REPORTER 銷售關鍵點

The smartest syslog reporter in the world

學術網路IT安全維運與雲管理-
建構新世代校園網路資安維運平台

石謂龍 Robin Shih

Product Director

rshih@npartnertech.com

+886-935784086

代理商 逸盈科技 | (02)6636-8889 | www.netfos.com.tw

N-Partner

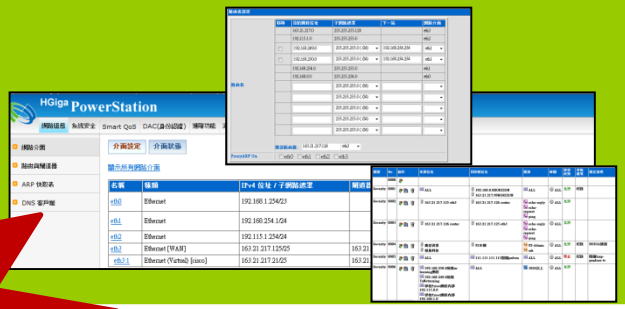
Next Generation Technologies & Security of Network

校園IT維運老師的工作循環與夢魘

報修

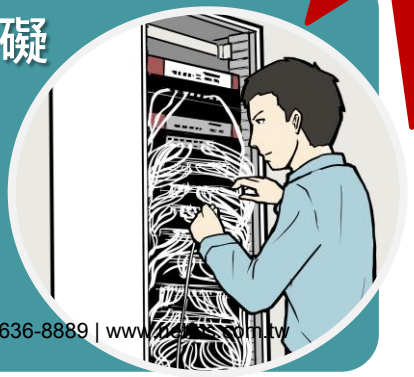
2小時?
3小時?
更久?

蒐集Log資料



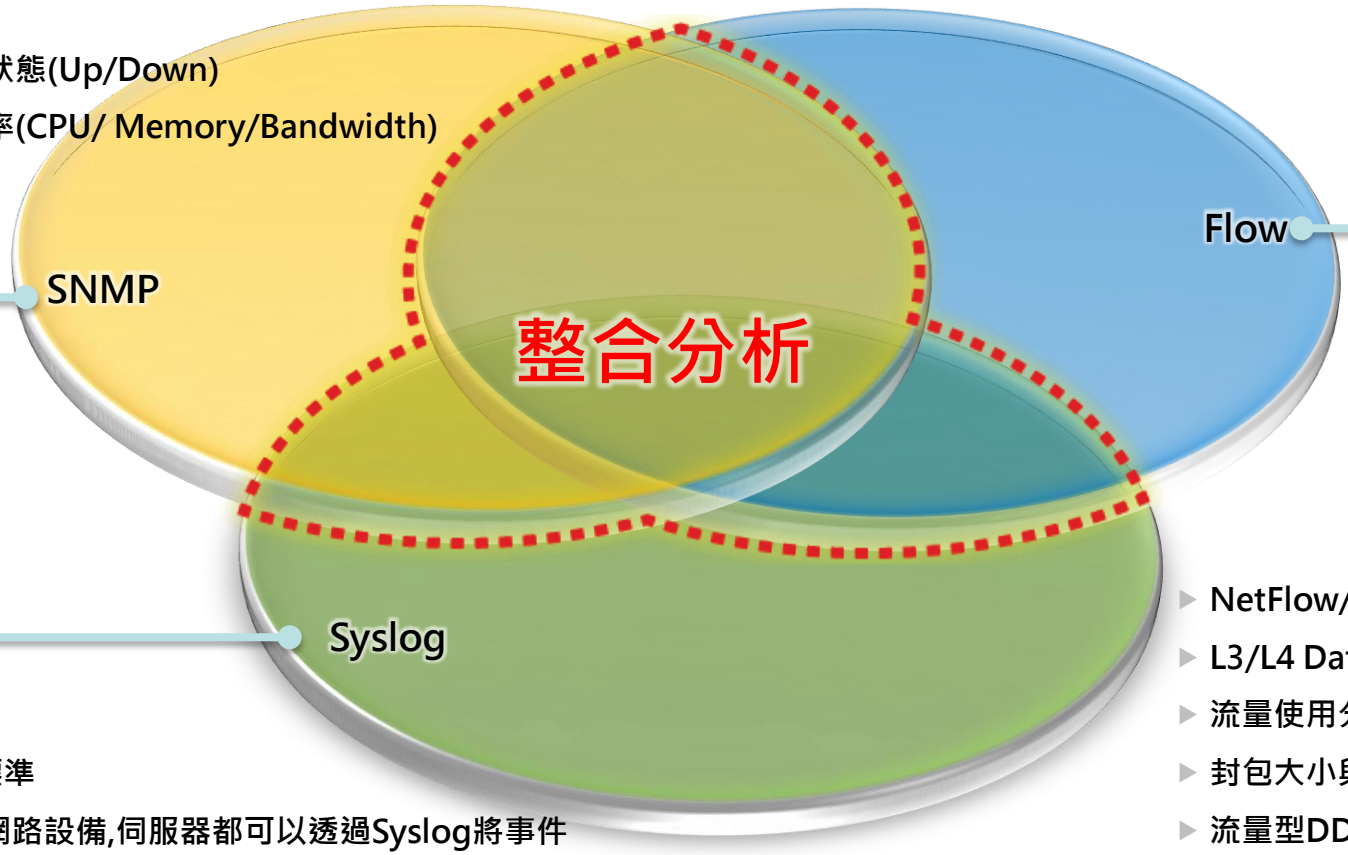
分析障礙根源

處置-消弭障礙



代理商 逸盈科技 | (02)6636-8889 | www.[illegible].com.tw

關鍵在於: 如何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

- 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

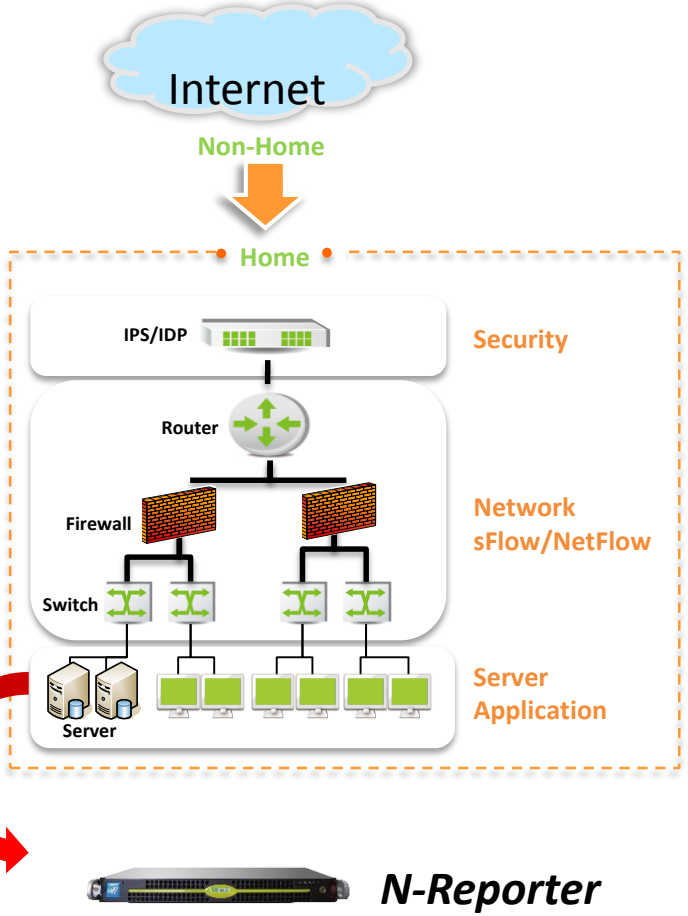
- NetFlow/sFlow
- L3/L4 Data
- 流量使用分析
- 封包大小與Protocol監控
- 流量型DDoS分析依據
- 能了解量大量小的問題
- 可以繪製流量圖

