

Windows系統 防護工具

成大計網中心

楊峻榮

2004/5/20

大綱

- ◆ 以系統內建或freeware或全校授權為主
- ◆ 同一安全邊界無須使用兩種以上相同的防護措施
- ◆ 防毒軟體：officescan client
- ◆ 系統漏洞修補：Auto update
- ◆ PC防火牆：XP內建防火牆，ZoneAlarm
- ◆ 連線監視軟體：Active port
- ◆ 弱點評估工具：Microsoft Baseline Security Analyze

個人防毒軟體 OfficeScan Client







- ◆ Client Server 架構，連至Server安裝並於Server上註冊。
- ◆ 只提供防毒功能（含即時，手動及mail掃描），不提供防火牆功能。
- ◆ Server有新病毒碼時，主動通知Client更新。
- ◆ Client開機時，也會至Server核對是否有新病毒碼更新。
- ◆ 虛擬IP或是浮動IP使用行動模式。
- ◆ 手動更新也可連至趨勢公司更新。
- ◆ 使用防火牆時須開啟ICMP echo/request，方可自動更新病毒碼。
- ◆ 安裝時需以Administrator或該群組登入，並以IE4.0以上版本，連至<http://140.116.6.10/officescan/clientinstall>
- ◆ 解安裝出現問題時，可下載ofcntcln.exe執行即可。

OfficeScan一般模式之圖示

圖示	說明	即時掃瞄	手動和預約掃瞄
	一般用戶端	已啓動	已啓動
	病毒碼檔案已過期	已啓動	已啓動
	正在執行立即掃瞄、手動掃瞄、或預約掃瞄	已啓動	已啓動
	即時掃瞄已關閉	已關閉	已啓動
	即時掃瞄已關閉，而且病毒碼檔案已過期	已關閉	已啓動
	即時掃瞄服務程式未執行	已關閉	已關閉
	即時掃瞄服務程式未執行，而且病毒碼檔案已過期	已關閉	已關閉
	與伺服器中斷連線	已啓動	已啓動
	與伺服器連線已中斷，而且病毒碼檔案已過期	已啓動	已啓動

OfficeScan之行動模式

- ◆ 非使用固定IP及長時間斷線者。
- ◆ 雖Server已設定行動模式Client可自動更新，但最好還是Client端固定時間執行[立即更新]。
- ◆ 行動模式圖示：

圖示	說明	即時掃描	手動和預約掃描
	行動用戶端	已啓動	已啓動
	即時掃描已關閉	已關閉	已啓動
	病毒碼檔案已過期	已啓動	已啓動
	即時掃描已關閉，而且病毒碼檔案已過期	已關閉	已啓動
	即時掃描服務程式未執行	已關閉	已關閉
	即時掃描服務程式未執行，而且病毒碼檔案已過期	已關閉	已關閉

漏洞修補

- ◆ 可直接執行開始／Windows Update(Windows 2000)或開始／程式集／Windows Update(Windows XP)。
- ◆ Windows Update也可設定讓PC自動下載及安裝(Auto Update)
- ◆ Windows Update網址：
<http://v4.windowsupdate.microsoft.com/zhtw/default.asp>
- ◆ Office Update網址：
<http://office.microsoft.com/officeupdate/default.aspx>
- ◆ 某些patch有其request，也就是須先安裝某些Patch或Services pack。某些patch是分離項目，也就是安裝此Patch後必須重開機再安裝其他Patch。故詳閱其列表說明（點選[掃描更新檔項目]後）。
- ◆ Windows Update主要是針對其作業系統之修正及改進，故不侷限在安全性修正，所以主要針對[重大更新及Service Pack]項目。

Windows Update

The screenshot shows the Microsoft Windows Update website in Chinese. The browser window title is "Microsoft Windows Update - Microsoft Internet Explorer". The address bar shows the URL "http://v4.windowsupdate.microsoft.com/zh-tw/default.asp". The page header includes the Microsoft logo and "Windows Update" text. The main content area features a blue header with "歡迎使用 Windows Update" and a sub-header "為您的電腦作業系統、軟體和硬體取得最新的更新檔。". Below this, there is a section titled "掃描更新檔項目" with a green arrow icon. A "注意" (Note) section states that Windows Update does not collect personal information. A prominent warning box with a yellow triangle icon is titled "如何保護您自己免於 Sasser 蠕蟲與其他變種的攻擊" (How to protect yourself from Sasser worm and other variants). It lists updates for Windows 2000 and Windows XP. The footer contains copyright information for Microsoft Corporation and navigation links.

