

無線網路環境 的安全威脅與防禦之道

諮安科技股份有限公司

蔡均璋

無線與有線網路的安全差異



◆線!線!永不整齊的線!

- 佈線成本
- 難以整理的線

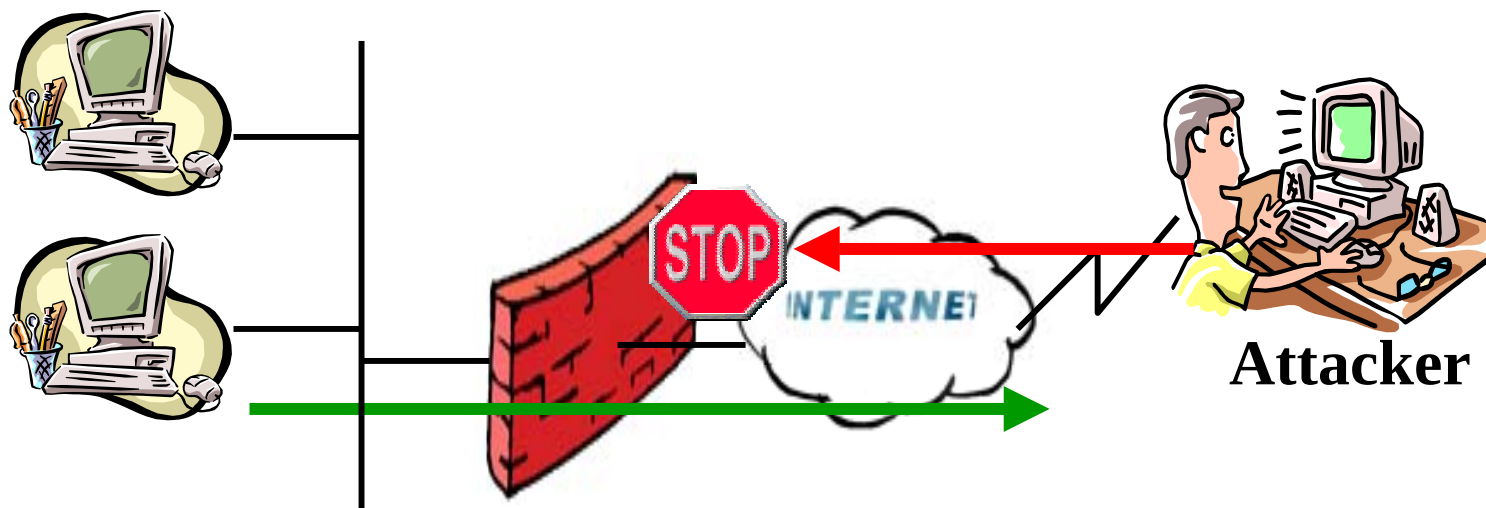


◆攻擊者必須和被攻擊者接觸才能攻擊:

- 必須接上線路可能進行攻擊
- 必須搭上線路可能竊聽
- 可透過實體保護避免被存取



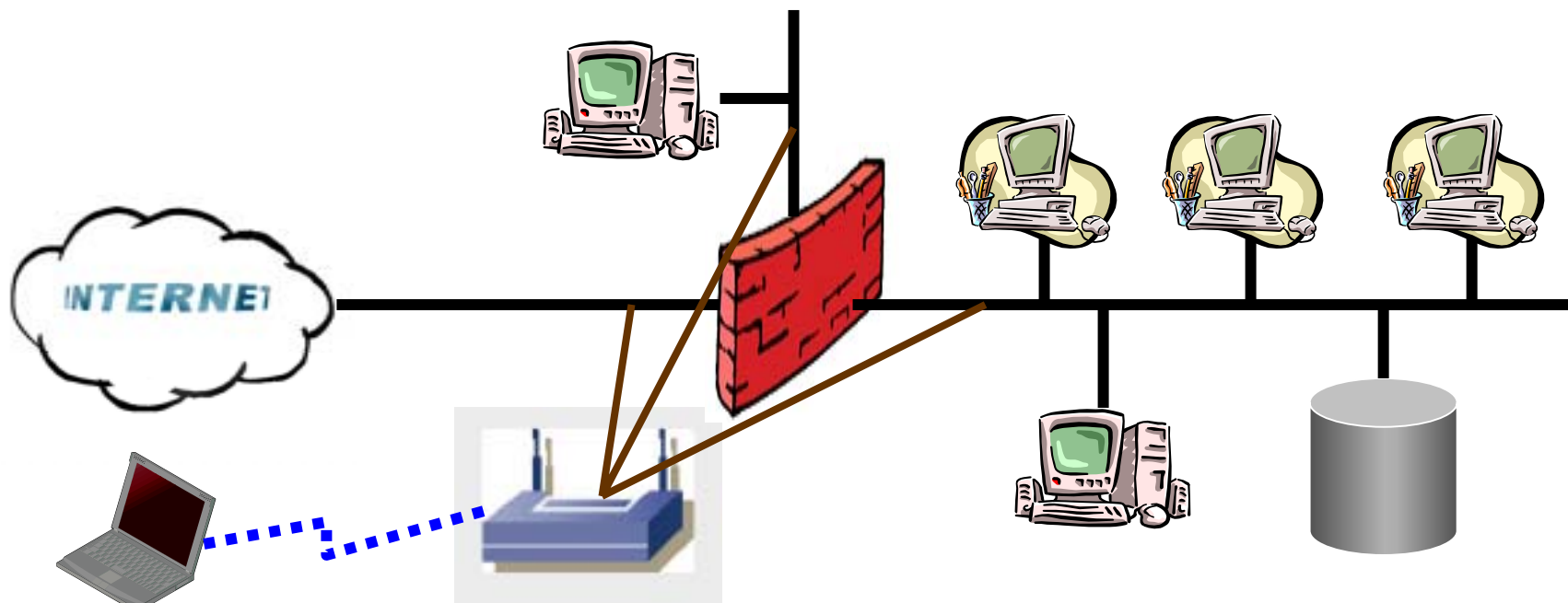
◆使用網路火牆阻隔(Internet)威脅來源:



- 開放越多服務帶來越多被入侵的機會
- 使用其他安全機制加強防護
- ◆ 實體線路限制線路直接被盜用的風險

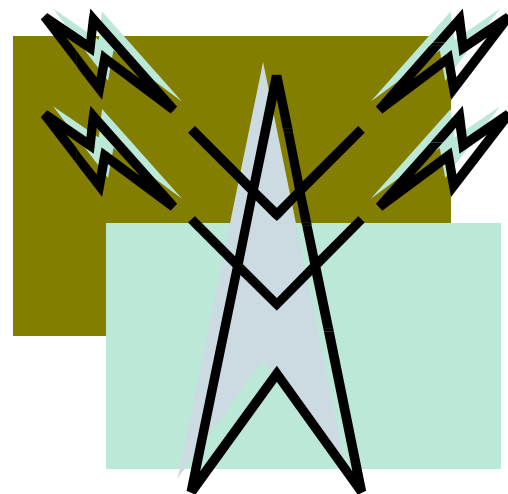
◆透過 AP 建立無線網卡和網路間之存取

- AP: Access Point, 類似基地台之角色
- AP 建置之位置關係其存取位置



◆無線的美麗新世界

- 解決佈線困難及成本
- 解決線路整理問題
- 增加移動能力

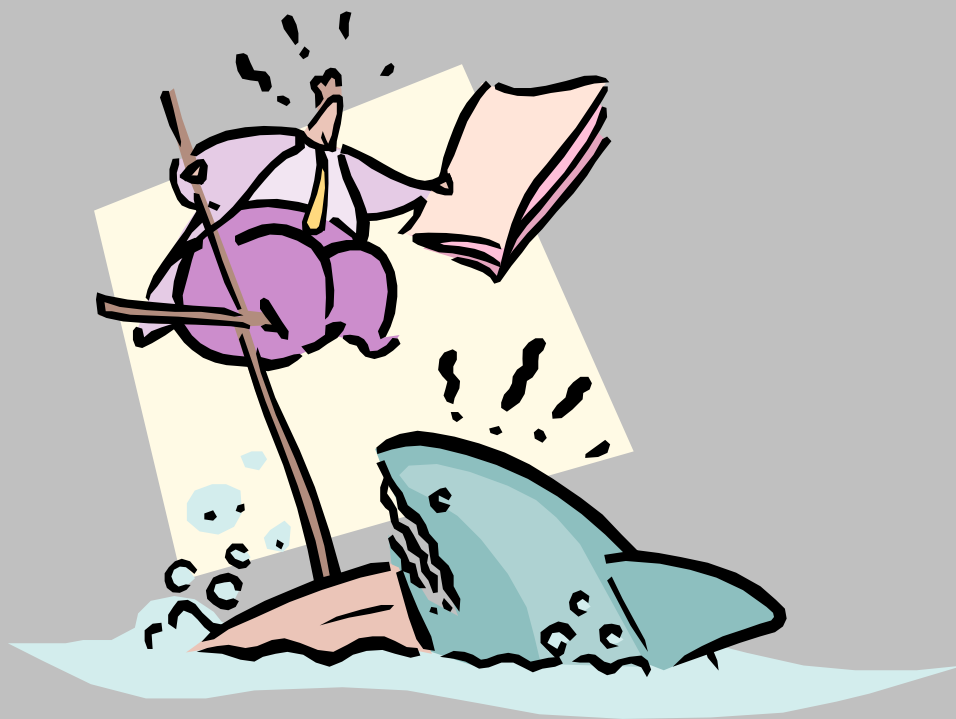


◆無線基地廣播電台

- 傳輸訊號在外散佈
- 無線 AP 與網卡通訊可被偵測
- 無須實體接觸
- 網際網路以外的另一個出入口



無線網路的安全威脅



- ◆ Notebook 可存取 12 哩外的 AP
- ◆ 攻擊者可監聽、使用/控制 12 哩外的 AP
 - 不被偵測



◆對無線網路的技術尚未真正了解

- 相較於 LAN 的技術，不知道實際

◆自我催眠的信心

- 如果這個問題這麼複雜，大概也不會有人可以破解
- 攻擊必須倚賴監聽工具，這些工具都很貴，而且很難找
- 想要攻擊必須倚賴昂貴、特殊的工具

◆出廠時的預設設定

- 多半以“開放”或“預設值”來簡化使用及設定
- 給予駭客猜測的機會

◆MAC Address 控制:

- 無線 AP 可以控制哪些 MAC Address 可以存取

◆安全問題:

- 即使是在 WEP (加密)狀態下，資料傳輸時 MAC 是以明碼傳送
- 使用者可以自己修改 MAC Address

◆使用封閉式網路(Close Network):

- 使用者必須知道此一無線網路的 Service Set ID(SSID) 才能夠加入此一無線網路

◆安全問題:

- SSID ≠ 密碼, 同一 AP 使用同一 SSID
- 許多 AP 有預設之 SSID
- 有些設備會廣播 SSID
- 使用者可能將 SSID 告訴親朋好友
- 無法用來辨識使用者身份

◆ WEP (Wired Equivalent Privacy)

