第8章 安全性

本章提要

- 安全性
- 共用資源的保護
- 使用者驗證
- 程式威脅
- 安全防護
- 電腦的安全等級

8-1安全性

- 資訊安全的威脅種類：
  - 中斷：阻止具有合法權利的使用者存取系統資源
  - 攔截：設法取得未經授權的資訊
  - 篡改：不合法地改變或刪除某些資訊
  - 偽造：偽造某些資訊
- 後3類的安全威脅，與一般正常的系統運算之間的主要差別，只是在於這些行為的執行者是否具有合法的權限
- 系統安全防護措施：安全程度與便利性及成本之間妥協後的結果

8-2共用資源的保護

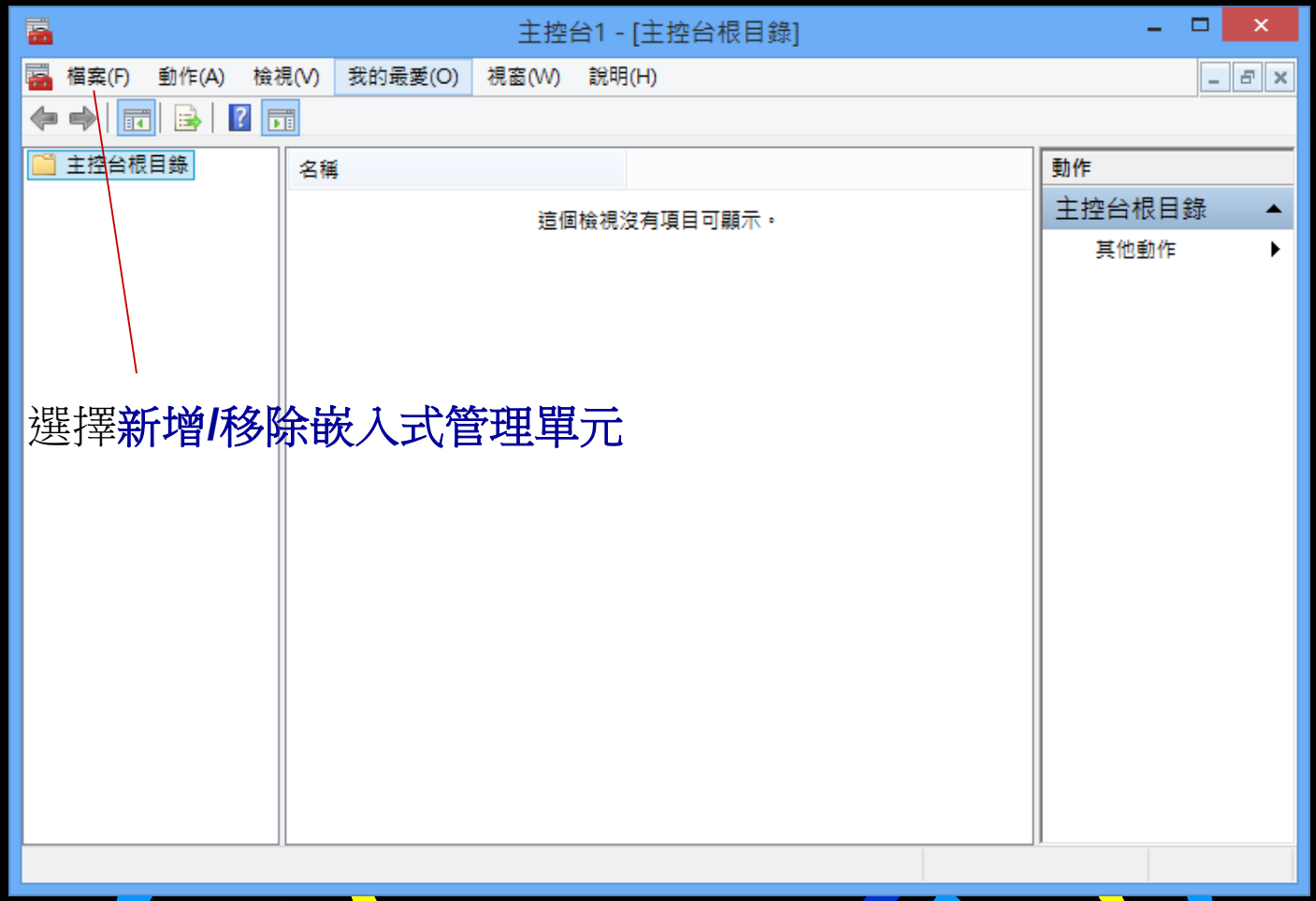
- I/O的保護
  - 使用者可能會發出不合法的I/O指令來存取作業系統的記憶體位址，或是干擾作業系統的正常運作→I/O指令都被定義為特權指令
  - 使用者要使用I/O的時候，都必須透過系統呼叫來完成
  - 如果中斷處理常式或是I/O驅動程式的設計不當，就可能會被用來取得在核心模式下的執行權利
- CPU的保護
  - 程式可能蓄意或無意地進入無窮迴圈，使得作業系統無法取得控制權→利用計時器根據設定的時間產生中斷
- 記憶體的保護
  - 如果使用者行程可以存取到作業系統的記憶體位址，就可能藉此取得核心模式的執行權利
  - 使用者的行程也可能會因為程式錯誤，而誤改了作業系統或其他行程的記憶體資料
  - 利用基底暫存器或重定址暫存器，來防止行程存取到不屬於自己的位址空間
- 檔案與週邊裝置的保護
  - 作業系統必須做到使用者身分驗證，與系統資源存取權限的管理

Windows的本機群組原則運作原理

- 群組原則是指一組電腦設定規則的集合，通常是用來規範使用者使用電腦的方式
  - 例如密碼的設定原則、是否可以使用隨身碟...
- Windows提供不同層級的本機群組原則物件，包括：
  - 本機電腦原則
  - 系統管理員及非管理員原則
  - 個別使用者原則
- 原則的套用：
  - 電腦開機時會先套用本機電腦原則
  - 使用者登入時，會先套用系統管理員或非系統管理員的本機群組原則，然後再套用該使用者的個別使用者原則

