

初學者指南

Outpost 防火牆 3.0

來自 Agnitum 公司的
個人防火牆軟體

摘要

本指南主要向初學用戶介紹網際網路和 Windows 作業系統基礎，以及 Outpost 防火牆軟體。

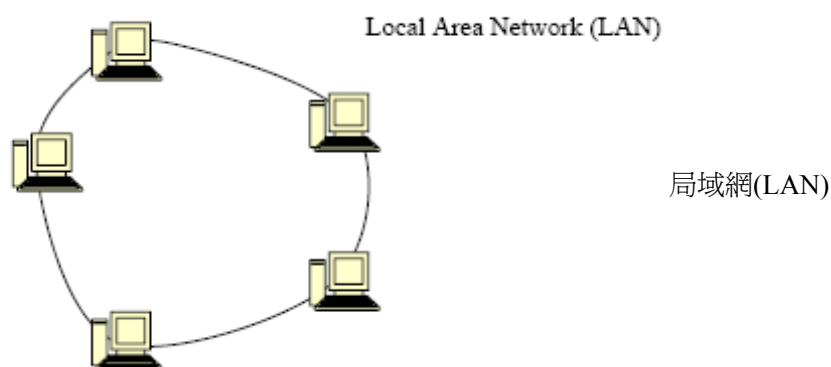
目錄

1 基礎	4
1.1 連網技術基礎.....	4
1.2 網際網路是如何工作的.....	5
1.3 網際網路的危險性.....	5
1.4 Windows 術語.....	7
2 OUTPOST 防火牆介紹	8
2.1 系統要求.....	8
2.2 OUTPOST 防火牆的性能.....	8
2.3 術語表.....	10
2.4 技術支援.....	16

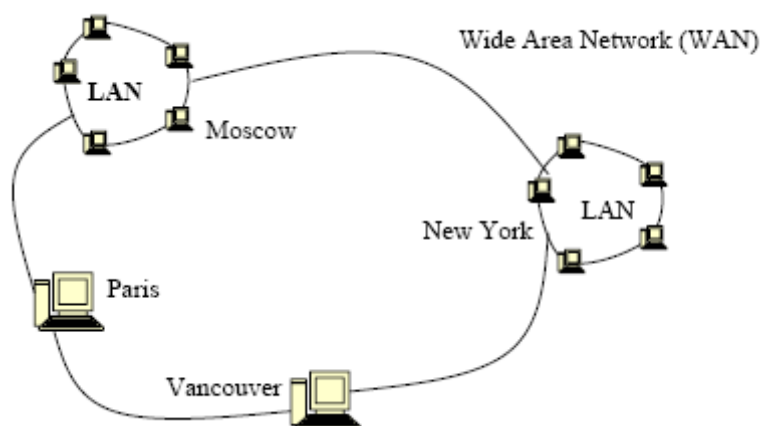
1 基礎

1.1 連網技術基礎

一個網路可以簡單地由兩台或兩台以上的電腦連接起來，從而，電腦上的檔能夠順利地在每台電腦之間進行共用或傳輸。最簡單的網路是局域網(LAN)，即局部區域網路。在局域網中，這些電腦處於相同的辦公室或辦公樓。一個局域網實際上能夠由許多台電腦組成。當您在辦公室或家中將兩台電腦連接起來，您便構建了一個局域網。



當位於不同大樓或城市的電腦被連接在一起時所形成的網路則被稱為廣域網(WAN)。一個廣域網可以由單個的電腦和局域網組成。



Wide Area Network (WAN) 廣域網(WAN)

LAN 局域網

Moscow 莫斯科

Paris 巴黎

New York 紐約

1.2 網際網路是如何工作的

網際網路是一個由眾多網路組成的網路。網際網路上存在著兩種基本類型的電腦，即伺服器和客戶機。伺服器是一台特別設置的用來為客戶機提供檔的電腦（使其檔可被客戶機流覽和下載）。客戶機則是您用來訪問網際網路的任何一台電腦：桌上型電腦，膝上型電腦，手提式電腦，手機等。伺服器向您的電腦提供的檔可以是網頁，視頻，聲音，圖像等。為了使您的家用電腦能夠從伺服器上接收檔或任何資料，您的電腦必須請求這些資訊。資訊請求發生在您在瀏覽器中輸入一個 URL 或您接收電子郵件的時候。

