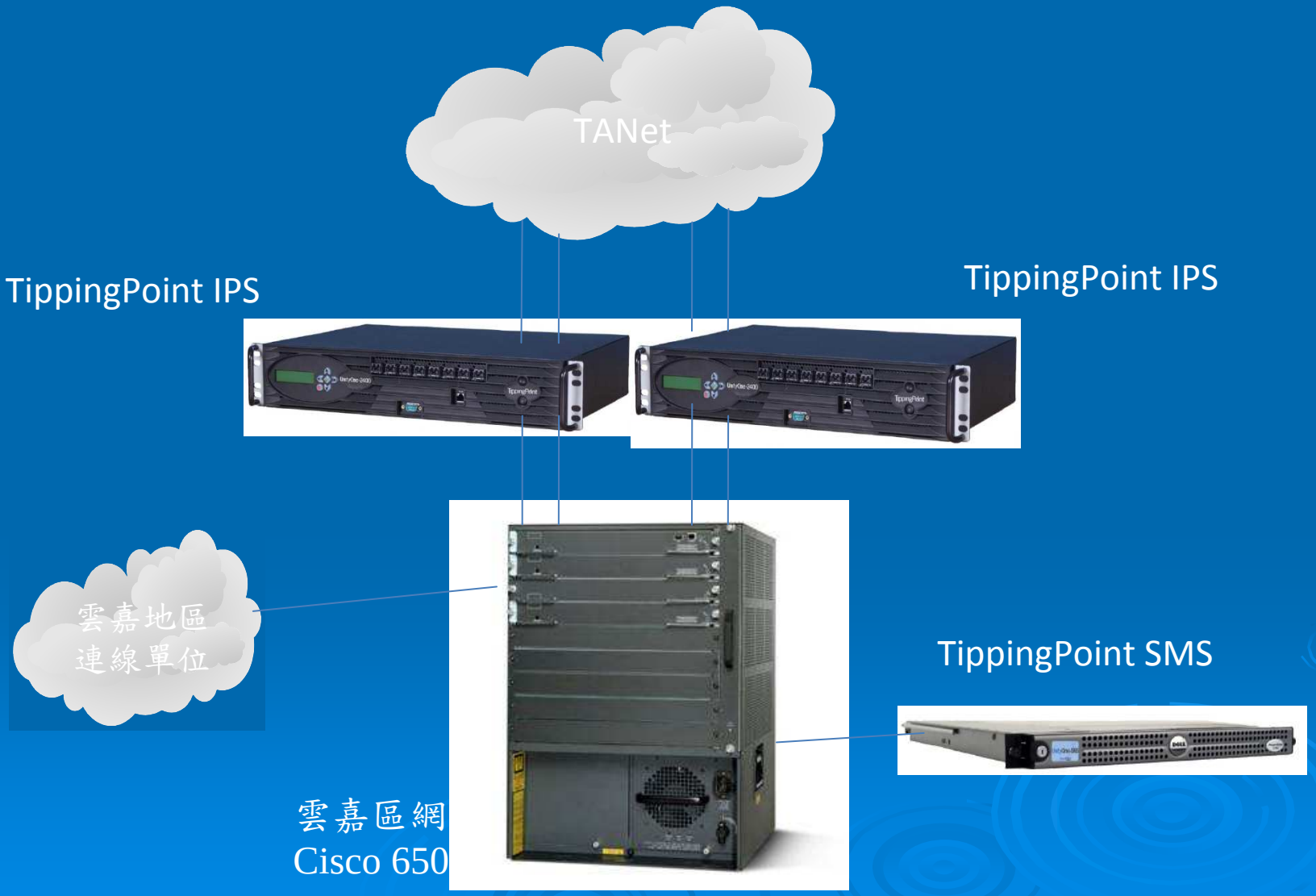
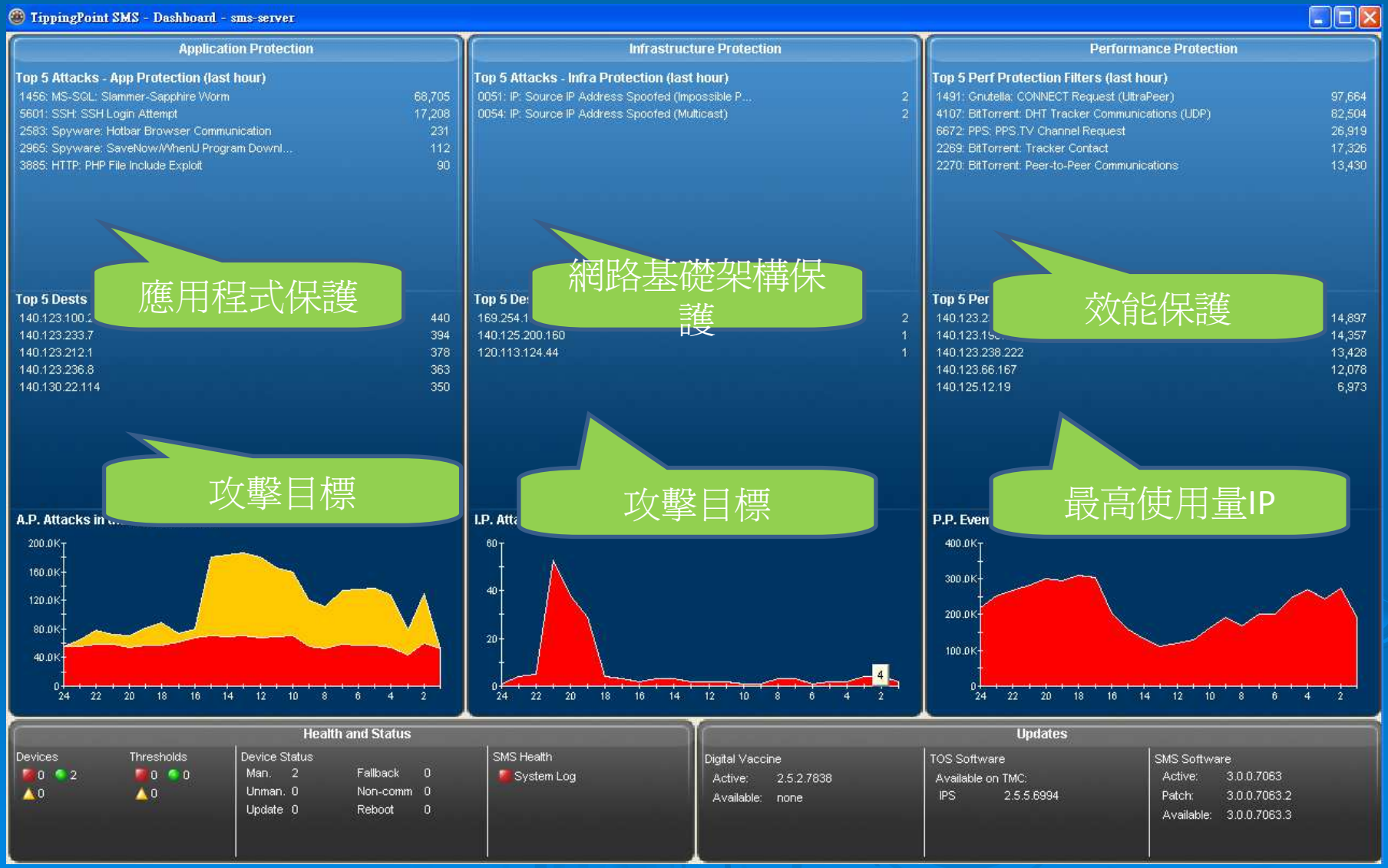
雲嘉區網網路管理機制

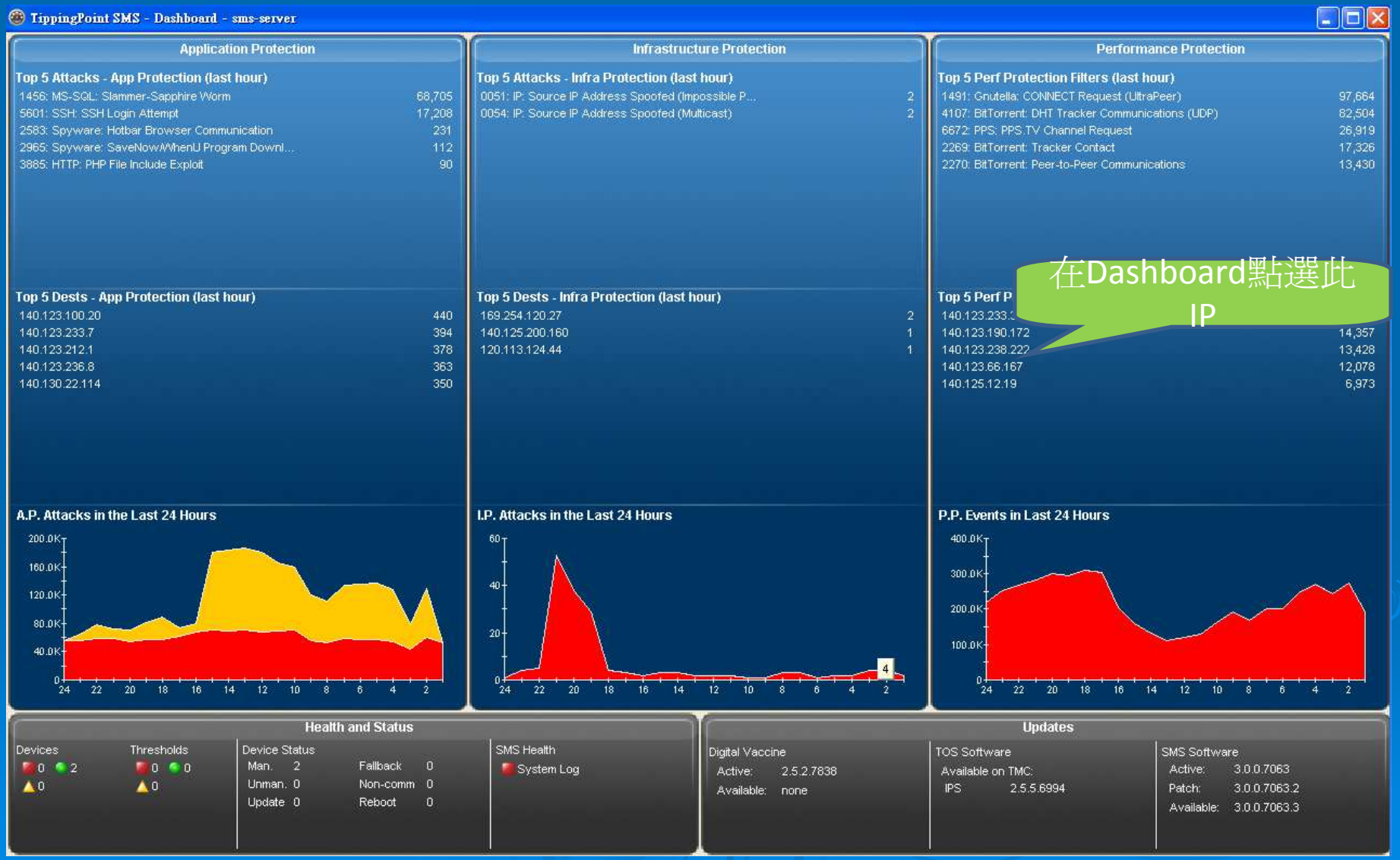
雲嘉區網網路管理架構


TANet
TippingPoint IPS
TippingPoint IPS
雲嘉地區
連線單位
TippingPoint SMS
雲嘉區網
Cisco 650

