member	Mode	Total Bandwidth	Spillover
1	ISP1	Active	1024 kbps	512 kbps
2	ISP2	Active	768 kbps	128 kbps

Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

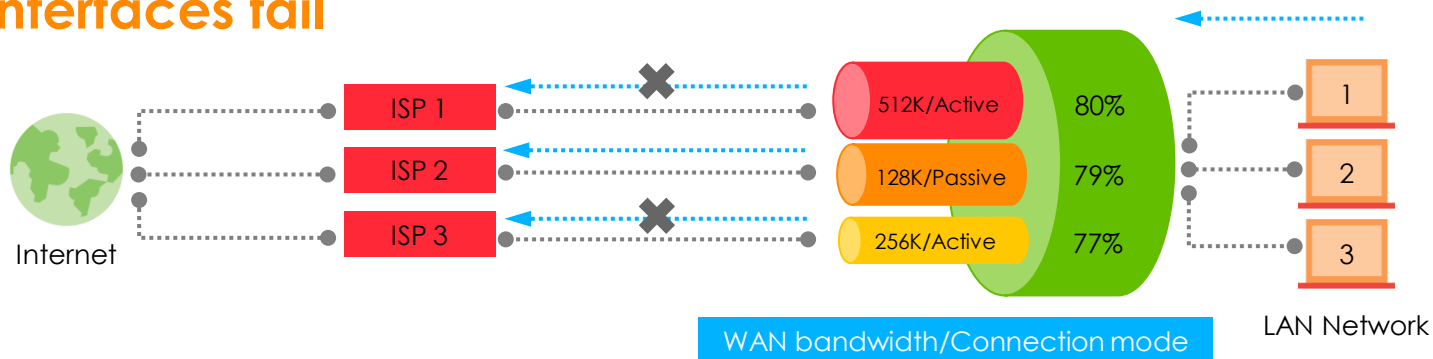
OK Cancel

# Trunk Failover (Active/Passive)使用情境

- **Trunk Failover**

- You can only set one of a group's interfaces to passive mode in a trunk.
- Example: Spillover algorithm
  - **ISP 1, ISP 3 (active mode)**
  - **ISP 2 (passive mode)**

- **The passive interface (ISP2) is activated when all active interfaces fail**



# Failover 的設定畫面

- 設定 > 網路 > 介面 > 線路負載平衡策略
  - Interface mode configuration page

Edit Spillover

Name: Spillover

Load Balancing Algorithm: Spillover

Load Balancing Index(es): Outbound

+ Add Edit Remove Move

#	Member	Mode	Egress Bandw...	Spillover
1	ISP1	Active	512 kbps	512 kbps
2	ISP2	Passive	128 kbps	0 kbps
3	ISP3	Active	256 kbps	256 kbps

Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

OK Cancel

# Object

# Outline

---

01  
**Zone**

---

02  
**User/Group**

---

03  
**AP Profile**

---

04  
**Address**

---

05  
**Service**

# Zone





# Agenda

---

01

**Zone** 物件介紹

02

**Zone** 的設定

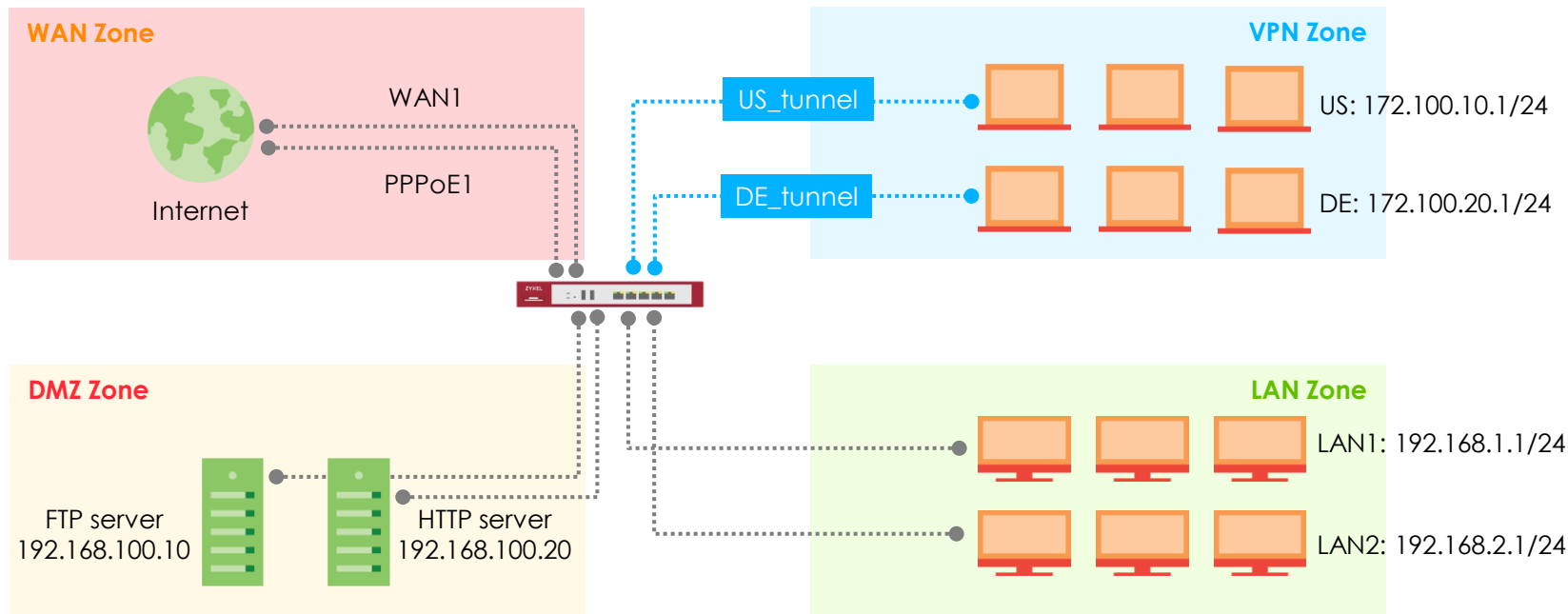
# Zone 基本原則

- 一個介面只能歸屬在一個 **Zone** 區域內
- 一個 **Zone** 區域可以包含多個介面
- 藉由 **Zone** 區隔網路並套用安全政策

# What You Need to Know

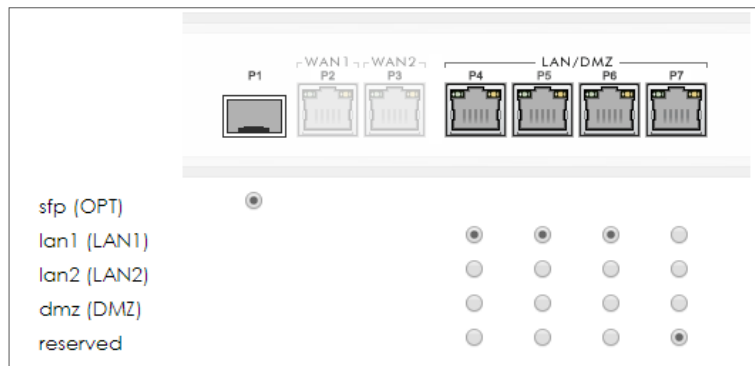
- **Zone 區域類型**
  - WAN, OPT, LAN1, LAN2 and DMZ
- **不同種類的流量**
  - Intra- Zone traffic
    - 相同 Zone 區域下，不同介面或 VPN 通道間的流量
  - Inter- Zone traffic
    - 不同 Zone 區域的介面或 VPN 通道間的流量
  - Extra- Zone traffic
    - 不屬於任何 Zone 區域的介面或 VPN 通道的流量

# 情境

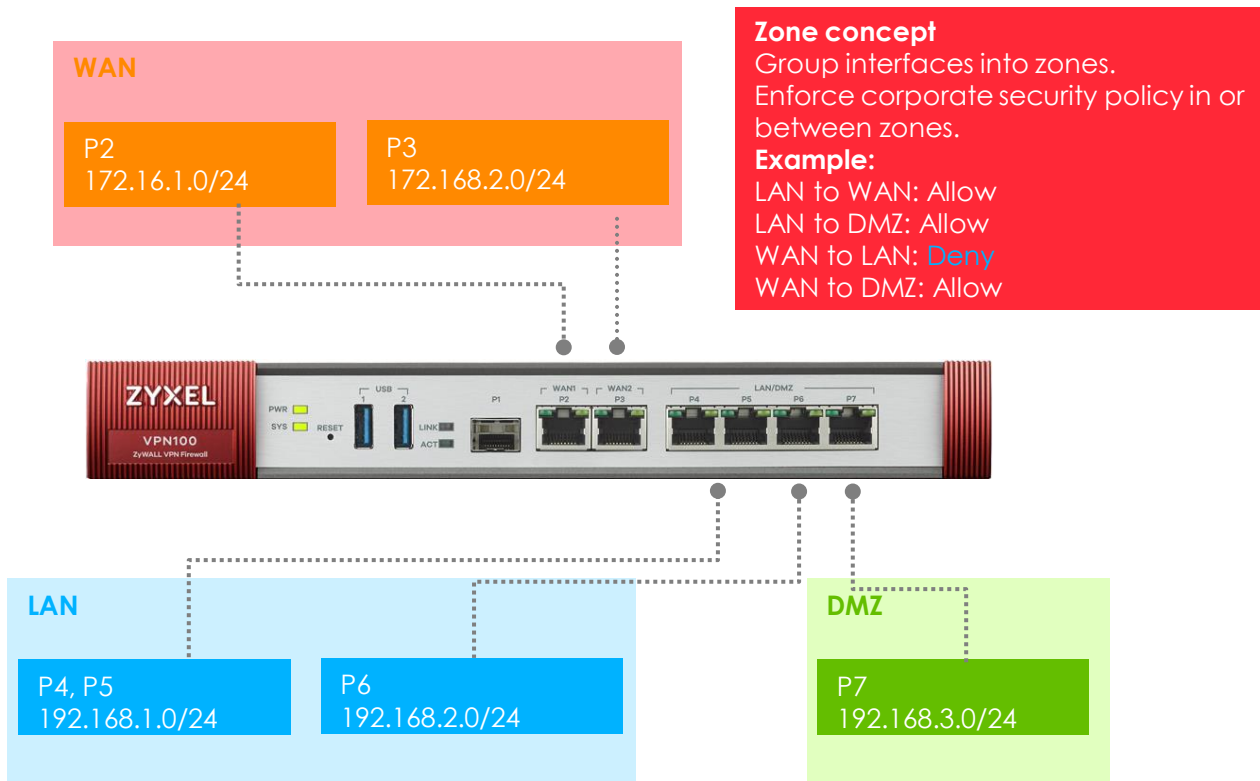


# 預設的 Zone 設定

- 預設的 Port, Interface 與 Zone ( VPN100 )
  - Port – 實體接線孔位
  - Interface – 介面名稱，描述介面用途與系統運作使用
  - Zone – 集合介面並用於安全政策的管理



# 範例



# Zone 區域設定 (1/2)

- 設定 > 物件 > 區域

區域

設定

- + 授權
- + 無線
- + 網路
- + VPN
- BWM
- Web 認證
- + 安全性策略
- + 安全服務
- 物件
- 區域
- 使用者/群組
- AP 設定組合
- MON 設定組合
- ZyMesh 設定組合
- 位址/Geo IP
- 服務
- 排程
- AAA 伺服器

使用者配置

+ 新增   編輯   移除   物件參考

#	名稱	成員	參考
<< 第 0 頁, 共0頁 >>   每頁顯示 50 行 沒有任何資料			

系統預設

編輯   物件參考

#	名稱	成員	參考
1	LAN1	lan1	4
2	LAN2	lan2	4
3	DMZ	dmz	4
4	WAN	wan1,wan2,wan1_ppp,wan2_ppp	5
5	OPT	sfp,sfp_ppp	0
6	SSL_VPN		4
7	IPSec_VPN		4
8	TUNNEL		4

||<< 第 1 頁, 共1頁 >>|| 每頁顯示 50 行 顯示 1 - 8 之 8

# Zone 區域設定 (2/2)

- 設定 > 物件 > 區域 > 編輯

**Edit Zone**

**Group Members**

Name: LAN1

**Member List**

Available	Member
=== Interface ===	=== Interface ===
ISP1	lan1
ISP2	
ISP3	
reserved	

OK Cancel



# User/Group



# Agenda

---

01

**User/Group**

物件介紹

02

**User/Group**

設定

# User/Group

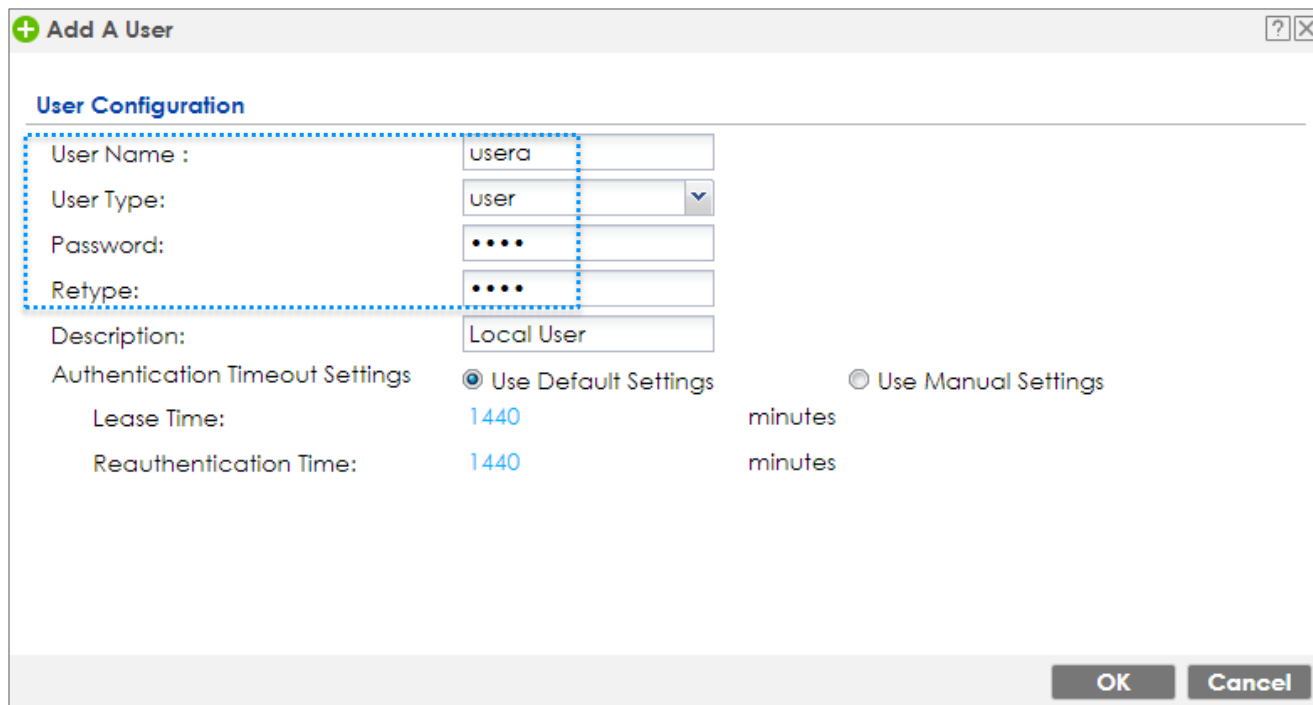
- 使用者類型與權限

- admin 預設使用本機使用者資料庫認證，無法變更

Type	Abilities	Login Method(s)
Admin Users		
admin	Change ZyWALL/USG/VPN/ATP configuration (web, CLI)	WWW, TELNET, SSH, FTP, Console
limited-admin	Look at ZyWALL/USG/VPN/ATP configuration (web, CLI) Perform basic diagnostics (CLI)	WWW, TELNET, SSH, Console
Access Users		
user	Access network services Browser user-mode command (CLI)	WWW, TELNET, SSH
guest	Access network services	WWW
ext-user	External user account	WWW
ext-group-user	External group user account	WWW
guest-manager	Create dynamic guest accounts	WWW

# Web GUI of User/Group (1/2)

- 設定 > 物件 > 使用者/群組
  - 新增使用者



The screenshot shows a web browser window titled "Add A User". The window contains a "User Configuration" section with the following fields and options:

- User Name :
- User Type:  (dropdown menu)
- Password:
- Retype:
- Description:
- Authentication Timeout Settings:
  - Use Default Settings
  - Use Manual Settings
- Lease Time: 1440 minutes
- Reauthentication Time: 1440 minutes

At the bottom right of the window, there are "OK" and "Cancel" buttons.

# Web GUI of User/Group (2/2)

- 設定 > 物件 > 使用者/群組
  - 新增使用者群組

**Add Group**

**Configuration**

Name:

Description:  (Optional)

**Member List**

Available	Member
=== Object ===	=== Object ===
ad-users	usera
billing-users	userb
ldap-users	
radius-users	
trial-users	
ua-users	

OK Cancel

# AP Profile

03



# Agenda

---

01

**AP**控管介紹

02

情境

03

佈建

# AP控管介紹(1/3)

- 內建無線控制器功能
  - AP 管理通訊協定 CAPWAP
  - 預設可控管 8 顆 AP （在不額外加購 AP License 的情況下）
- **ZyWALL/USG series**

ZLD 4.60	USG40(W) USG60(W)	USG110 USG210 ZyWALL110	USG310 Zywall310	USG1100 Zywall1100	USG1900	USG2200
Default (free)	8	8	8	8	8	8
Maximum	24	40	72	136	520	1032
License upgrade	Add 2/4/8 APs	Add 2/4/8 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs



# AP控管介紹(1/3)

- **USG FLEX/ATP series**

ZLD 4.60	ATP100(W) USG FLEX 100(W)	ATP200 USG FLEX 200	ATP500 USG FLEX 500	ATP700 USG FLEX 700	ATP800
Default (free)	8	8	8	8	8
Maximum	24	40	72	264	1032
License upgrade	Add 2/4/8 APs	Add 2/4/8 APs	Add 2/4/8 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs

# AP控管介紹(2/3)

- VPN series

ZLD 4.35	VPN50	VPN100	VPN300	VPN1000
Default (free)	8	8	8	8
Maximum	40	72	264	1032
License upgrade	Add 2/4/8 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs	Add 2/4/8/64 APs

# AP控管介紹(3/3)

- 內建 **WLAN** 控制器
  - 支援的 AP 型號

ZLD4.60	Supported Managed AP
ZyWALL/USG/USG FLEX/VPN/ATP	NWA3160-N NWA3550-N NWA3560-N NWA5160N NWA5550-N NWA5560-N NWA5121-NI NWA5123-NI NWA5121-N NWA5301-NJ WAC6502D-E WAC6502D-S WAC6503D-S WAC6553D-E WAC6103D-I NWA5123-AC WAC5302D-S NWA5123-AC HD WAC6303D-S WAC6552D-S WAX650S WAX510D WAX610D*

\* Compatible APs

# 無線控制器功能(1/4)

- 使用 ZyWALL/USG/VPN/ATP 管理 AP
- AP 註冊類型
  - Manual 手動
  - Always accept 必定接受



# 無線控制器功能(2/4)

- 註冊類型 **Always Accept**

- AP 連線控制器後，控制器自動把 AP 加到 Mgnt AP list

#	IP Address	MAC Address	Model	R1 Mode / Profile / ZyMesh Profile	Group	Mgnt. VL...	Mgnt. VL...	Description	R2 Mode / Profile / ZyMesh Prof...
1	192.168.1.33	A0:E4:CB:7C:FB:A0	WAC6503D-S	AP / default / -	default	1	0	AP-A0E4CB7CFBA0	AP / default2 / -

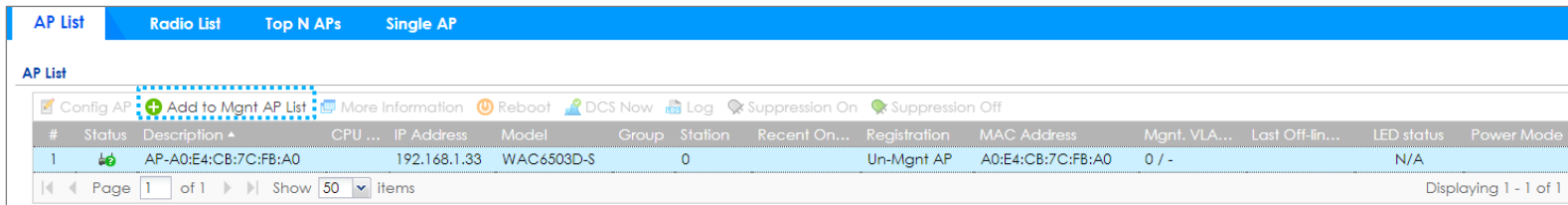
- Monitor / AP List

#	狀態	描述	CPU 使用量	IP 位址	MAC 位址	站台 2.4G	站台 5G	最近上線時間
1	✓	AP-B8ECA3B5236C	32 %	192.168.1.34	B8:EC:A3:B5:23:6C	0	0	Tue Mar 23 2021 11:4...

# 無線控制器功能(3/4)

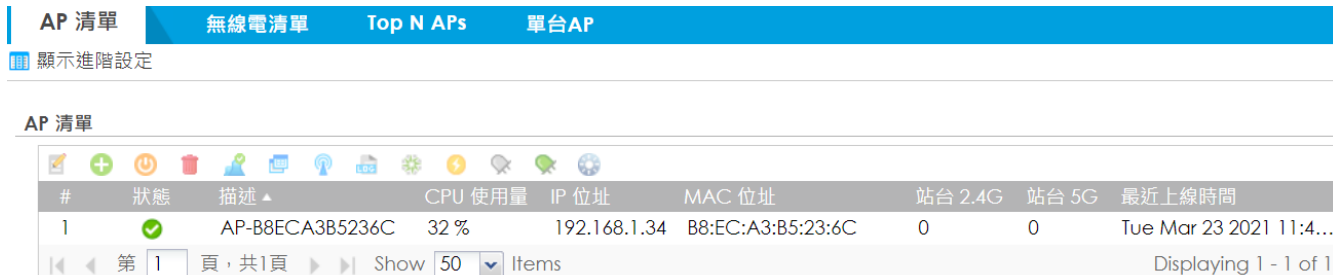
- 註冊型式 **Manual**

- 監控 > 無線 > AP 資訊
- AP 連線控制器後，管理者須手動把 AP 加入 Mgmt AP List



#	Status	Description	CPU ...	IP Address	Model	Group	Station	Recent On...	Registration	MAC Address	Mgmt. VLA...	Last Off-fn...	LED status	Power Mode
1	on-line	AP-A0:E4:CB:7C:FB:A0		192.168.1.33	WAC6503D-S		0		Un-Mgmt AP	A0:E4:CB:7C:FB:A0	0 / -		N/A	

- 手動加入後才會成為 on-line AP



#	狀態	描述	CPU 使用量	IP 位址	MAC 位址	站台 2.4G	站台 5G	最近上線時間
1	on-line	AP-B8ECA3B5236C	32 %	192.168.1.34	B8:EC:A3:B5:23:6C	0	0	Tue Mar 23 2021 11:4...

# 無線控制器功能(4/4)

- 設定 AP Profile

- 設定 > 物件 > AP 設定組合

- Radio profile

- SSID

- SSID list

- Security List

- MAC Filter List

The screenshot shows a web-based configuration interface for wireless settings. On the left is a navigation menu with the following items: 設定 (Settings), + 網路 (Network), + VPN, - BWM, - Web 認證 (Web Authentication), + 安全性策略 (Security Policy), + 安全服務 (Security Service), - 物件 (Objects), - 區域 (Zone), - 使用者/群組 (User/Group), - AP 設定組合 (AP Configuration Profile), - MON 設定組合 (MON Configuration Profile), and - ZyMesh 設定組合 (ZyMesh Configuration Profile). The 'AP 設定組合' item is selected and highlighted in blue.

The main content area is titled '無線電' (Wireless) and 'SSID'. Below the title is a '無線電摘要' (Wireless Summary) section. It includes a toolbar with icons for '新增' (Add), '編輯' (Edit), '移除' (Remove), '啟動' (Start), '停用' (Stop), and '物件參考' (Object Reference). Below the toolbar is a table with the following data:

#	狀態	設定組合名稱 ▲	頻帶	排程
1	🔆	default	2.4G	none
2	🔆	default2	5G	none
3	💡	Disabled-2G	2.4G	none
4	💡	Disabled-5G	5G	none

At the bottom of the table, there is a pagination control showing '第 1 頁, 共 1 頁' (Page 1 of 1), '每頁顯示 50 行' (Show 50 rows per page), and '顯示 1 - 4 之 4' (Showing 1 - 4 of 4).

# Address

05





# Agenda

---

01

**Address**  
物件設定

02

**Address Group**  
設定

# Address

- 設定 > 物件 > 位址/Geo IP > 位址

The screenshot displays the 'Address' configuration page in the ZyXEL management console. The left sidebar shows the navigation menu with '設定' (Settings) expanded to '物件' (Objects) > '位址/Geo IP' (Addresses/Geo IP). The main content area is titled 'IPv4 位址設定' (IPv4 Address Settings) and contains a table of existing address rules. A modal dialog box titled 'Add Address Rule' is open, showing the process of creating a new rule. The 'Name' field is set to 'PC', the 'Address Type' dropdown is set to 'HOST', and the 'IP Address' field contains '192.168.1.33'. A dropdown menu is open next to the 'Address Type' field, listing various options: HOST, RANGE, SUBNET, INTERFACE IP, INTERFACE SUBNET, INTERFACE, GATEWAY, GEOGRAPHY, and FQDN. The 'HOST' option is currently selected.

#	名稱	類型	IPv4 位址	參考
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24	0
2	IP6to4-Relay	HOST	192.88.99.1	0
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24	0
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	0
5	RFC1918_1	SUBNET	10.0.0.0/8	1
6	RFC1918_2	SUBNET	172.16.0.0/12	1
7	RFC1918_3	SUBNET	192.168.0.0/16	1

IPv4 位址設定

新增 編輯 移除 物件參考

第 1 頁, 共 1 頁 每頁顯示 50

**Add Address Rule**

Name: PC

Address Type: HOST

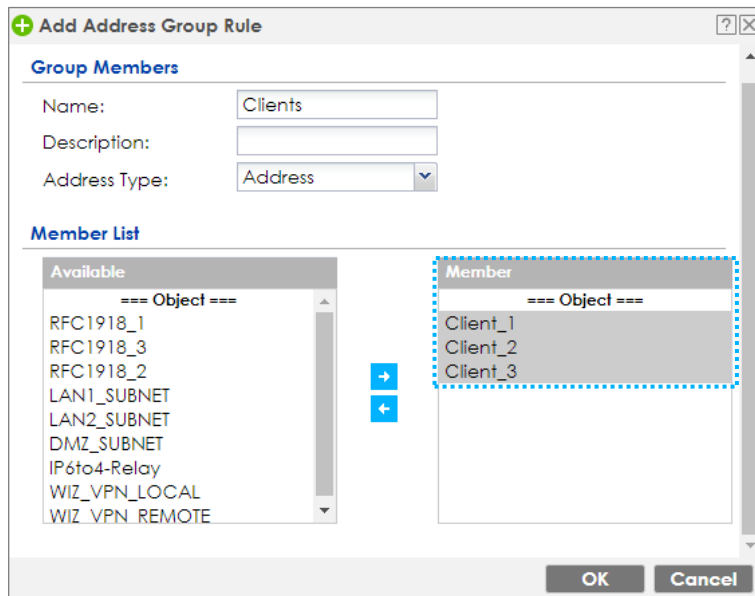
IP Address: 192.168.1.33

HOST  
RANGE  
SUBNET  
INTERFACE IP  
INTERFACE SUBNET  
INTERFACE  
GATEWAY  
GEOGRAPHY  
FQDN

OK Cancel

# Address Group

- Address Group
  - 選擇並群組 IP 物件



# Geo IP

- **Geo IP** 將 IP 位址依其地理位置(國家、區域)進行分類，提供作為安全政策使用
- 需要 **Content Filter license** 才能使用

The screenshot displays the configuration interface for Geo IP. On the left is a sidebar with navigation icons and a menu. The main area has tabs for '位址', '位址群組', and 'Geo IP'. Below the 'Geo IP' tab, there's a section for 'IPv4 位址設定' with a table of rules. A modal window is open for adding a new rule.

