REPORTER 銷售關鍵點

The smartest syslog reporter in the world

新一代校園網路維運與安全管理平台

*石謂龍 **Robin Shih***

Product Director

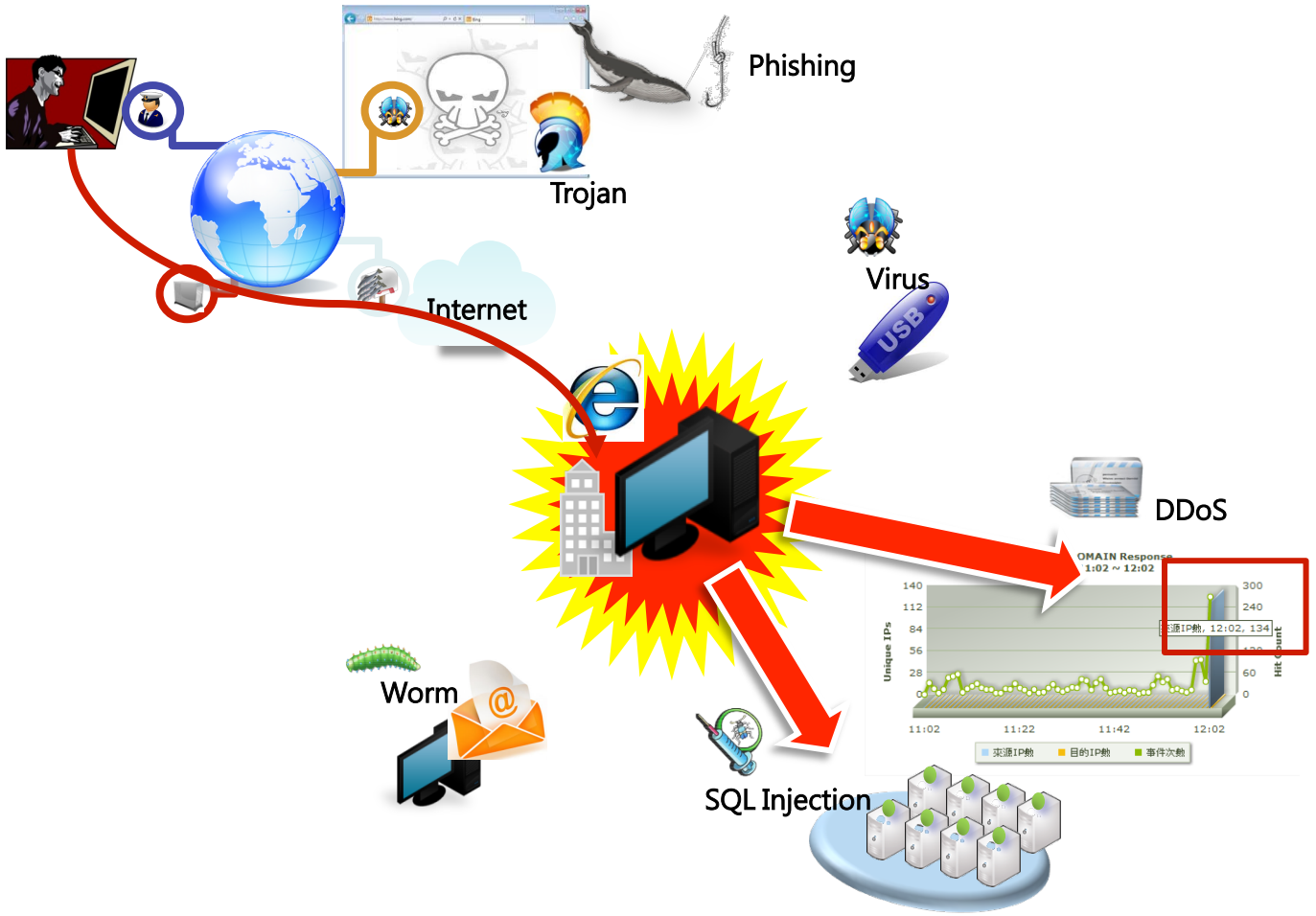
rshih@npartnertech.com

+886-935784086

N-Partner

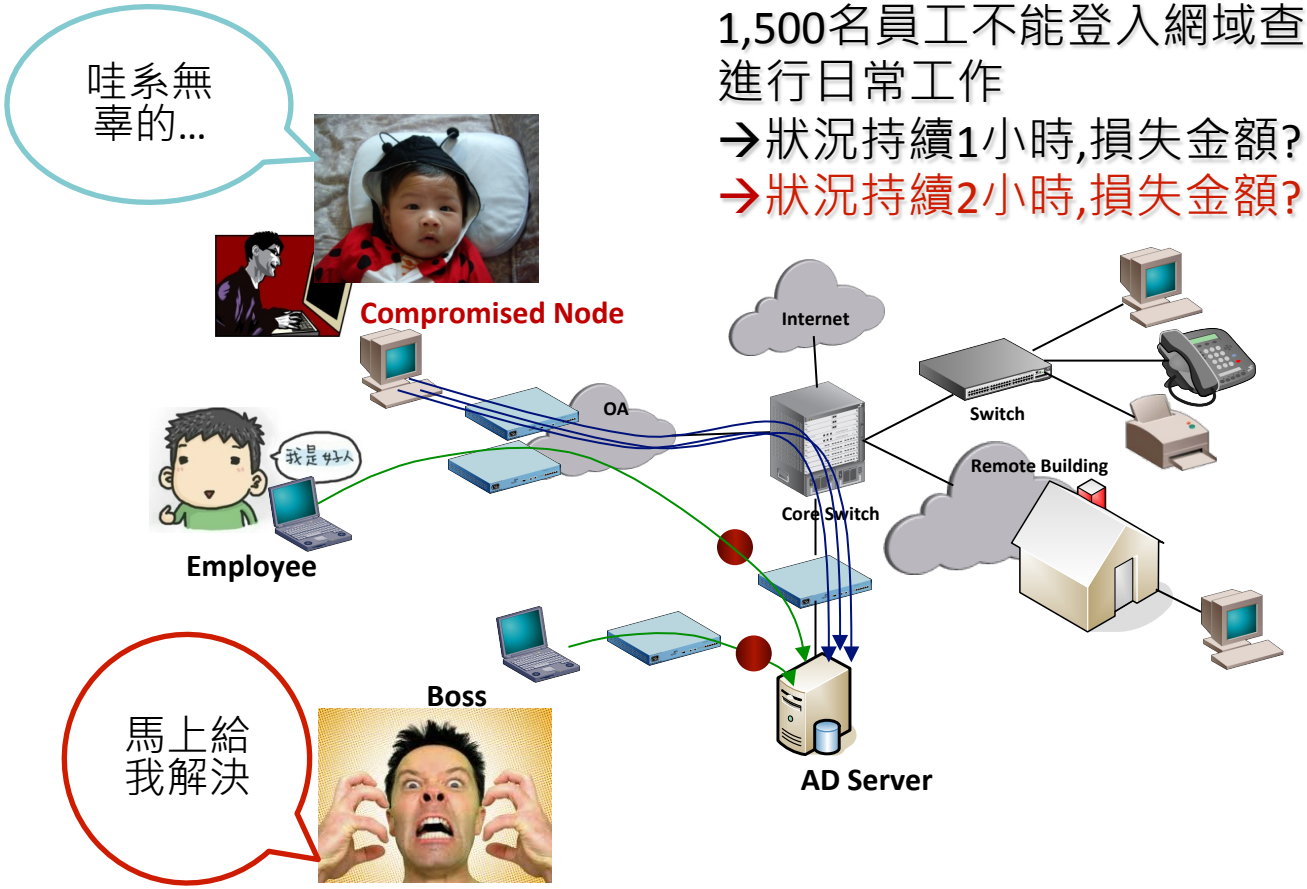
Next Generation Technologies & Security of Network

規畫防禦作為前先瞭解安全事件的起源



REAL CASE STUDY (無法登入網域)

來自內部的AD密碼暴力猜測攻擊→多數員工AD帳號遭Lock



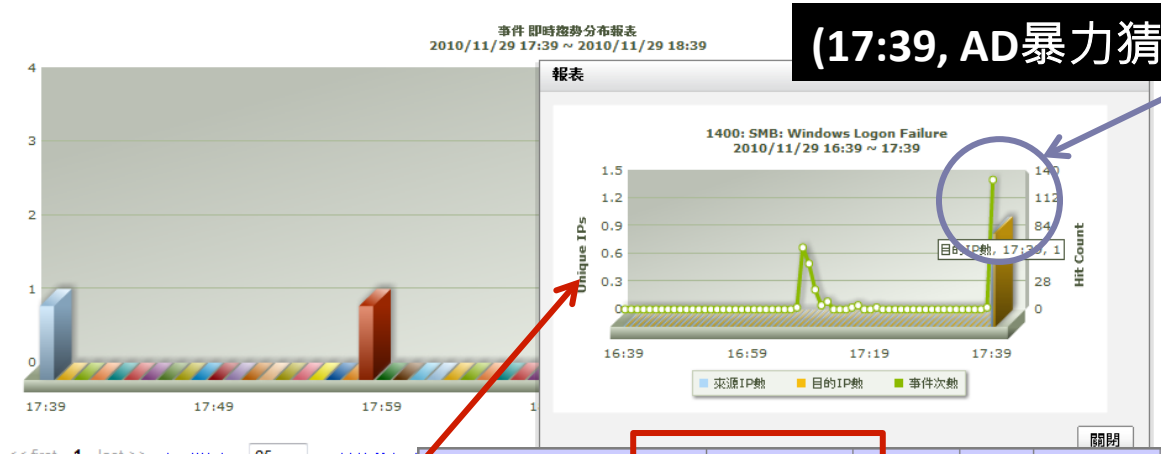
1,500名員工不能登入網域查閱資料與進行日常工作

→狀況持續1小時,損失金額?

→狀況持續2小時,損失金額?

Real Case Study (AD brute force attacks Cont.)

(17:39, AD暴力猜測行為發生突增)



<< first 1 last >> 每頁顯示: 25 目前所在頁

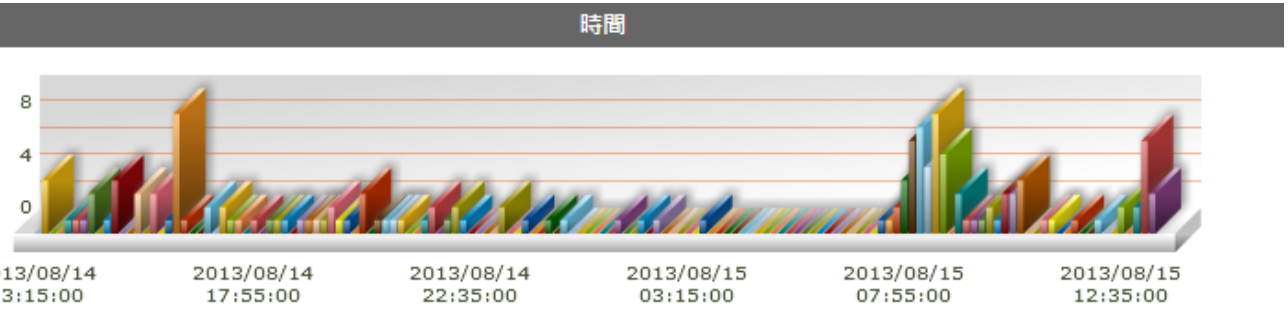
事件	突增
6924: DNS: NXDOMAIN Response	2010/11/
1400: SMB: Windows Logon Failure	2010/11/

(找到攻擊來源)