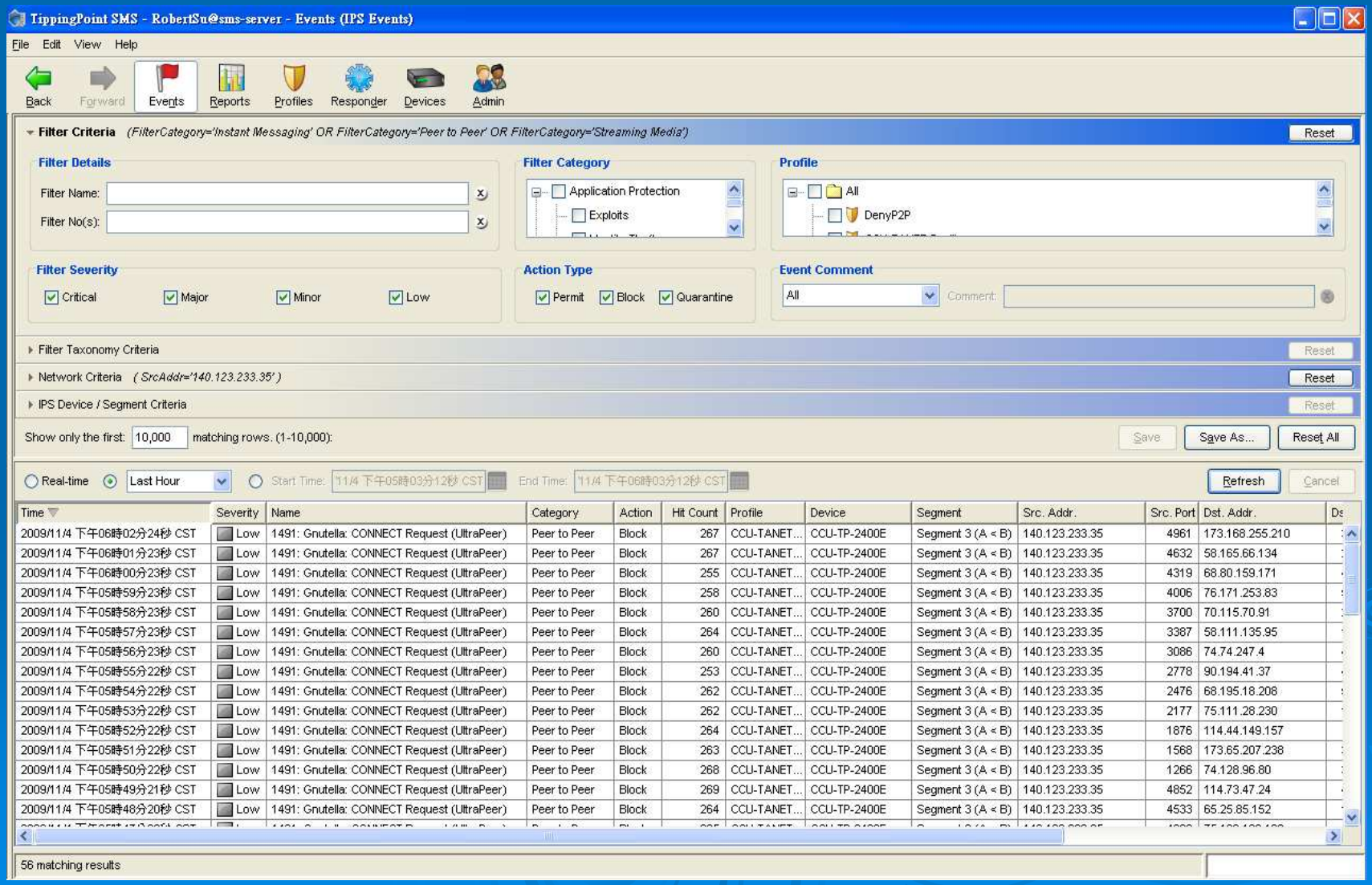
資安事件即時動態報表


TippingPoint SMS - Dashboard - sms-server
Application Protection
Top 5 Attacks - App Protection (last hour)
1456: MS-SQL: Slammer-Sapphire Worm 68,705
5601: SSH: SSH Login Attempt 17,208
2583: Spyware: Hotbar Browser Communication 231
2965: Spyware: SaveNowWhenU Program Downl... 112
3885: HTTP: PHP File Include Exploit 90
Top 5 Dests
140.123.100.2 440
140.123.233.7 394
140.123.212.1 378
140.123.236.8 363
140.130.22.114 350
A.P. Attacks in t...
200.0K
160.0K
120.0K
80.0K
40.0K
0
24 22 20 18 16 14 12 10 8 6 4 2
Infrastructure Protection
Top 5 Attacks - Infra Protection (last hour)
0051: IP: Source IP Address Spoofed (Impossible P... 2
0054: IP: Source IP Address Spoofed (Multicast) 2
Top 5 De:
169.254.1 2
140.125.200.160 1
120.113.124.44 1
I.P. Atta
60
40
20
0
4
24 22 20 18 16 14 12 10 8 6 4 2
Performance Protection
Top 5 Perf Protection Filters (last hour)
1491: Gnutella: CONNECT Request (UltraPeer) 97,664
4107: BitTorrent: DHT Tracker Communications (UDP) 82,504
6672: PPS: PPS.TV Channel Request 26,919
2269: BitTorrent: Tracker Contact 17,326
2270: BitTorrent: Peer-to-Peer Communications 13,430
Top 5 Per
140.123.2 14,897
140.123.15 14,357
140.123.238.222 13,428
140.123.66.167 12,078
140.125.12.19 6,973
P.P. Even
400.0K
300.0K
200.0K
100.0K
0
24 22 20 18 16 14 12 10 8 6 4 2
Health and Status
Devices
0 2
0
Thresholds
0 0
0
Device Status
Man. 2
Unman. 0
Update 0
Fallback 0
Non-comm 0
Reboot 0
SMS Health
System Log
Updates
Digital Vaccine
Active: 2.5.2.7838
Available: none
TOS Software
Available on TMC:
IPS 2.5.5.6994
SMS Software
Active: 3.0.0.7063
Patch: 3.0.0.7063.2
Available: 3.0.0.7063.3
應用程式保護
網路基礎架構保護
效能保護
攻擊目標
攻擊目標
最高使用量IP