Setting menu items: 設定, + 網路, + VPN, - BWM, - Web 認證, + 安全性策略, + 安全服務, 物件, - 區域, - 使用者/群組, - AP 設定組合, - MON 設定組合, - ZyMesh 設定組合, **位址/Geo IP**, - 服務, - 排程

IPv4 位址設定

新增 編輯 移除 物件參考

#	名稱	類型	IPv4 位址	參考
1	DMZ_SUBNET	新增位址規則		
2	IP6to4-Relay			
3	LAN1_SUBNET			
4	LAN2_SUBNET			
5	RFC1918_1			
6	RFC1918_2			
7	RFC1918_3			

新增位址規則

名稱: Taiwan

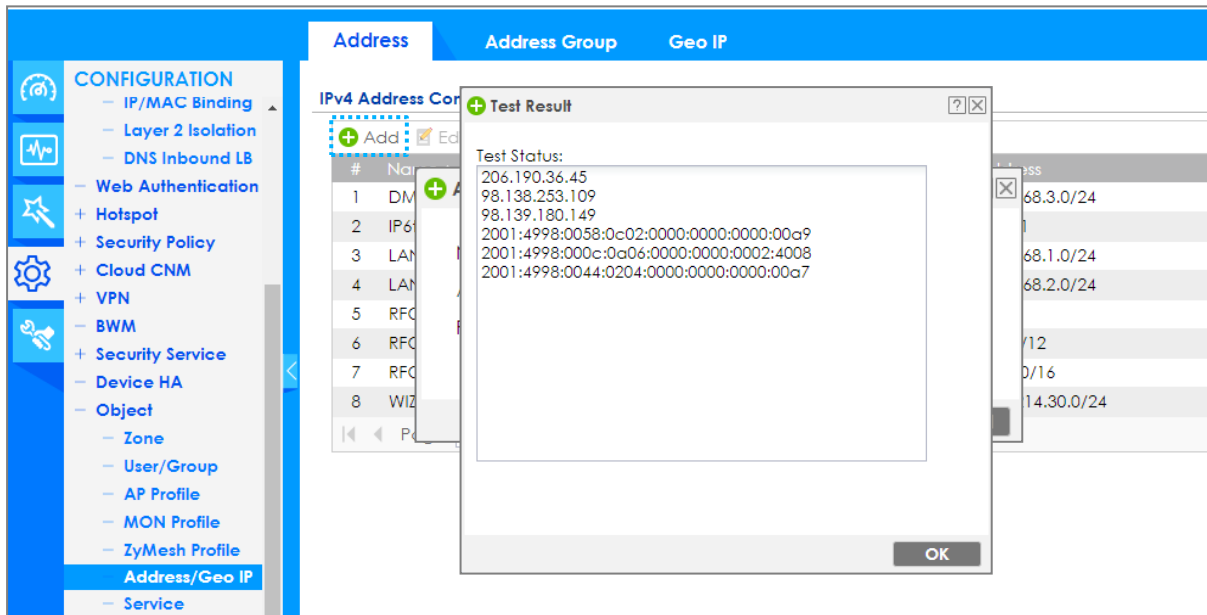
位址類型: GEOGRAPHY

地區: Taiwan

OK Cancel

# FQDN 物件

- FQDN 位址物件



# Wildcard FQDN Object

- FQDN pattern supports wildcard



The screenshot shows a dialog box titled "Add Address Rule" with a green plus icon on the left and help and close icons on the right. The dialog contains three input fields: "Name:" with the text "google", "Address Type:" with a dropdown menu set to "FQDN", and "FQDN:" with the text "\*.google.com". A "Test" button is located to the right of the FQDN field. At the bottom of the dialog are "OK" and "Cancel" buttons.

# Service



# Agenda

---

01

**Service**

物件介紹

02

**Service**

物件設定



# Service

- **IP 通訊協定**
  - TCP Application ( Transmission Control Protocol, IP protocol 6 )
  - UDP Application ( User Datagram Protocol, IP protocol 17 )
  - ICMP Message ( Internet Control Message Protocol, IP protocol 1 )
  - User-Defined Services

# Service 物件設定(1/2)

- 設定 > 物件 > 服務
  - Add one service

Service		Service Group	
Configuration			
+ Add Edit Remove Object References			
#	Name ^	Content	Reference
1	AH	Protocol=51	2
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	Any_TCP	TCP/1-65535	0
5	Any_UDP	UDP/1-65535	0
6	BGP	TCP=179	0

+ Add Service Rule

Name: service

IP Protocol: TCP

Starting Port: 8888

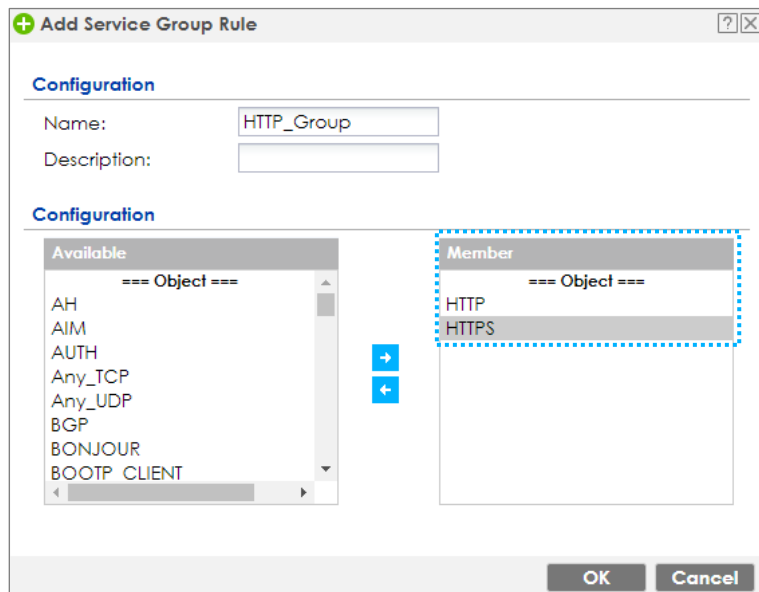
Ending Port: 8888

TCP  
UDP  
ICMP  
ICMPv6  
User Defined

OK Cancel

# Service 物件設定 (2/2)

- 設定 > 物件 > 服務 > 服務群組
  - 將服務加入群組



# BWM

# Outline

---

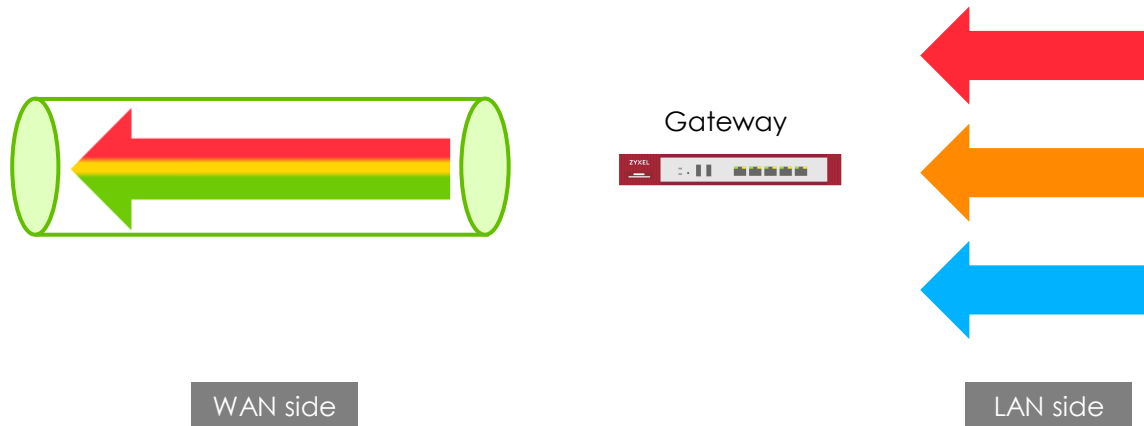
01  
**BMW**  
功能介紹

02  
**BMW** 設定

03  
**BMW** 限制

# 為何使用 BWM?

- 有效的限制頻寬使用
- 幫助排定流量優先順序



# BWM

- 啟用 BWM
  - 須先啟用全域性的頻寬管理總開關
  - 設定 > BWM

**BWM**

頻寬管理總開關

啟用 BWM

為 SIP 流量啟動最高的頻寬優先權 [i](#)

設定

+ 新增   編輯   移除   啟動   停用   移動

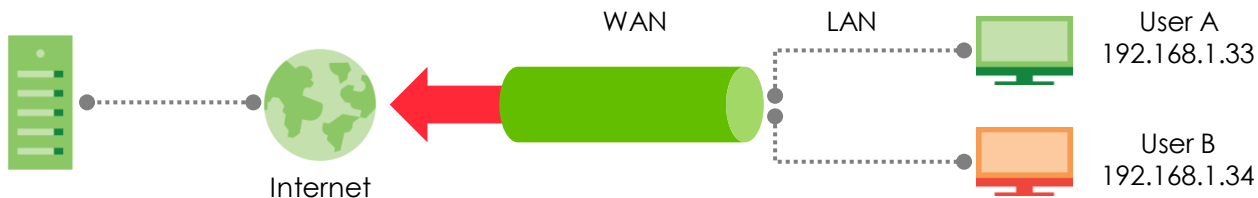
狀態	優先權	描述	BWM 類型	使用者	排程	內送介面	外送介面	來源	目的地	DSCP 代碼	服務	BWM 進向/優先權/出向優先權	DSCP ...
		default	shared	any	none	any	any	any	any	any	any	no/7/no/7	preserv...

第 1 頁，共 1 頁   每頁顯示 50 行   顯示 1 - 1 之 1

# BWM 類型 (1/3)

- **BWM type: Shared**

- 所有 IP/users 共享指定頻寬

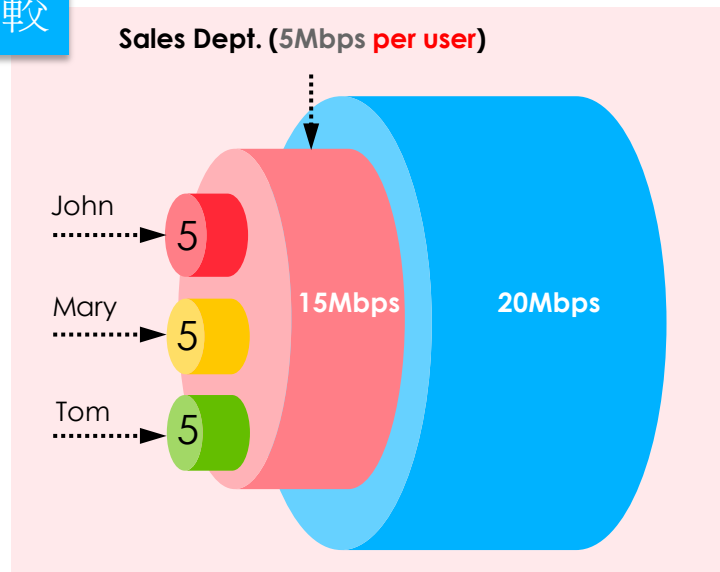
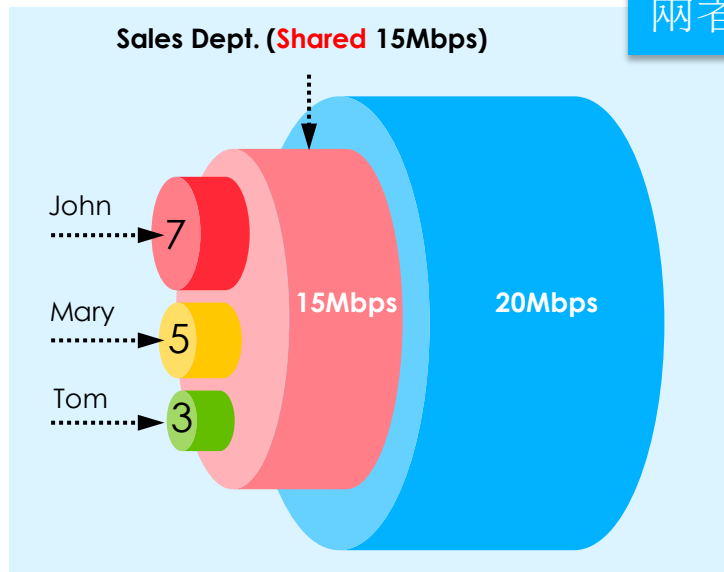




# BWM 類型 (2/3)

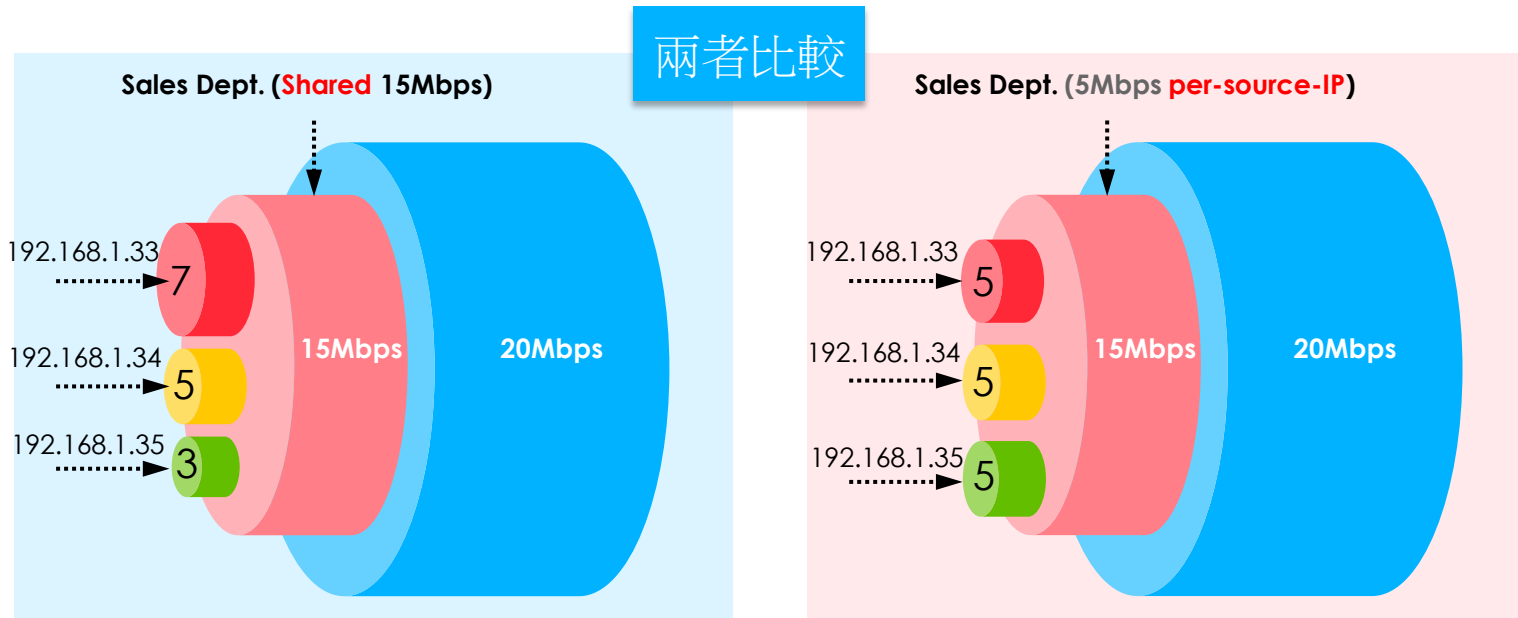
- BWM type: per-user

兩者比較



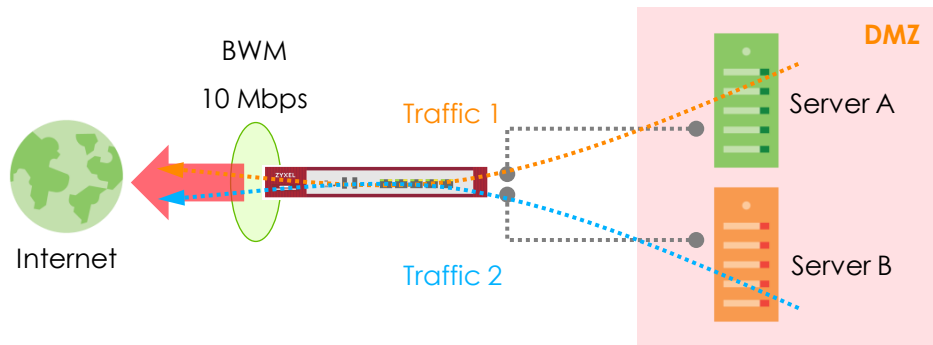
# BWM Type (3/3)

- BWM type: Per-Source-IP



# 排定優先順序的 BWM (1/5)

- 2 組不同的資料流量透過**Gateway**傳送，對外可用總頻寬為**10Mbps**.
- 2 組資料流量皆以 **100Mbps** 速度進行傳送
- **Gateway** 將控制進入的流量.



# 排定優先順序的 BWM (2/5)

- **Case 1: 限制速率**

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	7	No	1	7
T2	2	No	1	2

- **Case 2: 相同的速率限制，並且各別開啟最大頻寬使用功能**

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	5	Yes	1	5
T2	5	Yes	1	5

Max. means Maximize Bandwidth Usage

# 排定優先順序的 BWM (3/5)

- **Case 3: 皆限速 2Mbps, T1 啟用 Max. BW Usage**

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	2	Yes	1	2 + 6
T2	2	No	1	2

- **Case 4: 皆限速 5Mbps, 啟用 Max. BW Usage**

- T2: 目前傳送速率僅使用 2Mbps 時

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	5	Yes	1	5 + 3
T2	5	Yes	1	2

Max. means Maximize Bandwidth Usage

# 排定優先順序的 BWM (4/5)

- Case 5: BW Priority

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	8	Yes	1	8
T2	10	Yes	2	2

- Case 6: 高優先權流量永遠先被傳送

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	10	Yes	1	9.99
T2	10	Yes	2	≐ 0.01

Max. means Maximize Bandwidth Usage

# 排定優先順序的 BWM (5/5)

- **Case 7: Incoming Rate over the limit of all available BW**

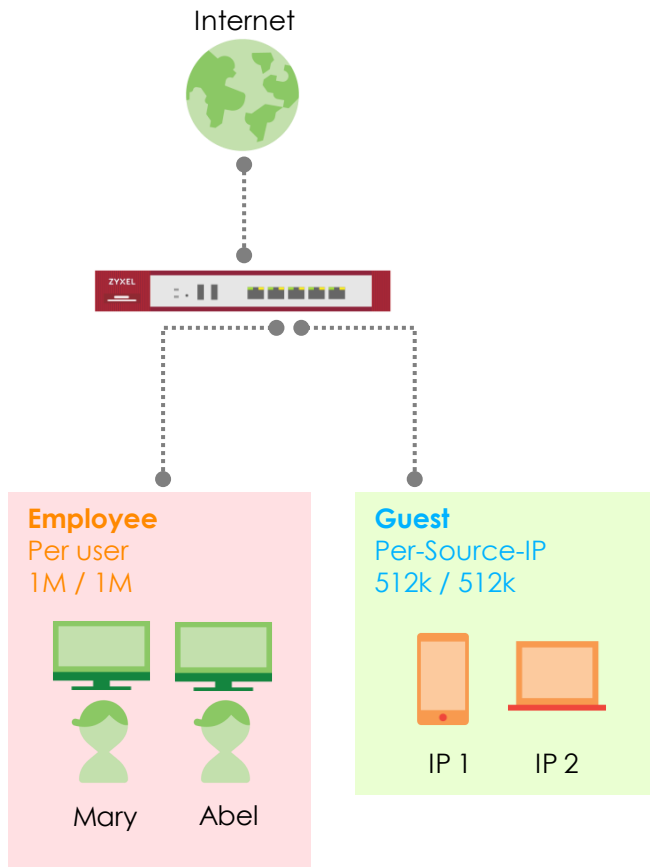
Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	40	No	1	6.6
T2	20	No	1	3.3

- **Case 8: Maximize Bandwidth Usage**

Traffic	Rate	Max. BW Usage	Priority	Client Result
T1	2	Yes	1	2 + 0~4
T2	4	Yes	2	4 + 0~4

Max. means Maximize Bandwidth Usage

# 情境範例



Note. 一種BWM類型只能應用在一個Subnet



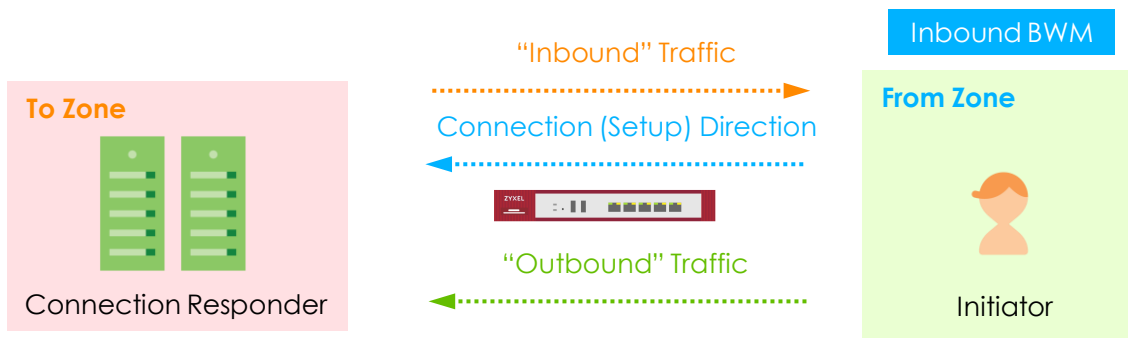
# BWM 設定

- **BWM 提供 Shared/ Per user / Per-Source-IP 三類**
  - 預設是 Shared
  - Per-source IP: 每個 IP 擁有相同的頻寬配置
  - Per user: 每個登入的使用者擁有相同的頻寬配置
  - 設定 > **BWM 新增/編輯**

The screenshot displays the BWM Configuration page. It features a 'Configuration' section with an 'Enable' checkbox checked, a 'Description' field, and three radio buttons for 'BWM Type': 'Shared' (selected), 'Per user', and 'Per-Source-IP'. A blue dashed box highlights the 'BWM Type' section. Below this is the 'Criteria' section, which includes dropdown menus for 'User', 'Schedule', 'Incoming Interface', 'Outgoing Interface', 'Source', 'Destination', 'DSCP Code', 'Service Type' (set to 'service-object'), and 'Service Object'.

# BWM 設定

- **outbound & inbound** 的定義
  - By connection initiator
    - Initiator → Responder: Outbound
    - Responder → Initiator: Inbound



# BWM 設定

- 設定 > BWM

**Edit Policy**

Create new Object ▾

**Criteria**

User: any ▾  
Schedule: none ▾  
Incoming Interface: any ▾  
Outgoing Interface: any ▾  
Source: PC ▾  
Destination: any ▾  
DSCP Code: any ▾  
Service Type:  Service Object  Application Object  
Application Object: BitTorrent ▾

**DSCP Marking**

DSCP Marking Inbound Marking: preserve ▾  
Outbound Marking: preserve ▾

**Bandwidth Shaping**

Guaranteed Bandwidth Inbound: 64 kbps (0 : disabled) Priority: 4  
 Maximize Bandwidth Usage Maximum: 0 kbps  
Outbound: 64 kbps (0 : disabled) Priority: 4  
 Maximize Bandwidth Usage Maximum: 0 kbps

OK Cancel

Configure how much bandwidth can use.

# Security Policy



# Agenda

---

01

**Types of  
Firewalls**

02

**Unified Security  
Policy**

03

**Configuration  
Flow**

# Types of Firewalls

- **Packet filter firewall (Layer 3)**

- 依據封包表頭的來源/目的位址進行檢查過濾

- **Stateful inspection firewall (Layer 4)**

- 不僅僅檢查 IP 表頭的來源/目的位址，還檢查了部份應用層的資訊如下：

- TCP Session state

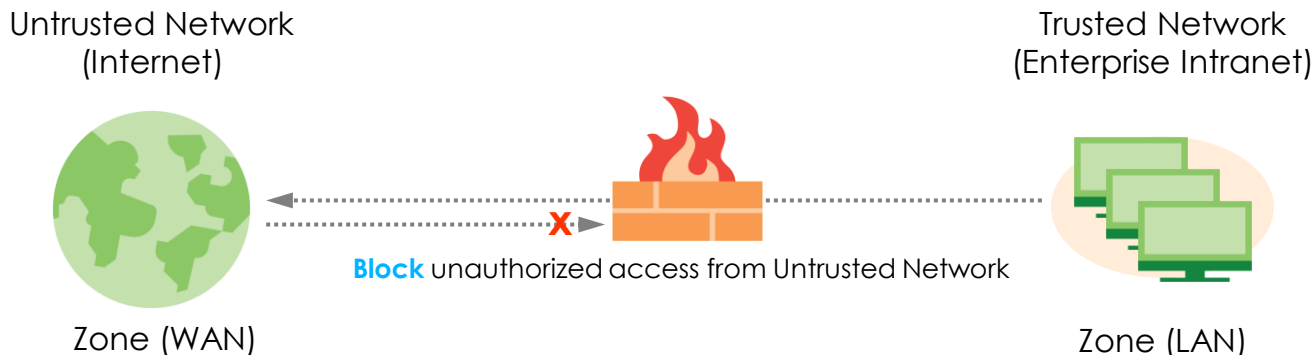
- TCP Sequence number

- **Application Proxy (Layer 7)**

- 檢查並分辨應用層的內容(如：應用程式類型)

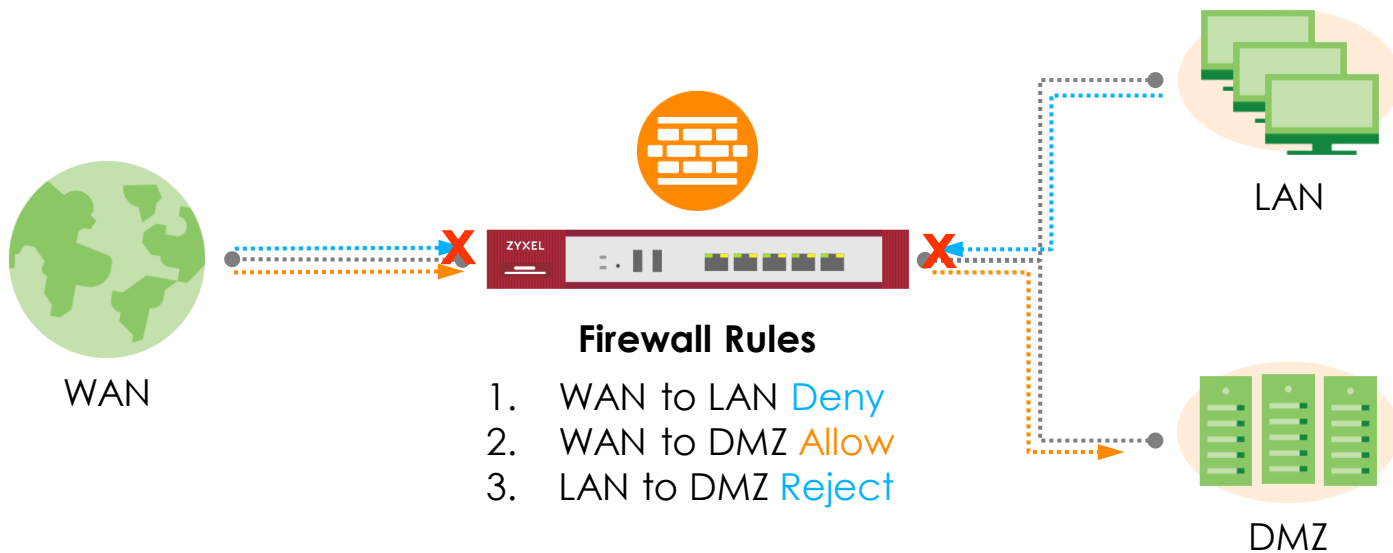
# Firewall

- 透過防火牆規則對來自於不同 **Zone** 區域的連線進行 **Allow**、**Deny** 或 **Reject** 的管理
  - In ZLD, we call this “**安全性策略 Security Policy**”



# Zone Protection

- **Firewall** 透過控制 **ZONE** 之間的 **Traffic** 提供防護





# 預設安全性策略

- Directional security policy behavior



# 整合的 Security Policy (1/2)

- 將 **Firewall** 規則與 **UTM** 規則整合成為單一控制規則



## Firewall Rules

- Zone
- Source IP
- Destination IP
- Destination port
- User
- Time

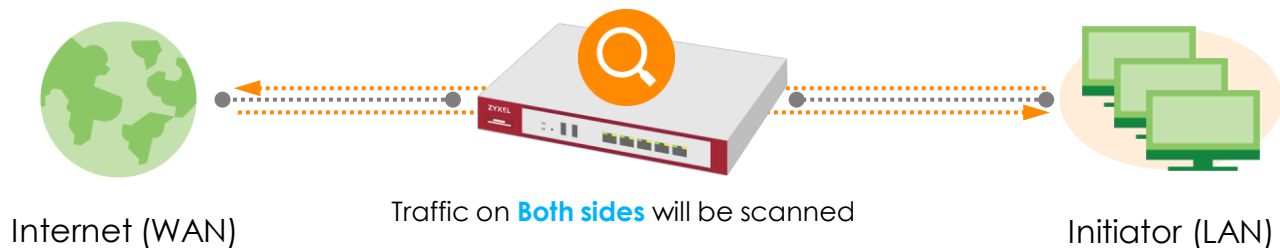


## UTM Profiles

- App. Intelligence
- Content Filtering
- SSL Inspection

# 整合的 Security Policy(2/2)

- 依據連線發起端來制訂規則
  - From : LAN
  - To : WAN
- 符合條件時，雙向資料流會被自動檢驗



# UTM Profile



# Agenda

---

01  
**Application  
Patrol**

02  
**Content Filter**

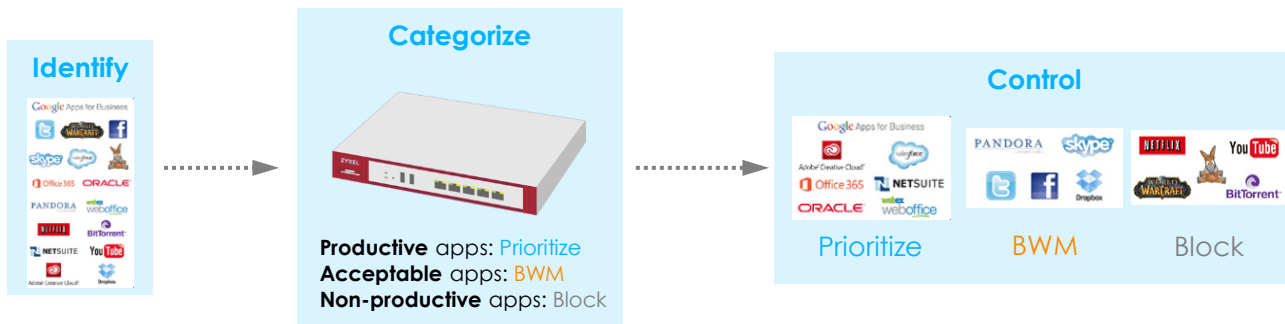
03  
**SSL Inspection**

# Application Patrol

- **Application Patrol** 介紹
- **App Patrol** 設定頁面
- **App Patrol** 範例

# 什麼是 APP Patrol?

- 具彈性且能細分、嚴謹的控制
  - 辨識、分類並控管多達 3,000 種以上的 Web 應用與行為
  - 多樣化的控管: 優先權、阻擋
  - 有效的針對 social media, gaming, P2P and other Web apps 執行控管.
- 特徵碼更新 → 每週更新



# App Patrol 設定頁面 (1/3)

- App Patrol profile management page

設定

安全服務

應用程式巡査

Add profile

The screenshot displays the 'App Patrol' interface with a 'Profile Management' sidebar on the left and a main content area. The 'Add Rule APP7351' dialog box is open, showing 'General Settings' (Name: Game, Description: ) and 'Profile Management' (My Application, Query Result). The 'Query Application' section is active, showing a search for applications by category. The 'Query Result' table is visible, listing applications like 'akinator', 'all\_slots\_casino', 'angry\_birds', and 'anipang'. The 'Add To My Application' button is highlighted at the bottom of the dialog.

