

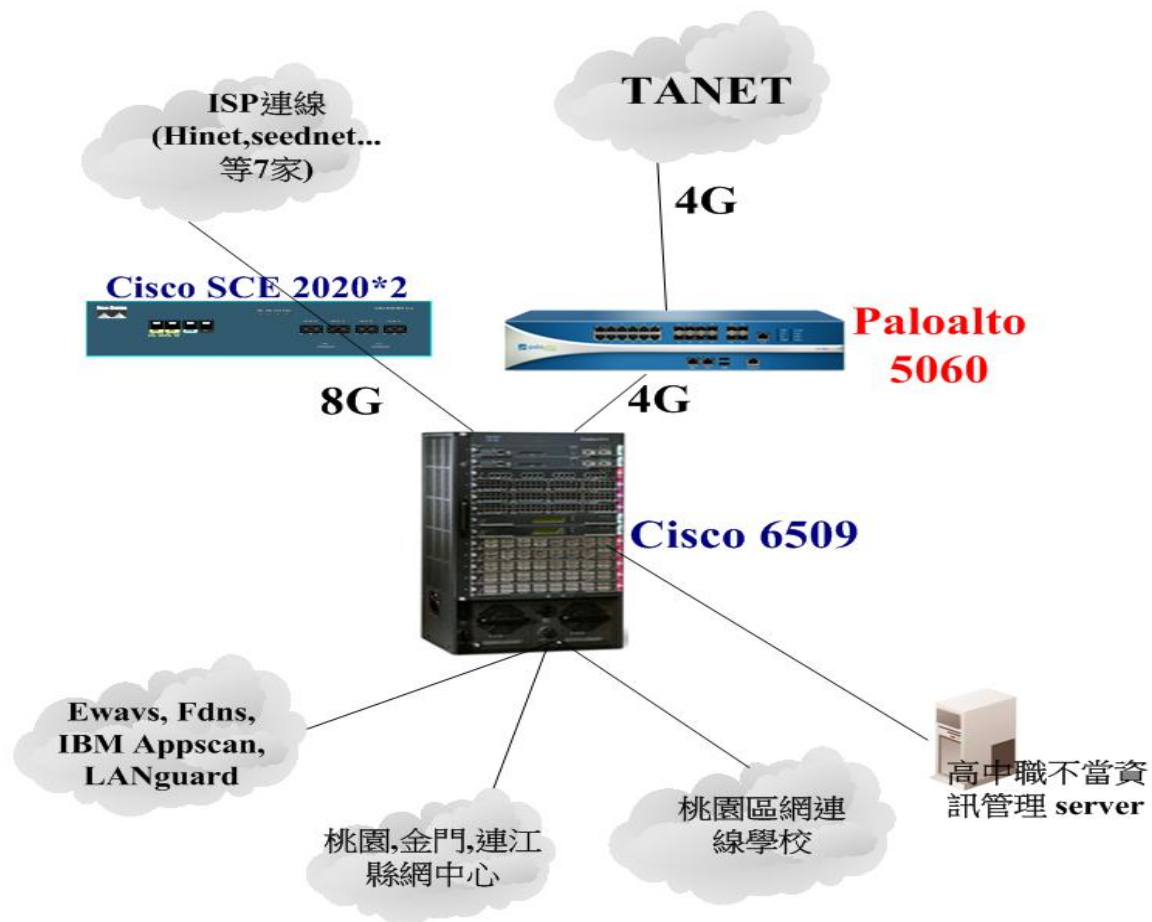


桃園區網頻寬管理說明

電算中心呂芳發
2013年4月



架構





目前設定組態

☐ In-line mode

☐ Ip群組:

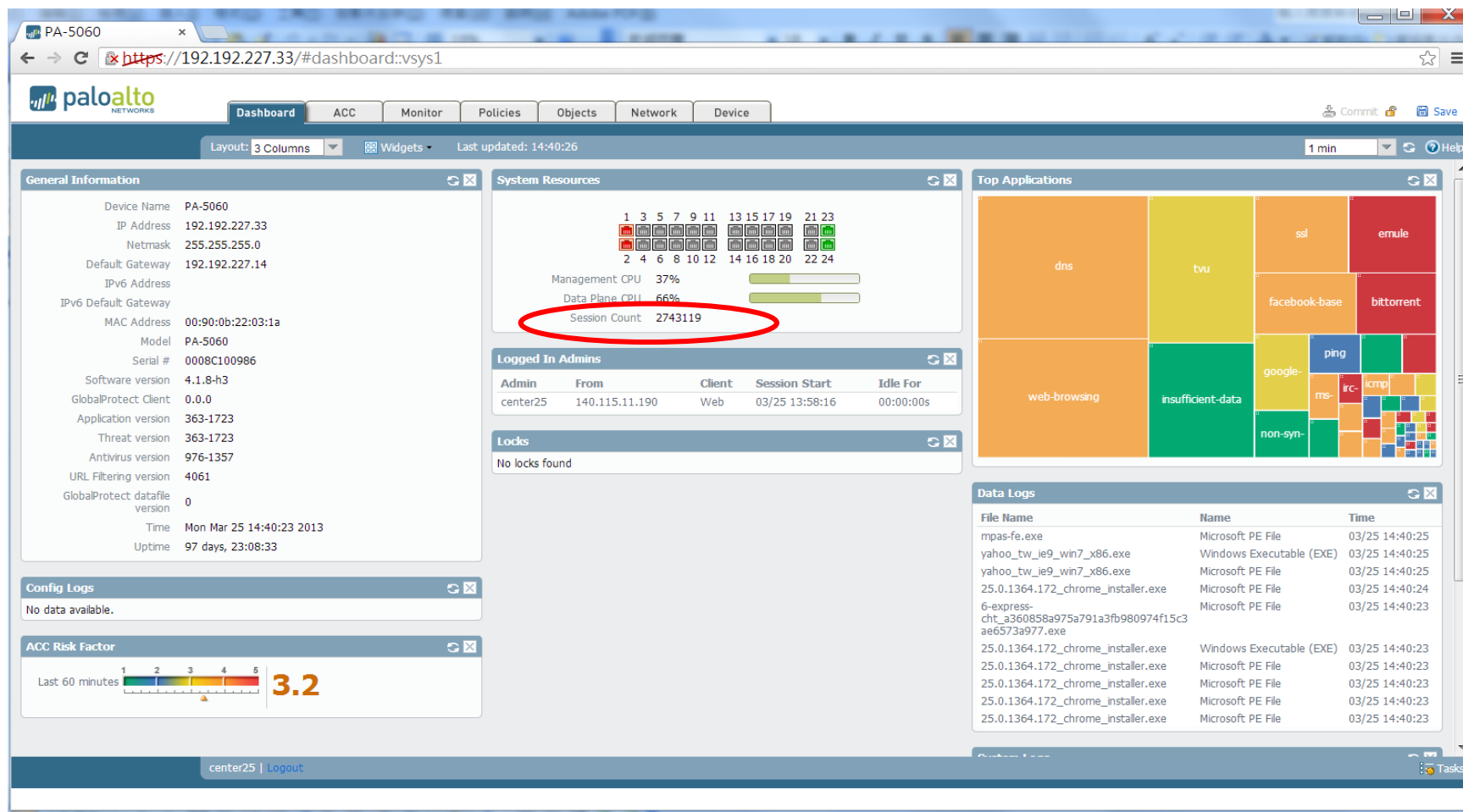
- Trust: tkm-ip group , other-ip group
- Untrust

☐ Policy:

- P2p阻擋
- security管制:
 - Antivirus
 - anti-spyware
 - Vulnerability:dns Brute-force DOS Attack, ssh Brute-force Attempt ...