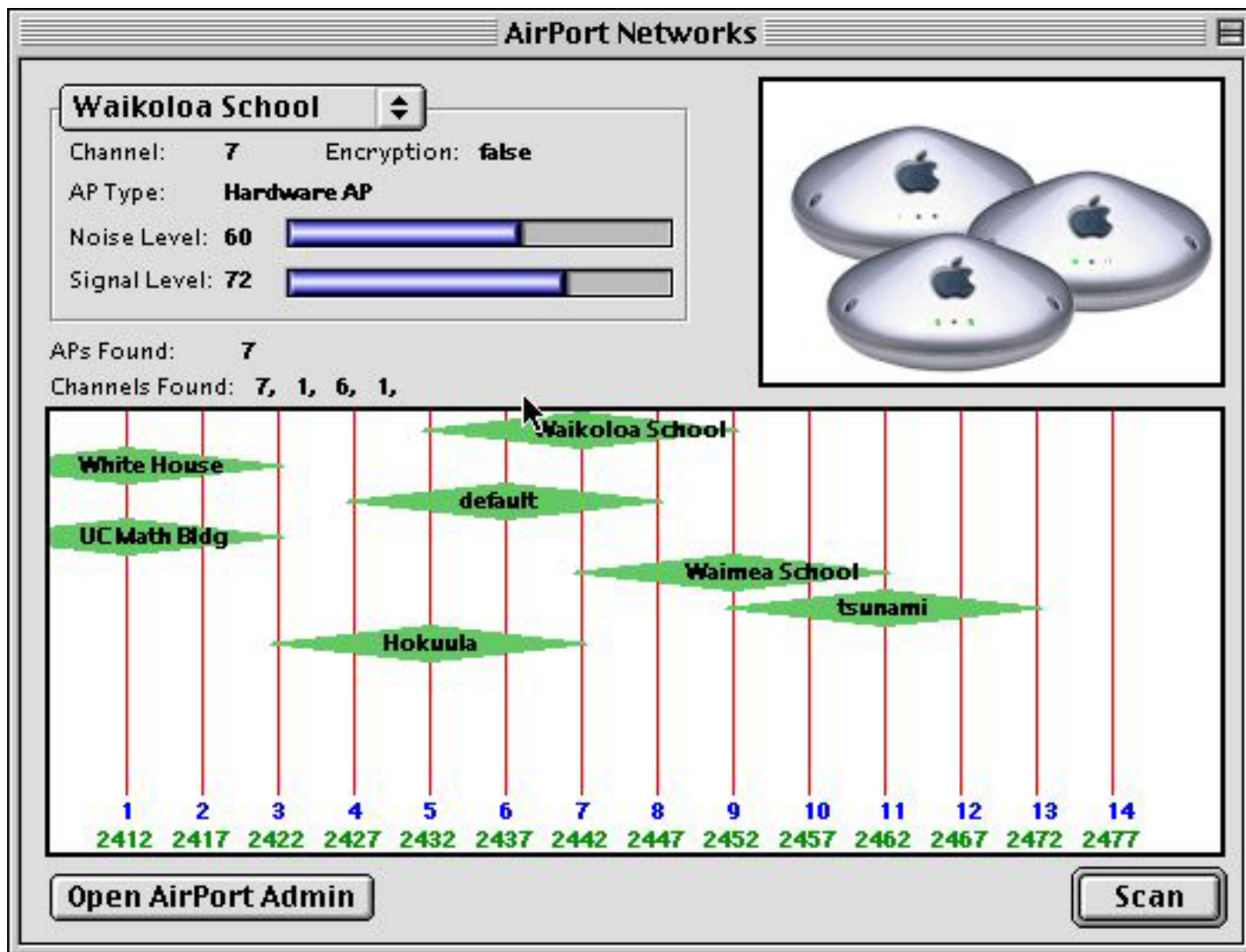
- 802.11 兩端加密的機制
- 使用 RC4 演算法
- 使用 64 或 128 (非標準) bit 的key



◆ 存在一些問題:

- 同一 AP 使用者使用相同的加密 Key
- 加密用的 Code 會被重複使用，傳輸量越大越容易被破解
- 蒐集 1到 4M 的 Frame 後可透過統計方式計算出 Key(一般可在六小時內被破解)

- ◆ **AP 掃描工具: AP scanner, Net Stumbler**
- ◆ **War driving**
- ◆ **封包監聽程式: Airtight, Airopoisk**
- ◆ **阻礙服務攻擊(DoS)**
- ◆ **偽冒攻擊: 假造 MAC Address**
- ◆ **假造的 AP: (Man in Middle attack)**



典型的 War Driving Scan

AP name	HW address	channel	snr	Managed?	Vendor	WEP
Schenk	00:30:65:1D:F3:D9	6	17	Managed	Apple	No
Castle Gymnasium	00:02:2D:31:C2:D1	1	36	Managed	Agere-Lucent	No
UC Library Airport	00:02:2D:09:4B:ED	6	36	Managed	Agere-Lucent	No
tsunami	00:04:5A:0C:5F:FC	6	19	Managed	Linksys	No
onaga	00:04:5A:DB:BC:6D	1	29	Managed	Linksys	No
opakapaka	00:06:25:54:9D:67	6	80	Managed	3Com	No
linksys	00:04:5A:EE:A3:5F	6	18	Managed	Linksys	No
kapu4u	00:40:96:47:57:7E	3	54	Managed	Cisco-Aironet	No
0e7a75	00:02:2D:0E:7A:75	1	60	Managed	Agere-Lucent	No
linksys	00:04:5A:FA:75:E3	6	20	Managed	Linksys	No
3a46c4	00:02:2D:3A:46:C4	1	19	Managed	Agere-Lucent	Yes
128063	BE:01:98:01:0E:03	6	85	Ad-hoc	unknown	No
hokuula_internal	00:02:2D:22:EB:36	1	65	Managed	Agere-Lucent	No
Administration Building	00:05:5D:A6:FA:06	5	49	Managed	unknown	No
Technology Center	00:60:1D:F7:37:F5	11	47	Managed	Agere-Lucent	No
physics	00:05:5D:D9:DD:14	11	49	Managed	unknown	No
101	00:01:24:F1:F9:7E	6	30	Managed	Acer	No
VC Mobile 1	00:02:2D:2D:1C:43	1	19	Managed	Agere-Lucent	No
Airport	00:30:65:04:1B:C4	1	35	Managed	Apple	Yes
NaKuaHiwi2	00:02:2D:0D:69:46	1	39	Managed	Agere-Lucent	No
hospice	00:50:18:07:D2:CE	6	58	Managed	Adv	No
linksys	00:04:5A:CF:7F:81	6	20	Managed	Linksys	No
default	00:05:5D:EC:CE:C8	6	26	Managed	unknown	No

GoodrichAirport	00:02:2D:27:CE:9C	1	26	Managed	Agere-Lucent	Yes
	00:05:5D:DA:22:A8	6	35	Managed	unknown	No
	00:50:18:07:91:7C	6	56	Managed	Adv	No
	00:04:5A:CE:6C:8D	6	19	Managed	Linksys	No
	00:50:18:03:CF:A0	6	42	Managed	Adv	No
	00:40:05:B5:D0:DB	6	29	Managed	D-Link	Yes
	00:05:5D:D6:C0:59	6	23	Managed	unknown	No
	00:40:05:B5:B5:39	6	30	Managed	D-Link	No
rockza	00:40:96:26:35:B8	1	42	Managed	Cisco-Aironet	No
HWVWIRELESS	00:40:96:57:4C:DD	6	25	Managed	Cisco-Aironet	No
naia	00:04:5A:0E:23:E1	11	43	Managed	Linksys	No
HWVWIRELESS	00:40:96:57:F4:AC	6	41	Managed	Cisco-Aironet	No
Taylor Commons	00:60:1D:1E:4C:59	1	92	Managed	Agere-Lucent	No
rockza	00:40:96:26:2B:B1	1	58	Managed	Cisco-Aironet	No
kapu4u	00:40:96:29:98:86	3	54	Managed	Cisco-Aironet	No
kobe	00:02:2D:3C:FF:F9	1	27	Managed	Agere-Lucent	No
katie	00:02:2D:3D:00:1D	6	28	Managed	Agere-Lucent	No
101	00:04:5A:DE:07:81	6	34	Managed	Linksys	No
Castle Auditorium	00:60:1D:F1:0F:68	1	93	Managed	Agere-Lucent	No
akule	00:06:25:54:97:30	1	63	Managed	3Com	No
hokuula2	00:02:2D:09:2A:52	6	45	Managed	Agere-Lucent	No
HWVWIRELESS	00:40:96:57:60:BC	6	37	Managed	Cisco-Aironet	No
HWVWIRELESS	00:40:96:57:EA:8E	6	46	Managed	Cisco-Aironet	No

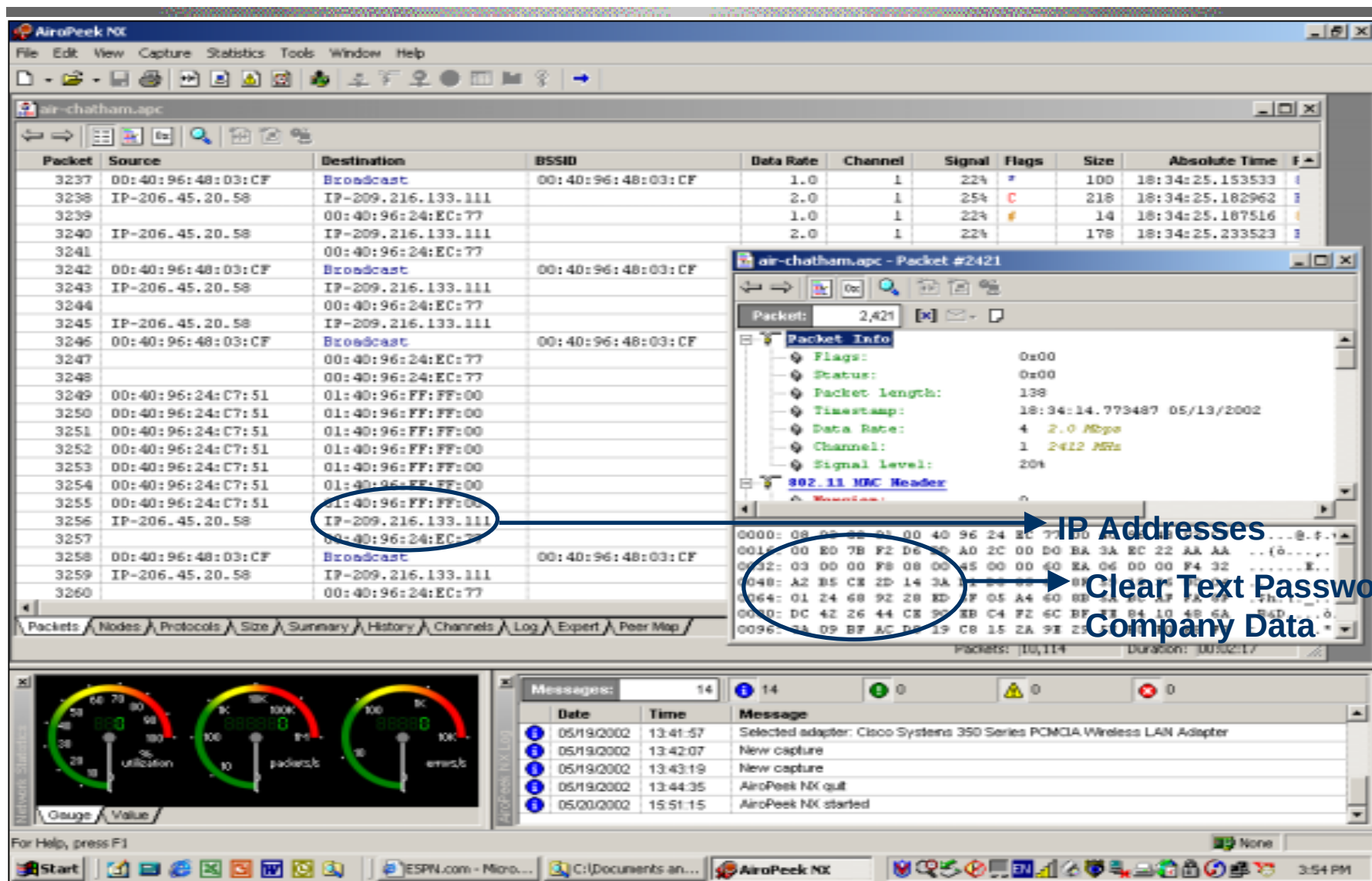
Network Stumbler - [bpg2.ns1]