#	Application	Category	Tag	Action	Log
1	akinator	Game	mobile gaming	forward	log
2	all_slots_casino	Game	web gaming	forward	log
3	angry_birds	Game	mobile gaming	forward	log
4	anipang	Game	mobile gaming	forward	log

Select applications

Add selected apps to profile



# App Patrol 設定頁面 (2/3)

- App Patrol profile management page

設定

安全服務

應用程式巡查

The screenshot displays the 'App Patrol' interface. At the top, there's a header 'App Patrol' and a sub-header 'Profile Management' with the 'Application Patrol' logo. Below this, there are navigation icons: '+ Add', 'Edit', 'Remove', and 'References'. A table lists two profiles:

#	Name	Description	Reference	Action
1	default_profile		0	
2	Game		0	

Below the table, there are navigation controls: 'Page 1 of 1', 'Show 50 items', and 'Displaying 1 - 2 of 2'. On the left, there's a 'Signature Information' section with details: 'Current Version: 1.0.0.2', 'Signature Number: 3147', and 'Released Date: 2018-0'. There's also a link 'Update Signatures'. An 'Info' dialog box is open in the center, containing a question mark icon and the text: 'Profile Game has been saved. A profile takes effect only when it is applied to a security policy. Apply this profile to a security policy now?'. The dialog has 'Yes' and 'No' buttons. A blue callout box at the bottom of the dialog says 'Select Yes to apply to a security policy'.

# App Patrol 設定頁面 (3/3)

- App Patrol profile management page

設定

安全服務

應用程式巡查

Apply Game to a security policy

Show Filter

IPv4 Configuration

Select security policy to apply

Pri...	Sta...	Name	From	To	IPv4 Source	IPv4 Destin...	Service	User	Schedule	Ac...	Log
<input checked="" type="checkbox"/>	1	LAN1_Outgoing	LAN1	any (Exclu...	any	any	any	any	none	all...	no
<input type="checkbox"/>	2	LAN2_Outgoing	LAN2	any (Exclu...	any	any	any	any	none	all...	no
<input type="checkbox"/>	3	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	all...	no
<input type="checkbox"/>	4	IPSec_VPN_Outg...	IPSec_VPN	any (Exclu...	any	any	any	any	none	all...	no
<input type="checkbox"/>	5	SSL_VPN_Outgoing	SSL_VPN	any (Exclu...	any	any	any	any	none	all...	no
<input type="checkbox"/>	6	TUNNEL_Outgoing	TUNNEL	any (Exclu...	any	any	any	any	none	all...	no

Page 1 of 1 Show 50 items

Displaying 1 - 6 of 6

OK Cancel

# App Patrol 範例

- 使用 App Patrol 限制使用 Facebook



# Configure App Patrol (1/3)

設定

安全服務

應用程式巡查

Add App Patrol profile and add the application object

Select Action and Log

Apply the App Patrol profile to security policy

The screenshot displays the App Patrol configuration interface. The top section is titled "Profile Management" and contains a table with the following data:

#	Name	Description	Reference	Action
1	default_profile		0	
2	Game		1	

Below the table, there is a "Query Application" section with a search bar containing "facebook" and a "Search" button. The "Query Result" section shows a list of applications with the following data:

#	Application	Category	Tag	Action	Log
1	facebook_live	Audio/Video	web mm_streaming	forward	log
2	facebook_messenger	Instant Messaging	im_mc_file_transfer social_net...	forward	log
3	facebook	Web	im_mc chat social_network w...	forward	log
4	facebook_Login	Web	im_mc chat social_network w...	forward	log
5	facebook_apps	Web	social_network web mobile g...	forward	log
6	facebook_video	Web	social_network web mm_stre...	forward	log
7	facebook_mail	Webmail	webmail social_network web	forward	log

# Configure App Patrol (2/3)

設定

安全服務

應用程式巡查

Add App Patrol profile and add the application object

Select Action and Log

Apply the App Patrol profile to security policy

The screenshot shows the 'Add Rule APP9939' configuration window. The 'My Application Rule' section is active, displaying a table of application rules. The table has columns for '#', 'Application', 'Category', 'Tag', 'Action', and 'Log'. The 6th row, 'facebook\_video', is selected, and its 'Action' and 'Log' dropdown menus are open, showing 'drop' and 'log alert' respectively. The 'Log' dropdown is highlighted with a blue dashed border.

#	Application	Category	Tag	Action	Log
1	facebook_live	Audio/Video	web mm_streaming	drop	log alert
2	facebook_messenger	Instant Messaging	im_mc file_transfer social_net...	drop	log alert
3	facebook	Web	im_mc chat social_network we...	drop	log alert
4	facebook_login	Web	im_mc chat social_network we...	drop	log alert
5	facebook_apps	Web	social_network web mobile ga...	drop	log alert
6	facebook_video	Web	social_network web mm_strea...	drop	log alert
7	facebook_mail	Webmail	webmail social_network web	forward drop reject	log alert playing 1 - 7 of 7

# Configure App Patrol (3/3)

設定

安全服務

應用程式巡查

Add App Patrol profile and add the application object

Select Action and Log

Apply the App Patrol profile to security policy

App Patrol

Profile Management

Application Patrol

Add Edit Remove References

#	Name	Description	Reference	Action
1	default_profile		0	
2	Game		1	
3	Facebook		0	

Page 1 of 1 Show 50 items

Displaying 1 - 3 of 3

Apply Facebook to a security policy

Show Filter

IPv4 Configuration

Pri...	St...	Name	From	To	IPv4 Sour...	IPv4 Des...	Service	User	Schedule	A...	Log
1		LAN1_Outgoing	LAN1	any (Exc...	any	any	any	any	none	all...	no
2		LAN2_Outgoing	LAN2	any (Exc...	any	any	any	any	none	all...	no
3		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	all...	no
4		IPSec_VPN_Out...	IPSec_...	any (Exc...	any	any	any	any	none	all...	no
5		SSL_VPN_Outgo...	SSL_VPN	any (Exc...	any	any	any	any	none	all...	no
6		TUNNEL_Outgo...	TUNNEL	any (Exc...	any	any	any	any	none	all...	no

Page 1 of 1 Show 50 items

Displaying 1 - 6 of 6

OK Cancel

# Content Filter

- 什麼是Content Filter?
- Content Filter 的設定
- Content Filter 範例

# 什麼是 Content Filter?

- 依據網站內容進行分級與分類管理
- 避免使用者存取不安全或未經授權的網站
- 依據設定配置進行放行、阻擋或警告

## Search Engine

- AOL
- Google
- YAHOO

## Malware Phishing





# Content Filter 的設定 (1/2)

- Content Filter profile 管理頁面

設定

安全服務

內容過濾

設定組合

**Profile** Trusted Web Sites Forbidden Web Sites

General Settings [Configuration Walkthrough](#) [Troubleshooting](#) [Content Filter](#)

- Enable HTTPS Domain Filter for HTTPS traffic
- Drop connection when HTTPS connection with SSL V3 or previous version
- Content Filter Category Service Timeout:  (1~60 Seconds)

**Message to display when a site is blocked**

Denied Access Message:

Redirect URL:

**Profile Management**

[Add](#) [Edit](#) [Remove](#) [Object References](#)

#	Name	Description	Reference
1	BPP	Business Productivity Protection	0
2	CIP	Children's Internet Protection	0
3	Filter_profile		

Page 1 of 1 Show 50 items

禁止瀏覽某個網頁時出現的訊息

Access Denied

Web access is restricted. Please contact the administrator. (Shopping)

Please link to <http://www.zyxel.com/homepage.shtml> for web access policy.

Edit Filter Profile BPP

編輯Profile

類別服務

自訂服務

一般設定

名稱:

描述:  (選擇性)

啟用SafeSearch

啟用內容過濾分級服務

記錄所有網頁存取

管理網頁採取的動作:

log

未分級網頁採取的動作:

log

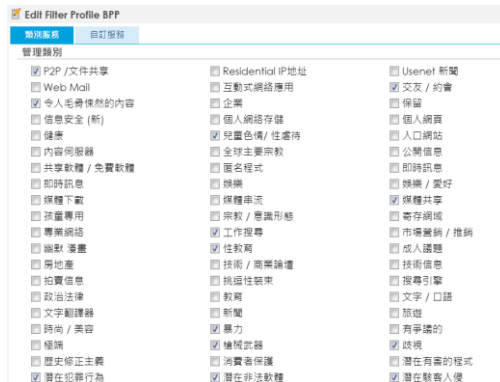
類別伺服器無回應時採取的動作:

log

ks

# Content Filter 的設定 (2/2)

- Content Filter profile configuration panel.



- 測試“URL”屬於哪個管理類別



# Content Filter 範例

- 使用 **Content Filter** 阻擋 **IGN** 及相同類型的網站
- 使用者嘗試存取這些網站會被阻擋，阻擋頁面並出現**ZYXEL** 官方網站的轉導連結

## Search Engine

- AOL
- Google
- YAHOO



# 設定 Content Filter (1/4)

設定

安全服務

內容過濾

設定組合

Configure the Redirect URL and Content Filter profile

Use "URL to test" function to check the website IGN's category.

Select the category on Managed Categories

Apply the Content Filter profile to security policy.

Check the Result

**Profile** | Trusted Web Sites | Forbidden Web Sites

**General Settings** | Configuration Walkthrough | Troubleshooting | Content Filter

- Enable HTTPS Domain Filter for HTTPS traffic ⓘ
- Drop connection when HTTPS connection with SSL V3 or previous version

Content Filter Category Service Timeout:  (1~60 Seconds)

**Message to display when a site is blocked**

Denied Access Message:

Redirect URL:

**Profile Management**

+ Add | Edit | Remove | Object References

#	Name ▲	Description	Reference
1	BPP	Business Productivity Protection	0
2	CIP	Children's Internet Protection	0
3	Filter_profile		1

Page 1 of 1 | Show 50 Items

# 設定 Content Filter (2/4)

設定

安全服務

內容過濾

設定組合

Configure the Redirect URL and Content Filter profile

Use "URL to test" function to check the website IGN's category.

Select the category on Managed Categories

Apply the Content Filter profile to security policy.

Check the Result

**Test Web Site Category**

URL to test:

**Test Against Content Filter Category Server**

[If you think the category is incorrect, click this link to submit a request to review it.](#)

**Message**

Content Filter Category: Games  
HTTPS Domain Filter Category: Games

**OK**

**Managed Categories**

<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol/Tobacco	<input type="checkbox"/> Arts
<input type="checkbox"/> Business	<input type="checkbox"/> Transportation	<input type="checkbox"/> Chat
<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Education
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Finance	<input type="checkbox"/> Gambling
<input checked="" type="checkbox"/> Games	<input type="checkbox"/> Government	<input type="checkbox"/> Hate & Intolerance
<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Job Search
<input type="checkbox"/> Streaming Media & Downloads	<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs
<input type="checkbox"/> Nudity	<input type="checkbox"/> Personal Sites	<input type="checkbox"/> Politics
<input type="checkbox"/> Pornography/Sexually Explicit	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion

# 設定 Content Filter (3/4)

設定

安全性策略

策略控制

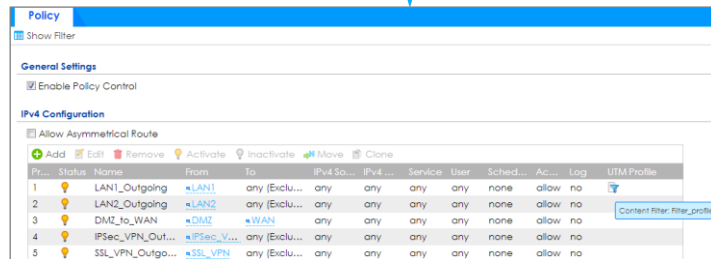
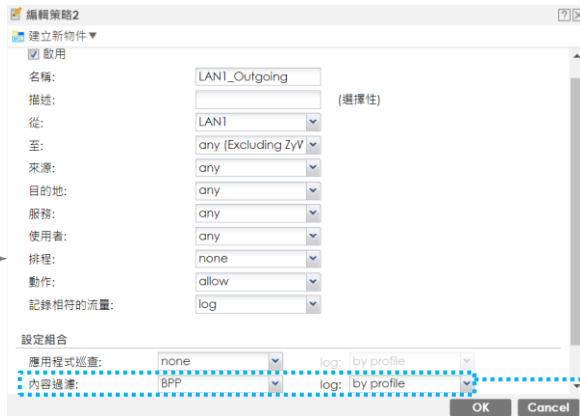
Configure the Redirect URL and Content Filter profile

Use "URL to test" function to check the website IGN's category.

Select the category on Managed Categories

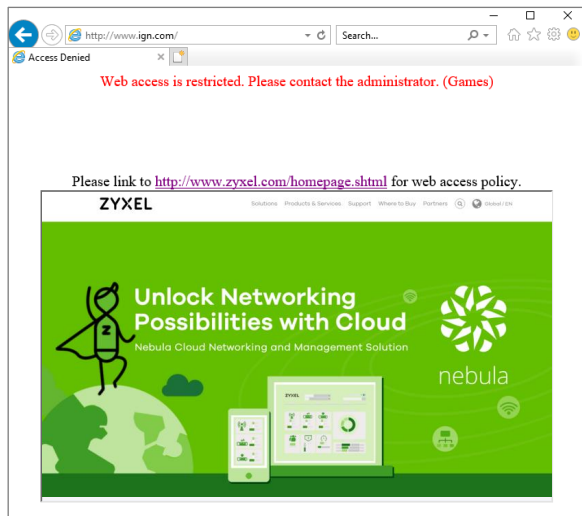
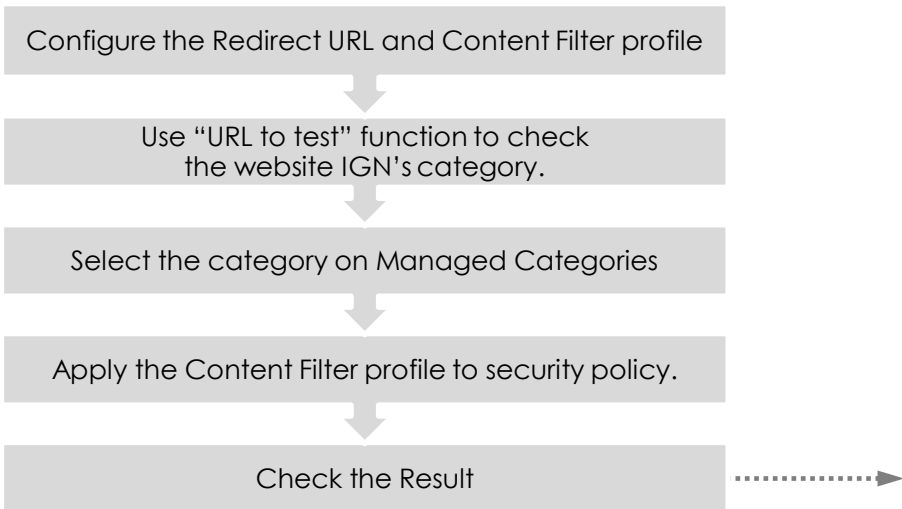
Apply the Content Filter profile to security policy.

Check the Result



# 設定 Content Filter (4/4)

- 使用者會看到禁止存取訊息並出現轉導的頁面



# Content Filter 2.0 加強對HTTPS網頁的控管

- **HTTPS Domain Filter**
- **Geo IP**

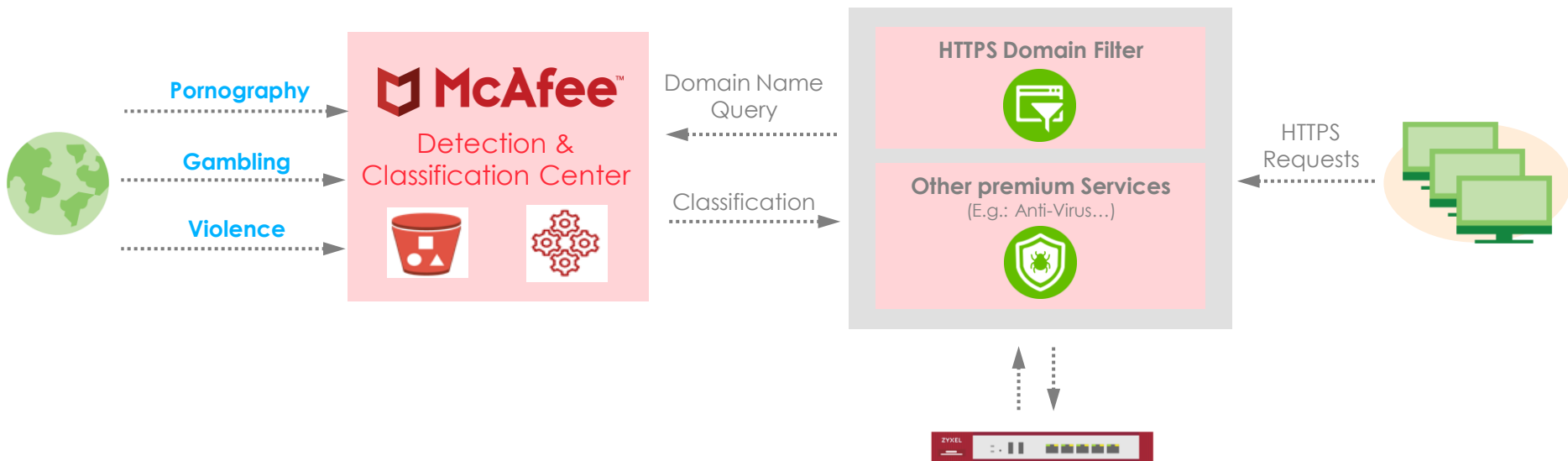


# HTTPS Domain Filter

- **HTTPS Domain Filter** 介紹
- **HTTPS Domain Filter** 設定

# HTTPS Domain Filter 應用情境

- 透過 HTTPS Domain Filter 功能過濾超過 105 種類型的 HTTPS 服務網站，例如：色情、賭博、暴力... 等



# HTTPS Domain Filter 介紹

- 需要 **Content Filter License**
- 辨識 **HTTPS 連線**
  - 不須啟用 SSL-Inspection
  - 專司於 HTTPS 的存取
- 透過分類, **ZyWALL/USG/VPN/ATP** 能夠阻擋不恰當或有疑慮的 **HTTPS 存取**
- 僅能檢查 **domain**, 而非整段 **URL**

# HTTPS Domain Filter 設定 (1/3)

- Content Filter general settings

設定 → 安全服務 → 內容過濾 → 設定組合 → 一般設定

設定組合: 信任/禁止網站

Content Filter

一般設定

- 啟用HTTPS 流量過濾  ⓘ
- 啟用HTTPS 內容過濾阻擋/警告
  - 阻擋/警示頁面:
- 使用SSL V3或更舊版本的SSL連接HTTPs時會斷線
- 內容過濾分級伺服器等候時間:  (1~60 秒數)

當封鎖網站時顯示的訊息

- 遭拒絕的存取訊息: [Web access is restricted. Please contact the administrator.](#)
- 重新導向 URL:

# HTTPS Domain Filter 設定 (2/3)

- Domain Query Tool



**Test Web Site Category**

URL to test:

**Test Against Content Filter Category Server**

[If you think the category is incorrect, click this link to submit a request to review it.](#)

**Message** [X]

Content Filter Category: Social Networking  
HTTPS Domain Filter Category: Social Networking

OK

# HTTPS Domain Filter 設定 (3/3)

- HTTPS Domain Filter Block/Warn Page

設定

安全服務

內容過濾

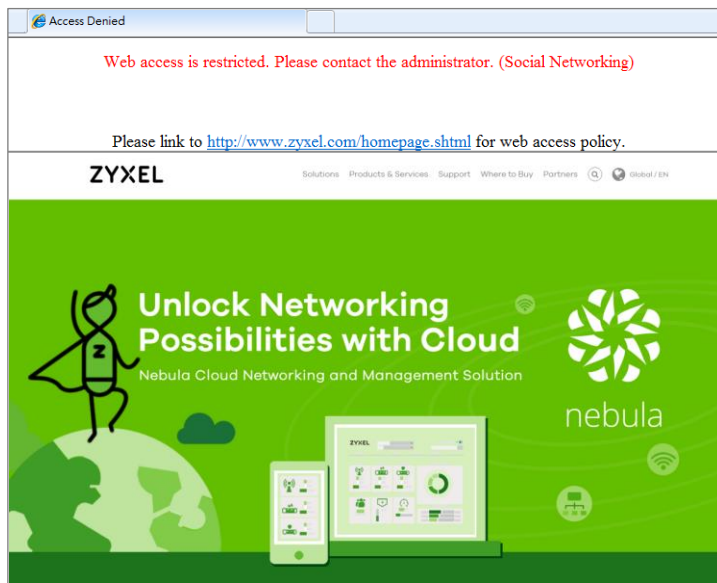
設定組合

The screenshot shows the configuration page for the 'Trust/Block Websites' (信任/禁止網站) profile. The left sidebar contains a navigation menu with 'Content Filter' (內容過濾) selected. The main content area is titled 'Content Filter' and includes the following settings:

- 啟用HTTPS 流量過濾 ⓘ
- 啟用HTTPS 內容過濾阻擋/警告
  - 阻擋/警示頁面: 54088
- 使用SSL V3或更舊版本的SSL連接HTTPS時會斷線
- 內容過濾分級伺服器等候時間: 10 (1~60 秒數)
- 當封鎖網站時顯示的訊息
  - 遭拒絕的存取訊息: [Web access is restricted. Please contact the administrator.](#)
  - 重新導向 URL:

# HTTPS Domain Filter 阻擋/告警頁面

- 輸入 <https://www.facebook.com>
  - HTTPS Domain Filter 顯示阻擋/告警



# HTTPS Domain Filter Logs

- Category: Blocked Website Logs



View Log View AP Log Dynamic Users Log

Show Filter

Logs

Category: Blocked web sites

Email Log Now Refresh Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	2018-01-13 04:12:...	alert	Blocked web sites	www.facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain Filter)	192.168.1.101:2968	31.13.87.36:443	WEB BLOCK
2	2018-01-13 04:12:...	alert	Blocked web sites	www.facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain Filter)	192.168.1.101:2962	31.13.87.36:443	WEB BLOCK

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Blocked web sites www.facebook.com : Social Networking, Rule\_id=1, SSI=N (HTTPS Domain Filter)

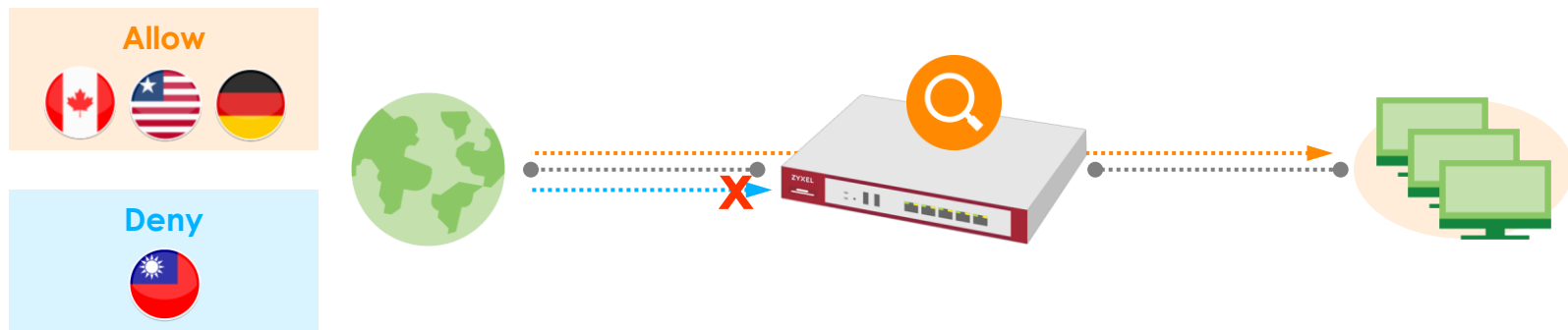


# Geo IP ( IP 地理位置)

- Geo IP 介紹
- Geo IP 設定

# Geo IP 使用情境

- 阻擋特定國家/洲 (continent) 流量
- 可自訂 IP 位址至指定的國家
  - 自訂 IP address/range/subnet 到指定國家
    - Ex: 設定 U.S IP 8.8.4.4 屬於台灣. 當防火牆設定阻擋來/去台灣的流量時, 則 8.8.4.4 也會被阻擋.



