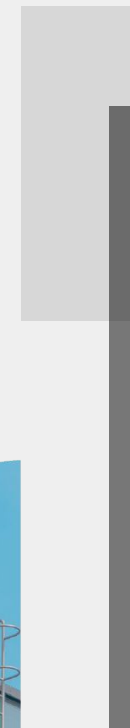
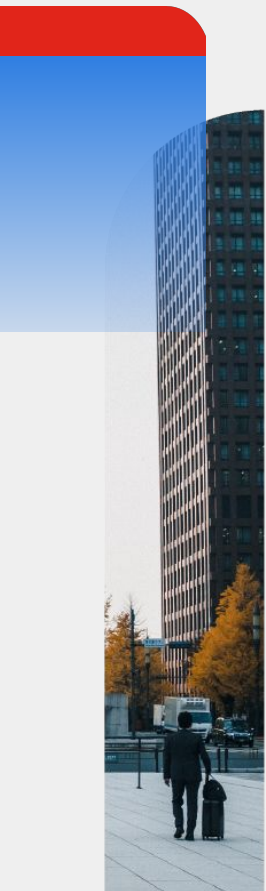


**FORTINET**<sup>®</sup>



# 正面迎戰!加密流量這場戰役你我都不缺席 FortiProxy+FortiSandbox

Josh Lin  
Technical Consultant Taiwan



# 人類世界不可缺少的三要素



陽光



空氣



水

# 資安世界不可缺少的三要素



可視性



即時回應



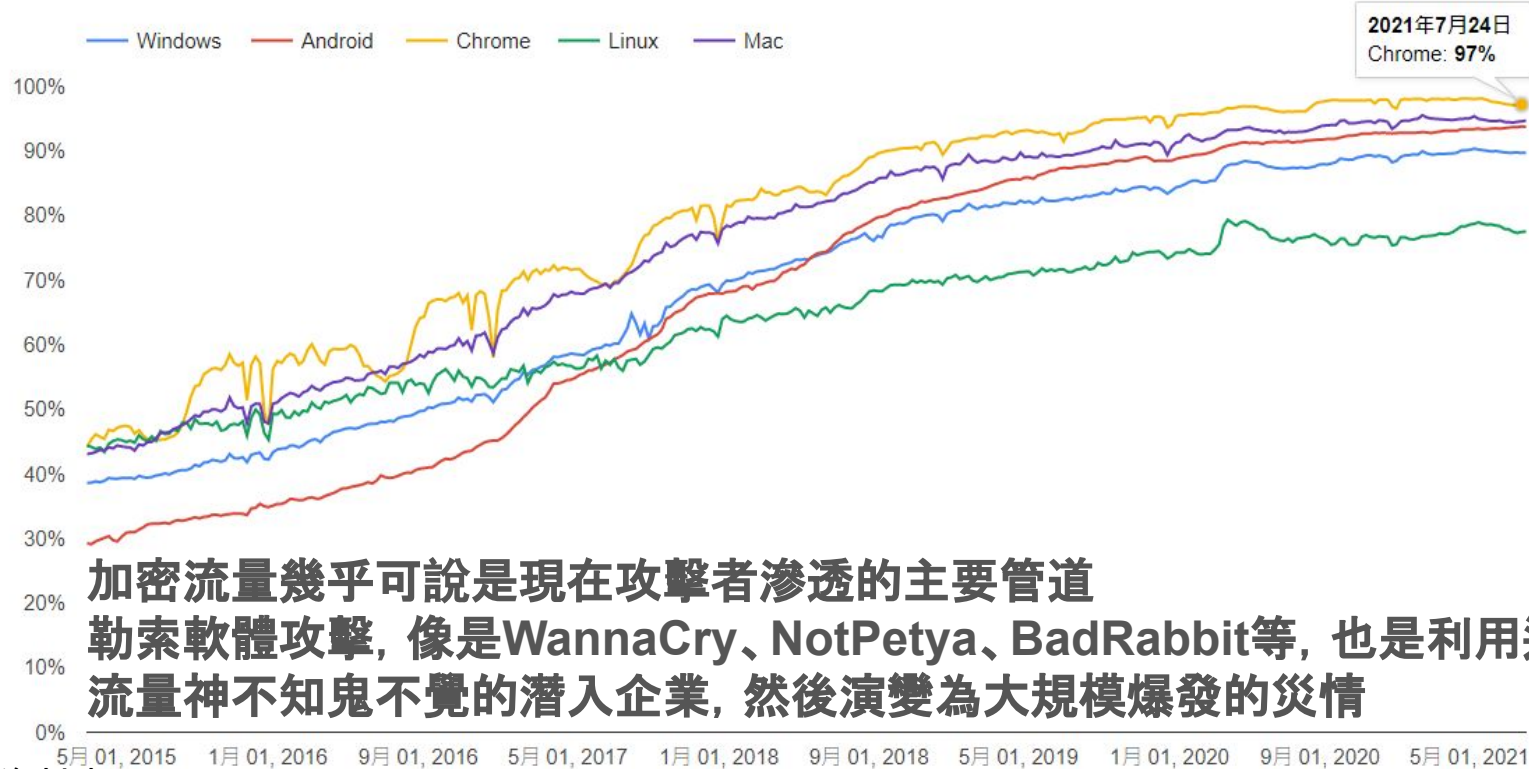
加密流量

# 加密流量已成主流

水能載舟亦能覆舟，加密流量已遭攻擊者濫用



使用 Chrome 載入 HTTPS 網頁的百分比 (依平台分類)



加密流量幾乎可說是現在攻擊者滲透的主要管道  
勒索軟體攻擊，像是WannaCry、NotPetya、BadRabbit等，也是利用這  
流量神不知鬼不覺的潛入企業，然後演變為大規模爆發的災情

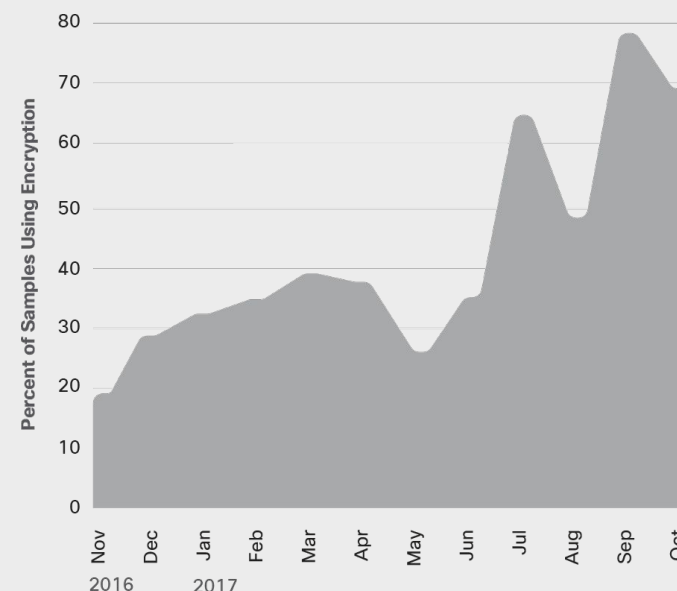
\*資料來源:

