

桃園區網現況

中央大學 電算中心

呂芳發

2013-10-31



大 網

- ❑ 102教育體系 資安通報演練
- ❑ 資安事件統計
- ❑ 資安管理policy
- ❑ IPv6 HAproxy



102教育體系資安通報演練

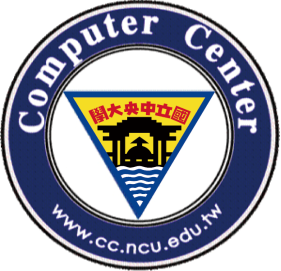
- ❑ 演練時間:10/14到10/18
- ❑ 桃園區網收到38件演練事件
- ❑ 注意事項
 - OID 號碼及密碼是否正確
 - 資安聯絡人資料是否正確, 至少兩位.



102教育體系資安通報演練

□ 資安聯絡人資料

- 7/15原本單一OID分割成五個OID，供每個資安連絡人使用，以加強安全性控管。
- 如果第一聯絡人帳號2.16.886.101.20003.20005.99903
- 第二聯絡人帳號2.16.886.101.20003.20005.99903.1
- 第三聯絡人帳號2.16.886.101.20003.20005.99903.2
- ...
- 密碼：第二聯絡人帳號及第三聯絡人密碼與尚未更新時第一連絡人密碼一樣



102教育體系資安通報演練

評分

各區（縣）網路中心評分標準說明

給分標準 評分項目	1	0
密碼更新率	達 80%	未達 80%
通報完成率	所轄連線單位 於 24 小時內完 成通報的比率 達 80%	所轄連線單位 於 24 小時內完 成通報的比率 未達 80%
審核及時率	所轄連線單位 事件單審核作 業於時限內完 成率達 70%以 上但未達 80%	所轄連線單位 事件單審核作 業於時限內完 成率未達 70%



102教育體系資安通報演練

評分

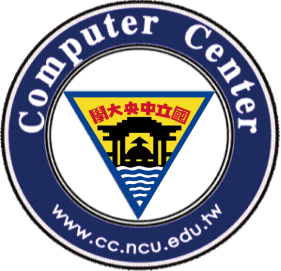
各機構及學校評分標準說明

給分標準 評分項目	2	1	0
通報及時率	4 小時內完成	24 小時內完成	24 小時內未完成
應變及時率	時限內完成	(時限+4 小時) 內完成	未於(時限+4 小時) 內完成
資料正確率	2 位以上資安 聯絡人所有欄 位資料填寫完 整	填寫 2 位以上 資安聯絡人， 但僅一位資安 聯絡人所有欄 位資料填寫完 整	1. 未填寫資安 聯絡人 2. 資安聯絡人 資料資料均不 完整



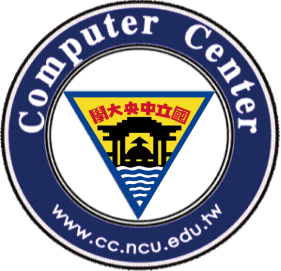
資安事件統計(1)

< << >> >				
連線單位	平均通報處理時間	平均應變處理時間	平均全部處理時間	資安事件數
國立中央大學	01:47:18	25:37:31	27:24:49	111
私立元智大學	03:21:49	00:00:00	03:21:49	90
中原大學	00:29:06	00:03:03	00:32:10	75
開南大學	00:46:10	00:00:00	00:46:10	49
萬能科技大學	00:30:33	00:00:00	00:30:33	36
健行科技大學	00:32:59	07:12:44	07:45:43	31
私立銘傳大學(桃園校區)	14:17:26	00:00:00	14:17:26	23
國立體育大學	03:02:28	00:00:00	03:02:28	11
中央區網中心	00:32:06	00:00:00	00:32:06	9
國防大學	12:58:21	00:00:00	12:58:21	8
中央警察大學	01:00:26	00:00:00	01:00:26	8
國立桃園高級農工職業學校	02:08:46	00:00:00	02:08:46	8
新生醫護管理專科學校	02:47:55	02:11:44	04:59:39	7
桃園縣私立清華高級中學	04:14:59	00:00:00	04:14:59	7
陸軍專科學校	29:41:33	00:00:00	29:41:33	5
財團法人桃園創新技術學院	00:33:22	18:04:21	18:37:43	4
桃園縣私立大華高級中學	00:10:53	50:13:58	50:24:51	4
國立武陵高級中學	00:25:24	00:00:00	00:25:25	4
桃園縣私立啟英高級中學	01:44:18	01:49:36	03:33:55	4
國立桃園高級中學	04:38:47	08:02:05	12:40:52	3
Page 1/2				
二級單位				
平均通報審核時間	平均應變審核時間			
01:27:02	00:00:00			