動手做做看-限制卸除式儲存裝置的使用

按下【windows】鍵+【R】鍵，輸入mmc，開啟主控台



選擇**新增/移除嵌入式管理單元**

以新增群組原則物件編輯器方式加入本機電腦原則

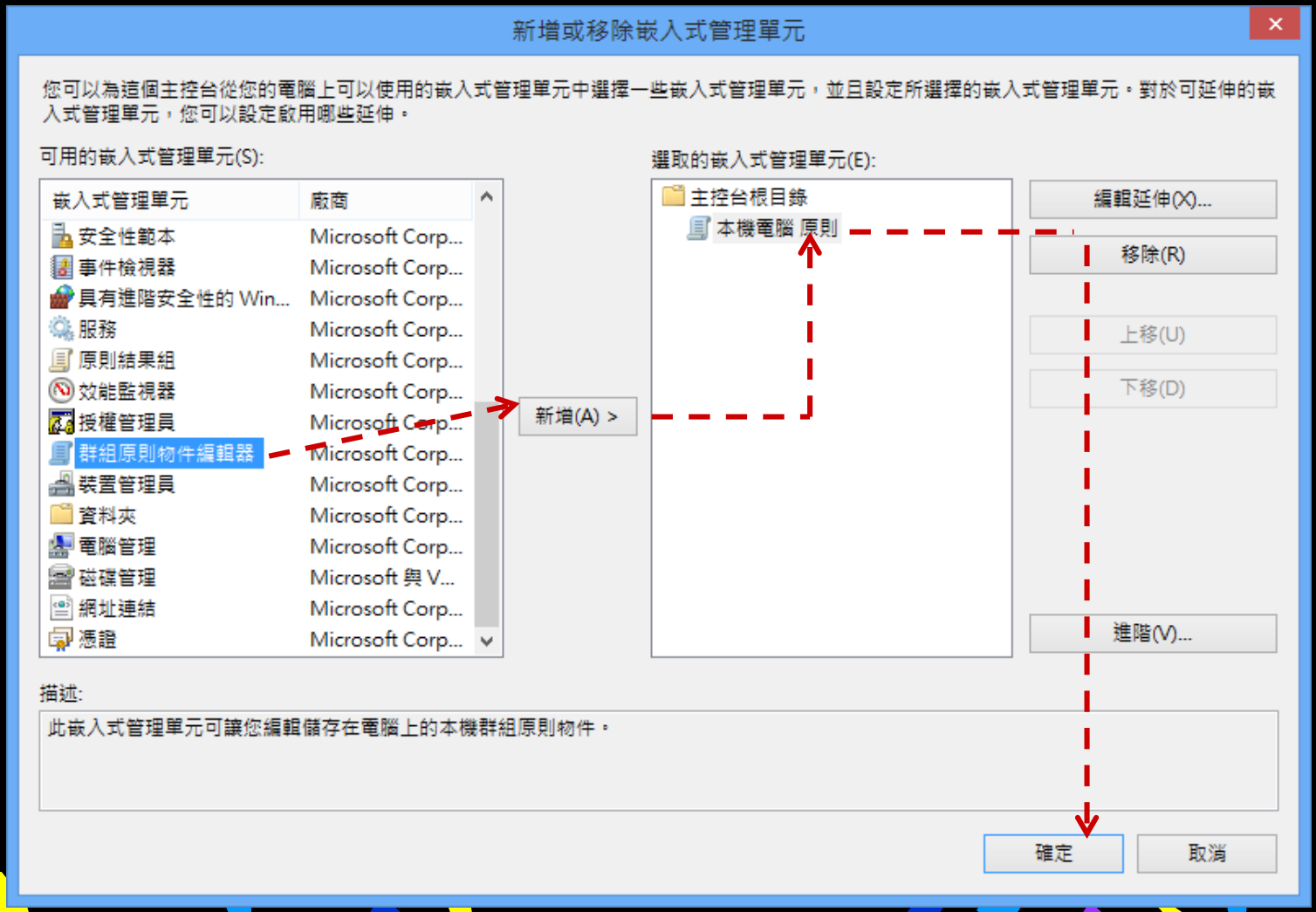
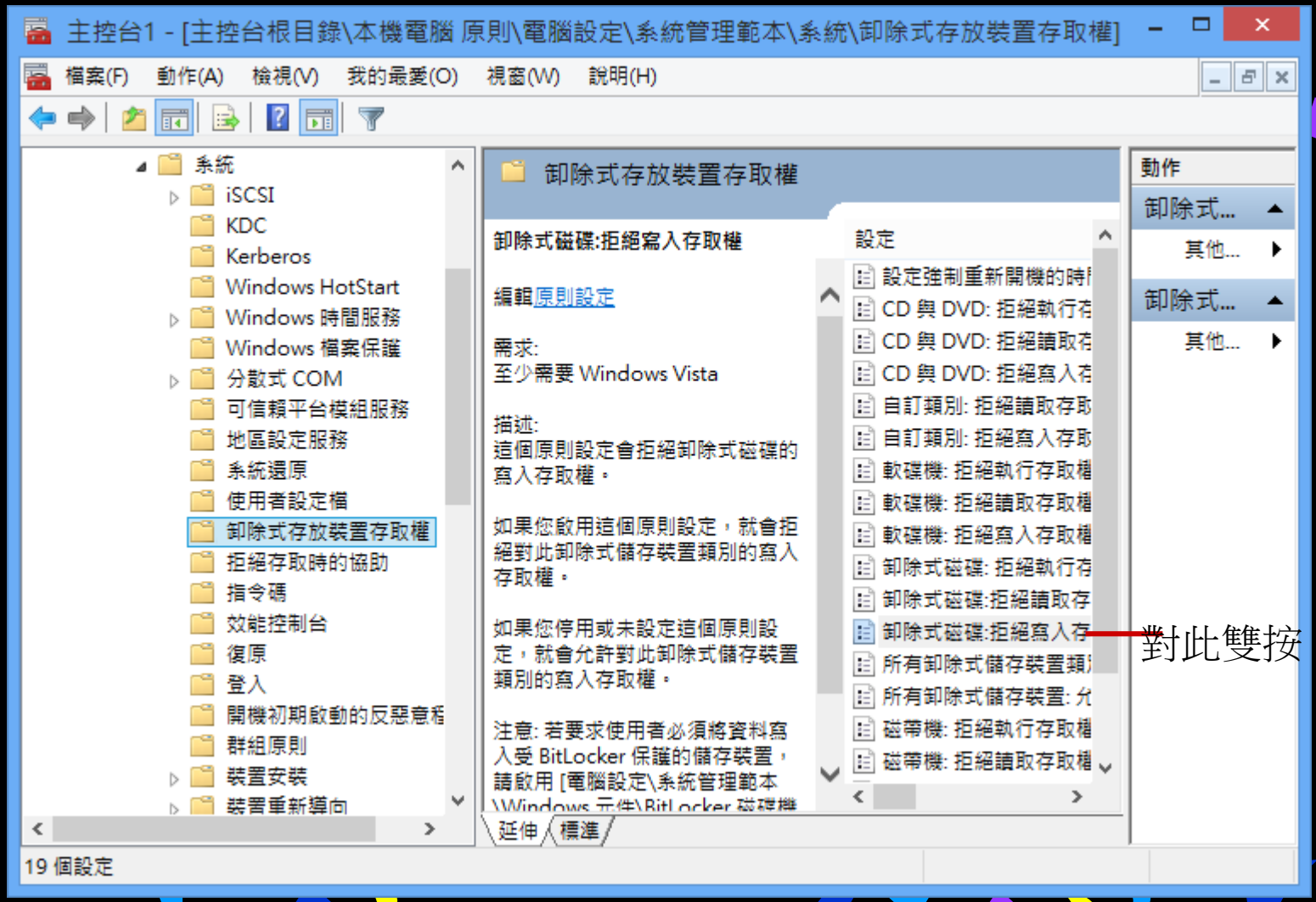


圖8-3於卸除式儲存裝置存取權中限制其寫入的存取權



對此雙按

使用者驗證

- 最簡便的入侵技巧之一，就是設法取得某個使用者的帳號與密碼
- 如何取得密碼？
  - 直接詢問
  - 從別人的電腦旁邊偷窺。
  - 設法存取到密碼檔。
  - 使用網路竊聽器來尋找未經加密的密碼。
  - 透過網路竊聽器取得加密過的密碼，重新組合成登入訊息，以欺騙作業系統進行登入。
  - 字典式攻擊
  - 暴力式攻擊