事件	來源IP	來源Port	區域	目的IP	目的Port	目的名稱解析	區域	次數
1400: SMB: Windows Logon Failure	111.148.238.223	2539		192.168.10.5	microsoft-ds(445)	台北辦公室		65
1400: SMB: Windows Logon Failure	111.148.238.223	2539		192.168.10.5	microsoft-ds(445)	台北辦公室		65
1400: SMB: Windows Logon Failure	111.148.238.223	58828		192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	111.148.238.223	58828		192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	58159	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	58159	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	65291	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	114.51.26.141	65291	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	114.51.26.141	60331	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	114.51.26.141	60331	JP	192.168.10.5	microsoft-ds(445)	台北辦公室		1
1400: SMB: Windows Logon Failure	80.191.236.226	1120	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		4
1400: SMB: Windows Logon Failure	80.191.236.226	1120	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		4
1400: SMB: Windows Logon Failure	80.191.236.226	3922	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	80.191.236.226	3922	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		2
1400: SMB: Windows Logon Failure	80.191.236.226	3922	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		10
1400: SMB: Windows Logon Failure	80.191.236.226	3922	IR	192.168.10.5	microsoft-ds(445)	台北辦公室		10

人工智慧的案例

從AD登入訊息發現密碼猜測



帳號密碼猜測 153

10.42.184.161
正在執行密碼猜測

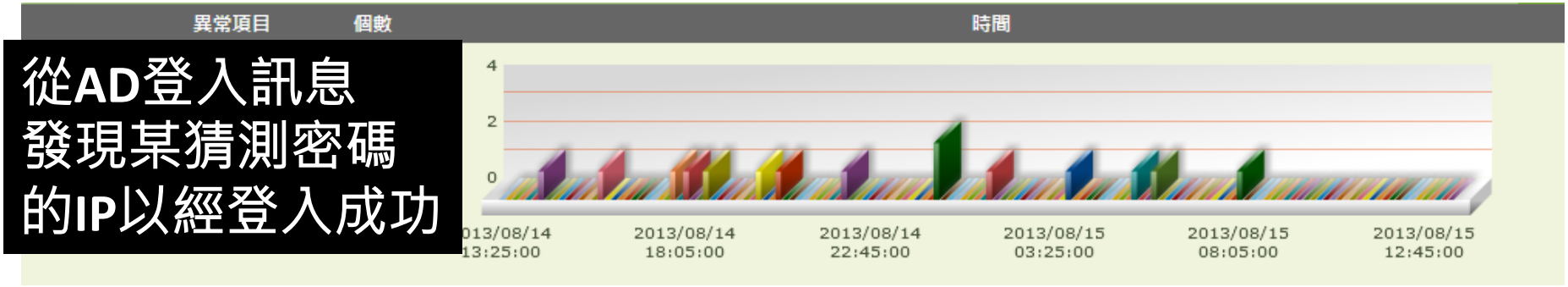
事件	來源IP	Audit User	時間	設備
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02
Invalid User Login (Security: 672)	10.42.184.161	jeff	2013/08/15 13:09:55	OA AD02

事件	來源IP	Audit User	時間
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:14
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/15 09:08:09

事件	來源IP	Audit User	時間
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11
Invalid User Login (Security: 672)	10.42.61.64	john6_ye	2013/08/14 17:31:11

人工智慧的案例

從AD登入訊息
發現某猜測密碼
的IP以經登入成功

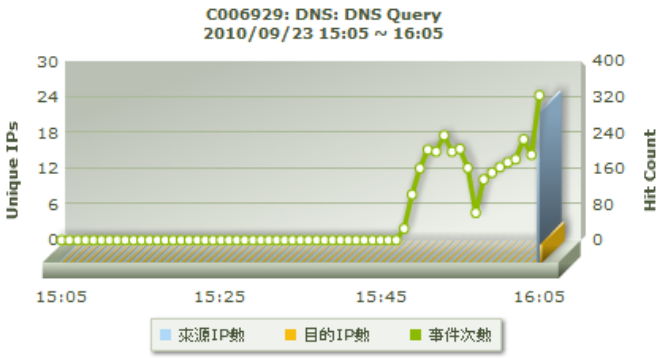


這個IP正在執行密碼猜測
最後成功登入

事件	來源IP	Audit User	時間	設備
Logon Success (Security: 673)	10.42.201.2	K000477	2013/08/15 00:20:01	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/15 00:18:46	OA AD02
Login Failure (Security: 675)	10.42.201.2	K1102366	2013/08/14 23:52:49	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:46:23	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000477	2013/08/14 23:45:33	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:39:37	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:37:12	OA AD02
Login Failure (Security: 675)	10.42.201.2	K000474	2013/08/14 23:33:56	OA AD02

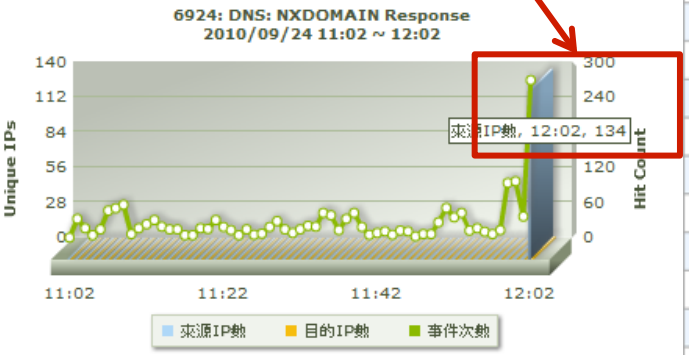
Real Case Study (校園DNS Server遭DDoS癱瘓)

巨量DNS詢問請求→FW/DNS無法負荷→Internet網路緩慢



事件	來源IP	目的IP	目的Port	次數
C006929: DNS: DNS Query	210.60.205.37	7.126.1	domain(53)	348
C006929: DNS: DNS Query	210.60.205.30	7.126.1	domain(53)	204
C006929: DNS: DNS Query	163.27.126.250	7.126.1	domain(53)	193
C006929: DNS: DNS Query	210.60.205.56	7.126.1	domain(53)	132
C006929: DNS: DNS Query	210.60.205.19	7.126.1	domain(53)	121
C006929: DNS: DNS Query	163.27.126.253	7.126.1	domain(53)	86
C006929: DNS: DNS Query	210.60.205.29	7.126.1	domain(53)	81
C006929: DNS: DNS Query	210.60.205.85	7.126.1	domain(53)	76

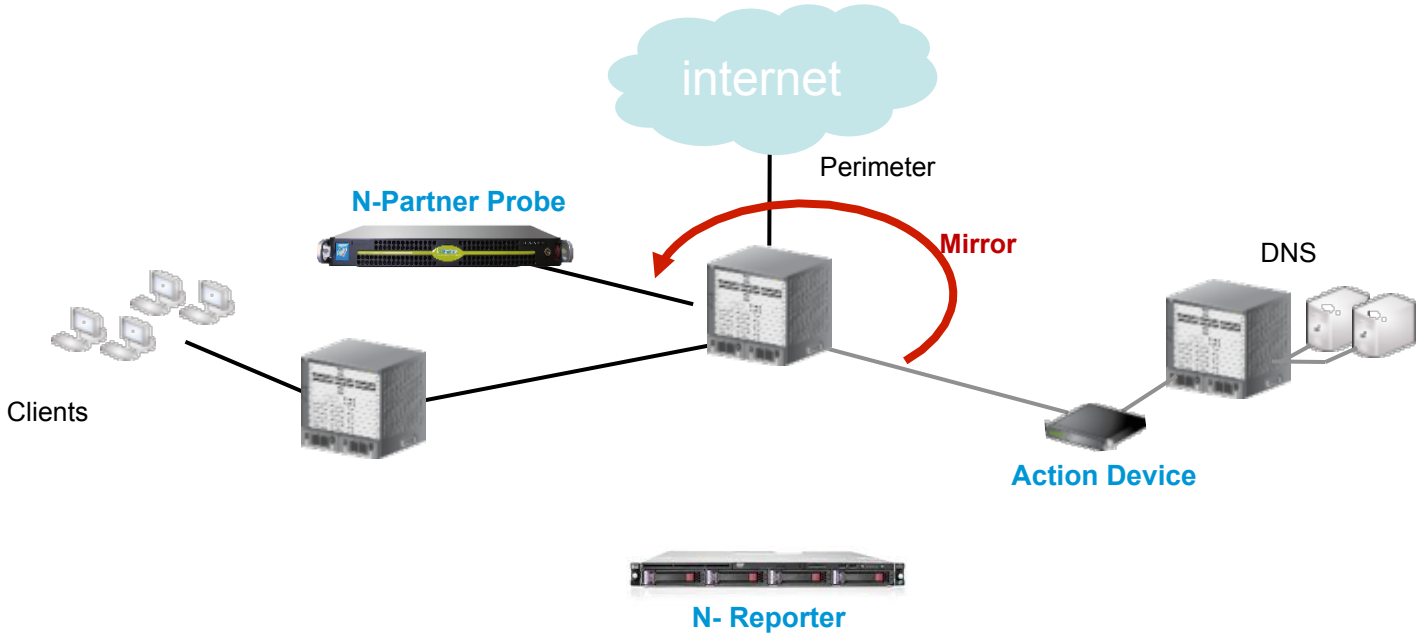
(134個來源IP
同時發起不存在網址詢問)



事件	來源IP	區域	目的IP	目的Port	次數
6924: DNS: NXDOMAIN Response	200.28.4.130	CL	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	200.28.4.157	CL	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	202.102.199.82	CN	.126.1	domain(53)	4
6924: DNS: NXDOMAIN Response	61.147.37.196	CN	.126.1	domain(53)	4
6924: DNS: NXDOMAIN Response	220.167.29.243	CN	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	220.167.29.239	CN	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	61.233.154.42	CN	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	218.85.152.21	CN	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	218.85.157.74	CN	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	80.190.211.10	DE	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	62.146.0.10	DE	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	212.123.96.110	DE	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	200.107.10.62	EC	.126.1	domain(53)	2
6924: DNS: NXDOMAIN Response	80.12.204.167	FR	.126.1	domain(53)	2

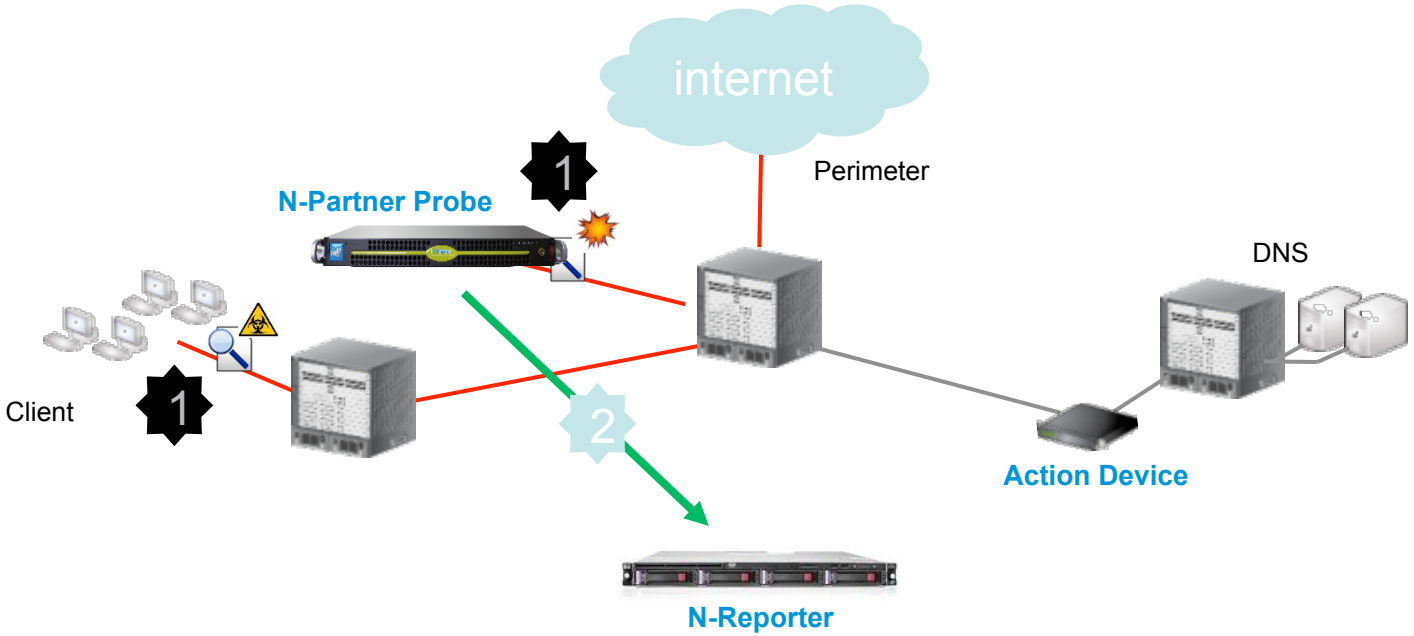
DNS Protection Solution: Deployment Example