資安事件統計(2)

<<>>				
連線單位	平均通報處理時間	平均應變處理時間	平均全部處理時間	資安事件數
桃園縣私立振聲高級中學	06:44:19	00:00:00	06:44:19	3
國立龍潭高級農工職業學校	01:11:07	00:00:00	01:11:07	2
國立桃園啟智學校	03:24:23	00:00:00	03:24:23	1
桃園縣私立新興高級中學	00:28:46	00:00:00	00:28:46	1
國立楊梅高級中學	00:24:31	00:00:00	00:24:31	1
桃園縣私立成功高級工商職業學校	00:20:13	00:00:00	00:20:13	1
國立內壢高級中學	00:14:42	00:44:26	00:59:08	1
國立中壢高級商業職業學校	00:00:00	00:00:00	00:00:00	1
桃園縣私立六和高級中學	01:09:51	00:00:00	01:09:51	1
桃園縣私立永平高級工商職業學校	00:11:36	00:00:00	00:11:36	1
Page 2/2				
二級單位				
平均通報審核時間	平均應變審核時間			
01:27:02	00:00:00			

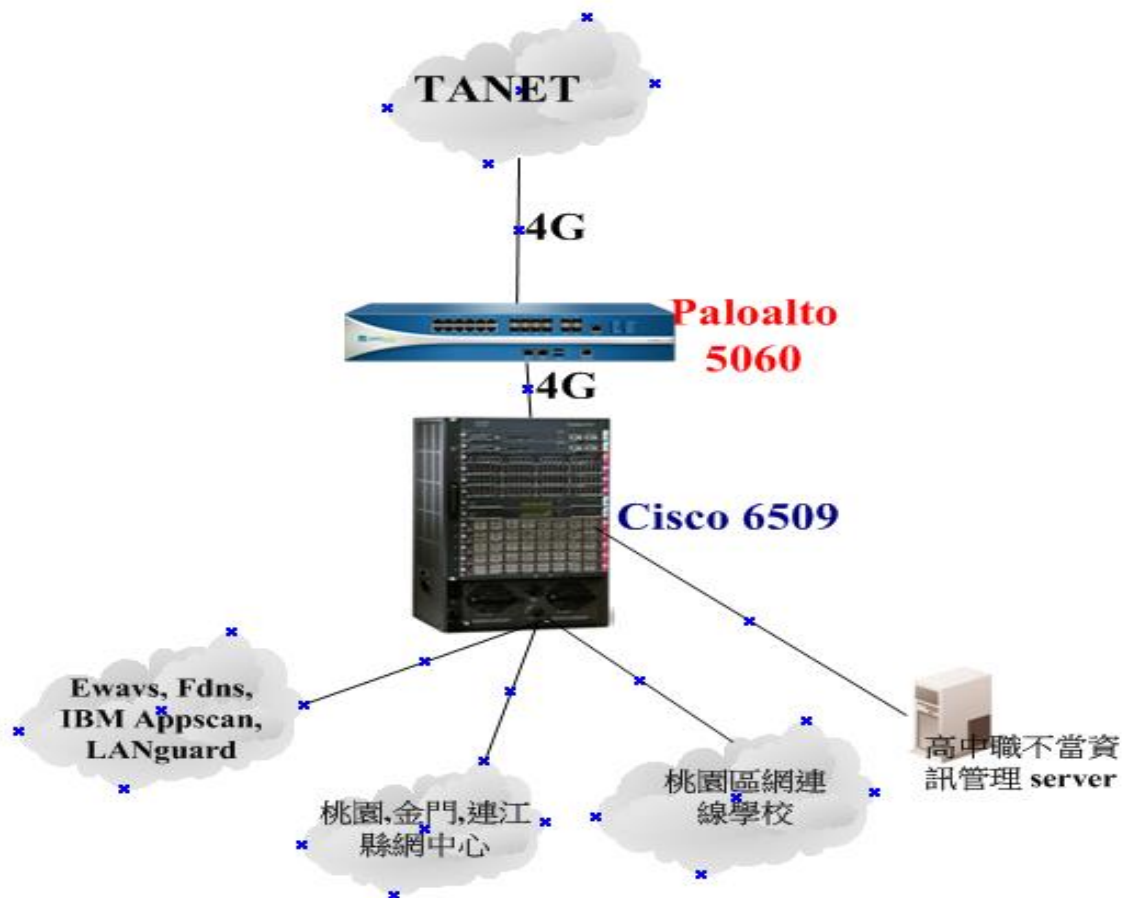


資安事件統計(3)