N REPORTER

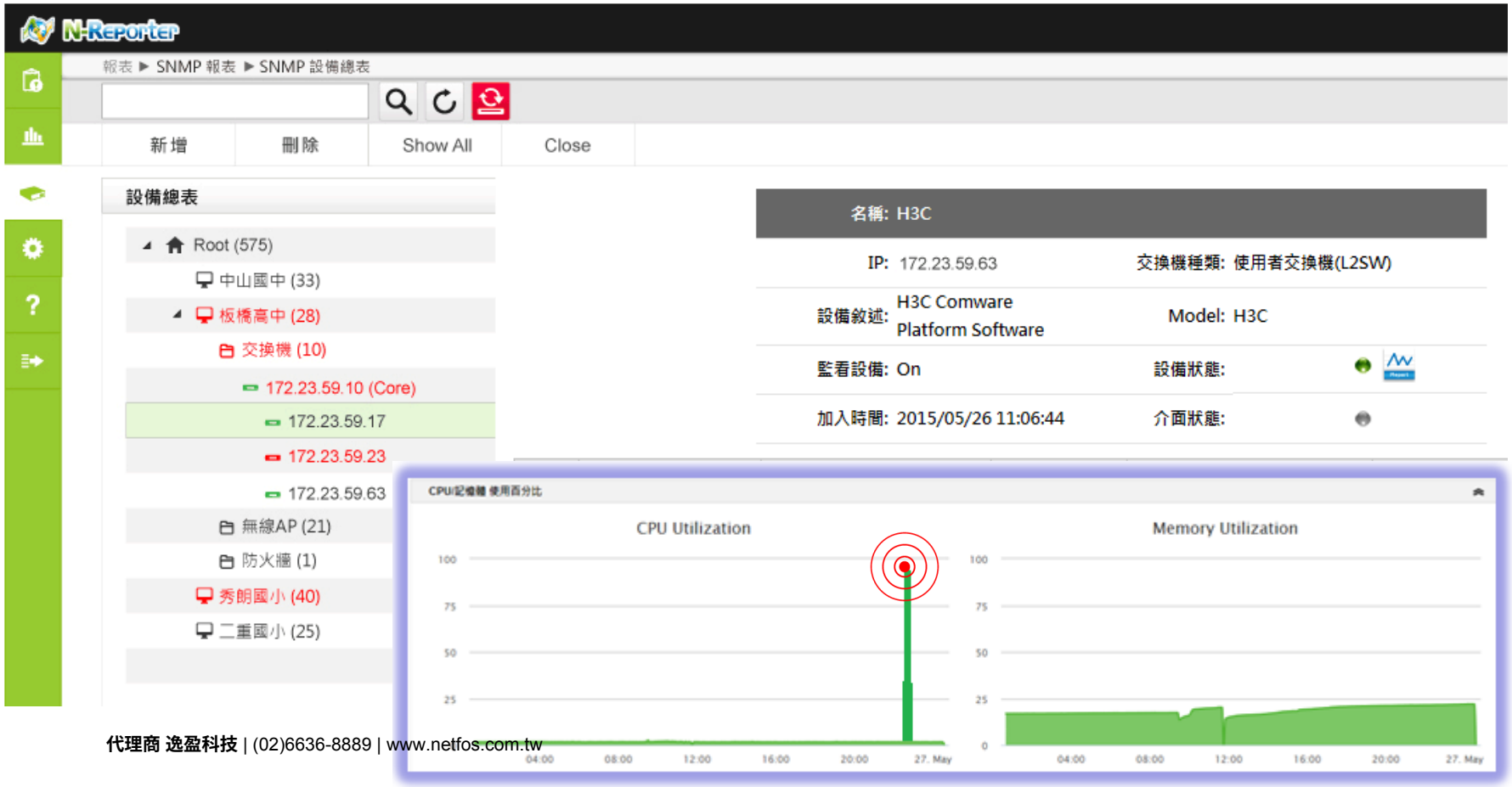
蒐集學校不同品牌設備的訊息，揮別IT各自除錯舊法

- 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

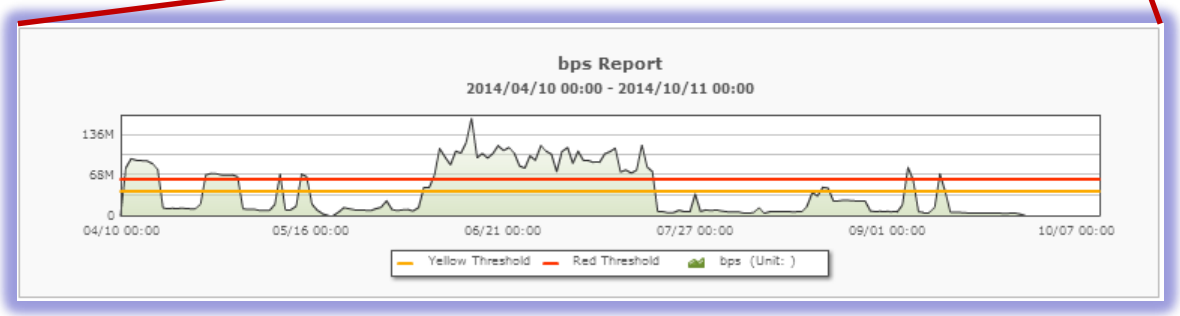


揮別傳統不清晰的拓墣圖,全新設計樹狀收合
一目了然掌握全域設備健康狀態



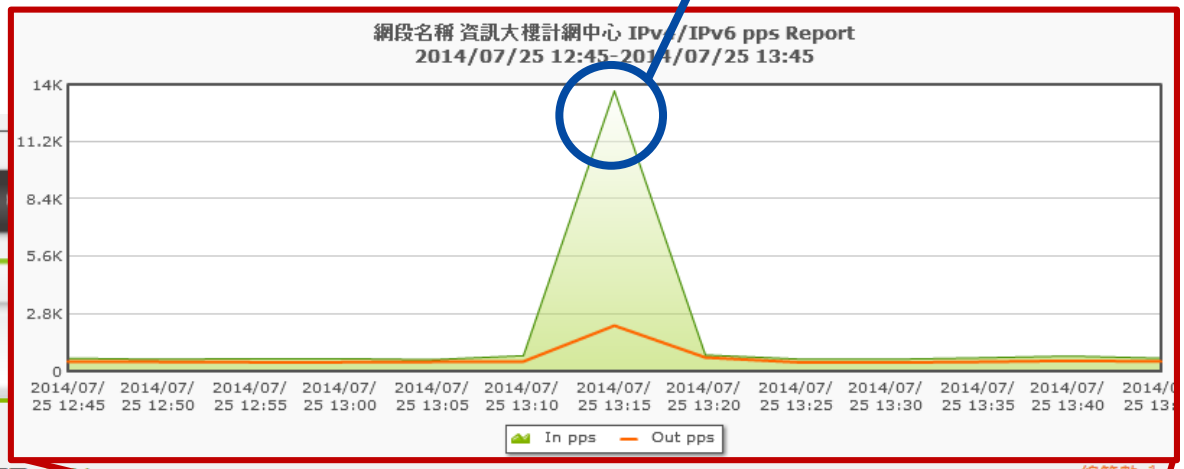
以人的組織做為流量分析的單位,異常用量即時告警- 優先處理網路品質不良單位

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	



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
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
83.245	E化 Server Form	210.70.162.21	資訊大樓計網中心	195,584	191K	183.65M
0.101	Home	210.70.162.21	資訊大樓計網中心	29,184	28.5K	28.05M
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