Microsoft Windows Update - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 保護

網址(地址) http://v4.windowsupdate.microsoft.com/zh-tw/default.asp 移至 連結

Microsoft Windows Update

產品資訊 | 技術支援 | 搜尋 | 台灣微軟

Microsoft

首頁 | Windows Catalog | Windows 系列 | Office Update | 全球的 Windows Update

歡迎使用 Windows Update

為您的電腦作業系統、軟體和硬體取得最新的更新檔。

Windows Update 會掃描您的電腦，並提供一個針對您量身訂做的更新檔選擇。

[掃描更新檔項目](#)

注意 Windows Update 不會從您的電腦蒐集任何形式的個人資料。
[請閱讀我們的隱私權聲明](#)

如何保護您自己免於 Sasser 蠕蟲與其他變種的攻擊

若您的電腦執行下列其中一種作業系統，則可以安裝適當的更新，協助保護您的電腦免於 Sasser 蠕蟲與其他變種的攻擊：

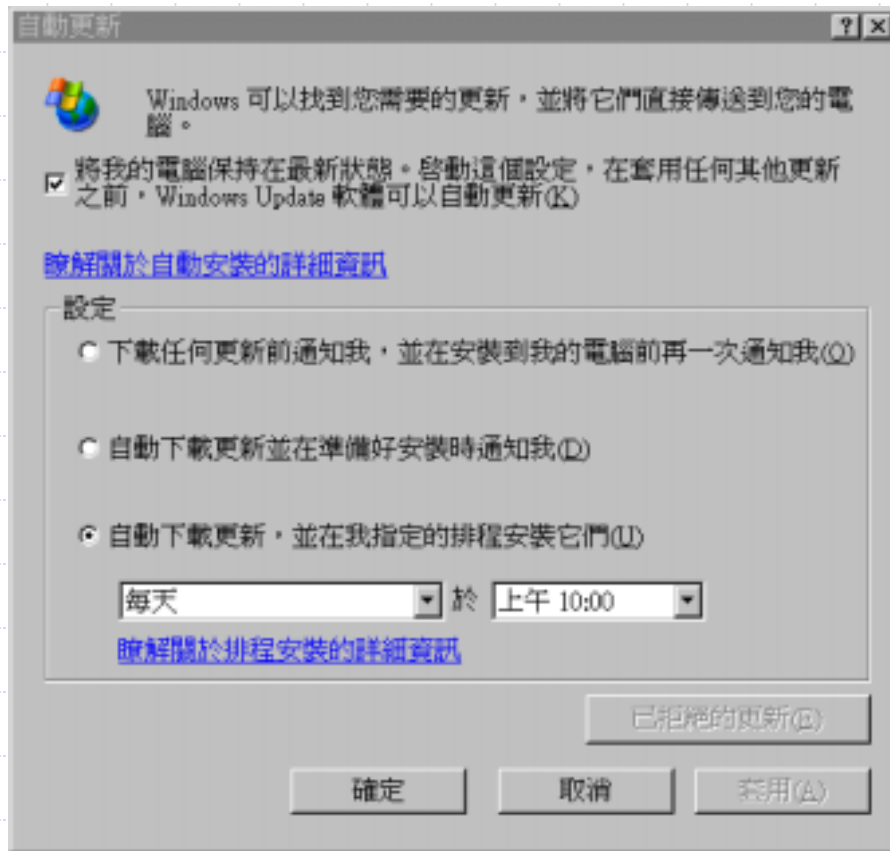
- Windows 2000 Service Pack 2 或更新的版本，請安裝「KB835732：Windows 2000 安全性更新」
- 對於 Windows XP，請安裝「KB835732：Windows XP 安全性更新」

按下 [掃描更新] 後，Windows Update 將會判斷您是否需要此安全性更新；若需要，「重大更新」與「Service Pack」網頁會列出此更新。

© 2004 Microsoft Corporation. All rights reserved. [使用規定](#) [協助工具](#)

網際網路

Auto Update 設定



- ◆ 當有新的Patch時會自動下載，但須設定其安裝模式。
- ◆ Windows 2000於 設定／控制台／自動更新。
- ◆ Windows XP於 開始／控制台／系統／自動更新。
- ◆ 儘可能設定為[自動下載更新，並在我指定的排程安裝它們]。