<https://transparencyreport.google.com/https/overview>

<https://blogs.cisco.com/security/as-encrypted-malicious-web-traffic-increases-defenders-need-advanced-tools-that-provide-visibility>

Increase in volume of malicious binaries leveraging some encrypted network communication

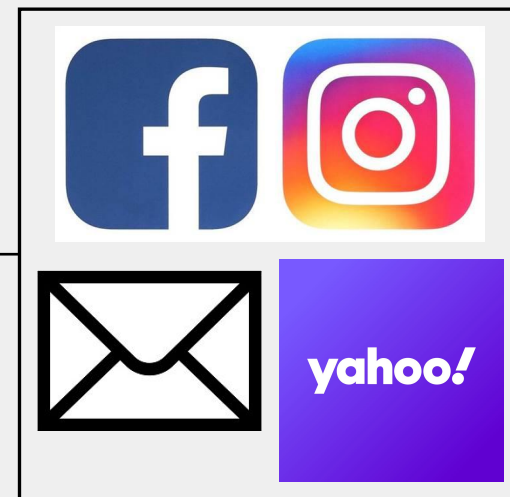
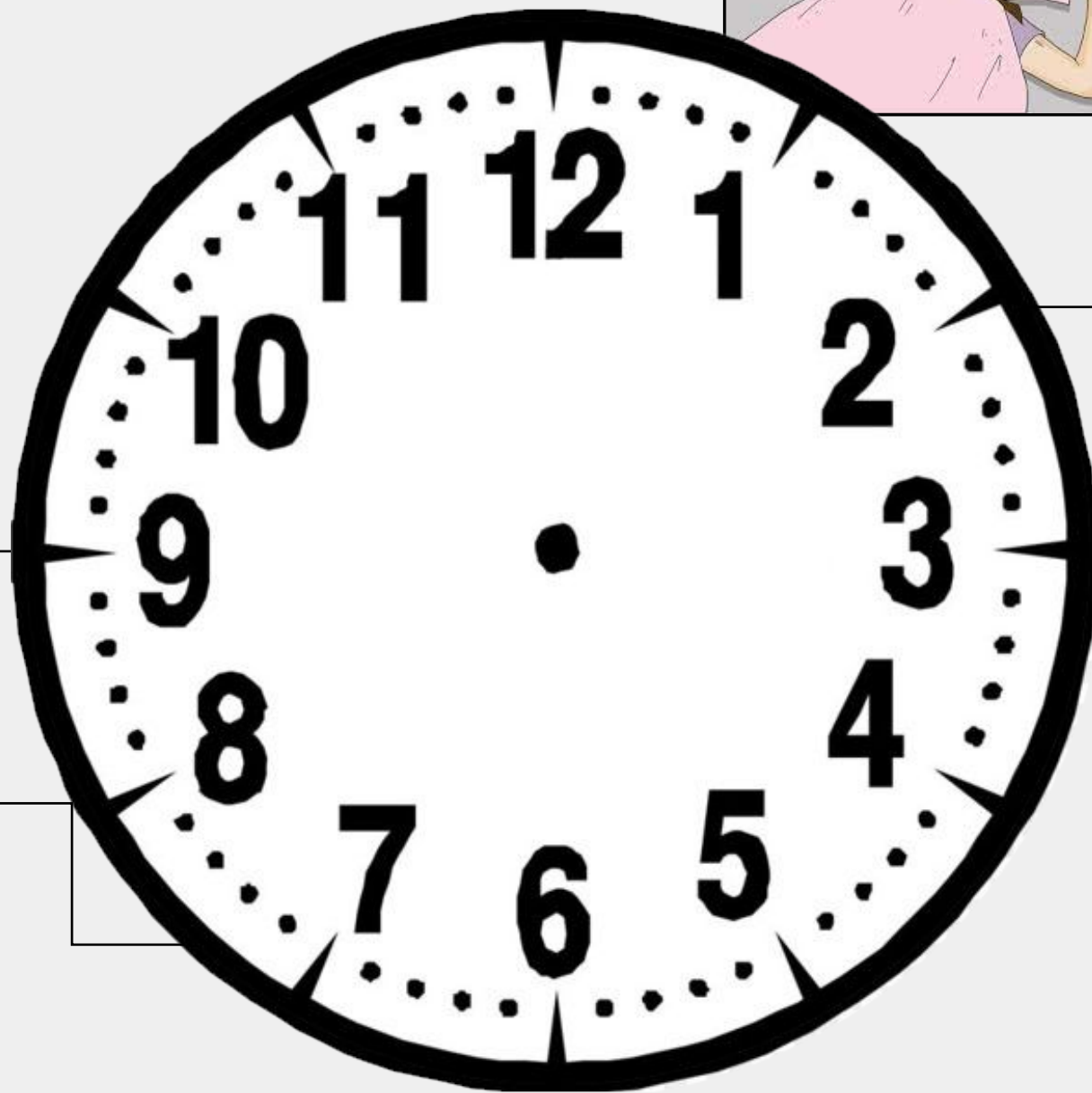
Source: Cisco Security Research



For more info visit: [cisco.com/go/acr2018](https://cisco.com/go/acr2018)