任何電腦都可以設置成爲一台伺服器或一台客戶機。當您的電腦連接到網際網路，在沒有適當的安全措施的情況下，任何人都能訪問您電腦上的檔。這就是爲什麼要使用防火牆的原因。防火牆是用來防止未經您的允許而訪問您電腦上的檔的情況發生的一種簡單方法。有很多不同種類的防火牆，並且這些不同種類的防火牆具有不同的性能。如同大部分軟體一樣，性能最強大的防火牆也是最難操作的。而目前唯一知道的例外則是 **Outpost 防火牆**，這款防火牆軟體從一開始便被設計成爲具有極強大的性能卻又很容易爲用戶使用。

1.3 網際網路的危險性

我們都聽說過網際網路和電腦空間的危險性。儘管其中某些危險性已被大大地誇大，但這並不能改變連接到網際網路上的電腦易於受到非常現實的攻擊的這一事實。不幸的是，我們的生活中存在著感到無助而被迫使其生活有別於其他人的瘋狂者和犯罪者（這兩種特質常常出現在一個人身上）。這些人當中有些人熟知電腦，並知道如何遠端存取電腦上的檔。這種人被稱爲電腦駭客或[解密高手](#)。爲了使他們遠離我們的系統，我們需要使用一款性能強大的防火牆。

以下是存在於網際網路上的主要危險性：

- 未經授權的應用程式可以背著您或不受您的控制即被傳輸到您的電腦上並獲得執行（例如，您流覽的網頁中插入的 [ActiveX](#) 或 [Java applets](#)）。這些程式能夠在您的電腦上執行任何操作，包括將包含您隱私資訊的檔傳輸到其他電腦上或僅僅刪除您電腦系統上的所有檔。
- 如果您的系統未能正確配置，無須秘密地在您的電腦上載入特殊軟體，其他電腦就能夠直接訪問您電腦上的檔。

- 某些資訊（以 [cookies](#) 或 [referrers](#) 形式）能夠被放置在您的電腦上，所以廣告者和其他人可以追蹤到您訪問過的網站，以及您感興趣的內容。
- [特洛伊木馬\(Trojan horses\)](#)能夠被放置在您的電腦上。特洛伊木馬是電腦駭客（[解密高手](#)）用來打开通向您的私人資訊大門的程式，如密碼，銀行資料以及信用卡號碼。特洛伊木馬和病毒之間的根本差異之一在於：存在於您電腦上的病毒是自發執行的，而特洛伊木馬則是由遠端入侵者設置並直接運行的。
- 網際網路[蠕蟲\(Worms\)](#)能夠作為電子郵件資訊的附件到達您的電腦。一些電子郵件程式未請求許可便打開附件。一些未意識到威脅的網路用戶則人工地打開所有附件。這些附件一旦被打開，蠕蟲便開始橫行並迅速感染您的電腦系統。
- [橫幅\(Banners\)](#)形式的非必要資料以及其他廣告會耗盡您的帶寬。儘管這些物件不能直接訪問或破壞您電腦上的資料，但他們將嚴重減慢您的網路連接速度，尤其對於撥號上網的電腦。
- [間諜軟體\(Spyware\)](#)在很多方面都和特洛伊木馬十分相似。這些程式未經您的同意而收集關於您和您的興趣（如您的上網習慣，您個人電腦上的其他軟體等等）。間諜軟體主要被線上軟體公司用於市場行銷目的。

1.4 Windows 術語

Windows 環境中存在著很多不同的物件，我們對這些不同的物件進行命名並陳列於以下表格中。因此，當這些術語涉及到 Outpost 檔時，就不會出現誤解或混淆。

對象	名稱
<input checked="" type="checkbox"/> 最小化到系統託盤	檢查框被選中
<input type="checkbox"/> 關閉按鈕最小化，不存在介面	檢查框被清除
<input type="radio"/> 入站	選項按鈕被選中
<input type="radio"/> 出站	選項按鈕被清除
常規 應用	跳格鍵
寬度：100	邏輯框