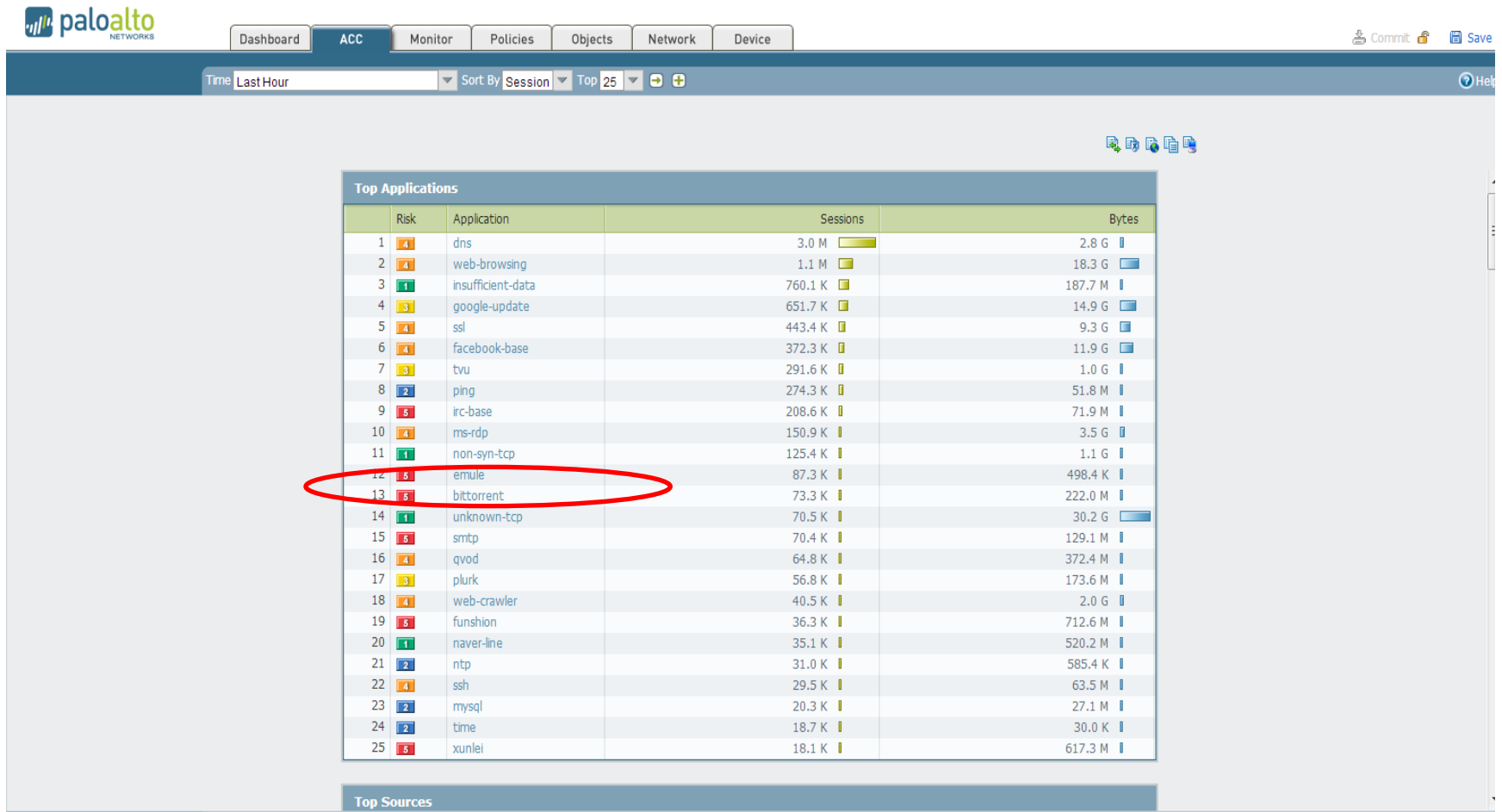


未啟動p2p管制



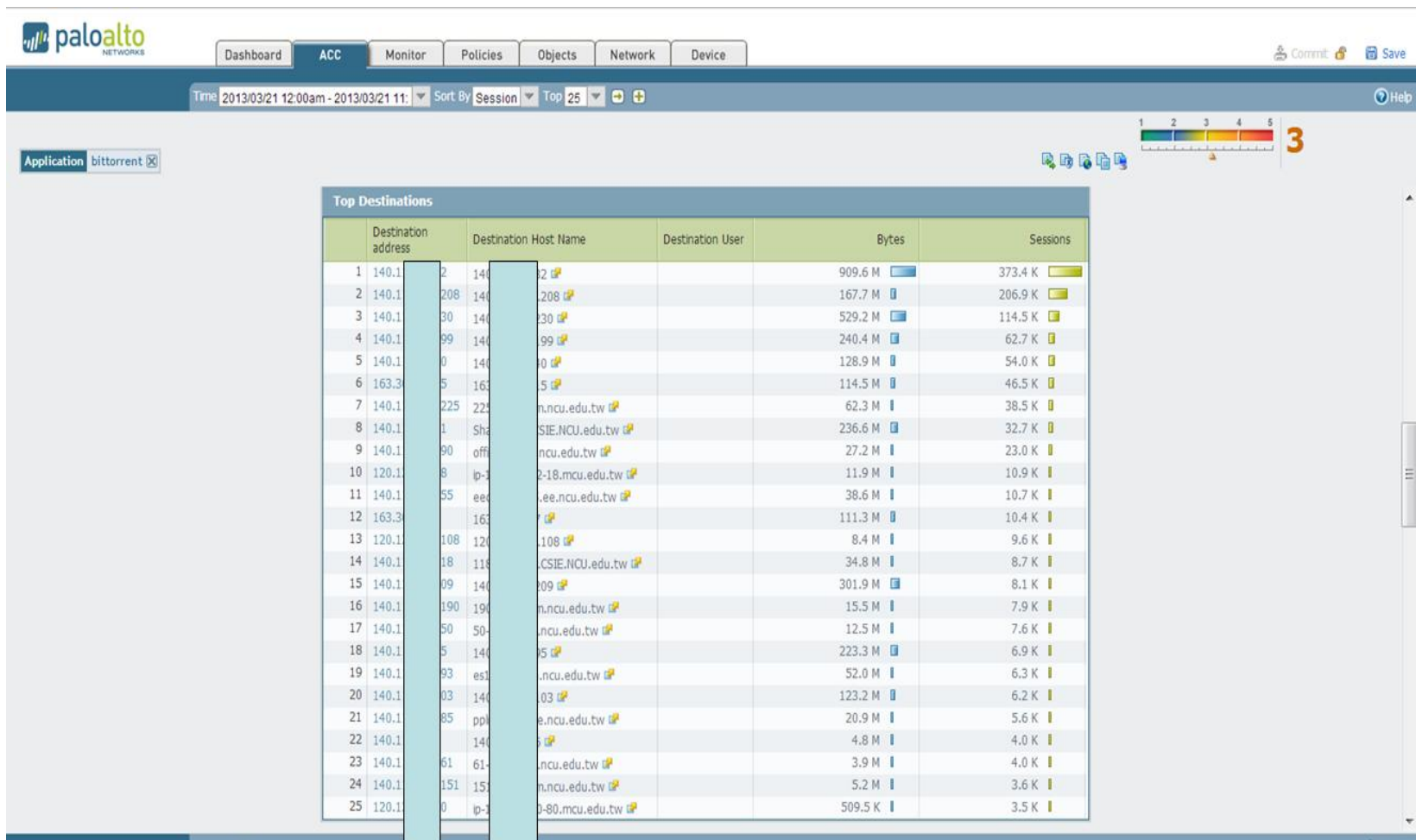


未啟動p2p管制



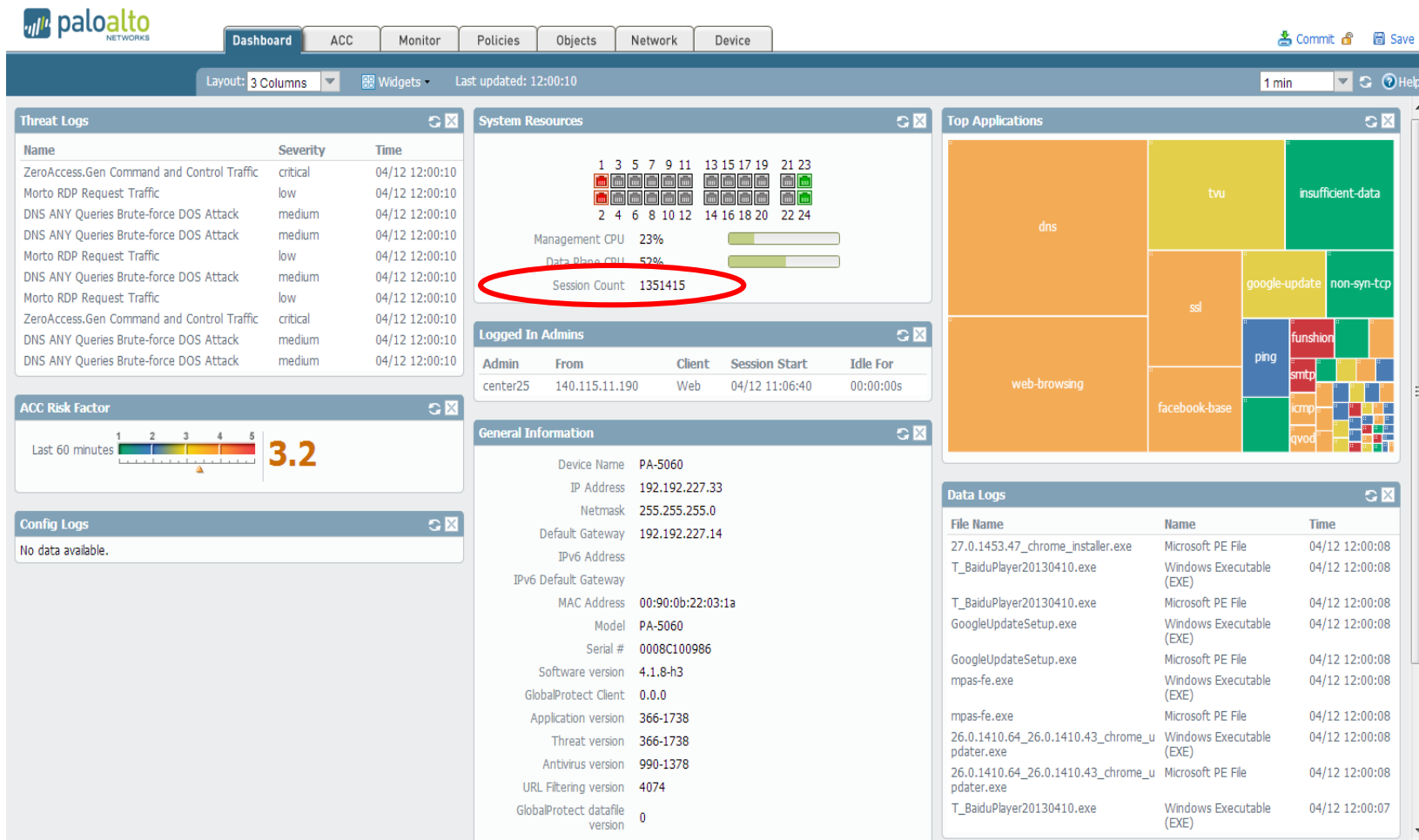


未啟動p2p管制





啟動p2p管制





Ssh Attempt及dns ddos統計量

Palo Alto Networks interface showing the Monitor tab and a Custom Report window for 'dns-rdp-ssh'.

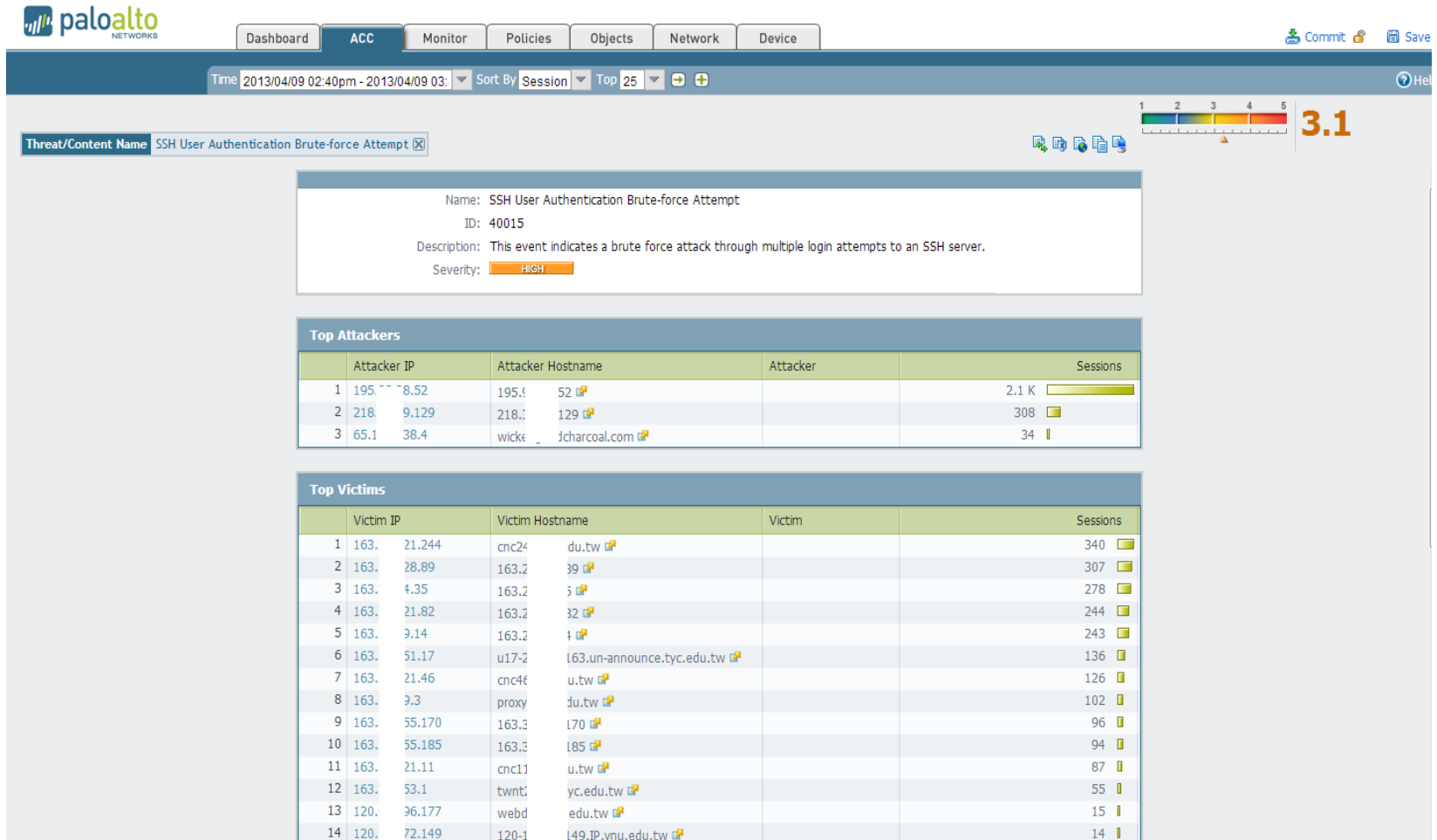
The Custom Report window displays the following data:

Threat/Content Name	ID	Count
1 DNS ANY Queries Brute-force DOS Attack	40033	2.3 M
2 SSH User Authentication Brute-force Attempt	40015	2.5 K
3 Microsoft SQL Server User Authentication Brute-force Attempt	40010	600

Export options: Export to PDF, Export to CSV, Export to XML. Buttons: OK, Cancel.