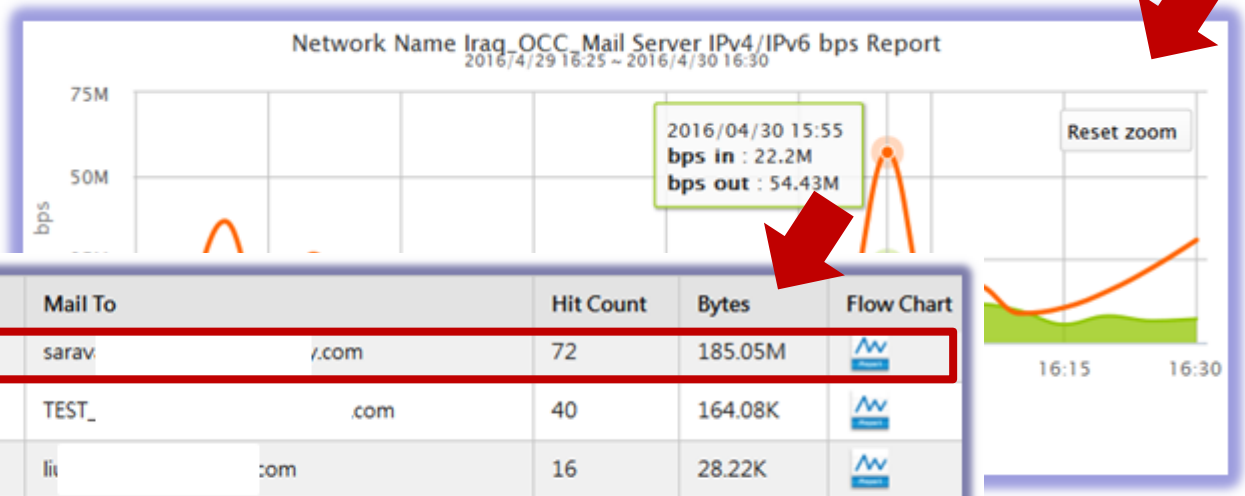
網段搜尋

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	

人工智慧的案例- 大宗郵件寄送即時告警

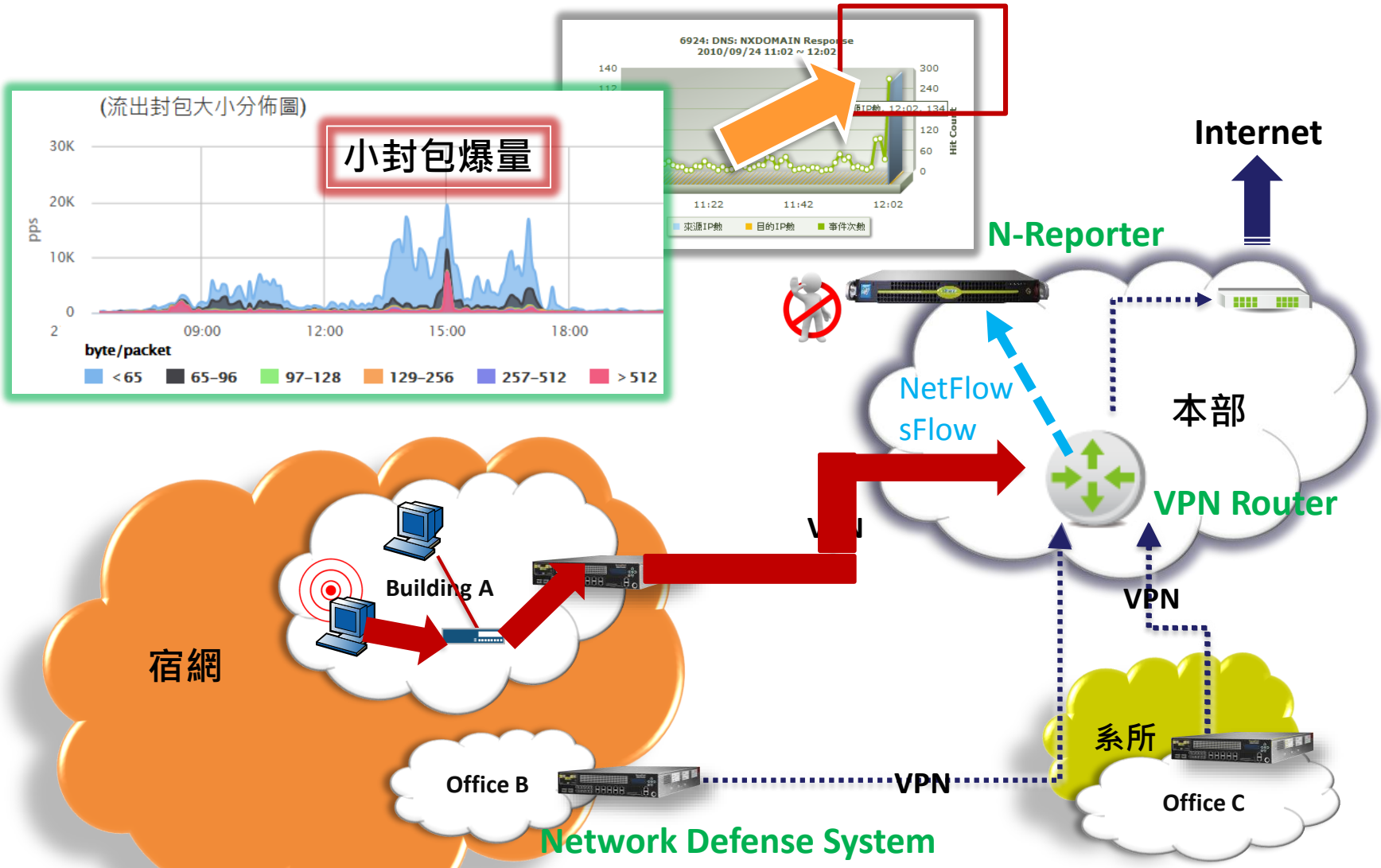
Mapping Name	Volume of traffic in			Volume of traffic out			Alert Time	Flow
	Session/sec	pps	bps	Session/sec	pps	bps		
in_Controller	206.07	5.28K	3.59M	207.36	7.15K	77.93M	2016/04/30 15:55:00	
Mail Server	1.38K	5.64K	22.2M	1.92K	5.42K	54.43M	2016/04/30 15:55:00	
I_DNS Server	28.39	4.67K	2.22M	19.15	6.39K	73.34M	2016/04/30 15:55:00	
ouse Office Area	7.39							
ireless	0.35							
ffice area	18.92							
Wireless System Guest	1.38K							
Office Network System	25.22K							
Room308	3.65							



NO.	Mail From	Mail To	Hit Count	Bytes	Flow Chart
2	mai com	sarav .com	72	185.05M	
3	mo .com	TEST_ .com	40	164.08K	
4	liuli com	li com	16	28.22K	
5	gac om	g .com	16	39.13K	
6	hait y.com	A y.com	12	182.01M	
7	fc.d y.com	jc com	10	93.83K	
8	selv om	s .com	10	2.35M	
9	joh .com	mus .com	8	1.88M	
10	ps_ .com	tri .com	8	8.33M	

代理商 逸盈科技 | (02)6636-8889 | www.netfos.com.tw

自我療癒網路運作流程

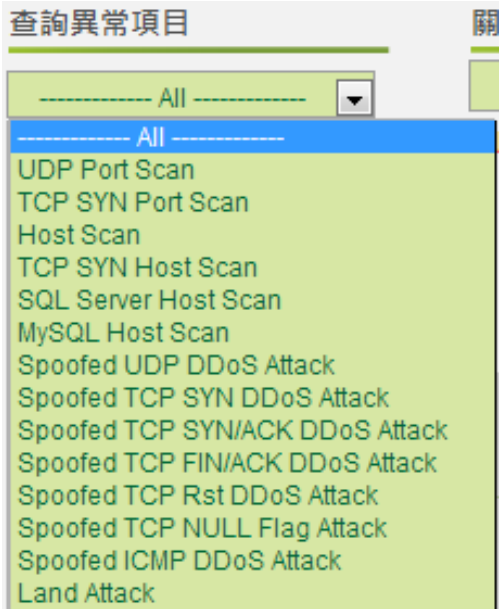

(流出封包大小分佈圖)
小封包爆量
30K
20K
10K
0
pps
09:00
12:00
15:00
18:00
byte/packet
<65
65-96
97-128
129-256
257-512
>512
6924: DNS: NXDOMAIN Response
2010/09/24 11:02 ~ 12:02
140
300
240
120
60
0
Hit Count
11:22
11:42
12:02
來源IP數
目的IP數
事件次數
Internet
N-Reporter
NetFlow
sFlow
本部
VPN Router
VPN
Building A
宿網
Office B
VPN
系所
Office C
Network Defense System