File Edit View Options Window Help

Channels
SSIDs
Filters

MAC	SSID	Name	Chan	Vendor	Type	WEP	SNR	Signal+	Noise-	SNR+	Latitude
00045A0E3EA0	linksys		6	Linksys	AP			-91	-100	9	
00045AE838CB	linksys		6	Linksys	AP			-84	-102	15	
00022D2C82DA	2c82da		1	Agere (...)	AP	Yes		-75	-99	21	
000124F05623	default		6		AP			-95	-98	3	
00045A0E3A4A	linksys		6	Linksys	AP			-71	-104	32	
00045ADA770F	ANY		6	Linksys	AP	Yes		-90	-101	10	
00045AE85F93	linksys		6	Linksys	AP			-88	-102	13	
00045A0F2264	linksys		6	Linksys	AP			-87	-98	11	
00062550331E	linksys		6		AP			-89	-99	9	
00045AE81743	peggyp		3	Linksys	AP			-81	-100	17	
00030A000D54	aa		11		AP	Yes		-82	-99	17	
0030F1102D35	WLAN		11		AP	Yes		-85	-99	14	
00022D3F21CE	3f21ce		1	Agere (...)	AP	Yes		-85	-100	15	
00045AD00E47	linksys		6	Linksys	AP	Yes		-91	-98	7	
0030651C568A	Office		1	Apple	AP	Yes		-93	-96	3	
0040964569DC	NEUSTAR		6	Cisco (A...	AP	Yes		-90	-100	10	
0040964576BD	NEUSTAR		6	Cisco (A...	AP	Yes		-90	-99	9	
003065030058	Better then Windows		1	Apple	AP	Yes		-89	-95	6	
00045ACE3A63	pchan		6	Linksys	AP			-88	-101	11	
00601DF0438E	sproj		3	Agere (...)	AP	Yes		-88	-99	11	
000625504834	Falcos		10		AP			-80	-101	18	
00409632DE23	luckgoose		4	Cisco (A...	AP			-93	-100	7	
00304B0B617A	Roming		6	Delta N...	AP	Yes		-86	-97	11	
004096485D54	leesburg2		1	Cisco (A...	AP	Yes		-63	-100	36	
00409659F7BE	1SU		6	Cisco (A...	AP			-58	-102	40	
00409659D4EF	1SU		6	Cisco (A...	AP			-57	-100	42	
004096486D0F	leesburg2		1	Cisco (A...	AP	Yes		-85	-100	13	

Ready Not scanning GPS: Disabled



❖ 私自架設的網路

- 使用者常為了方便或規避網路控制而私自架設網路
- 自行架設 AP

❖ 通常沒有經過嚴格的存取控制

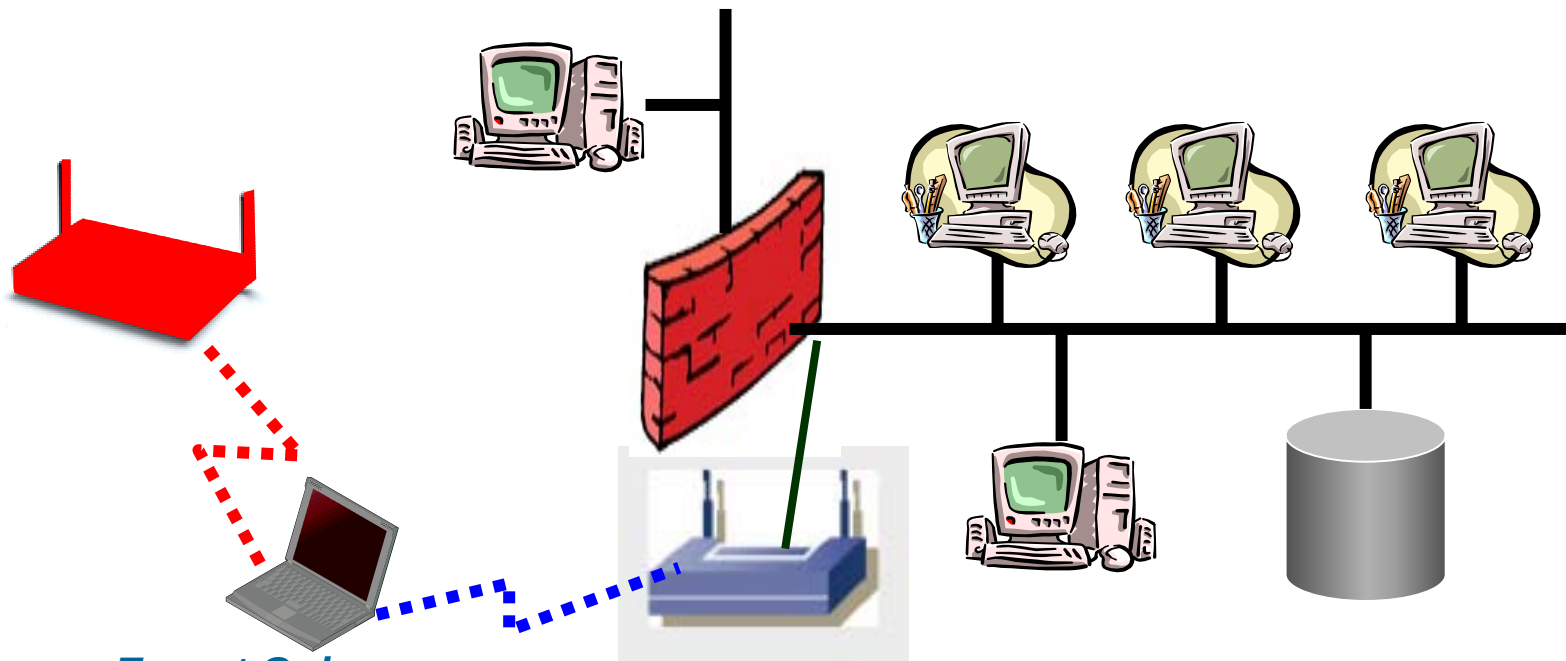
- 可能遭受 War Driving 和監聽問題

❖ 管理者可能完全沒有意識到此一現象

- 無法管理，難以稽核
- 成為不知道的後門

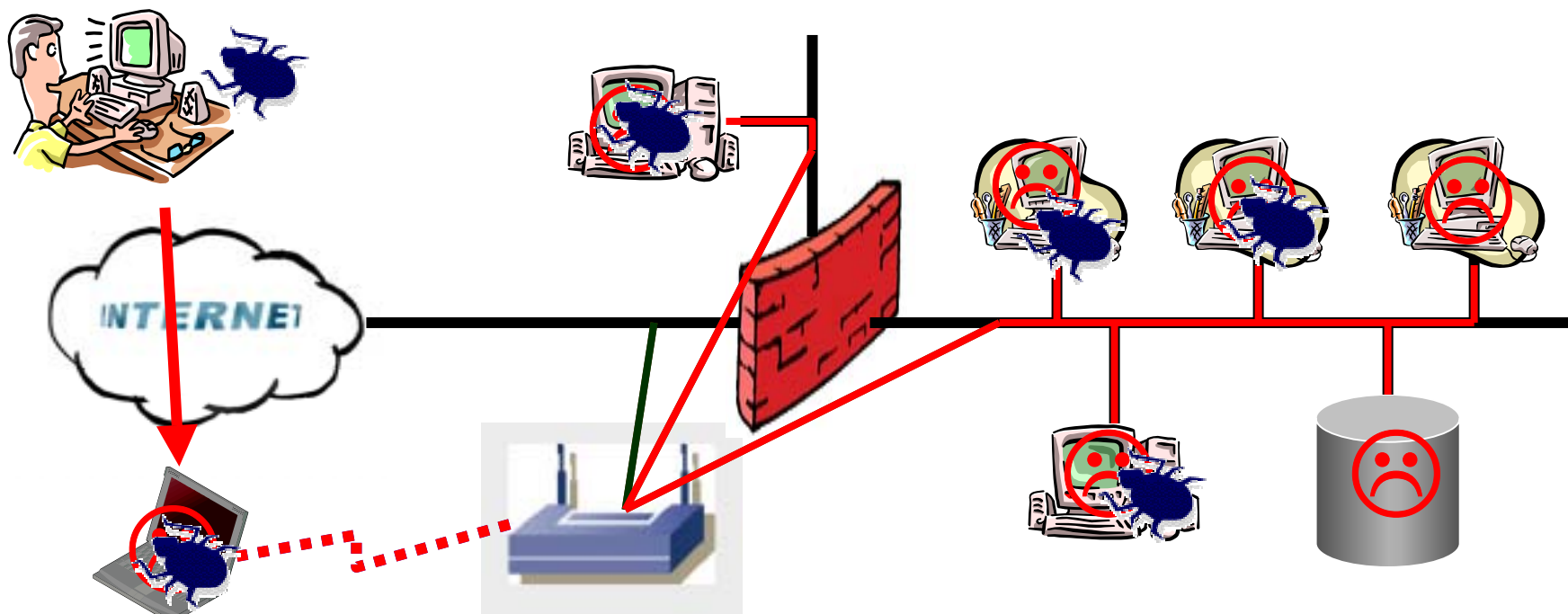
◆攻擊者架設假造的 AP

- 讓使用者誤認為是要存取的 AP
- 盜取使用者資訊或密碼



◆ AP 的建置位置嚴重影響最終之安全性

- 攻擊者可以利用用戶端及 AP 進入內部網路
- 用戶端感染之蠕蟲可藉由 AP 進入內部網路



無線網路的安全防護之道



- ◆針對自有環境進行調查：
 - 公告無線網路安全政策
 - 找出未經授權的 AP
- ◆啟動無線 AP 之基本安全功能
- ◆導入其他安全保護機制
 - 使用 Radius, VPN 或其他之認證機制
- ◆持續檢查無線 AP 環境
 - 定期檢查無線 AP 之安全設定
 - 考慮使用和攻擊者類似的工具自我檢查

安全



- 無線網路不受牆的限制
- 預設設定毫無安全性可言
- 協定標準的安全性低於安全的標準要求
- 無線網路可能成為另一個攻擊者的大門

移動性



- AP 間的移交 (Handover)
- 漫遊跨越 IP 網路時的解決之道
- 安全不因使用者的移動而變化
- 對語音和資料的支援

管理能力



- 誰在使用我們的網路?
- QoS(Quality of service)?
- 可否集中管理?
- 是否具有足夠的稽核和警示能力?
- 是否僅能針對特定 AP 管理?