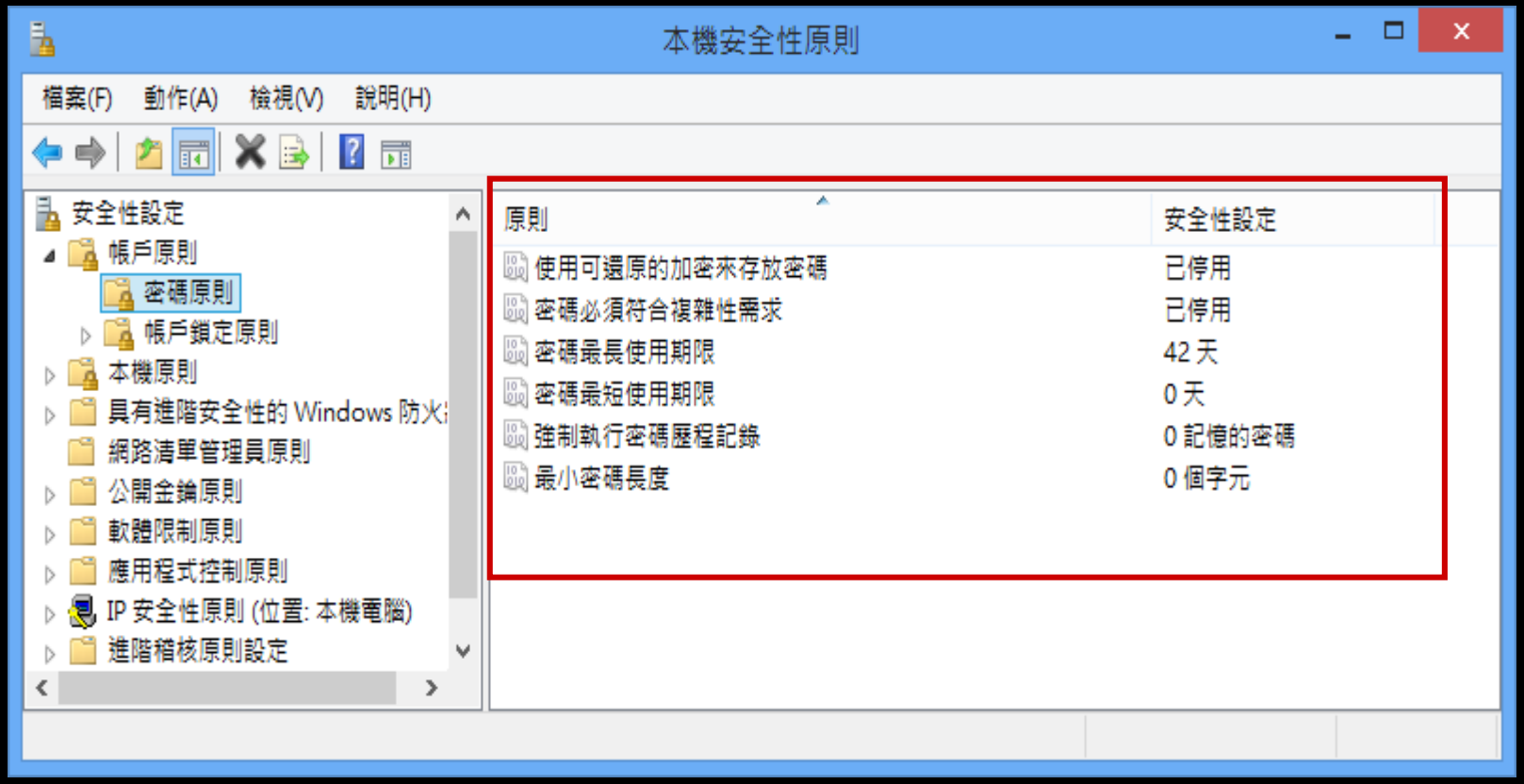
實作討論—Unix對密碼提供的保護

- Unix上的密碼管理功能中（passwd命令），可以設定密碼的有效期限，以及還有多久就會逾期的提示訊息
- 提供/etc/shadow檔案功能

動手做做看
設定Windows的密碼原則

- Windows允許系統管理者設定關於使用者密碼的一組規則，不過目前只有商用入門版以上的版本才提供原則的設定功能
- 打開檔案總管，在網址列輸入控制台\所有控制台項目\系統管理工具\本機安全性原則

圖8-4 Windows的本機安全性原則設定畫面



8-4 程式威脅

- 病毒(Virus)：
  - 只是一段程式碼, 而非一支完整的電腦程式, 會將本身複製到其他乾淨的檔案或開機區，並且以相同的方式繼續散播出去
  - 傳統的電腦病毒大致上可分為下列幾種：
    - 開機型
    - 檔案型
    - 開機與檔案混合型
    - 巨集型
- 蟲毒(Worm)：蠕蟲
  - 能夠透過電腦網路自我複製的程式
  - 現代的蟲毒經常透過電子郵件或網際網路聊天室來傳播，不但會自我複製, 有些還包含惡意的攻擊，Ex.「我愛您」蟲毒
  - 唯一的預防之道操之在終端使用者之手

電子郵件附加病毒的濫觴--梅莉莎病毒

- 梅莉莎是最早透過電子郵件的附加檔來散播的電腦病毒
- 它是感染word檔案的巨集病毒：
  - 當使用者開啟一個含有梅莉莎病毒的Word文件時, 病毒會立刻感染Word的範本文件Normal.dot, 進而感染其他的word文件。而且還會自行從outlook的通訊錄中找尋50名使用者, 自動寄出包含病毒附加檔的電子郵件
  - 這種病毒企圖偽裝成從朋友寄來的信件 並以誘人的標題與內容來吸引使用者打開受到病毒感染的附加文件檔
- 這種自動以電子郵件進行傳播的方式, 很快就導致各大公司的網路服務癱瘓, 也開啟了以網際網路傳播病毒的新紀元。
- 自從梅莉莎病毒問世之後, 以電子郵件的附件檔來傳播各式病毒成為主要的病毒感染模式
- 此外, 這類病毒多半會透過微軟的Outlook，自動傳播電子郵件來進行散播。

程式威脅(二)

- 特洛伊木馬：在看來無害的外表背後，隱藏著惡意的程式碼
- 間諜軟體：通常是在瀏覽某些商業性網站時，隨著網頁內容入侵電腦
- 後門：偷偷引入、未經批准的登入或驗證方法
- 緩衝區溢位：輸入超出緩衝區長度的資料，使得資料從緩衝區溢出而覆蓋掉原本放置某些程式指令的另一塊記憶體
- 邏輯炸彈：預先埋在程式中的一段程式碼，要在特定時刻將系統「炸掉」
- 阻絕服務：促使目標主機的硬體或軟體發生癱瘓的情況，使正當的使用者無法正常使用該主機提供的服務

實作討論：特洛伊木馬程式Back Orifice

- Back Orifice 是常見的特洛伊木馬遠端控制程式
- 包含客戶端程式及伺服端程式兩個部份
- 入侵者駭客經常將伺服端程式偽裝成特洛伊木馬，以引誘無辜的使用者在自己電腦上安裝伺服端程式
- 駭客利用客戶端程式，可以跟受害者電腦互傳檔案、在對方電腦上執行應用程式、重新啟動或鎖住對方電腦、以及記錄對方電腦上的按鍵動作
- 伺服端程式只是一支約 122 KB 的可執行檔, 它會在視窗系統目錄中建立自己的備份, 並且將它的檔名加到視窗登錄檔
- Back Orifice的伺服端程式只能在 Windows 95 及 98 中運作，而且在攻擊者與目標機器間不能有安裝防火牆

8-5 安全防護

- 追蹤與稽核：定期的檢視系統，來防止安全上的漏洞
  - 可能檢視項目：
    - 太短或容易猜中的密碼
    - 在系統目錄中的非授權程式
    - 非預期的行程
    - 不正確的目錄或檔案權限設定
    - 重要系統檔案的完整性檢查與變動記錄
    - 通訊埠的異常流量，或是有不該被用到的通訊埠被使用
  - 使用日誌功能來偵測、分析、以及回應網路上的安全意外事件