今年各月份資安事件

1	96
2	76
3	116
4	83
5	46
6	49
7	16
8	11
9	6
10	12

資安設備架構



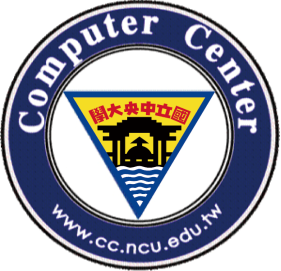


❑ Paloalto5060 Applications and Threats 特徵碼
有問題，暫時回復上一版本



資安設備問題

- 6/24 確認BT應用程式的Session相關參數，會造成Session table被填滿，所以造成連線異常
- 7/2 正確的Applications and Threats 特徵碼 release 出來
- 7/4 Paloalto5060 更新Applications and Threats 特徵碼



資安管理policy

	Severity	Threat/Content Name	ID	Threat/Content Type	Count
1	CRITICAL	ZeroAccess.Gen Command and Control Traffic	132...	spyware	37.6 K
2	HIGH	MAIL: User Login Brute-force Attempt	400...	vulnerability	8.2 K
3	LOW	Sipvicious.sundayddr User-Agent Traffic	132...	spyware	2.3 K
4	CRITICAL	Win32.Conficker.C p2p	125...	spyware	1.5 K
5	CRITICAL	Microsoft SQL Server Stack Overflow Vulnerability	300...	vulnerability	855
6	LOW	Sipvicious.Gen User-Agent Traffic	132...	spyware	703
7	HIGH	SSL Renegotiation Denial of Service Brute-force	400...	vulnerability	668
8	LOW	Morto RDP Request Traffic	132...	spyware	458
9	CRITICAL	Morto DNS Request Traffic	131...	spyware	243
10	MEDIUM	Suspicious user-agent strings	100...	spyware	206
11	MEDIUM	Suspicious User-Agent Traffic	100...	spyware	143
12	MEDIUM	Microsoft Internet Explorer HTTPS Proxy Information Disclosure Vulnerability	312...	vulnerability	88
13	MEDIUM	DNS ANY Queries Brute-force DOS Attack	400...	vulnerability	86
14	CRITICAL	IMDDOS.Gen Command And Control Traffic	131...	spyware	85
15	HIGH	FTP: login Brute-force attempt	400...	vulnerability	82
16	CRITICAL	Bot: Mariposa Command and Control	126...	spyware	80
17	HIGH	Microsoft Windows win.ini access attempt	308...	vulnerability	60
18	CRITICAL	Pushdo.Gen Denial of Service Traffic	133...	spyware	52
19	HIGH	MS-RDP Brute-force Attempt	400...	vulnerability	51
20	MEDIUM	Malware/Win32.emogen.ckl	228...	virus	48
21	MEDIUM	Trojan/Win32.renos.glft	219...	virus	46
22	MEDIUM	Trojan-Downloader/Win32.agent.dhxmu	226...	virus	39
23	MEDIUM	Nsanti User-Agent Traffic	100...	spyware	32
24	HIGH	Worm.Brontok.C	125...	spyware	30
25	MEDIUM	HTTP SQL Injection Attempt	305...	vulnerability	30






資安管理policy

Anti-Spyware Profile

Name:

Description:

Rules | Exceptions

Ena...	Id	Threat Name	Rule	Category	Severity	Action	Packet Capture ▼
<input type="checkbox"/>		and Control	critical			(drop-all-packets)	
<input checked="" type="checkbox"/>	13118	Morto DNS Request Traffic		net-worm	critical	block-ip (source,30)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13195	IMDDOS.Gen Command And Control Traffic		botnet	critical	block-ip (source,90)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13235	ZeroAccess.Gen Command and Control Traffic		botnet	critical	block-ip (source,3...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13272	Sipvicious.Gen User-Agent Traffic		spyware	low	block-ip (source,1...	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13274	Morto RDP Request Traffic		net-worm	low	block-ip (source,90)	<input type="checkbox"/>
<input checked="" type="checkbox"/>	13301	Pushdo.Gen Denial of Service Traffic		botnet	critical	block-ip (source,60)	<input type="checkbox"/>