OfficeScan 之立即更新

立即更新設定

網域名稱 / IP 位址：

伺服器連接埠：

Proxy 伺服器

使用 proxy 伺服器

位址：

連接埠：

使用者名稱：

密碼：

立即更新(U)... 取消

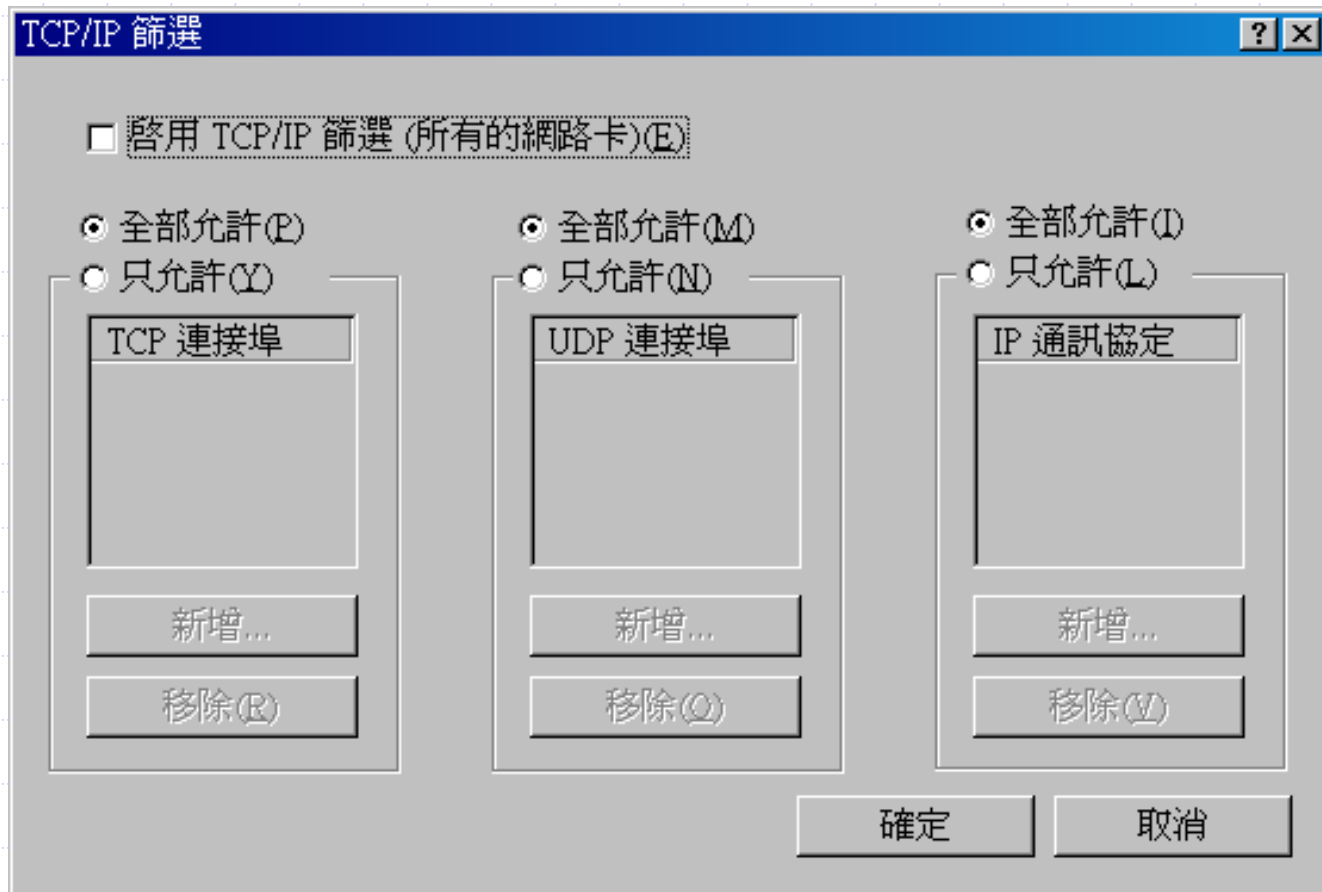
個人防火牆

定義：管制網路上之範圍或Service 對於主機之存取

- ◆ 使用XP之內建防火牆
- ◆ 使用系統內建之TCP/IP篩選(2000/XP)
- ◆ 使用防毒軟體之防火牆功能
- ◆ 使用主機型防火牆軟體(ZoneAlarm)