實作討論—Unix上的稽核功能

- Unix家族的作業系統提供syslog程式，能夠根據syslog.conf檔案的設定，從不同的來源接收訊息
- syslog.conf設定範例：

```
#ident	"@(#)syslog.conf	1.5	98/12/14 SMI"	/* SunOS 5.0 */
#
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
*.err;kern.notice;auth.notice                  /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit       /var/adm/messages
*.alert;kern.err;daemon.err                    operator
*.alert                                        root
*.emerg                                        *
mail.*                                        /var/log/maillog
user.err                                       /dev/sysmsg
user.err                                       /var/adm/messages
user.alert                                     `root, operator'
user.emerg                                     *
```

syslog的日誌檔範例

Jan 21 03:10:07 euler syslogd: line 25: unknown priority name "*“

Jan 22 00:57:46 euler named[166]: [ID 295310 daemon.warning] check_hints: A records for B.ROOT-SERVERS.NET class 1 do not match hint records

Jan 22 14:55:32 euler ftpd[5569]: [ID 214291 daemon.notice] FTP LOGIN REFUSED (ftp not in /etc/passwd) FROM xyz.adsl.abc.net.tw [111.169.30.61], anonymous

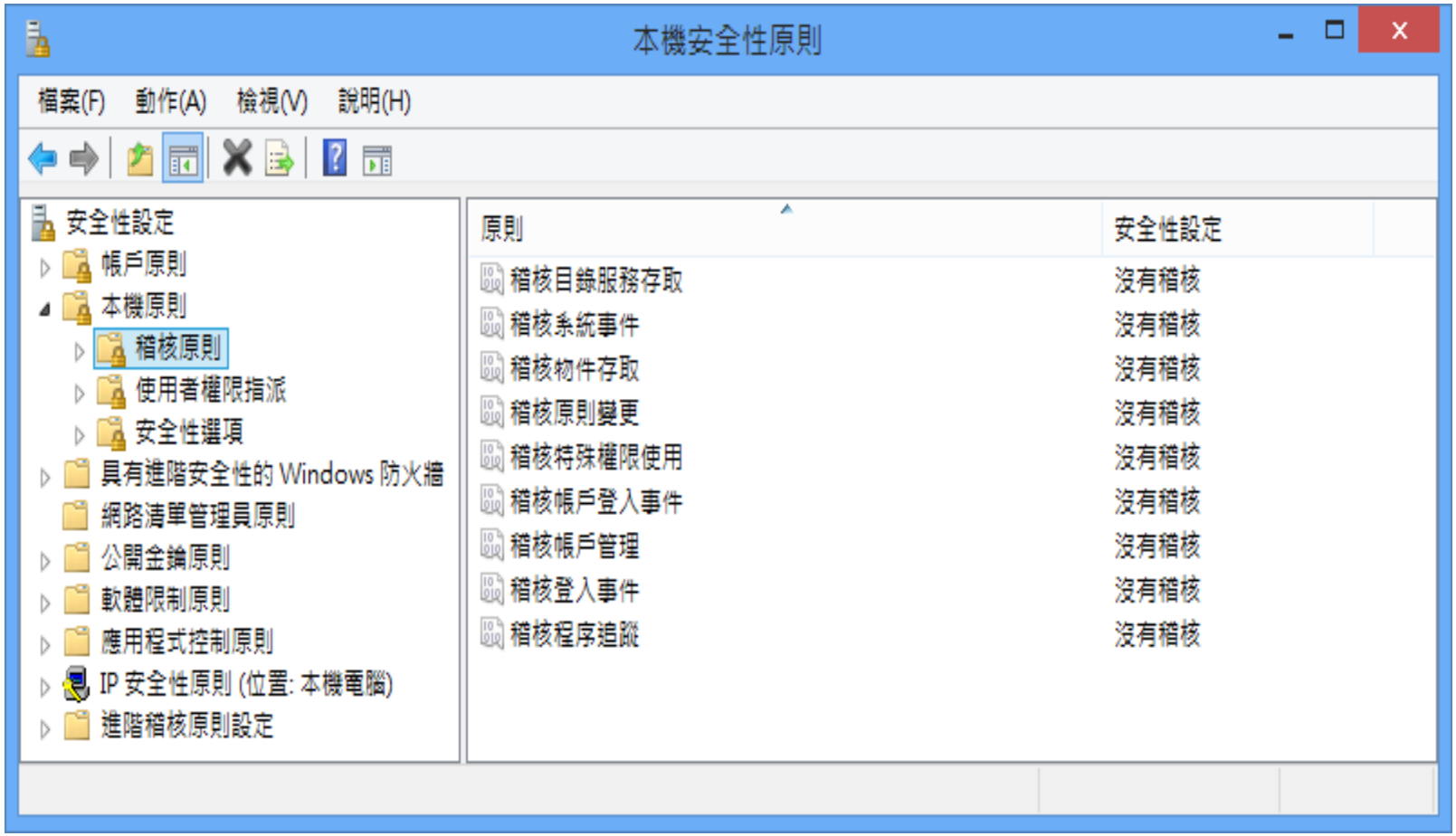
Jan 22 14:55:34 euler ftpd[5570]: [ID 214291 daemon.notice] FTP LOGIN REFUSED (ftp not in /etc/passwd) FROM xyz.adsl.abc.net.tw [111.169.30.61], anonymous

Jan 22 16:36:15 euler ftpd[5888]: [ID 214291 daemon.notice] FTP LOGIN REFUSED (ftp not in /etc/passwd) FROM ijk.customer.opq.net [65.2.126.61], anonymous

實作討論—Windows上的稽核功能

- 可以透過本機安全性原則設定稽核原則
- 並且透過事件檢視器檢視這些事件日誌
- 在Windows中可以開啟的稽核功能包括：
  - 帳戶登入事件
  - 帳戶管理
  - 目錄服務存取
  - 登入事件
  - 物件存取
  - 原則變更
  - 特殊權限使用
  - 程序追蹤
  - 系統事件

圖8-5 Windows上的安全性稽核設定畫面



概念介紹--網路掃描程式

- 有些軟體能夠掃描整個網路，產生哪些埠正在使用的詳細報表，進行密碼破解，並且檢視伺服器的帳號細節，是進行網路稽核很有用的工具
- 網路掃描軟體通常會使用下列一或多個方法：
  - 網際網路封包groper (ping) 的全面清查, 以找出IP位址。
  - SNMP的全面清查，以找出相容的裝置
  - TCP/UDP通訊埠的掃描
  - 掃描登入帳號以取得使用者名稱及密碼
- Nmap是UNIX版本的通訊埠掃描工具

防火牆

- 在共享資源的電腦之間築起一道防線，檢查所有流經的網路交通是否符合使用者設定的規則，並且拒絕所有不符合規則的交通
- 個人防火牆可以安裝在終端用戶的個人電腦上，以協助阻擋對該台電腦的非法入侵攻擊

概念介紹--何謂防火牆？

- 可能是硬體、軟體、或是兩者的混合, 用來過濾進出的資料
- 可以分為下面3種：
  - 封包過濾防火牆：根據封包層的資訊, 例如TCP或IP的標頭（header）, 來同意或拒絕網路交通
  - 應用層防火牆：是在應用層進行過濾
  - 線路層防火牆：能夠確保網際網路上的主機跟企業內部網路中的主機，不會直接相連
    - 它會建立會談, 但自己扮演“中間人”的角色, 負責拷貝兩端的資訊, 並加以傳送