# 網路和生活已密不可分

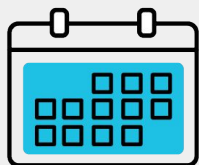


# 90% 的網路攻擊來自於網頁瀏覽和郵件

## 網頁瀏覽威脅



**1,400+**  
每年有新的瀏覽器外掛  
程式, 含有惡意威脅



**78%** 的網站可被用於  
惡意軟體下載



每  
秒 **4**  
一個未知的惡意軟體被下載

## 郵件和釣魚威脅

**83%**

的增長是由釣  
魚郵件啟動



**55%**

的大企業是釣叉式釣魚攻擊  
的目標

**12%**

使用者點擊了不被信任  
的連結或附件

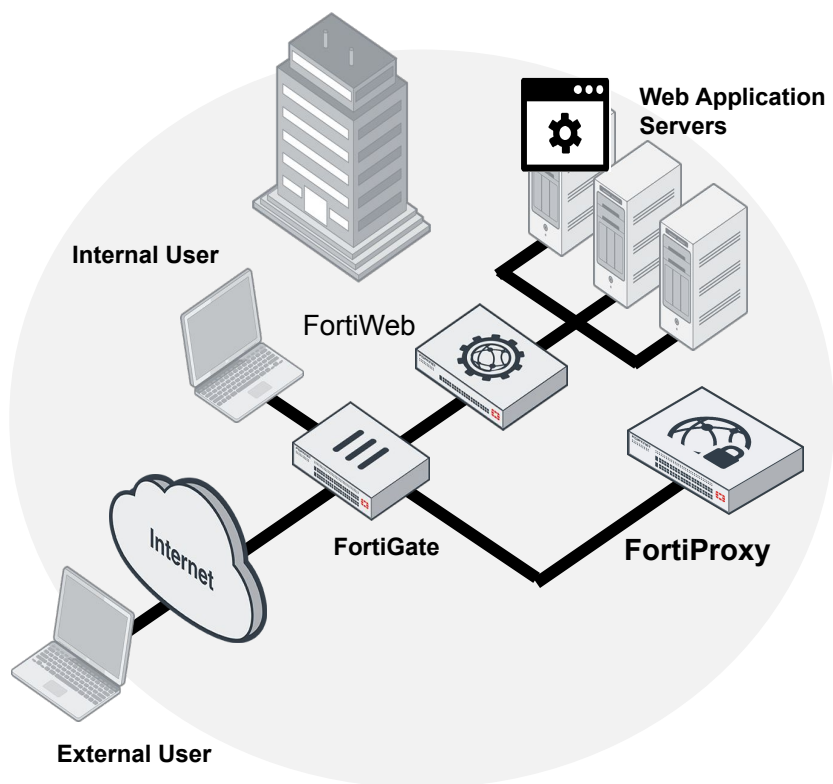


# 上網安全閘道 - Gartner怎麼說？

## Gartner

上網安全閘道(SWG)利用URL過濾, 進階威脅和傳統惡意軟件防禦, 保護用戶免受**網際網路的威脅**, 並**幫助企業實施合規公司策略的上網政策**

今日上網安全閘道(SWG)的部署, 主要是因為它們的安全功能。專注於**提供強大的阻擋惡意軟體和進階威脅檢測功能**的供應商最有能力在這個市場中獲得領先優勢地位



\*資料來源: <https://www.gartner.com/en/information-technology/glossary/secure-web-gateway>

# 為什麼要專屬的加解密設備

## NSS Labs Findings

- The average proportion of SSL traffic within a typical enterprise is 25% – 35%.
- The NSS threat database<sup>1</sup> has uncovered a small percentage (~1%) of malware using SSL.
- NSS research indicates that the majority of threats that are using SSL as a transport fall under the targeted persistent attack (TPA) category.
- The mean average of performance loss across 7 NGFW's:
  - ~74% with 512b and 1024b ciphers
  - ~81% with 2048b ciphers.
- The mean average of transactions per second (TPS) loss across 7 NGFW's:
  - ~86.80% with a 512b cipher
  - ~87.79% with a 1024 cipher
  - ~92.28% with a 2048 cipher
- The Sourcefire NGFW had the highest rated TPS performance. However, Sourcefire was the only vendor that used a dedicated SSL appliance.
- The Dell SonicWALL SuperMassive E10800 NGFW had the highest rated TPS performance with onboard SSL decryption.
- Juniper was rated the best with regards to performance loss and reduction in TPS.
- All vendors had significant performance issues and TPS loss with 2048b ciphers.
- **NSS has concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices.**





# 加密流量管理的最佳工具



- 高效能與可擴充的代理 (Proxy) 設備
- 專屬**上網防護**及**加密流量管理**解決方案
- 按需購買的授權方案(Pay As You Grow)
- 多層次偵測與預防威脅機制
- 使用認證授權的 **WEB 應用程式控管**
- 網路**頻寬優化**與進階網頁內容快取機制



## SSL 加密流量解析



- 硬體加速專用晶片
- 加密流量的可視化
- 多種威脅檢測保護

## 多層次防禦策略



- 整合世界級 FortiGuard 威脅情資
- 支援整合地端/雲端 FortiSandbox

## 認證存取機制



- 精細的應用程式控管政策
- 即時主動式的活動監控
- 基於用戶或群組的社群網站限制存取

# 多層安全防護及強大的效能

## 安全防護

- Intrusion Prevention System
- Application Control
- Antivirus
- Web Filtering
- DNS Filtering
- Web Rating Overrides
- Data Leak Prevention
- SSL-VPN
- SSL IPsec
- External threat inspection list
- SSL/SSH Inspection
- Content Analysis (3<sup>rd</sup> party solution)
- User Authentication
- Sandbox Inspection Integration (On-Premises and Cloud)

## 效能

- Full Proxy Application
- Content Caching
- WAN Optimization
- Video Caching & Stream Splitting

## 行為可視性

- Monitor and Logging
- FortiAnalyzer Integration
- FortiView Integration
- FortiCloud Intergation



# 彈性且細緻的控管能力

FortiProxy VM64 FPX-VM

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Policy > Traffic Shapers > Traffic Shaping Policy > Central SNAT > Pac Policy > Policy Test > **Addresses** ☆ > Internet Service Database

New Address

Category: Address | IPv6 Address | **Proxy Address**

Name:

Color: [Change]

Type: **✓ URL Pattern** | Host Regex Match | URL Category | HTTP Method | User Agent | HTTP Header | Advanced (Source) | Advanced (Destination)

Host:

URL Path Regex:

Show in Address List:

Comments:

OK Cancel



# 應用程式識別

**Edit Application Service**

Name: YouTubeApps

Proxy:  Enable  Disable

Protocol: ALL

Application Service Type:  Disable  Application ID  Application category

Application category: Video/Audio

TCP PortRange: 0 - 65535

**Select Entries**

Search: [ ]

- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Industrial
- Mobile
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio**
- VoIP
- Web.Client

**Edit Application Service**

Name: Facebook

Proxy:  Enable  Disable

Protocol: ALL

Application Service Type:  Disable  Application ID  Application category

Application ID:

- Facebook
- Facebook\_AppName
- Facebook\_Apps
- Facebook\_Chat
- Facebook\_File.Download
- Facebook\_File.Upload
- Facebook\_Like.Button
- Facebook\_Login
- Facebook\_Messenger.Image.Trans
- Facebook\_Messenger.Video.Trans
- Facebook\_Messenger.Voice.Mess:
- Facebook\_Messenger.VoIP.Call
- Facebook\_Personal
- Facebook\_Plugins
- Facebook\_Post
- Facebook\_Search
- Facebook\_Video.Play

TCP PortRange: 0 - 65535

**Select Entries**

Search: [ ]

- FIREWALL APPLICATION (2,098)
- Business (148)
- Acronis.Snap.Deploy**
- Act!
- ActiveCampaign
- ActiveCampaign\_File.Upload
- ADP
- AirWatch.MDM
- Alibaba
- Apache.Cassandra
- Applane.CRM
- Atlassian.JIRA
- AutoDesk.360
- AutoDesk.360\_Upload
- Autodesk.Buzzsaw
- Baidu.PC.Faster
- BambooHR
- BambooHR\_File.Download
- BambooHR\_File.Upload
- Base.CRM
- Blinksale
- Brightpearl
- Bugzilla
- Censhare
- Centrify
- Channels.Manager