使用系統之TCP/IP篩選

開始/設定/控制台/網路和撥號連線/{連線名稱} 選TCP/IP 內容/進階/選項 之TCP/IP篩選



使用系統之TCP/IP篩選

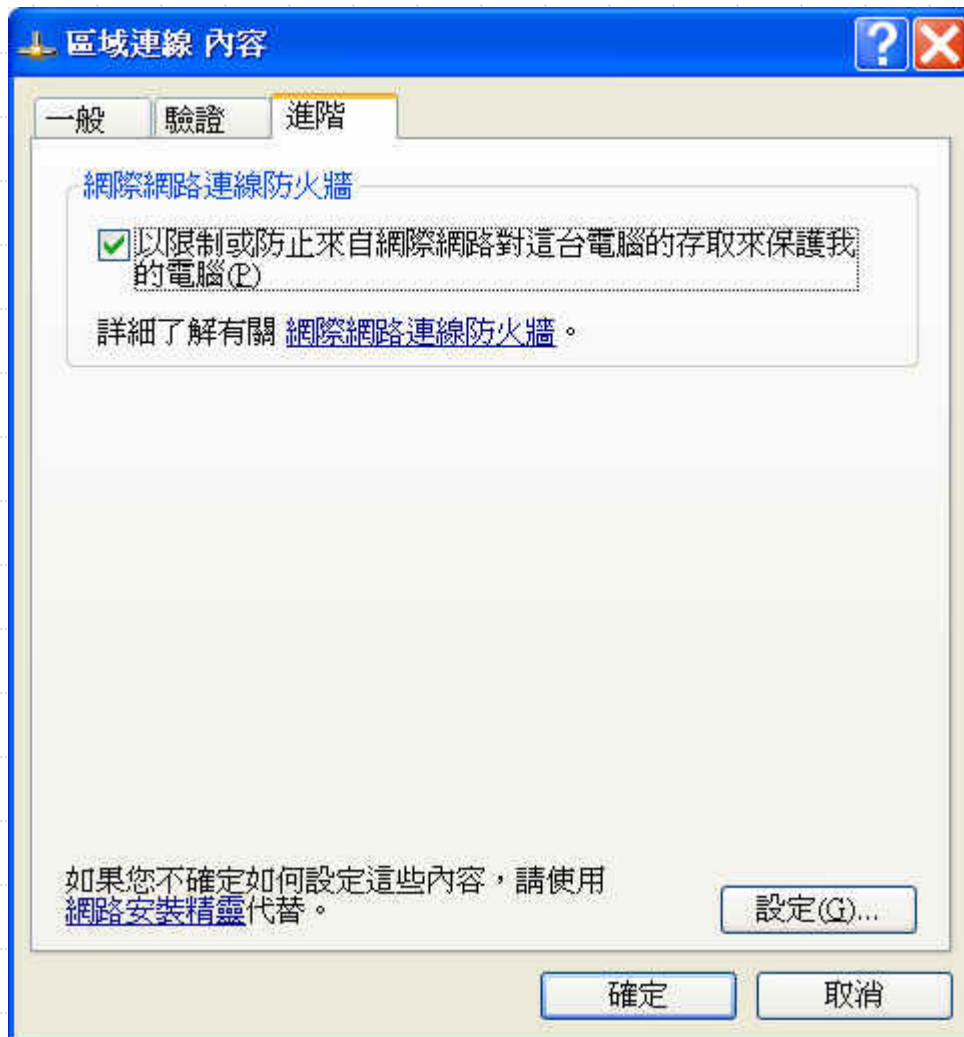
TCP/UDP port : 參考

\WINNT\System32\service\drivers\etc\services

IP Protocol :

ICMP	1	Internet Control Message Protocol
IGMP	2	Internet Group Management Protocol
GGP	3	Gateway-to -Gateway Protocol
IP	4	IP in IP encapsulation
TCP	6	Transmission Control Protocol
EGP	8	Exterior Gateway Protocol
IGP	9	Interior Gateway Protocol
UDP	17	User Datagram Protocol

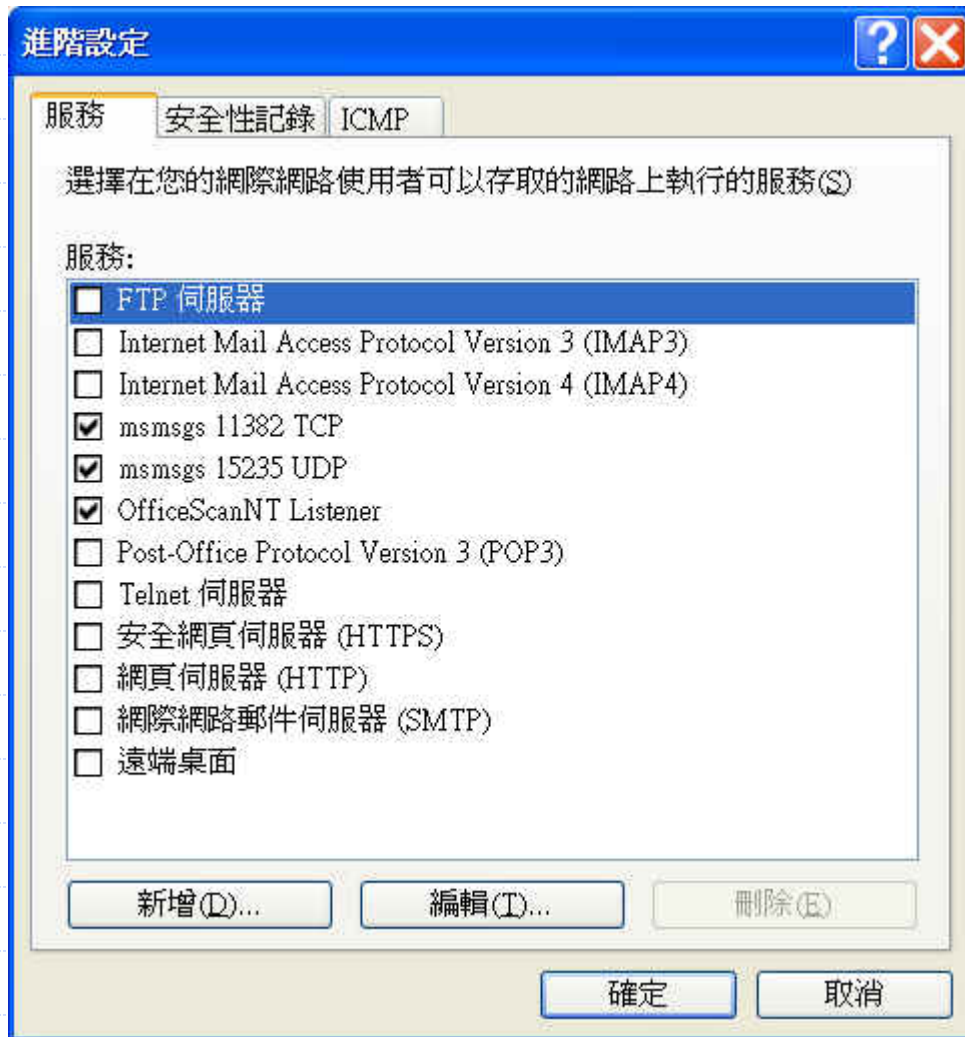
使用XP系統之網路連線防火牆



開始/設定/控制台/網路連線/{連線名稱}/內容/進階

勾選[以限制或防止...]