圖8-6 封包過濾防火牆

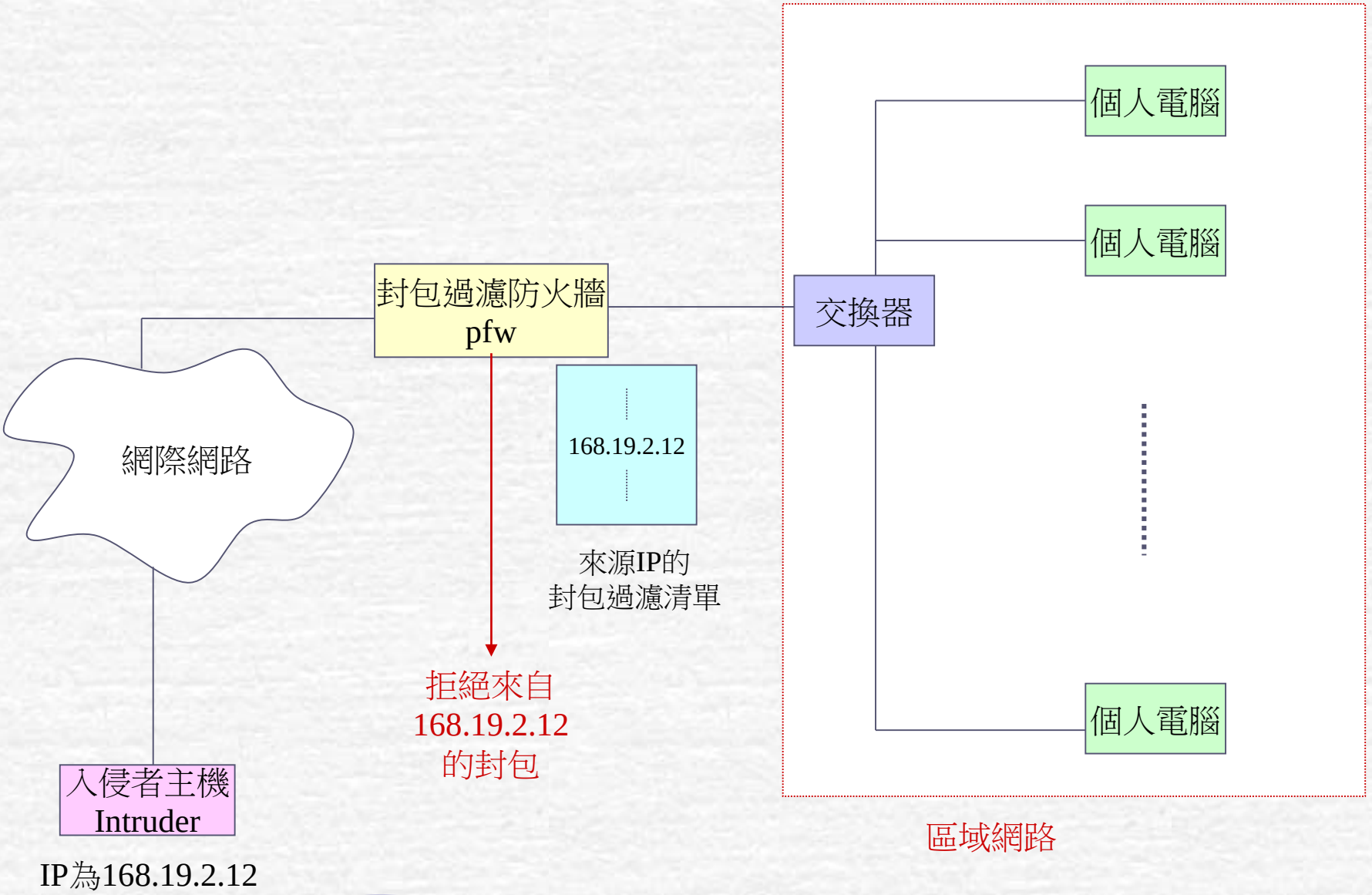
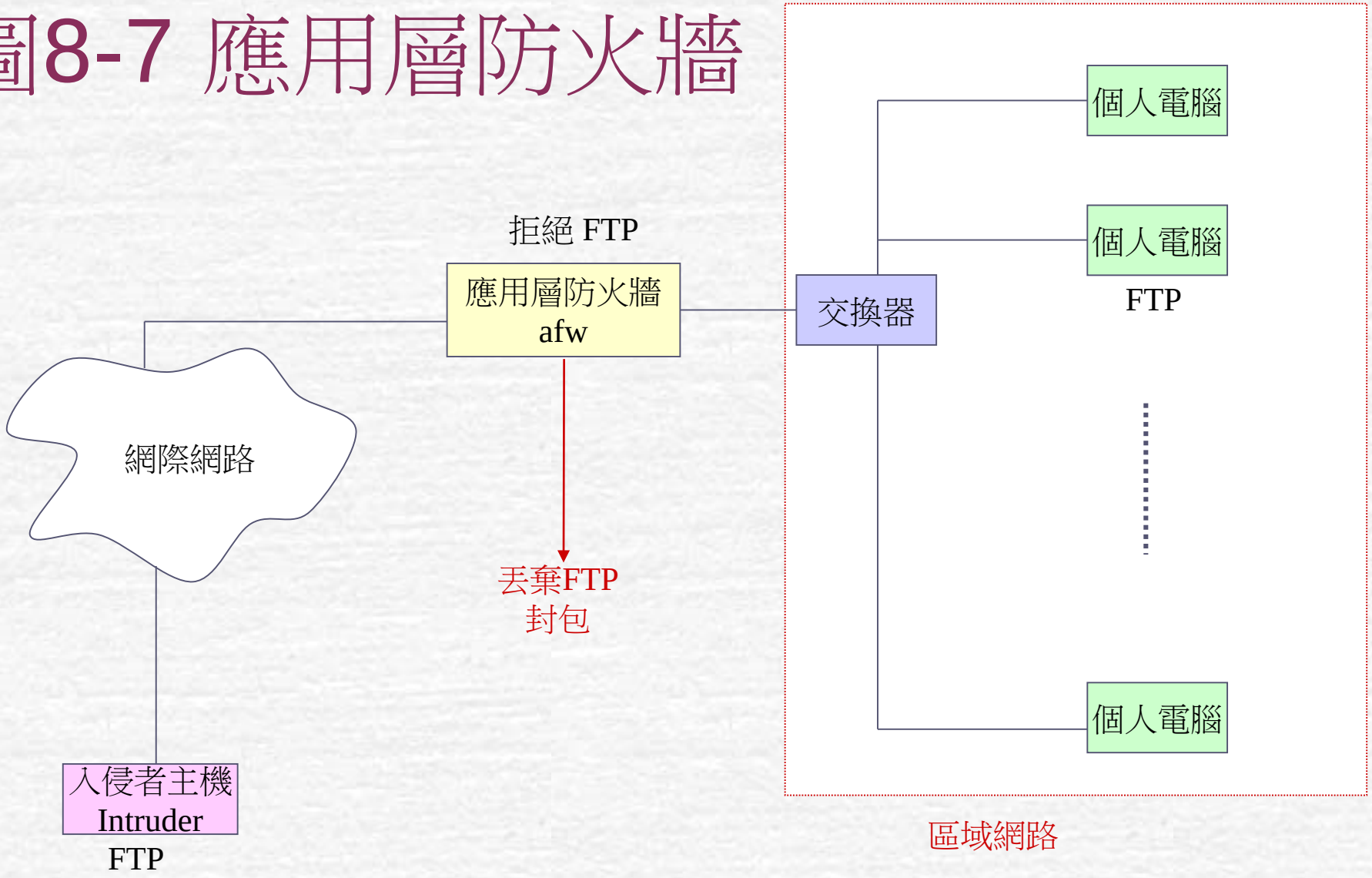

