

校園資訊安全監控機制

建置 IDP 入侵偵測防禦系統：

本組於 97 年中於學校網路出口建置一台 IDP(Intrusion Detection Prevention)入侵偵測防禦系統，搭配既有的防火牆來監控與主動阻絕來自校內與校外的網路攻擊或蠕蟲感染。

建置校園網路管理系統：

本組已於校園網路建置一套「校園網路流量監控系統」。用來監控校園網路流量，並且提供全校網路異常流量查詢以及全校網路使用率統計報表。

建置網路流量管制系統：

有鑒於 P2P 下載傳輸流量過大影響一般正常使用者，資訊組將於 97 學年度管制具有 P2P 下載特徵的網路封包。有效管制異常網路流量，以保障正常網路應用。

The screenshot displays the TippingPoint management interface. At the top, it shows the current user as 'SuperUser' and the login time as '2008-12-18 14:04:57 GMT+8'. The main content area is divided into several sections:

- System Status:** A row of seven green status indicators for System Log, Traffic Threshold, Performance, Disk Space, Memory, HA Status, and Power Supply Status.
- Packet Stats:** A table showing network statistics: Received (69.06 G), Blocked (103.04 M), Rate Limited (0), and Dropped (3). A 'Reset' button is present.
- Log Summary:** A table listing various log types and their counts.
- Product Specifications:** A table providing details about the device, including model number, product code, serial number, and version information.

Type	Entries	Events	Functions
Alert Log	17,202	1,297,279	
Audit Log	1,181	n/a	
Block Log	12,395	7,276,968	
System Log	812	n/a	
Packet Trace Log	n/a	n/a	

Model Number	600E
Product Code	TPT-UNITYONE-600
Serial Number	U600F-8811-0709
TOS Version	2.5.3.6933
Digital Vaccine	2.5.2.7611 Up to date
Boot Time	2008-09-19 16:41:14 GMT+8
Up Time	12 weeks, 5 days, 22 hours, 33 minutes, 10 seconds

Blocked Streams

Search for blocked stream(s)

Protocol

Src/Dest Address

Port

Blocked Streams (50 out of 3290)

Refresh

A maximum of 50 streams is shown in the table below. Blocked streams matching a specific IP address and/or port can be queried via the search function.

<input type="checkbox"/>	Protocol	Src/Dest Address	Port	Src/Dest Address	Port	Virtual Segment	Reason
<input type="checkbox"/>	TCP	83.53.171.0	4662	163.15.47.156	3358	1A-1B	2586: eDonkey/eMule/Overnet: File Transfer Request
<input type="checkbox"/>	TCP	81.250.28.1	34930	163.15.47.156	2856	1A-1B	2586: eDonkey/eMule/Overnet: File Transfer Request
<input type="checkbox"/>	TCP	163.15.38.1	1524	77.247.178.9	80	1A-1B	2269: BitTorrent: Tracker Contact
<input type="checkbox"/>	TCP	163.15.38.1	1530	61.220.57.17	28080	1A-1B	2269: BitTorrent: Tracker Contact
<input type="checkbox"/>	TCP	163.15.38.1	1525	77.247.176.132	80	1A-1B	2269: BitTorrent: Tracker Contact
<input type="checkbox"/>	TCP	163.15.38.1	1521	77.247.176.134	80	1A-1B	2269: BitTorrent: Tracker Contact

[功能設定](#)
[服務信箱](#)
[30Min即時報表](#) | [日報表](#) | [週/月歷史報表](#) | [30Min歷史報表](#) | [日歷史報表](#) | [資料查詢](#)

[home]

Wed, Dec 17 2008

< [Prev Report](#) | [Index](#)

流入區網之目的 IP 流量統計

IP 位址	流入封包數	%	流入 (Bytes)	%
Outside=>Inside	18,440,781	100%	10,888,294,839	100%
163.015.040.055	2,233,072		1,033,136,646	
163.015.040.054	1,881,589		963,807,778	
163.015.040.053	1,765,981		856,302,138	
163.015.040.052	1,658,730		847,167,995	
163.015.040.056	1,502,763		815,919,374	
163.015.040.069	539,563		739,834,753	
163.015.040.057	1,429,007		661,656,108	
163.015.040.060	808,854		456,400,722	
163.015.040.059	785,548		378,053,573	
163.015.040.051	820,089		369,642,826	
163.015.040.066	242,807		341,756,102	
163.015.040.058	680,131		286,910,593	
163.015.041.143	956,309		210,502,885	
163.015.039.205	147,889		204,188,863	

流出區網之來源 IP 流量統計

IP 位址	流出封包數	%	流出 (Bytes)	%
Inside=>Outside	19,459,522	100%	13,012,037,277	100%
163.015.046.036	4,551,833		4,852,034,112	
163.015.040.055	1,900,472		1,245,899,983	
163.015.040.054	1,560,178		901,775,341	
163.015.040.052	1,334,750		838,572,884	
163.015.040.053	1,415,025		783,781,009	
163.015.041.143	1,085,211		732,281,910	
163.015.040.057	1,149,165		716,797,342	
163.015.040.056	1,256,173		701,139,888	
163.015.040.051	727,386		509,884,832	
163.015.040.058	584,952		384,392,557	
163.015.040.059	614,479		383,341,433	
163.015.040.060	600,776		296,506,135	
163.015.040.019	130,876		178,871,858	
163.015.040.154	209,205		65,617,958	

完成


網際網路

100%

Home nsisg2000 ?

Up time: 489 days 06:08:39, System time: 2008-12-18 13:17:37 GMT Time Zone 07:00

manually Refresh



NetScreen-ISG 2000

- Home
- Configuration
- Network
- Screening
- Policies
- MCast Policies
- VPNs
- Objects
- Reports
- Wizards
- Help
- Logout

Toggle Menu

Device Information

Hardware Version: 3010(0)
Firmware Version: 5.3.0r3.0 (Firewall+VPN)
Serial Number: 0079122005000351
Host Name: nsisg2000

System Status (Root)

Administrator: netscreen
Current Logins: 1 [Details](#)

Resources Status

CPU:

Memory:

Sessions:

Policies:

[Start from here...](#)

Interface link status: [More...](#)

Name	Zone	Link
mgt	MGT	Up
ethernet1/1	V1-Trust	Down
ethernet1/2	V1-Untrust	Down
ethernet3/1	V1-Trust	Up
ethernet3/2	V1-Untrust	Up

The most recent alarms: [More...](#)

Date/Time	Level	Description
2008-12-18 13:13:28	crit	Fragmented traffic! From 207.171.62.149:...
2008-12-18 13:06:10	crit	SYN and FIN bits! From 122.53.95.6:5141 ...
2008-12-18 13:03:37	crit	Fragmented traffic! From 192.168.1.10:64...
2008-12-18 13:01:06	crit	Fragmented traffic! From 207.171.62.150:...
2008-12-18 12:52:31	crit	Fragmented traffic! From 207.171.62.150:...

The most recent events: [More...](#)

Date/Time	Level	Description
2008-12-18 13:17:36	warn	Admin user "netscreen" logged in for Web...
2008-12-18 13:14:23	info	SNMP: NetScreen device has responded suc...