- *Mirror DNS traffic to Probe Analyzer*

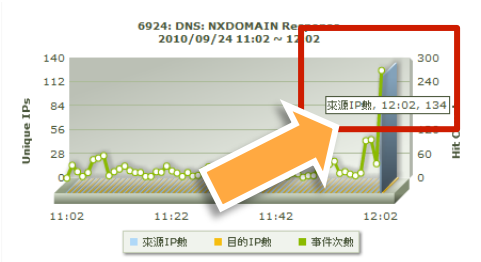


DNS Protection Solution: Deployment Example

- *1: Probe sends NX Domain Logs to N-Reporter*



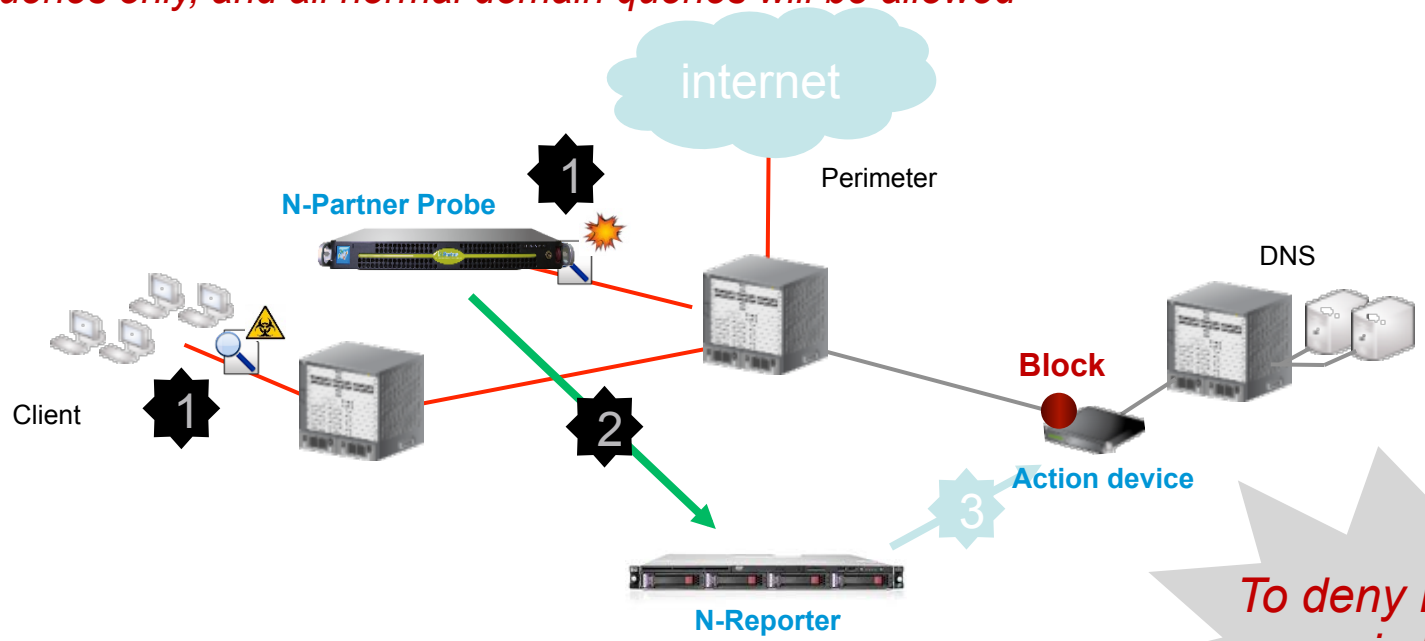
- *2: N-Reporter generates NX Domain list*

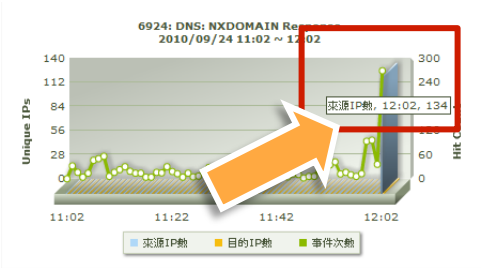


N REPORTER

DNS Protection Solution: Deployment Example

- *3: N-Reporter sends NX Domain list to action device. It's not IP isolation. We block NX Domain queries only, and all normal domain queries will be allowed*





To deny NX Domain query is the best solution against NX Domain attacks using spoof IPs

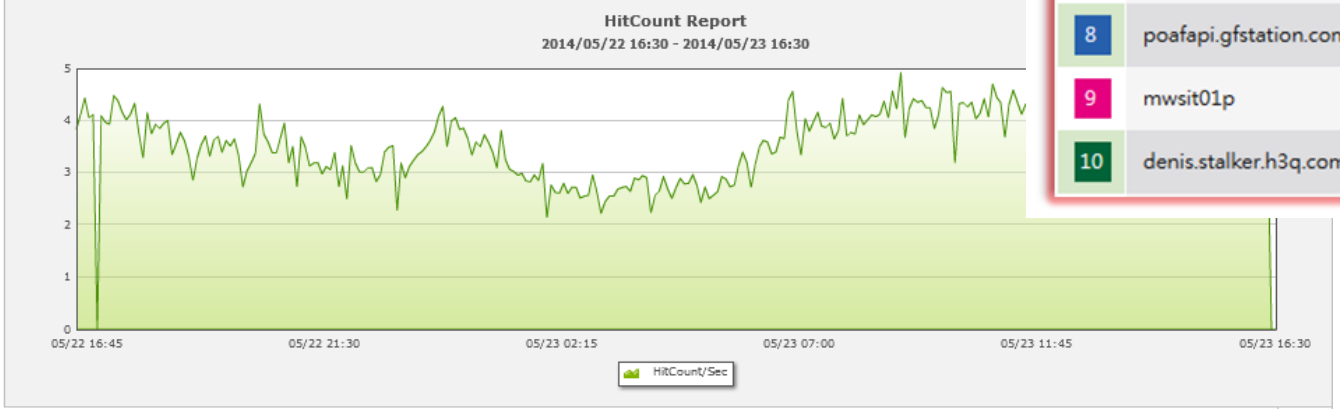
N REPORTER

NX Domain Query Behavior- 24 hours monitoring result

NO.	NX Domain Name	Hit Count
1	[redacted].net.tw	75.86K
2	bcmlbsqa1@broadcom.com	28.09K
3	ssl	24.36K
4	samsungvuieventlog.vlingo.com	15.51K
5	api.mapbee.com	7.82K
6	h-slp.mnc001.mcc466.pub.3gppnetwork.org	2.48K
7	f1.bumpserver.com	2.2K
8	poafapi.gfstation.com	1.39K
9	mwsit01p	1.37K
10	denis.stalker.h3q.com	1.36K

	Hit Count	Session	Packets
平均	3.55	0.00	0.00
最大值	5	0	0
最小值	2	0	0

HitCount



REPORTER

NX Domain Query TOP 10 Makers- 24 hours statistic

NO	Event Name	Source IP	Src Country	Destination IP	Dest Country	Hit Count
1	N-Box 1031: NXDomain	[redacted]	TW	[redacted]	TW	2.07K
2	N-Box 1031: NXDomain		TW		TW	1.7K
3	N-Box 1031: NXDomain		TW		TW	1.55K
4	N-Box 1031: NXDomain		TW		TW	1.5K
5	N-Box 1031: NXDomain		TW		TW	1.49K
6	N-Box 1031: NXDomain		TW		TW	1.46K
7	N-Box 1031: NXDomain		TW		TW	1.35K
8	N-Box 1031: NXDomain		TW		TW	1.28K
9	N-Box 1031: NXDomain		TW		TW	1.27K
10	N-Box 1031: NXDomain		TW		TW	1.23K

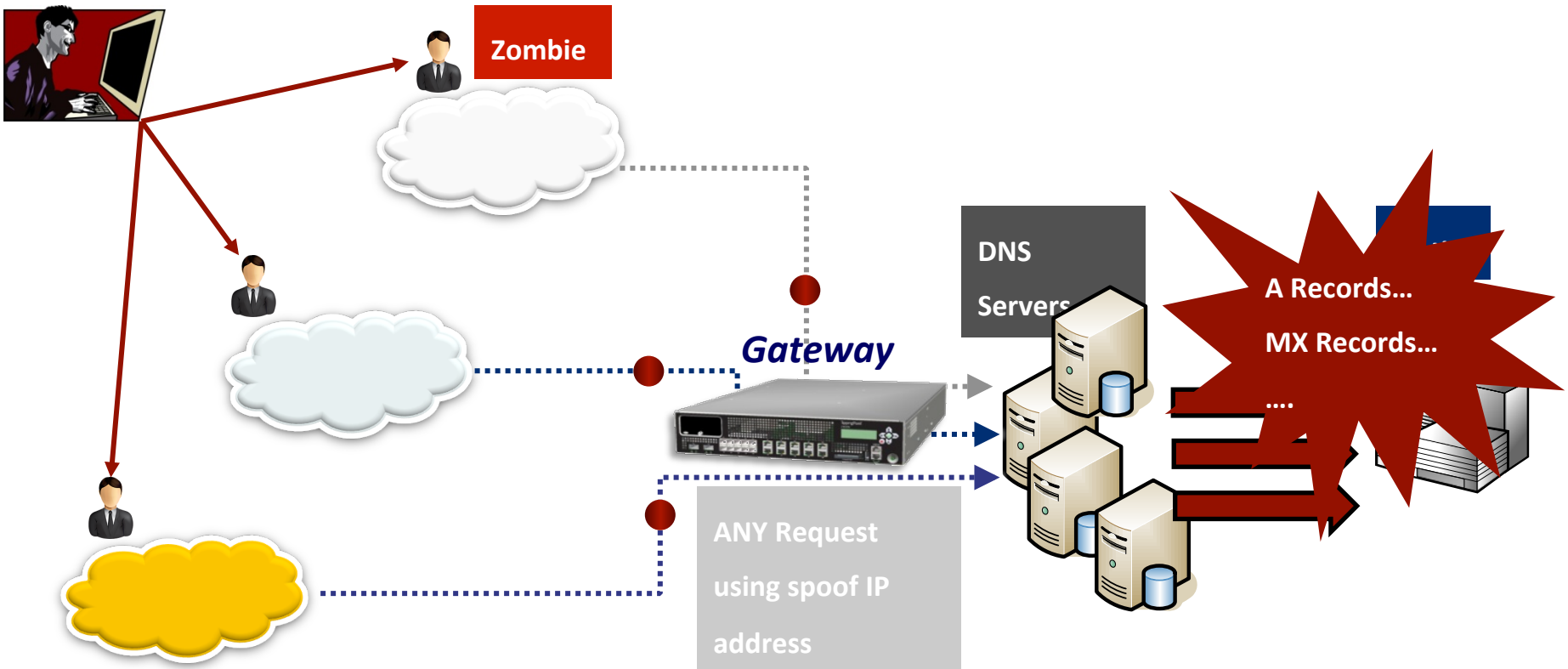
Deny NX Domain Query- 24 hours statistic