# Policy設定&検査順序

Name	Source	Destination	Schedule	Service	Action	Security Profiles	Log
web-proxy → port1 15							
	<ul style="list-style-type: none"> <li>r/https-post/</li> <li>r/proxy-connection</li> </ul>	all	always	webproxy	DENY	<ul style="list-style-type: none"> <li>PRX default</li> <li>SSL certificate-inspection</li> </ul>	All
	<ul style="list-style-type: none"> <li>all</li> <li>my-grp-ntlm</li> <li>ljosh</li> </ul>	all	always	webproxy	ACCEPT	<ul style="list-style-type: none"> <li>WEB default</li> <li>PRX default</li> <li>SSL deep-inspection</li> </ul>	All
Auth by SSO	<ul style="list-style-type: none"> <li>all</li> <li>my-grp-ntlm</li> <li>ljosh</li> </ul>	all	always	webproxy	ACCEPT	<ul style="list-style-type: none"> <li>WEB default</li> <li>APP default</li> <li>PRX default</li> <li>SSL certificate-inspection</li> </ul>	All
hd/referrer test	all	4xion-preload	always	webproxy	ACCEPT	<ul style="list-style-type: none"> <li>PRX default</li> <li>SSL deep-inspection</li> </ul>	All
	all	<ul style="list-style-type: none"> <li>*.cnn.com</li> <li>*.ruten.com.tw</li> </ul>	always	webproxy	DENY	<ul style="list-style-type: none"> <li>PRX default</li> <li>SSL certificate-inspection</li> </ul>	Disabled



# Policy元件的組成

1

Type	Explicit
Name	Auth by SSO
Explicit Web Proxy	web-proxy
Outgoing Interface	port1
Source	all ljosh my-grp-ntlm
Destination	all
Schedule	always
Application/Service	webproxy
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input checked="" type="checkbox"/> REDIRECT <input checked="" type="checkbox"/> ISOLATE

2

### Cache / Network Options

Web Cache	<input checked="" type="checkbox"/>
Reverse Cache	<input type="checkbox"/>
Web Cache For HTTPS Traffic	<input type="checkbox"/>
Webproxy Profile	<input checked="" type="checkbox"/> header
Web Proxy Forwarding Server	<input checked="" type="checkbox"/> fpx111
Scan Outgoing Connections to Botnet Sites	<input checked="" type="checkbox"/> Disable <input type="checkbox"/> Block
SSH Policy Redirect	<input type="checkbox"/> Enable <input checked="" type="checkbox"/> Disable

3

### Security Profiles

AntiVirus	<input type="checkbox"/>
Web Filter	<input checked="" type="checkbox"/> WEB default
Application Control	<input checked="" type="checkbox"/> APP default
IPS	<input type="checkbox"/>
DLP Sensor	<input type="checkbox"/>
Content Analysis	<input type="checkbox"/>
ICAP	<input type="checkbox"/>
Proxy Options	<input checked="" type="checkbox"/> PRX default
SSL/SSH Inspection	<input checked="" type="checkbox"/> SSL certificate-inspection

4

### Logging Options

Log Allowed Traffic	<input checked="" type="checkbox"/> Security Events <input checked="" type="checkbox"/> All Sessions
Log HTTP Transaction	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Disable



# 聯防他牌資安設備

## Internet Content Adaptation Protocol (ICAP)

- ICAP一種應用層協議，用於將**掃描或清洗任務**導向至他牌專用的資安設備，如：防毒牆、DLP
  - ICAP Request Mode: 當收到新請求時，將請求發送到掃描設備以確保它是一個有效的訪問請求
  - ICAP Response Mode: 當新請求有效時，將掃描任何返回的內容

1

Edit ICAP Server

Name fpx-avscan  
IP Version IPv4 IPv6  
IP Address 10.1.219.109  
Port 1344

Malware W32/Agent.NTM!tr	
Mark as clean (false positive)	
Received	Nov 02 2016 16:42:17
Started	Nov 02 2016 16:42:18
Status	Done
Rated By	AV Scanner
Submit Type	Adapter (ICAP)
Client IP	192.168.1.223
Endpoint IP	192.168.1.3
Digital Signature	No
Scan Bypass Configuration	N/A
Virus Total	🔍
More Details	

ICAP default

Search

ICAP default

# 聯防他牌資安設備 (cont'd)

## Decrypted Traffic Mirror

- 解密並將流量複製(mirror)到指定端口
- 可依**政策**配置將解密後的SSL流量複製給**自家或他牌**資安設備監看

1

Create Decrypted Traffic Mirror

Name

Destination MAC

Decrypted Traffic Type  SSL  SSH

Decrypted Traffic Source **Clients** Server Both

Interface

2

Security Profiles

AntiVirus  AV default

Web Filter  WEB default

Application Control

IPS

DLP Sensor

Content Analysis

ICAP  ICAP default

Proxy Options  PRX default

SSL/SSH Inspection  SSL deep-inspection

Decrypted Traffic Mirror

Logging Options

Log Allowed Traffic  Secur





# Log & 報表

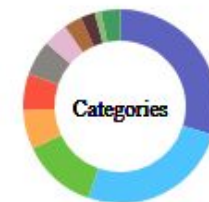
Source	Group	Destination
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 139.175.87.67 (139-175-87-67.dialup.dynam
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 23.11.183.207 (a23-11-183-207.deploy.static
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 13.107.6.171
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 13.107.6.171
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 13.107.42.11
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 52.114.132.23
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 52.139.155.175
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 40.90.23.206
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 139.175.107.80 (139-175-107-80.dialup.dyn
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇺🇸 13.105.74.49
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇮🇪 52.114.77.34
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 23.11.183.207 (a23-11-183-207.deploy.static
ljosh@ftnttw.net (10.1.219.13)	my-grp-ntlm	🇹🇼 23.11.183.207 (a23-11-183-207.deploy.static

## Top 20 Most Active Users

#	User (or IP)	Requests
1	👤 ljosh@ftnttw.net	6,694

## Top Categories by Request

🔍 Search Engines and Portals	29.80%
💻 Information Technology	25.56%
📢 Advertising	12.49%
🌐 Social Networking	6.53%
🌐 Content Servers	6.02%
🏢 Business	5.89%
📰 News and Media	4.09%
🌐 Web-based Applications	3.02%
📊 Web Analytics	2.36%
🏦 Finance and Banking	1.09%
🌐 Others	3.15%