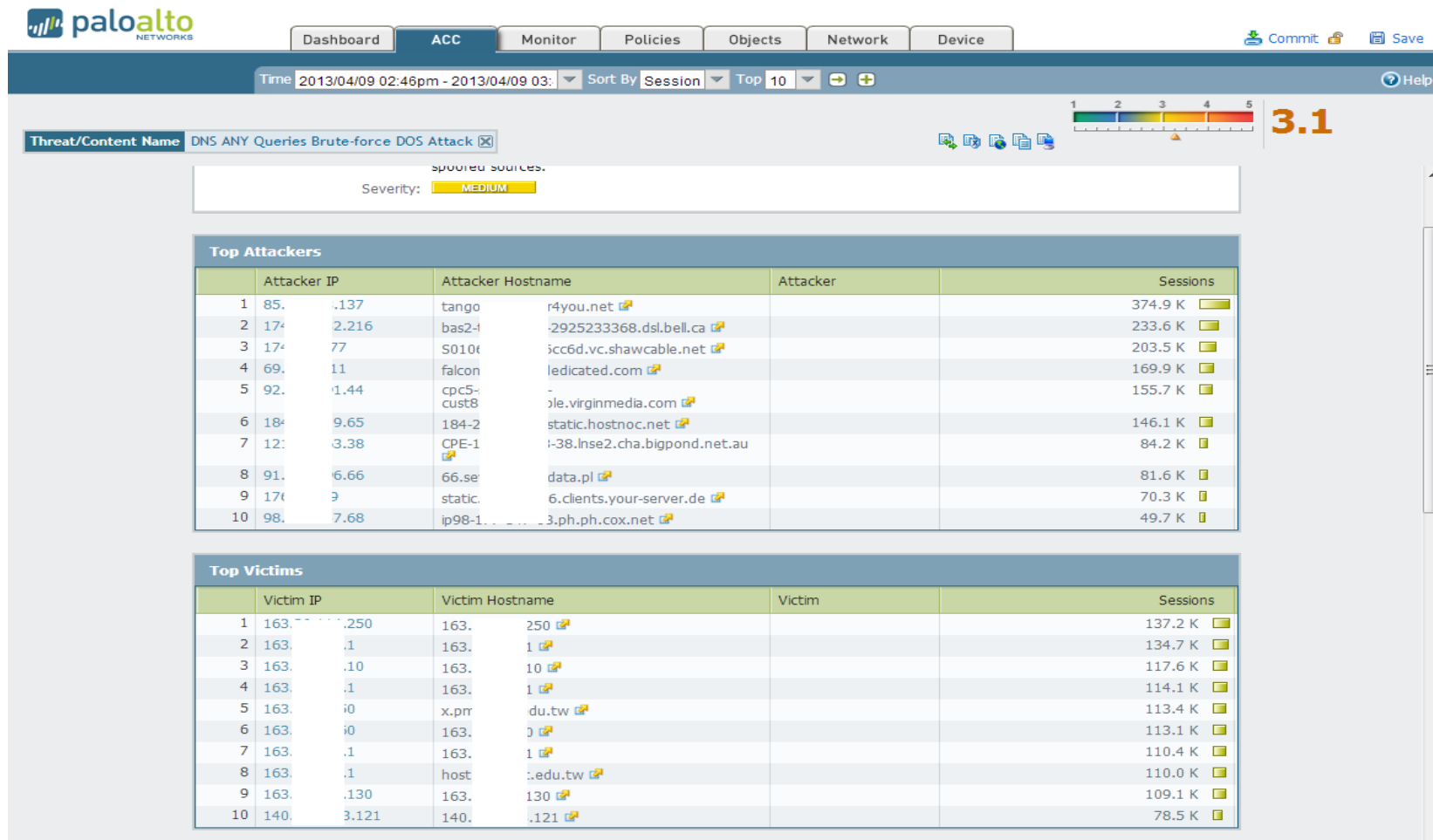


Ssh Attempt





dns ddos





啟動Ssh Attempt及dns ddos 阻擋

paloalto NETWORKS

Dashboard ACC **Monitor** Policies Objects Network Device

Commit Save

Help

Logs

- Traffic
- Threat
- URL Filtering
- Data Filtering
- HIP Match
- Configuration
- System
- Alarms

Packet Capture

App Scope

- Summary
- Change Monitor
- Threat Monitor
- Threat Map
- Network Monitor
- Traffic Map

Session Browser

Botnet

PDF Reports

- Manage PDF Summary
- User Activity Report
- Report Groups
- Email Scheduler

Manage Custom Reports

Reports

Custom Report

Report Setting dns-rdp-ssh

	Threat/Content Name	ID	Count
1	DNS ANY Queries Brute-force DOS Attack	40033	723.7 K
2	Microsoft SQL Server User Authentication Brute-force Attempt	40010	419
3	SSH User Authentication Brute-force Attempt	40015	4

Export to PDF Export to CSV Export to XML

OK Cancel

severity

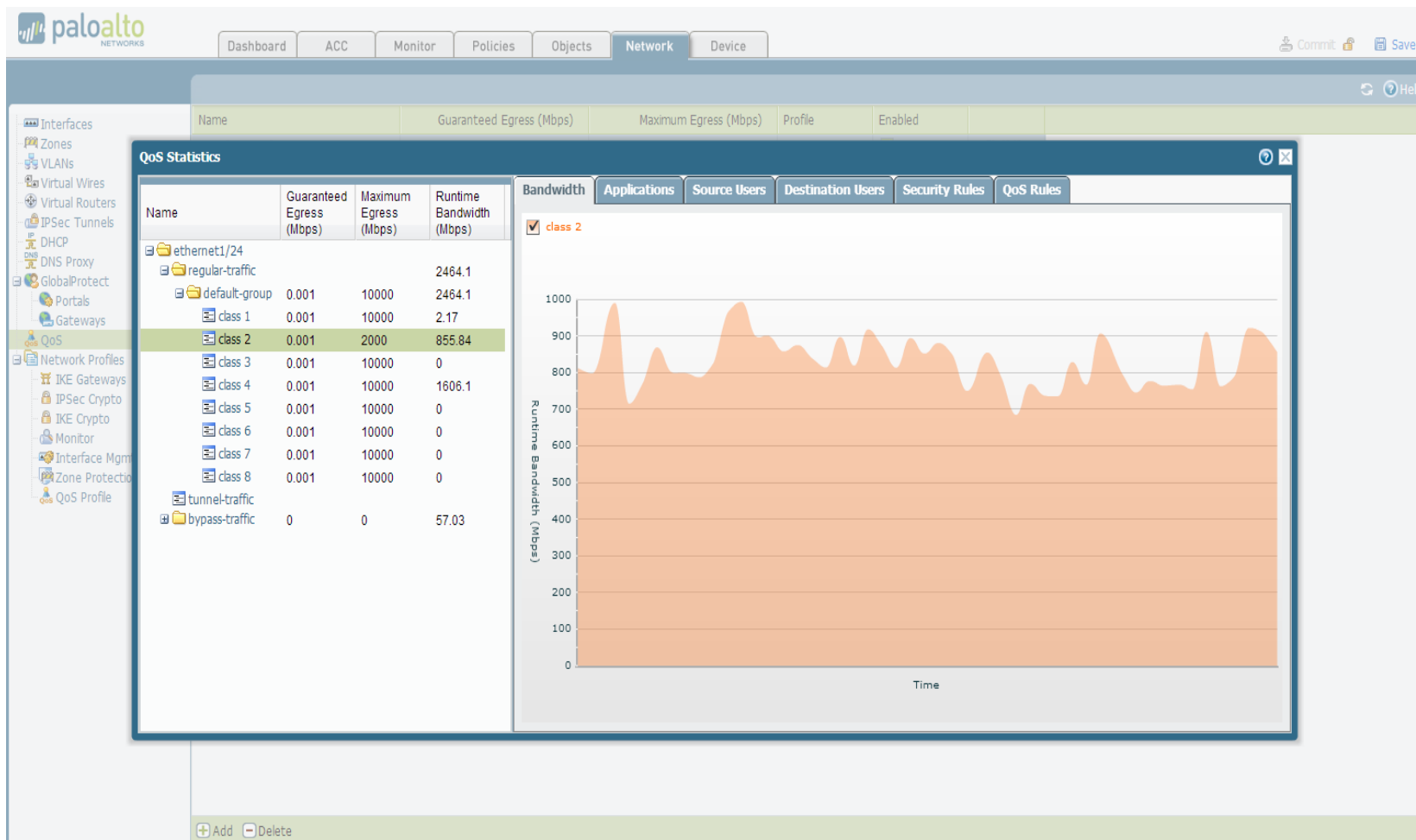
Group By

Scheduled

+ Add - Delete Clone



tkm-ip group 流量





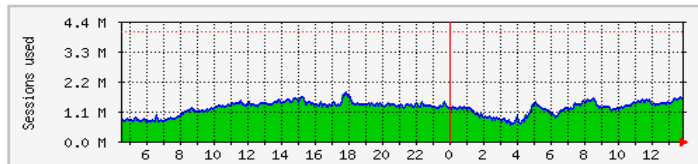
sessions使用量監控

Sessions for Paloalto5060

System: NCU Paloalto5060

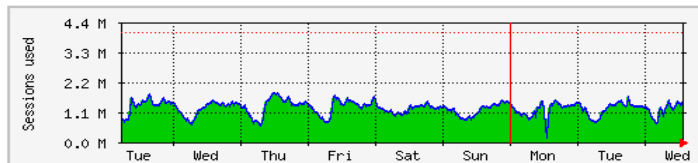
上次統計更新時間: 2013 四月 17 日, 星期三, 13:50.
設備名稱 'PaloAlto 5060', 已運作時間(uptime): 329 days, 21:59,.