# Geo IP 功能介紹

- **Geo IP** 可以辨識網際網路上的使用者所在地理區域.
- **MaxMind** 資料庫提供幾近 **100%** 準確率的 **IP** 地理位置資料庫並每週進行更新.
  - 例如:
    - 8.8.8.8 位於美國的 IP
    - 168.95.1.1 位於台灣的 IP
    - 131.111.150.25 位於英國的 IP
    - 203.32.178.10 位於澳洲的 IP



# Geo IP 概念

- **Geo IP 是...**

- USG/ATP 系列：Content Filter 其中一項服務
- VPN 系列：一項可獨立購買的服務（Geo-Enforce）
- 視為一個 Address 物件管理.

- **Geo IP 可以...**

- 套用至任何的 Security Policy / BMW/Web Auth./ DNS Inbound LB/Session Control.
- 可自行定義 IP 至任意國家.

# Geo IP 設定 (1/4)

- Address object 管理頁面

設定

物件

位址/Geo IP

位址

#	名稱	類型	IPv4 位址
1	Yahoo	FQDN	tw.yahoo.com
2	Africa	GEOGRAPHY	Africa-All
3	China	GEOGRAPHY	China-All
4	Germany	GEOGRAPHY	Germany-All
5	Japan	GEOGRAPHY	Japan-All
6	Taiwan	GEOGRAPHY	Taiwan-All
7	USA	GEOGRAPHY	United States-All
8	H-8-8-8-8	HOST	8.8.8.8
9	IP6to4-Relay	HOST	192.88.99.1
10	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
11	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
12	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
13	RFC1918_1	SUBNET	10.0.0.0/8
14	RFC1918_2	SUBNET	172.16.0.0/12
15	RFC1918_3	SUBNET	192.168.0.0/16

新增位址規則

名稱: Taiwan

位址類型: GEOGRAPHY

地區: Taiwan

OK Cancel

# Geo IP 設定 (2/4)

- Geography IP 管理頁面



設定 位址 位址群組 **Geo IP**

國家/地區資料庫更新

最新版本: 20210311  
目前版本: 20210311

備註  
安全套件授權必須有效才能取得最新版更新。

**立即更新**

自動更新

每週: 星期一 (日期) 11 (時)

自定義IPv4到地理規則

1.1.1.1 **由IPv4查地區** Australia

+ 新增 - 移除

#	地區	類型	IPv4 位址
1	Taiwan-All	SUBNET	10.251.31.0/24

第 1 頁, 共 1 頁 每頁顯示 50 行

地區與洲的對應

地區: Japan **由地區查洲**

地區	洲
Japan	Asia

**新增對應**

地區: Taiwan

位址類型: SUBNET

網路: 10.251.31.0

網路遮罩: 255.255.255.0

OK Cancel

# Geo IP 設定(3/4)

- Geography IP 管理頁面-輸入地區查詢洲別



位址 位址群組 Geo IP

地區與洲的對應

地區: Japan 由地區查詢

地區	洲
Japan	Asia

洲: Africa 地區列表

- Algeria
- Angola
- Benin
- Botswana
- Burkina Faso
- Burundi
- Cameroon
- Cabo Verde
- Central African Republic
- Chad
- Comoros
- Republic of the Congo

設定

- 授權
- + 無線
- + 網路
- + VPN
- BWM
- Web 認證
- + 安全性策略
- + 安全服務
- 物件
  - 區域
  - 使用者/群組
  - AP 設定組合
  - MON 設定組合
  - ZyMesh 設定組合
  - 位址/Geo IP
- 服務
- 排程
- AAA 伺服器
- 認證方式
- 憑證
- ISP 帳號

# Geo IP 設定(3/3)

- Security Policy 管理頁面-禁止瀏覽中國網頁

設定

安全性策略

策略控制

策略

顯示過濾器

一般設定

啟用策略控制

IPv4 設定

允許非對稱路由

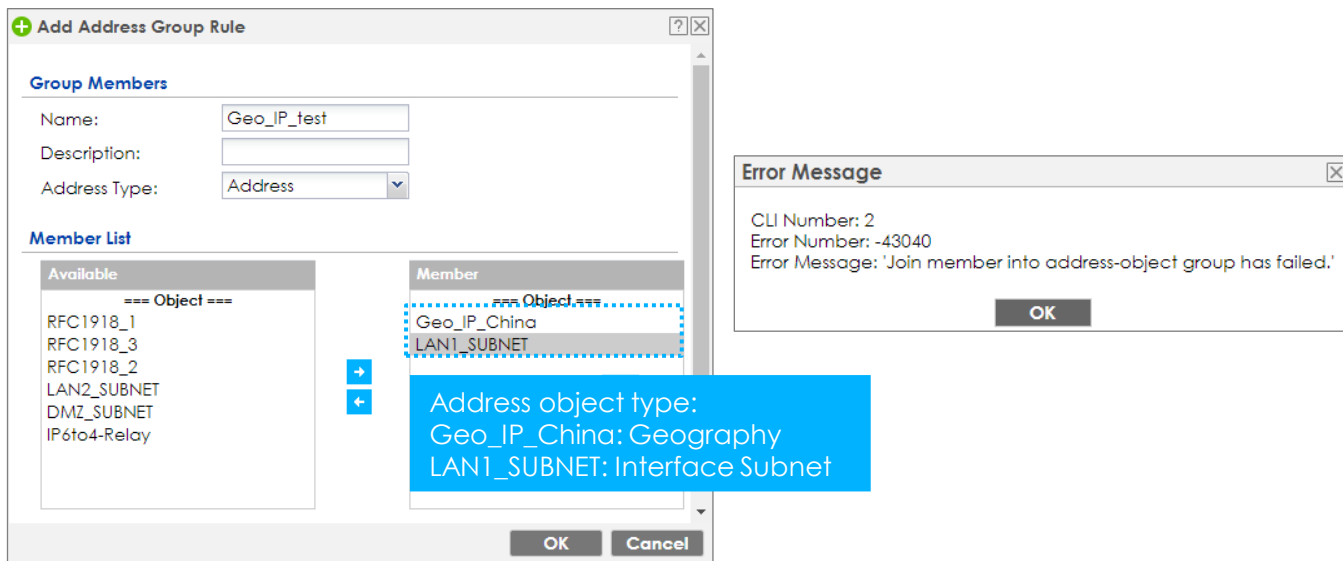
+ 新增   編輯   移除   啟動   停用   移動   複製

優...	狀...	名稱	從	至	IPv4 來源	IPv4 目的地	服務	使用者	排程	動作	log
1	🟡	Block_China	LAN1	WAN	any	China	any	any	none	deny	log alert
2	🟡	Lan1_Outgoing	LAN1	any (Excluding ZyWALL)	any	any	any	any	none	allow	log
3	🟡	LAN2_Outgoing	LAN2	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
4	🟡	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no
5	🟡	IPSec_VPN_Out...	IPSec_V...	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
6	🟡	SSL_VPN_Outg...	SSL_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
7	🟡	TUNNEL_Outgoi...	TUNNEL	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
8	🟡	LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	allow	no
9	🟡	LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no
10	🟡	DMZ_to_Device	DMZ	ZyWALL	any	any	De...	any	none	allow	no
11	🟡	WAN_to_Device	WAN	ZyWALL	any	any	De...	any	none	allow	no
12	🟡	IPSec_VPN_to_...	IPSec_V...	ZyWALL	any	any	any	any	none	allow	no
13	🟡	SSL_VPN_to_De...	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no



# Geo IP 設定上的限制

- Geo IP 位址物件無法與其他類型的物件組成群組



# SSL Inspection

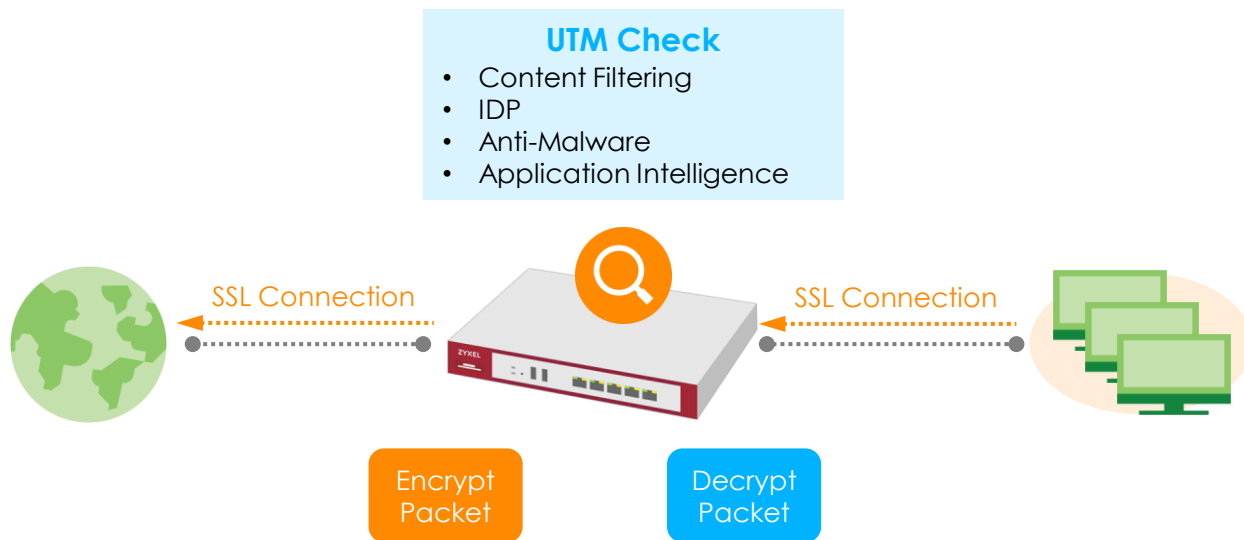
- SSL Inspection
- SafeSearch

# 為何需要 SSL Inspection?

- **SSL (Secure Sockets Layer)** 無所不在 (EX: HTTPs)
- 資料加密提供安全與隱私，傳輸內容無法被解讀，但也提高資安的風險
  - 惡意軟體可以藉由 SSL 加密傳送而不被發現
- **SSL Inspection** 將加密資訊解開檢驗保護網路傳輸內容的安全

# SSL Inspection

- **SSL inspection** 將加密內容解開後 **UTM** 功能就可以對內容進行檢查與過濾



# What You Need to Know

- 支援的演算法
  - DES / 3DES / AES
- 支援的 **SSL** 加密協議版本
  - SSLv3
  - TLSv1
- 支援的型號
  - ZyWALL/USG110/VPN100 and above
  - FLEX/ATP series
- 用戶端必須支援 **certificate** 並信任匯入之 **certificate**
- 不支援檢驗 **Anti-Spam/Email Security**

# SSL Inspection 的設定 (1/4)

- Add Profile



設定組合 排除清單 更新憑證

一般設定  
伺服器簽署密鑰模式: ECDSA-RSA-1024

設定組合管理  
+ 新增 編輯 移除 物件參考

#	名稱	描述	CA 憑證	參考
---	----	----	-------	----

每頁顯示 50 行

+ Add rule

General Settings

Name: SSL\_Inspection

Description:

CA Certificate: default

SSL/TLS version supported minimum: ssl3 Log: no

Action for connection with unsupported suit: pass Log: no

Action for connection with untrusted cert chain: pass Log: log

OK Cancel

# SSL Inspection 的設定 (2/4)

## • Monitor Report



摘要 **憑證快取清單**

一般設定

收集統計資料

**套用** **重設** **重新整理** **清空資料**

狀態

最大現行連線數:	2000
現行連線數:	0

摘要

SSL 連線數總計:	0
檢查的連線數:	0
已解密 (Kb):	0
已加密 (Kb):	0
封鎖的連線數:	0
通過的連線數:	0

當達到「最大現行連線數」時，防火牆會直接Pass Session不進行掃描

# Maximum Concurrent Session

- ZyWALL/USG/VPN series

ZLD 4.60	USG110	USG210	USG310	USG1100	USG1900	USG2200 -VPN
Maximum Concurrent Sessions	1000	1000	3000	3000	3000	5000

ZyWALL110	ZyWALL310	ZyWALL1100	VPN100	VPN300	VPN1000
1000	3000	3000	1000	3000	4000

- USG FLEX/ATP series

ZLD 4.5x	ATP100(W) USG FLEX 100	ATP200 USG FLEX 200	ATP500 USG FLEX 500	ATP700	ATP800
Maximum Concurrent Sessions	2000	2000	3000	4000	4000



# SSL Inspection 的設定 (3/4)

- **Exclude List**：若欲Bypass某個網站不進行傳輸內容解密、掃描、再加密，可將網站加入排除清單



設定組合 排除清單 更新憑證

設定

- + 授權
- + 無線
- + 網路
- + VPN
- BWM
- Web 認證
- + 安全性策略
- 安全服務
  - 應用程式巡查
  - 內容過濾
  - 防惡意程式
  - 信譽評等過濾
  - 入侵偵測與防
  - 沙箱
  - 電子郵件安全
  - **SSL 檢查**
  - IP例外清單

一般設定

啟用排除日誌清單

排除清單設定 ⓘ

+ 新增 編輯 移除

#	憑證識別身分的排除清單
1	*.google.com
2	*.zyxel.com

◀ ◁ 第 1 頁, 共1頁 ▷ ▶ ▶▶ 每頁顯示 50 行

# SSL Inspection 的設定 (4/4)

- Certificate Cache List



憑證快取清單

新增到排除清單

#	在排除清單中	時間	共用名稱	伺服器名稱指示	SSL 版本	目的地	有效時間 (秒)
1		2021-03-15 ...	*.facebook.com	edge-chat.facebook.com	TLS1.3	31.13.87.1:443	86400
2		2021-03-15 ...	*.ftpe8-1.fna.fbcdn.net	video.ftpe8-1.fna.fbcdn....	TLS1.3	203.74.69.18...	86400
3		2021-03-15 ...	*.ftpe8-4.fna.fbcdn.net	video.ftpe8-4.fna.fbcdn....	TLS1.3	203.74.69.21...	86400
4		2021-03-15 ...	*.ftpe8-1.fna.fbcdn.net	scontent.ftpe8-1.fna.fbc...	TLS1.3	203.74.69.17...	86400
5		2021-03-15 ...	*.ftpe8-2.fna.fbcdn.net	scontent.ftpe8-2.fna.fbc...	TLS1.3	203.74.69.81...	86400
6		2021-03-15 ...	*.ftpe8-3.fna.fbcdn.net	scontent.ftpe8-3.fna.fbc...	TLS1.3	203.74.69.14...	86400
7		2021-03-15 ...	*.ftpe8-4.fna.fbcdn.net	scontent.ftpe8-4.fna.fbc...	TLS1.3	203.74.69.20...	86400
8		2021-03-15 ...	upload.video.google.com	safebrowsing.googleapis...	TLS1.3	216.58.200.4...	86340
9		2021-03-15 ...	*.facebook.com	static.xx.fbcdn.net	TLS1.3	31.13.77.15:...	86220
10		2021-03-15 ...	*.facebook.com	scontent.xx.fbcdn.net	TLS1.3	31.13.87.5:443	86340
11		2021-03-15 ...	*.facebook.com	www.facebook.com	TLS1.3	31.13.87.36:...	86220
12		2021-03-15 ...	*.gstatic.com	ssl.gstatic.com	TLS1.3	172.217.160....	86340
13		2021-03-15 ...	*.google-analytics.com	www.googletagmanag...	TLS1.3	74.125.203.9...	86280
14		2021-03-15 ...	*.facebook.com	facebook.com	TLS1.3	31.13.87.36:...	86220
15		2021-03-15 ...	www.google.com	www.google.com	TLS1.3	216.58.200.3...	86220
16		2021-03-15 ...	*.google.com	play.google.com	TLS1.3	172.217.27.1...	86220
17		2021-03-15 ...	*.google.com	google.com	TLS1.3	108.177.125...	86220

# SafeSearch

- **SafeSearch** 功能介紹
- **SafeSearch** 設定

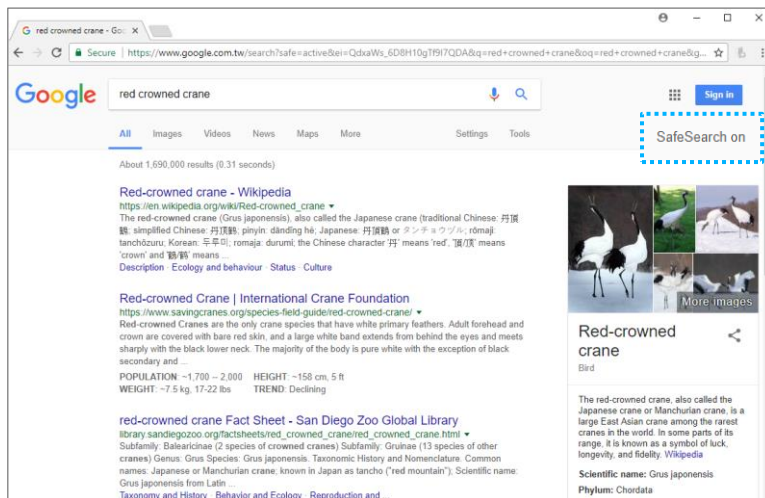
# SafeSearch 功能介紹

- **SafeSearch on ZyWALL/USG/VPN/ATP**
  - 避免搜尋到不適當內容或露骨圖像
  - 支援市面上大多數受歡迎的搜尋引擎
  - 需具備 Content Filter 授權
- **優點**
  - 單一化 SafeSearch 管理.
  - Filtering sexually explicit video and images from search result pages.



# SafeSearch 應用情境

- 避免搜尋引擎搜尋出不適當的內容（過濾掉色情影片或圖像）
  - When SafeSearch is on, sexually explicit video and images will be filtered from search engine result pages, along with results that might link to explicit content.



# 支援的 Search Engine

- Yahoo, Google, Bing, Yandex
- A9, Alltheweb, Altavista, Ask, Youtube, Lycos, Otange



# SafeSearch 的管理

- **SafeSearch 的使用需要啟用 SSL Inspection**
- 當 **SafeSearch** 功能啟用，**firewall** 會增加一些特殊字串到搜尋的 **URL** 上。
  - <https://www.google.com.tw/search?q=Red+crowned+crane&safe=active>



# SafeSearch 功能設定

- SafeSearch



設定組合 信任/禁止網站

Edit Filter Profile BPP

類別服務 自訂服務

一般設定

名稱: BPP

描述: Business Productivity I (選擇性)

啟用SafeSearch

啟用內容過濾分級服務

記錄所有網頁存取

管理網頁採取的動作: Block  log

未分級網頁採取的動作: Warn  log

類別伺服器無回應時採取的動作: Pass  log



# VPN Overview

# Agenda

---

01

什麼是 VPN?

02

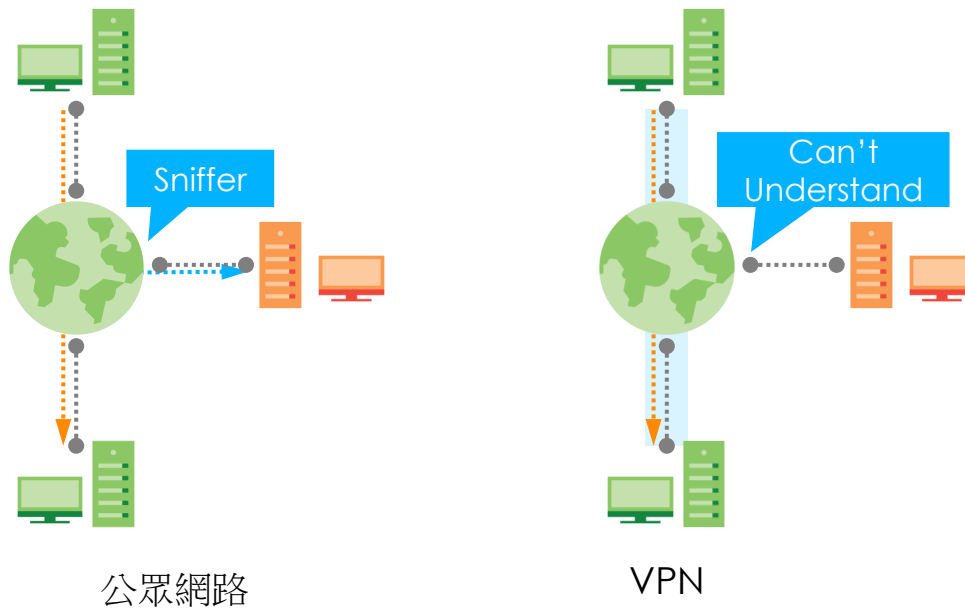
為何使用 VPN?

# 什麼是 VPN?

- **VPN = Virtual Private Network**
- VPN 的全名是「虛擬私人網路」，能針對您的網路流量進行加密，同時保護您所傳輸資料的完整性與機密性。

# Virtual Private Network

- 擁有 VPN 建立相關資訊的裝置或人員才能進行 VPN 連結
- 透過加密資料與資料檢驗的技術確保資料的完整性與機密性

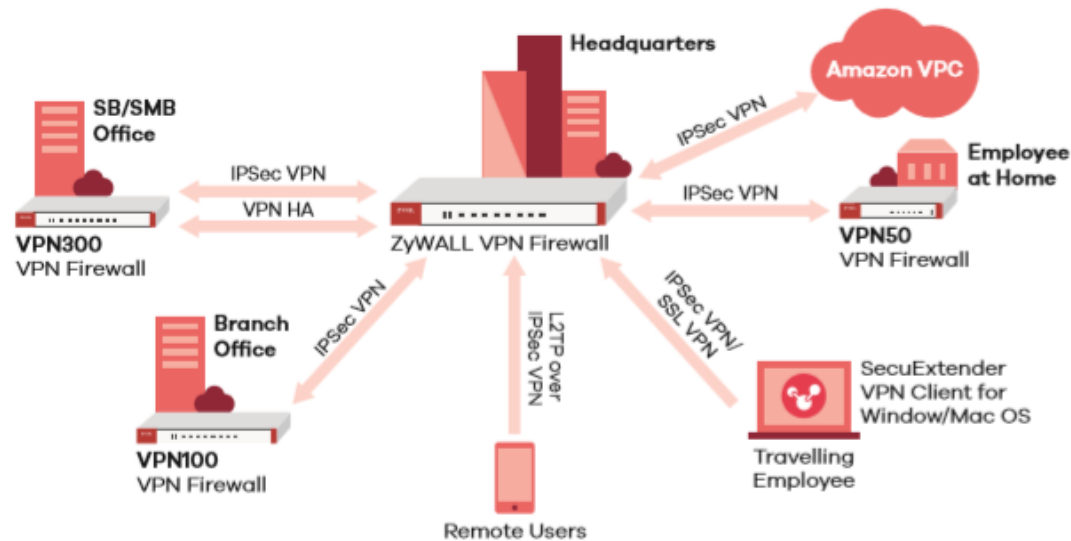


# 為何需要 VPN?

- 商業面
- 便利性

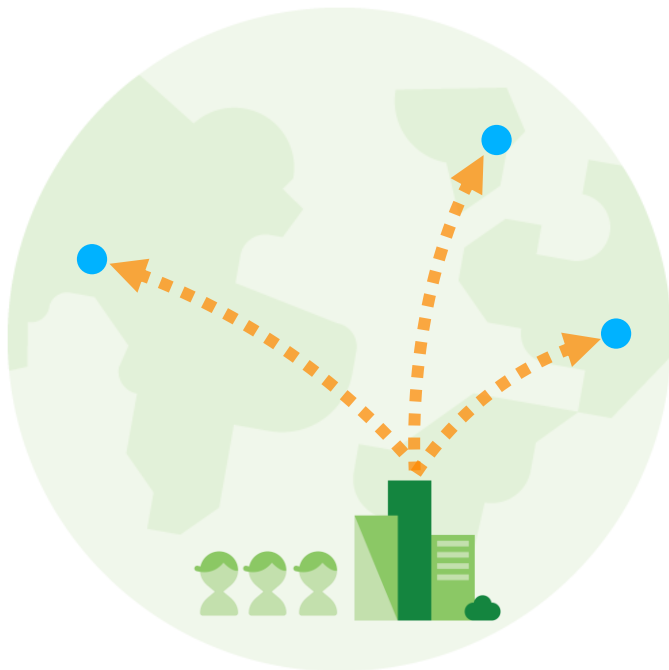
# 商業面

- 延伸網路連結到不同地理區域但不使用成本較高的專線
- 提供資料交換的安全性
- 提供遠端辦公室或人員安全的存取內部網路



# 便利性

- 簡單、快速的存取不同區域的內部網路。
  - 人不須在當地即可以適當權限存取公司內部資源



# VPN 如何運作？

- 如何讓“公眾”網路變“私有”？
- 驗證與加密



# 如何讓“公眾”網路變“私有”?(1/2)

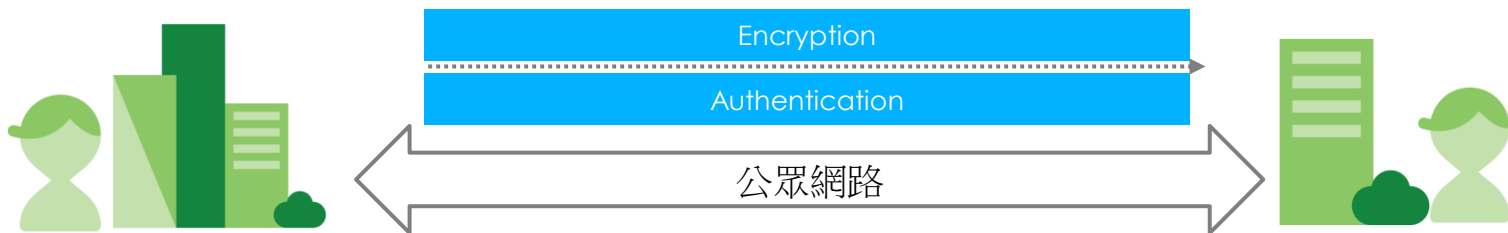
- 私有網路 V.S 公眾網路

- 私有網路是能被控制
- 私有網路是被信任且具有私密性



# 如何讓“公眾”網路變“私有”? (2/2)

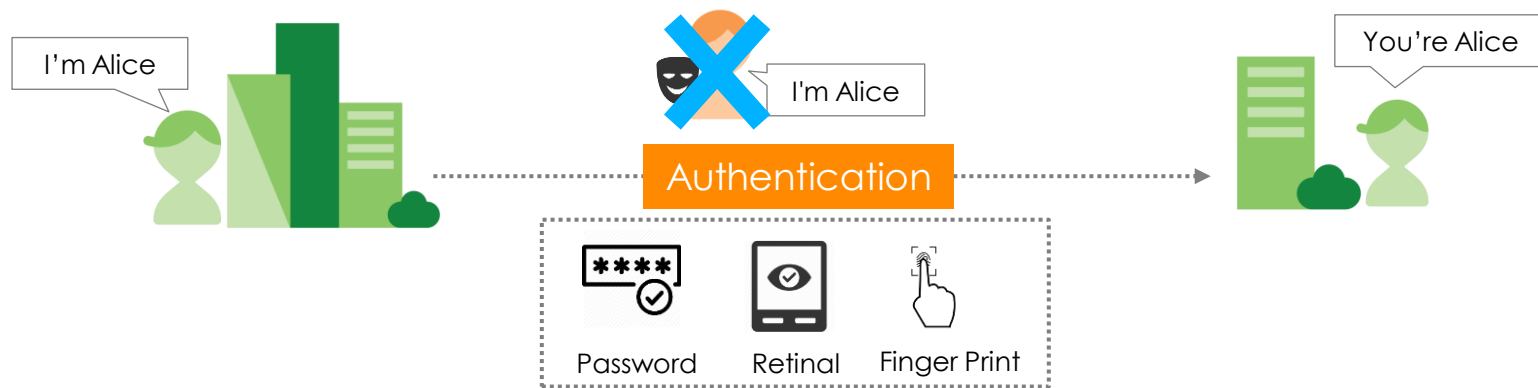
- **VPN = 讓“公眾”網路變“私有”**
- 你無法讓公眾網路變成可控
- 然而你可以讓公眾網路變成可信任且安全
  - 可信任 = (Peer) Authentication
  - 安全 = (Data) Encryption



- **Still not** in control
- But (Peer)Trusted and (Data)Secured

# Authentication

- **Authentication** 判斷對方身份是否為偽冒.