- *Deny NX Domain queries- Save DNS servers*

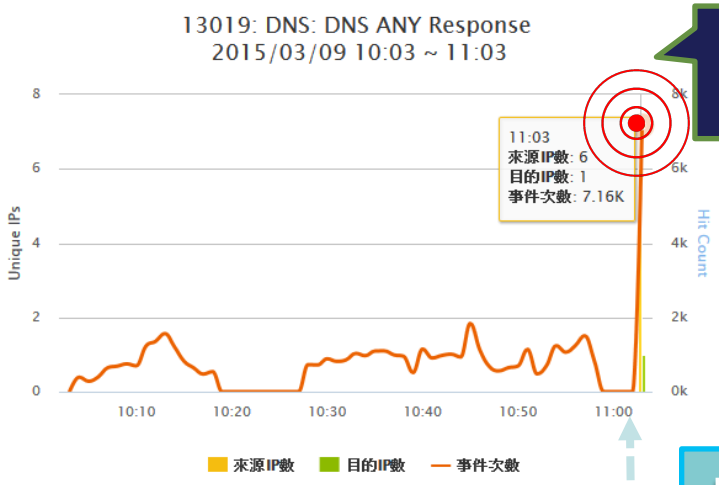
NO.	Event Name	Source IP	Src Country	Destination IP	Hit Count
1	NXDomain-Black-List _sip._tcp.sip.linkyes.com.tw.	7.107	TW	92.201	46.99K
2	NXDomain-Black-List ssl.	.41	TW	92.201	46.8K
3	NXDomain-Black-List ssl.	7.66	TW	92.201	43.67K
4	NXDomain-Black-List bcmlbsqa1@broadcom.com.	00.199	TW	92.201	43.28K
5	NXDomain-Black-List bcmlbsqa1@broadcom.com.	92.43	TW	92.201	42.39K
6	NXDomain-Black-List ssl.	.113	TW	92.201	42.13K
7	NXDomain-Black-List bcmlbsqa1@broadcom.com.	21.151	TW	92.201	41.81K
8	NXDomain-Black-List samsungvuieventlog.vlingo.com.	26.183	TW	92.201	41.13K
9	NXDomain-Black-List lipin.ctrip.cnc.ccgslb.net.	192.191	TW	5.39	32.26K

DNS Amplify – 可以放大28-40倍數的流量

- *主要目的- 消耗頻寬資源*



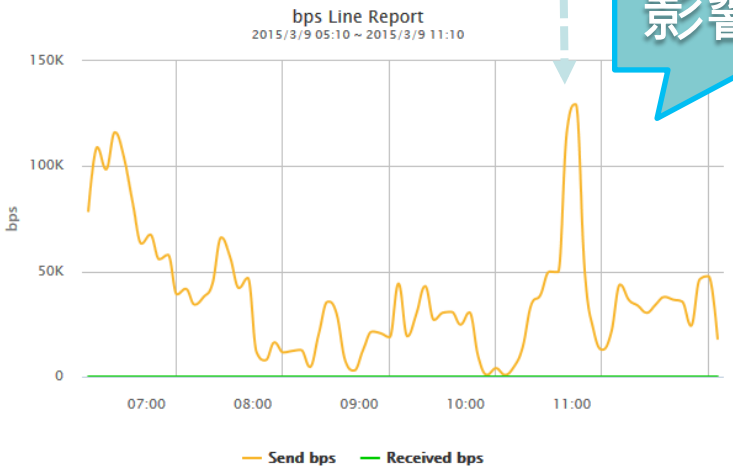
3/9 11:03- 遭受DNS放大攻擊

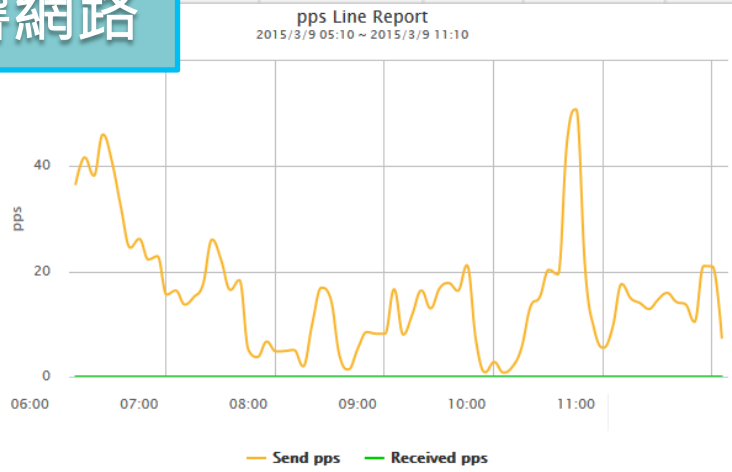


DNS攻擊事件

		來源區域	目的IP	目的Port	目的IP名稱解析	次數
	135	US	223	53	微行社	13,059
	2.189	HK	223	53	微行社	6,965
13019: DNS: DNS ANY Response	71.120.142.229	US	223	53	微行社	6,783
13019: DNS: DNS ANY Response	113.28.163.227	HK	223	53	微行社	4,815
13019: DNS: DNS ANY Response	69.27.199.74	US	223	53	微行社	3,357
13019: DNS: DNS ANY Response	68.41.37.35	US	223	53	微行社	3,122
13019: DNS: DNS ANY Response	63.141.198.179		223	53	微行社	2,633
13019: DNS: DNS ANY Response	113.28.162.147	HK	223	53	微行社	2,006
13019: DNS: DNS ANY Response	63.141.198.217		223	53	微行社	1,801
sponse	104.255.76.117		223	53	微行社	1,136

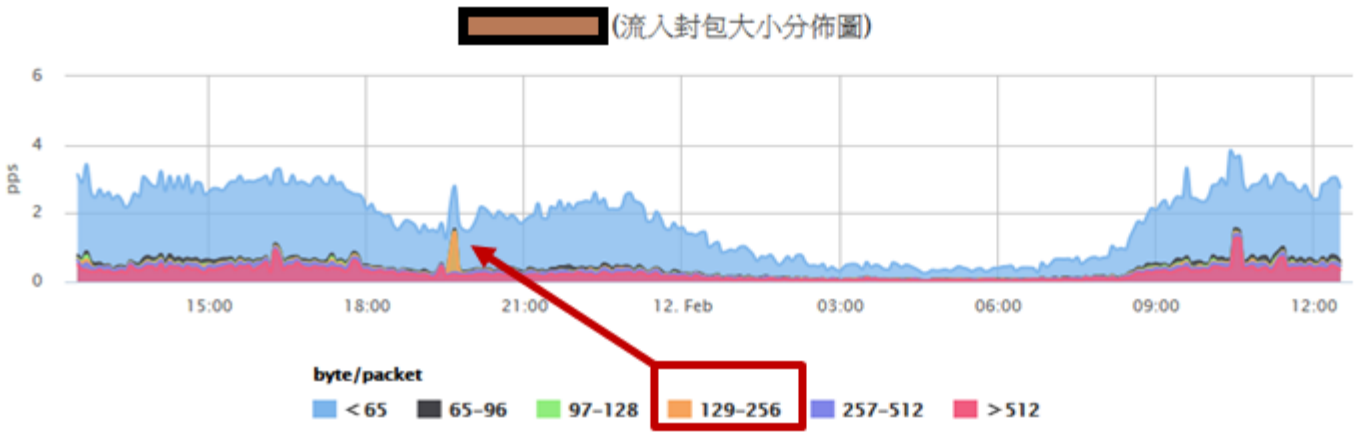
影響網路





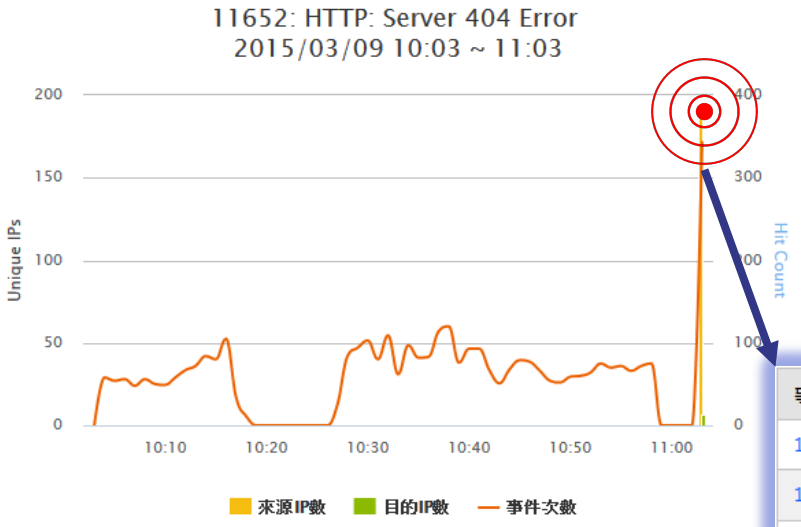
N REPORTER

封包大小異常分析- 掌握服務遭受攻擊的細節



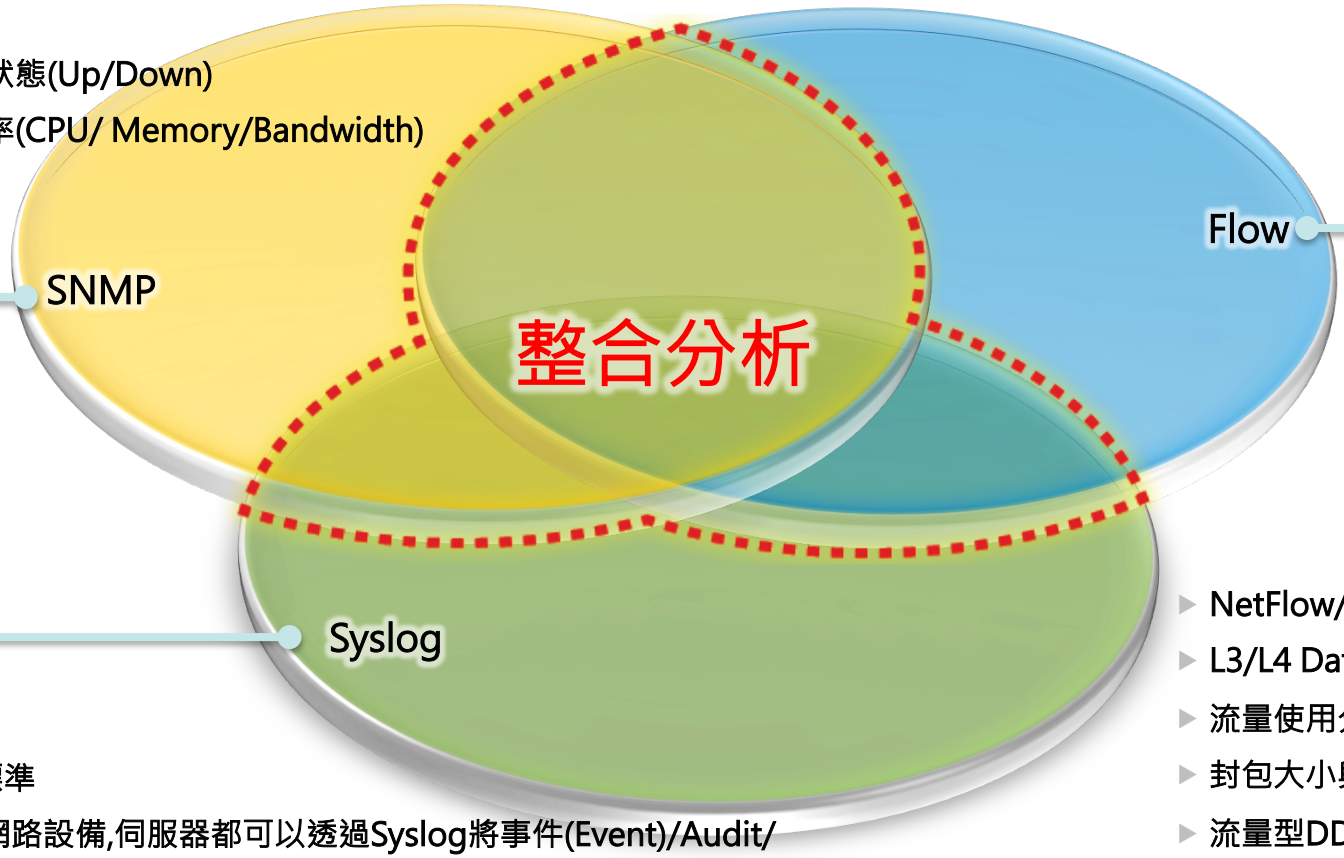
事件	來源IP	來源Port	來源區域	目的IP	目的Port	目的IP名稱解析	次數
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4885	CN	223.	443	旅行社	85
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4885	CN	223.	443	旅行社	79
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	4706	CN	223.	443	旅行社	36
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	4706	CN	223.	443	旅行社	36
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5003	CN	223.	443	旅行社	11
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5003	CN	223.	443	旅行社	11
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5221	CN	223.	443	旅行社	3
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5221	CN	223.	443	旅行社	3
16270: TLS: OpenSSL ChangeCipherSpec Request	121.15.2.177	5112	CN	223.	443	旅行社	2
16538: TCP: OpenSSL ClientHello Message	121.15.2.177	5112	CN	223.	443	旅行社	2