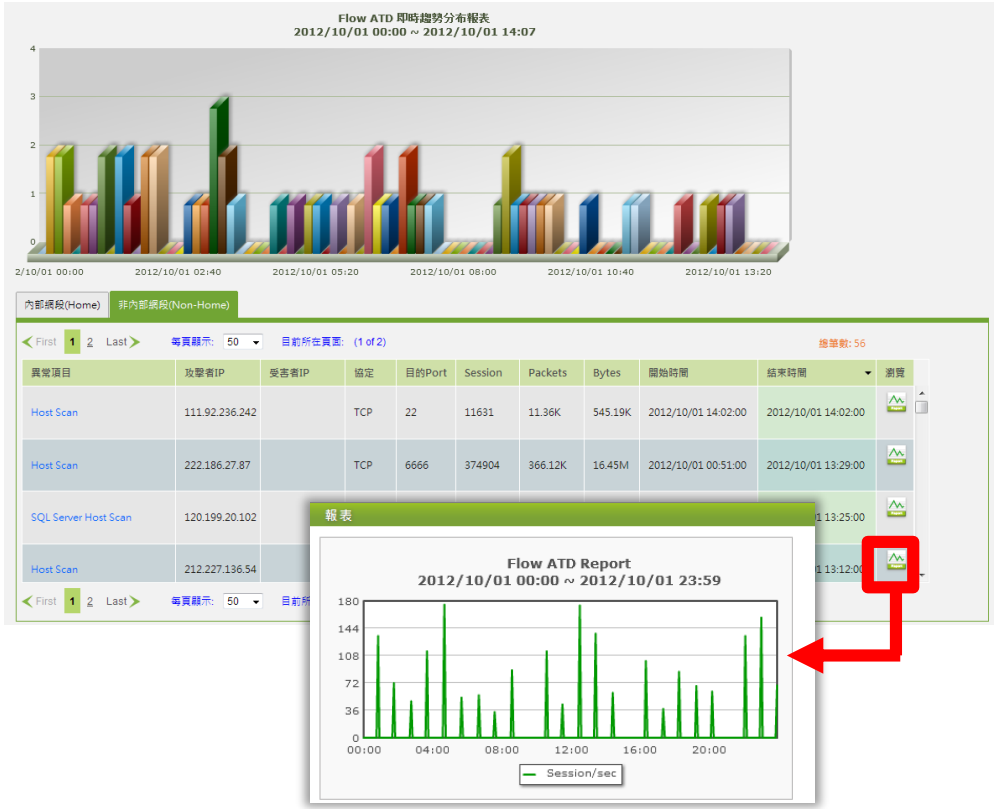
封包大小異常分析- 掌握服務遭受攻擊的細節

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

FLOW即時分析是防禦流量型DDOS攻擊的利器

- 內建多種DDoS分析演算法,根據NetFlow/sFlow資料即時並主動發掘DDoS攻擊



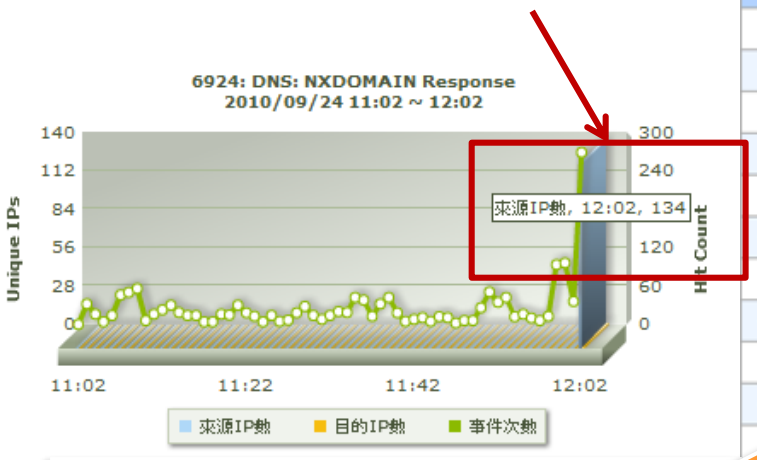


N REPORTER

實例說明 (DNS Server遭DDoS癱瘓)

巨量DNS詢問請求→FW/DNS無法負荷→Internet網路緩慢

(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: N	220.167.29.243	CN	.126.1	domain(53)	2
6924: DNS: N	220.167.29.239	CN	.126.1	domain(53)	2
6924: DNS: N	61.233.154.42	CN	.126.1	domain(53)	2
6924: DNS: N	218.85.152.21	CN	.126.1	domain(53)	2
6924: DNS: N	218.85.157.74	CN	.126.1	domain(53)	2
6924: DNS: N	80.190.211.10	DE	.126.1	domain(53)	2
6924: DNS: N	62.146.0.10	DE	.126.1	domain(53)	2
6924: DN	212.123.96.110	DE	.126.1	domain(53)	2
XDOMAIN Response	200.107.10.62	EC	.126.1	domain(53)	2
DNS: NXDOMAIN Response	80.12.204.167	FR	.126.1	domain(53)	2