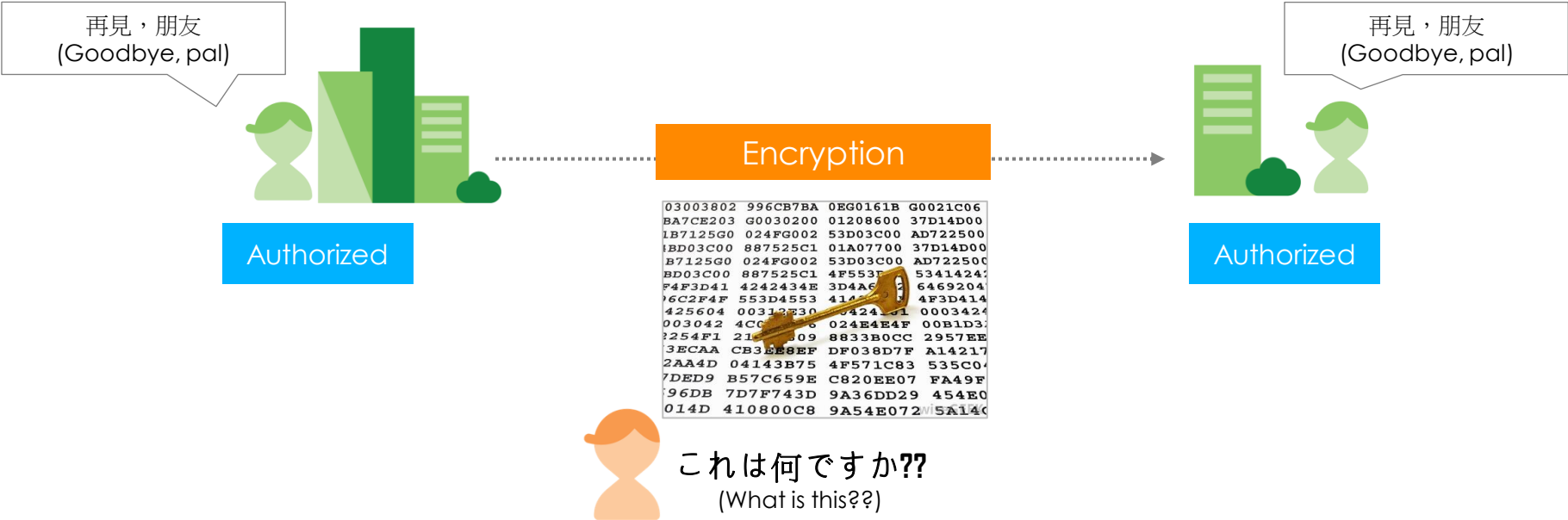
# Hash Algorithms 演算法

- 用於驗證資料是否遭竄改
- 長度越長越難破解

Name	Publish	Max Input Size	Digest	Description & Note
<b>MD5</b>	1991	$(2^{64}-1)$ bits	128 bits	<ul style="list-style-type: none"><li>• Designed by Ron Rivest</li></ul>
SHA-0	1993	$(2^{64}-1)$ bits	160 bits	<ul style="list-style-type: none"><li>• Withdrawn shortly after publication</li></ul>
<b>SHA-1</b>	1995	$(2^{64}-1)$ bits	160 bits	<ul style="list-style-type: none"><li>• The standard was no longer approved for most cryptographic uses after 2010.</li><li>• Designed by the NSA.</li></ul>
<b>SHA-2</b>	2001	$(2^{64}-1)$ bits	256 bits(SHA-256)	<ul style="list-style-type: none"><li>• Designed by the NSA.</li></ul>
		$(2^{128}-1)$ bits	512 bits(SHA-512)	
SHA-3	2012	—	224 bits (SHA3-224) 256 bits (SHA3-256) 384 bits (SHA3-384) 512 bits (SHA3-512)	<ul style="list-style-type: none"><li>• Its internal structure differs significantly from the rest of the SHA family.</li></ul>

# Encryption

- 加密：對原訊息進行編碼使得未授權人員無法解讀內容

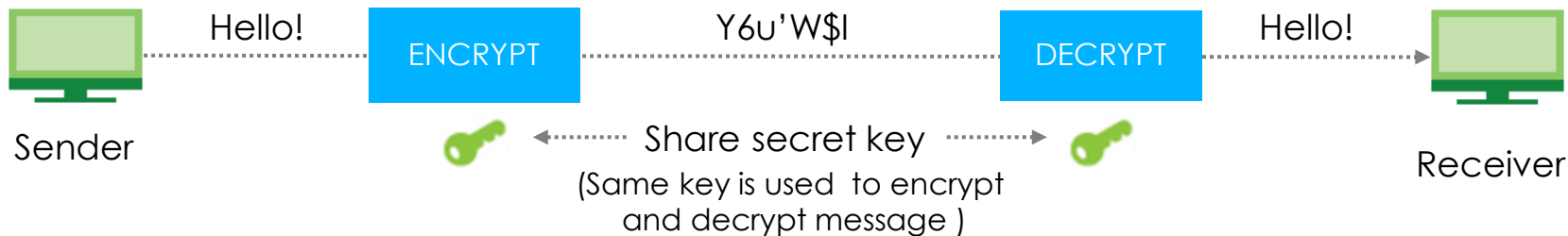


# Encryption Algorithms

- Encryption 的類型
- Encryption 演算法

# Encryption 類型(1/2)

- **Symmetric key encryption** (對稱式加密) : 加、解密使用相同金鑰. 因此通訊雙方需要擁有相同的金鑰才有辦法進行祕密通訊 (EX: IPsec)
  - DES, 3DES, AES

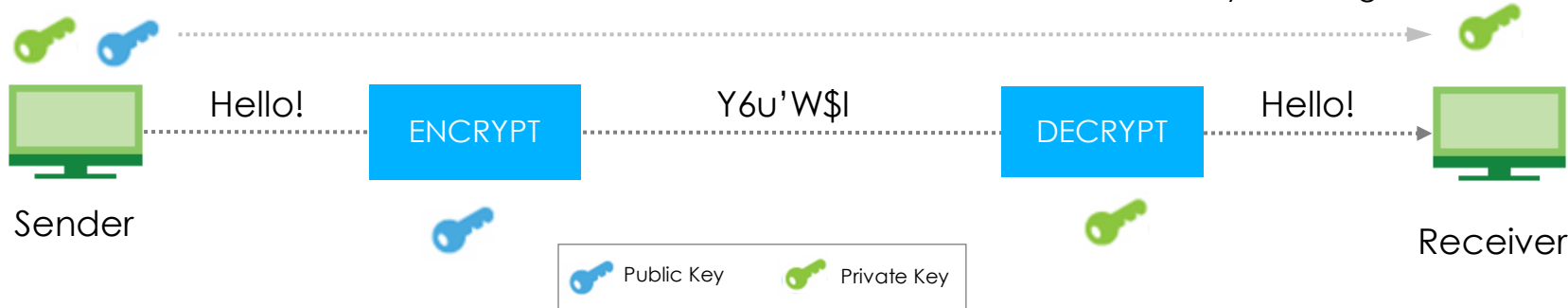


# Encryption 類型(2/2)

- **Asymmetric key encryption** (非對稱式加密) : 加密用的金鑰發給任何想要加密訊息的人. 但只有擁有私密金鑰的人才能做解密訊息的動作(**EX: HTTPS**)
  - RSA, DSA

1. Generate Key Pair

2. Public Key Exchange





# Encryption 演算法

- **DES(Data Encryption Standard)**
- **3DES(Triple Data Encryption Standard)**
- **AES(Advanced Encryption Standard)**

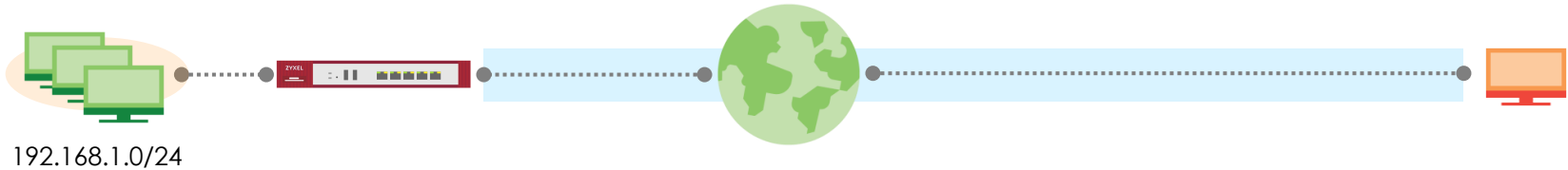
Name	Published	Key Size	Description & Note
DES	1977	56 bits	<ul style="list-style-type: none"><li>• Developed by IBM</li><li>• DES is now considered to be insecure due to the 56-bit key size being too small</li></ul>
3DES	1998	168 bits	<ul style="list-style-type: none"><li>• Applies the DES cipher algorithm three times to each data block</li></ul>
AES	2001	128 bits (AES128) 192 bits (AES192) 256 bits (AES256)	<ul style="list-style-type: none"><li>• AES has been adopted by the U.S. government and is now used worldwide</li></ul>

# VPN 類型

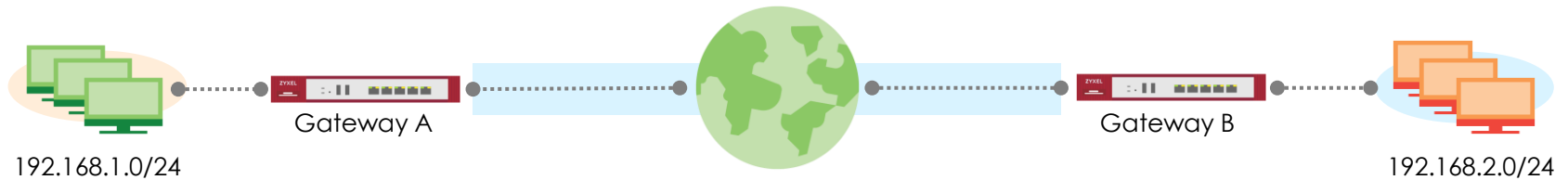
- VPNs 可以是 remote-access (connecting a computer to a network) 或是 site-to-site (connecting two networks)
- 經常使用的 VPNs 技術是：
  - IPsec VPN(site-to-site & remote access)
  - L2TP over IPSec VPN (remote access)
  - SSL VPN (remote access)

# VPN Types

- Remote Access VPN



- Site to Site VPN



# IPSec VPN 設定

- **IPSec VPN 設定重點**

- SA 參數一致
- 指定要建立 VPN 通道的端點
- 不是所有流量都進 VPN, 指定符合哪種條件時流量才須進 VPN



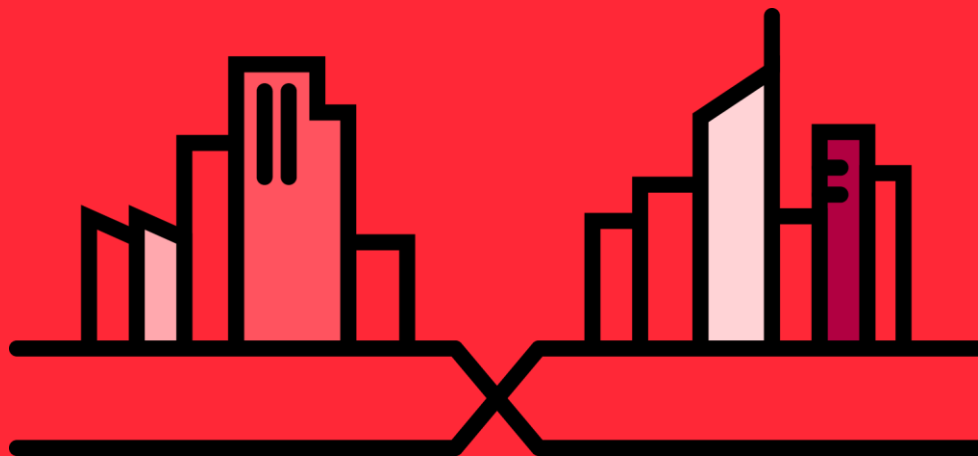
# VPN 設定

The screenshot shows a network management interface with a sidebar on the left and a main content area. The sidebar contains a navigation menu with the following items: 設定, + 授權, + 無線, + 網路, - VPN, - IPsec VPN, - SSL VPN, - L2TP VPN, - BWM, - Web 認證, + 安全性策略, + 安全服務, + 物件, + Cloud CNM, + 系統, + 日誌與報告. The main content area has a top navigation bar with 'VPN 連線', 'VPN 閘道器', '集訊器', and '設定配置'. Below this, there are links for '全域設定', 'Configuration Walkthrough', 'Troubleshooting', 'Download VPN Client', and 'VPN'. The main content area also contains several checkboxes: '使用策略路由控制動態 IPsec 規則' and '忽略IPv4封包'. Below these is an 'IPv4 設定' section with '+ 新增' and '編' buttons, and a table with columns '#', '狀態', and '第 0'. A '快速設定' dialog box is open in the foreground, containing three options: 'WAN 介面', 'VPN用戶端遠端存取設定', and 'VPN 設定'. Each option has an icon and a brief description.

**快速設定**

- WAN 介面**  
WAN 快速設定會引導您逐一執行步驟，將裝置連接至線上。
- VPN用戶端遠端存取設定**  
不論何時何地提供安全可靠VPN連接到公司內部網路。
- VPN 設定**  
若要建立節點之間的安全通訊，VPN 快速設定可提供完成此項工作的簡化程序。

# 進階安全防護



# 功能介紹



# Agenda

---

01

**Intrusion  
Prevention**  
(入侵防禦)

02

**Sandboxing**  
(沙箱)

03

**Malware  
Blocker**  
(惡意程式阻擋)



# Intrusion Prevention(入侵防禦)



# IDP設定簡化

- IDP設定
  - 不需設定IDP管理組合
    - 一鍵啟用按鈕
  - 雲端查詢特徵碼 & 自訂特徵碼整合在同一頁面

The screenshot displays the IDP configuration page with a left-hand navigation menu and a main configuration area. The main area is divided into sections: General Settings, Query Signatures, Query Result, and Custom Signature Rules. Red boxes highlight the 'Enable' checkbox, the 'Query Signatures' section, and the 'Custom Signature Rules' section. Blue callout boxes point to the 'Enable IDP' button, the 'Query IDP signatures' button, and the 'Custom IDP signature' button. The 'Query Result' section shows a table with columns for #, Status, SID, Name, Severity, and Classification. The 'Custom Signature Rules' section shows a table with columns for #, SID, and Name, along with pagination controls.

**CONFIGURATION**

- Licensing
  - Registration
  - Signature Update
- + Wireless
- Network
  - Interface
  - Routing
  - DDNS
  - NAT
  - Redirect Service
  - ALG
  - UPnP
  - IP/MAC Binding
  - Layer 2 Isolation
  - DNS Inbound LB
  - IPnP
- + VPN
- BWM
- Web Authentication
- Security Policy

**IDP**

Show Advanced Settings

**General Settings**

Enable **Enable IDP**

**Query Signatures** **Query IDP signatures**

Name:  (Optional) **Search**

Signature ID:  (Optional)

Advance

**Query Result**

Activate Inactivate Log Action

#	Status	SID	Name	Severity	Classifica...	Platform	Serv
---	--------	-----	------	----------	---------------	----------	------

**Custom Signature Rules** **Custom IDP signature**

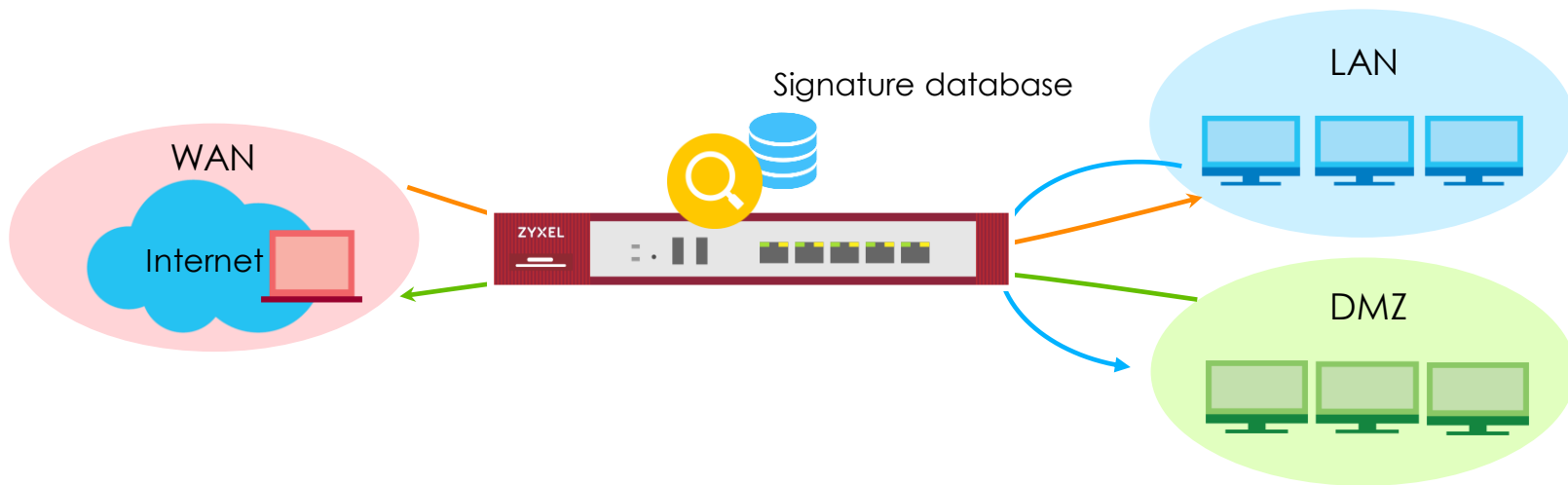
+ Add Edit Remove Export

#	SID	Name
---	-----	------

Page 0 of 0 Show 50 Items

# IDP設定簡化

- ATP 將會檢查所有通過閘道器的流量

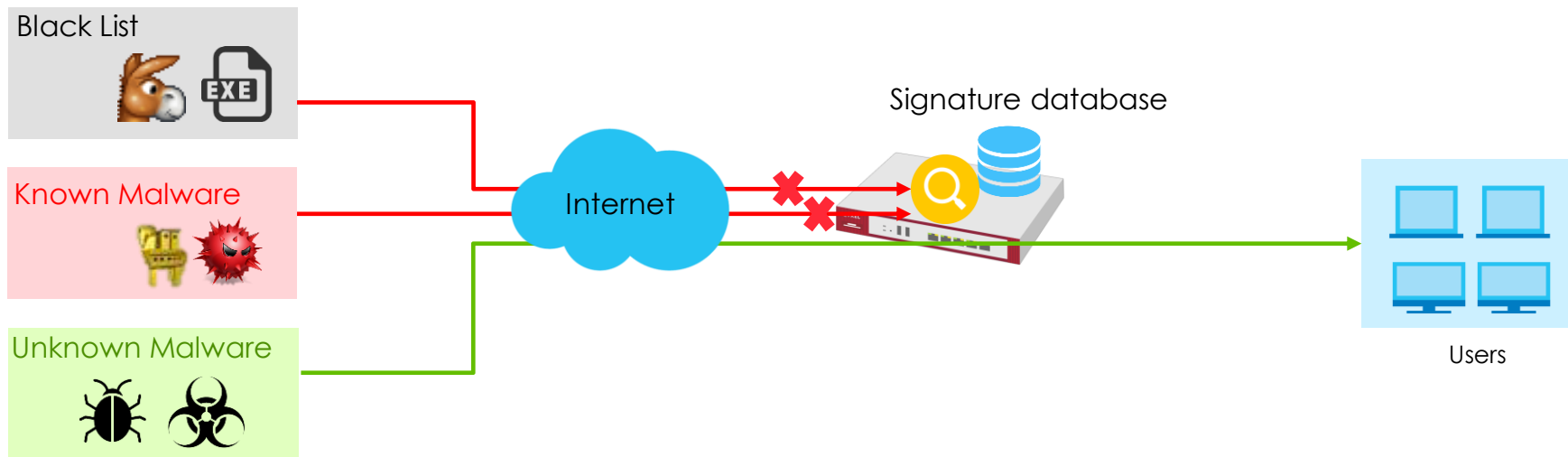


# Sandbox(沙箱)



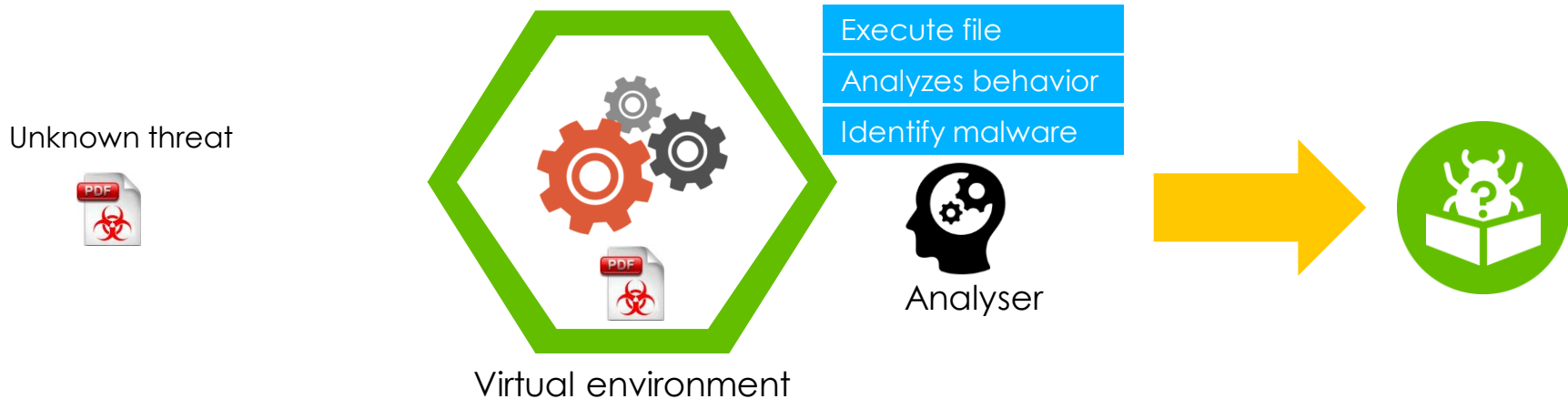
# 為何需要sandbox(沙箱)

- 以特徵碼為基礎的Anti-virus 及 IDP 無法發現未知的威脅



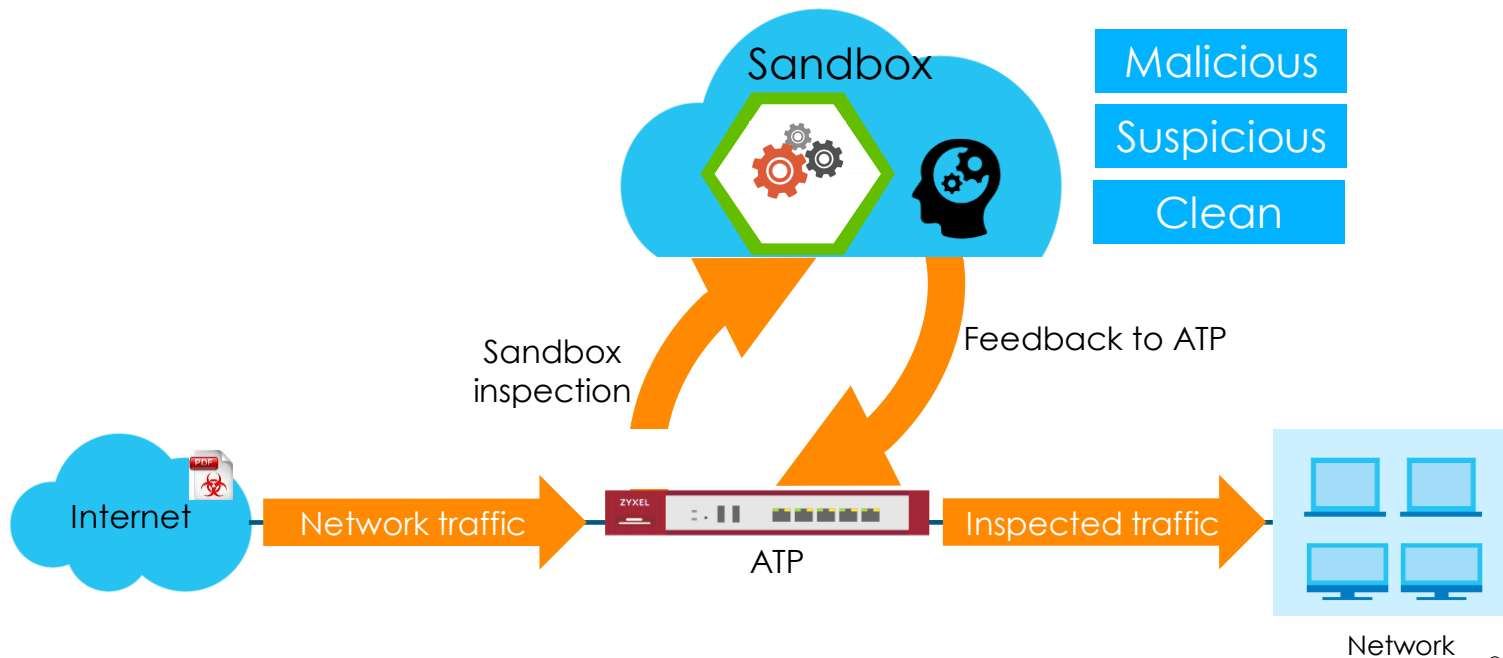
# 什麼是Sandbox(沙箱)?