每日 圖表 (5 分鐘 平均)



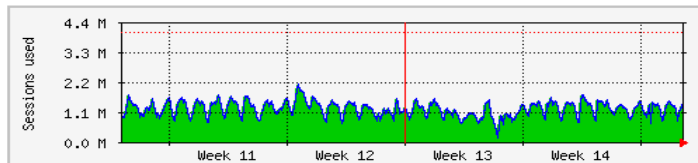
最大 1809.9 ks 平均 1249.3 ks 目前 1608.1 ks
最大 Sessions Utilization: 1809.9 ks 平均 Sessions Utilization: 1249.3 ks 目前 Sessions Utilization: 1608.1 ks

每週 圖表 (30 分鐘 平均)



最大 1816.0 ks 平均 1273.2 ks 目前 1522.0 ks
最大 Sessions Utilization: 1816.0 ks 平均 Sessions Utilization: 1273.2 ks 目前 Sessions Utilization: 1522.0 ks

每月 圖表 (2 小時 平均)





Monitor traffic

paloalto NETWORKS

Dashboard ACC **Monitor** Policies Objects Network Device

Manual

Logs

- Traffic
- Threat
 - URL Filtering
 - Data Filtering
 - HIP Match
 - Configuration
 - System
 - Alarms
- Packet Capture
- App Scope
 - Summary
 - Change Monitor
 - Threat Monitor
 - Threat Map
 - Network Monitor
 - Traffic Map
- Session Browser
- Botnet
- PDF Reports
 - Manage PDF Summary
 - User Activity Report
 - Report Groups
 - Email Scheduler
 - Manage Custom Reports
 - Reports

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Bytes
	04/12 11:46:36	deny	V-untrust	V-trust	202.174		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.139		8.2.2	58175	bittorrent	deny	outbound-deny	314
	04/12 11:46:36	deny	V-untrust	V-trust	119.132		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.7.162		37.1.41	49001	bittorrent	deny	outbound-deny	140
	04/12 11:46:36	deny	V-untrust	V-trust	218.51		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-untrust	V-trust	115.0.160		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.2.98		218.138	6261	emule	deny	outbound-deny	60
	04/12 11:46:36	deny	V-trust	V-untrust	140.2.98		88.1.1.45	22201	emule	deny	outbound-deny	60
	04/12 11:46:36	deny	V-trust	V-untrust	140.75		5.13.186	6881	bittorrent	deny	outbound-deny	98
	04/12 11:46:36	deny	V-trust	V-untrust	140.2.98		222.72.136	5157	emule	deny	outbound-deny	60
	04/12 11:46:36	deny	V-trust	V-untrust	140.2.98		222.38.40	25748	emule	deny	outbound-deny	60
	04/12 11:46:36	deny	V-trust	V-untrust	140.2.98		117.1.91	38080	emule	deny	outbound-deny	60
	04/12 11:46:36	deny	V-trust	V-untrust	140.209		201.30.230	51582	bittorrent	deny	outbound-deny	339
	04/12 11:46:36	deny	V-trust	V-untrust	140.7.162		24.227	37578	bittorrent	deny	outbound-deny	140
	04/12 11:46:36	deny	V-trust	V-untrust	140.49		2.96	11867	bittorrent	deny	outbound-deny	62
	04/12 11:46:36	deny	V-trust	V-untrust	140.4.216		91.2.186	6899	bittorrent	deny	outbound-deny	104
	04/12 11:46:36	deny	V-trust	V-untrust	140.166		79.1.3.132	19044	bittorrent	deny	outbound-deny	140
	04/12 11:46:36	deny	V-untrust	V-trust	175.4.115		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-untrust	V-trust	14.1.56		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.5.230		62.1.1.230	6881	bittorrent	deny	outbound-deny	317
	04/12 11:46:36	deny	V-untrust	V-trust	58.1.17		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.108		60.2.146	27650	bittorrent	deny	outbound-deny	140
	04/12 11:46:36	deny	V-trust	V-untrust	140.5.236		79.1.100	25717	bittorrent	deny	outbound-deny	248
	04/12 11:46:36	deny	V-untrust	V-trust	58.5.14		163.244	4672	emule	deny	inbound-deny	69
	04/12 11:46:36	deny	V-trust	V-untrust	140.62		83.6.08	19535	bittorrent	deny	outbound-deny	148
	04/12 11:46:36	deny	V-trust	V-untrust	140.4.216		78.1.1.84	41841	bittorrent	deny	outbound-deny	104

1 2 3 4 5 6 7 8 9 10 Resolve hostname

Displaying logs 1 - 50 50 per page DESC



Monitor Threat

paloalto NETWORKS

Dashboard ACC **Monitor** Policies Objects Network Device

Manual [Dropdown] [Refresh] [Help]

Logs
Traffic
Threat
URL Filtering
Data Filtering
HIP Match
Configuration
System
Alarms
Packet Capture
App Scope
Summary
Change Monitor
Threat Monitor
Threat Map
Network Monitor
Traffic Map
Session Browser
Botnet
PDF Reports
Manage PDF Summary
User Activity Report
Report Groups
Email Scheduler
Manage Custom Reports
Reports

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
[Icon]	04/12 11:49:48	spyware	Sipicious.sundayddr User-Agent Traffic	V-untrust	V-trust	115.34		120.1.1.17	5060	sip	alert	low
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	123.120		140.1.1.103	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	Win32.Conficker.C p2p	V-untrust	V-trust	109.30		140.1.1.44.51	10636	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	vulnerability	DNS ANY Queries Brute-force DOS Attack	V-untrust	V-trust	50.3	4	163.1.1.130	53	dns	drop-all-packets	medium
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	125.18		120.1.1.15	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-trust	V-untrust	140.50		64.1.1.169	53456	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-untrust	V-trust	180.254		140.1.1.244	61982	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	69.1	5	140.1.1.40.113	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-trust	V-untrust	120.31		103.1.1.35	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	190.29		192.1.1.143	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	Pushdo.Gen Denial of Service Traffic	V-trust	V-untrust	140.50		199.1.1.5.78	80	web-browsing	alert	critical
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-untrust	V-trust	68.1	27	140.1.1.12.15	60003	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	209.200		192.1.1.1.29	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-trust	V-untrust	140.50		98.1.1.61	53738	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	213.252		140.1.1.79.154	3389	t.120	alert	low
[Icon]	04/12 11:49:48	vulnerability	DNS ANY Queries Brute-force DOS Attack	V-untrust	V-trust	76.9	1	163.1.1.3.10	53	dns	drop-all-packets	medium
[Icon]	04/12 11:49:48	spyware	Morto RDP Request Traffic	V-untrust	V-trust	83.2	33	140.1.1.76.136	3389	t.120	alert	low
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-trust	V-untrust	140.50		58.7.1.47	60488	unknown-udp	drop-all-packets	critical
[Icon]	04/12 11:49:48	spyware	ZeroAccess.Gen Command and Control Traffic	V-trust	V-untrust	140.50		75.1.1.3.223	63109	unknown-udp	drop-all-packets	critical

1 2 3 4 5 6 7 8 9 10 [Dropdown] [Resolve hostname] Displaying logs 1 - 20 20 per page DESC

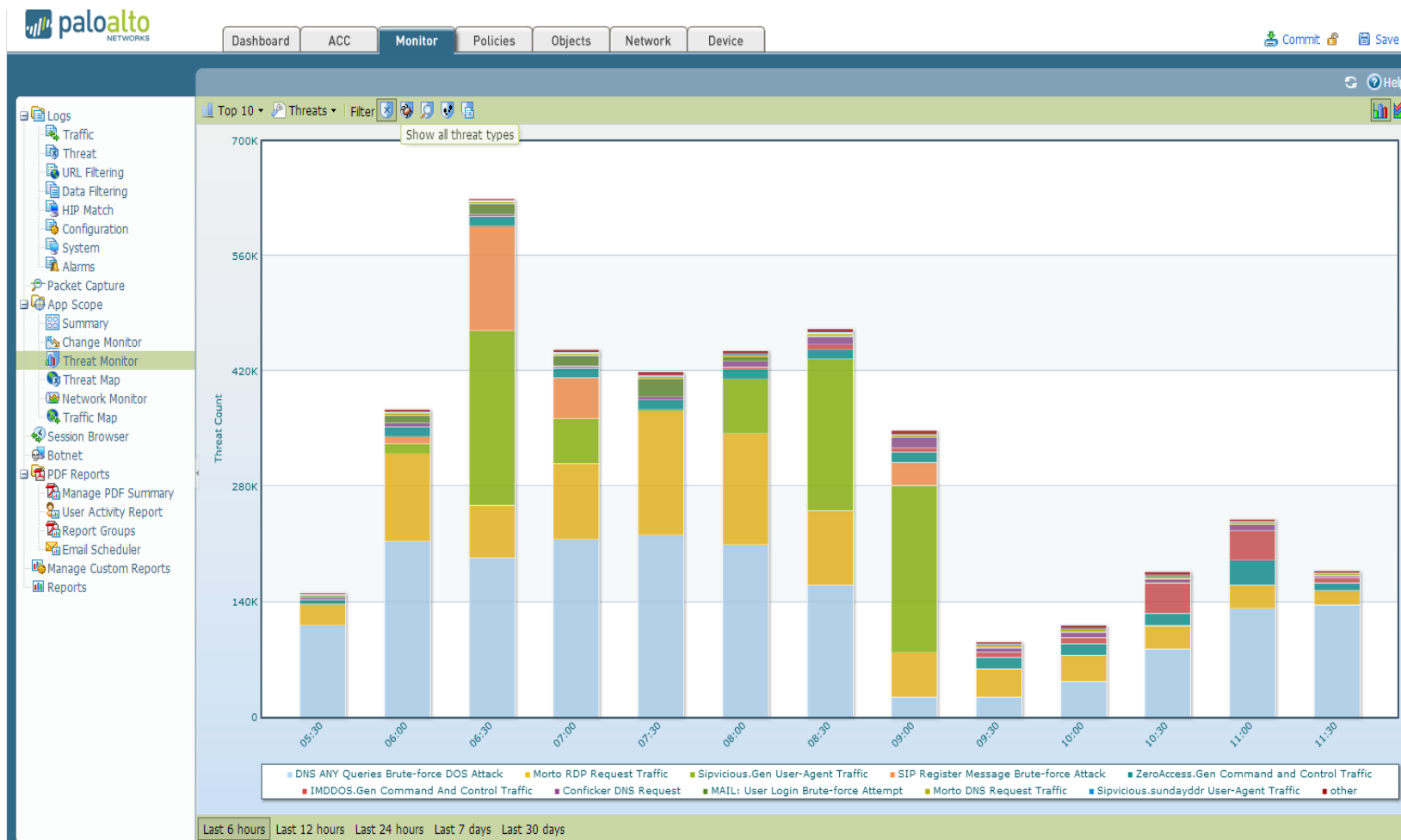


報表App summary





報表 Threat summary





報表

Application Reports

- Applications
- Application Categories
- Technology Categories
- HTTP Applications
- Denied Applications