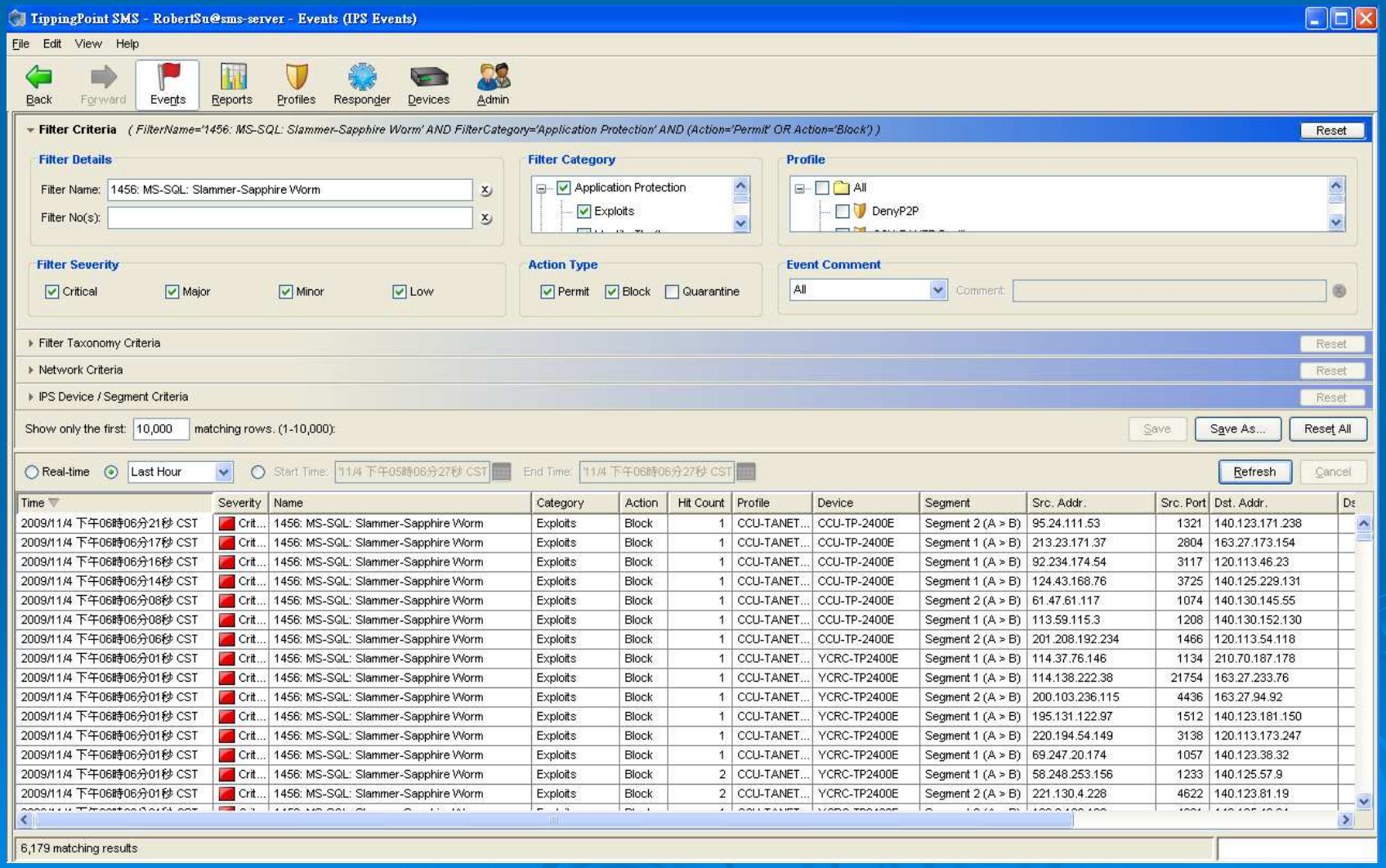
點選IP，自動帶出此IP相關資料



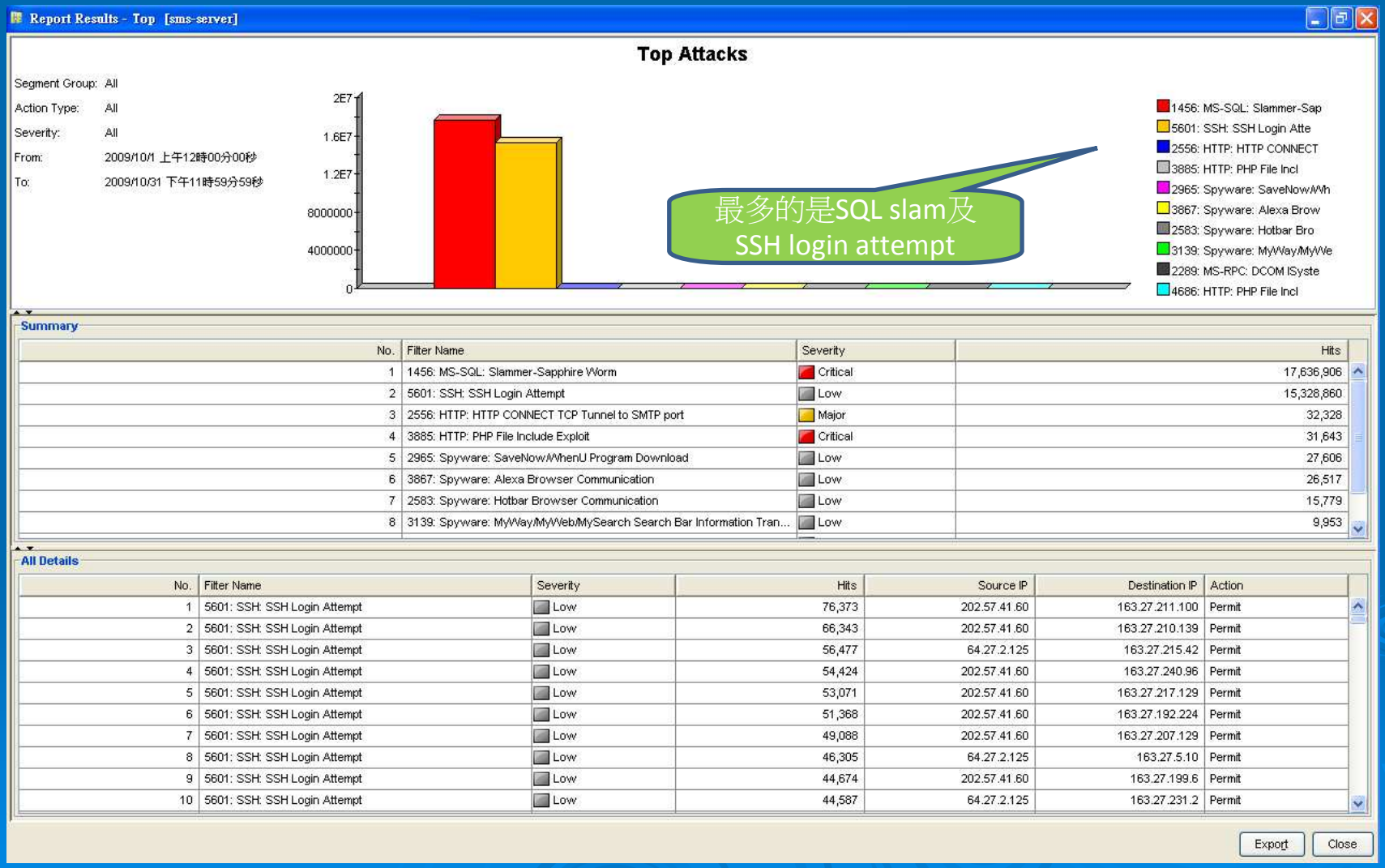
發生事件IP相關資料


TippingPoint SMS - RobertSu@sms-server - Events (IPS Events)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
Filter Criteria (FilterCategory='Instant Messaging' OR FilterCategory='Peer to Peer' OR FilterCategory='Streaming Media')
Reset
Filter Details
Filter Name:
Filter No(s):
Filter Category
Application Protection
Exploits
Profile
All
DenyP2P
Filter Severity
Critical Major Minor Low
Action Type
Permit Block Quarantine
Event Comment
All
Comment:
Filter Taxonomy Criteria
Network Criteria (SrcAddr='140.123.233.35')
IPS Device / Segment Criteria
Show only the first: 10,000 matching rows. (1-10,000):
Save Save As... Reset All
Real-time Last Hour Start Time: 11/4 下午05時03分12秒 CST End Time: 11/4 下午06時03分12秒 CST
Refresh Cancel
Time Severity Name Category Action Hit Count Profile Device Segment Src. Addr. Src. Port Dst. Addr.
2009/11/4 下午06時02分24秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 267 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4961 173.168.255.210
2009/11/4 下午06時01分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 267 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4632 58.165.66.134
2009/11/4 下午06時00分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 255 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4319 68.80.159.171
2009/11/4 下午05時59分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 258 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4006 76.171.253.83
2009/11/4 下午05時58分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 260 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 3700 70.115.70.91
2009/11/4 下午05時57分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 264 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 3387 58.111.135.95
2009/11/4 下午05時56分23秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 260 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 3086 74.74.247.4
2009/11/4 下午05時55分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 253 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 2778 90.194.41.37
2009/11/4 下午05時54分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 262 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 2476 68.195.18.208
2009/11/4 下午05時53分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 262 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 2177 75.111.28.230
2009/11/4 下午05時52分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 264 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 1876 114.44.149.157
2009/11/4 下午05時51分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 263 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 1568 173.65.207.238
2009/11/4 下午05時50分22秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 268 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 1266 74.128.96.80
2009/11/4 下午05時49分21秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 269 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4852 114.73.47.24
2009/11/4 下午05時48分20秒 CST Low 1491: Gnutella: CONNECT Request (UltraPeer) Peer to Peer Block 264 CCU-TANET... CCU-TP-2400E Segment 3 (A < B) 140.123.233.35 4533 65.25.85.152
56 matching results

點選SQL slam


TippingPoint SMS - RobertSu@sms-server - Events (IPS Events)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
Filter Criteria (FilterName='1456: MS-SQL: Slammer-Sapphire Worm' AND FilterCategory='Application Protection' AND (Action='Permit' OR Action='Block'))
Reset
Filter Details
Filter Name: 1456: MS-SQL: Slammer-Sapphire Worm
Filter No(s):
Filter Category
Application Protection
Exploits
Profile
All
DenyP2P
Filter Severity
Critical Major Minor Low
Action Type
Permit Block Quarantine
Event Comment
All
Comment:
Filter Taxonomy Criteria
Network Criteria
IPS Device / Segment Criteria
Show only the first: 10,000 matching rows. (1-10,000):
Save Save As... Reset All
Real-time Last Hour Start Time: 11/4 下午05時06分27秒 CST End Time: 11/4 下午06時06分27秒 CST
Refresh Cancel
Time Severity Name Category Action Hit Count Profile Device Segment Src. Addr. Src. Port Dst. Addr.
2009/11/4 下午06時06分21秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 2 (A > B) 95.24.111.53 1321 140.123.171.238
2009/11/4 下午06時06分17秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 1 (A > B) 213.23.171.37 2804 163.27.173.154
2009/11/4 下午06時06分16秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 1 (A > B) 92.234.174.54 3117 120.113.46.23
2009/11/4 下午06時06分14秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 1 (A > B) 124.43.168.76 3725 140.125.229.131
2009/11/4 下午06時06分08秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 2 (A > B) 61.47.61.117 1074 140.130.145.55
2009/11/4 下午06時06分08秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 1 (A > B) 113.59.115.3 1208 140.130.152.130
2009/11/4 下午06時06分06秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... CCU-TP-2400E Segment 2 (A > B) 201.208.192.234 1466 120.113.54.118
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 114.37.76.146 1134 210.70.187.178
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 114.138.222.38 21754 163.27.233.76
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 2 (A > B) 200.103.236.115 4436 163.27.94.92
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 195.131.122.97 1512 140.123.181.150
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 220.194.54.149 3138 120.113.173.247
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 69.247.20.174 1057 140.123.38.32
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 2 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 58.248.253.156 1233 140.125.57.9
2009/11/4 下午06時06分01秒 CST Crit... 1456: MS-SQL: Slammer-Sapphire Worm Exploits Block 2 CCU-TANET... YCRC-TP2400E Segment 2 (A > B) 221.130.4.228 4622 140.123.81.19
6,179 matching results