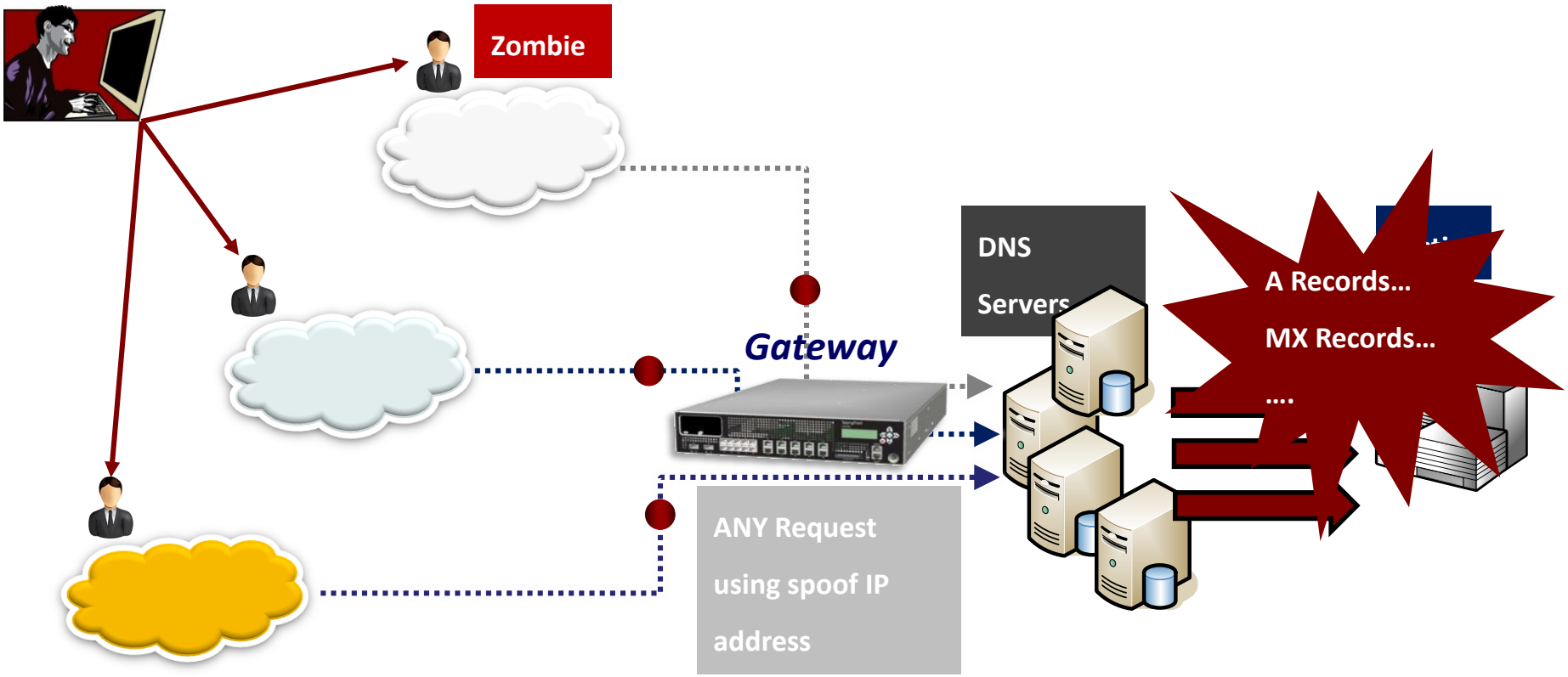
智利

- 分項統計
- 條件加入此事件
- 條件排除此事件
- 加入來源IP
- 排除來源IP
- 加入目的IP
- 排除目的IP
- 阻擋來源IP
- 阻擋目的IP

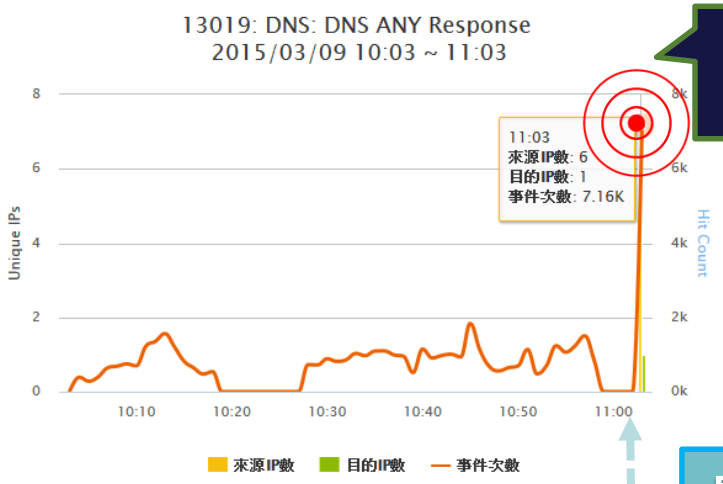
Action模組可搭配合作品牌
網路設備執行阻擋IP設定

DNS Amplify – 可以放大28-40倍數的流量

- *主要目的- 消耗頻寬資源*



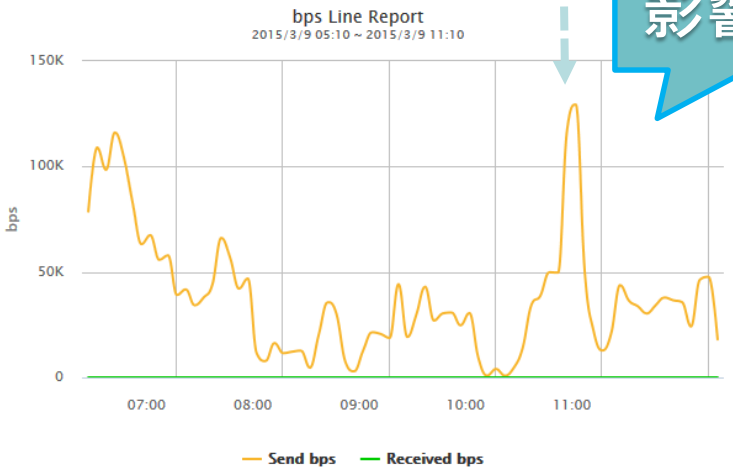
3/9 11:03- 遭受DNS放大攻擊

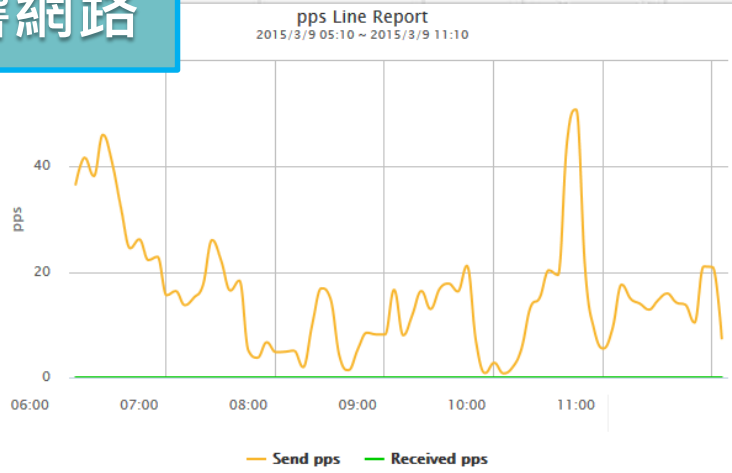


DNS攻擊事件

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

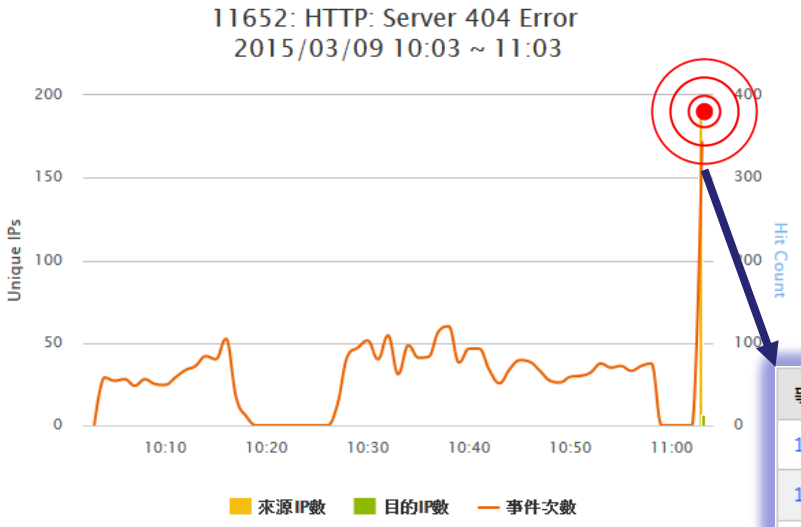
影響網路





N REPORTER

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

不同系統間的關聯性整合案例

Get these data from DNS

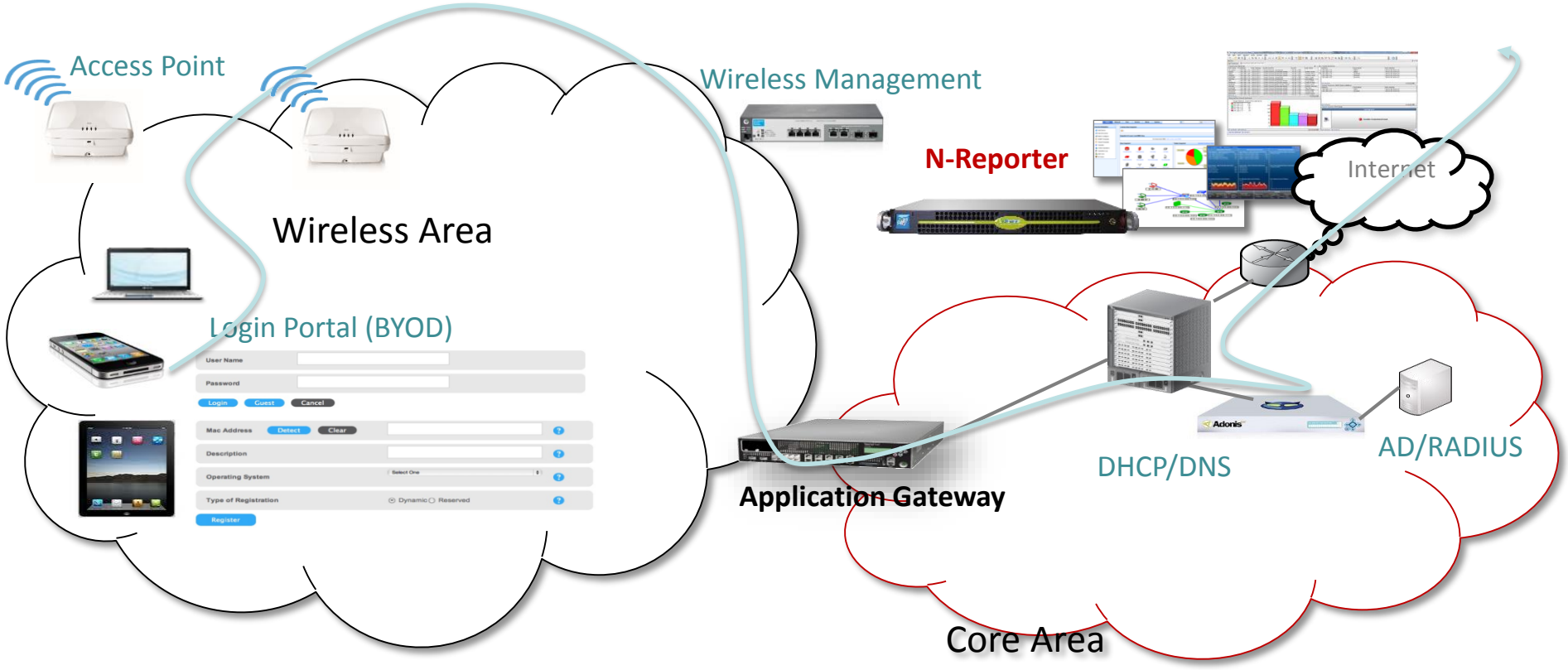
Get these data from AD

Get these data from DHCP

Query via SNMP

Event	Src IP	Src User	Source MAC	Src Host Name	SrcIP Switch/Port
nexus.officeapps.live.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CAI[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
dnl-09.geo.kaspersky.com	172.102.0.13	c[redacted]	60:67:20:17:75:E4	ED-CAI[redacted].local	NB-[redacted]/Gi0/48, S5752-F...
content.cdn.viber.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.msftncsi.com	10.163.17.76	s[redacted]na	2C:27:D7:20:A6:40	HFO-C[redacted] hfy.local	CPF[redacted]Gi0/4, CPF1-PR...
crl.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...
www.microsoft.com	172.102.8.29	h[redacted]	6C:3B:E5:1F:5C:75	DPHP8[redacted]local	NB-[redacted]Gi0/48, S5752-F...