使用XP系統之網路連線防火牆



上一畫面按下[設定],
出現此畫面

在服務內勾選所開放的
服務

安裝需要連入之軟體時,
會將該軟體加至列表,
如此例加上

OfficeScanNT 1成芟及

個人防火牆軟體ZoneAlarm

Click on a feature name to learn more.

ZoneAlarm PRO



Protect against hackers, email viruses, internal tampering, web profiling, spyware, rogue applications, and more

Buy
Try

ZoneAlarm PLUS



Protect against hackers, email viruses, and internal tampering

Buy
Try

ZoneAlarm®
Download

Advanced PC Protection

Firewall	NEW! Expert Controls Mobile PC Protection Password Protection Advisor Services NEW! Complete Mailsafe Hacker ID Firewall	NEW! Cache Cleaner Pop Up and Ad Blocking Cookie Control NEW! Expert Controls Mobile PC Protection Password Protection Advisor Services NEW! Complete Mailsafe Hacker ID Firewall
----------	--	--

個人防火牆軟體ZoneAlarm

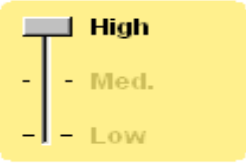
- ◆ 個人防火牆軟體ZoneAlarm版本屬Freeware，可阻擋非法的入侵攻擊，還可控制自己電腦內那些軟體可以使用網路連線，以杜絕駭客利用病毒入侵你的電腦。
- ◆ 原廠網址：
<http://www.zonelabs.com/store/content/home.jsp>
- ◆ 將所連線之IP設在事先以Zone（區域）定義之信任區（Trusted）及不信任區（Internet），分別施以不同之管制等級，並可動態改變區域設定。

ZoneAlarm安裝

- ◆ 省略其中部份畫面說明
- ◆ 當出現User Information視窗時，鍵入一些基本資料，並勾選“I want to register so I can download updates”及“Inform me about important updates and news”
- ◆ 在 Review Alert Setting畫面，出現“What kind of blocked traffic do you want to be alerted to ?”提示，選擇“Alert me whenever ZoneAlarm blocks traffic”
- ◆ 在 Secure Programs畫面，出現“Do you want ZoneAlarm to preconfigure access permission?”，選取“Yes”
- ◆ 在eBay FRAUD PREVENTION畫面，出現“Would you like ZoneAlarm to prevention your eBay password from being sent to unauthorized sites?”，選取“No thank you, not at this time”

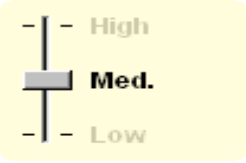
ZoneAlarm firewall/Main設定

Internet Zone Security



High: Stealth mode. Your computer is hidden and protected from hackers. Sharing is not allowed. This setting is recommended for the Internet Zone.

Trusted Zone Security



Medium: Sharing mode: Computers can see your computer and share its resources. This setting is recommended for the Trusted Zone only.

- Internet Zone之[High]表示您的電腦完全隱藏，也不允許sharing，[Mid]為可見您的電腦，但sharing還是不允許，[Low]為關閉firewall
- Trusted Zone之[High]為您的電腦完全隱藏，也不允許sharing，而[Med]為可見您的電腦，而且允許sharing，[Low]為關閉firewall
- 建議Internet Zone設為[High]，Trusted設為[Med]，將需要分享你資源之電腦之IP加在Trusted內

ZoneAlarm firewall/Zones設定

The screenshot displays the ZoneAlarm Firewall control panel. At the top, there's a status bar with 'INTERNET' and 'IN OUT' indicators, a 'STOP' button, and 'PROGRAMS' with 'All Systems Active' status. The main interface has a sidebar with navigation options: Overview, Firewall, Program Control, Alerts & Logs, and E-mail Protection. The 'Firewall' tab is active, showing a table of zones and a dialog box for adding a new host/site.

Firewall

Use this tab to add computers and networks to your Trusted Zone.

Example: Put a computer or network you want to share with into the Trusted Zone.

All traffic sources not listed here are in the Internet Zone by default.

Name	IP Address / Site	Entry Type	Zone
backup_server	140.116.2.247	Host/Site	Trusted
D-Link DFE-530T...	140.116.2.248/255.255.255.0	Adapter ...	Internet
sam	140.116.2.246	Host/Site	Trusted
yang-xp	140.116.2.245	Host/Site	Trusted

Add Host/Site

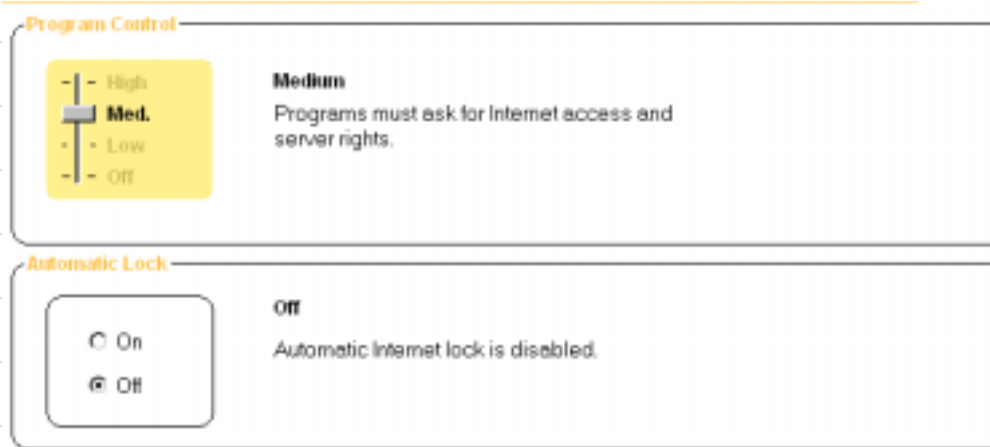
Add a Web host/site to your Trusted Zone by completing the fields below. Name the Web host/site for easy reference later so you always know who you're trusting and who you're not.