◆存取控制及安全管理

- 使用者認證(Authentication)
- 使用者授權(Authorization)
- 無線通訊的隱私性問題(Privacy)
- 實體安全

◆資料傳輸增加密度

- 需要進行頻寬管理, 避免頻寬被耗盡

◆相容性:

- 設備相容性:筆記型電腦、PDA、Scanner、手機、其他網路設備
- 應用相容性: 利用無線網路進行語音通訊將會越來越頻繁

◆管理容易度:

- 登入方式: Web 登入是目前最簡易的方式
- 是否支援透通式的登入方式
- 用戶端的軟體維護需求

◆對“無線頻寬”的有效管理

- 讓加密的負擔只在必要的時候出現
- 高用量區域的頻寬分享能力

◆滿足不同無線網路使用者不同的存取需求

- 部分服務(如 FTP) 對某些無線網路使用者可能並非必要
- 某些存取目標可能必須要限制(例如: 內部資料庫)
- 提供 Guest / Visitor 存取的能力

- ◆ **WEP(Wired Equivalent Privacy)**
 - 嘗試讓無線網路達到和有線網路一樣的保密能力
 - 容易破解
- ◆ **802.1x (PEAP, Cisco-LEAP, TLS, TTLS, MD5)**
 - 提供認證能力和 Key Exchange 架構
- ◆ **Wi-Fi Protected Access (WPA)**
 - 讓 802.1x 的加密機制具有加密 key 更新的能力
 - Wi-Fi Alliance 針對 Pre-802.11i 狀態的暫時協議(並非 IEEE 802.11 的標準)
 - 僅有簡單的 開/關 存取能力, 提供基本的保護
- ◆ **802.11i**
 - 將加解密演算法使用 AES 取代
 - 尚未成為正式標準(2004 年可能成為標準), 尚無產品可以使用
- ◆ **VPN (IPSec)**
 - 較為安全, 但是缺乏移動能力和運作彈性



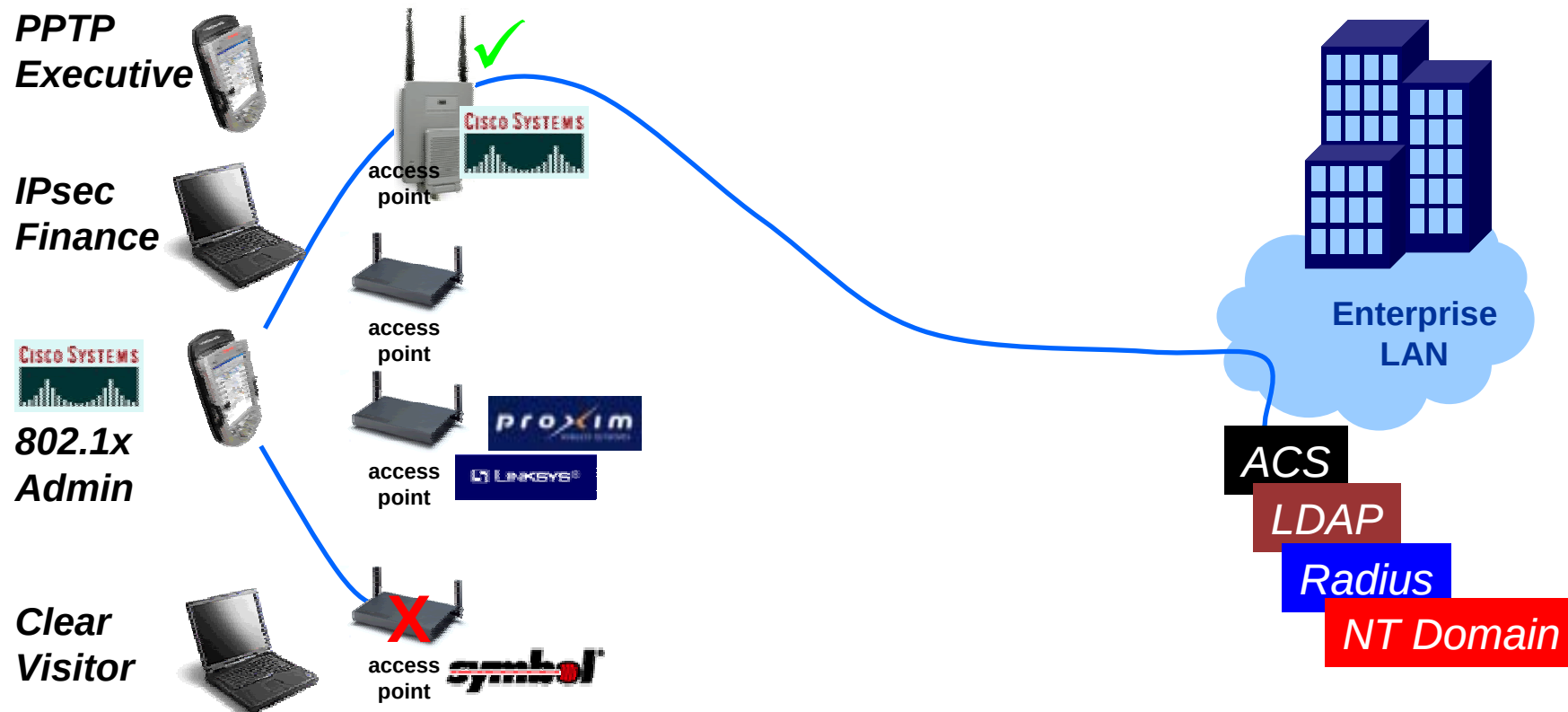
BlueSecure Intrusion Protection System &

Bluesocket Wireless Gateway

RF監督、安全政策捍衛

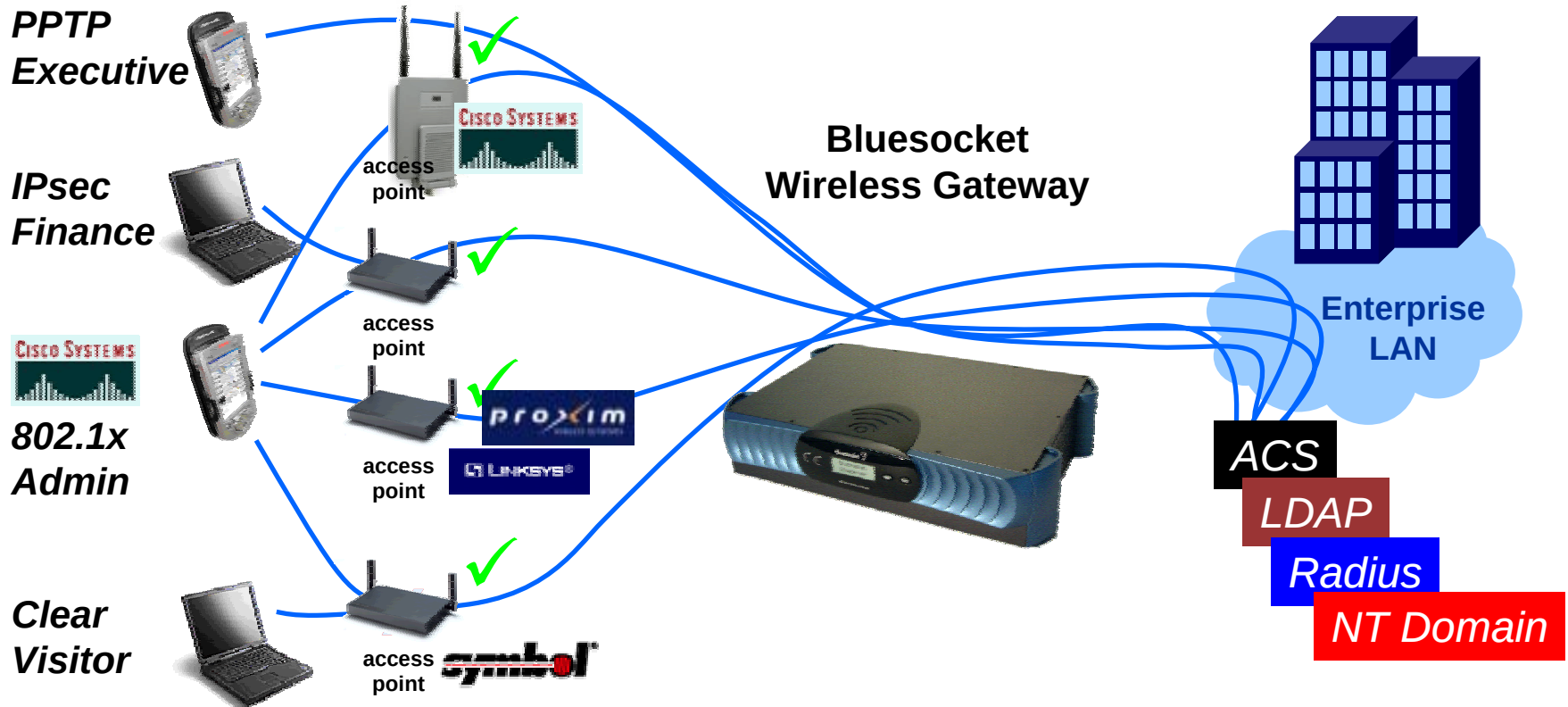
以及WLAN 資料和語音流量管理完整解決方案

Authentication, Encryption, Policy Management, Secure Mobility

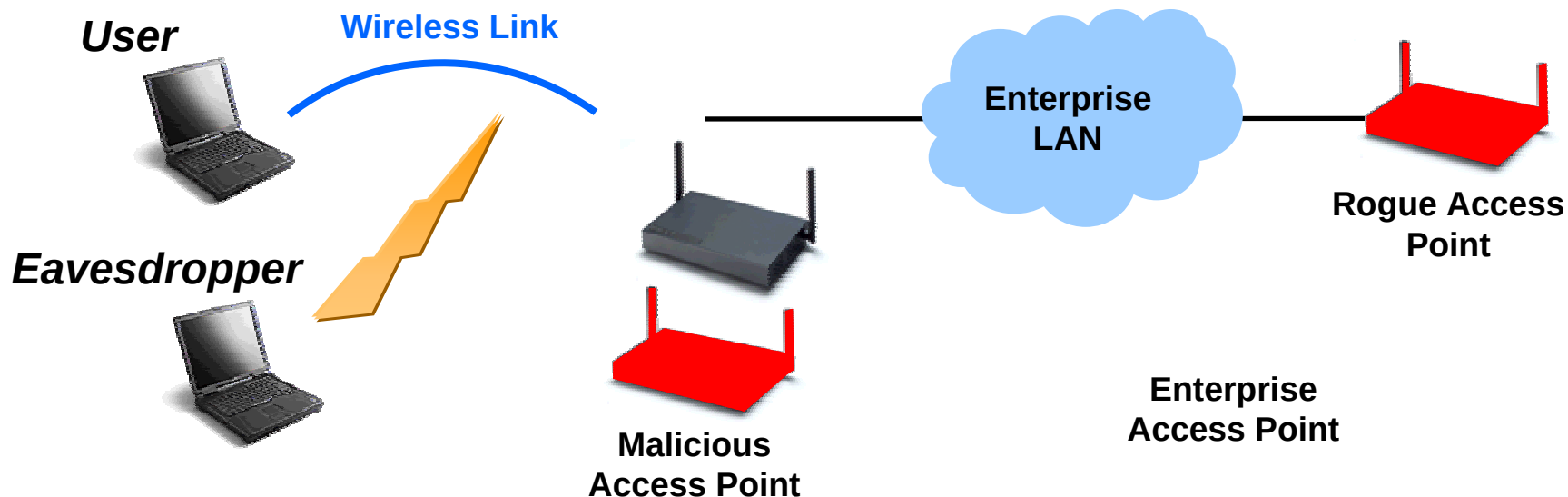


Bluesocket Wireless Gateway

Open, Standards-based Interoperability
for Multi-vendor Networks



- ◆ 未經授權的存取(Unauthorized Access)
- ◆ 竊聽通訊內容 (Eavesdrop)
- ◆ 偽造的 AP (Malicious AP)
- ◆ 惡意的 AP 後門(Rogue AP)