N-Reporter與無線網路BYOD應用的結合

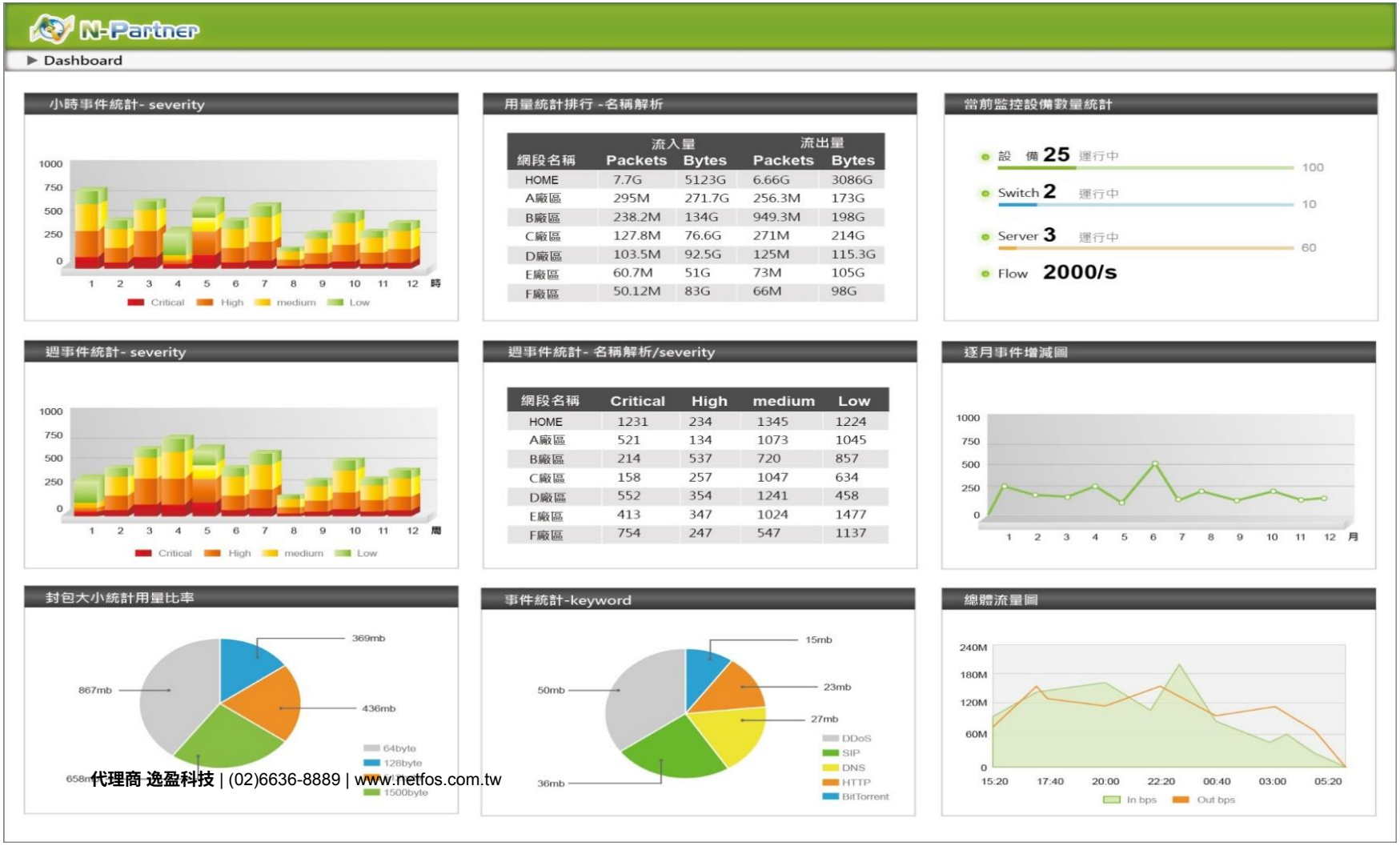


關聯事件,一張表格讓IT人員掌握BYOD的使用情況

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

N-Reporter是新一代智慧IT營運平臺

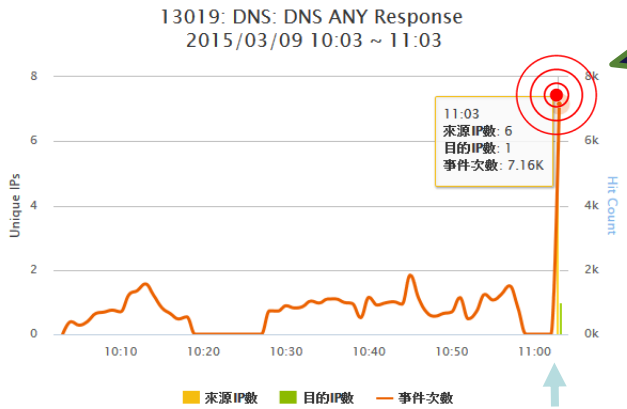
-IT系統與網路狀態一目了然



大數據分析技術的運用
+
雲時代的來臨

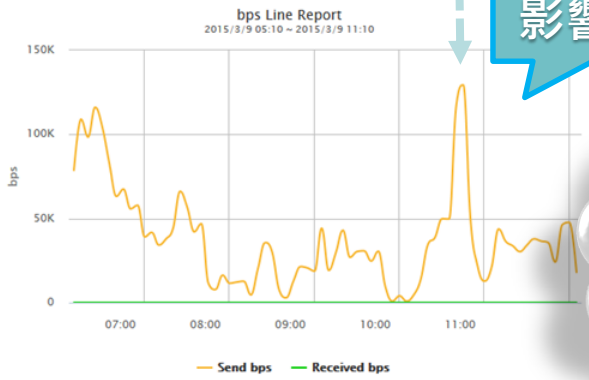
創建校園新一代網路與資安維運雲平台

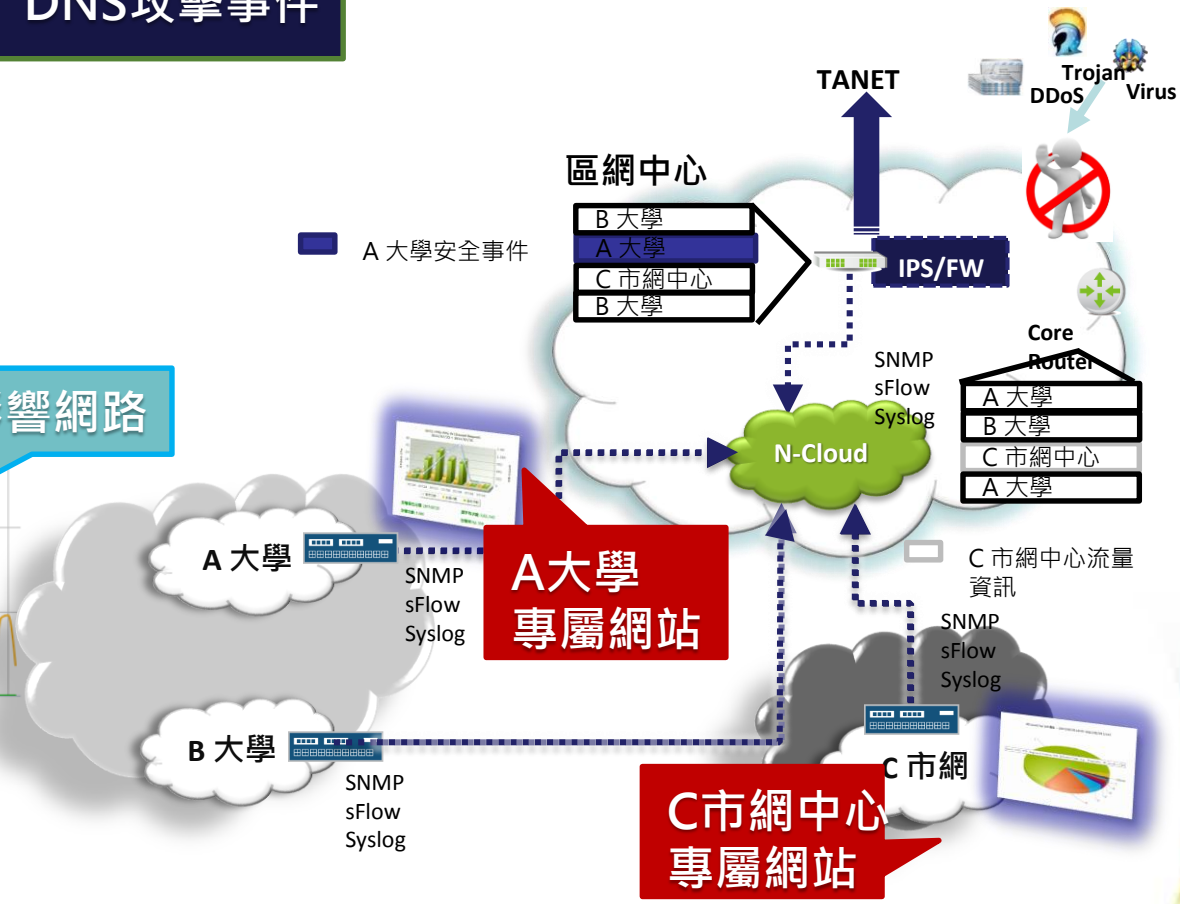
教育資安雲運用-區網中心安全事件與流量分享到各校



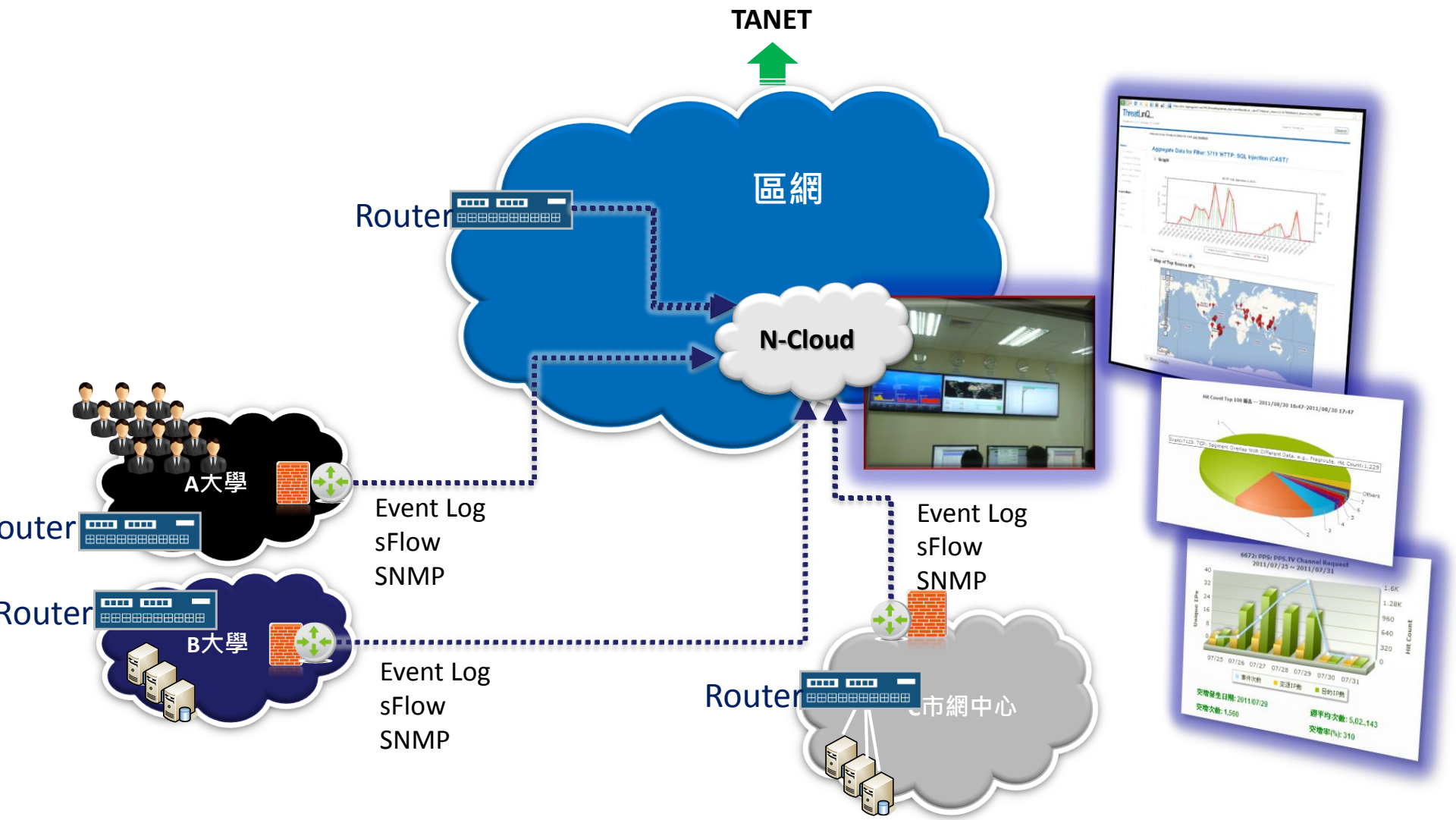
DNS攻擊事件

影響網路