Traffic Reports

- Security Rules
- Sources
- Source Countries
- Destinations
- Destination Countries
- Connections
- Source Zones
- Destination Zones
- Ingress Interfaces
- Egress Interfaces
- Denied Sources
- Denied Destinations
- Unknown TCP Sessions
- Unknown UDP Sessions

Threat Reports

- Botnet
- Threats
- Attackers
- Attacker Countries
- Victims
- Victim Countries
- Viruses
- Spyware
- Vulnerabilities
- Spyware Infected Hosts

URL Filtering Reports

- URL Categories
- URL Users
- URL User Behavior
- Web Sites
- Blocked Categories
- Blocked Users
- Blocked User Behavior
- Blocked Sites



報表-Topapp





報表-Topapp

單日網路應用量分布 x

140.115.2.27/Links/viewAllTopApps.do

桃園區網中心

ASOC_Abuse 通報 區網服務台 區網連線檢查 網管好幫手 區網 TopN 流量 中央 TopN 流量 流量異常偵測 區網網管平台

Links 連線狀態偵測與通告

- * Links 偵測首頁
- * 網管通訊錄
- * 連線介面
- * 連線計分
- * 連線狀態 (10-minutes)
- * 連線中斷紀錄
- * 連線中斷處理
- 連線狀況月報表
- 連線計分月報表
- * 單日 Botnet 感染主機
- * 單日網路應用量分布

Year (4-digit): 2013 Month: 04 Day: 23 Submit: Display

桃園區網中心 網路應用分類 資訊(20130423)

網路應用名稱	Bytes 資訊	Session 資訊
dns	83.29 GB	160.20 M
web-browsing	2.78 TB	80.17 M
insufficient-data	65.02 GB	64.12 M
tvu	424.94 GB	60.52 M
ssl	1.05 TB	30.25 M
facebook-base	1.12 TB	26.39 M
non-syn-tcp	145.82 GB	21.91 M
ping	4.01 GB	16.74 M
smtp	44.71 GB	12.82 M
funshion	627.31 GB	11.49 M
unknown-tcp	8.01 TB	10.79 M
mssql-db	5.77 GB	7.71 M
unknown-udp	303.22 GB	6.75 M
web-crawler	209.99 GB	4.43 M
qvod	651.94 GB	3.77 M
icmp	582.48 MB	3.20 M
ppstream	86.98 GB	2.55 M
ms-rdp	103.05 GB	2.21 M
plurk	9.22 GB	1.77 M
sip	186.92 MB	1.58 M
360-safeguard-update	7.21 GB	1.49 M
google-update	362.41 GB	1.44 M
ntp	1.79 GB	1.38 M
pando	7.25 GB	1.30 M



報表-Host流量排行





報表 Botnet ip

檔案(F)	編輯(E)	檢視(V)	文件(D)	注釋(C)	表格(R)	工具(T)	進階(A)	視窗(W)	說明(H)
botnet									
PA-5060 : Thursday, April 11, 2013									
confidence	源地址	源用戶	虛擬系統						
4	140.156.238	vsys1		Repeatedly visited (813) the same malicious URL "mine2.btcguild.com/"					
4	140.156.2169	vsys1		Repeatedly visited (77580) the same malicious URL "dolgnik.net/" . □ Repeatedly visited (37) the same					
4	140.156.347	vsys1		Repeatedly visited (5) the same malicious URL "www.updatesync.info/get/?product=OptimizerPro&f					
4	120.156.20	vsys1		Repeatedly visited (5) the same malicious URL "www.updatesync.info/get/?product=OptimizerPro&f					
4	163.156.129	vsys1		Repeatedly visited (25) the same malicious URL "lyuchta.org/" . □ Repeatedly visited (97) the same					
4	140.156.16.190	vsys1		Repeatedly visited (5) the same malicious URL "www.updatesync.info/get/?product=OptimizerPro18					
4	140.156.25.23	vsys1		Repeatedly visited (7) the same malicious URL "www.9918edu.com/favicon.ico"					
4	140.156.160	vsys1		Repeatedly visited (6) the same malicious URL "lyuchta.org/" . □ Repeatedly visited (35) the same					
4	140.156.3.126	vsys1		Repeatedly visited (5) the same malicious URL "js.2008xxx.com/js/qq168.js" . □ Repeatedly visited					
4	140.156.204.3	vsys1		Repeatedly visited (5) the same malicious URL "www.updatesync.info/get/?product=WxDFAST&publi					
4	140.156.204.43	vsys1		Repeatedly visited (5) the same malicious URL "www.updatesync.info/get/?product=OptimizerPro18					
3	120.156.17.26	vsys1		Repeatedly (13) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
3	140.156.12.145	vsys1		Repeatedly (5) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
3	140.156.55.158	vsys1		Repeatedly (7) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
3	140.156.17.68	vsys1		Repeatedly (5) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
3	140.156.20.133	vsys1		Repeatedly (10) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
3	120.156.1.167	vsys1		Repeatedly (6) downloads executables from the same unknown URL up.bddyy.com/T_BaiduPlayer2					
2	120.156.12.102	vsys1		Repeatedly visited (59) the same URL "220.181.141.104/msvquery"					
2	140.156.1.51	vsys1		Repeatedly visited (7) the same dynamic DNS URL "ssl14.ovh.net/"					
2	120.156.16.41	vsys1		Repeatedly visited (7) the same URL "50.22.154.176/caketw/gateway/"					
2	140.156.18.53	vsys1		Repeatedly visited (5) the same recently created domain URL "ahqesportsclub.com/"					
2	120.156.204.117	vsys1		Repeatedly visited (10) the same URL "119.147.146.110/query2"					
2	140.156.1.64	vsys1		Repeatedly visited (122) the same URL "61.160.228.1/p2p/TGxgoESATGwd0K2y-L1x4CVJqS-m-ph					
2	140.156.14.25	vsys1		Repeatedly visited (22) the same URL "140.154.13.222/bsc-sta-"					



報表 Botnet ip

← → C 140.115.2.27/Links/viewAllBotnets.do ☆ ≡

ASOC_Abuse 通報 區網服務台 區網連線檢查 網管好幫手 區網 TopN 流量 中央 TopN 流量 流量異常偵測 區網網管平台

Links 連線狀態偵測與通告

- * Links 偵測首頁
- * 網管通訊錄
- * 連線介面
- * 連線計分
- * 連線狀態 (10-minutes)
- * 連線中斷紀錄
- * 連線中斷處理
- 連線狀況月報表
- 連線計分月報表
- * 單日 Botnet 感染主機
- * 單日網路應用量分布