攻擊行為統計

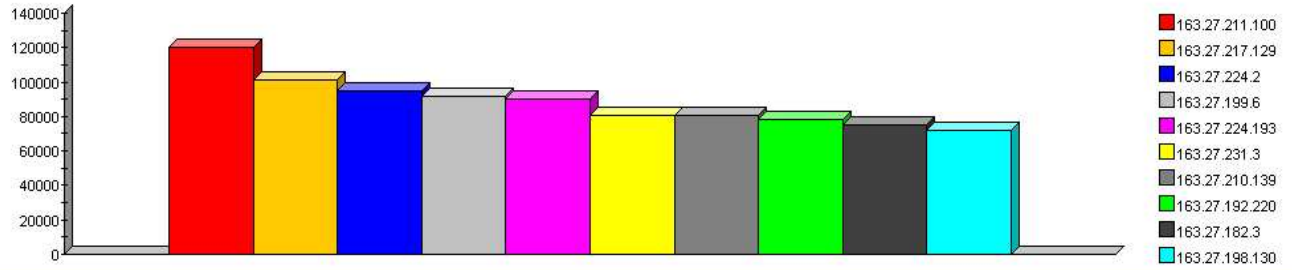

Report Results - Top [sms-server]
Top Attacks
Segment Group: All
Action Type: All
Severity: All
From: 2009/10/1 上午12時00分00秒
To: 2009/10/31 下午11時59分59秒
2E7
1.6E7
1.2E7
8000000
4000000
0
最多的是SQL slam及
SSH login attempt
1456: MS-SQL: Slammer-Sap
5601: SSH: SSH Login Atte
2556: HTTP: HTTP CONNECT
3885: HTTP: PHP File Incl
2965: Spyware: SaveNow/Wh
3867: Spyware: Alexa Brow
2583: Spyware: Hotbar Bro
3139: Spyware: MyWay/MyWe
2289: MS-RPC: DCOM ISyste
4686: HTTP: PHP File Incl
Summary
No. | Filter Name | Severity | Hits
1 | 1456: MS-SQL: Slammer-Sapphire Worm | Critical | 17,636,906
2 | 5601: SSH: SSH Login Attempt | Low | 15,328,860
3 | 2556: HTTP: HTTP CONNECT TCP Tunnel to SMTP port | Major | 32,328
4 | 3885: HTTP: PHP File Include Exploit | Critical | 31,643
5 | 2965: Spyware: SaveNow/WhenU Program Download | Low | 27,606
6 | 3867: Spyware: Alexa Browser Communication | Low | 26,517
7 | 2583: Spyware: Hotbar Browser Communication | Low | 15,779
8 | 3139: Spyware: MyWay/MyWeb/MySearch Search Bar Information Tran... | Low | 9,953
All Details
No. | Filter Name | Severity | Hits | Source IP | Destination IP | Action
1 | 5601: SSH: SSH Login Attempt | Low | 76,373 | 202.57.41.60 | 163.27.211.100 | Permit
2 | 5601: SSH: SSH Login Attempt | Low | 66,343 | 202.57.41.60 | 163.27.210.139 | Permit
3 | 5601: SSH: SSH Login Attempt | Low | 56,477 | 64.27.2.125 | 163.27.215.42 | Permit
4 | 5601: SSH: SSH Login Attempt | Low | 54,424 | 202.57.41.60 | 163.27.240.96 | Permit
5 | 5601: SSH: SSH Login Attempt | Low | 53,071 | 202.57.41.60 | 163.27.217.129 | Permit
6 | 5601: SSH: SSH Login Attempt | Low | 51,368 | 202.57.41.60 | 163.27.192.224 | Permit
7 | 5601: SSH: SSH Login Attempt | Low | 49,088 | 202.57.41.60 | 163.27.207.129 | Permit
8 | 5601: SSH: SSH Login Attempt | Low | 46,305 | 64.27.2.125 | 163.27.5.10 | Permit
9 | 5601: SSH: SSH Login Attempt | Low | 44,674 | 202.57.41.60 | 163.27.199.6 | Permit
10 | 5601: SSH: SSH Login Attempt | Low | 44,587 | 64.27.2.125 | 163.27.231.2 | Permit
Export
Close

被攻擊IP統計

Report Results - Top [sms-server]

Top Destinations

Segment Group: CCU-TANET
Action Type: All
Severity: All
From: 2009/10/1 上午12時00分01秒
To: 2009/10/31 下午11時59分59秒



Summary

No.	Destination IP	Hits
1	163.27.211.100	120,461
2	163.27.217.129	100,865
3	163.27.224.2	94,863
4	163 (163.27.217.129)	91,550
5	163.27.224.193	90,394
6	163.27.231.3	80,833
7	163.27.210.139	80,384
8	163.27.192.220	78,569

All Details

Source IP	Destination IP	Filter	Severity	Action	Hits
202.57.41.60	163.27.211.100	5601: SSH: SSH Login Attempt	Low	Permit	76,373
202.57.41.60	163.27.210.139	5601: SSH: SSH Login Attempt	Low	Permit	66,343
202.57.41.60	163.27.217.129	5601: SSH: SSH Login Attempt	Low	Permit	53,071
202.57.41.60	163.27.199.6	5601: SSH: SSH Login Attempt	Low	Permit	44,674
221.142.226.5	163.27.231.3	5601: SSH: SSH Login Attempt	Low	Permit	43,795
202.57.41.60	163.27.198.130	5601: SSH: SSH Login Attempt	Low	Permit	42,386
202.57.41.60	163.27.224.193	5601: SSH: SSH Login Attempt	Low	Permit	41,477
221.142.226.5	163.27.224.2	5601: SSH: SSH Login Attempt	Low	Permit	40,621
64.27.2.125	163.27.217.129	5601: SSH: SSH Login Attempt	Low	Permit	40,506
221.142.226.5	163.27.192.220	5601: SSH: SSH Login Attempt	Low	Permit	39,541

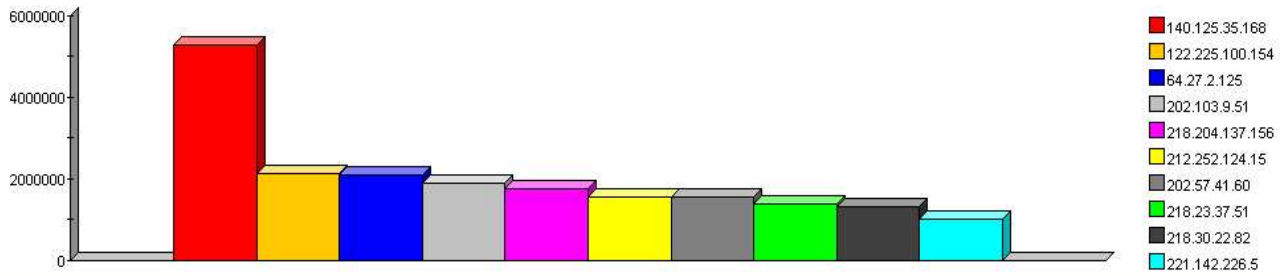
Export Close

攻擊來源統計

Report Results - Top [sms-server]

Top Sources

Segment Group: CCU-TANET
Action Type: All
Severity: All
From: 2009/10/1 上午12時00分01秒
To: 2009/10/31 下午11時59分59秒



Summary

No.	Source IP Address	Hits
1	140.125.35.168	5,277,562
2	122.225.100.154	2,127,543
3	64.27.2.125	2,106,452
4	202.103.9.51	1,903,816
5	218.204.137.156	1,758,230
6	212.252.124.15	1,564,627
7	202.57.41.60	1,546,556
8	218.23.37.51	1,387,201