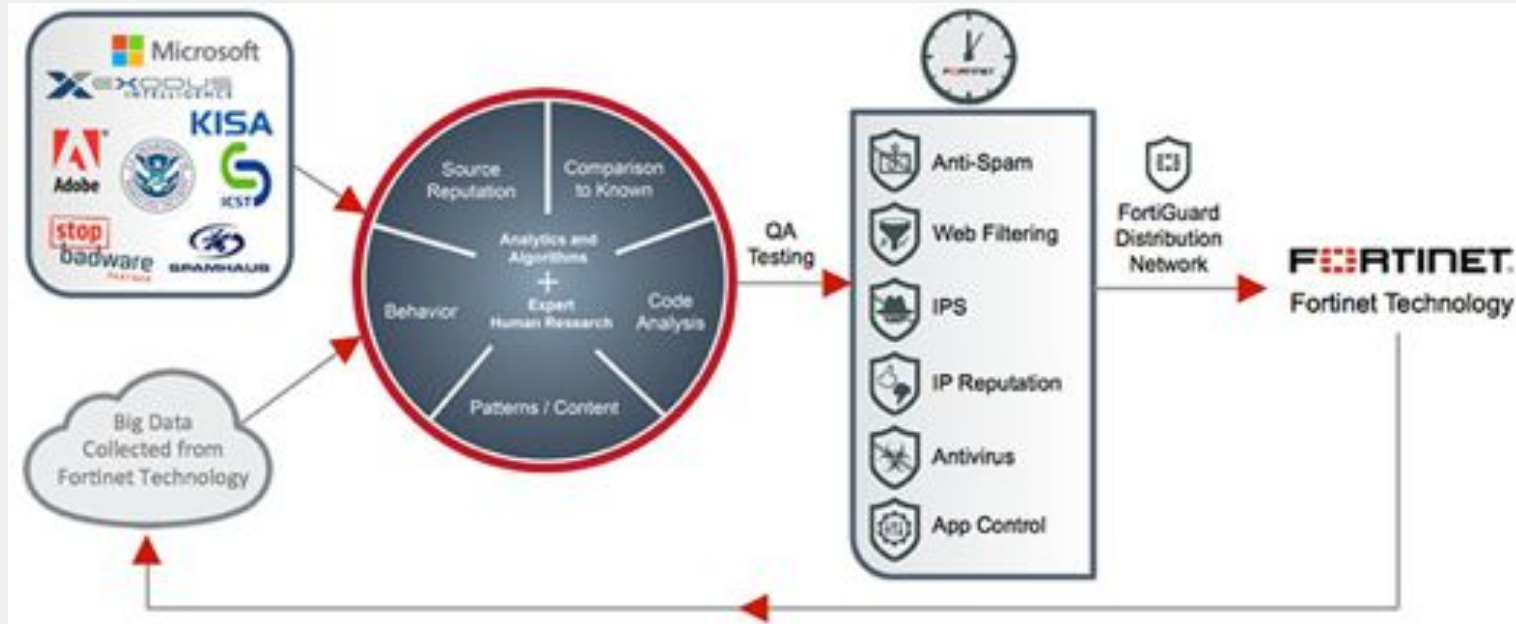
## Top 20 Allowed Web Categories

#	Category	Requests
1	🔍 Search Engines and Portals	1,995
2	💻 Information Technology	1,711
3	📢 Advertising	836
4	🌐 Social Networking	437
5	🌐 Content Servers	403
6	🏢 Business	394
7	📰 News and Media	274
8	🌐 Web-based Applications	202
9	📊 Web Analytics	158
10	🏦 Finance and Banking	73
11	📺 Streaming Media and Download	56
12	📁 File Sharing and Storage	56
13	🛒 Shopping	29
14	📧 Web-based Email	20
15	🗑️ Meaningless Content	13
16	💬 Instant Messaging	13
17	📰 Newsgroups and Message Boards	8
18	📺 Internet Radio and TV	6
19	📖 Reference	5
20	🎨 Arts and Culture	3



# 豐富即時的威脅情資和保護- FortiGuard

## 全球最大的資安雲



- 結合了領先業界的資安廠商和Fortinet的威脅情報，以提供最大程度的保護
- 大數據、機器學習、自動化以及Fortinet專利的分析和研究
- 已出貨超過 220 萬台設備，擁有超過 250,000 名客戶，提供世界一流的威脅情報
- 針對已知和未知威脅的最佳保護

# FortiProxy 產品線

## FPX-400E



- 500 – 4,000 users
- 3 Gbps Proxy Mode
- 1.5 Gbps AV, WF, App
- 1 Gbps AV, WF, App.Ctrl, IPS, SSL Full Inspection

## FPX-2000E



- 2,500 – 15,000 users
- 9 Gbps Proxy Mode
- 4 Gbps AV, WF, App
- 3 Gbps – AV, WF, App.Ctrl, IPS, SSL Full Inspection

## FPX-4000E



- 10,000 – 50,000 users
- 18 Gbps Proxy Mode
- 9 Gbps AV, WF, App
- 6 Gbps – AV, WF, App.Ctrl, IPS, SSL Full Inspection

## FPX-VM



- 100 – 50,000 users
- Performance HW dependent



Web/DNS Filtering

Application Control

Anti-Virus

Intrusion Prevention

Content Analysis

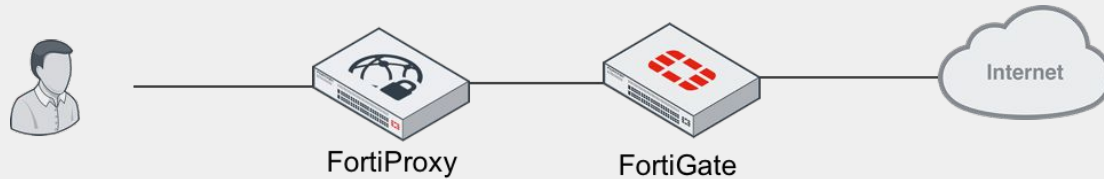
Traffic Shaping

Advanced Caching and WAN Opt. + DNS Protection



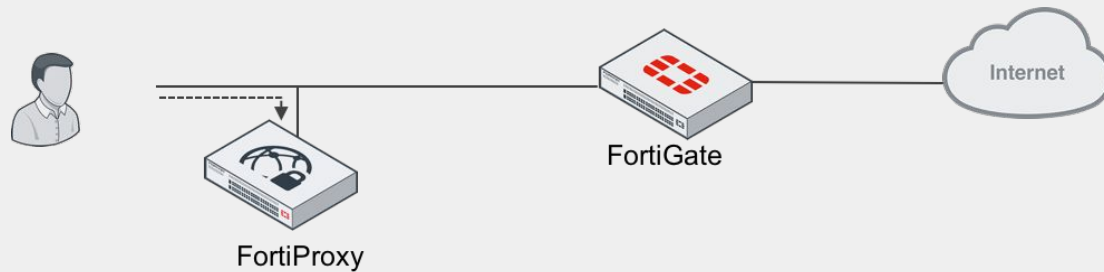
# 彈性的部署模式

## Inline (L2/L3) Deployment



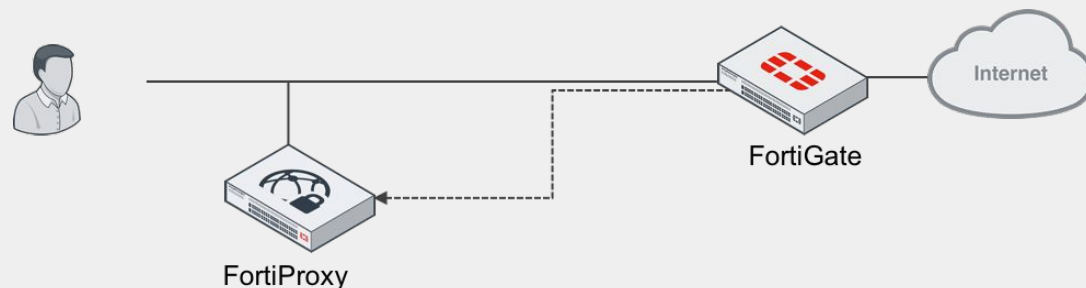
- 設備在網路環境扮演橋接設備(inline), 監控解析通過設備本身的使用者連線內容