☐ Show all signatures

Page of 1 | Displaying 1 - 8/ 8 threats (Selected 8)

OK **Cancel**



資安管理policy

Vulnerability Protection Profile

NameDNSANYQueriesDOS_Attack-reset

Description

Rules

Exceptions

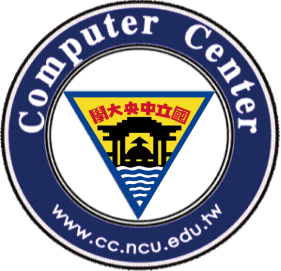
Ena...	Id	Threat Name	Rule ▼	CVE	Vendor ID	Host	Category	Severity	Action	Packet Capture	
<input checked="" type="checkbox"/>	30190	SLMail POP3 Server PASS Command Parsing Buffer Overflow Vulnerability		CVE-2003-0264		server	code-execution	high	drop-all-packets	<input type="checkbox"/>	▲
<input checked="" type="checkbox"/>	40001	FTP: login Brute-force attempt				server	brute-force	high	drop-all-packets	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40007	MAIL: User Login Brute-force Attempt				server	brute-force	high	block-ip (source,30)	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40008	MySQL Authentication Brute-force Attempt				server	brute-force	high	drop-all-packets	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40010	Microsoft SQL Server User Authentication Brute-force Attempt				server	brute-force	high	drop-all-packets	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40015	SSH User Authentication Brute-force Attempt				server	brute-force	high	block-ip (source,180)	<input type="checkbox"/>	≡
<input checked="" type="checkbox"/>	40016	SIP INVITE Method Request Flood Attempt				server	brute-force	high	block-ip (source,60)	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40021	MS-RDP Brute-force Attempt				server	brute-force	high	drop-all-packets	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40031	HTTP Unauthorized Brute-force Attack				server	brute-force	high	reset-both	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	40033	DNS ANY Queries Brute-force DOS Attack				server	brute-force	medium	block-ip (source,30)	<input type="checkbox"/>	▼

☐ Show all signatures

Page 1 of 1 | Displaying 1 - 11/ 11 threats (Selected 11)

OK

Cancel



IPv6 HAproxy

□ HAProxy

- The Reliable, High Performance TCP/HTTP Load Balancer <http://haproxy.1wt.eu/>
- 透過 HAProxy 將 IPv6 的連線轉到 IPv4 only 的 server 上