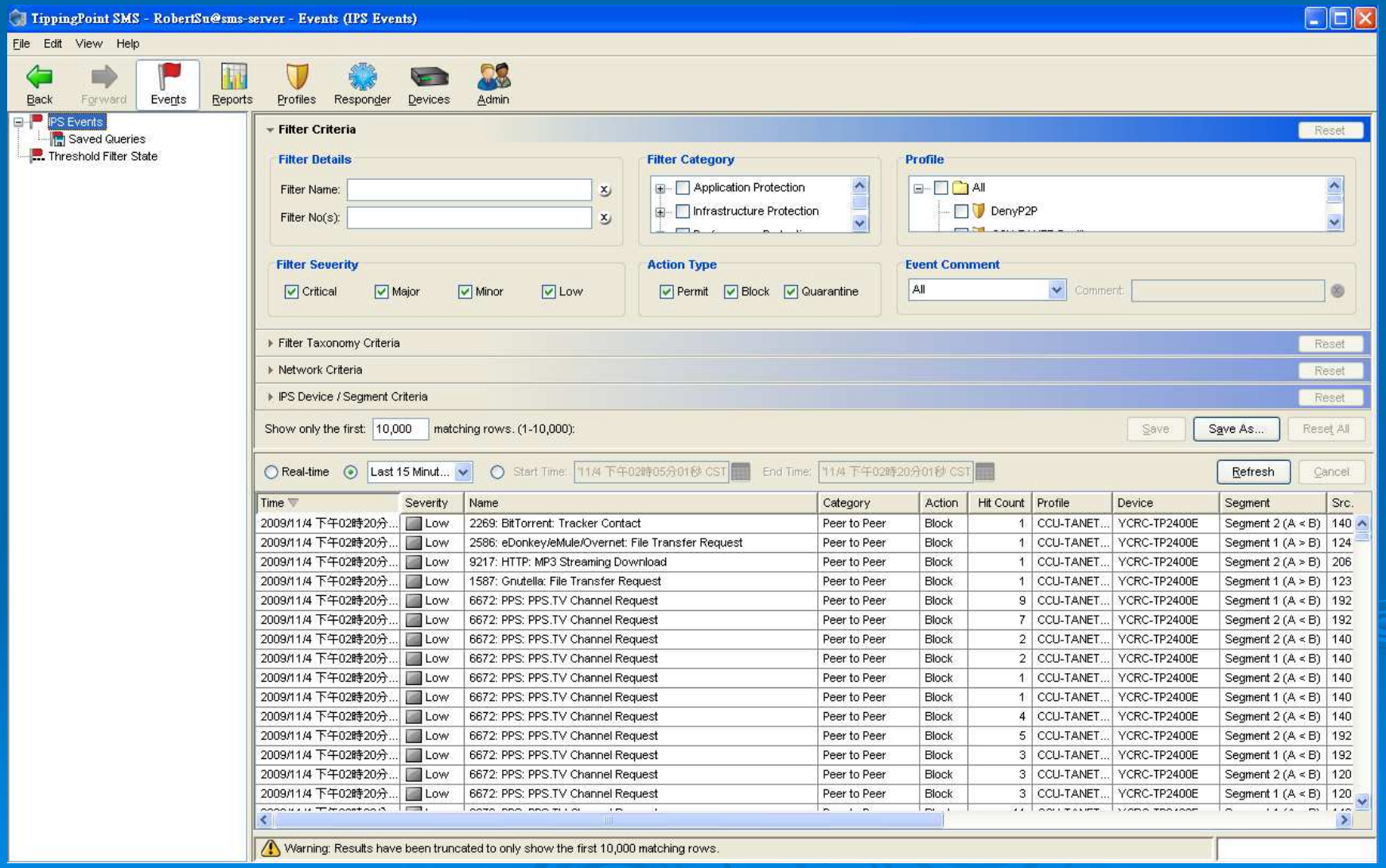
5,277,562

All Details

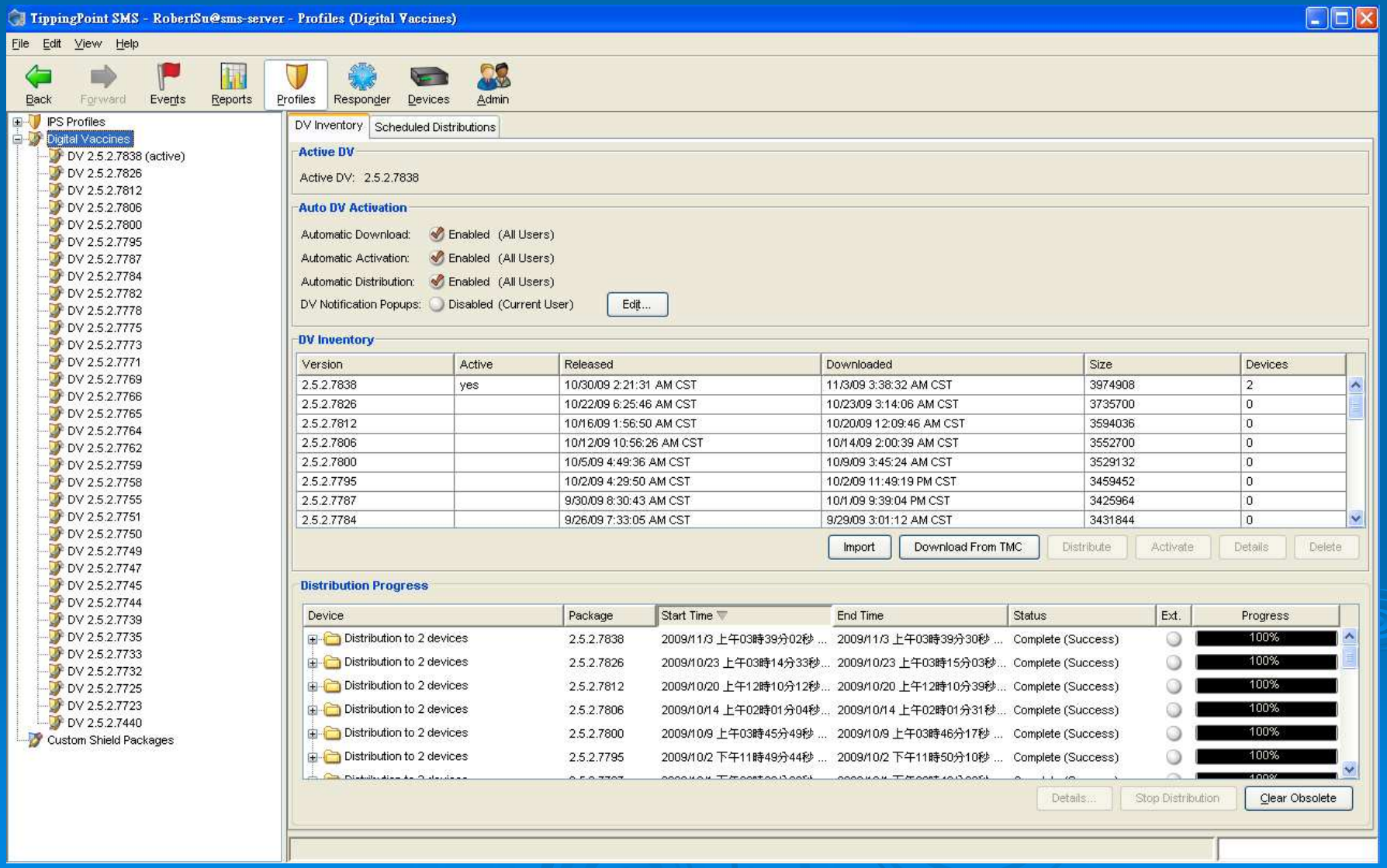
Source IP	Destination IP	Filter	Severity	Action	Hits
202.57.41.60	163.27.211.100	5601: SSH: SSH Login Attempt	Low	Permit	76,373
202.57.41.60	163.27.210.139	5601: SSH: SSH Login Attempt	Low	Permit	66,343
64.27.2.125	163.27.215.42	5601: SSH: SSH Login Attempt	Low	Permit	56,477
202.57.41.60	163.27.240.96	5601: SSH: SSH Login Attempt	Low	Permit	54,424
202.57.41.60	163.27.217.129	5601: SSH: SSH Login Attempt	Low	Permit	53,071
202.57.41.60	163.27.192.224	5601: SSH: SSH Login Attempt	Low	Permit	51,368
202.57.41.60	163.27.207.129	5601: SSH: SSH Login Attempt	Low	Permit	49,088
64.27.2.125	163.27.5.10	5601: SSH: SSH Login Attempt	Low	Permit	46,305
202.57.41.60	163.27.199.6	5601: SSH: SSH Login Attempt	Low	Permit	44,674
64.27.2.125	163.27.231.2	5601: SSH: SSH Login Attempt	Low	Permit	44,587

Export Close

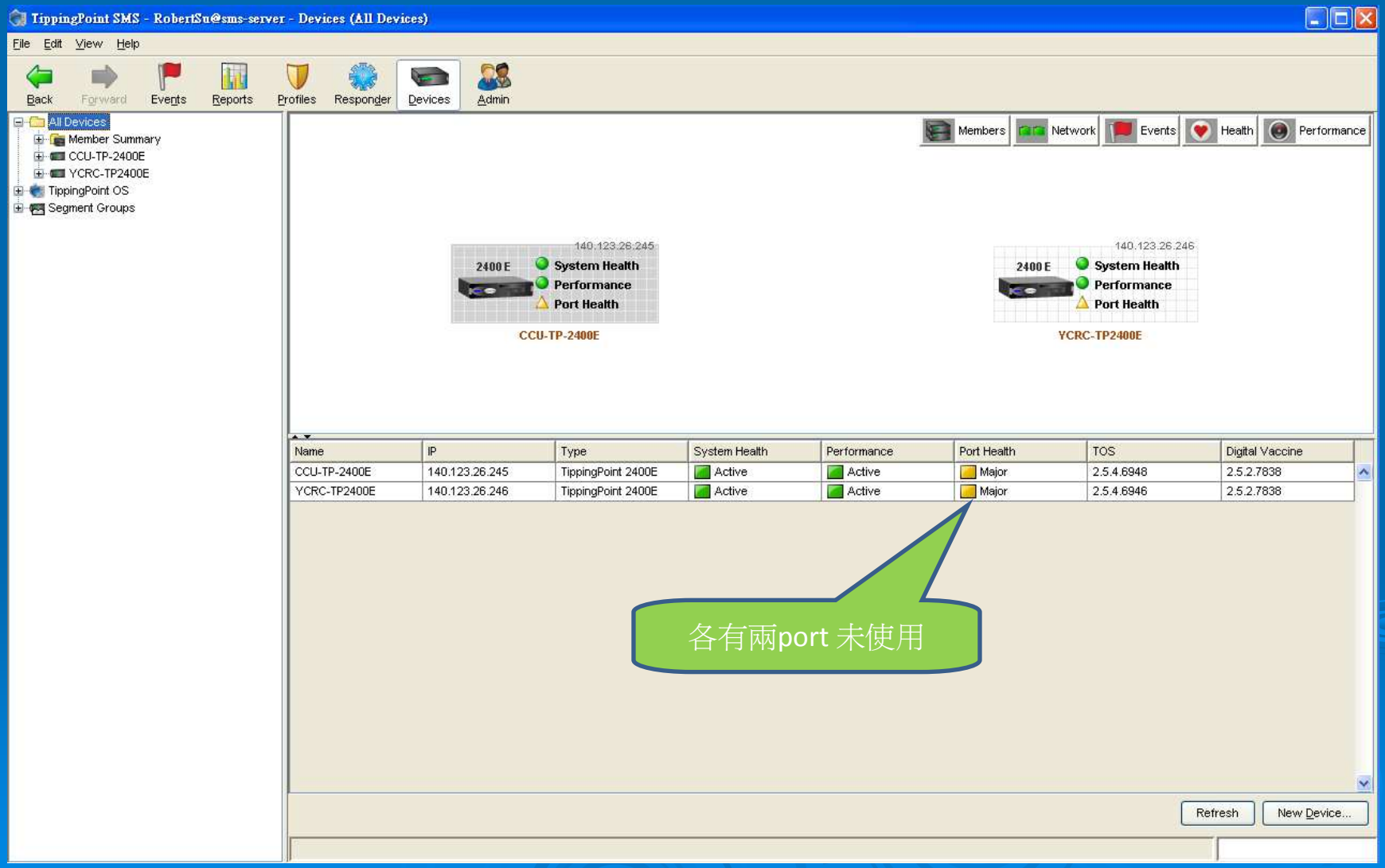
可以針對問題IP查詢


TippingPoint SMS - RobertSu@sms-server - Events (IPS Events)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
IPS Events
Saved Queries
Threshold Filter State
Filter Criteria
Reset
Filter Details
Filter Name:
Filter No(s):
Filter Category
Application Protection
Infrastructure Protection
Profile
All
DenyP2P
Filter Severity
Critical Major Minor Low
Action Type
Permit Block Quarantine
Event Comment
All
Comment:
Filter Taxonomy Criteria
Network Criteria
IPS Device / Segment Criteria
Show only the first: 10,000 matching rows. (1-10,000):
Save Save As... Reset All
Real-time Last 15 Minut... Start Time: 11/4 下午02時05分01秒 CST End Time: 11/4 下午02時20分01秒 CST
Refresh Cancel
Time Severity Name Category Action Hit Count Profile Device Segment Src.
2009/11/4 下午02時20分... Low 2269: BitTorrent: Tracker Contact Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 140
2009/11/4 下午02時20分... Low 2586: eDonkey/eMule/Overnet: File Transfer Request Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 124
2009/11/4 下午02時20分... Low 9217: HTTP: MP3 Streaming Download Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 2 (A > B) 206
2009/11/4 下午02時20分... Low 1587: Gnutella: File Transfer Request Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A > B) 123
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 9 CCU-TANET... YCRC-TP2400E Segment 1 (A < B) 192
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 7 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 192
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 2 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 140
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 2 CCU-TANET... YCRC-TP2400E Segment 1 (A < B) 140
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 140
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 1 CCU-TANET... YCRC-TP2400E Segment 1 (A < B) 140
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 4 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 140
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 5 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 192
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 3 CCU-TANET... YCRC-TP2400E Segment 1 (A < B) 192
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 3 CCU-TANET... YCRC-TP2400E Segment 2 (A < B) 120
2009/11/4 下午02時20分... Low 6672: PPS: PPS.TV Channel Request Peer to Peer Block 3 CCU-TANET... YCRC-TP2400E Segment 1 (A < B) 120
Warning: Results have been truncated to only show the first 10,000 matching rows.