個人電腦
個人電腦
封包過濾防火牆
pfw
交換器
網際網路
168.19.2.12
來源IP的
封包過濾清單
個人電腦
拒絕來自
168.19.2.12
的封包
入侵者主機
Intruder
IP為168.19.2.12
區域網路

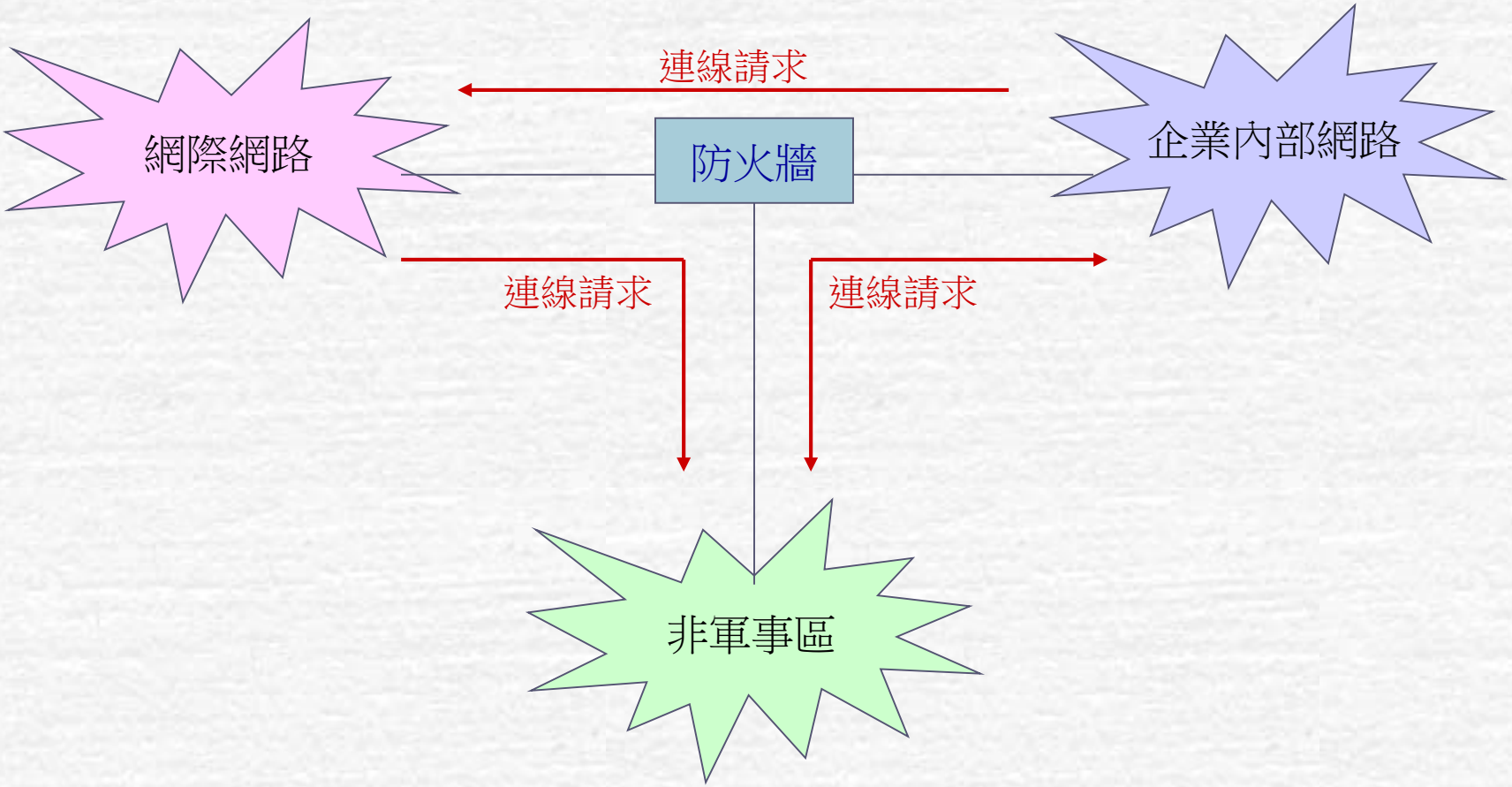
圖8-7 應用層防火牆


拒絕 FTP
應用層防火牆
afw
交換器
個人電腦
個人電腦
FTP
網際網路
丟棄FTP
封包
入侵者主機
Intruder
FTP
個人電腦
區域網路

防火牆的架設與管理

- 一般常見的設定方式之一，是利用防火牆架構出區隔企業內部網路、非軍事區、與網際網路三種不同安全等級的網路
- 企業內部與網際網路上的主機都可以透過防火牆連上非軍事區的網路
- 企業內部可以透過防火牆連到網際網路上的主機，但網際網路上的主機則沒有辦法主動連到企業內部網路上的電腦。
- 非軍事區的目的是希望將企業內部網路，與用來提供網際網路服務的網路區域隔離