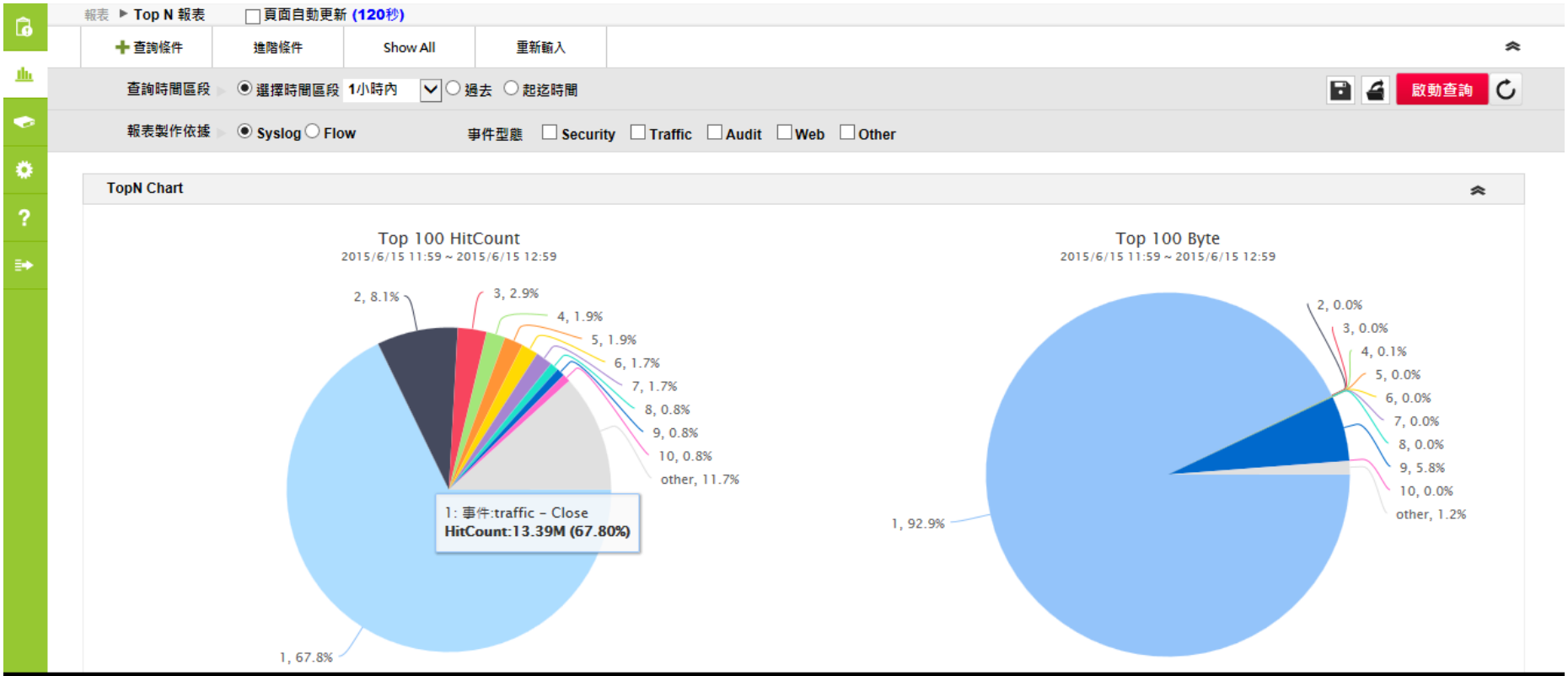
教育資安雲運用-跨校區的資訊搜集



N REPORTER

各校擁有自己專屬Portal

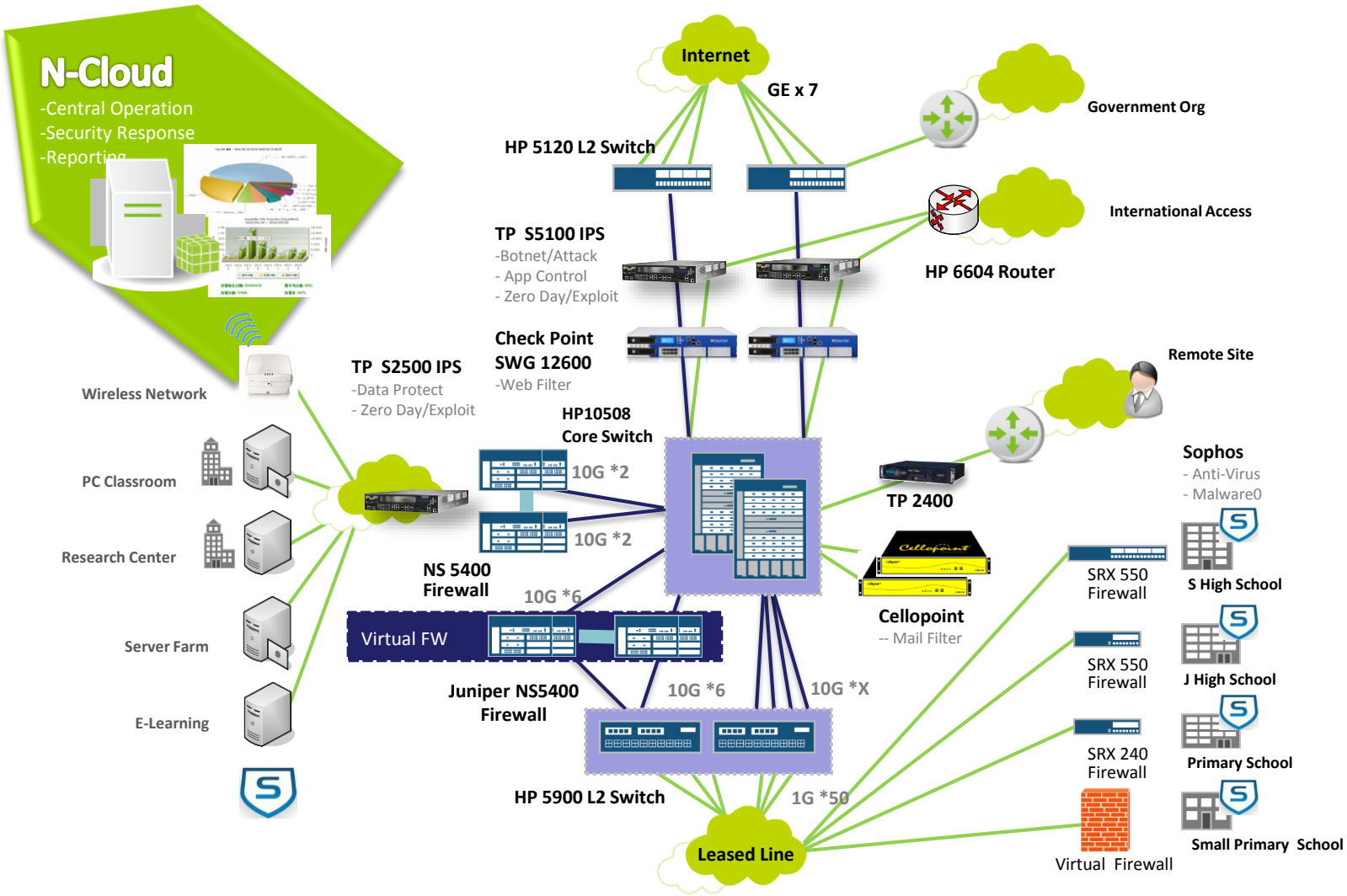
擁有完整的查詢,分析,報表製作功能



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
Sophos
- Anti-Virus
- Malware0
Research Center
NS 5400
Firewall
10G *6
Cellopoint
-- Mail Filter
SRX 550
Firewall
S High School
Server Farm
Virtual FW
SRX 550
Firewall
J High School
E-Learning
Juniper NS5400
Firewall
10G *6
10G *X
SRX 240
Firewall
Primary School
HP 5900 L2 Switch
1G *50
Small Primary School
Leased Line
Virtual Firewall

N REPORTER

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）

教育雲使用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

某市網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.而採用之N-Cloud僅耗資數百萬,卻得到更好的成果

■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

Thanks for your coming!

石謂龍 Robin Shih
Product Director
rshih@npartnertech.com
+886-935784086