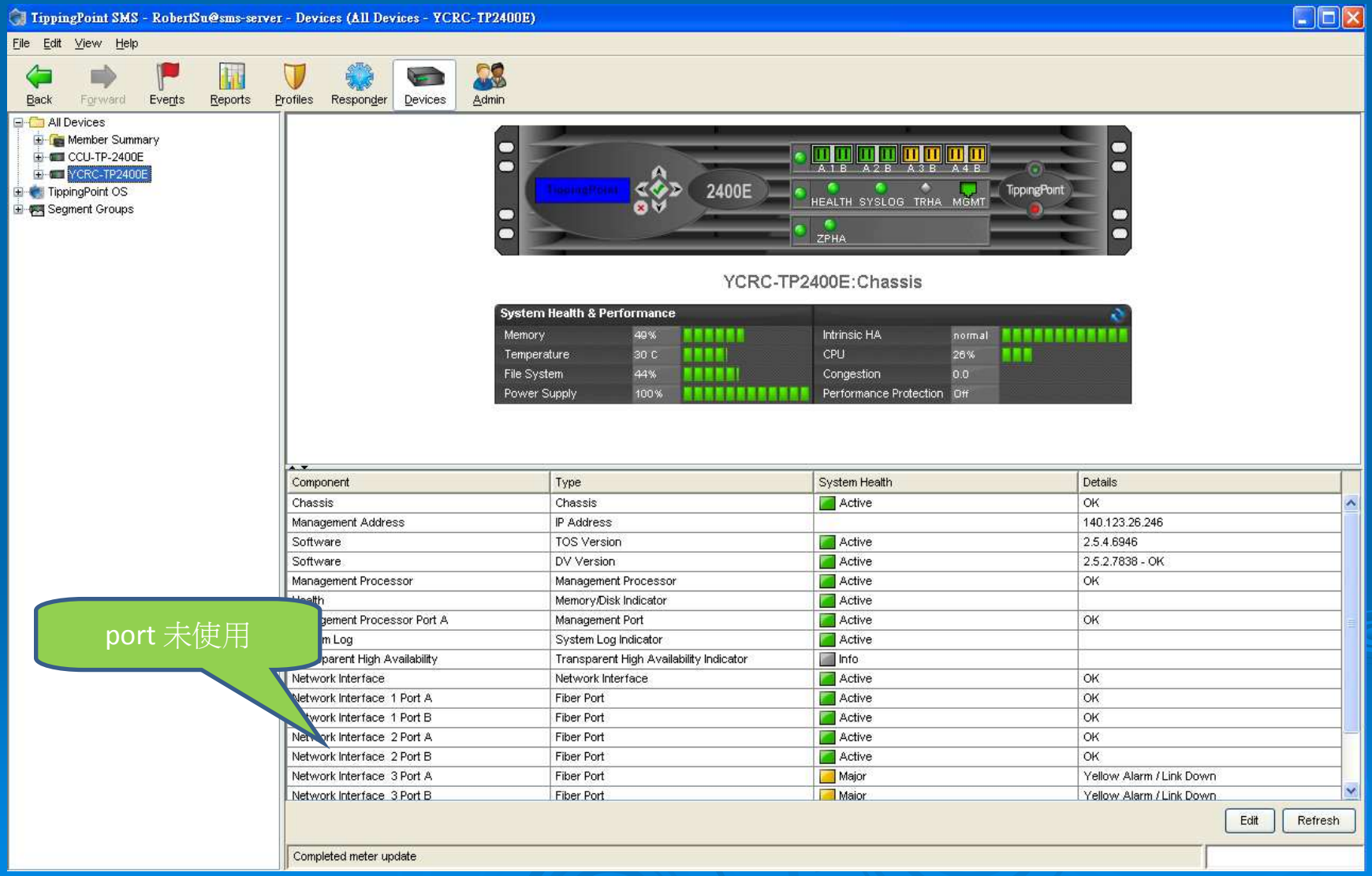
數位疫苗自動更新


TippingPoint SMS - RobertSu@sms-server - Profiles (Digital Vaccines)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
IPS Profiles
Digital Vaccines
DV 2.5.2.7838 (active)
DV 2.5.2.7826
DV 2.5.2.7812
DV 2.5.2.7806
DV 2.5.2.7800
DV 2.5.2.7795
DV 2.5.2.7787
DV 2.5.2.7784
DV 2.5.2.7782
DV 2.5.2.7778
DV 2.5.2.7775
DV 2.5.2.7773
DV 2.5.2.7771
DV 2.5.2.7769
DV 2.5.2.7766
DV 2.5.2.7765
DV 2.5.2.7764
DV 2.5.2.7762
DV 2.5.2.7759
DV 2.5.2.7758
DV 2.5.2.7755
DV 2.5.2.7751
DV 2.5.2.7750
DV 2.5.2.7749
DV 2.5.2.7747
DV 2.5.2.7745
DV 2.5.2.7744
DV 2.5.2.7739
DV 2.5.2.7735
DV 2.5.2.7733
DV 2.5.2.7732
DV 2.5.2.7725
DV 2.5.2.7723
DV 2.5.2.7440
Custom Shield Packages
DV Inventory
Scheduled Distributions
Active DV
Active DV: 2.5.2.7838
Auto DV Activation
Automatic Download: Enabled (All Users)
Automatic Activation: Enabled (All Users)
Automatic Distribution: Enabled (All Users)
DV Notification Popups: Disabled (Current User)
Edit...
DV Inventory
Version Active Released Downloaded Size Devices
2.5.2.7838 yes 10/30/09 2:21:31 AM CST 11/3/09 3:38:32 AM CST 3974908 2
2.5.2.7826 10/22/09 6:25:46 AM CST 10/23/09 3:14:06 AM CST 3735700 0
2.5.2.7812 10/16/09 1:56:50 AM CST 10/20/09 12:09:46 AM CST 3594036 0
2.5.2.7806 10/12/09 10:56:26 AM CST 10/14/09 2:00:39 AM CST 3552700 0
2.5.2.7800 10/5/09 4:49:36 AM CST 10/9/09 3:45:24 AM CST 3529132 0
2.5.2.7795 10/2/09 4:29:50 AM CST 10/2/09 11:49:19 PM CST 3459452 0
2.5.2.7787 9/30/09 8:30:43 AM CST 10/1/09 9:39:04 PM CST 3425964 0
2.5.2.7784 9/26/09 7:33:05 AM CST 9/29/09 3:01:12 AM CST 3431844 0
Import
Download From TMC
Distribute
Activate
Details
Delete
Distribution Progress
Device Package Start Time End Time Status Ext. Progress
Distribution to 2 devices 2.5.2.7838 2009/11/3 上午03時39分02秒 ... 2009/11/3 上午03時39分30秒 ... Complete (Success) 100%
Distribution to 2 devices 2.5.2.7826 2009/10/23 上午03時14分33秒... 2009/10/23 上午03時15分03秒... Complete (Success) 100%
Distribution to 2 devices 2.5.2.7812 2009/10/20 上午12時10分12秒... 2009/10/20 上午12時10分39秒... Complete (Success) 100%
Distribution to 2 devices 2.5.2.7806 2009/10/14 上午02時01分04秒... 2009/10/14 上午02時01分31秒... Complete (Success) 100%
Distribution to 2 devices 2.5.2.7800 2009/10/9 上午03時45分49秒 ... 2009/10/9 上午03時46分17秒 ... Complete (Success) 100%
Distribution to 2 devices 2.5.2.7795 2009/10/2 下午11時49分44秒 ... 2009/10/2 下午11時50分10秒 ... Complete (Success) 100%
Details...
Stop Distribution
Clear Obsolete

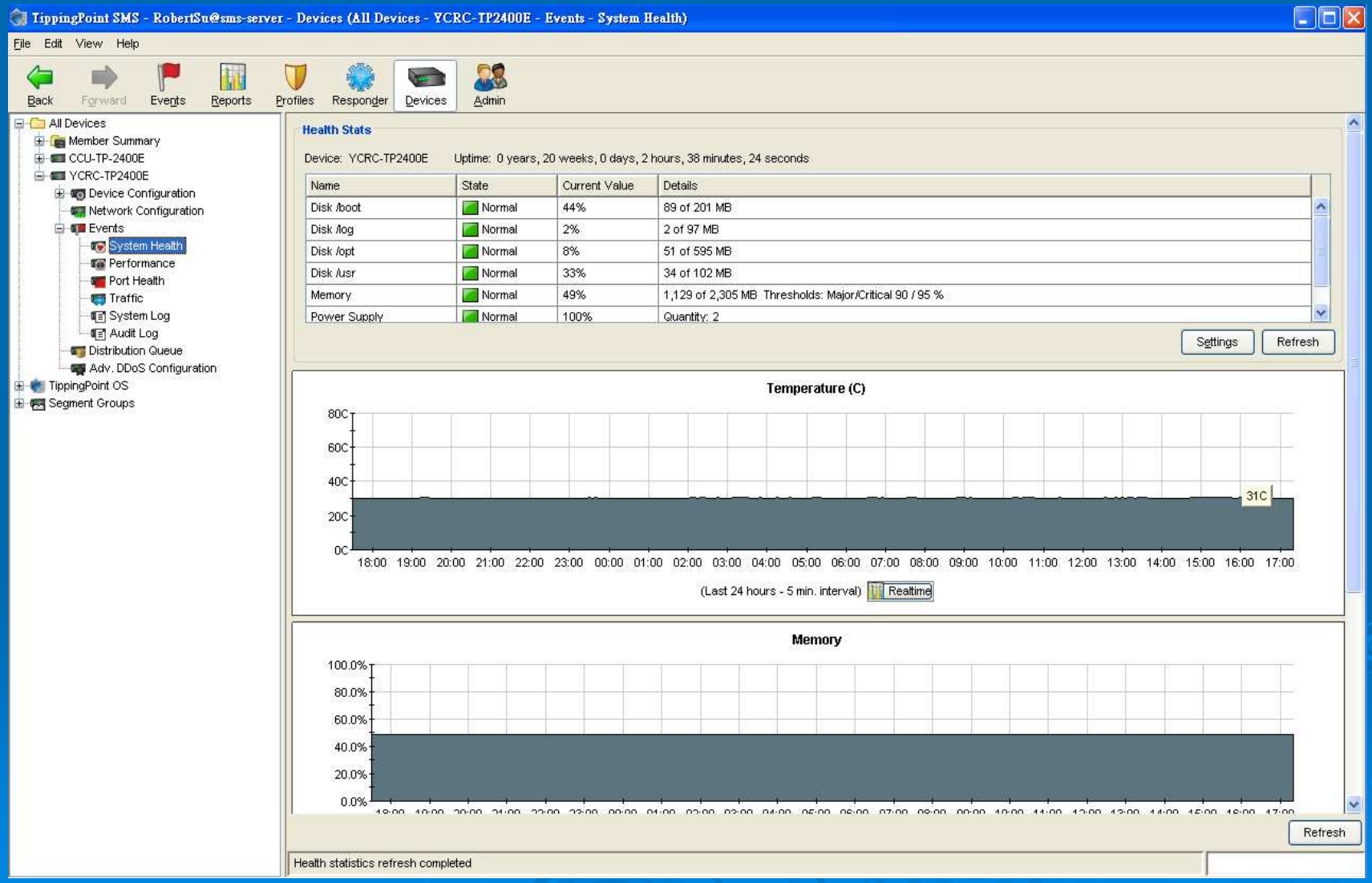
線上監控設備狀態


TippingPoint SMS - RobertSu@sms-server - Devices (All Devices)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
TippingPoint OS
Segment Groups
Members Network Events Health Performance
140.123.26.245
2400 E
System Health
Performance
Port Health
CCU-TP-2400E
140.123.26.246
2400 E
System Health
Performance
Port Health
YCRC-TP2400E
Name IP Type System Health Performance Port Health TOS Digital Vaccine
CCU-TP-2400E 140.123.26.245 TippingPoint 2400E Active Active Major 2.5.4.6948 2.5.2.7838
YCRC-TP2400E 140.123.26.246 TippingPoint 2400E Active Active Major 2.5.4.6946 2.5.2.7838
各有兩port 未使用
Refresh
New Device...