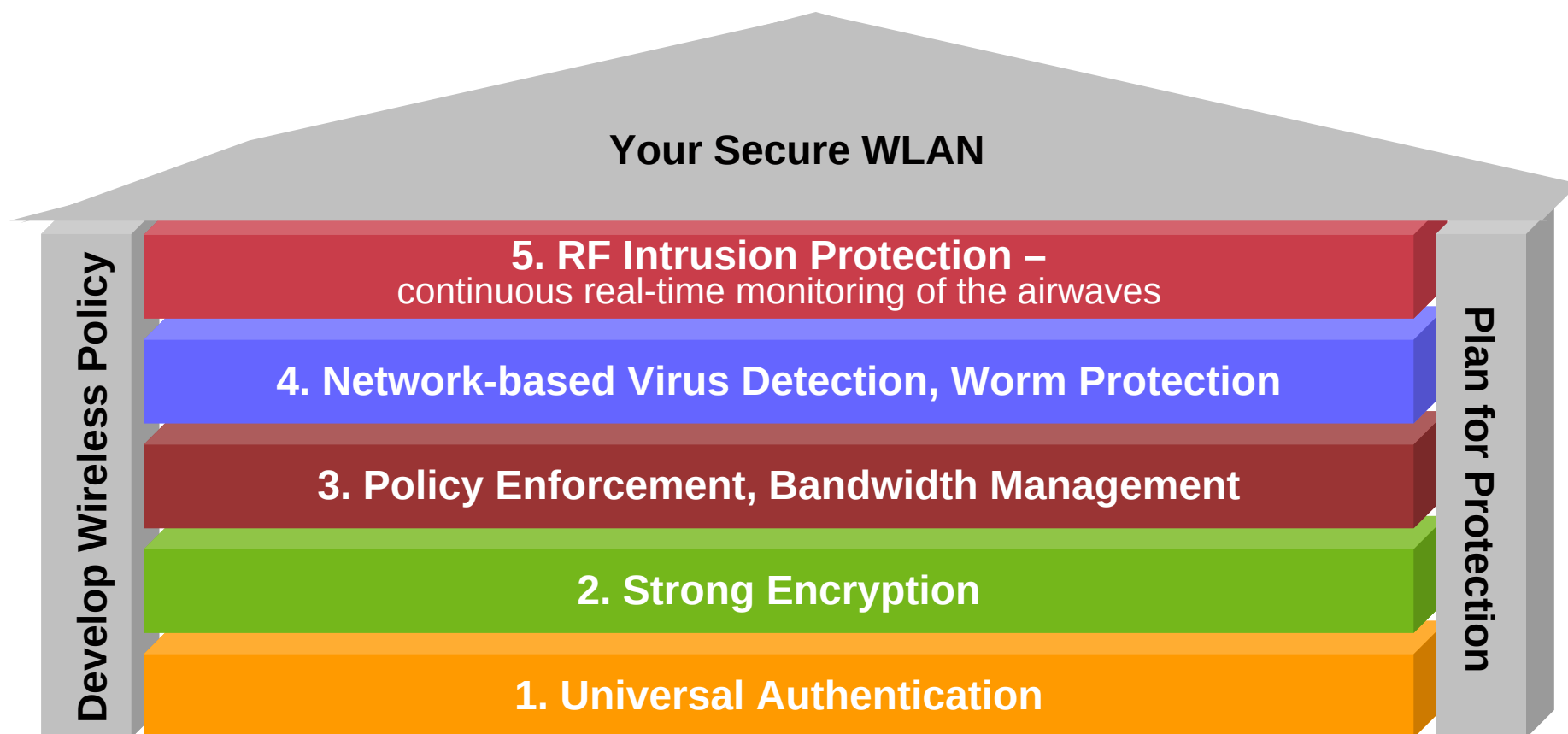


不過真的已經解決了無線網路的安全問題了嗎？

Feature	802.11i, WPA, 802.1x	Missing Parts
Authentication	✓	
Dynamic WEP Encryption/TKIP/AES	✓	
Alternate Encryption (IPSec, PPTP, SSL)		✓
Access Control and Policy Management		✓
Guest/Visitor Access (Support for "client-free" devices)		✓
Bandwidth Management		✓
Support for any mobile device		✓
Support for Secure Roaming		✓
Intrusion Detection/Protection		✓
Rogue Access Point Detection		✓

- ◆ 使用針對有線環境設計的入侵偵測系統
 - 無法辨識 無線網路環境獨有的攻擊
- ◆ 使用針對有線環境設計的弱點檢查工具
 - 無法辨識 無線網路環境獨有的弱點
 - 容易出現誤判
- ◆ 使用移動式的無線網路掃描及測試工具
 - 僅能得到概略性的了解, 被動式的進行
- ◆ 針對 **AP** 和 **Switch** 的基本安全監督工具
 - Airespace, Aruba, Cisco, Proxim, Symbol, Trapeze
 - 有限的警示功能, 僅能針對特定的廠牌

五種建立堅實的無線網路安全性的基本要素



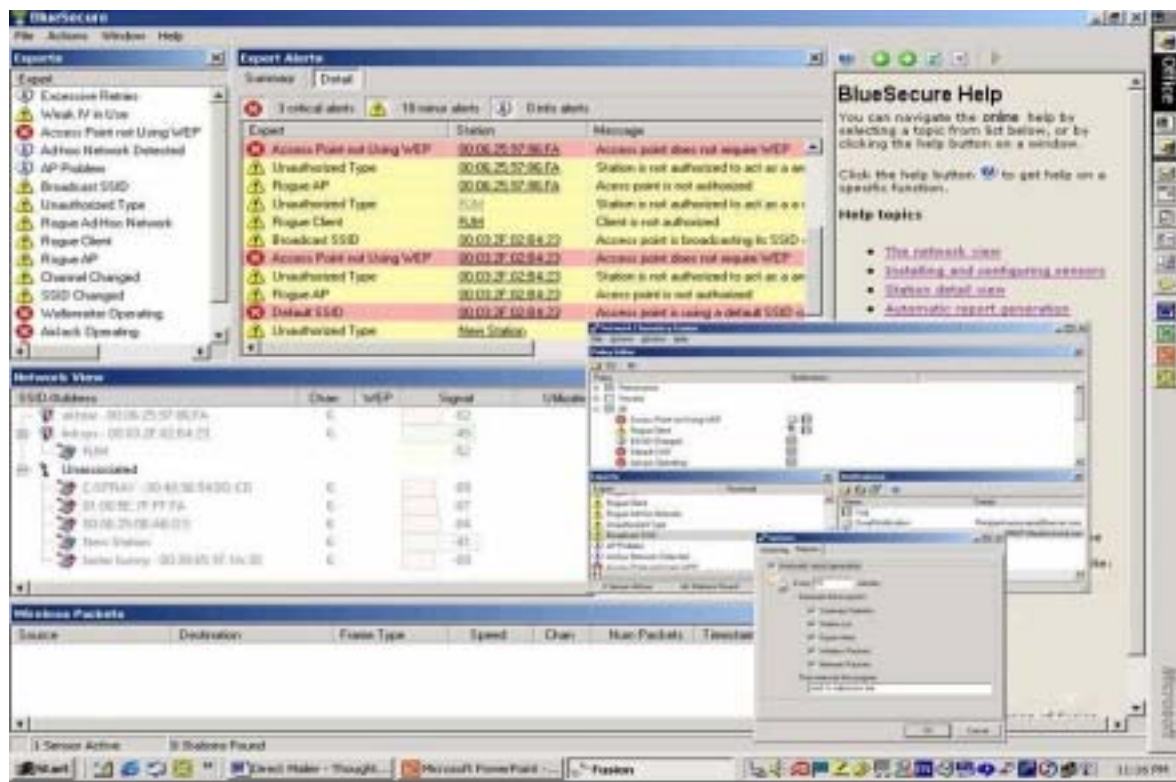
- ◆刺探攻擊(Probe Attack): AP 掃描
- ◆監聽攻擊: 竊聽通訊內容
- ◆偽造 AP: Man in middle Attack
- ◆阻礙服務(DoS): Storms
- ◆網路入侵
- ◆用戶端入侵

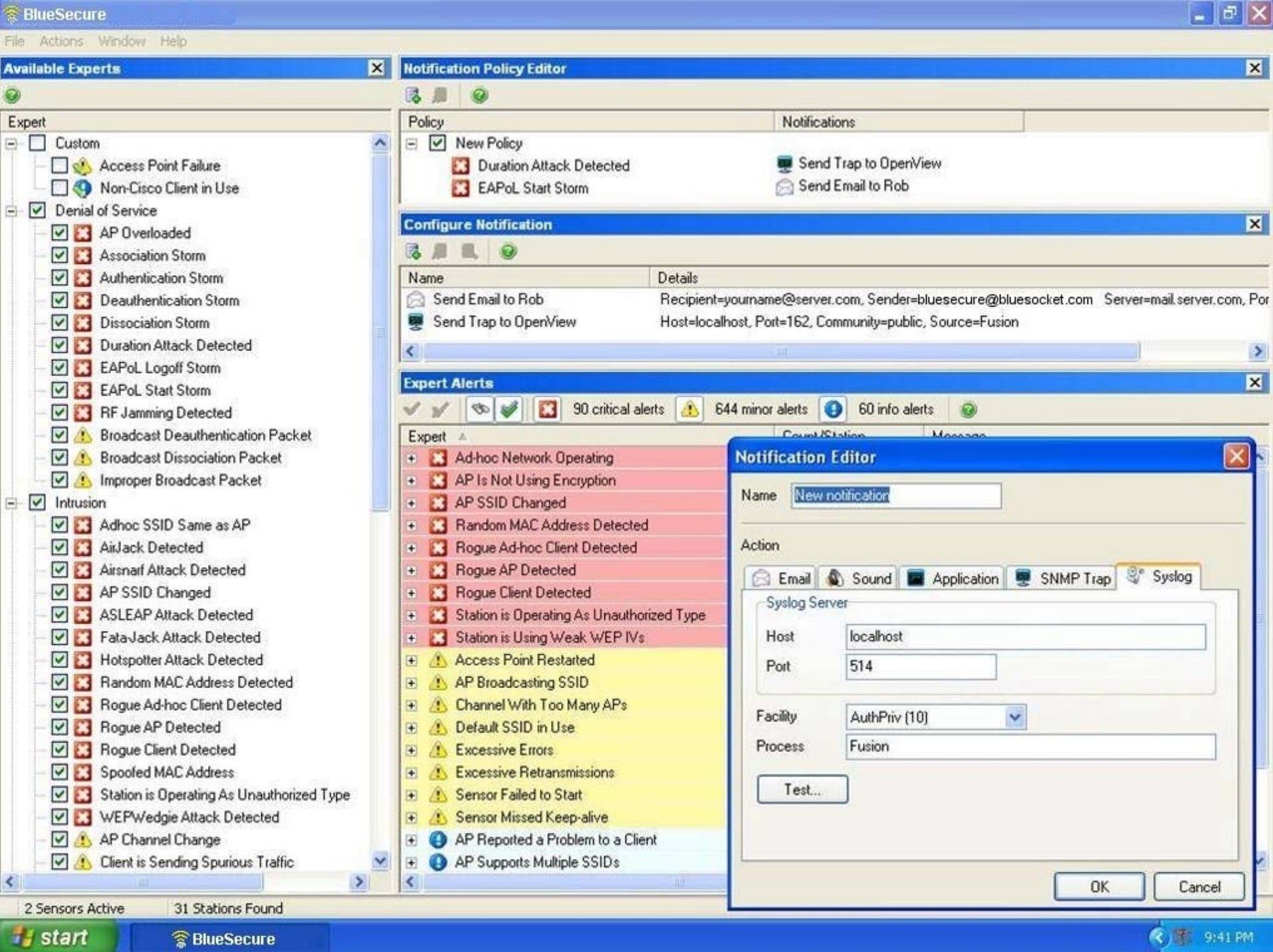
一旦成功入侵:

- 竊取用戶端或網路中的資料
- 破壞網路運作
- 植入 Worm 或是木馬程式
- 利用網路當作跳板

- ◆ 特殊設計的監聽設備
- ◆ 擷取 AP 和用戶端間的無線網路封包
- ◆ 外界無法發現此一設備的存在
- ◆ 建置在接近 WLAN 的地方以覆蓋多個 AP
- ◆ 由 BlueSecure Server 進行分析以提升擴充性
- ◆ 支援 802.11 a/b/g







BlueSecure

File Actions Window Help

Available Experts

Expert

Custom

Access Point Failure

Non-Cisco Client in Use

Denial of Service

AP Overloaded

Association Storm

Authentication Storm

Deauthentication Storm

Dissociation Storm

Duration Attack Detected

EAPoL Logoff Storm

EAPoL Start Storm

RF Jamming Detected

Broadcast Deauthentication Packet

Broadcast Dissociation Packet

Improper Broadcast Packet

Intrusion

Adhoc SSID Same as AP

AirJack Detected

Airsnarf Attack Detected

AP SSID Changed

ASLEAP Attack Detected

Fata-Jack Attack Detected

Hotspotter Attack Detected

Random MAC Address Detected

Rogue Ad-hoc Client Detected

Rogue AP Detected

Rogue Client Detected

Spooled MAC Address

Station is Operating As Unauthorized Type

WEPWedgie Attack Detected

AP Channel Change

Client is Sending Spurious Traffic

Notification Policy Editor

Policy

New Policy

Duration Attack Detected

EAPoL Start Storm

Notifications

Send Trap to OpenView

Send Email to Rob

Configure Notification

Name

Details

Send Email to Rob

Recipient=yourname@server.com, Sender=bluesecure@bluesocket.com Server=mail.server.com, Por

Send Trap to OpenView

Host=localhost, Port=162, Community=public, Source=Fusion

Expert Alerts

90 critical alerts

644 minor alerts

60 info alerts

Expert

Ad-hoc Network Operating

AP Is Not Using Encryption

AP SSID Changed

Random MAC Address Detected

Rogue Ad-hoc Client Detected

Rogue AP Detected

Rogue Client Detected

Station is Operating As Unauthorized Type

Station is Using Weak WEP IVs

Access Point Restarted

AP Broadcasting SSID

Channel With Too Many APs

Default SSID in Use

Excessive Errors

Excessive Retransmissions

Sensor Failed to Start

Sensor Missed Keep-alive

AP Reported a Problem to a Client

AP Supports Multiple SSIDs

Notification Editor

Name

New notification

Action

Email

Sound

Application

SNMP Trap

Syslog

Syslog Server

Host

localhost

Port

514

Facility

AuthPriv (10)

Process

Fusion

Test...

OK

Cancel

2 Sensors Active

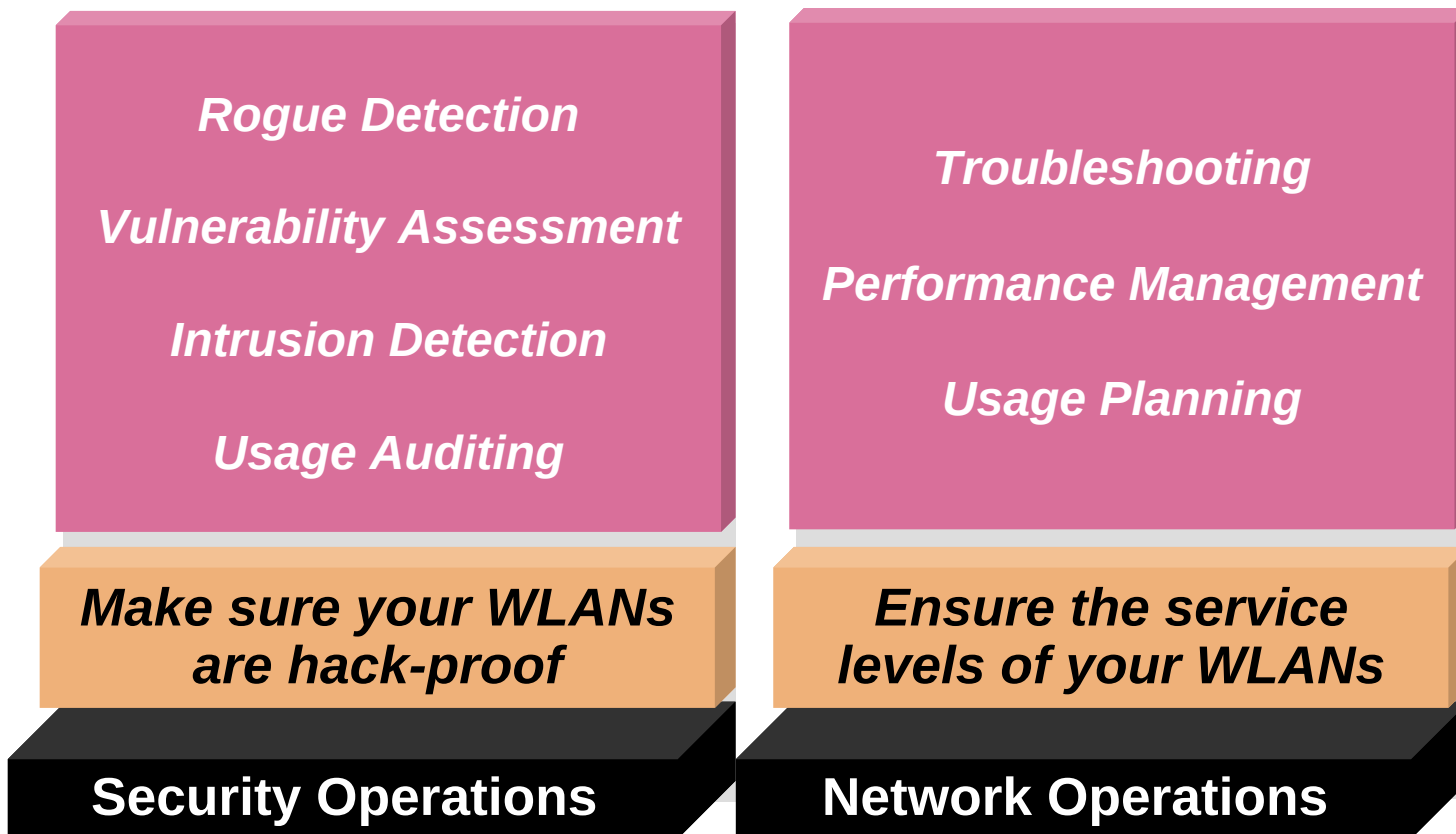
31 Stations Found

start

BlueSecure

9:41 PM

Deployed 802.11 RF Monitoring System for:



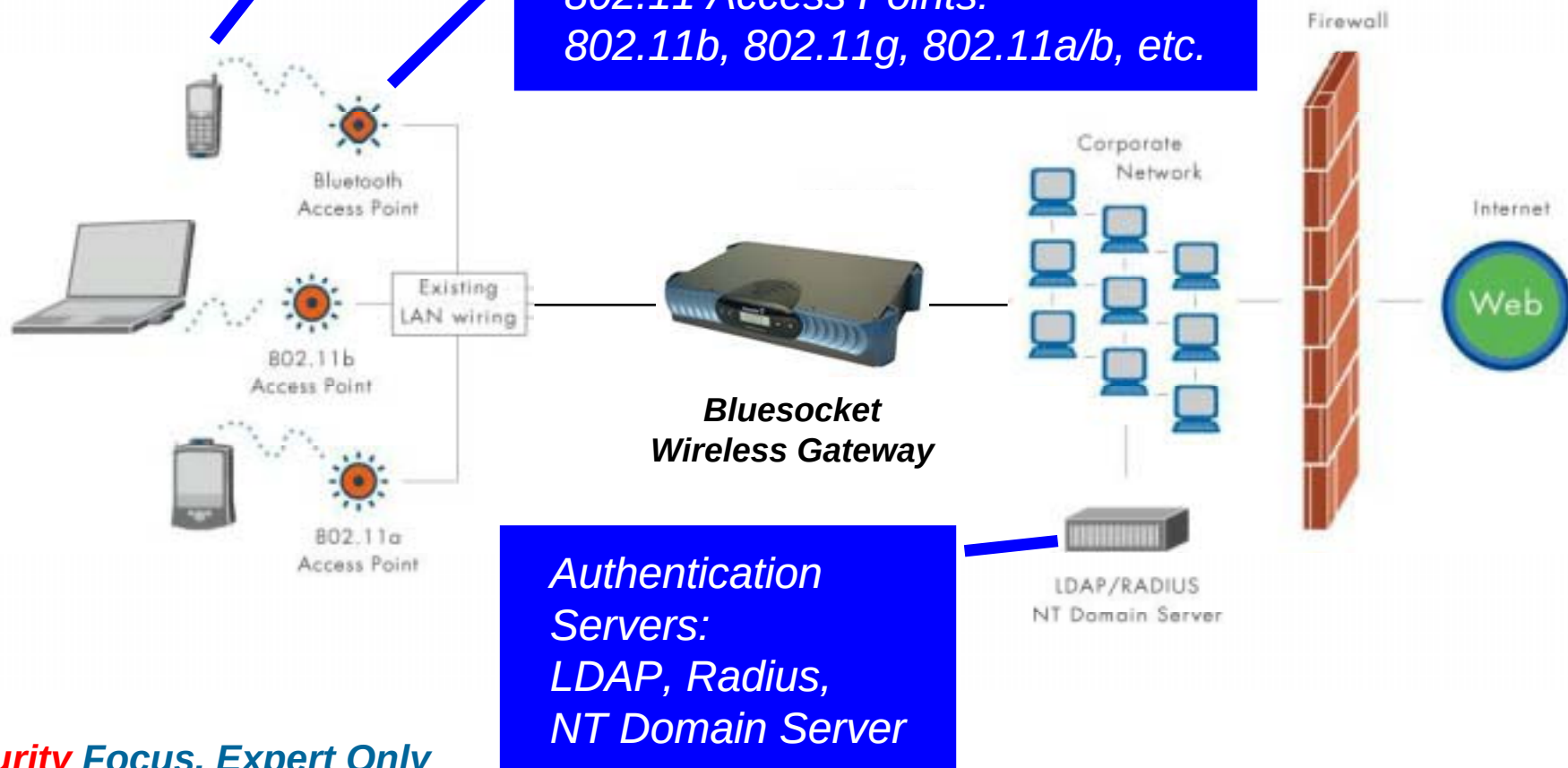
- ◆ 提供 **WLAN** 的完整安全解決方案:
 - BlueSecure Intrusion Protection System: RF 安全及政策 Policy
 - Bluesocket Wireless Gateway: 使用者安全及政策
- ◆ 特製的 **RF Monitoring Sensor**
- ◆ 提供精確的警示功能: **Multi-Method, Correlated, RapidScan**
- ◆ 最佳的架構: 堅實的架構、強大的延展性
- ◆ 開放的架構支援不同廠商的整合能力
- ◆ **Plug-n-Play** 的設定及運作能力
- ◆ 低導入成本、低擁有成本 (**Total Cost of Ownership**), 快速的投資回報(**ROI**)