- 識別未知威脅的最佳方法是在安全的虛擬環境中執行未知的文件
- 沙箱提供了這樣的一個獨立安全的環境



# Zyxel Sandbox

Zyxel沙箱是一種雲端服務，讓ATP可以檢測下載文件/電子郵件附件中藏有的新的或未知惡意軟件。



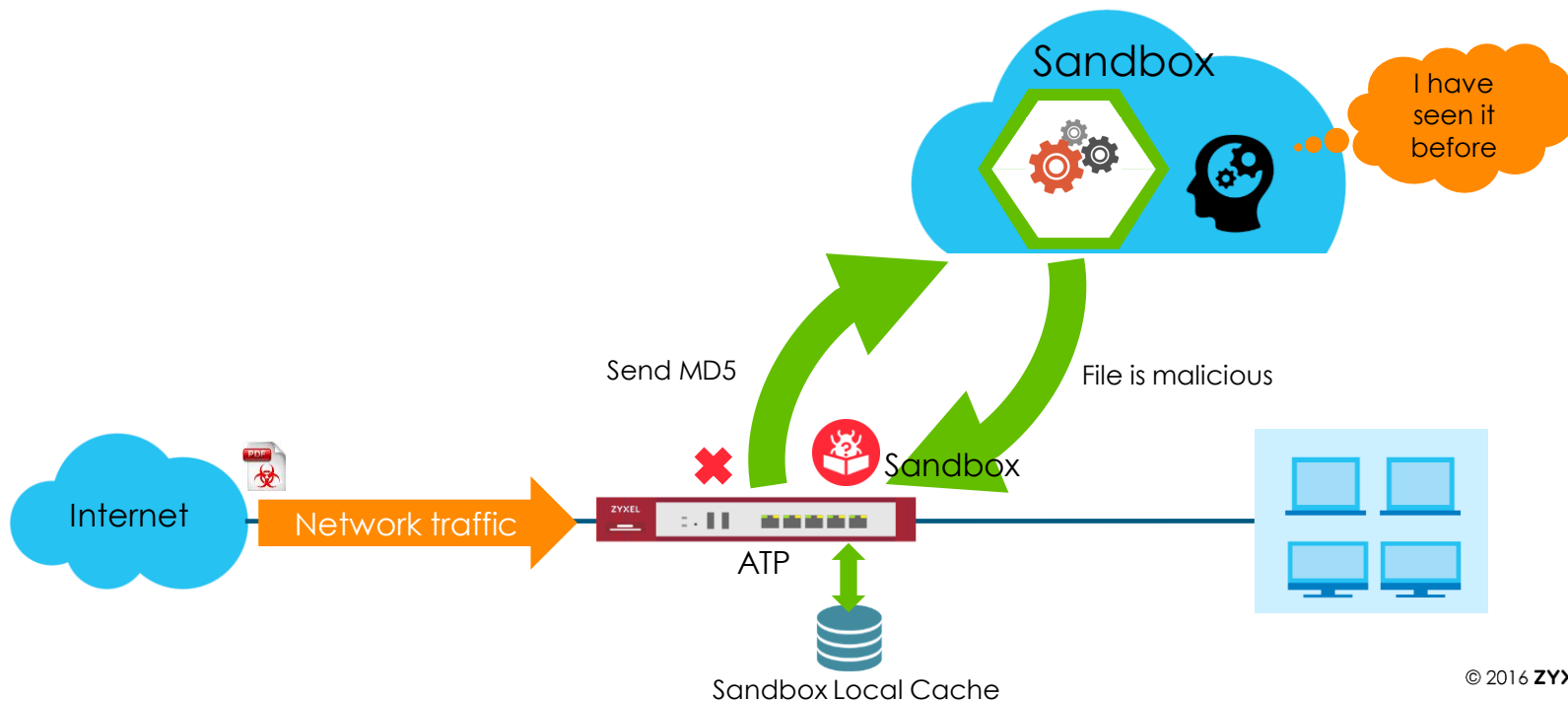
# Zyxel Sandbox

- 支援虛擬機OS版本
  - Windows and Mac OSX Operating System
- 支援協定
  - HTTP, FTP, POP3, SMTP and their equivalent SSL-encrypted versions



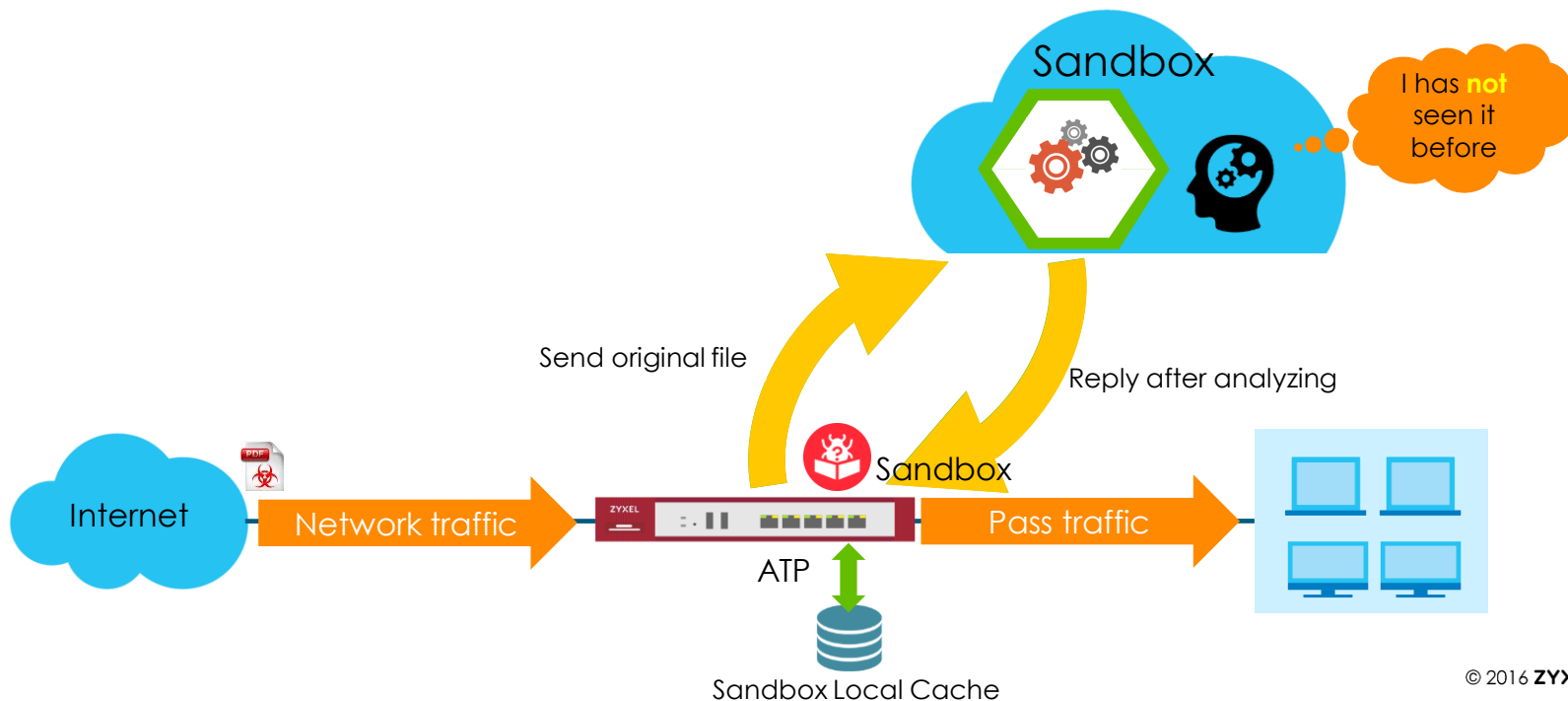
# Advanced Inspection for Sandbox

- ATP 會先上傳檔案的MD5 Hash到雲端沙箱
  - 沙箱2秒內回覆查詢結果



# Advanced Inspection for Sandbox

- 當沙箱告知沒見過類似檔案時，ATP上傳檔案至沙箱
  - Gateway forward the file before sending to sandbox



# Supported Protocols and File Types

- Protocol support
  - HTTP, FTP, POP3, SMTP, HTTPS, FTPS, POP3S, SMTPS
- File type
  - Archives(.zip)
  - Executable (.exe)
  - MS Office Documents (.xls, .xlsx, .xls, .pptx, .ppt, .pps, .doc,.docx)
  - Macromedia Flash Data (.swf)
  - PDF
  - RTF
- File size
  - $32B \leq \text{File} \leq 10 \text{ MB}$

# Sandbox Configuration

- 設定 > 安全服務 > 沙箱

**Sandboxing**

**General**

Enable Sandboxing **Enable Sandboxing**

Action For Malicious File:

Log For Malicious File:

Action For Suspicious File:

Log For Suspicious File:

**Advanced Inspection**

Inspect Selected Downloaded Files **Enable advanced inspection**

The file types you select will be regarded as a possible threat. This feature inspects the files which are being downloaded from the Internet and have never been inspected before. Safe files will be passed through after inspection.

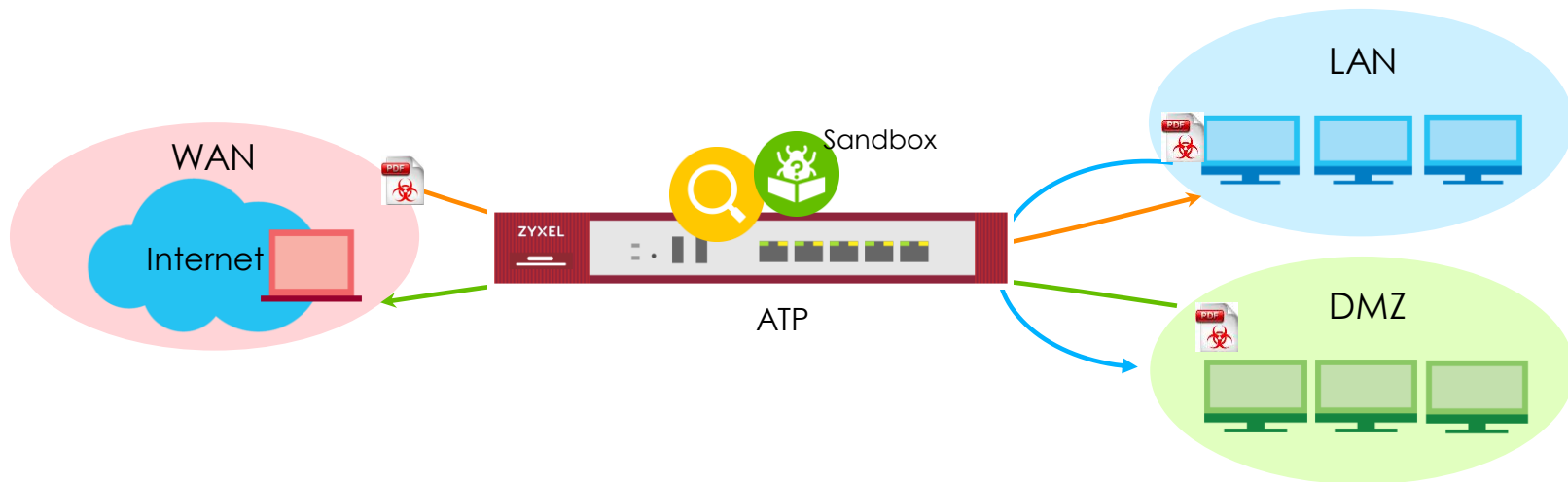
**Note:**  
Downloads may be interrupted and need to be restarted.

**File Submission Options**

Archives (.zip)  
 Executables  
 MS Office Documents  
 Macromedia Flash Data  
 PDF  
 RTF **Select file types are send to cloud sandbox**

# Sandbox- 流量檢查

- 沙箱引擎會檢查所有通過閘道器的流量，掃描並檢測隱藏其中的惡意軟體



# Sandbox(沙箱)統計頁面

- 監控 > 資安統計資料 > 沙箱

## Summary

### Collect Sandboxing Statistics

Collect Statistics since 2018-04-27 17:36:04 to 2018-05-02 09:04:22

[Apply](#) [Reset](#) [Refresh](#) [Flush Data](#)

#### Submission Summary

Total:	173
Scanning:	0
Scanned:	173
Destroyed File:	0

掃描摘要

#### Scan Result

Malicious File:	1
Suspicious File:	0
Clean File:	172
Other:	0

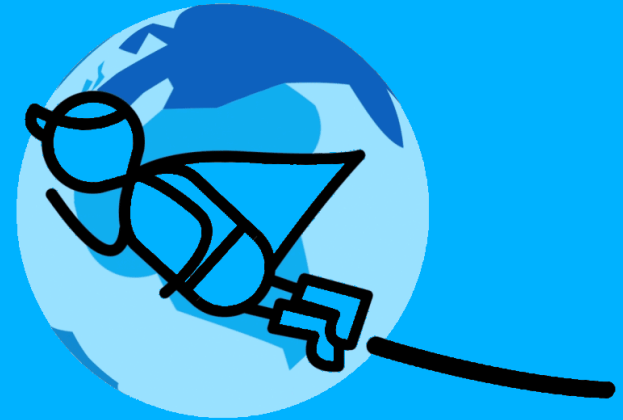
掃描結果

#### Statistics

#	File Name	Hash	Type	Occurence	Update Time
1	eicar_com.zip	6ce6f415d8475545be5ba114f208b0ff	Malicious	1	2018-04-27 17:39:32

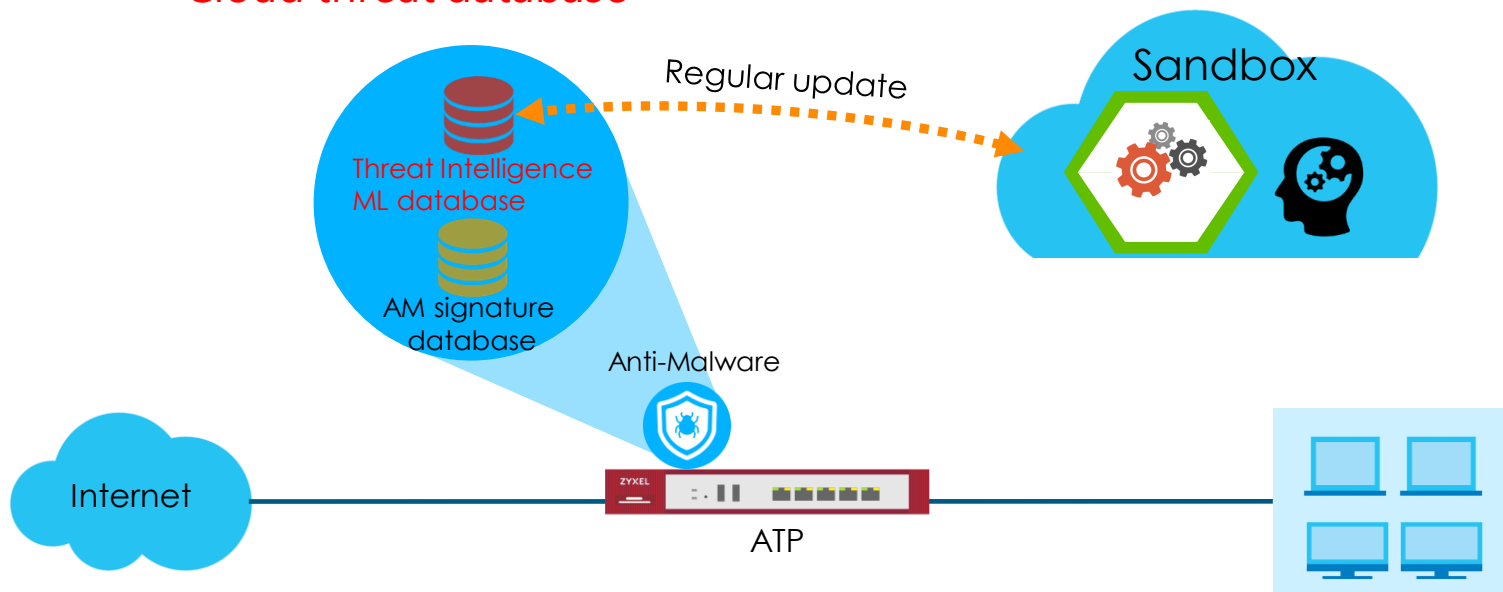
Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1

# Anti-Malware



# 多重威脅資料庫

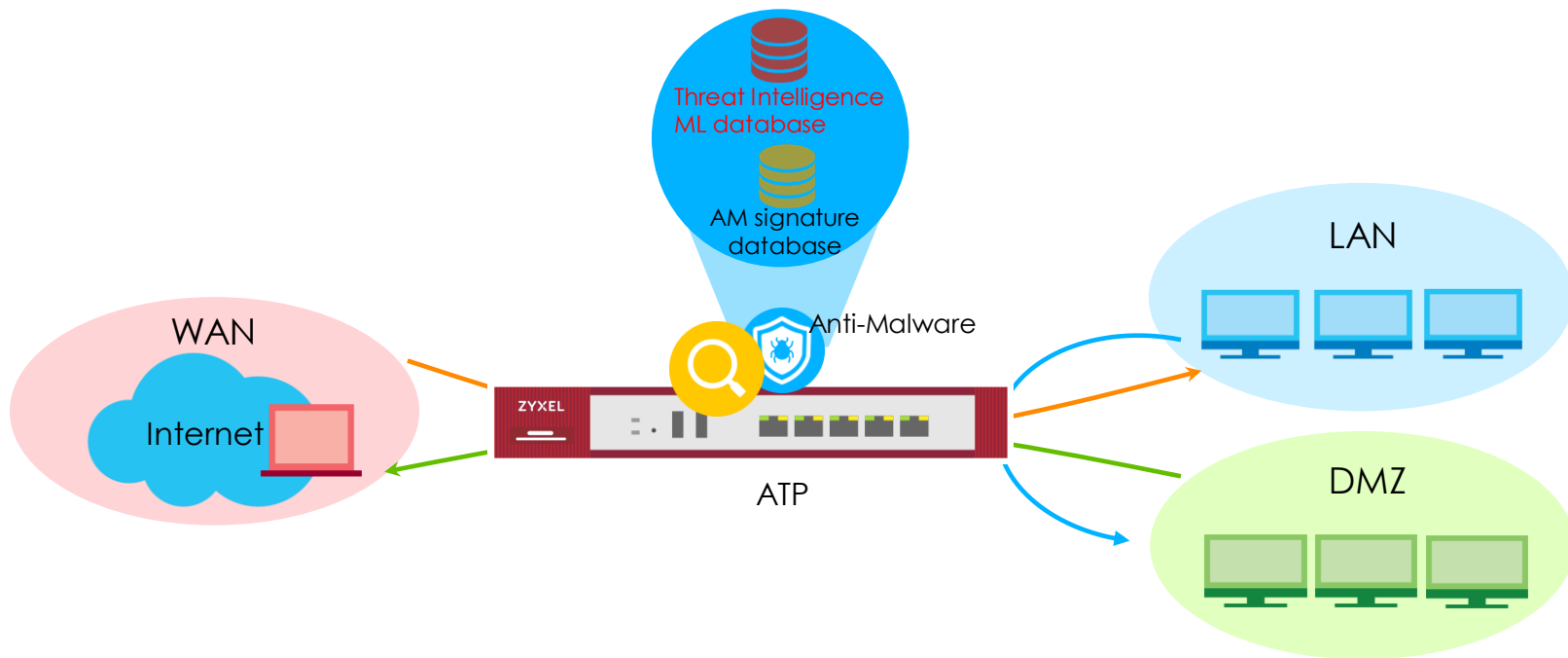
- Anti-Malware 支援多個資料庫以全面保護您的網路
  - Anti-Malware Signature
  - Threat Intelligence Machine Learning database ( update from Sandbox)
  - **Cloud threat database**





# Anti-Malware 簡易設定

- 當開啟Anti-Malware後,ATP會確認所有經過閘道器的流量



# Anti-Malware 設定

- 啟用「防惡意程式」及選擇「掃描模式」

防惡意程式

黑白名單 特徵碼

顯示進階設定

一般設定 **Anti-Malware**

啟用

掃描與偵測EICAR

Scan Mode

Express Mode  Stream Mode  Hybrid Mode **只有ATP支援**

進階設定

掃描檔案類型

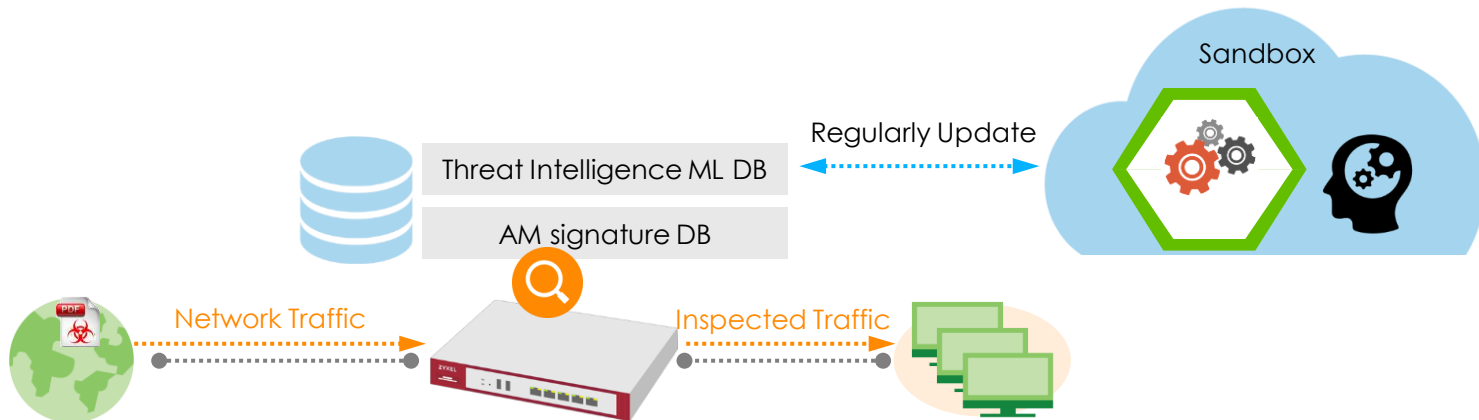
可支援的檔案類型	已選取的檔案類型
7z Archive (7z)	Executables (exe)
AVI Video (avi)	Macromedia Flash Data (swf)
BMP Image (bmp)	MS Office Document (doc...)
BZ2 Archive (bz2)	PDF Document (pdf)
GIF Image (gif)	RTF Document (rtf)
GZ Archive (gz)	ZIP Archive (zip)
JPG Image (jpg)	
MOV Video (mov)	

套用 重設

16 ZYXEL 26  
9

# Stream Mode(1/3)

- 在 **Stream Mode, Anti-Malware** 掃描引擎依賴本地端病毒資料庫進行檔案偵測，以判斷是否遭惡意程式感染
  - Anti-Malware Signature (From Bitdefender)
  - Threat Intelligence Machine Learning database ( From Sandbox, support ATP、USG Flex)



# Stream Mode(2/3)

- 在 2018 年，Bitdefender 憑藉著優異的偵測率，分別獲 2 家資安分析公司頒發「最佳防護力榮譽獎章」
  - AV-Comparatives consistently awards Bitdefender the highest possible rating (Advanced+)



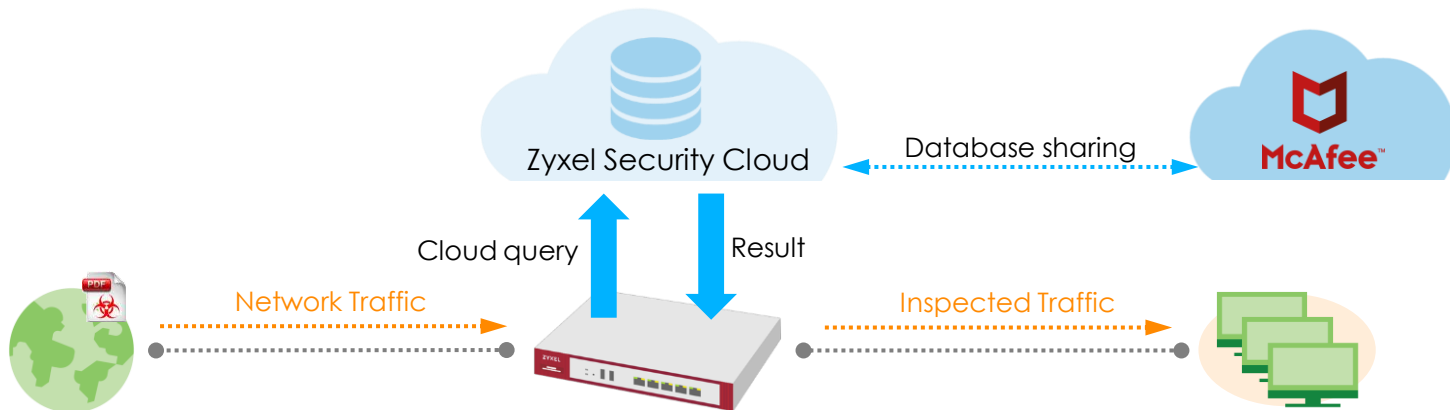
# Stream Mode (3/3)

- 支援的協定
  - HTTP, HTTPS, FTP, FTPS, POP3, POP3S, SMTP, SMTPS
- 支援的檔案類型
  - All types
- 檔案大小
  - No file size limits

# Express Mode (1/2)

**Gateway** 傳送檔案的 **MD5 Hash** 值到雲端資料庫進行比對，雲端資料庫於 **2 秒內** 回應查詢結果給 **Gateway**

- Expand the detection coverage by cooperating with McAfee
- Shorten the time gap between daily signatures update



# Express Mode (2/2)

- 支援的協定

- HTTP, HTTPS, FTP, FTPS, POP3, POP3S, SMTP, SMTPS

- 支援的檔案類型

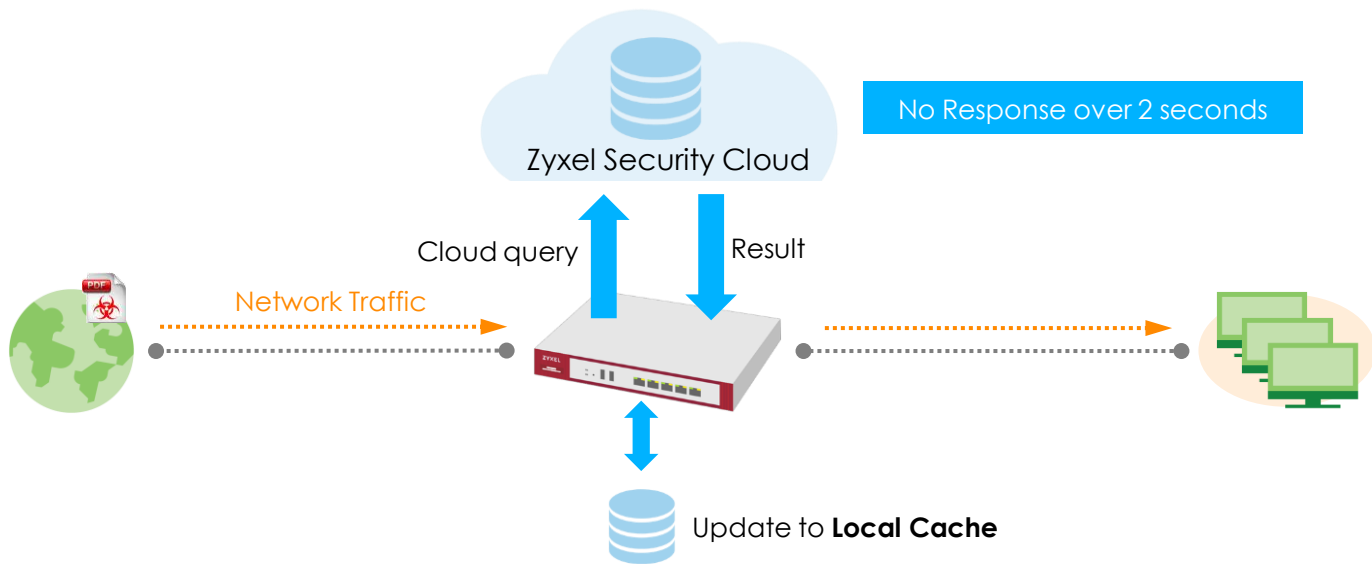
- Archives: 7Z, RAR, ZIP, BZIP2, GZIP
- Adobe: PDF, SWF
- Executables: EXE
- Microsoft Office: Word, Excel, PowerPoint, Outlook and more
- Video/Audio/Image: AVI, BMP, GIF, JPG, MOV, MP3, MPG, PNG, RM, TIFF, WAV

- 檔案大小

- No file size limits

# 注意事項

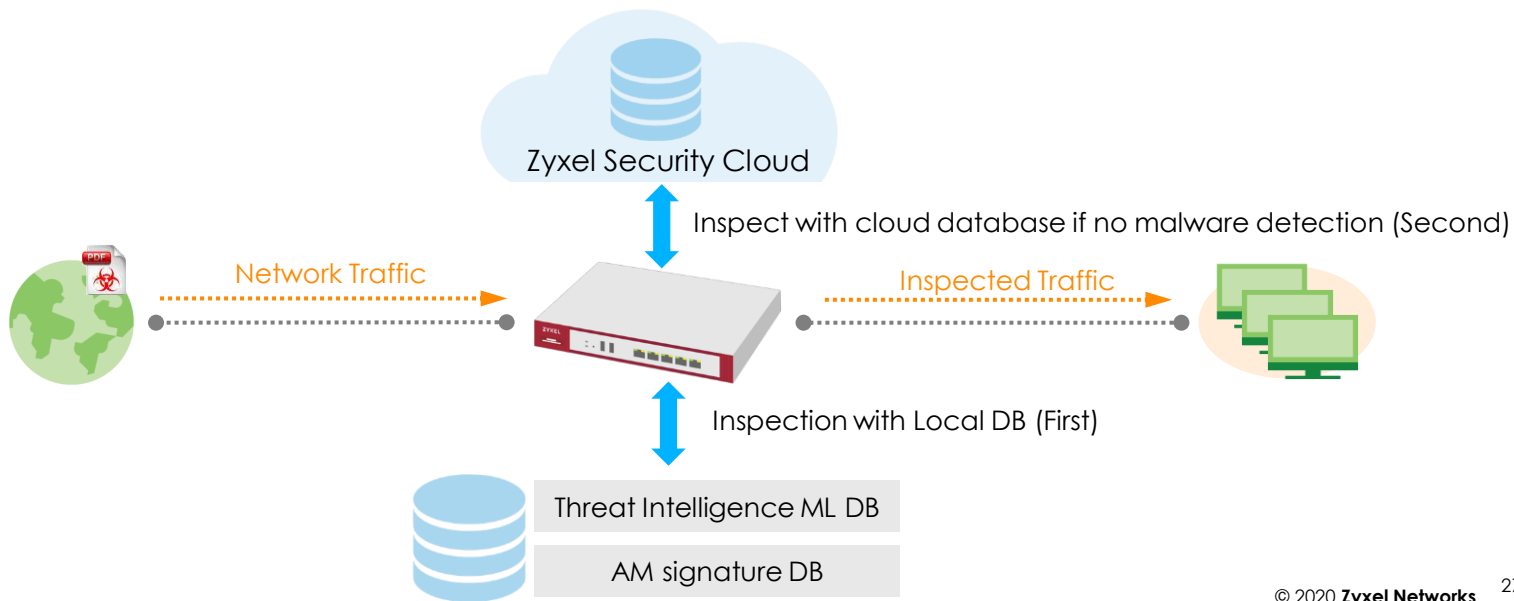
- **Gateway** 如果在 **2** 秒內未得到雲端資料庫的回應將會傳送檔案至目的地.
  - Late response but not over 60 seconds will be stored in local cache