Zone:

Host name:

Description:

ZoneAlarm Program control/Main



- [High]：只有 Pro版本方可設定。
- [Med]：當程式需至Internet 存取時，會詢問您。
- [Low]：學習模式，程式需至Internet 存取時，不會詢問
















ZoneAlarm Program control/Programs

Program Control

These are programs that have tried to access the Internet or local network.

Access and Server columns show the permissions the program has for each Zone.

Change a program's permissions by left-clicking the icons in the Access or Server column.

Programs	Access		Server		Lock
	Trusted	Internet	Trusted	Internet	
 Dr.eye 2000 Auto...	✓	✓	?	?	
 Generic Host Pro...	✓	✓	?	?	
 Internet Explorer	✓	✓	?	?	
 Messenger	✓	✓	?	?	
 Microsoft Telnet ...	✓	✓	?	?	
 Microsoft Word L...	?	?	?	?	
 netterm.exe	✓	✓	?	?	
 mfs.exe	?	?	?	?	
 mymgr.exe	✓	✓	✓	✓	
 Outlook Express	✓	✓	?	?	
 pcAnywhere Host	✓	✓	✓	✓	
 PCNT	?	?	?	?	
 POP3Trap	✓	✓	?	?	
 putty.exe	✓	✓	?	?	
 RealNetworks Ev...	✓	✓	?	?	

- Access 中之勾選為允許這軟體程式向外存取，問號表需提示
- Server 表示是否允許此程式將此PC當成Server端

ZoneAlarm之Logs

Alerts & Logs

This is a record of your security activity.

Click an alert in the list, then read details about it in the Entry Detail window.

To get an analysis from AlertAdvisor, click More Info.

To add the traffic source to a Zone, click Add to Zone.

View only the last alerts.

Rating	Date / Time	Type	Protocol	Program	Source IP	Des
High	2004/05/18 13:23:58+...	Firewall	TCP (flags:S)		219.110.41.239:2278	140.1
Medium	2004/05/18 13:22:06+...	Firewall	ICMP (type:3/subtype:3)		163.28.113.2	140.1
Medium	2004/05/18 13:19:40+...	Firewall	TCP (flags:S)		140.116.116.149:1924	140.1
Medium	2004/05/18 13:19:28+...	Firewall	TCP (flags:S)		140.116.57.23:4864	140.1
Medium	2004/05/18 13:19:02+...	Firewall	TCP (flags:S)		218.172.162.32:4510	140.1
Medium	2004/05/18 13:16:02+...	Firewall	TCP (flags:S)		140.116.144.54:1846	140.1
Medium	2004/05/18 13:15:36+...	Firewall	TCP (flags:S)		140.116.116.149:1856	140.1
Medium	2004/05/18 13:13:48+...	Firewall	TCP (flags:S)		140.116.143.161:4030	140.1
Medium	2004/05/18 13:12:24+...	Firewall	TCP (flags:S)		140.116.133.30:1977	140.1
Medium	2004/05/18 13:08:38+...	Firewall	ICMP (type:3/subtype:3)		163.28.113.2	140.1
Medium	2004/05/18 13:08:22+...	Firewall	TCP (flags:S)		140.116.223.5:2794	140.1
Medium	2004/05/18 13:04:50+...	Firewall	TCP (flags:S)		140.116.22.130:2066	140.1
Medium	2004/05/18 13:03:02+...	Firewall	TCP (flags:S)		140.116.32.70:4953	140.1

可在 Log 畫中選擇將該來源改設為 Trusted, 以改變管制等級

Entry Detail

Description Packet sent from 163.28.113.2 to 140.116.2.248 (ICMP Unreachable) was blocked
Direction Incoming
Type Firewall
Source DNS mchis.nctu.edu.tw
Source IP 163.28.113.2

Add to Zone >>

More Info

Alert 設定及顯示

Alerts & Logs

Informational Alerts Shown:
Choose whether non-program alerts will generate pop-up messages.

Note: Program alerts are always shown because they require a 'Yes' or 'No' from you.