—
OK 按鈕

隱藏 Outpost 防火牆
顯示防火牆日誌查看器
策略
選項……
總在最前面
註冊……
關於……
退出並關閉 Outpost 防火牆

快顯功能表
通常在某物上或某個區域內右擊後彈出圖片。
如果您右擊 Outpost 防火牆系統託盤圖示（即藍色圈內的白色問號），
該圖片則顯示出現的功能表。

對話方塊

<p>選項</p> <p>常規 應用 系統 策略 插件</p> <p>啓動 _____</p> <p>選擇 Outpost 防火牆啓動模式</p> <p><input type="radio"/> 正常</p> <p><input type="radio"/> 背景</p> <p><input type="radio"/> 禁用</p> <p>雜項 _____</p> <p><input checked="" type="checkbox"/> 最小化到系統託盤</p> <p><input checked="" type="checkbox"/> 最小化主窗口到關閉</p> <p>密碼保護 _____</p> <p>設置密碼來保護您的設置</p> <p><input type="radio"/> 啓用</p> <p><input type="radio"/> 禁用 設置密碼……</p> <p>OK 撤銷 應用</p>

在 Windows 環境中，很多物件，如檔，對話方塊等，可以通過拖動滑鼠來移動。
拖動一個物件：

1. 將游標移動至您想拖動的對象。
2. 單擊滑鼠左鍵，並按住直至游標移動到您想拖動的對象。
3. 釋放滑鼠左鍵。

2 Outpost 防火牆入門

2.1 系統要求

Outpost 防火牆的最低系統要求為：

- 233MHz 英代爾奔騰或相容中央處理器
- 32MB 隨機記憶體
- Windows 98/2000/XP 或 2003 伺服器作業系統
- 30MB 硬碟空間

注：本軟體的正常操作不需要特殊的網路適配器或數據機，以及特殊的網路配置。

2.2 Outpost 防火牆的性能

Outpost 個人防火牆系統是一款高級的防火牆軟體，它結合了能力和高級特性，並擁有相當易於使用的介面。為了有效地使用 **Outpost 防火牆**，您無需瞭解 Windows 的內部運行。我們的工程師特別為您配置了默認設置。當然，您可以隨時更改這些設置的任何項目。請參見 Outpost 用戶指南以瞭解更多詳細內容。

Outpost 防火牆不容置疑的實力在於其模組結構。Outpost 防火牆的性能通過被稱作 [插件程式](#) (即帶 .ofp 副檔名的檔) 的特殊模組來實現。每個模組都是獨立的，並且能很容易地被添加到安裝的系統上。

Outpost 防火牆的主要益處是：

- **Outpost 防火牆**能保護您免遭從隱私到資料洩露和利用的眾多安全威脅。
- 在安裝後，無需任何客戶化，本防火牆即可立即使用。
- 本防火牆可自動配置達到最佳保護或使您簡單迅速地使用系統提示及默認設置來創建您自定義的安全配置，而無需打擾您的工作。
- 本防火牆的介面通過幾次擊鍵就能執行非常複雜的調整，從而調整您系統的安全性。
- 多種語言：**Outpost 防火牆**支援 14 種語言。

以下是 **Outpost 防火牆** 的眾多優點：

- 大量設置可以用來限制到達您的電腦以應用的網路訪問。高級用戶還可以根據需要調整服務協定，並創建特殊安全設施。
- 當您照常流覽網際網路時，秘密模式使您的電腦不被電腦駭客看見。
- 本系統的模組化結構使您添加了插件形式的新的保護性模組。
- 本系統與 Windows 98/2000/XP 和 2003 伺服器的所有版本都相容。
- 極低的系統要求。
- 您可以限制一系列訪問網路的應用程式，並指定每個應用程式容許的協定，埠和訪問方向（進入或離開）。
- 阻止或限制正被輸入您電腦的非經要求的資訊，特別是：
 - 橫幅廣告
 - 網頁上的彈出窗口
 - 來自特殊網頁的令人厭惡的內容
- 限制或禁止網頁內置的程式成分的操作，如 [Java applets](#), [Active X](#) 和 [JavaScript](#)。
- 限制或禁止 cookies 的使用。
- 指定一個“友好” IP 位址區域，例如您自己的局域網。在此區域內，**Outpost 防火牆** 不會控制或限制網路交換。
- 本防火牆可以對電子郵件的附件進行隔離，從而保護您的系統不受網際網路蠕蟲的感染。
- 本防火牆能對來自任何其他電腦的攻擊發出告警，並迅速阻止其訪問您的電腦。
- 高級資料庫驅動的日誌系統支援資料挖掘任務的自定義查詢。
- 在眾所周知的“洩露試驗”上十分成功。