# Hybrid Mode (ATP Only)

- 先使用本機資料庫進行掃描比對，若比對不到再進行雲端查詢



# 防惡意程式

- 提供多種不同掃描方式以滿足客戶的需要

	USG ZLD4.38	USG FLEX ZLD4.55	ATP ZLD4.55
Stream Mode (本地掃描)	●	●	●
Express Mode (雲端查詢)	●	●	●
Hybrid Mode (本地掃描+雲端查詢)			●

# 防惡意程式

- Express Mode 建議用在須避免延遲的環境下，特別是經常進行大檔案下載的這種狀況
- Stream Mode 提供離線偵測及偵測變種病毒（突變病毒有相同特徵碼）

防護高

	USG ZLD4.38	USG FLEX ZLD4.55	ATP ZLD4.55	Advantages	Disadvantages
Hybrid Mode (Local Scan + Cloud Query)			●	<ul style="list-style-type: none"> <li>Best level of Protection</li> </ul>	<ul style="list-style-type: none"> <li>Throughput limited by hardware</li> <li>Higher cost</li> </ul>
Stream Mode (Local Scan)	●	●	●	<ul style="list-style-type: none"> <li>Supports offline protection</li> <li>Better for fresh mutant malware detection</li> </ul>	<ul style="list-style-type: none"> <li>Throughput limited by hardware</li> <li>No. of Signatures limited by hardware</li> </ul>
Express Mode (Cloud Query)	●	●	●	<ul style="list-style-type: none"> <li>Over 2x performance increase (UTM)</li> <li>Threat intelligence will evolve from AI</li> <li>World leading detection rate</li> </ul>	<ul style="list-style-type: none"> <li>Won't work in isolated environment (requires internet)</li> <li>Mutant Malware may be skipped Initially</li> </ul>

Performance高

# 防惡意程式

設定

安全服務

防惡意程式

黑/白名單

- 自訂白名單/黑名單
  - 支援 MD5 Hash、File Pattern
  - File Pattern支援 wildcard

White List Black List

Check White List

+ Add Edit Remove Activate Inactivate

#	Status	Type	Value
1	🔦	File Pattern	abc.pdf
2	🔦	MD5 Hash	9A57429A0D4AD3CC2A8665FEC88EFD9F
3	🔦	File Pattern	*.pdf

Page MD5 Hash File Pattern Show 50 items

# 防惡意程式

設定

安全服務

防惡意程式

黑/白名單

- **Anti-Malware Black/White List**

- Support wildcard as input
  - Case 1 - Pattern: abc, Match file: abc
  - Case 2 - Pattern: \*abc, Match file: GGabc
  - Case 3 - Pattern: abc\*, Match file: abc.bin, abcGG.bin

防惡意程式 黑名單 特徵碼

白名單 黑名單

啟用黑名單

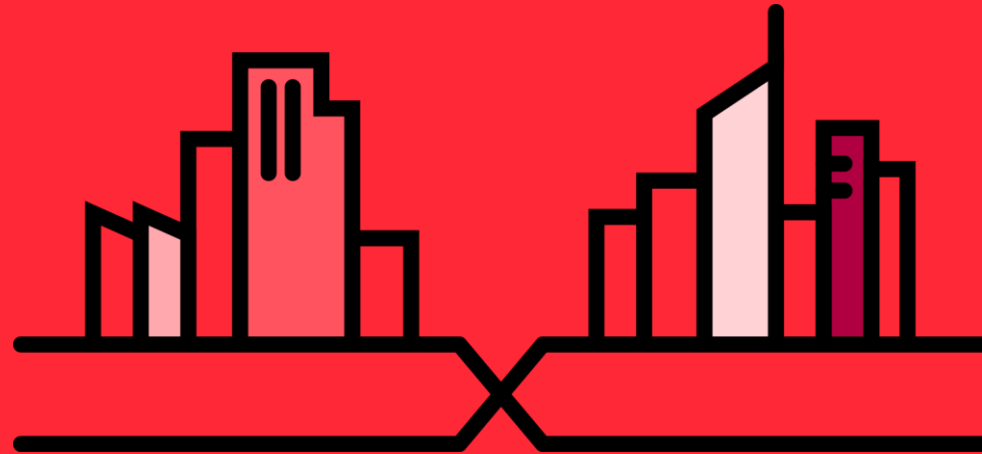
規則摘要

#	狀態	類型	Value
1	🔦	File Pattern	*abc

新增 編輯 移除 啟動 停用

第 0 頁, 共 0 頁 每頁顯示 50 行

# Secureporter



# Agenda

---

01

**SecuReporter**  
簡介

02

**SecuReporter**  
設定

03

**SecuReporter**  
示範

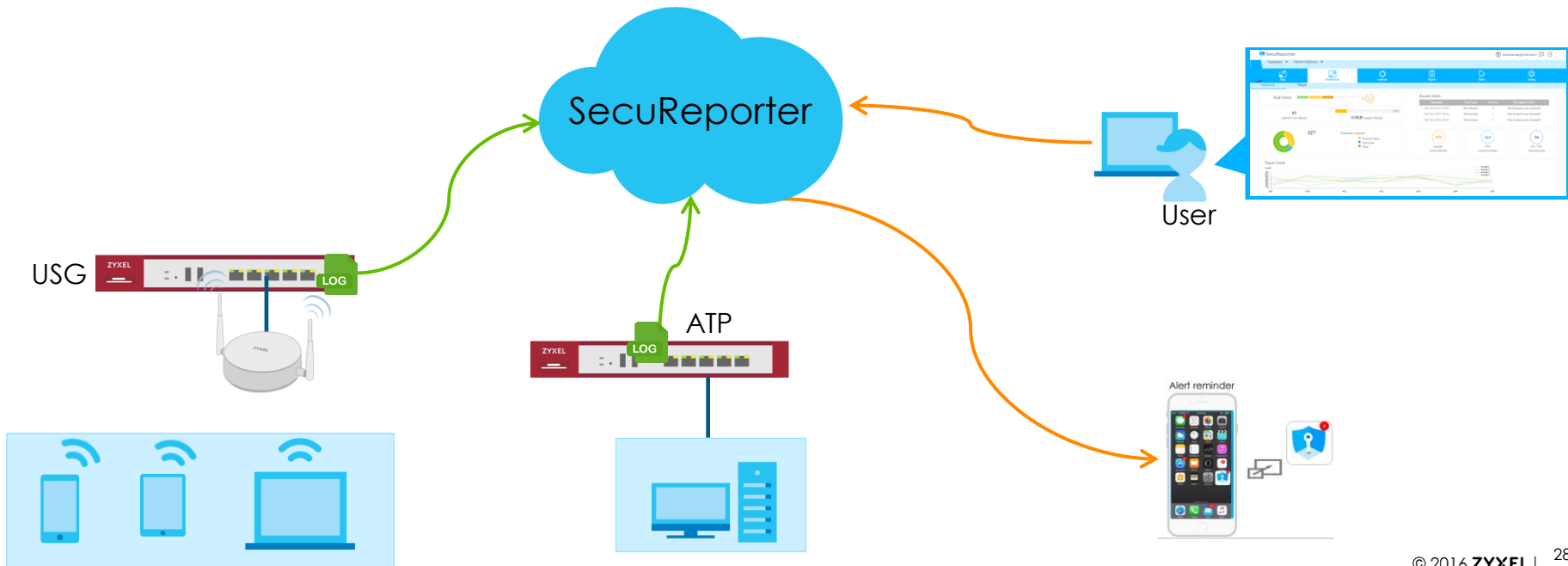
# SecuReporter 簡介





# SecuReporter 簡介

- SecuReporter 從安全閘道器上蒐集相關日誌，並運用智能技術將分析後的結果以一目了然的統計圖表/分析報告呈現



# 資料收集與保護

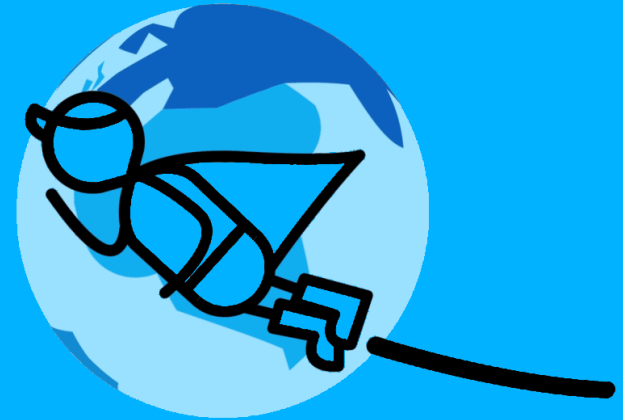
- SecuReporter 只蒐集閘道器上的log,而非全部流量.
  - Security service logs
    - ADP/IDP logs
    - Anti-Virus/Anti-Malware logs
    - Anti-Spam/Email security logs
    - Content filter logs
    - Application patrol logs
  - Traffic logs
    - Inbound/outbound traffic on each interfaces
  - Device information logs
    - CPU/Memory usage
    - Concurrent session
    - Login/logout history

# 資料收集與保護

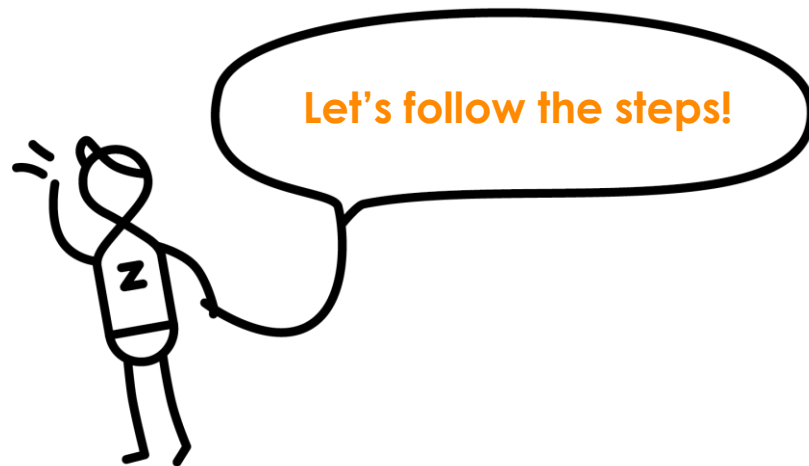
- 閘道器使用 **https** 傳送logs至 **SecuReporter** 伺服器

Protocol	Port Number	Usage
TCP	443	Device sends log data SecuReporter Server

# SecuReporter Configuration



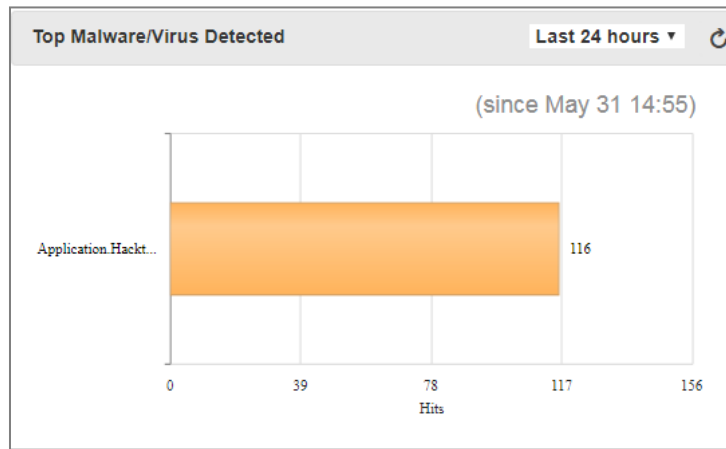
# SecuReporter的初始配置



# 閘道器開啟UTM Log

- 需先開啟UTM log 以傳送到Secureporter server
  - ADP/IDP, App patrol, Content filter, Anti-Malware, Email security

The screenshot shows the configuration page for Anti-Malware. The left sidebar contains navigation options like '設定', '+ 授權', '+ 無線', '+ 網路', '+ VPN', '- BWM', '- Web 認證', '+ 安全性策略', '- 安全服務', '- 應用程式巡査', '- 內容過濾', and '防惡意程式'. The main area is titled '防惡意程式' and includes tabs for '黑白名單' and '特徵碼'. Under '一般設定', 'Anti-Malware' is selected, and '啟用' is checked. Under 'Scan Mode', 'Express Mode' is selected. Under '相符時行動', 'log:' is set to 'log alert' in a dropdown menu, which is highlighted with a red box. A blue callout box with the text 'Select Log or Log alert' points to this dropdown menu.



# 蒐集相關統計資訊

- 您只需要收集App Patrol統計信息，該統計訊息在SecuReporter上會按應用程序顯示流量

Summary

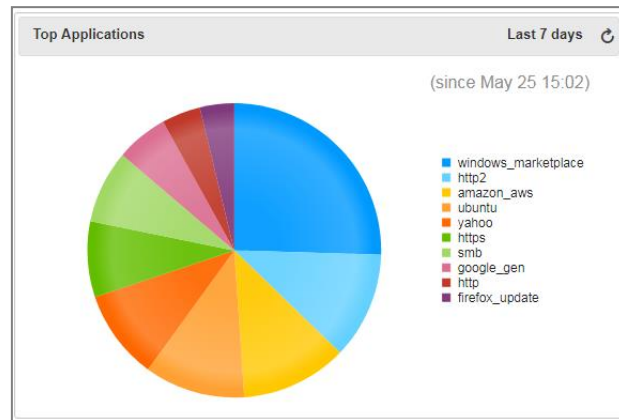
General Settings **Collect App patrol statistics**

Collect Statistics since 2018-05-30 17:27:37 to 2018-06-01 15:00:01

Apply Reset Refresh Flush Data

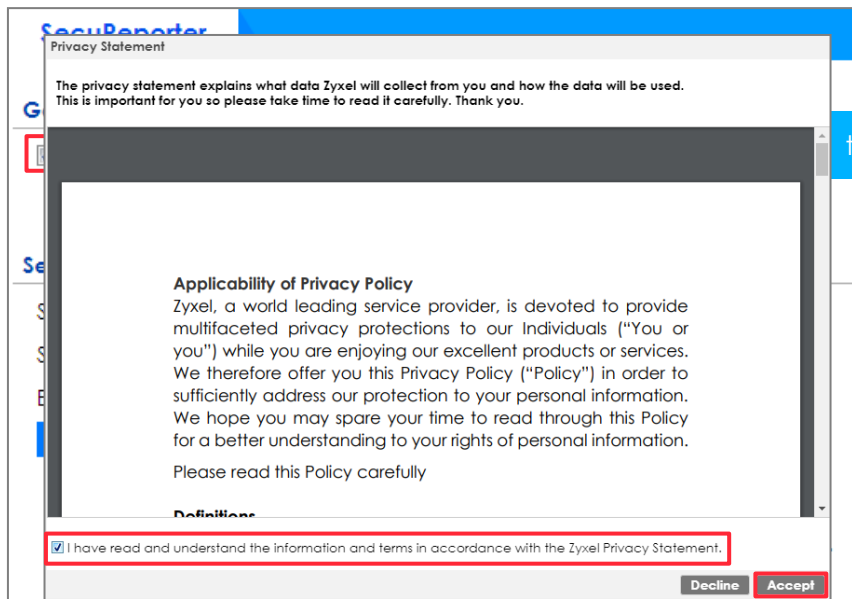
AppPatrol Statistics

#	Application	Forwarded Data[KB]	Dropped D...	Rejected D...
1	ftp_data	875127	0	0
2	windows_mark...	117503	0	0
3	http	41043	0	0
4	dropbox	27289	Application traffic	
5	google_gen	10434	0	0
6	https	10053	0	0
7	cloudflare	7259	0	0
8	teamviewer	6851	0	0
9	gstatic	6587	0	0



# 在閘道器上開啟SecuReporter

- 允許閘道器將相關log傳送到SecuReporter 伺服器
  - 設定 > Cloud CNM > SecuReporter





# 登入SecuReporter 頁面 (1/3)

- 您可以從Web GUI或 SecuReporter快速訪問

URL: <https://secureporter.cloudcnm.zyxel.com>

The screenshot displays the SecuReporter web interface. At the top, there is a blue header with the text "SecuReporter". Below the header, the "General Settings" section is visible, containing two checked options: "Enable SecuReporter" and "Include Traffic Log", each with an information icon. The "SecuReporter Service License Status" section follows, showing "Service Status: Activated" with a "Renew" link, "Service Type: Standard", and "Expiration Date: 2019-04-28". A blue button labeled "Go to the SecuReporter portal" is highlighted with a red border. A blue callout box points to this button with the text "Click to go to SecuReporter portal". Below the button, a "Note" section provides instructions: "1. If you want to activate license, please go to [portal.myzyxel.com](\"http://portal.myzyxel.com\")." and "2. See our policy on [General Data Protection Regulation \(GDPR\)\\_privacy](\"#\")."

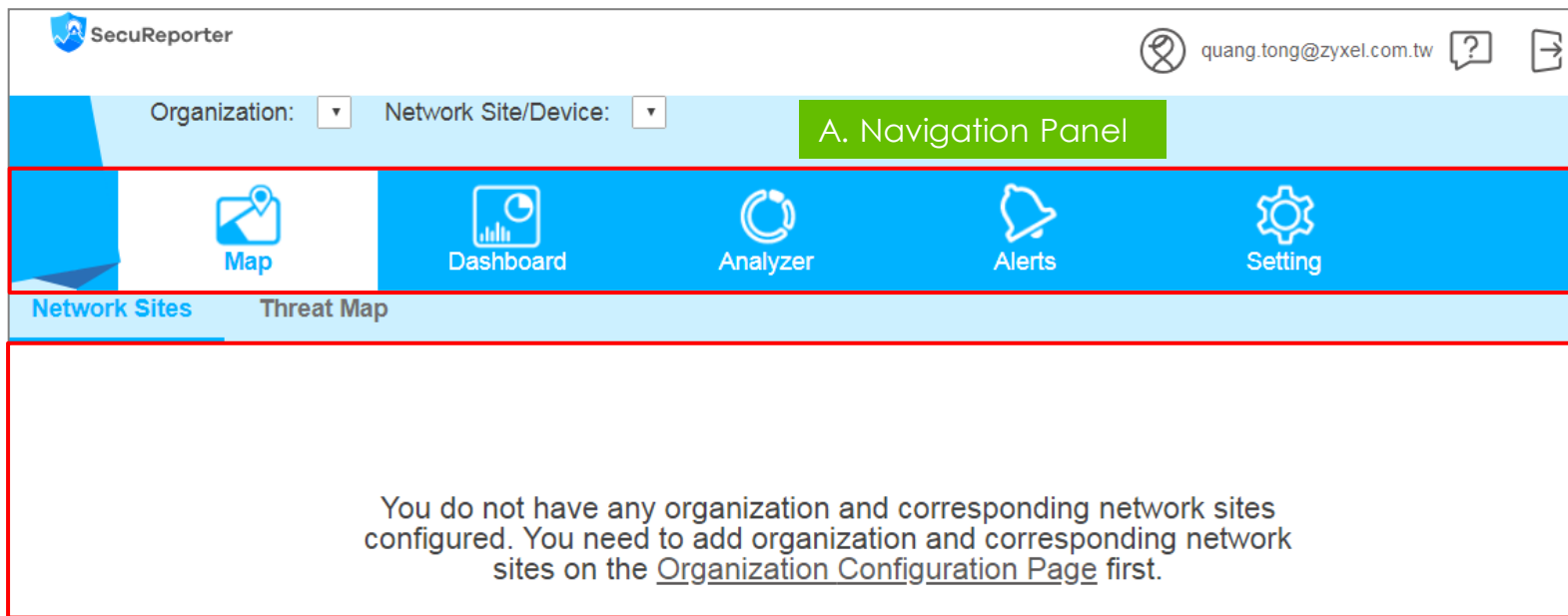
# 登入SecuReporter 頁面 (2/3)

- 在MZC登入 account

Login SecuReporter with MZC account

# 登入SecuReporter 頁面 (3/3)

- 在配置組織/站點之前，SecuReporter無法顯示網路信息。



B. Status screen

# 創建組織

- Create an organization
  - [Setting > Organization & Network Sites](#)

The screenshot displays the ZyXEL management interface. At the top, there are dropdown menus for 'Organization:' and 'Network Site/Device:'. Below these are navigation icons for Map, Dashboard, Analyzer, Report, Alerts, and Setting. The 'Setting' icon is highlighted, and the 'Organization & Network Sites' sub-tab is selected. The main content area shows a 'Summary' section with a table. A modal dialog box titled 'Organization' is open, allowing the user to add a new organization. The dialog has a close button (X) and a title bar. The 'Organization Name' field contains 'ZYXEL' and is highlighted with a red box. The 'Description' field is empty. There are 'Save' and 'Cancel' buttons at the bottom of the dialog. A green callout box points to the 'Add new organization' button in the top right corner of the dialog. Another green callout box points to the 'Organization Name' field with the text 'Name the organization'.

# 在組織中新增設備

- 將閘道器添加到組織中。
  - **Setting > Organization & Network Sites**

Organization: ZYXEL Network Site/Device:

Map Dashboard Analyzer Alerts Setting

Organization & Network Sites User Account

### Summary

+ Add Organization

	Organization	Network Sites	Unclaimed Device	Creator	Action
1	ZYXEL	0	26	quang.tong@zyxel.com.tw	Edit Delete

Add unclaimed gateway into organization

# 在組織中新增設備

- 每個閘道器都會有一個網絡站點。
  - 組織中未限定閘道器的數量。

The screenshot displays the ZyXEL management interface. At the top, the organization is set to 'ZYXEL' and the 'Network Site/Device' dropdown is open. A 'Map' icon is visible on the left. The main content area shows a 'Network Site' configuration dialog with three steps: '1. Device Setting', '2. Data protection policy', and '3. Data protection select'. The 'Device Info' section lists: Model Name: ATP200, MAC Address: E4:18:6B:FB:C4:29, and Serial Number: S162L44290003. The 'Network Site Name' field contains 'ATP200' and is highlighted with a red box, with a green callout box saying 'Name network site'. Below it is a 'Description' field. In the background, a table with columns 'M' and 'Action' is visible, with a '+' button in the 'Action' column highlighted by a red box and a green callout box saying 'Add device into organization'. At the bottom of the dialog are 'Previous' and 'Next' buttons.

M	Action
1	+
2	
3	
4	

# 在組織中新增設備

- 閱讀數據保護政策
  - 選擇符合您國家數據保護法規的數據處理類型

The screenshot shows a web-based configuration interface titled "Network Site". At the top, there are three navigation tabs: "1. Device Setting", "2. Data protection policy", and "3. Data protection select". The main content area is titled "Please select data processing" and lists three options:

- Clearing: personal information are disclosure**
  - Analysis: personal data are clear
- Pseudonymization: Replacing most identifying fields within a data record by one or more artificial identifiers, or pseudonyms.**
  - Analysis: personal data are clear
- Anonymization: personal data rendered anonymous in such a way that the data subject is not or no longer identifiable**
  - Analysis: personal data are not identifiable

A green callout box points to the "Pseudonymization" option with the text "Select the data processing method in example". A red box highlights the "Pseudonymization" option and its description. At the bottom right, there are "Previous" and "Save" buttons, with the "Save" button also highlighted by a red box.