Alert Events Shown

On

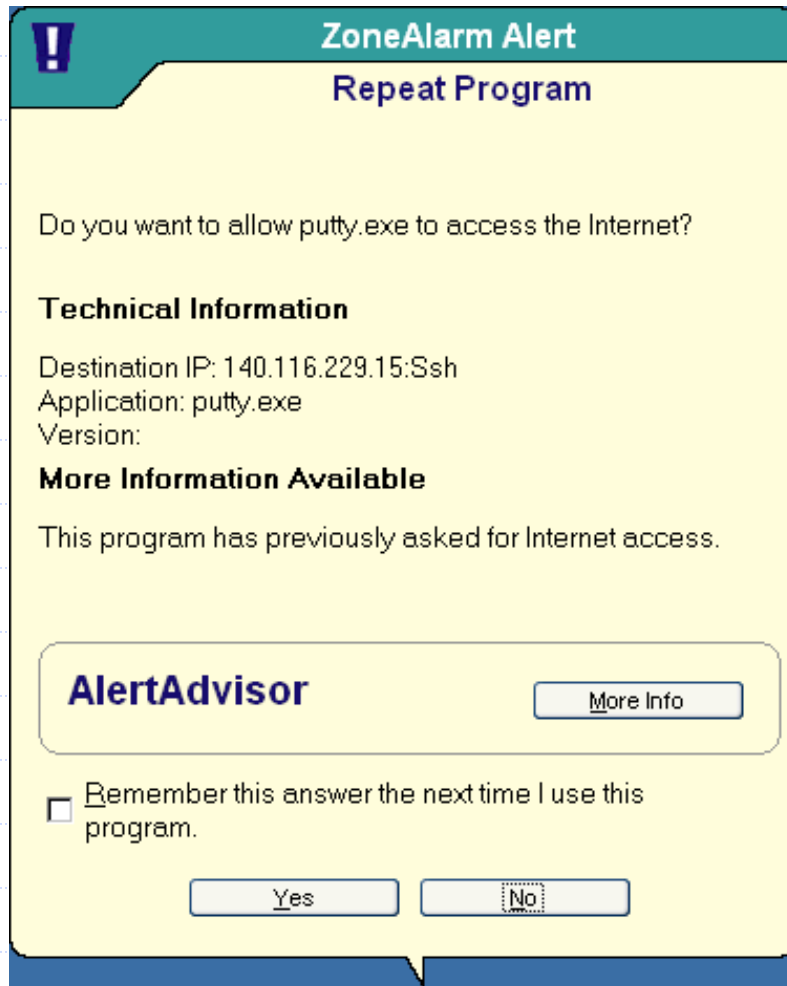
Show all alerts.

Off

當ZoneAlarm針對連入之阻檔動作，所產生之提醒畫面



程式連外之提示



- 其中之Yes表示允許連外，而No則不允許
- 其中之Remember this answer the next time to use this Program表示將來此程式之處理比照此次之處理，也就是此選項勾選時，並選擇Yes，表示將來此程式執行要連外時，不需再詢問，直接連接

Active Ports

- ◆ Active Ports為SmartLine出品，為免費軟體，用來監視電腦所有打開的TCP/IP/UDP埠，
- ◆ 可以將所有的埠顯示出來，還顯示所對應的程式所在的路徑，本地IP和遠端IP。
- ◆ 提供了一個關閉埠的功能，在發覺此埠或其程式有問題時。
- ◆ WindowsNT/2000/XP平臺下。
- ◆ 下載網址
<http://www.smartline.ru/software/aports.zip>

Active Ports

Active Ports

File Options ?