2.3 術語表

ActiveX-創建動態網頁的一項技術。這項技術由ActiveX控制元件執行，即瀏覽器指定一個矩形區域的專門程式來執行，在此，該程式對用戶介面負全部責任。ActiveX技術支援全自動安裝。當瀏覽器遇到一個連接到控制元件的HTML鏈結時，ActiveX會首先檢查此元件是否已經存在於用戶的電腦上（比如，該元件以前是否被使用過）。如果檢查到該控制元件，瀏覽器將啟動該元件，並將運行該元件所必須的資料傳輸到該元件處。如果電腦上未發現該元件，瀏覽器將訪問HTML文件主體中規定的網站位址，然後下載，安裝並向Windows註冊新的控制元件。此項技術必須在Windows 9x/NT的特殊運行環境中使用。

Banner(橫幅)-通常是一個矩形的圖形表示的GIF或JPG格式的廣告，該廣告位於網頁上，並具有通向廣告者伺服器的超鏈結。

Broadcast(廣播)-用來向網路的各節點指派消息的特殊種類的IP地址。該廣播包含2種形式的廣播消息：
廣播或廣播消息-如果IP位址中的每個二進位位元為1，則資料包從消息包的來源處被指派至每個節點。
限制廣播或限制廣播消息-如果IP位址中的節點號中的每個二進位位元為1，則具有該位址的資料包將被指派至帶有指定號碼的各個節點。

Client(客戶機)-和**伺服器**相反，是用於訪問網際網路的電腦。

Cookie-由伺服器傳輸至瀏覽器並保存於用戶電腦上的小塊資訊。瀏覽器存儲此資訊，並不時將其傳輸至伺服器。某些cookies僅在一段時期內被存儲，當瀏覽器被關閉時，則被刪除。其他cookies則能被安裝至一段持續時間。

Datagram(資料報)-在TCP/IP網路中傳送的資料或資料包的單位。每個資料報包含來源，目的地址和資料。

DHCP(動態主機配置協定)-專用於IP位址動態分配的協定。除了動態分配，DHCP(動態主機配置協定)還支援允許人工和自動位址分配的更為簡單的靜態位址分配。DHCP(動態主機配置協定)會引發問題。第一個問題是在DHCP(動態主機配置協定)和DNS(功能變數名稱系統)服務中協調位址資料庫。第二個問題則是令網路控制進程複雜化的IP位址的頻繁變更。

DNS(功能變數名稱系統)-正式分配給網際網路上的單個網路和伺服器的名稱系統。與一串 IP 號碼相比，功能變數名稱系統是一種記住那些名稱的更簡單的方法。例如：www.agnitum.com 比 IP 地址 207.44.236.84 容易記的多。功能變數名稱系統服務能自動將這些名稱翻譯成相應的 IP 位址。該功能變數名稱系統要求其 tables 的靜態配置，此靜態配置一一對應對電腦名稱和 IP 地址進行定義。功能變數名稱系統協定在應用水準上是一個輔助服務協定。該協定為非對稱協定，其中定義了功能變數名稱系統伺服器和功能變數名稱系統客戶機。功能變數名稱系統伺服器存儲了包含對應名稱和 IP 位址的分散式資料庫。該資料庫根據網際網路上的管理域進行分佈。功能變數名稱系統伺服器的客戶機能識別其管理域內伺服器的 IP 位址，並能根據 IP 協定傳輸功能變數名稱系統名稱請求，然後等待與此名稱對應的 IP 位址。如果請求的資訊存儲於功能變數名稱系統伺服器的資料庫中，則伺服器將立即將回復傳輸至瀏覽器。否則，伺服器將該請求傳輸至另一區域的功能變數名稱系統伺服器，此伺服器不是處理請求本身就是將請求傳輸到其他功能變數名稱系統伺服器。所有功能變數名稱系統伺服器都根據網際網路的域分級制度併入層次結構。客戶機（瀏覽器）將查詢這些名稱伺服器直到找到必須的對應為止。功能變數名稱系統資料庫具有一個稱作功能變數名稱區域的樹狀結構，該樹狀結構中每個域（樹的節點）具有一個名稱，並包含子域。域的名稱確定了其在資料庫中的相對於父域的位置，並指出了名稱中相對於域節點的獨立部分。