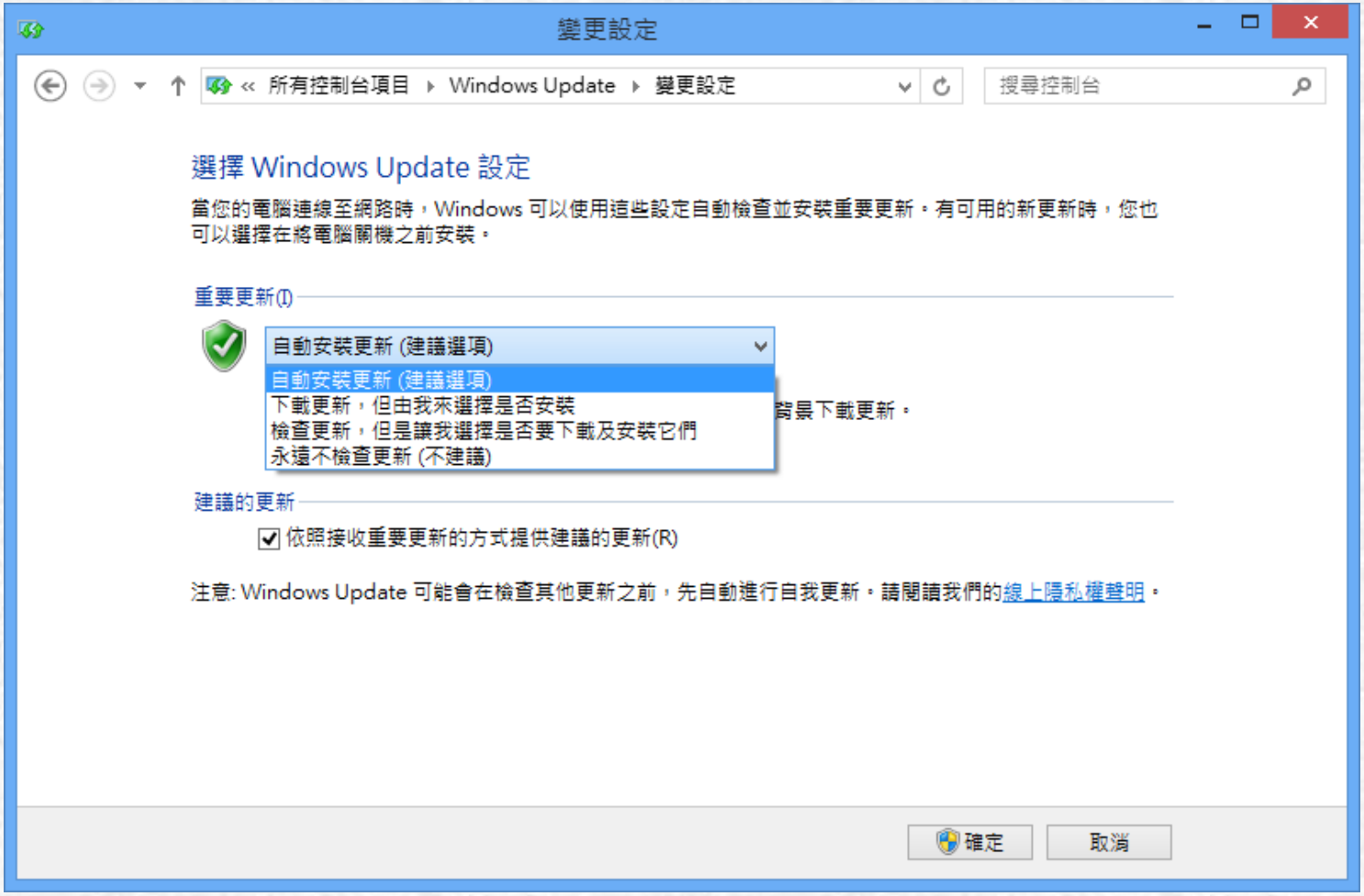
圖8-8 防火牆與非軍事區範例



定期更新作業系統與防毒軟體

- 定期更新作業系統的版本或修補程式，有助於降低被入侵的風險
- 定期更新防毒軟體的病毒碼也是非常重要的工作。

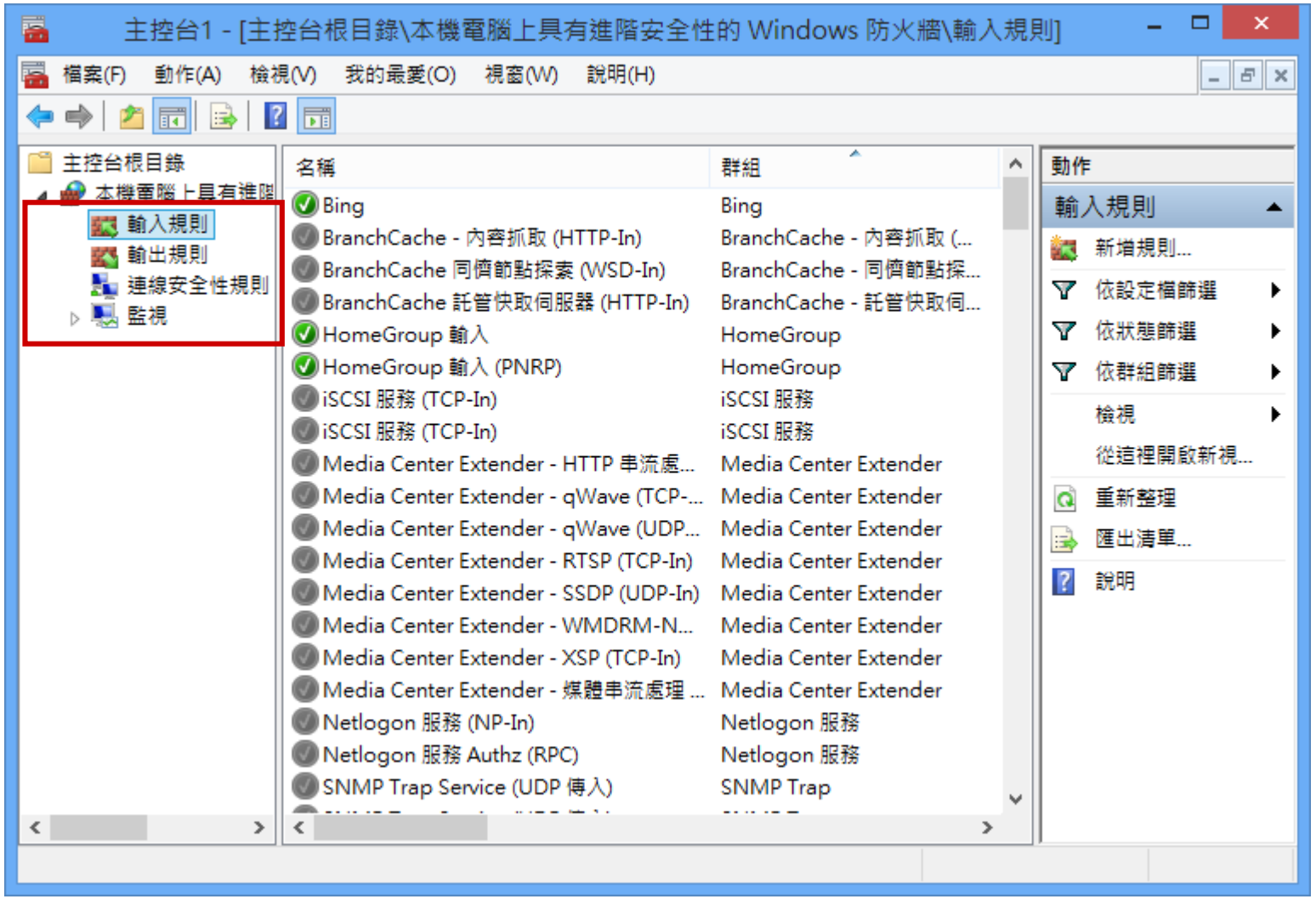
圖8-9 Window的自動更新設定畫面



Windows的防火牆功能

- Windows XP內建的簡易防火牆
  - 檢視或設定它目前允許連入的應用類型
  - 利用「新增連接埠」的功能，指定封鎖特定TCP或UDP的連接埠
- Windows Vista之後的防火牆
  - 提供雙向的能力，不僅可以阻止未經授權的網路交通流入，也可以防止未經授權的網路交通流出
  - 其他新功能：
    - IPSec (IP Security)協定
    - IPv6環境
    - 進入與離開防火牆的例外規則
    - 應用在特定電腦與使用者的例外規則
    - 應用在多種協定(不止TCP與UDP)上的例外規則
    - 應用在本機與遠端通訊埠的例外規則
    - 應用在特定界面類型(區域網路、遠端存取、或無線網路)的例外規則
    - 應用在特定Windows服務上的例外規則
    - 支援命令列形式的防火牆控制功能

圖 8-10 Windows防火牆管理畫面



動手做做看
使用Windows Defender
來掃描系統中是否有惡意程式

- 間諜軟體經常是伴隨使用者主動下載的物件，例如下載程式、螢幕保護程式等，而悄悄地植的電腦中
- 個人防火牆沒辦法把間諜軟體擋在門外
- Windows提供了間諜軟體防護程式--Windows Defender