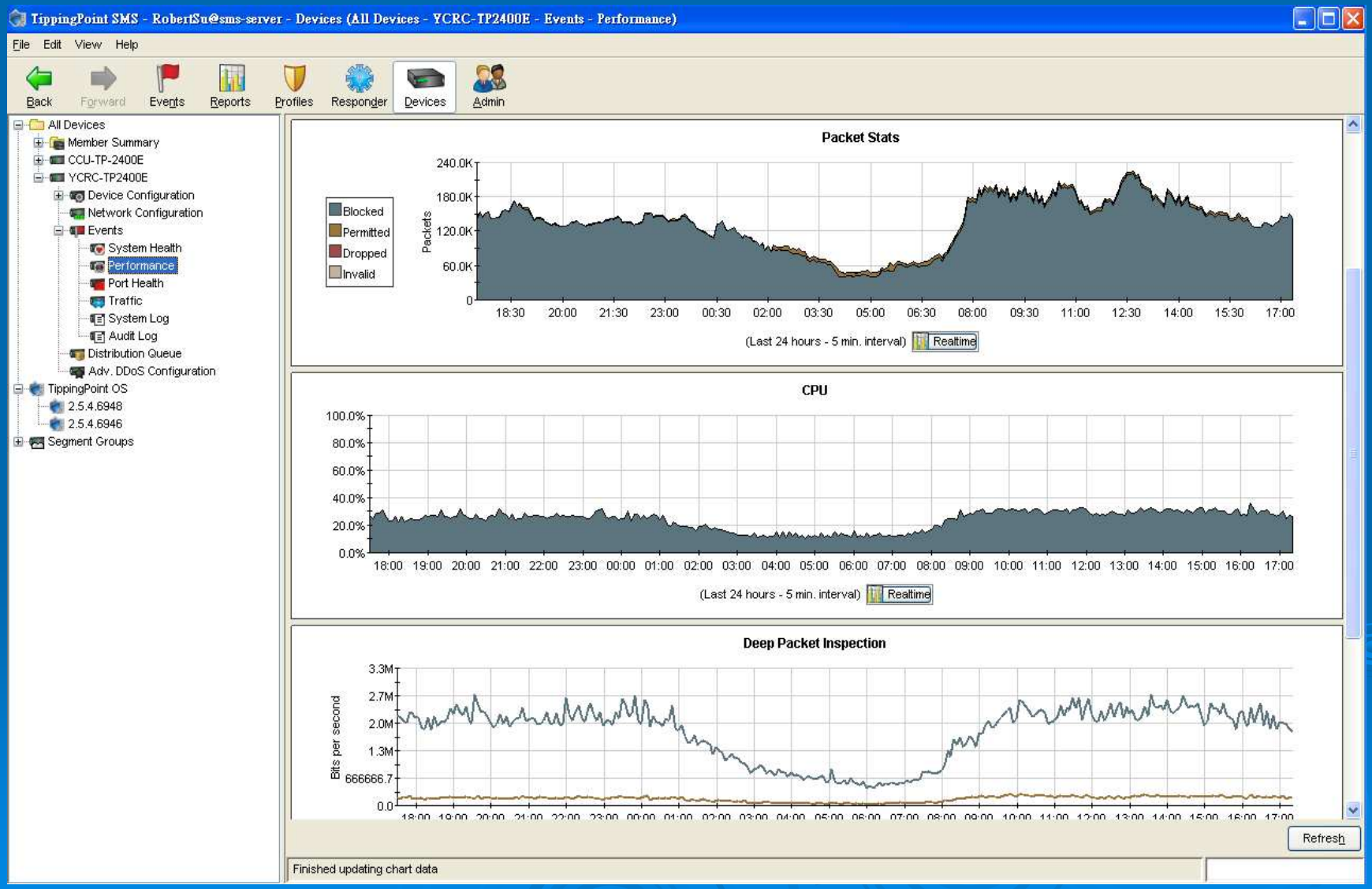
IPS設備狀態


TippingPoint SMS - RobertSu@sms-server - Devices (All Devices - YCRC-TP2400E)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
TippingPoint OS
Segment Groups
2400E
A 1 B A 2 B A 3 B A 4 B
HEALTH SYSLOG TRHA MGMT
ZPHA
TippingPoint
YCRC-TP2400E:Chassis
System Health & Performance
Memory 49%
Temperature 30 C
File System 44%
Power Supply 100%
Intrinsic HA normal
CPU 26%
Congestion 0.0
Performance Protection Off
Component Type System Health Details
Chassis Chassis Active OK
Management Address IP Address 140.123.26.246
Software TOS Version Active 2.5.4.6946
Software DV Version Active 2.5.2.7838 - OK
Management Processor Management Processor Active OK
Memory/Disk Indicator Active
Management Port Active OK
System Log Indicator Active
Transparent High Availability Indicator Info
Network Interface Active OK
Network Interface 1 Port A Fiber Port Active OK
Network Interface 1 Port B Fiber Port Active OK
Network Interface 2 Port A Fiber Port Active OK
Network Interface 2 Port B Fiber Port Active OK
Network Interface 3 Port A Fiber Port Major Yellow Alarm / Link Down
Network Interface 3 Port B Fiber Port Major Yellow Alarm / Link Down
Edit Refresh
Completed meter update
port 未使用

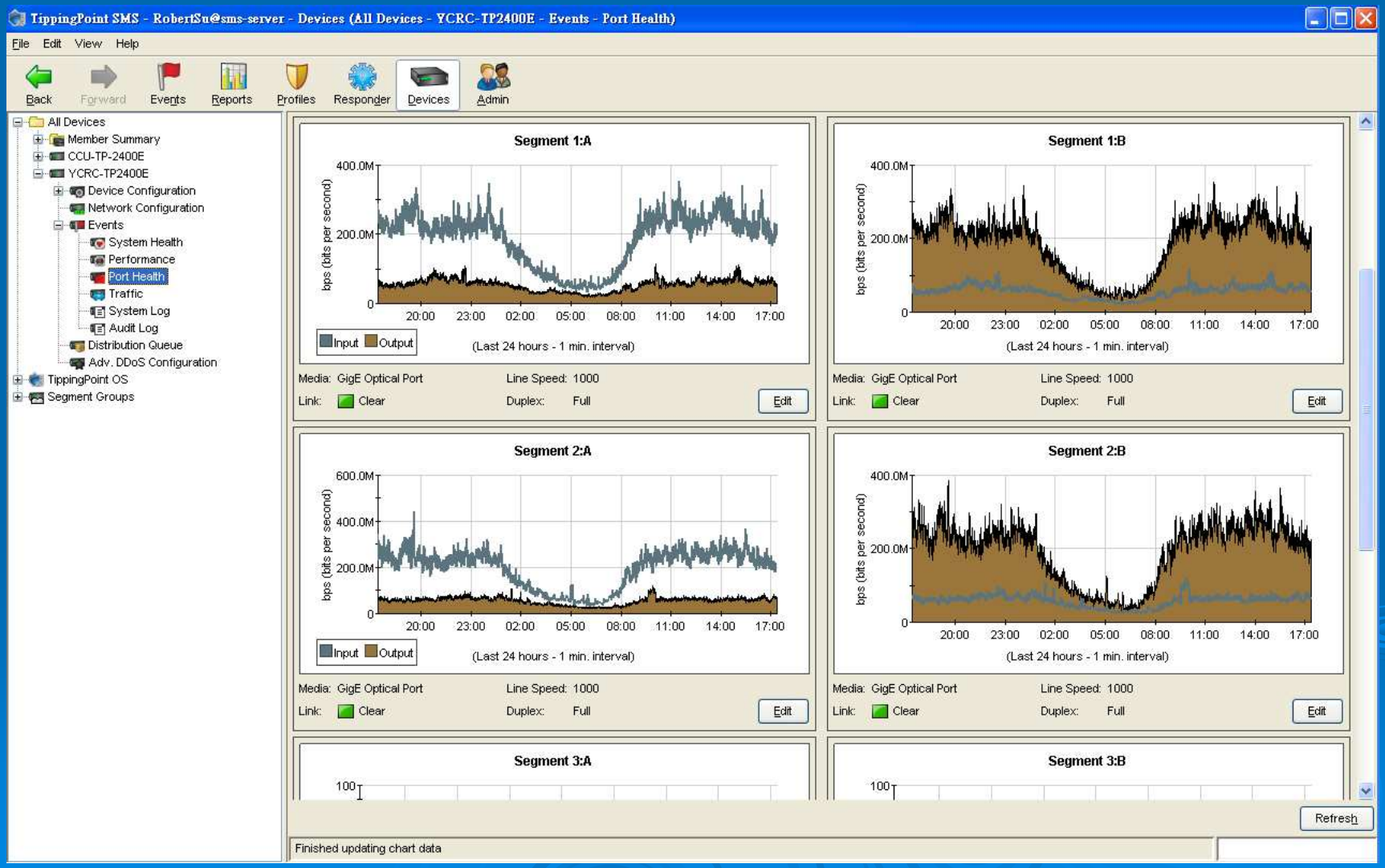
系統的建康狀態


TippingPoint SMS - RobertSu@sms-server - Devices (All Devices - YCRC-TP2400E - Events - System Health)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
Device Configuration
Network Configuration
Events
System Health
Performance
Port Health
Traffic
System Log
Audit Log
Distribution Queue
Adv. DDoS Configuration
TippingPoint OS
Segment Groups
Health Stats
Device: YCRC-TP2400E Uptime: 0 years, 20 weeks, 0 days, 2 hours, 38 minutes, 24 seconds
Name State Current Value Details
Disk /boot Normal 44% 89 of 201 MB
Disk /log Normal 2% 2 of 97 MB
Disk /opt Normal 8% 51 of 595 MB
Disk /usr Normal 33% 34 of 102 MB
Memory Normal 49% 1,129 of 2,305 MB Thresholds: Major/Critical 90 / 95 %
Power Supply Normal 100% Quantity: 2
Settings Refresh
Temperature (C)
80C 60C 40C 20C 0C
31C
18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00
(Last 24 hours - 5 min. interval) Realtime
Memory
100.0% 80.0% 60.0% 40.0% 20.0% 0.0%
Refresh
Health statistics refresh completed