DNS Address(功能變數名稱系統位址)-字元類型的網路位址，採用圓點(.)將不同的域的名稱分隔開來。該位址和功能變數名稱系統資料庫中的網路位址相對應。例如，www.agnitum.com

DOS(拒絕服務)攻擊-在網際網路或某個網路上，來自其他電腦的對某人電腦的攻擊。這種類型的攻擊利用網路軟體或協定中的錯誤來干擾您電腦的正常運行狀態。

Flash Animation(Flash 動畫)-Marcomedia Flash 技術製作的多媒體晶片。將大大擴展了網頁功能性和外觀的互動網頁內容傳遞給用戶。

FTP(檔傳輸協議)-將檔從一台電腦傳輸到另一台電腦上的一項網際網路服務。

Gateway(閘道)-連接兩個網路，並將資料包從一個網路傳輸到另一個網路的電腦。(和路由器一樣)

GGP(閘道到閘道協定)-一種協定，在此協定中兩個閘道往往與另一個相互作用，特別在執行控制任務的過程中。

GRE(通用路由封裝)-將不同的電腦系統連接起來，使他們之間能交換資料的一種方法。

GUI(圖形用戶介面)-在過去的10年中，實現了大多數電腦用戶的期望的軟體介面類型。這種介面運用了按鈕圖像，圖示，桌面類比等元素。蘋果公司的Macintosh電腦是使用GUI(圖形用戶介面)的第一批受歡迎的電腦之一。微軟Windows則是稍後出現的圖形用戶介面。

Page Navigation Scripts(網頁導航腳本)-當網路用戶導航至或離開該網頁時，用於處理網頁載入和卸載事件的腳本。由於這些是用戶在網際網路上衝浪時實施的最普通行為，網頁導航腳本則是最經常執行的，並可能執行令人厭惡的行動，如展示彈出視窗或橫幅廣告。

Hidden Frame(隱藏幀)-幀頁，也叫框架標記，即分成兩個或兩個以上幀頁的網頁，每個幀頁指向一個獨立的網頁。一個幀頁上的幀還可以指向另一個幀頁。幀可以隱藏起來，因此他們不在瀏覽器視窗顯示，不被用戶所見，但仍可被瀏覽器載入並處理。隱藏幀包含無需為用戶所察覺而運行的元素，並且導致妥協的安全性和較低的隱私性。

HTML(超文本標記語言)-一種可以嵌入到文字檔案中的標記語言，這種語言被瀏覽器用於製作特製網頁，並使瀏覽器可以在網際網路上到處流覽。有了HTML(超文本標記語言)，網頁設計者可以將圖形和文本結合起來，提高文本外觀的美化程度，並在頁面上添加鏈結，從而向流覽網頁的用戶提供一種互動。

ICMP(網際網路控制資訊協定)-允許網際網路節點對異常運行狀況報告錯誤或提交資訊。ICMP資訊通過IP資料報的資料領域中的網際網路進行傳輸。ICMP資訊的最終目標既不是應用程式也不是目的機器上的用戶，而是某人電腦上的IP軟體。任何電腦都可以將ICMP資訊發送至任何其他電腦。