## Explicit Deployment



- Explicit模式代理使用者發起的所有web連線
- 客戶端瀏覽器必須指向代理伺服器, 支援PAC files; 同時也可以扮演PAC server

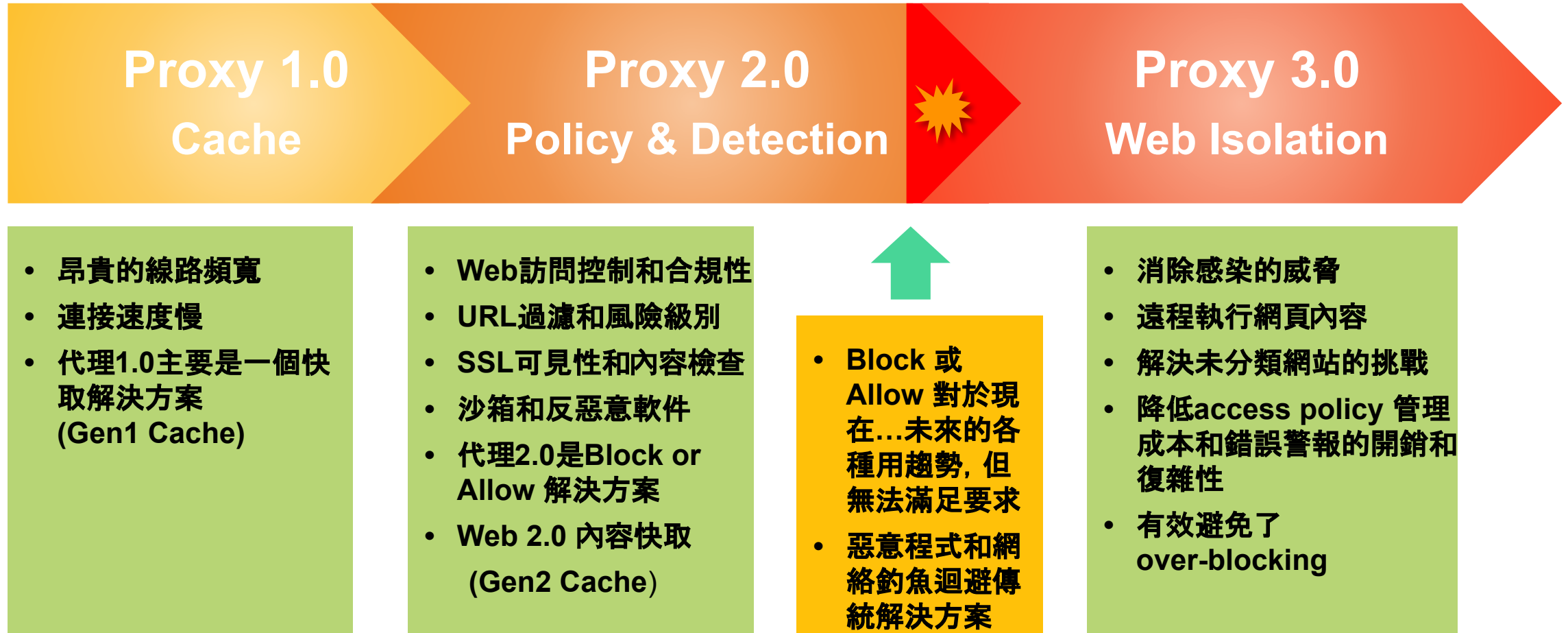
## Transparent/WCCP Deployment



- 設備在網路環境透明代理(transparent)使用者連線請求, 監控解析通過設備本身的使用者連線內容
- PBR(Policy-Based Route)/WCCP 可與現有網路架構集成並提供可擴展性和負載平衡





# 上網控管的演變歷程



# 問題: 過度阻擋”灰色地帶”網站

## Web 控管策略

- VIP用戶 特權瀏覽
- 總是允許 特定URL類別及網站
- 總是阻擋 特定URL類別及網站
- 關鍵問題 – 灰色地帶
  - 過度阻擋 – 造成用戶問題, 體驗不佳
  - 寬鬆政策 – 惡意軟體風險增加

Allowed Categories	Categories where some access may be required			UnCategorized	Threat Cats		
Health, Financial Services, etc	Dynamic DNS Host	File Storage /Sharing	Hacking	Uncategorized	Suspicious	Malicious In/Out...	...
ALLOW	ALLOW or DENY depending on organizational needs  Often requires additional ops to whitelist specific domains/users			DENY for security best practices at the expense of user experience. Often requires additional ops to whitelist specific domains/users	Mostly DENY 	DENY	

Copyright © 2015 Symantec Corporation



# 解決過度阻擋的問題

## Web 控管策略

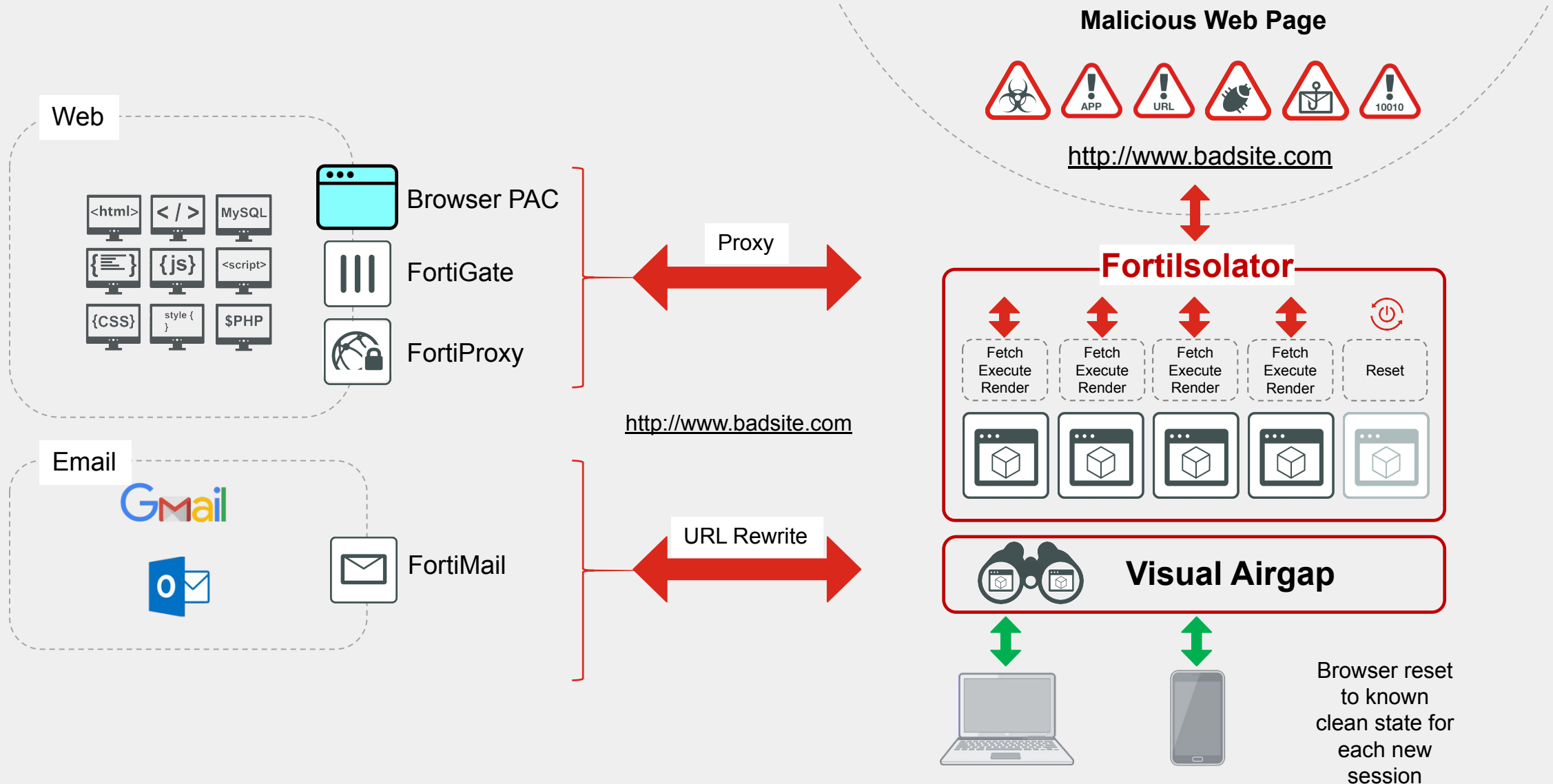
- VIP用戶 特權瀏覽
- 總是允許 特定URL類別及網站
- 總是阻擋 特定URL類別及網站
- 關鍵問題 – 灰色地帶
  - 過度阻擋 – 造成用戶問題, 體驗不佳
  - 寬鬆政策 – 惡意軟體風險增加