Process	P...	Local IP	Local Port	Remote IP	Remote P...	State	Protocol	Path
System	8	140.116.2.248	138			LISTEN	UDP	
System	8	140.116.2.248	137			LISTEN	UDP	
System	8	0.0.0.0	1035			LISTEN	TCP	
System	8	140.116.2.248	3181			LISTEN	TCP	
System	8	0.0.0.0	445			LISTEN	TCP	
System	8	140.116.2.248	139			LISTEN	TCP	
lsass.exe	224	140.116.2.248	500			LISTEN	UDP	C:\WINNT\system32\lsass.exe
svchost.exe	424	0.0.0.0	135			LISTEN	TCP	C:\WINNT\system32\svchost.exe
spoolsv.exe	448	0.0.0.0	3012			LISTEN	UDP	C:\WINNT\system32\spoolsv.exe
svchost.exe	560	0.0.0.0	3002			LISTEN	UDP	C:\WINNT\System32\svchost.exe
nvpngr.exe	592	0.0.0.0	20031			LISTEN	UDP	C:\Program Files\NetVault5\bin\nvpngr.exe
nvpngr.exe	592	127.0.0.1	1025			LISTEN	UDP	C:\Program Files\NetVault5\bin\nvpngr.exe
nvpngr.exe	592	0.0.0.0	20031			LISTEN	TCP	C:\Program Files\NetVault5\bin\nvpngr.exe
nvpngr.exe	592	127.0.0.1	1027	127.0.0.1	20032	ESTAB...	TCP	C:\Program Files\NetVault5\bin\nvpngr.exe
nvpngr.exe	592	127.0.0.1	20032	127.0.0.1	1027	ESTAB...	TCP	C:\Program Files\NetVault5\bin\nvpngr.exe
nvpngr.exe	592	127.0.0.1	1026	127.0.0.1	20032	ESTAB...	TCP	C:\Program Files\NetVault5\bin\nvpngr.exe
MSTask.exe	808	0.0.0.0	1028			LISTEN	TCP	C:\WINNT\system32\MSTask.exe
tlntlisten.exe	836	0.0.0.0	12345			LISTEN	TCP	C:\OfficeScan NT\tlntlisten.exe
svchost.exe	944	0.0.0.0	3231			LISTEN	TCP	C:\WINNT\system32\svchost.exe
svchost.exe	944	0.0.0.0	3236			LISTEN	TCP	C:\WINNT\system32\svchost.exe
svchost.exe	944	0.0.0.0	3233			LISTEN	TCP	C:\WINNT\system32\svchost.exe
Explorer.EXE	1288	127.0.0.1	3602			LISTEN	UDP	C:\WINNT\Explorer.EXE
MsnMgr.Exe	1368	0.0.0.0	4730			LISTEN	UDP	C:\Program Files\MSN Messenger\MsnMgr.Exe
MsnMgr.Exe	1368	140.116.2.248	9			LISTEN	UDP	C:\Program Files\MSN Messenger\MsnMgr.Exe
MsnMgr.Exe	1368	127.0.0.1	3030			LISTEN	UDP	C:\Program Files\MSN Messenger\MsnMgr.Exe
MsnMgr.Exe	1368	140.116.2.248	4725	207.46.107.67	1863	ESTAB...	TCP	C:\Program Files\MSN Messenger\MsnMgr.Exe
MsnMgr.Exe	1368	0.0.0.0	3493			LISTEN	TCP	C:\Program Files\MSN Messenger\MsnMgr.Exe
MsnMgr.Exe	1368	140.116.2.248	3495	211.20.185.2	80	CLOSE...	TCP	C:\Program Files\MSN Messenger\MsnMgr.Exe
Serv-U32.exe	1400	0.0.0.0	1234			LISTEN	TCP	C:\Program Files\Serv-U\Serv-U32.exe
awhost32.exe	1820	0.0.0.0	5632			LISTEN	UDP	C:\Program Files\Symantec\pcAnywhere\awhost
awhost32.exe	1820	0.0.0.0	5631			LISTEN	TCP	C:\Program Files\Symantec\pcAnywhere\awhost
Pop3Trap.exe	1996	127.0.0.1	110			LISTEN	TCP	C:\OfficeScan NTPop3Trap.exe
ieexplore.exe	16932	127.0.0.1	4335			LISTEN	UDP	C:\Program Files\Internet Explorer\ieexplore.exe
ieexplore.exe	16932	140.116.2.248	4348	202.39.12.27	80	ESTAB...	TCP	C:\Program Files\Internet Explorer\ieexplore.exe
ieexplore.exe	16932	140.116.2.248	4347	202.39.12.27	80	ESTAB...	TCP	C:\Program Files\Internet Explorer\ieexplore.exe

Terminate Process Query Names X Exit

Baseline Security Analyzer

- Baseline Security Analyzer (MBSA) 掃描本機及網域中其他的電腦，看是不是有安裝所有的 Hotfix 及其他程式的修正程式
- 執行掃描之平台為Windows2000/XP , Windows Server 2003, 及需要 Internet Explorer 5.01 以上，未使用此版本以上者，必須下載安裝XML剖析器。
- 可掃描Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0/5.0, SQL Server 7.0/2000, Internet Explorer (IE) 5.01 以上，以及 Office 2000/XP。
- 其他如密碼安全性查核、分享資料夾等等對安全性造成影響的行為，檢查並做出建議。
- 下載網址為：
<http://www.microsoft.com/technet/security/mbsahome.mspx>
- 掃描別部主機，須有該主機之Administrator權限，故一般應用在掃描本機。



Microsoft

Baseline Security Analyzer

Microsoft

Microsoft Baseline Security Analyzer

- [Welcome](#)
- [Pick a computer to scan](#)
- [Pick multiple computers to scan](#)
- [Pick a security report to view](#)
- [View a security report](#)

See Also

- [Microsoft Baseline Security](#)

Pick a computer to scan

Specify the computer you want to scan. You can enter either the computer name or its IP address.

Computer name:

IP address:

Security report name:

Options:

Check for Windows vulnerabilities

Check for weak passwords

Check for IIS vulnerabilities

Check for SQL vulnerabilities

Check for security updates

Use SS

Server:

Learn more about [Scanning Options](#)

 [Start scan](#)



Microsoft Baseline Security Analyzer

Microsoft

Microsoft Baseline Security Analyzer

- [Welcome](#)
- [Pick a computer to scan](#)
- [Pick multiple computers to scan](#)
- [Pick a security report to view](#)
- [View a security report](#)

See Also

- [Microsoft Baseline Security](#)

Actions

[Print](#)
[Copy](#)

View security report

Sort Order: ▾

Computer name:	Workgroup\Yang-notebook
IP address:	169.254.9.148
Security report name:	Workgroup - Yang-notebook (10-20-2003 00-39 AM)
Scan date:	2003/10/20 12:39
Scanned with MBSA version:	1.1.1
Security update database version:	1.0.1.502
Security assessment:	Severe Risk (One or more critical checks failed.)

Security Update Scan Results

Score	Issue	Result
	Windows Media Player Security Updates	1 critical security updates are missing. What was scanned Result details How to correct this
	Windows Security Updates	No critical security updates are missing. What was scanned
	IIS Security	IIS is not running on this computer.

Previous security report

Next security report