3/9 11:03- 出現爆量Server 404 Error



事件	來源IP	來源區域	目的IP	目的IP名稱解析	次數
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.83	五福旅行社	291
11652: HTTP: Server 404 Error	118.163.159.210	TW	223.26.68.83	五福旅行社	112
11652: HTTP: Server 404 Error	118.163.240.108	TW	223.26.68.83	五福旅行社	38
11652: HTTP: Server 404 Error	220.132.130.176	TW	223.26.68.27	五福旅行社	35
11652: HTTP: Server 404 Error	114.33.36.179	TW	223.26.68.83	五福旅行社	31
11652: HTTP: Server 404 Error	122.116.208.32	TW	223.26.68.83	五福旅行社	31
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.27	五福旅行社	26
11652: HTTP: Server 404 Error	61.222.59.107	TW	223.26.68.83	五福旅行社	26
11652: HTTP: Server 404 Error	61.220.141.217	TW	223.26.68.38	五福旅行社	24
11652: HTTP: Server 404 Error	125.227.123.223	TW	223.26.68.83	五福旅行社	23

善用網路管理三大技術



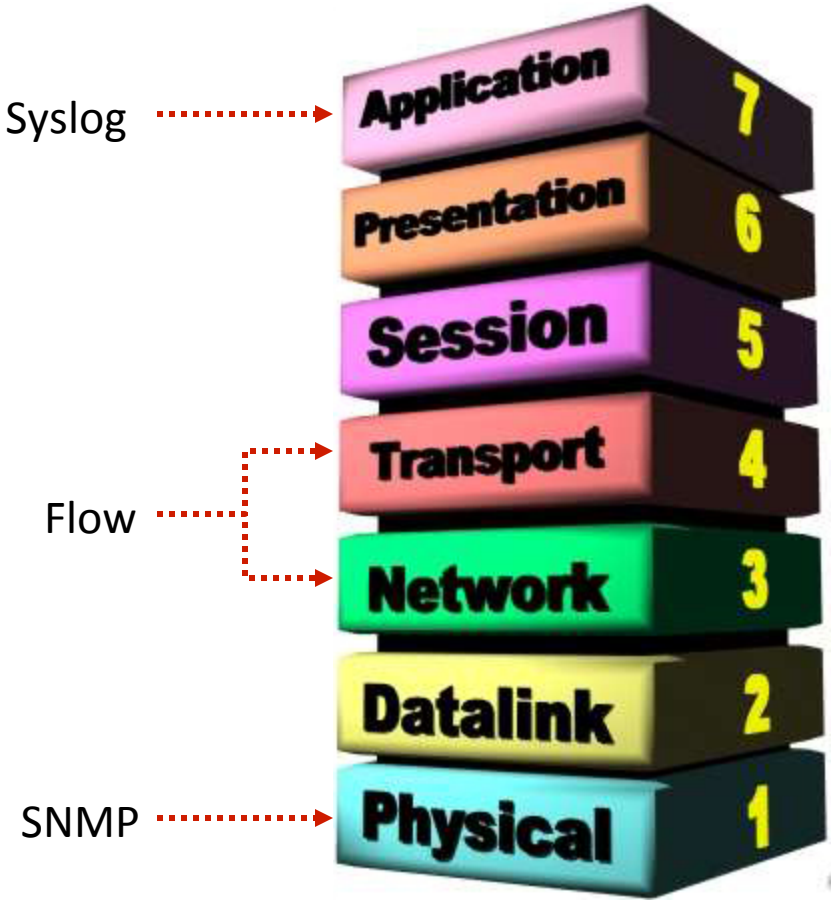
- 設備健康狀態(Up/Down)
- 效能使用率(CPU/ Memory/Bandwidth)
- 資產清單

- NetFlow/sFlow
- L3/L4 Data
- 流量使用分析
- 封包大小與Protocol監控
- 流量型DDoS分析依據
- 能了解量大量小的問題
- 可以繪製流量圖

- 已經成為標準
- 安全產品,網路設備,伺服器都可以透過Syslog將事件(Event)/Audit/ System Log丟出
- 事件(Event) Log記載人的使用行為
- 可以用來分析資安
- L7 (Application Layer) Data

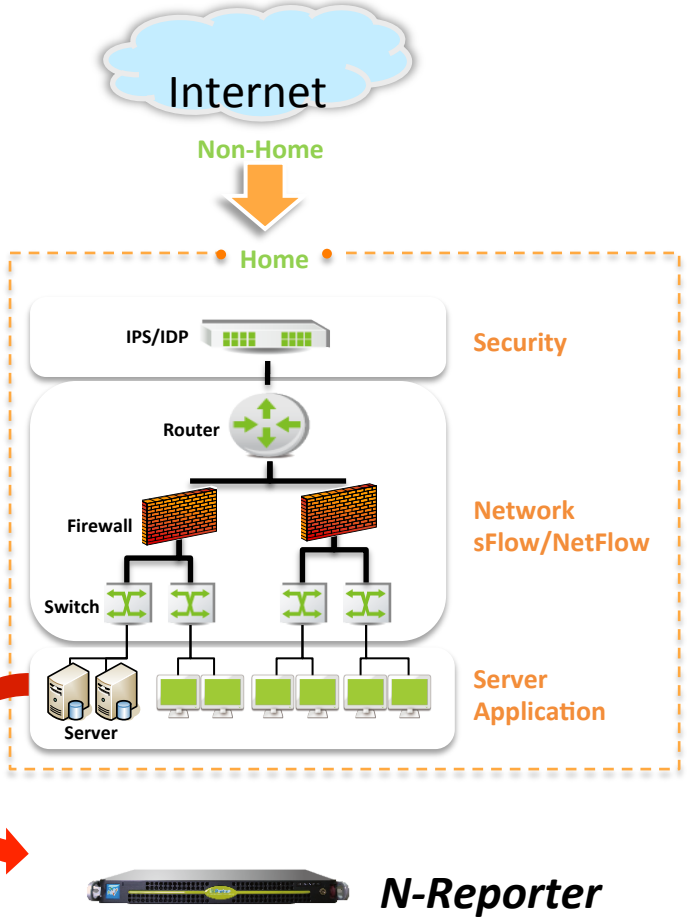
N REPORTER

三大技術的OSI涵蓋領域

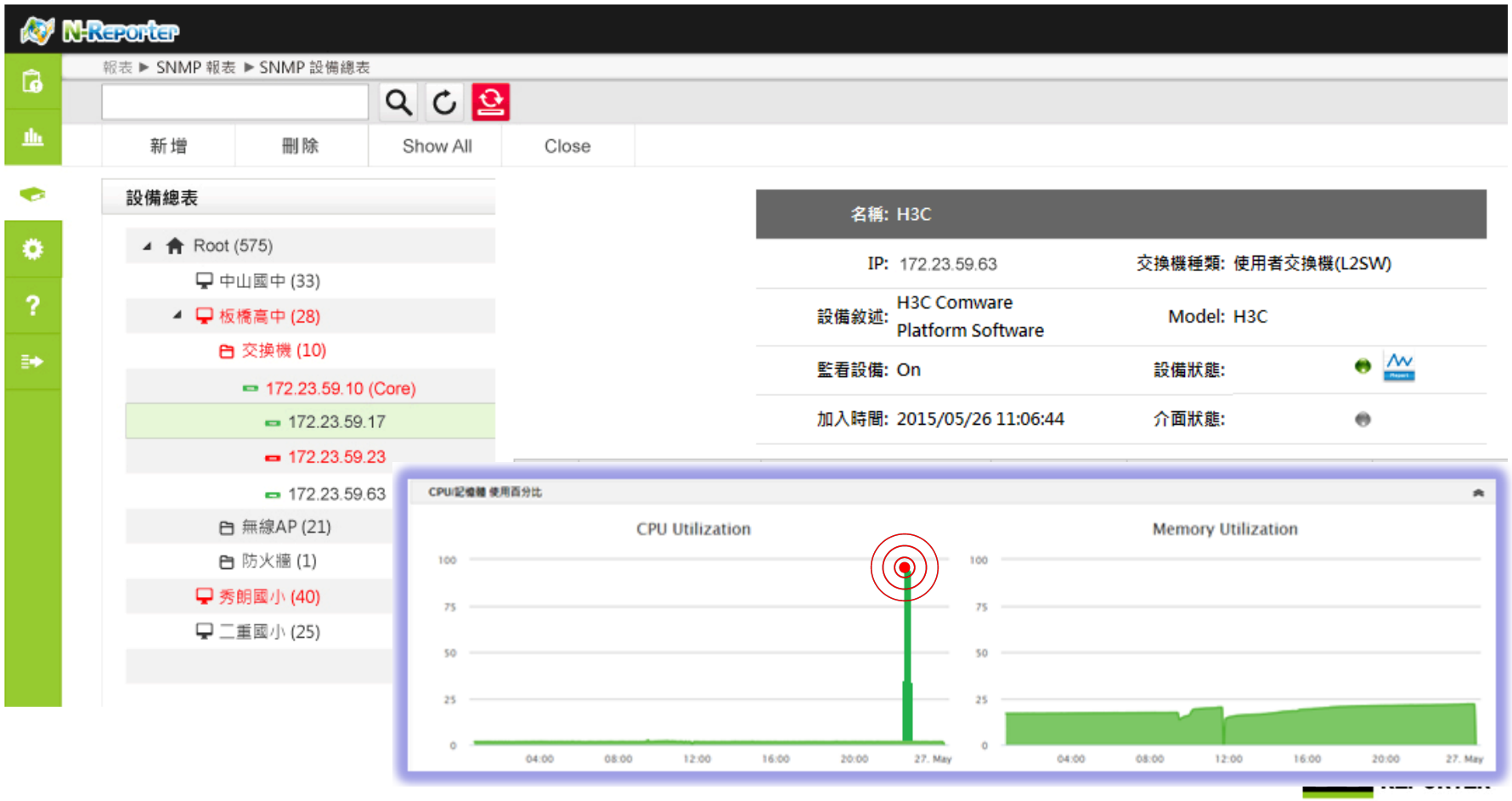


蒐集組織內不同品牌設備的日誌，揮別IT各自除錯舊法

- 整合SNMP, Flow, Syslog
  - ✓ SNMP: Network Device
  - ✓ 資安 Syslog: IPS/IDS, UTM, WAF, NGFW, Wireless
  - ✓ Flow: Netflow(v5/v9)/sFlow/Jflow
  - ✓ Syslog Traffic: Firewall
  - ✓ Server/Application: Web Server(Apache), AD, Database(Oracle, MSSQL), Server(Linux, Mail)…
- 整合于單一管理介面，管理者無須忙碌於多個系統間查詢和人工比對