Allowed Categories	Categories where some access may be required			UnCategorized	Threat Cats		
Health, Financial Services, etc	Dynamic DNS Host	File Storage /Sharing	Hacking	Uncategorized	Suspicious	Malicious In/Out...	...
ALLOW	ISOLATE				DENY		

Copyright © 2015 Symantec Corporation



# 上網隔離(FIS)怎麼運作

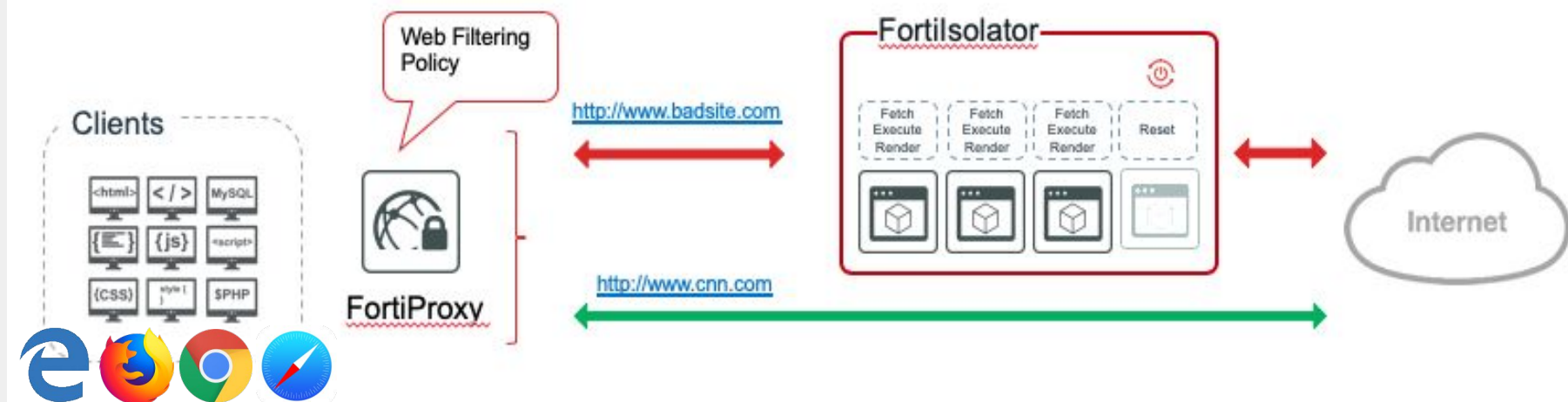




# 隔離瀏覽- 零信任Web存取

- 毋須安裝用戶端程式在本機電腦
  - 相容支援HTML5的瀏覽器
  - 使用原來慣用的瀏覽器軟體, 就能得到上網防護
- 消除上網產生的惡意威脅, 同時保持生產力
  - 沒有第三方程式碼在本地電腦上運行
  - 瀏覽連線在乾淨的容器(Container)中運行
  - 安全的網頁內容呈現給用戶端
  - 支援互動式網頁, 例如:連結、表格、影音

Type	Explicit
Name	Isolate Unrated Uncategorized
Explicit Web Proxy	web-proxy
Outgoing Interface	port1
Source	all
Destination	Newly Observed-Registered Dom Unrated Category
Schedule	always
Application/Service	webproxy
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input checked="" type="checkbox"/> REDIRECT <input checked="" type="checkbox"/> ISOLATE
Isolator Server	FIS



# 簡易的設定，讓你幾乎忘了曾設定過

## Integration – FortiProxy

The screenshot displays the FortiProxy KVM interface. On the left, a navigation menu shows 'Isolator Server' selected, marked with a red circle '1'. The main area shows the 'Edit Isolator Server' configuration for 'fis1', with fields for Name, Comments, Address Type (IP/FQDN), IP (172.22.245.189), and Port (8888). A central navigation menu has 'Policy & Objects' selected, with 'Policy' highlighted, marked with a red circle '2'. On the right, the 'Edit Policy' configuration is shown, including Type (Explicit), Name (Auth by SSO), Explicit Web Proxy (web-proxy), Outgoing Interface (port1), Source (all, ljosh, myg-vip), Destination (all), Schedule (always), Application/Service (webproxy), Action (ACCEPT, DENY, REDIRECT, ISOLATE), Isolator Server (fis1), and Web Cache (fis1).