□ 限制

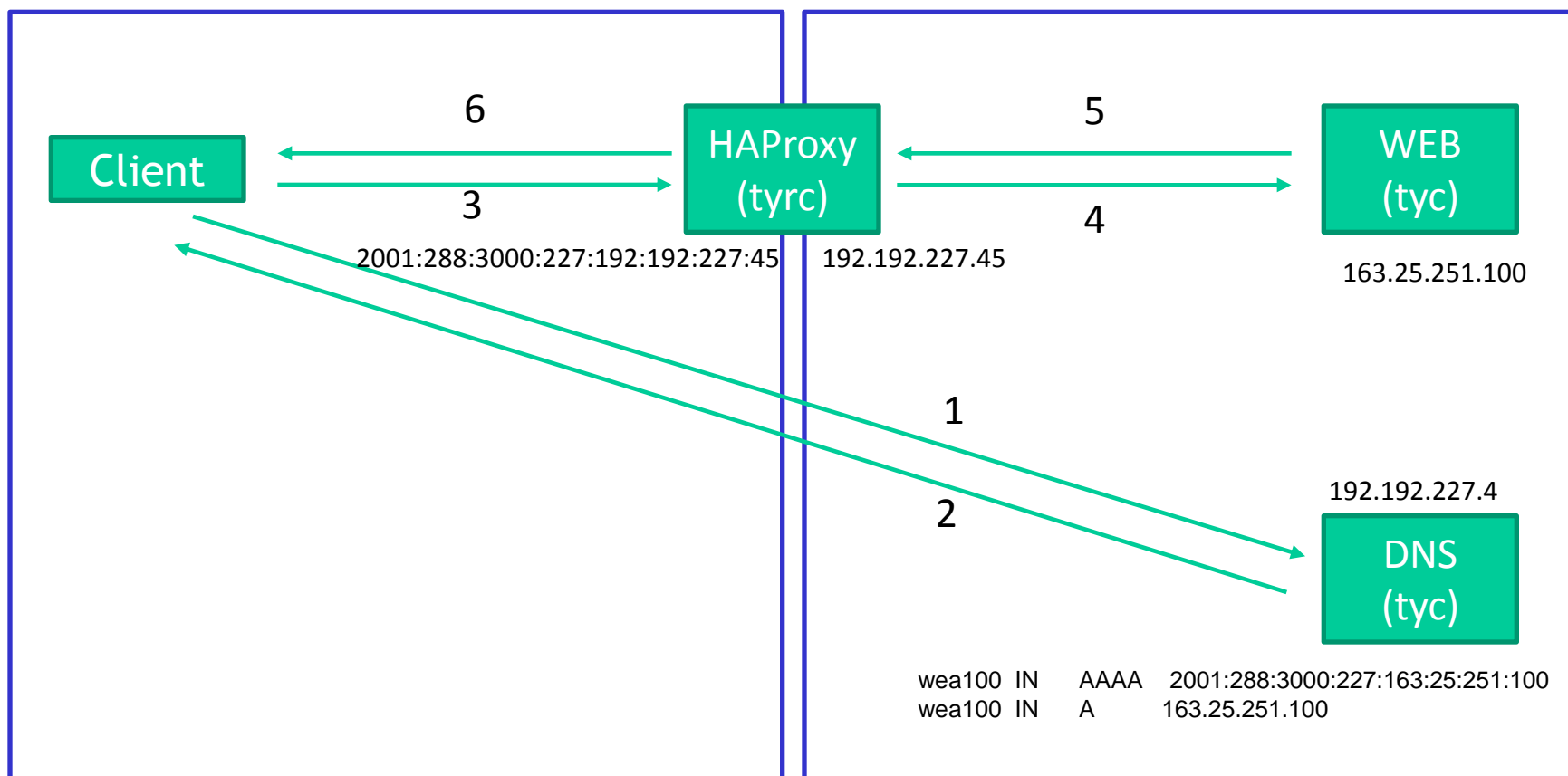
- IPv4 only 環境下的 DNS server 必須支援 IPv6
- 必須有一個已支援 dual-stack 的第三方



IPv6 HAproxy

IPv4 / IPv6 Dual- Stack

IPv4 Only





IPv6 HAproxy

❑ CentOS 若無haproxy套件，需新增套件

➤ CentOS/RHEL 5 , 32 bit:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/5/i386/epel-release-5-4.noarch.rpm
```

➤ CentOS/RHEL 5 , 64 bit:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/5/x86_64/epel-release-5-4.noarch.rpm
```

➤ CentOS/RHEL 6 , 32 bit:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/i386/epel-release-6-8.noarch.rpm
```

➤ CentOS/RHEL 6 , 64 bit:

```
rpm -Uvh http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```



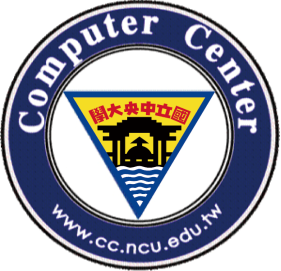
IPv6 HAproxy

□ 新增 IPv6 IP address

➤ 1:1 轉換

➤ `ip -6 address add 2001:288:3000:227:192:192:227:244/64 dev eth0`

➤ 若設定多筆轉換，需逐筆新增，並寫入/etc/rc.local
以便開機時自動載入設定



IPv6 HAproxy

- ❑ yum安裝 HAProxy

```
yum install haproxy
```

- ❑ 設定 haproxy.cfg

```
vi /etc/haproxy/haproxy.cfg
```

- ❑ 設定http proxy功能，增加以下4行(以weal00.tyc.edu.tw為例)

```
listen weal00.tyc.edu.tw 2001:288:3000:227:163:25:251:100:80
```

```
mode http
```

```
option forwardfor
```

```
server weal00.tyc.edu.tw 163.25.251.100:80
```

- ❑ 重開HAProxy

```
/etc/init.d/haproxy restart
```



Computer Center, National Central University.



Thank You!