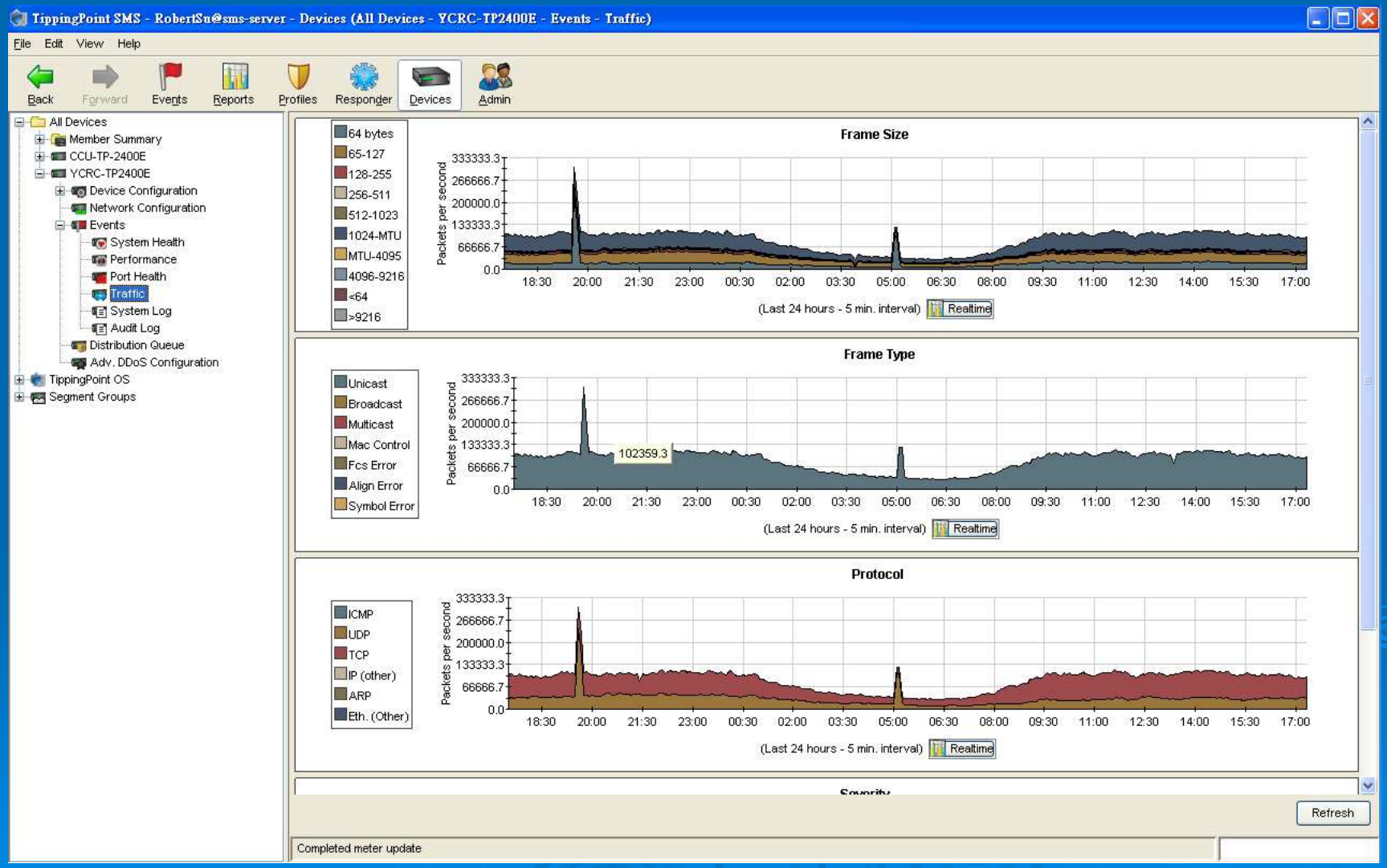
系統效能


TippingPoint SMS - RobertSu@sms-server - Devices (All Devices - YCRC-TP2400E - Events - Performance)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
Device Configuration
Network Configuration
Events
System Health
Performance
Port Health
Traffic
System Log
Audit Log
Distribution Queue
Adv. DDoS Configuration
TippingPoint OS
2.5.4.6948
2.5.4.6946
Segment Groups
Packet Stats
Blocked
Permitted
Dropped
Invalid
Packets
240.0K
180.0K
120.0K
60.0K
0
18:30 20:00 21:30 23:00 00:30 02:00 03:30 05:00 06:30 08:00 09:30 11:00 12:30 14:00 15:30 17:00
(Last 24 hours - 5 min. interval) Realtime
CPU
100.0%
80.0%
60.0%
40.0%
20.0%
0.0%
18:00 19:00 20:00 21:00 22:00 23:00 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00
(Last 24 hours - 5 min. interval) Realtime
Deep Packet Inspection
Bits per second
3.3M
2.7M
2.0M
1.3M
666666.7
0.0
Refresh
Finished updating chart data

Port的建康狀態


TippingPoint SMS - RobertSu@sms-server - Devices (All Devices - YCRC-TP2400E - Events - Port Health)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
Device Configuration
Network Configuration
Events
System Health
Performance
Port Health
Traffic
System Log
Audit Log
Distribution Queue
Adv. DDoS Configuration
TippingPoint OS
Segment Groups
Segment 1:A
Segment 1:B
Segment 2:A
Segment 2:B
Segment 3:A
Segment 3:B
bps (bits per second)
400.0M
200.0M
600.0M
0
20:00 23:00 02:00 05:00 08:00 11:00 14:00 17:00
Input Output
(Last 24 hours - 1 min. interval)
Media: GigE Optical Port
Line Speed: 1000
Link: Clear
Duplex: Full
Edit
Refresh
Finished updating chart data

流量狀態

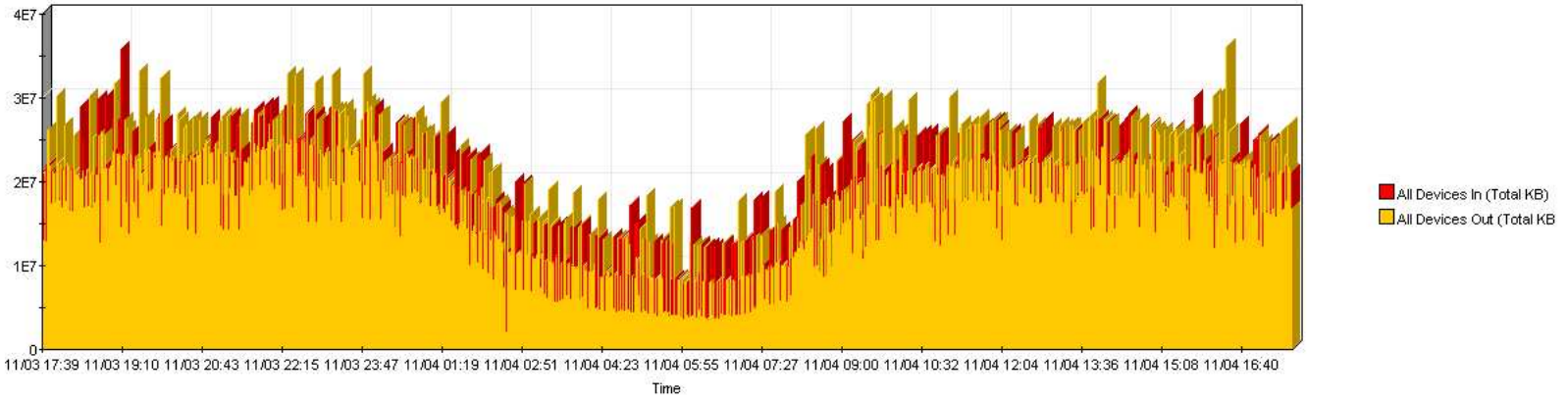

TippingPoint SMS - RobertSu@sms-server - Devices (All Devices - YCRC-TP2400E - Events - Traffic)
File Edit View Help
Back Forward Events Reports Profiles Responder Devices Admin
All Devices
Member Summary
CCU-TP-2400E
YCRC-TP2400E
Device Configuration
Network Configuration
Events
System Health
Performance
Port Health
Traffic
System Log
Audit Log
Distribution Queue
Adv. DDoS Configuration
TippingPoint OS
Segment Groups
Frame Size
64 bytes
65-127
128-255
256-511
512-1023
1024-MTU
MTU-4095
4096-9216
<64
>9216
Packets per second
333333.3
266666.7
200000.0
133333.3
66666.7
0.0
18:30 20:00 21:30 23:00 00:30 02:00 03:30 05:00 06:30 08:00 09:30 11:00 12:30 14:00 15:30 17:00
(Last 24 hours - 5 min. interval) Realtime
Frame Type
Unicast
Broadcast
Multicast
Mac Control
Fcs Error
Align Error
Symbol Error
102359.3
Protocol
ICMP
UDP
TCP
IP (other)
ARP
Eth. (Other)
Refresh
Completed meter update

port流量統計

Report Results - Device Traffic [sms-server]

IPS Physical Port

Traffic Type: Port Statistics:
Time Units: Minutes
Device: All
From: 2009/11/3 下午05時39分39秒
To: 2009/11/4 下午05時39分39秒
Data Units: Bytes



Time	Device	Segment	Port A In	Port B Out	Port B In	Port A Out	All In	All Out
2009/11/3 下午05時39分...	All Devices	All Segments	13,287,491,659	13,112,848,128	7,735,439,274	7,775,818,605	21,022,930,933	20,888,666,733
2009/11/3 下午05時40分...	All Devices	All Segments	9,268,908,688	9,267,233,299	8,021,702,977	3,703,395,779	17,290,611,665	12,970,629,078
2009/11/3 下午05時41分...	All Devices	All Segments	13,101,977,233	17,868,929,775	7,832,070,299	3,311,941,944	20,934,047,532	21,180,871,719
2009/11/3 下午05時42分...	All Devices	All Segments	9,590,663,481	9,361,325,832	3,258,519,418	7,606,445,787	12,849,182,899	16,967,771,619
2009/11/3 下午05時43分...	All Devices	All Segments	9,308,136,443	9,549,422,805	3,272,125,185	3,202,357,224	12,580,261,628	12,751,780,029
2009/11/3 下午05時44分...	All Devices	All Segments	14,490,744,400	18,556,637,988	7,557,333,349	7,613,469,970	22,048,077,749	26,170,107,958
2009/11/3 下午05時45分...	All Devices	All Segments	9,801,155,970	9,708,953,066	7,550,215,263	7,536,260,793	17,351,371,233	17,245,213,859
2009/11/3 下午05時46分...	All Devices	All Segments	14,014,095,367	18,783,934,045	3,282,274,880	7,491,074,075	17,296,370,247	26,275,008,120
2009/11/3 下午05時47分...	All Devices	All Segments	14,606,337,544	14,264,568,584	7,549,242,111	7,598,440,543	22,155,579,655	21,863,009,127
2009/11/3 下午05時48分...	All Devices	All Segments	15,002,852,286	14,558,000,477	3,156,185,062	3,356,853,678	18,159,037,348	17,914,854,155
2009/11/3 下午05時49分...	All Devices	All Segments	13,773,504,827	14,141,315,289	7,545,702,370	3,187,926,946	21,319,207,197	17,329,242,235
2009/11/3 下午05時50分...	All Devices	All Segments	9,264,722,350	13,565,328,672	7,679,366,631	7,674,677,270	16,944,088,981	21,240,005,942
2009/11/3 下午05時51分...	All Devices	All Segments	8,985,584,830	9,216,758,853	3,360,711,383	3,282,241,755	12,346,296,213	12,499,000,608

Export Close