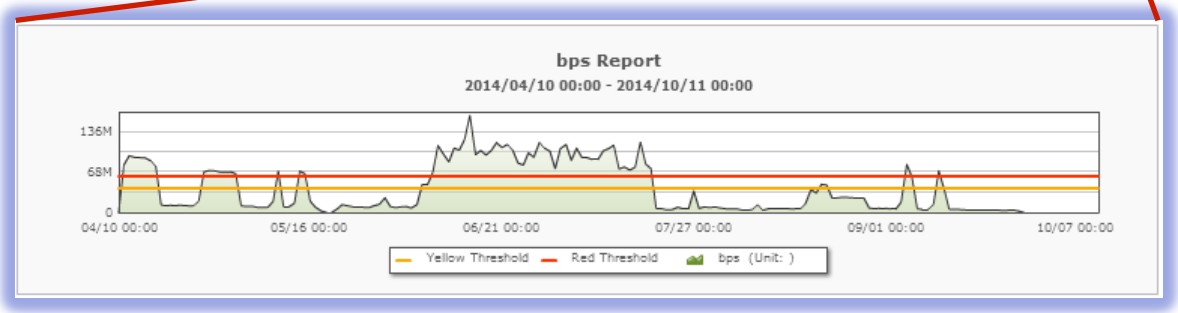


揮別傳統不清晰的拓撲圖,全新設計樹狀收合
一目了然掌握全域設備健康狀態



以人的組織做為流量分析的單位,異常用量即時告警- 優先處理網路品質不良單位

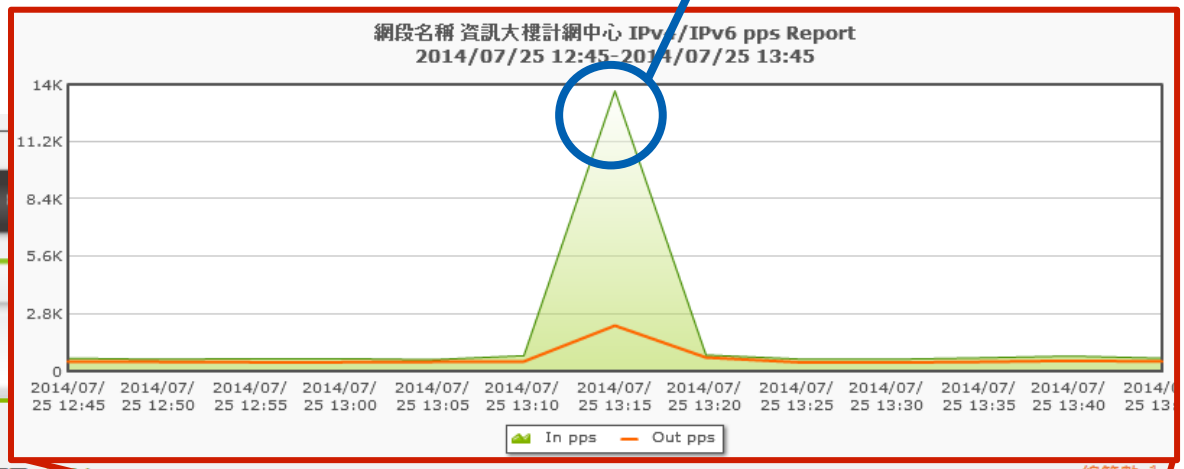
操作	報表名稱	報表製作依據	報表建立時間	最近修改時間	狀態				瀏覽
					Hit Count/S	Session/Se	pps	bps	
	Sales	Flow	2013/12/05 21:26	2013/12/08 01:09		Green	Green	Green	
	TP Office	Flow	2013/12/05 21:26	2013/12/08 01:48		Green	Green	Green	
	Marketing	Flow	2013/08/29 20:36	2013/09/17 09:08		Green	Green	Green	
	IT	Syslog	2013/09/16 16:21	2013/09/16 16:23	Green				
	Manufacture	Flow	2013/09/16 17:23	2013/09/16 22:40		Red	Red	Red	



N REPORTER

單位流量異常告警
即時掌握異常原因

來源IP	來源名稱解析	目的IP	目的名稱解析	Session	Packets	Bytes
[redacted]83.181	E化 Server Form	210.70.162.74	資訊大樓計網中心	3,917,824	3.74M	5.42G
[redacted]83.245	E化 Server Form	210.70.162.21	資訊大樓計網中心	195,584	191K	183.65M
[redacted]0.101	Home	210.70.162.21	資訊大樓計網中心	29,184	28.5K	28.05M
[redacted]83.242	E化 Server Form	210.70.162.21	資訊大樓計網中心	7,168	7K	8.83M



網段流量異常告警

查詢時間區段 ○ 選擇時間區段 7天內 ○ 過去

查詢條件

網段搜尋

First 1 Last 每頁顯示: 50 目前所在頁面: 1 of 1 總筆數: 1

網段名稱	流入量		流出量		告警發生時間	流量圖
	pps	bps	pps	bps		
資訊大樓計網中心	13.36K	149.92M	2.16K	3.2M	2014/07/25 13:15:00	

N REPORTER

不同系統間的關聯性整合

來自Syslog的訊息
提供L7內容

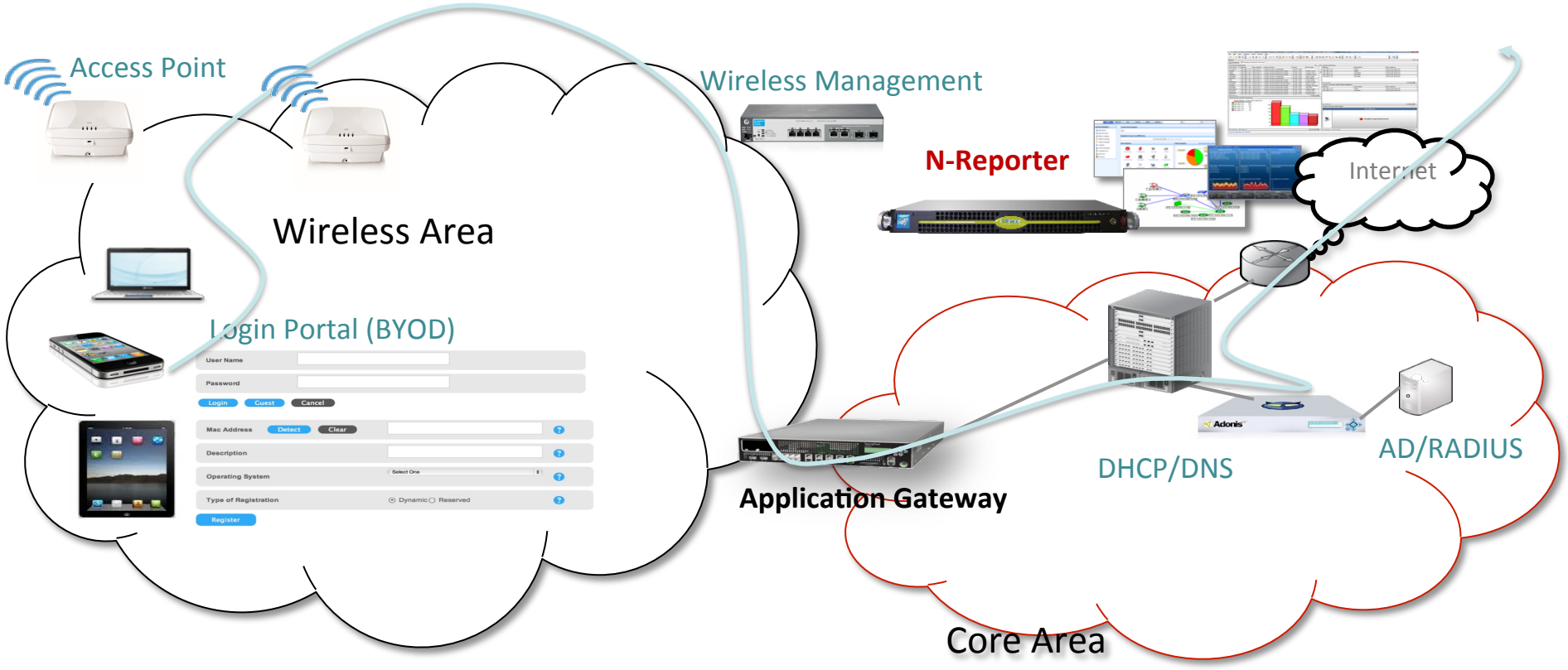
來自AD的訊息
提供使用者名稱

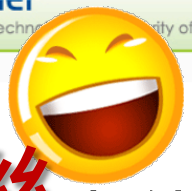
來自Flow的訊息
提供L3/L4用量

事件	次數	來源IP	來源使用者	來源Port	來源區域	目的IP	目的Port	目的區域	Packets	Bytes
C006929: DNS: DNS Query	306	[redacted]1.166	[redacted]d_user9	51378	TW	[redacted]1.1	53	TW	1K	1.44M
C006929: DNS: DNS Query	615	[redacted]1.166	[redacted]d_user9	57299	TW	[redacted]1.1	53	TW	1K	1.46M
C006929: DNS: DNS Query	1	[redacted]1.131	[redacted]d_user8	60890	TW	[redacted]1.1	53	TW	1K	75K
C006929: DNS: DNS Query	6	[redacted]1.131	[redacted]d_user8	53403	TW	[redacted]1.1	53	TW	1K	52K
6924: DNS: NXDOMAIN Response	2	[redacted]1.2	[redacted]d_user2	2523	TW	[redacted]128.30	53	US	1K	40K
6924: DNS: NXDOMAIN Response	3	[redacted]1.2	[redacted]d_user2	20730	TW	[redacted]6.22	53	TW	1K	40K