IGMP(網際網路組管理協定)-被節點和路由器用來支援資訊的組指派。IGMP(網際網路組管理協定)向實體網路通知當前結合到組的節點，以及這些節點屬於哪些組。

IP(網際網路協定)-網際網路協定的網路級設置。

IP Address(IP 位址)-由 4 個位元組組成的位址，通常由被一個圓點(.)隔開的 4 個小數表示。例 64.176.127.178.IP 位址用於網路級。當配置電腦和路由器時，網路管理器將指定 IP 位址。IP 位址由兩部分組成：網路號和節點號。如果網路未連接到網際網路上，則網路管理器能夠任意選擇網路號。否則，IP 位址則根據特殊網際網路子部分(網路資訊中心 NIC)的建議進行分配。

IP Datagram(IP 資料報)-在 TCP/IP 網路中傳輸的資料或資料包的單位。每個資料包包含來源，目的地址和資料。

Java Applet-用 Java 編程語言編寫的電腦程式，該程式嵌入在網頁中。儘管被直接併入網頁中，該程式仍作為一個獨立的檔被存儲。

JavaScript-嵌入在網頁中的一種程式，其用途通常為提高閱讀者流覽網頁的經驗。

Loopback(回送)-在無需在網路上發送資料包的情況下，在節點上測試軟體，為測試回饋所保留的一個特殊 IP 位址(127.0.0.1)。

Multicast(多播)-以順序 255 為起點的一組特殊的 IP 地址。如果多播位址被規定為資料包中的分配位址，則所有具有該位址的節點將接收該資料包。這些節點通過他們屬於哪些組來識別他們自身。相同的節點可被包括在幾個組中。這種資訊被稱為組資訊。組位址不被劃分到網路和節點號領域，且由路由器以一種特殊方式加以處理。

NetBIOS(網路基礎輸入/輸出系統)-由 IBM 公司開發的一種基礎網路協定，該協定用於網路上的檔和印表機共用。IBM(IBM 個人電腦廣域網)，Novell NetWare，微軟 Windows 以及其他公司的網路均支援 NetBIOS(網路基礎輸入/輸出系統)。

Plug-in(插件程式)-可以添加到套裝軟體或從套裝軟體移除，從而擴展該軟體的性能的一種獨立的元件。軟體必須設計並建立為支援插件程式。插件技術允許第三方開發者針對該軟體創建特定的插件，從而使該軟體相對於原來設計的軟體能做更多事情。

Pop-up Window(彈出視窗)-無需用戶介面而創建的瀏覽器實例，其用途是展示如橫幅或廣告這類討厭的內容。這種彈出視窗將會降低網際網路的速度及舒適度，還可能危及瀏覽安全性。

Port(埠)-與資料類型相對應的號碼，因此不同類型的資料可以被有效地發送至適當的應用程式。埠不是物理意義上的插頭或插座，而是邏輯意義上的埠，它僅指派在軟體中。

PPTP(點到點隧道協議)-啓用網際網路上的安全通信的一種技術，能夠使通信不被中途攔截。

Preset(預置)-Outpost 防火牆中的預置是事件或行動的預定義設置或設置組。通過單擊滑鼠，預置可以同步應用很多設置。這樣，預置可以為需要人工應用每個設置的用戶節約時間。

Protocol(協議)-特殊類型的通信交換的一組公認準則。當兩台電腦在雙方之間傳輸資料時按程式使用相同的協定，該資料將被正確地延遲。否則，如果兩個不同的協議被使用，那麼資料傳輸將不會發生。

Proxy Server(代理伺服器)-管理發送器和接收器之間的連接的軟體。所有輸入被重新定向到不同的埠，該埠能防止解密高手訪問專用網路。

Referrer(推薦者)-HTTP 請求的一部分，該 HTTP 請求包含請求之前最後訪問的網頁的 URL。

Router(路由器)-連接兩個網路並將資料包從一個網路傳輸至其他網路的電腦（和**閘道**一樣）。

RPC(遠端程式呼叫)-支援分散式應用程式（元件位於不同電腦上的那些應用程式）。當需要使用涉及相同網路中另一電腦的功能時，應用程式會發出一個 RPC(遠端程式呼叫)。RPC(遠端程式呼叫)應用於涉及微軟 Windows 環境的客戶機/伺服器應用程式。