Bluesocket Wireless Gateway

Plug-n-Play Enterprise WLAN Security/Control

Mobile Devices: NIC or Built-In 802.11

*802.11 Access Points:
802.11b, 802.11g, 802.11a/b, etc.*



◆通用的認證能力

- 可以使用 帳號/密碼、數位憑證、Smart Card、證 Token 等方式，完全根據安全需求調整
- 使用者資料可放置在 Local 或是集中的資料庫 (LDAP、RADIUS 或 NT Domain) 以方便管理

◆提供安全保護

- 提供 “Role-based” 管理，可針對不同類型的使用者開放不同的權限
- 支援個種安全的 VPN 機制，例如：PPTP、L2TP 或是 IPSec 等

◆提供安全的移動能力 (Secure Mobility™)

- 使用者可以無接縫的跨越不同的網段，同時還能保持無線網路的私密性

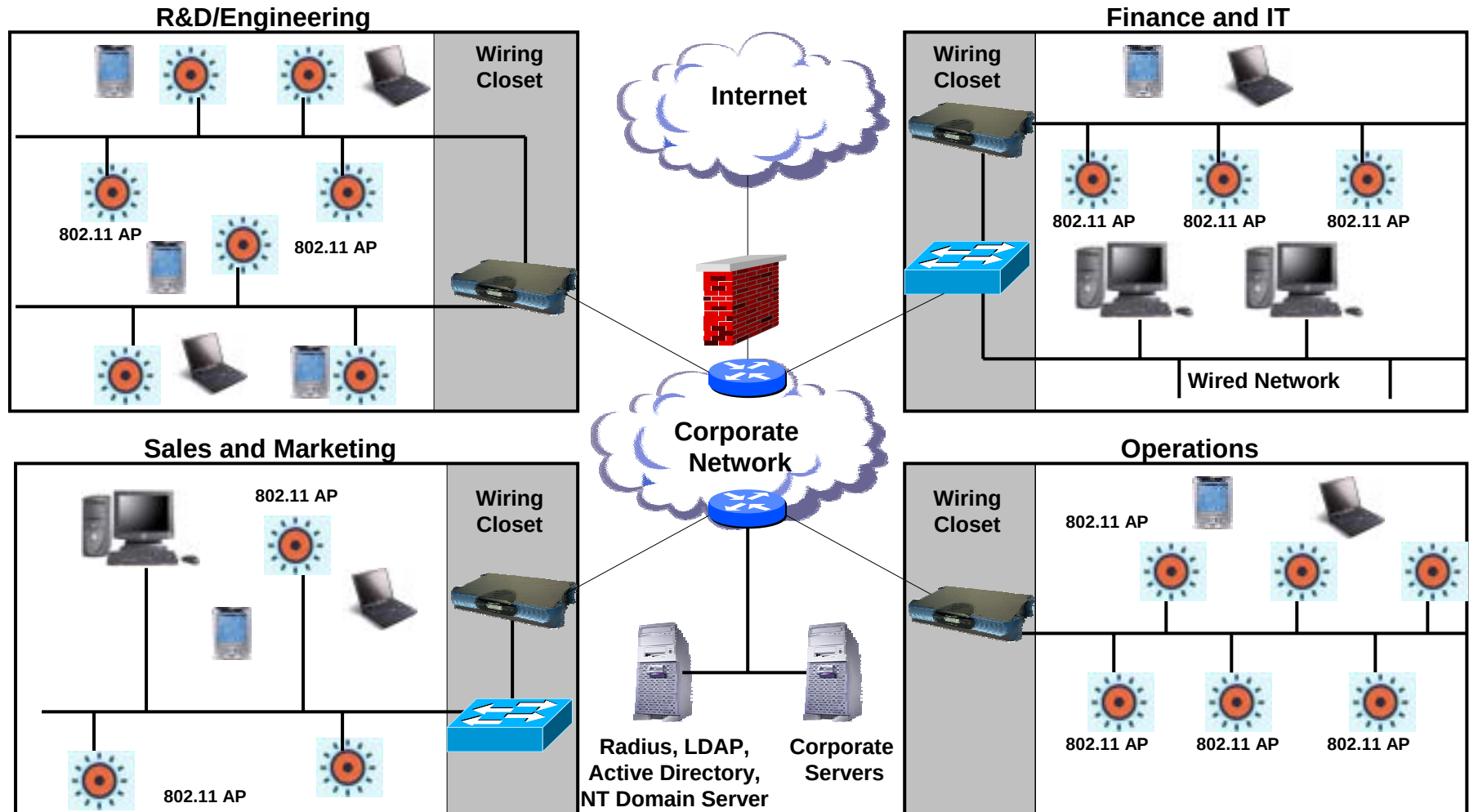
◆管理能力

- Web-base 管理介面，並且可以方便及由遠端集中管理

◆QoS 功能(Quality of Service)

- 提供網路優先權控制
- 可針對對時間敏感的服務降低封包延遲以提升效能

Mobile Devices + Off-the-shelf APs + Wireless Gateways + Unchanged Legacy Network



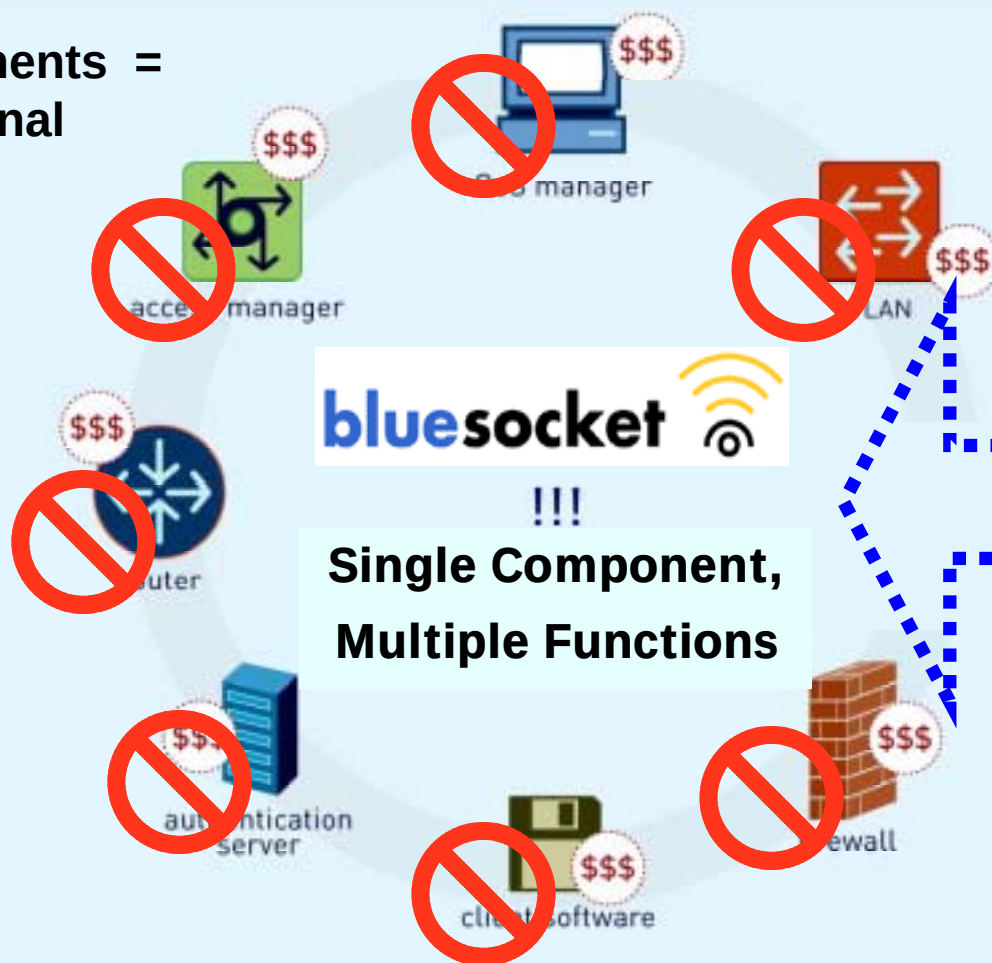
◆安全政策強化

- 具體的 WLAN 安全政策支援
- 可根據使用者角色(role)、使用者、使用時間、使用服務等進行控制
- 每一種使用者可以給予不同的最大頻寬限制來保證 QoS

◆相容性

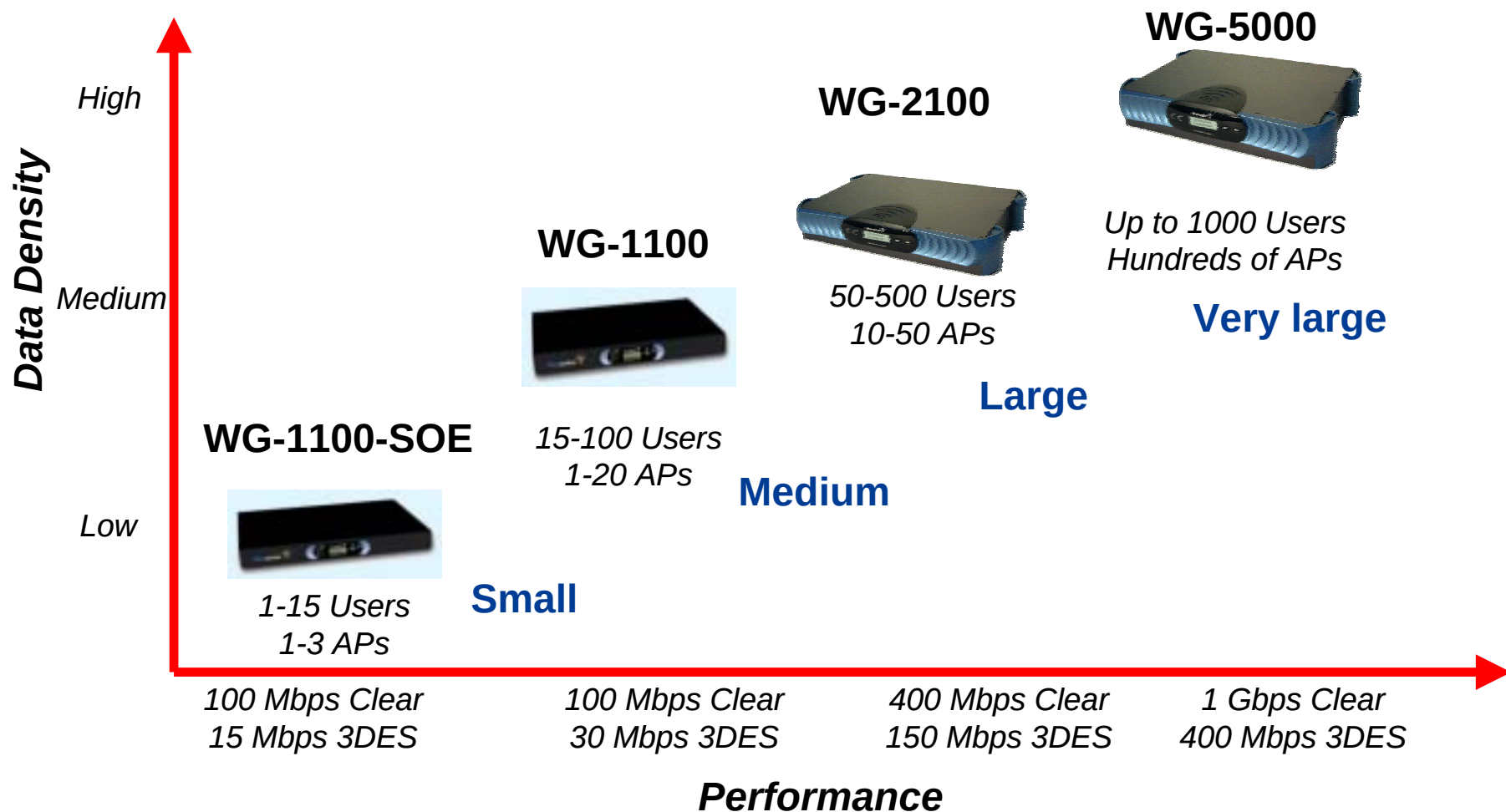
- 提供任意廠牌的設備連線
- 和過去、現在、未來所有主要的 AP 廠商相容
- 支援各式的移動式設備，不需特殊的用戶端軟體