# 隔離前後差異

## Before Isolation

```
<!DOCTYPE html>  
<html id="Stencil1" lang="zh-Hant-TW" class="StencilRoot my3columns ua-uk ua-win ua-6.1 ua-uk537 1-out Pos-r https://fp.fp-defau  
bktcc_bucket_shopping_6and12_2020_q1">  
<head>  
<meta http-equiv="X-UA-Compatible" content="IE=edge">  
<title>Yahoo奇摩</title><meta http-equiv="x-dns-prefetch-control" content="on"><link rel="dns-prefetch" href="//s.yimg.com/  
prefetch" href="//css.bsap.bc.yahoo.com"><link rel="preconnect" href="//css.bsap.bc.yahoo.com"><link rel="dns-prefetch" href="//  
<link rel="dns-prefetch" href="//comet.yahoo.com"><link rel="preconnect" href="//comet.yahoo.com"><link rel="dns-prefetch" href=  
href="//video-api.yql.yahoo.com"> <meta http-equiv="Content-Type" content="text/html; charset=utf-8">  
<meta name="description" content="新聞、電子信箱和搜尋功能只是起點。每天發覺更多精彩內容。打造專屬自我的 Yahoo奇摩體驗。">  
<meta name="keywords" content="yahoo, yahoo奇摩, yahoo奇摩首頁, yahoo首頁, yahoo搜尋, yahoo 信箱, yahoo 即時通訊, 新聞, 股市, </br><meta property="og:title" content="Yahoo奇摩" />  
<meta property="og:type" content="website" />  
<meta property="og:url" content="http://tw.yahoo.com/" />  
<meta property="og:description" content="新聞、電子信箱和搜尋功能只是起點。每天發覺更多精彩內容。打造專屬自我的 Yahoo奇摩體驗。"/>  
<meta property="og:image" content="https://s.yimg.com/cv/apiv2/social/images/yahoo_default_logo.png"/>  
<meta property="og:site_name" content="Yahoo奇摩" />  
<meta property="fb:app_id" content="399384933466174" />  
<meta name="format-detection" content="telephone=no" />  
<link rel="icon" sizes="any" mask href="https://s.yimg.com/cv/apiv2/default/icons/favicon_y19_32x32_custom.svg">  
<meta name="theme-color" content="#400090">  
<link rel="shortcut icon" href="https://s.yimg.com/rz/l/favicon.ico" />  
<link rel="canonical" href="https://tw.yahoo.com/" /> <meta property="fb:pages" content="230899156962824" /> <meta  
href="https://s.yimg.com/aan/fo/css/tv2-wafer-category/atomic_ltr_0840a289.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-featurebar/atomic_ltr_292e4f0.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-profile/atomic_ltr_05ab7e3d.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-locker/atomic_ltr_0088a50e.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-locker/custom_3c3e7988.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-header/atomic_ltr_6ad2a8e.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-horoscope/atomic_ltr_04f4086.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-weather/atomic_ltr_ce39e12.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-scores/atomic_ltr_2f31168.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-storywarn/atomic_ltr_bd2dae3.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-countdown/atomic_ltr_3eac07b8.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-finance/atomic_ltr_d16c450e.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-weather/common_desktop.cb2aaf3.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-loyalty/atomic_ltr_0f7642e.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-loyalty/custom_281b20a.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-stream/custom_desktop_33a0dac3.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-footer/atomic_ltr_047acee1.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-stream/atomic_desktop_ltr_729cbdb8.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/aan/fo/css/tv2-wafer-ntk/atomic_desktop_ltr_83807bac.css" rel="stylesheet" type="text/css">  
<link href="https://s.yimg.com/os/fo/atomic-css.a41904e4.css" rel="stylesheet" type="text/css">
```

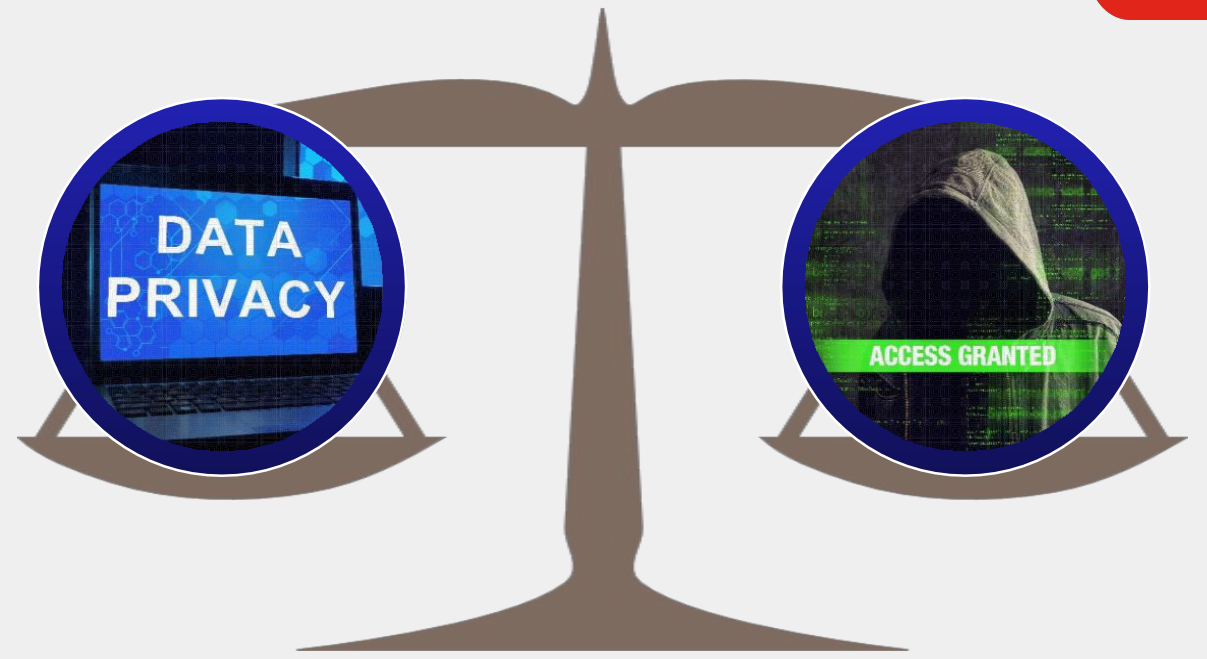
## After Isolation

```
<html><head>  
<meta charset="utf-8">  
<meta name="viewport" content="width=device-width">  
<link rel="stylesheet" href="https://172.22.245.189/ftnt.css">  
<script src="https://172.22.245.189/jquery.js"></script>  
<script src="https://172.22.245.189/ftnt.js"></script>  
<title>Yahoo奇摩</title></head>  
<body>  
<script>  
$(document).ready(  
function() {  
updateAddress("https://tw.yahoo.com/", false);  
initNetwork("172.22.245.189", 45099, 443, "722187e48fb85fc264d5495d3fa8f4f68d998df0b1  
disableBackMethod());  
});  
</script>  
<div id="statusDiv" hidden="hidden"></div>  
<canvas id="mainCanvas" width="1016" height="612" style="cursor: pointer;"></canvas>  
<canvas id="popupCanvas"></canvas>  
<textarea id="ftnt_input" style="height: 0px; width: 0px; outline: none; top: 428.4p
```



# 加密流量管理工具怎麼選

## 3加1口訣



## 好的加密流量管理解決方案：

- **加值**現有的安全基礎設施防護能力
- **加強**可視性，打擊隱藏在加密流量的安全威脅
- 確保機密數據，如針對醫療保健和銀行網站間溝通的訊息，仍可保持**加密**狀態
- 專屬**一台**為應付 SSL 流量所開發的高效能高安全性解決方案

**FORTINET**®