N REPORTER

N-Reporter與無線網路BYOD應用的結合

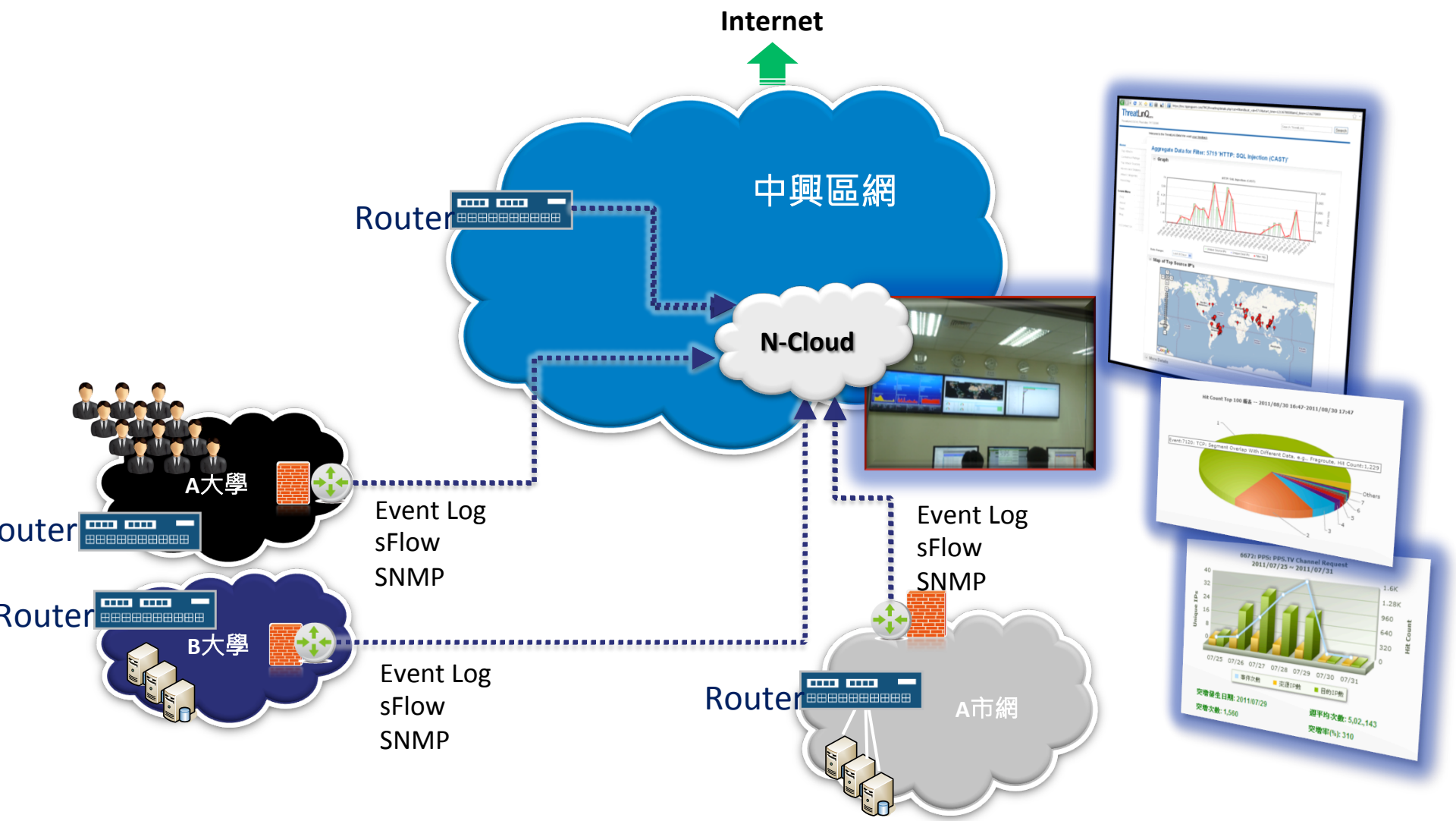




關聯事件,一張表格讓IT人員掌握BYOD的使用情況

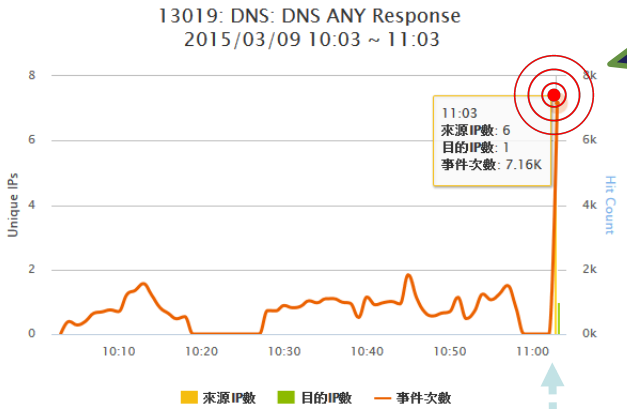
Time	Event	Hit Count	Private SourceIP	Public SourceIP	Username	Source MAC	Location
2012/5/7 21:36	1400: SMB Windows Logon Failure	152	192.168.1.222	210.100.38.101	Robin Shih	00-50-56-C0-00-01	AP-1
2012/5/7 21:44	9991: HTTPS: Google Gmail Access	2	192.168.1.33	210.100.38.101	Sandy Chen	00-50-56-DF-11-1A	AP-1
2012/5/7 21:45			192.168.2.166	210.100.38.102	Ken Yip	00-50-56-62-13-2F	AP-2
2012/5/7 21:52	2270: BitTorrent: Peer-to-Peer Communications	69	192.168.1.33	210.100.38.101	Sandy Chen	00-50-56-DF-11-1A	AP-1
2012/5/7 21:59			192.168.1.45	210.100.38.101	Richard Chou	00-50-56-00-14-B4	AP-1
2012/5/7 22:17	6545: MS-RPC: Microsoft Server Service Buffer Overflow	1	192.168.2.88	210.100.38.102	Peter White	00-50-56-77-11-54	AP-2
2012/5/7 22:22			192.168.1.77	210.100.38.101	Jeremy Lin	00-50-56-DD-30-6A	AP-1
2012/5/7 22:25	5670: HTTP: SQL Injection (SELECT)	17	192.168.2.88	210.100.38.102	Peter White	00-50-56-77-11-54	AP-2

教育維運雲運用-跨校區的資訊搜集



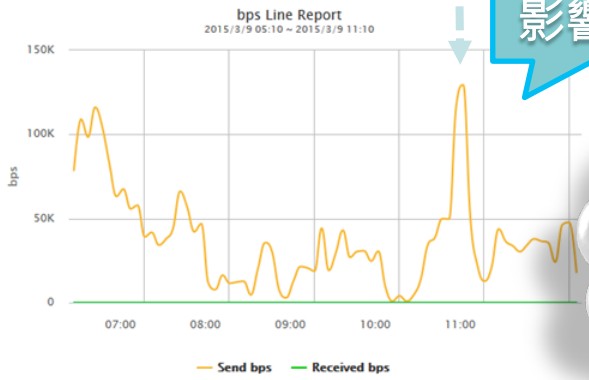
N REPORTER

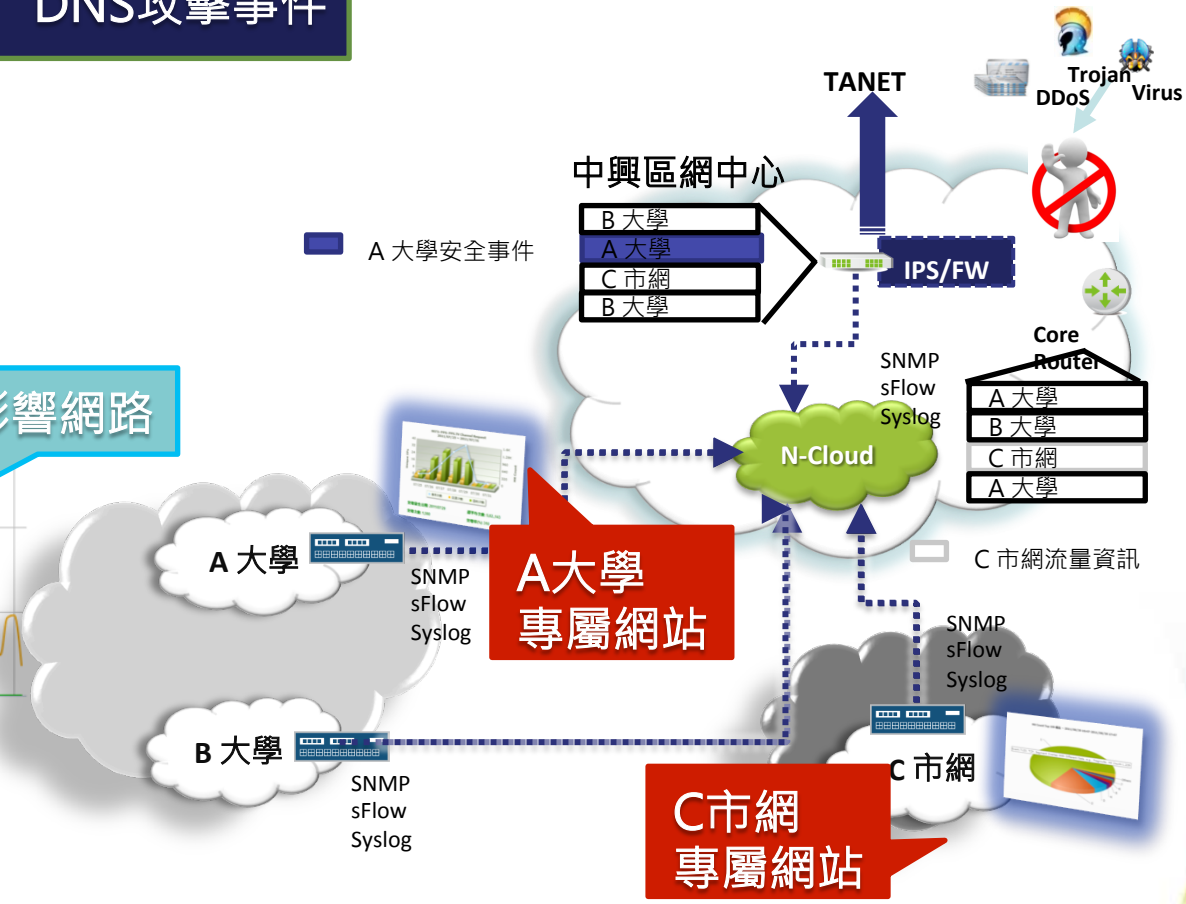
教育資安雲運用-市網中心安全事件與流量分享到各校



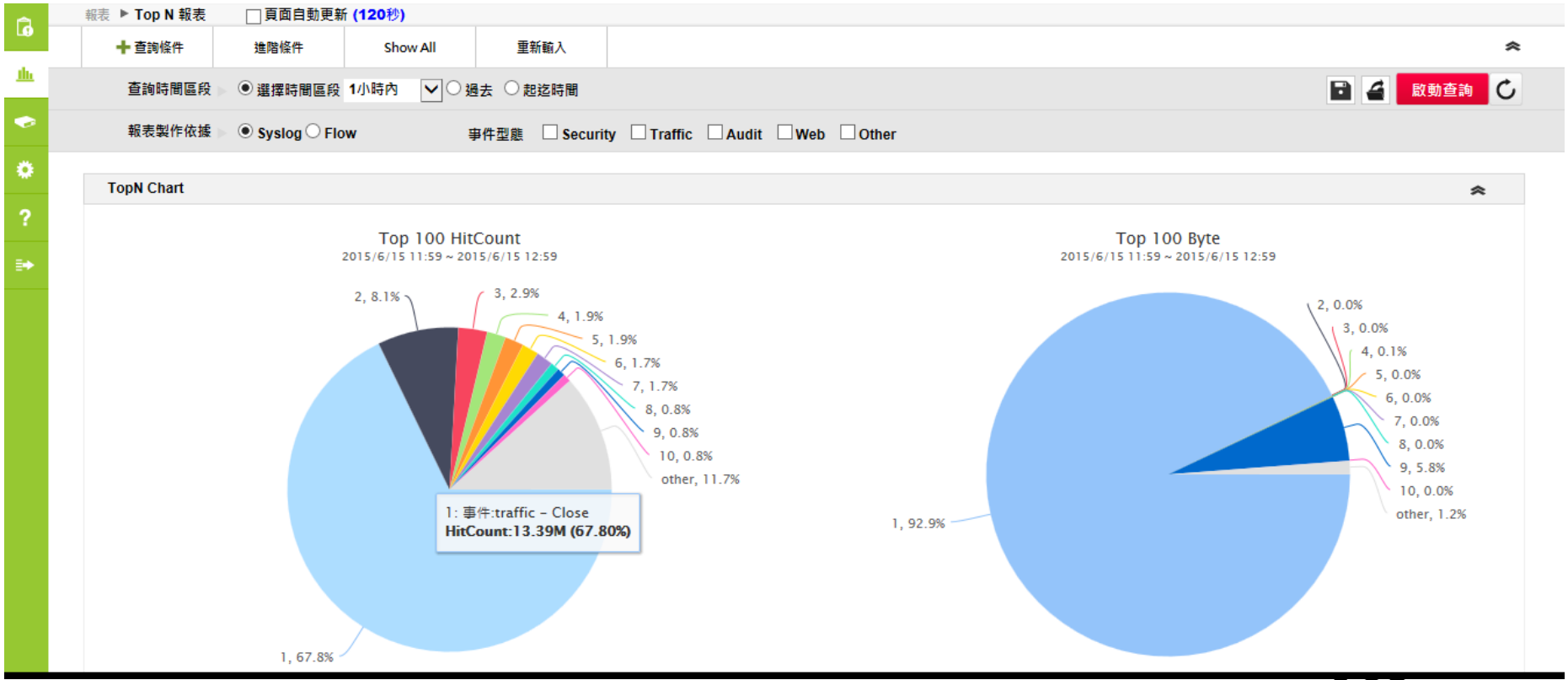
DNS攻擊事件

影響網路





各校擁有自己專屬Portal
擁有完整的查詢,分析,報表製作功能



雲架構分權管理的優點

■中心的管理者

- ■可以查詢所有設備的資安及流量資料
- ■可以製作全網 TOPN 及流量報表
- ■可以查詢特定學校的事件或流量（變身為某學校管理者）
- ■執行全網的聯防，在IPS設定阻擋外部的攻擊，在防火牆設定阻擋內部的異常