# 在組織中新增設備

- 創建新網路站點成功

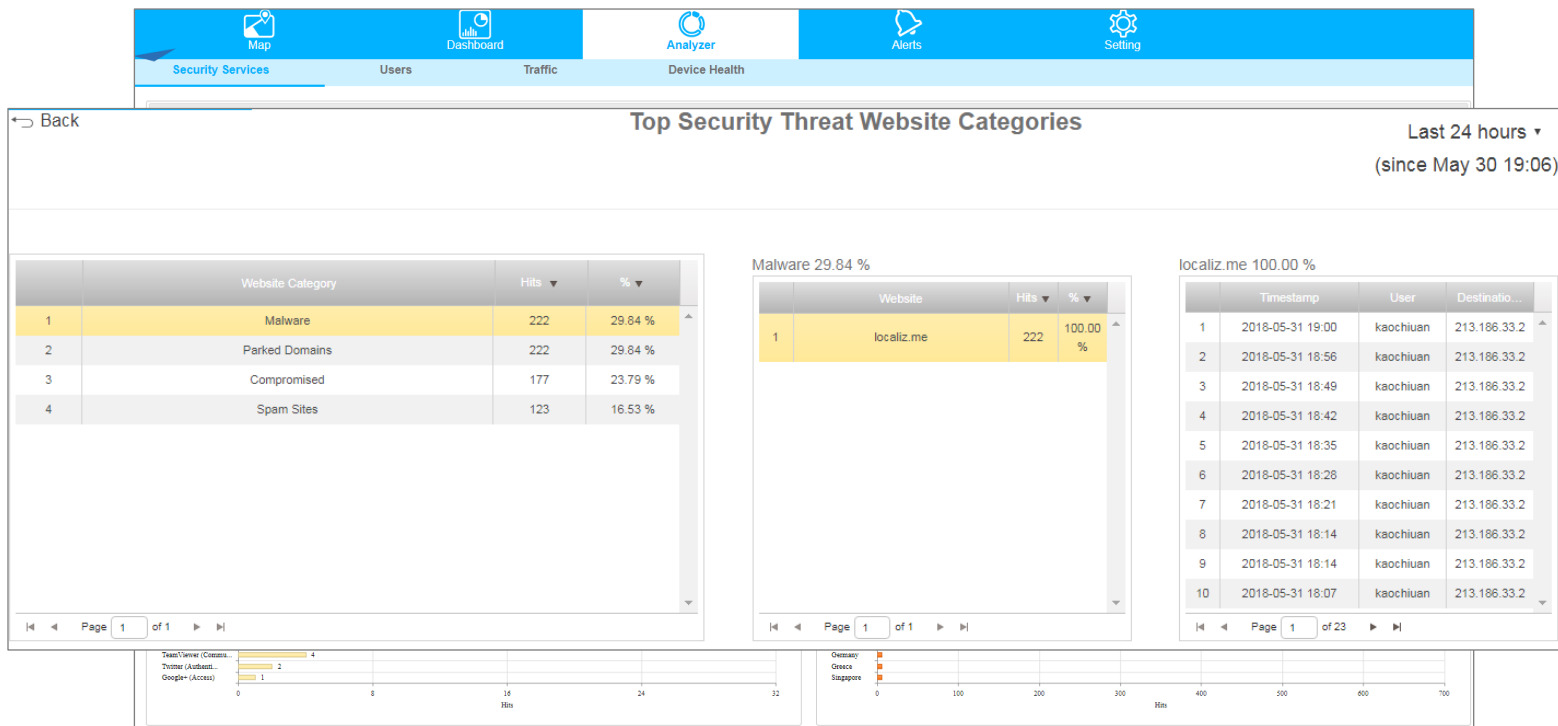
The screenshot displays the ZYXEL Network Sites management interface. At the top, the organization is set to 'ZYXEL' and the selected network site/device is 'ATP200'. The navigation bar includes icons for Map, Dashboard, Analyzer, Alerts, and Setting. Below the navigation bar, there are tabs for 'Organization & Network Sites', 'User Account', and 'Personal Data'. The main content area is titled 'ZYXEL Network Sites' and features a 'Back' button. A table lists the network sites, with one entry highlighted in red:

	Network Sites	Model Name	Firmware Version	WAN IP Address	Service Expi...	Data Processing type	Action
1	ATP200	ATP200	4.32(ABFW.0)b3	111.243.158.87	331	Pseudonymization	<a href="#">Edit</a> <a href="#">Delete</a>



# 監控網路狀態和活動

- 使用者可以觀看安全事件與網路流量,例如被阻擋的網站、偵測到的惡意軟體、應用程式使用狀況。



# 個人資料保護

- Clearing
  - 如用戶名，主機名，IP地址，MAC地址，電子郵件地址之類的所有個人信息均被披露。
- Example: Top block applications

	Application	Hits	%
1	Facebook (authority)	1541	54.57 %
2	LINE (Authentication)	257	9.10 %
3	Mozilla Firefox (access)	257	9.10 %
4	TeamViewer (Communication)	257	9.10 %
5	Gmail (Authentication)	256	9.07 %
6	Google Chrome (access)	256	9.07 %

Facebook (authority) 54.57 %			
	User	Hits	%
1	Jacky	1285	83.39 %
2	admin	256	16.61 %

Personal information is disclosure

# 個人資料保護

- 部分匿名
  - 針對某位使用者的個人資訊進行匿名處理

Personal Data Category: User Name

Raw value	Protected value	
1 admin	USER-5b1edb21-da92-59a2-a185-42fb2effa9b5	X Delete
	USER-b70004b5-0ed5-56f7-8a01-6e6ab4d7c0ba	X Delete
		X Delete
		X Delete
5 kaochiuan		

Personal information in plaintext

Personal information in ciphertext

Delete to anonymize

Application	Hits	%
1 Facebook (authority)	1541	54.57 %
2 LINE (Authentication)	257	9.10 %
3 Mozilla Firefox (access)	257	9.10 %
4 TeamViewer (Communication)	257	9.10 %
5 Gmail (Authentication)	256	9.07 %
6 Google Chrome (access)	256	9.07 %

Facebook (authority) 54.57 %

User	Hits	%
1 Jacky	1285	83.39 %
2 USER-5b1edb21-da92-59a2-a185-42fb2effa9b5	256	16.61 %

\*Note: Anonymizing personal data is not recoverable

# 個人資料保護

- Anonymization
  - 預設情況下，所有個人信息都是匿名的
- Example: Top block applications

	Application	Hits ▼	% ▼
1	Facebook (authority)	1541	54.57 %
2	LINE (Authentication)	257	9.10 %
3	Mozilla Firefox (access)	257	9.10 %
4	TeamViewer (Communication)	257	9.10 %
5	Gmail (Authentication)	256	9.07 %
6	Google Chrome (access)	256	9.07 %

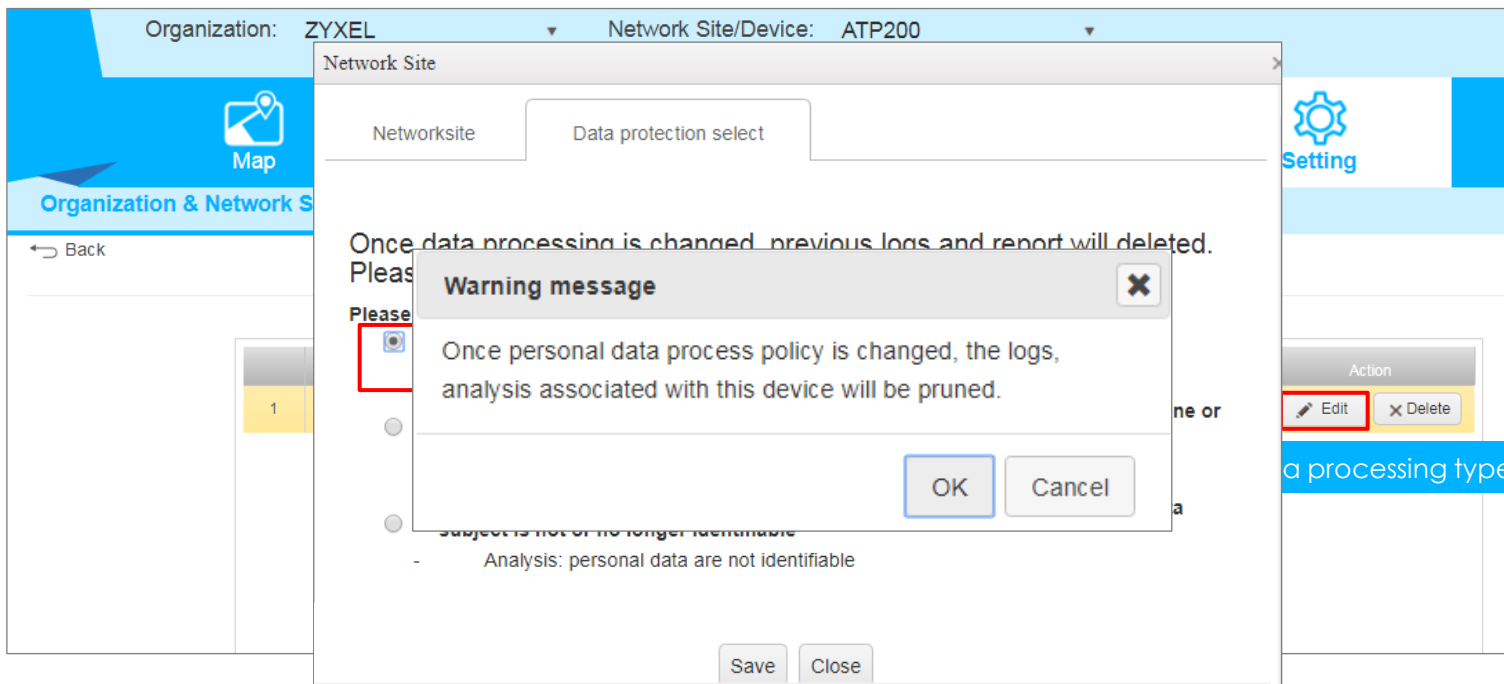
  

	User	Hits ▼	% ▼
1	USER-e2e586cf-c996-5e7d-8ddd-ca5ac0d747f8	1285	83.39 %
2	USER-5b1edb21-da92-59a2-a185-42fb2effa9b5	256	16.61 %

All personal information are anonymized

# 更改數據處理類型

- 更改數據處理類型後，該閘道器所有先前分析的日誌和相關信息將被刪除。



# 在組織中刪除設備

- 刪除設備/網路站點後，所有之前分析過的日誌及相關信息將被刪除。

Organization: ZYXEL Network Site/Device: ATP200

Map Dashboard Analyzer Alerts Setting

Organization & Network Sites User Account Personal Data

← Back

**Network site delete message**

Once claim device is deleted, the logs, analysis and reports associated with this device will be pruned and this device will be moved to unclaim device. Please download the logs and reports before delete this device.

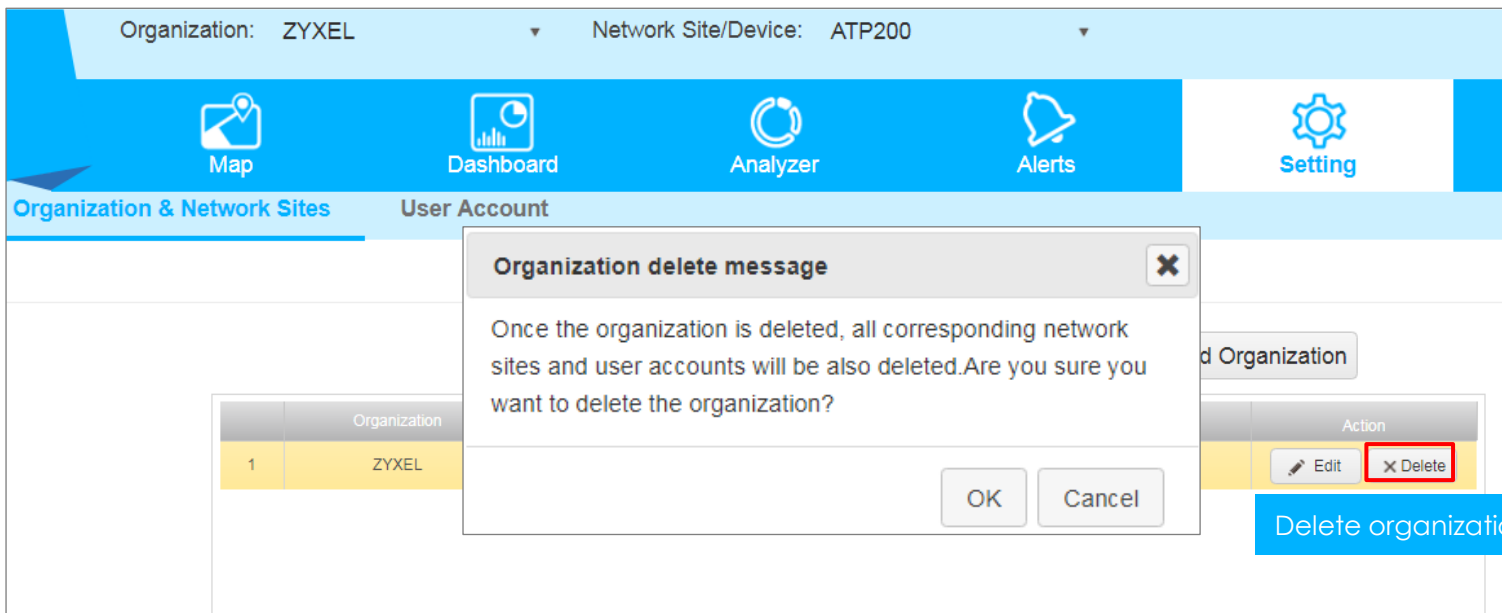
OK Cancel

Processing type	Action
Optimization	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

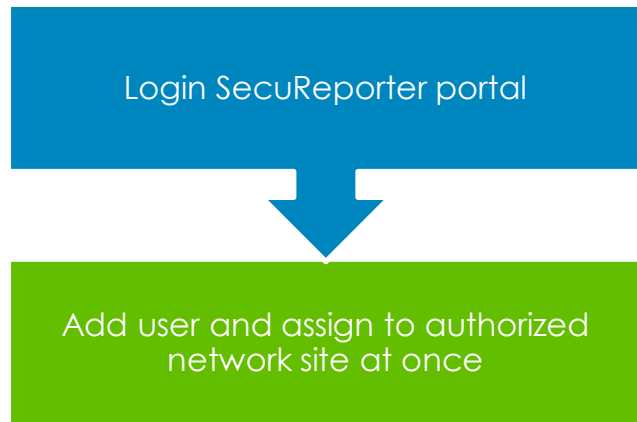
Delete gateway or network site

# 刪除組織

- 刪除組織後，所有相應的站點和使用者帳戶也將被刪除。



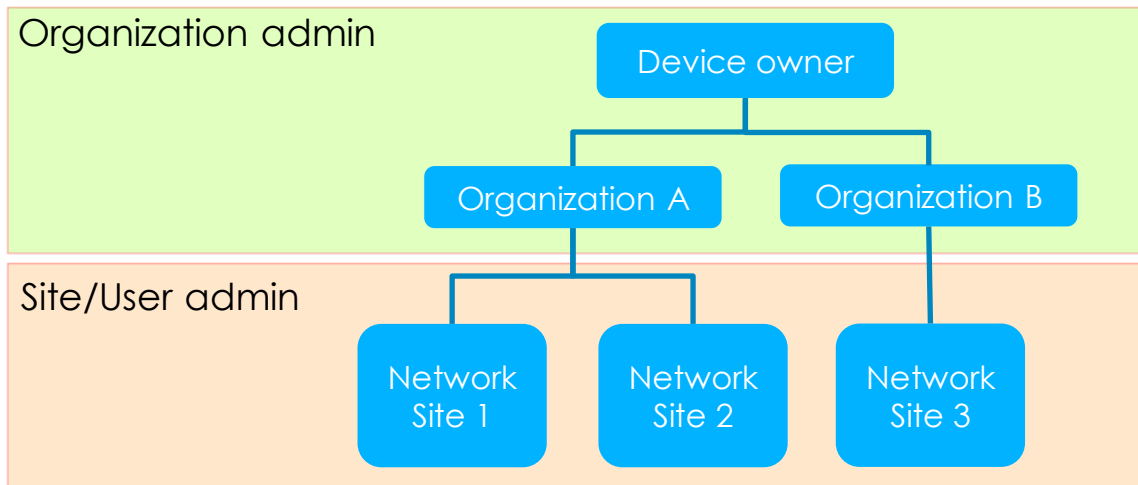
# 在SecuReporter Portal新增使用者





# 使用者角色類型

- SecuReporter 使用者有三種類型來管理組織



Role Type	SSO (MZC)	Privilege
Organization admin	Yes	- Full access for whole organizations
Site admin	Yes	- Full access for assigned site
Site user	Yes	- Monitor only for assigned site

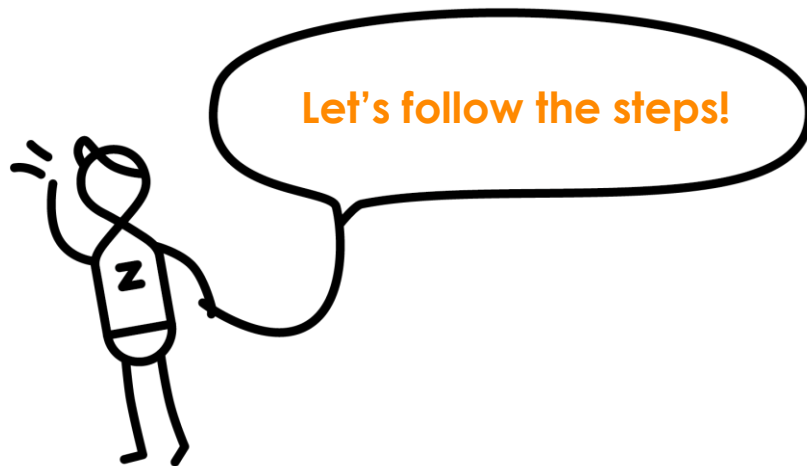
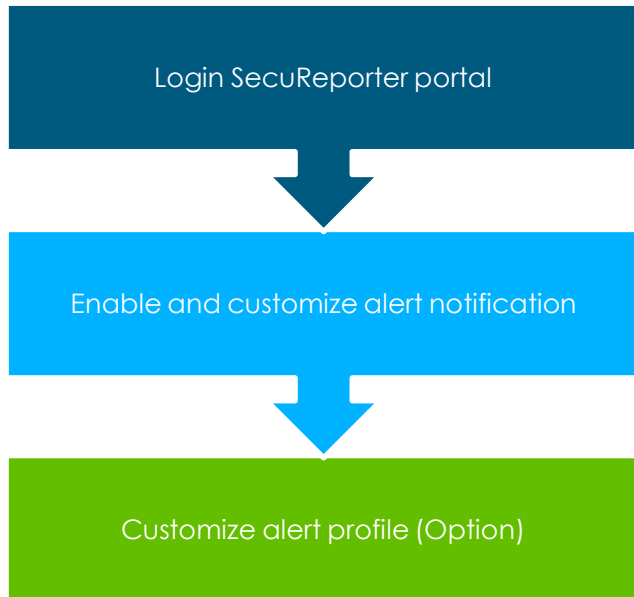
# 在SecuReporter Portal新增使用者

- 您可以新增使用者，將其分配到授權的網路站點
  - 使用者必須在MZC上註冊以登入SecuReporter
  - [Setting > User Account > Add User](#)

The screenshot shows the 'User Account' configuration window. The 'Login Email' field is highlighted with a red box and contains 'charnyster@gmail.com'. A blue callout box points to this field with the text 'User's email registered on MZC'. Below the email field is a table with columns: 'Organization / Devices', 'Default Organization R...', 'Admin Role', and 'User Role'. The 'ATP200' row is highlighted with a red box, and a blue callout box points to its 'Admin Role' checkbox with the text 'Assign to be site admin'. To the right of the table, the 'Add User' button is highlighted with a red box. Below it, a blue callout box points to a 'new user' button. At the bottom of the window, 'Save' and 'Cancel' buttons are visible.

Organization / Devices	Default Organization R...	Admin Role	User Role
賽成工業	None	<input type="checkbox"/>	<input type="checkbox"/>
▶ CHUYANG	None	<input type="checkbox"/>	<input type="checkbox"/>
Merry	None	<input type="checkbox"/>	<input type="checkbox"/>
ZyTC	None	<input type="checkbox"/>	<input type="checkbox"/>
◀ ZyTPE	None	<input type="checkbox"/>	<input type="checkbox"/>
ATP200		<input checked="" type="checkbox"/>	<input type="checkbox"/>
CHT_testing_ATP500		<input type="checkbox"/>	<input checked="" type="checkbox"/>
CSO_500		<input type="checkbox"/>	<input type="checkbox"/>
USG110		<input type="checkbox"/>	<input type="checkbox"/>

# 使用電子郵件發送告警通知



# 啟動與設定告警通知

- 啟動告警通知：讓 SecuReporter 傳送符合觸發條件的告警訊息給使用者
  - Alerts > Custom Alerts

The screenshot shows the 'Custom Alerts' configuration page in the SecuReporter interface. The page is titled 'Trend & List' and 'Custom Alerts'. It features several configuration options:

- Email Notification:** A toggle switch is set to 'ON', with a blue callout box stating 'Enable alert notification via email'.
- Email Title & Description:** A text box contains 'The Alert Notification From SecuReporter' and a description box contains 'Please check the following alert from ATP200 network site'. A blue callout box points to these fields, stating 'Email title & description (Optional)'.
- Event Severity:** Checkboxes for 'High', 'Medium', and 'Low' are visible, with 'High' and 'Medium' selected. A blue callout box states 'Select event severity which be alerted when criteria match'.
- Email Group:** Two lists are shown: 'User Account' (containing 'quang.tong@zyxel.com.tw' and 'test@gmail.com') and 'Email Recipients' (containing 'zyxel4you@gmail.com'). A blue callout box points to the 'Email Recipients' list, stating 'Add recipient's email address from group user's'.
- Alert Profile:** A table at the bottom lists alert profiles. A blue callout box points to the table, stating 'Alert profile'.

Category	Event Type	Alert Criteria	Severity	Threshold
Network Security	Attack counts	Highest Severity Attack counts > threshold within 5 minutes.	High	1 counts
Network Security	Attack counts	Attack counts > threshold within 5 minutes.	High	10 counts
Network Security	Malware/virus detection	malware/virus attack counts > threshold within 5 minutes.	High	10 counts

# 自定義告警配置資料

- Alert profiles are classified into high, medium and low severity. Some alert profiles allow user edit threshold

Alert Profile

Category	Event Type	Alert Criteria	Severity	Threshold
Network Security	Attack counts	Highest Severity Attack counts > threshold within 5 minutes.	High	1 counts
Network Security	Attack counts	Attack counts > threshold within 5 minutes.	High	10 counts
Network Security	Malware/virus detection	malware/virus attack counts > threshold within 5 minutes.	High	<input type="text" value="10.00"/>
Network Security	Malware/virus detection	Same malware/virus detected times > threshold within 15 minutes.	Medium	
Network Security	Alert counts	Alert counts > threshold.	High	
Network Site/GW	Online status	Device off-line for more than 15 minutes	Medium	15 mins
Network Site/GW	Concurrent sessions	Session numbers > 90%	Low	90 %
Anomaly	Login failure	Login failure over threshold within 1 minutes	Medium	10 times
Anomaly	Traffic anomaly	Number of scan/flood detected > threshold within 5 minutes	High	1 counts
		Number of TCP/UDP/ICMP/IP decoder > threshold within 5		

Page 1 of 1

Edit alert threshold to meet user's

# 告警資料-可調整

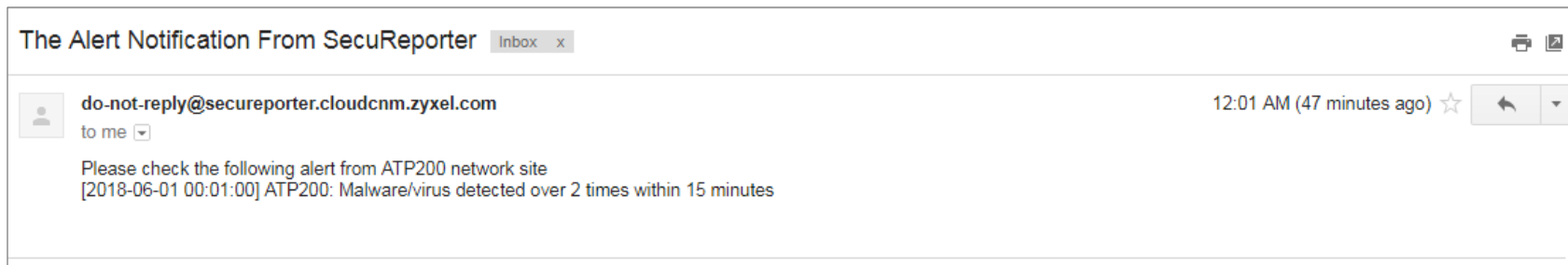
Alert Criteria	Severity (Fixed)	Default Threshold (Configurable)
Attack counts > threshold within 5 minutes.	High	10 counts
Malware/virus attack counts > threshold within 5 minutes.	High	10 counts
Alert counts > threshold.	High	10 counts
Number of scan/flood detected > threshold within 5 minutes	High	1 counts
Number of TCP/UDP/ICMP/IP decoder > threshold within 5 minutes	High	1 counts

# 告警資料-不可調整

Alert Criteria	Severity (Fixed)	Default Threshold (Fixed)
Highest Severity Attack counts > threshold within 5 minutes.	High	1 counts
Same malware/virus detected times > threshold within 15 minutes.	Medium	2 times
Device off-line for more than 15 minutes	Medium	15 minutes
Login failure over threshold within 1 minutes	Medium	10 times
Session numbers > 90%	Low	90 %

# 告警訊息範例

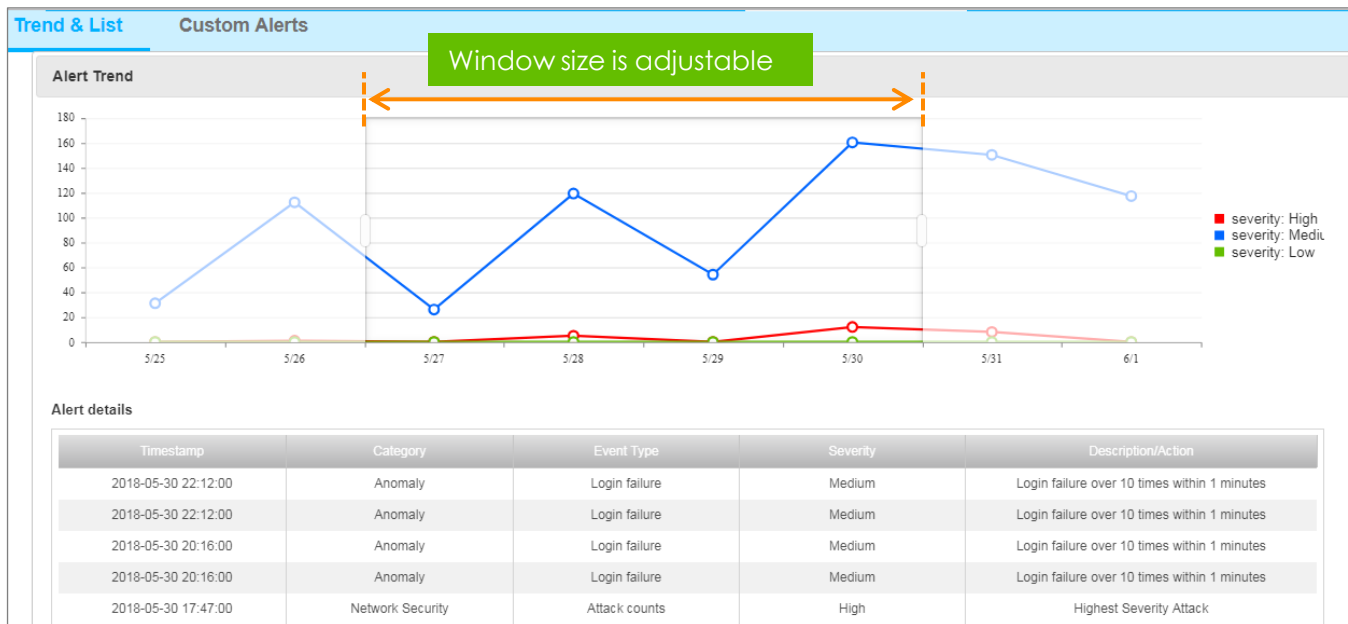
- 告警訊息可幫助您追蹤異常的網路活動，例如設備離線、偵測到病毒。
- 每條訊息都顯示事件發生的日期和時間。



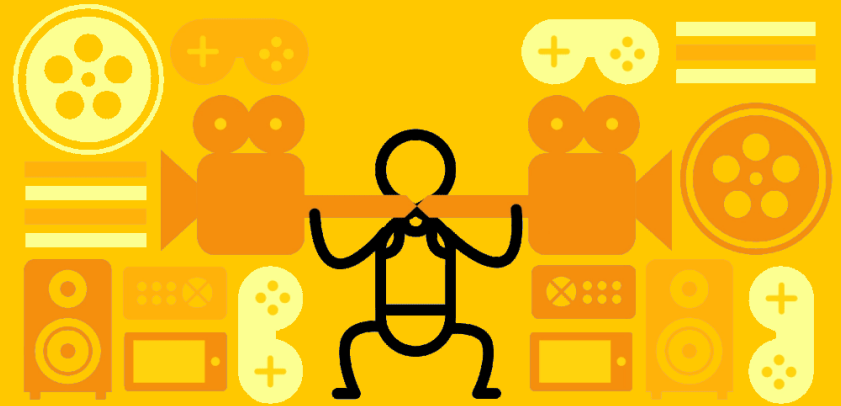


# SecuReporter Portal 告警保留

- SecuReporter portal 過去7天的告警
  - Alert > Trend & List



# Appendix



# Log Resource

Main menus	Sub menu		Log Resource	Note
Analyzer	Security Services	Threat trend	IDP, ADP, Anti-Malware, Email Security, Content Filter	
		Top blocked websites	Content Filter (blocked websites)	
		Top security threat website categories	Content Filter ( Security Threat Web Pages)	Has not supported for ATP
		Top blocked applications	App Patrol (blocked applications)	
		Top blocked destination countries	IDP, ADP, App Patrol, Content Filter	
		Anomaly packet trend	ADP	
		Application patrol	App Patrol (allowed and blocked applications)	
		IDP	IDP	
		Top malware/virus detected	Anti-Malware	
		Top spam received	Email Security	
		Top spam sent	Email Security	
		Top Potentially malicious websites	Content Filter (Security Threat Web Pages)	Has not supported for ATP
	Most popular applications	App Patrol (allowed applications)		
	Most popular websites	Content Filter (allowed websites)		
	Most popular website categories	Content Filter (allow website by categories)		
	Users	Security events	IDP, ADP, Anti-Malware, Email Security, Content Filter	
		Application usage	App Patrol statistics	
		Website usage	Content Filter	
Top destination countries		Traffic log		
Login/Logout history		Device information log		
Traffic upload/download usage trend		Traffic log		
Device Health	CPU/Memory usage trend	Device information log		
	Concurrent sessions	Device information log		
	Interface traffic usage trend	Device information log		
Map	Threat Map	Threat Map	ADP, Anti-Malware, IDP, Email Security	
Dashboard	Risk Factor	Malware/virus detected	Anti-Malware	
		Requests blocked	ADP, IDP, Content Filter, Application Patrol	
		Total emails inspected	Email Security	

# 安全日誌的預設定義嚴重性

Security log type		Severity
ADP		2
IDP		1-5 (Defined by device signature)
Anti-Malware		4
Spam		3
App Patrol	Blocked application	1

# 安全日誌的預設定義嚴重性

Security log type		Severity	
Content Filter	Blocked website	1	
	Security threat website	Botnets	4
		Compromised	4
		Malware	4
		Phishing & Fraud	4
		Spam sites	3
		Parked Domains	3
		Anonymizers	2
		Network Errors	1



☑ 您需要詢價、功能解說嗎？

☑ 您有遇到網路建置的問題嗎？

# 來Line問就對了

## 這裡問最快，不怕電話佔線沒接到

快line Zyxel小編，讓我們協助您^^



**ZYXEL**

Your Networking Ally