圖8-11 Windows Defender

圖8-12更新Windows Defender的病毒及間諜程式定義檔

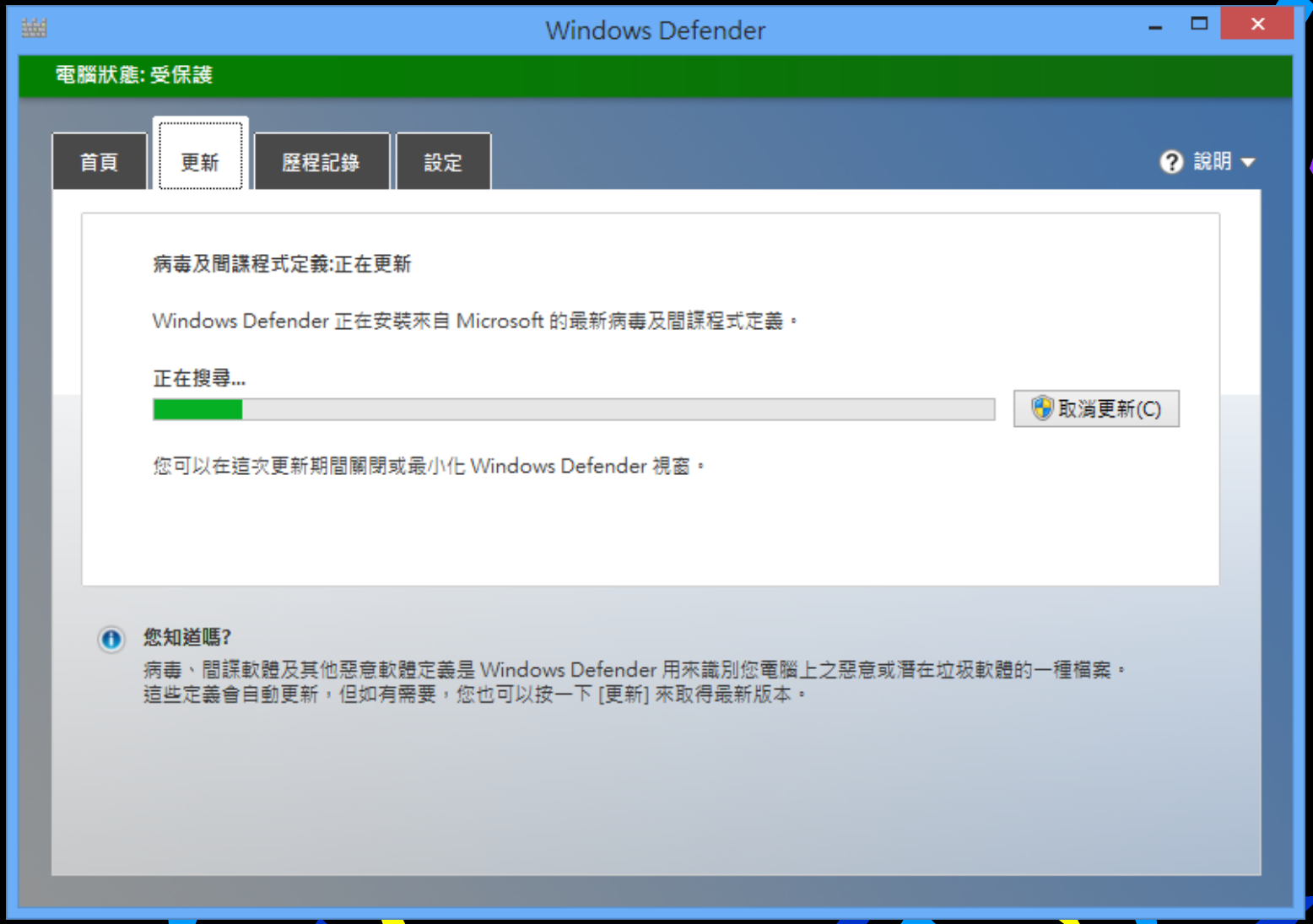
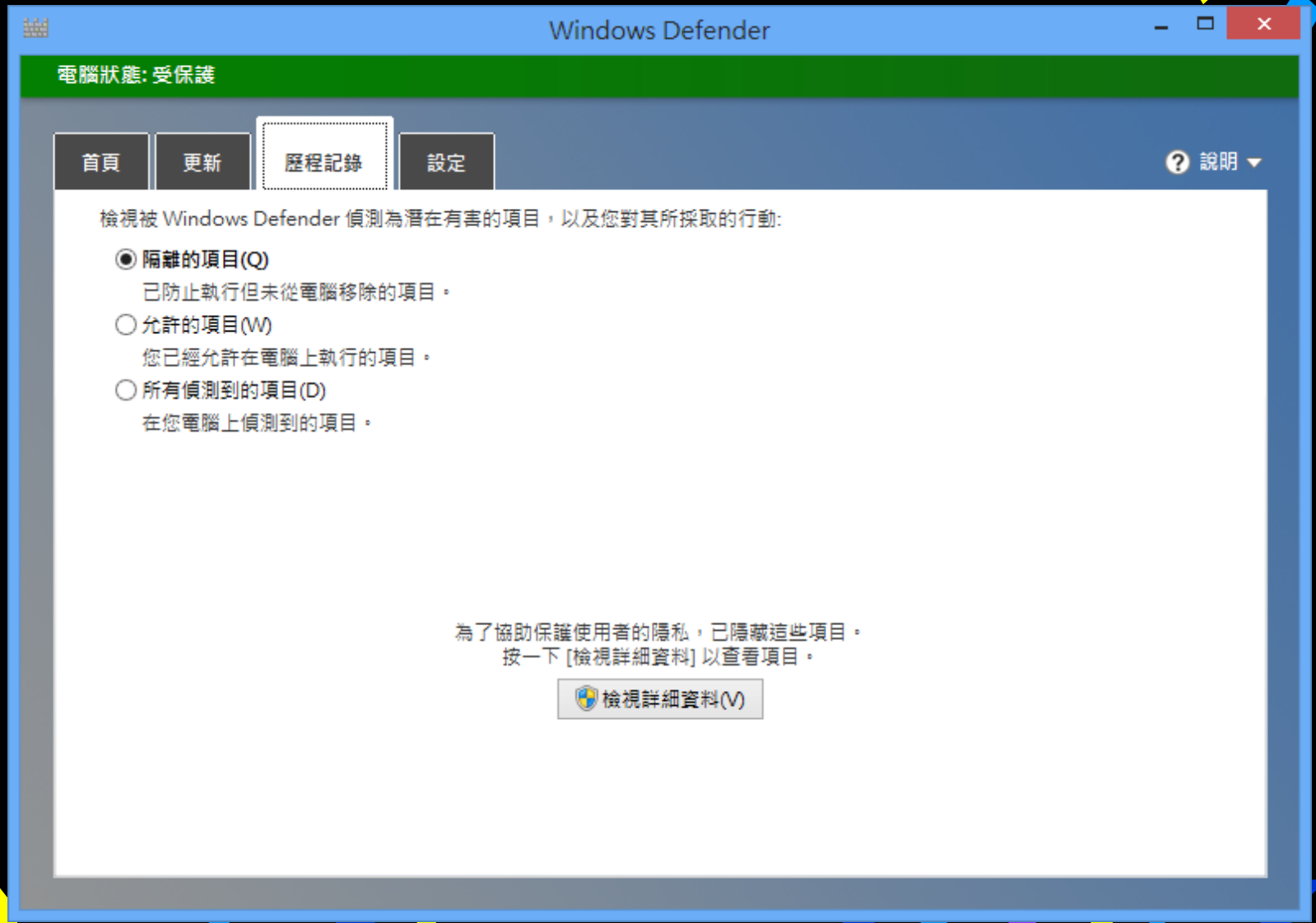


圖8-13 Windows Defender的歷程紀錄畫面



8-7電腦的安全等級

- 由美國國防部制定的電腦系統信任評估標準：
  - D級：最低保護
  - C級：自定式保護
    - C1又稱為鑑別式安全保護系統。大多數的Unix都是屬於C1等級
    - 在C2的環境中，系統上所有的活動都必須受到監督，並且將特定的權限分給某個使用者
  - B級：強制式保護
    - B1開始加入多層安全等級的管理
    - B2將安全層級的標示擴大到所有的裝置，並且開始考慮不同安全等級的物件互相溝通時的安全問題
    - B3等級的系統提供存取控制清單
  - A級：可驗證之保護。經過正規化查證的設計與測試