Many Components =
High Operational
Expense

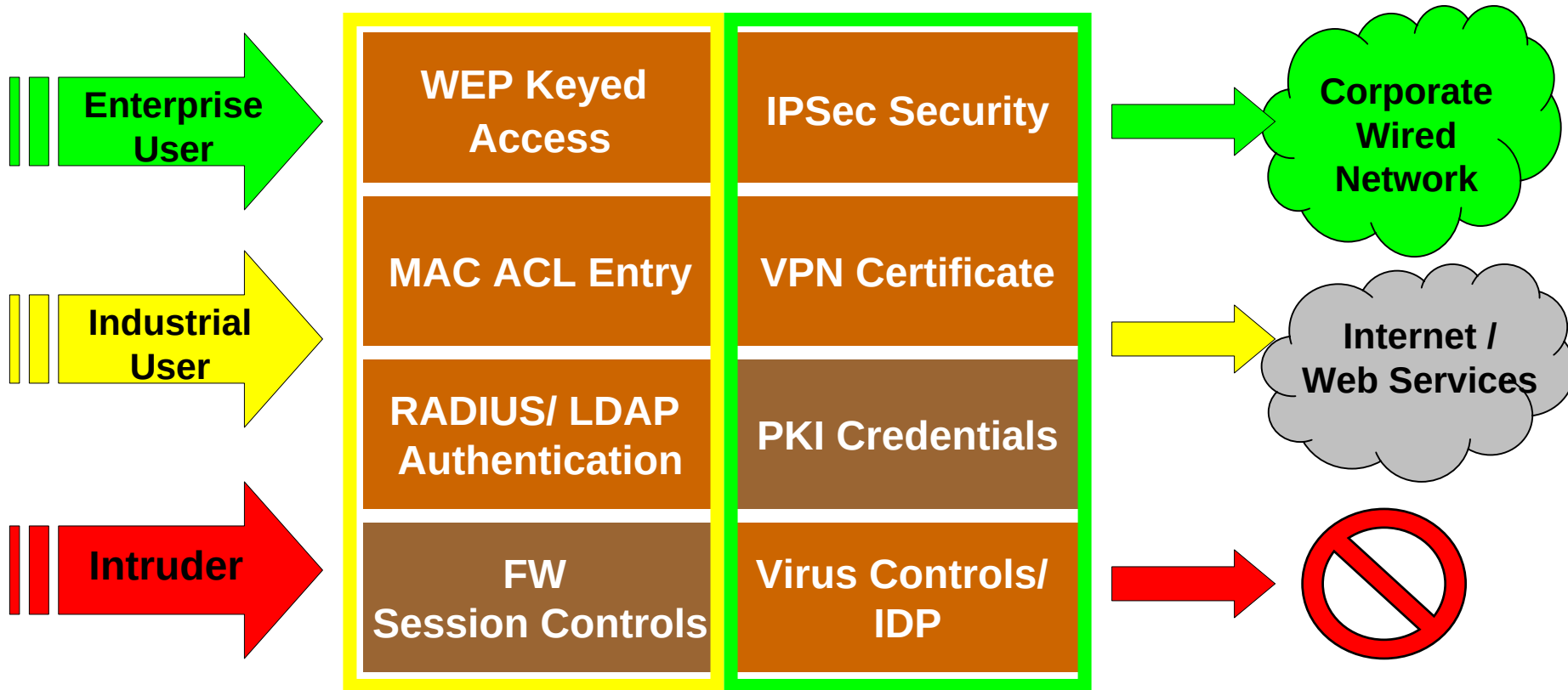


**Single Component,
Multiple Functions**

-  Authentication
-  Encryption
-  Firewall
-  Mobility
-  QOS/ BWM
-  Policy
-  Interoperability
-  Bandwidth Mgt



Multi-Layered Security



◆4.0 新增功能

- 提供入侵偵測及蠕蟲防護功能
- 更強的 Cisco 的整合能力
 - 第一個支援 Cisco 802.1x EAP-FAST 的設備 (整合 LEAP, PEAP, TLS, TTLS)
- 提供 Voice over WLAN 的安全的漫遊能力
- 提供大規模 WLAN 環境的 Load Sharing 能力
- 支援 HP OpenView
- 其他額外的功能特色

- ◆ 攻擊者不再只從外界進入
- ◆ 避免 “Zero-Day Attack”
 - 在病毒碼更新前阻擋快速擴散的蠕蟲
- ◆ 用戶端軟體可能無法完全掌控
 - 訪客、約聘人員可能使用各種不同的 OS 或軟體
- ◆ 弱點掃描無法解決使用者自行的惡意行為
- ◆ 需要針對使用者行為的即時的監督機制辨識及阻擋對網路有害的行為



◆ **Bluesocket** 即時監視所有的 WLAN 流量

◆ 根據管理者設定的門檻值檢查使用者行為

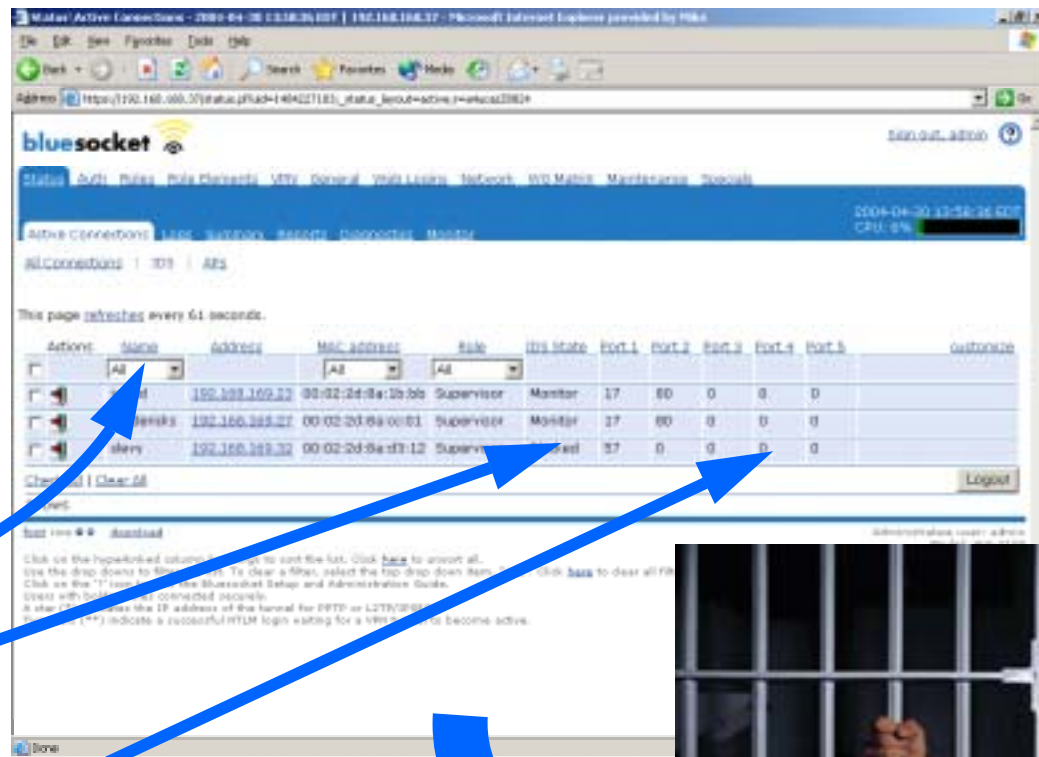
◆ 提供 Zero-Day 保護, 不需倚賴

Name of User
Attacking or
Infected

IDS State
(ex: "Blocked
or Monitored")

Ports being
used in
attack/worm
exploit

管控能力



◆ 針對 Cisco AP-Base 網路的額外功能

◆ 第一個支援 Cisco 802.1x EAP-FAST 的設備 (整合LEAP, PEAP, TLS, TTLS)

◆ Cisco 環境檢視

➢ 監控 Cisco APs

➢ 辨識使用者在 AP 的頻寬

AP Name,
Location
and MAC

Cisco Firmware

Which user is
on
the AP

What Cisco
Model
and Firmware

Active Connections

This page refreshes every 61 seconds.

Actions	Name	Address	MAC address	Associations	ESSID	Vendor	Info	password
☐	Lobby	0.0.0.220	00:40:96:50:39:11		Picnic	Cisco Systems	350 Series/5.30.30	
☐	9th Floor	0.0.0.225	00:40:96:50:39:17	john alex jared mrover mike	Picnic	Cisco Systems	350 Series/5.30.30	
☐	Office floor	0.0.0.228	00:40:96:50:39:5A	Fredericks john bob pow	Picnic	Cisco Systems	1100 IOS 12.2	

3 rows

- ◆ **WLAN 安全 and 管理的領導廠商**
 - 使用者和頻寬的安全和政策管理
- ◆ **提供完整的 WLAN 安全和控制解決方案**
 - 針對不同規模的環境提供適當的解決方案
 - 針對 WLAN 環境的入侵防禦系統
- ◆ **經過實証的 WLAN 開放式系統**
 - 完全開放的架構— 和多種廠商相容
 - 不限制客戶的選擇: (AP, 設備, 認證, 機密)

Education



HARVARD



Healthcare



Government



Enterprise

Honeywell



TOYOTA



校園環境成功案例



HARVARD UNIVERSITY



University of Edinburgh



WAYNE STATE
UNIVERSITY



UNIVERSITY OF ROCHESTER

UNIVERSITY OF CALIFORNIA
HASTINGS COLLEGE OF THE LAW



The University of Georgia



THE UNIVERSITY OF ARIZONA®

Singapore Polytechnic

無線與有線網路的整體安全防護



- ◆ 在每一個網路入口建立安全機制
 - 網路防火牆: 存取控制
 - 保護遠端存取機制: 可控制權限的 VPN
 - 入侵偵測及入侵防禦
- ◆ 保護 Email 資料流:
 - 病毒及垃圾郵件防護, 安全政策控制
 - 遠端存取
- ◆ 保護用戶端
- ◆ 在無線網路的入口建立控管機制
- ◆ 使用弱點管理進行安全強化

Thank You!