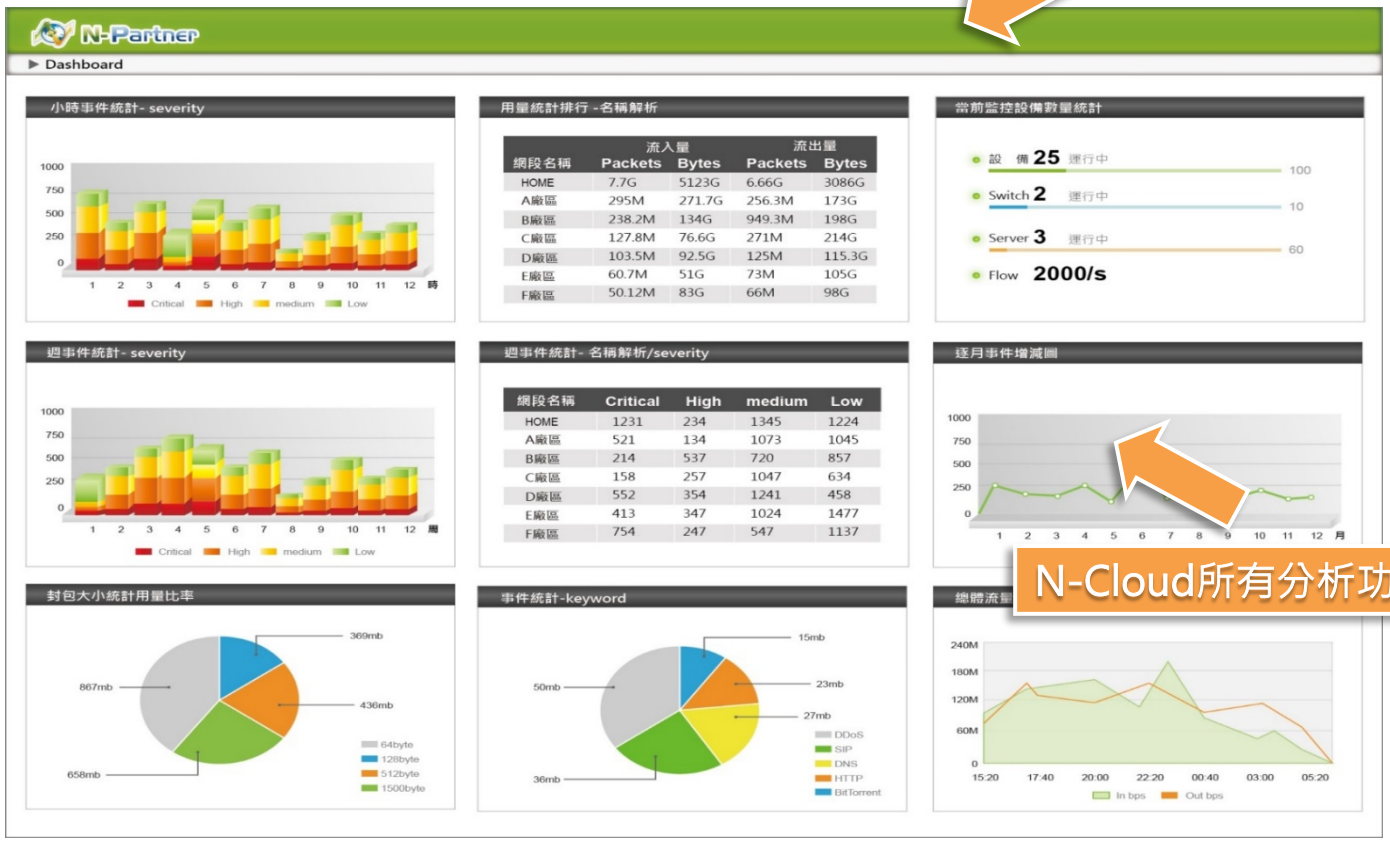
■各學校的管理者

- ■可以查詢學校相關的資安及流量資料（自己學校設備的資料、或中心分配的資料）
- ■各學校可以新增管理各自的設備
- ■製作該學校的TOPN 及流量報表
- ■執行所屬學校的阻擋功能，迅速排除異常(Action 模組的功能）

新一代NOC/SOC教育雲-
High Level觀點,隨時掌握各校狀態

- 專業NOC/SOC等級即時監控畫面
- Drill-Down進階查詢詳細資料內容

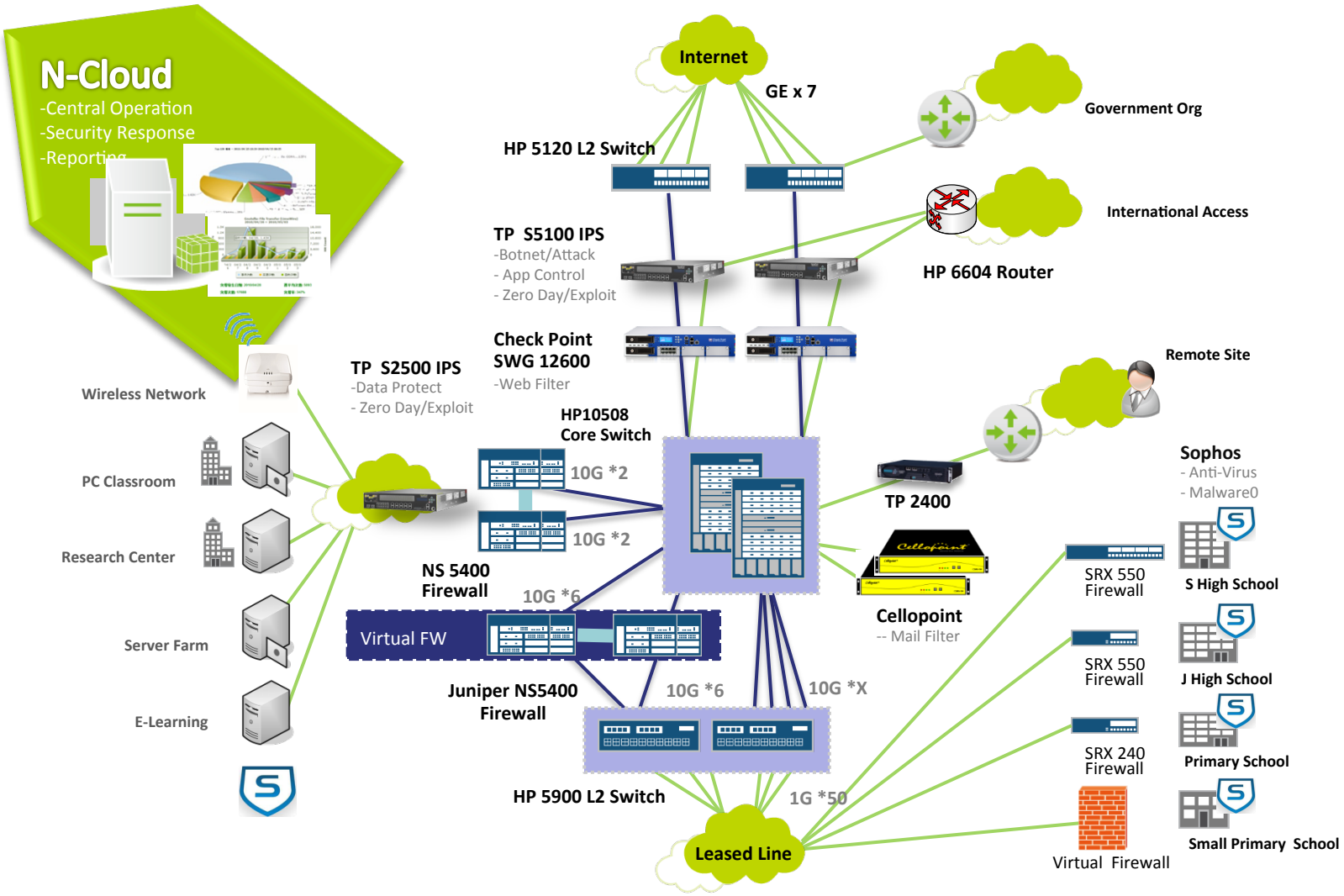
自訂Dashboard呈現窗口



N REPORTER

實際佈署案例

- 背景
  - ✓產業類型: Government/Education Center
  - ✓網路總使用人數: Over 320,000
  - ✓Internet Bandwidth Usage: Over 7Gbps
  - ✓下轄單位數: 1 Center, 400 Schools, 50 Admin Organizations, Server Farm
  - ✓IT管理人員數: Over 500 (Access N-Cloud at the same time)
  - ✓Syslog/Flow設備總數: Over 700
  - ✓Syslog EPS: Up to 40,000 event per second
  - ✓Flow Record: Up to 30,000 record per second
  - ✓ Raw Data儲存要求: At least 5 Years
  - ✓N-Cloud設備總數: 16x1U Servers


N-Cloud
-Central Operation
-Security Response
-Reporting
Internet
GE x 7
Government Org
HP 5120 L2 Switch
International Access
TP S5100 IPS
-Botnet/Attack
- App Control
- Zero Day/Exploit
HP 6604 Router
Check Point
SWG 12600
-Web Filter
Remote Site
TP S2500 IPS
-Data Protect
- Zero Day/Exploit
Wireless Network
HP10508
Core Switch
PC Classroom
10G *2
10G *2
TP 2400
Research Center
NS 5400
Firewall
10G *6
Sophos
- Anti-Virus
- Malware0
Virtual FW
Cellopoint
-- Mail Filter
SRX 550
Firewall
S High School
Server Farm
SRX 550
Firewall
J High School
Juniper NS5400
Firewall
10G *6
10G *X
E-Learning
SRX 240
Firewall
Primary School
HP 5900 L2 Switch
1G *50
Small Primary School
Leased Line
Virtual Firewall

N REPORTER

本案使用N-Cloud所獲得的效益

■讓蒐集與分析全域的建置成本大幅降低

該用戶曾評估如果下轄各校與單位都要建置類似網路與資安維運系統將耗費超過新台幣兩億,而且還無法做到跨校集中監控與分析的需求.本案採購之N-Cloud僅耗資數百萬

■全面提升各校的網路與資安技術能力

採用雲架構與大數據分析引擎為核心的N-Cloud提供了讓數百位管理者同時上線執行查詢與報表製作等所需之高速效能,中心端管理者與學校管理者可以透過相同的分析報表畫面討論與交流

■讓中心端資安與網路設備的訊息傳達到各單位,各單位內的網路情況也傳到中心

全域各種品牌網路與資安設備訊息收容於一個管理中心,中心端可以觀看全域狀態,每個單位都有一個專屬Portal可以查詢屬於自己的事件與流量,而過去中心端設備的資訊非常難即時分享.各校亦可將自己內部的資訊上傳到N-Cloud進行監控與分析,讓中心端協助網路維運

■讓網路維運變得容易,除錯時間大幅縮短

學校原本嚴重的Botnet問題解決不少,網路異常流量發生時都能藉由N-Cloud的智慧型自動分析功能即時掌握.此外,透過聯防機制,發生於校內的封鎖於該校設備,避免影響其他單位,來自外網的則阻擋於最外端的IPS.整體網路品質與穩定度大幅提升