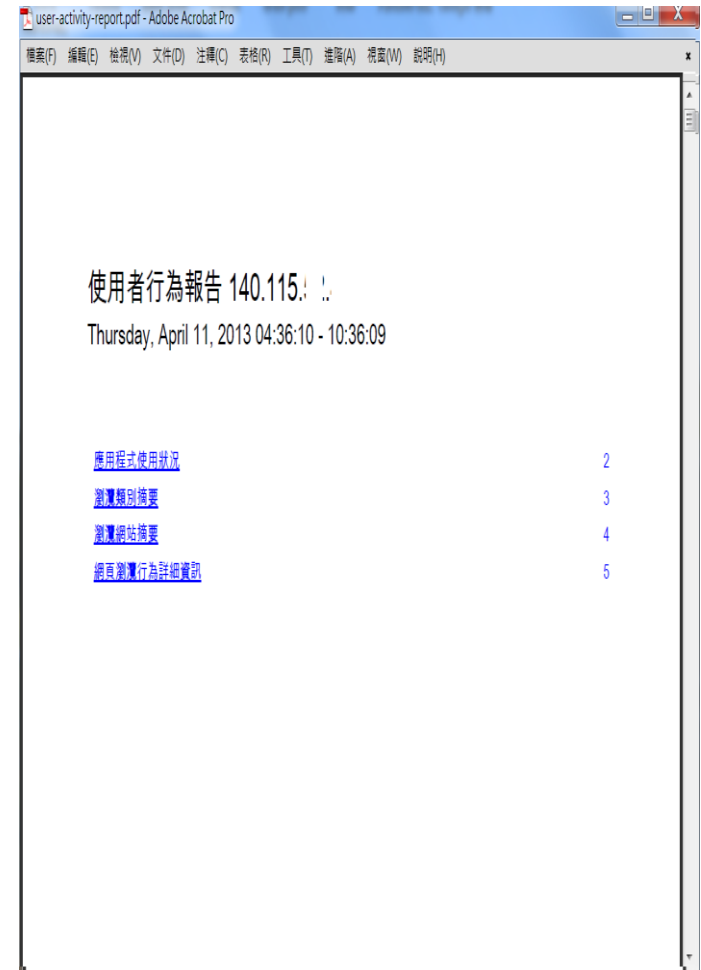
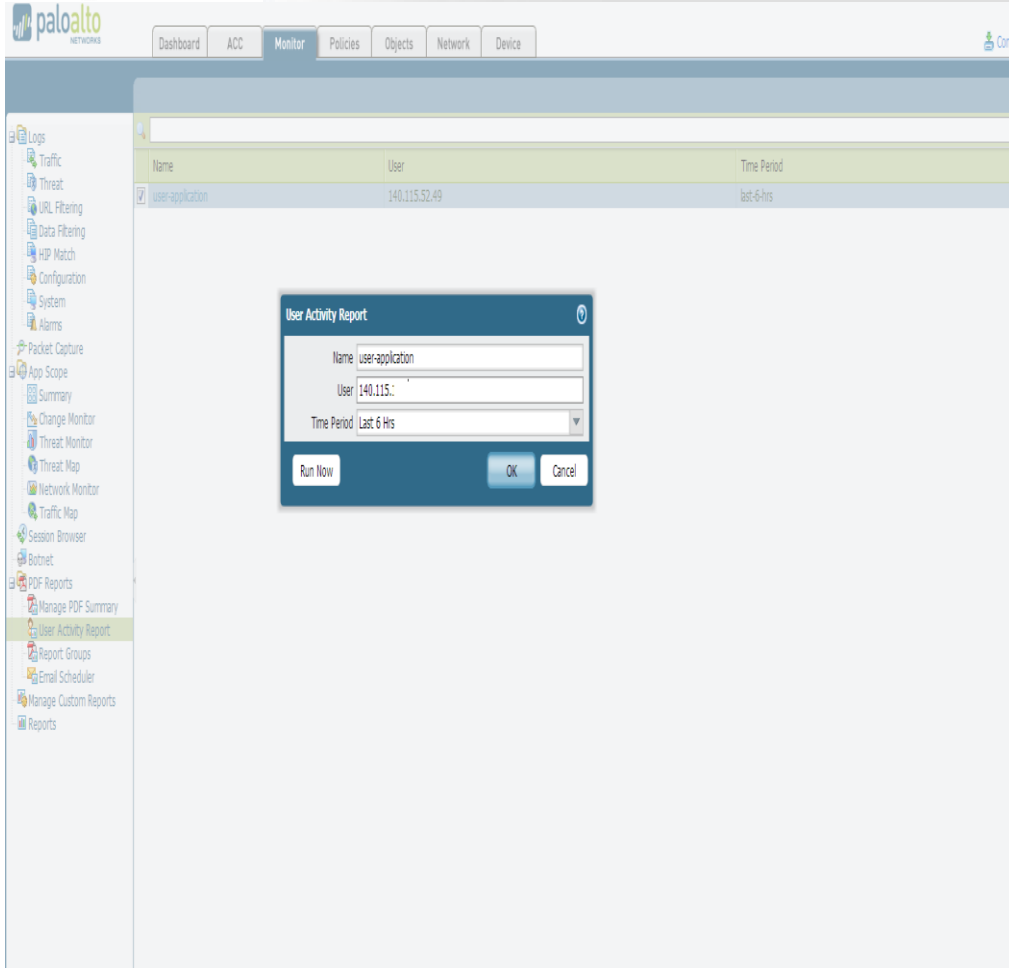
Year (4-digit): 2013 Month: 04 Day: 23 Submit: Display

桃園區網中心 Botnet 資訊(20130423)

信賴程度	主機 IP	判斷依據資訊
4	120.124.252.88	vsys1 Repeatedly visited (6) the same malicious URL "tavis.tw/ezfiles/0/1000/style/95/image/s/hdarrow.gif"
4	163.30.108.16	vsys1 Repeatedly visited (36) the same malicious URL "lyuchta.org"
4	163.30.108.23	vsys1 Repeatedly visited (30) the same malicious URL "lyuchta.org"
4	140.115.156.238	vsys1 Repeatedly visited (15) the same malicious URL "mint.bitminter.com"
4	140.115.210.101	vsys1 Repeatedly visited (5) the same malicious URL "mvts.com"
4	163.30.38.129	vsys1 Repeatedly visited (127) the same malicious URL "lyuchta.org"
4	163.30.197.82	vsys1 Repeatedly visited (58) the same malicious URL "lyuchta.org"
4	120.124.104.243	vsys1 Repeatedly visited (6) the same malicious URL "r1.reportbox1.info/?report_version=5&"
4	140.115.581	vsys1 Repeatedly visited (14) the same malicious URL "kiev-usa.biz"
4	163.30.134.75	vsys1 Repeatedly visited (200) the same malicious URL "lyuchta.org"
2	163.30.255.163	vsys1 Repeatedly visited (11) the same URL "103.246.36.212/1/R/Q856W-4CJRR/BLU00001/0/GET/http/www.668bjw.com/80/biaoge1.txt"
2	140.138.21	vsys1 Repeatedly visited (22) the same URL "31.13.75.17"

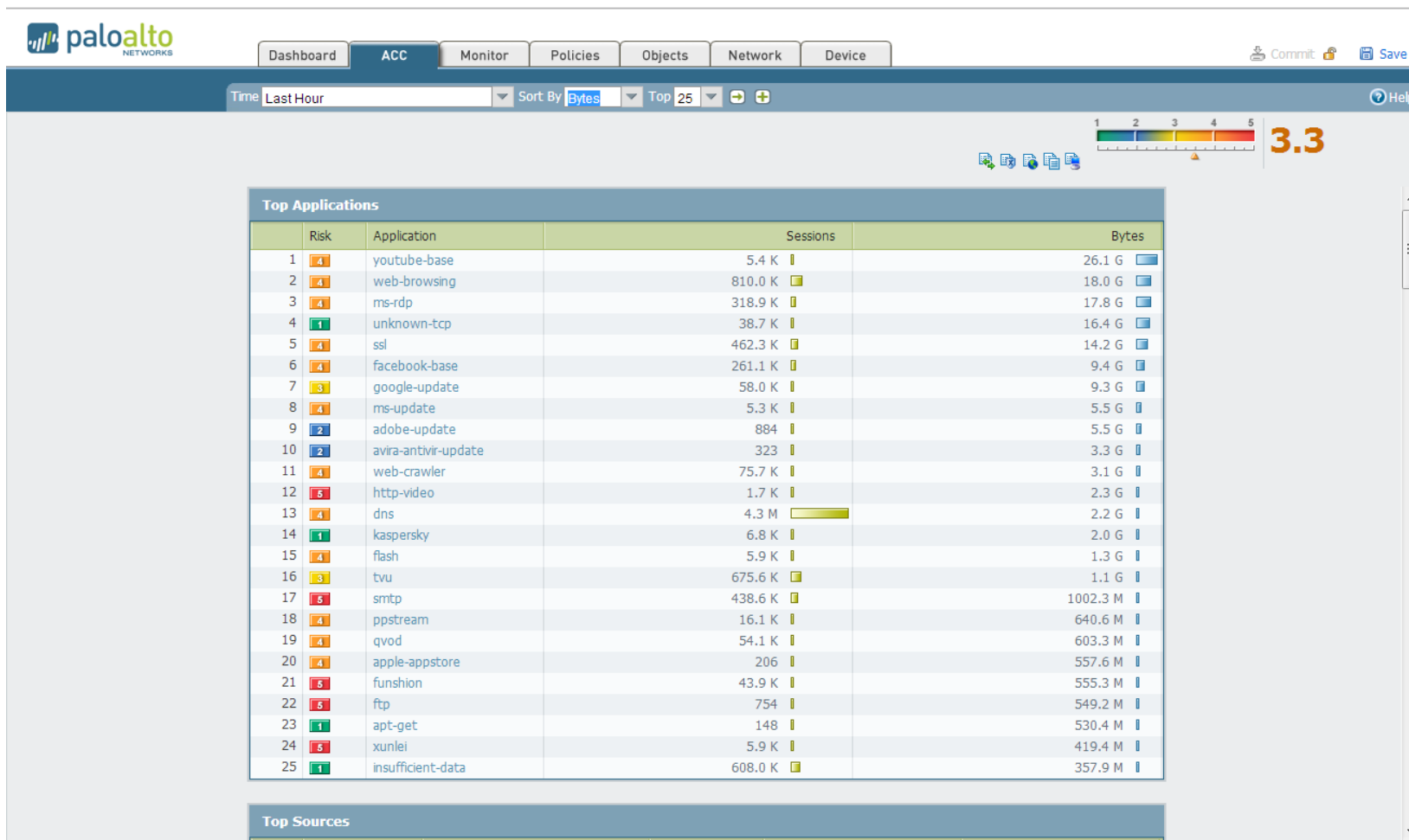


報表: user ip traffic統計



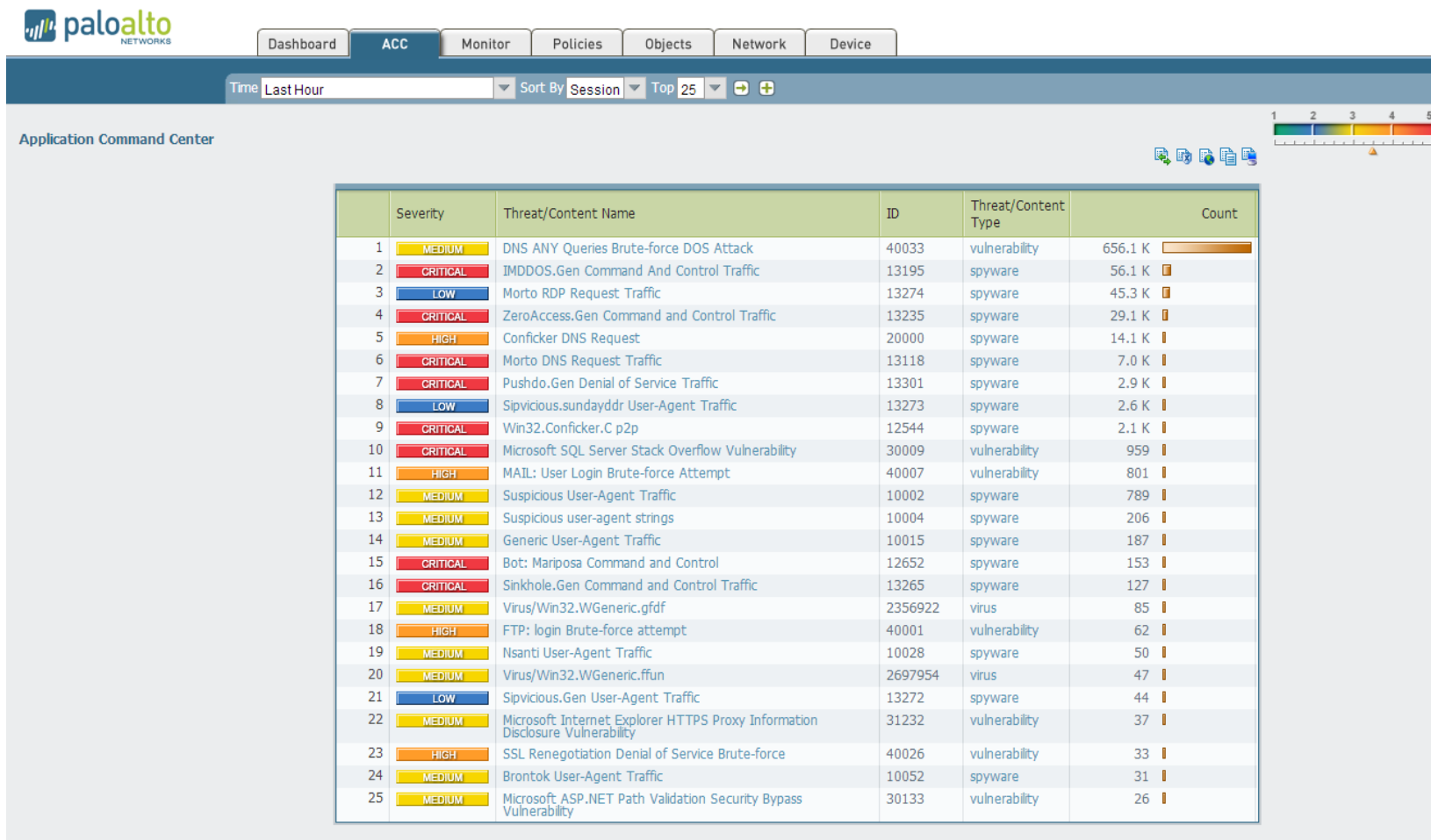


流量分析





流量分析-threat





流量分析-threat policy

paloalto NETWORKS

Dashboard ACC Monitor Policies **Objects** Network Device

Commit Save

Help

Addresses Address Groups Regions Applications Application Groups Application Filters Services Service Groups GlobalProtect HIP Objects HIP Profiles Custom URL Categories Custom Signatures Data Patterns Spyware Vulnerability Security Profiles Antivirus Anti-Spyware Vulnerability Profiles URL Filtering File Blocking Data Filtering DoS Protection Security Profile Groups Log Forwarding Schedules

Anti-Spyware Profile

Name: **tyrc-ant-spy**

Description:

Rules Exceptions

Ena...	Id	Threat Name	Rule	Category	Severity	Action	Packet Capture
<input checked="" type="checkbox"/>	12544	Win32.Conficker.C.p2p	simple-critical	adware	critical	default (drop-all-packets)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	12652	Bot: Mariposa Command and Control	simple-critical	spyware	critical	default (drop-all-packets)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13118	Morto DNS Request Traffic		net-worm	critical	drop-all-packets	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13195	IMDDOS.Gen Command And Control Traffic	simple-critical	botnet	critical	default (reset-both)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13235	ZeroAccess.Gen Command And Control Traffic		botnet	critical	drop-all-packets	<input type="checkbox"/>

☐ Show all signatures

Page 1 of 1 | Displaying 1 - 5/ 5 threats (Selected 5)

OK Cancel

+ Add - Delete Clone



Qos : tkm-ip group

paloalto NETWORKS

Dashboard ACC Monitor **Policies** Objects Network Device

Commit Save

Security
NAT
QoS
Policy Based Forwarding
Decryption
Application Override
Captive Portal
DoS Protection

Addresses

Source					Destination					
Name	Tag	Zone	Address	User	Zone	Address	Application	Service	Class	Schedule
PPS-100M	none	V-trust	any	any	V-untrust	any	ppstream	any	1	08-18
tkm-ip	none	V-trust	163.25.120.... 163.25.128.... 163.25.132.... 163.25.20.0/... 163.25.24.0/... 163.30.0.0/16	any	V-untrust	any	any	any	2	8-17

Name Address



Qos:tkm-ip group service統計

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Save

Help

Interfaces

QoS Statistics

Name	Guaranteed Egress (Mbps)	Maximum Egress (Mbps)	Runtime Bandwidth (Mbps)
ethernet1/24			
regular-traffic			2848.6
default-group			
class 1	0.001	10000	0.61
class 2	0.001	2000	931.91
class 3	0.001	10000	0
class 4	0.001	10000	1916.08
class 5	0.001	10000	0
class 6	0.001	10000	0
class 7	0.001	10000	0
class 8	0.001	10000	0
tunnel-traffic			
bypass-traffic	0	0	43.51

Bandwidth Applications Source Users Destination Users Security Rules QoS Rules

Name	Sessions	Bytes
google-talk-base	10	12526
windows-push-notifications	2	226
yahoo-voice	1	57
telnet	7	3528
google-plus-base	1	304
unknown-tcp	1	184
ssl	10	27188
naver-line	1	83
msn-base	3	1214
google-maps	1	79
teredo	15	4606
unknown-udp	1	346
tvu	1	524
ping	233	627
teamviewer-base	6	10462
facebook-chat	1	404
gmail-base	3	496628
ipv6	8	19
web-browsing	4	1138
facebook-base	10	8340
dropbox	1	79
facebook-sociallogin	1	5034

Page 1 of 1

Displaying 1 - 30 of 30



Computer Center, National Central University.



Thank You!