Scripting ActiveX Elements(Scripting ActiveX 元件)-不直接併入 HTML(超文本標記語言)網頁代碼，而是從在該網頁運行的腳本上創建的 ActiveX 元件。儘管流覽網頁的用戶不是總能看到相關腳本，但這些 ActiveX 元件可以揭露對於用戶系統的威脅。

Server(伺服器)-通過網路將檔和網頁發送至客戶機的電腦。

SMB(服務資訊塊)-與 NetBIOS(網路基礎輸入/輸出系統)一起應用的檔共用的一種方法。SMB(服務資訊塊)主要通過一系列客戶機要求和伺服器回應來工作。SMB(服務資訊塊)客戶機及伺服器軟體存在於各個版本的微軟 Windows 中。

Spyware(間諜軟體)-秘密或安裝在您電腦上的隱藏軟體或某些軟體的隱藏部分。Spyware(間諜軟體)背著網路用戶收集資訊（通常出於行銷目的）並將收集到的資訊發送至開發該間諜軟體的作者或組織。

SSL(安全套接字層)-用於支持 Web 伺服器的安全訪問的特殊協定。該協定是一種對客戶機和伺服器之間的交換進行編碼的主要協定。

TCP(傳輸控制協定)-確保資訊的可靠傳遞的一種主要的通信協議。TCP 連接總是在兩點之間進行。

Telnet(電信網路協定)-連接網際網路工具（如流覽器（帶資料庫），圖書館目錄及其他世界範圍的資訊資源）的程式。

Trojan Horse(特洛伊木馬)-秘密放置於您的電腦上的一種程式，這種程式與遠端入侵者建立了連接。特洛伊木馬根據來自攻擊者電腦的指示運行或自動傳輸入侵者編制的資訊。這種資訊通常是密碼或其他存儲於用戶電腦上的機密資料。

UDP(用戶資料報協定)-直接向應用程式提供簡單的低水準網路資料包傳輸和接收工具的協定。UDP(用戶資料報協定)不控制資料傳輸，也不定義接收或發送的單個資訊之間的相互關係。由於 UDP(用戶資料報協定)不保證可靠的資料傳輸，使用該協定的應用程式通常對每個資料包進行編號，如有必要的話，還

將對資料重傳進行初始化。要求一個廣播或 IP 連接的群體功能的所有應用程式只應與 UDP(用戶資料報協定)一起運行。

URL(統一資源定位器)-關於網上資源識別和檢索的環球網公認的地址，如網站，網頁，圖像，視頻，檔等。統一資源定位器具有以下外部特徵：

[協議]://主機[:埠][路徑]，其中：

- 協定是一個協定名稱，如 http，ftp 等。如果未指定協議，則默認為 http。
- 主機為 IP 位址或 DNS(功能變數名稱系統)位址。
- 埠是規定伺服器的埠號的任選參數。例如，在 http 協定中，通常使用埠 80；如果 http 協議中未規定埠，則默認為埠 80。
- 路徑是通向檔的全稱路徑，包括其名稱。如未規定路徑，則伺服器傳輸其主頁。

VBScript-嵌入網頁中的一個程式，其用途通常為提高閱讀者流覽網頁的經驗。

Web-抽象的網際網路空間，在此空間中，網路用戶能夠訪問由超鏈結連接的多種檔類型和檔案。還可參見 HTML(超文本標記語言)。

Worm(也稱為網際網路蠕蟲)-蠕蟲是一種在網路上通過繁殖自身的自我複製程式。它們會損害檔系統並/或僅僅佔用帶寬。蠕蟲通常使用電子郵件客戶在網路上複製其自身。當康乃爾大學的羅伯特·莫里斯(Robert Morris)於 1998 年在網際網路上製造了關閉眾多 Unix 電腦的蠕蟲病毒程式時，蠕蟲開始變得臭名昭著了。近期的蠕蟲病毒是 MyDoom(諾維格)及其變種—NetSky(網路天空)和 Bagel。

2.4 技術支援

如果您在使用 Outpost 防火牆上需要協助，請訪問 <http://www.outpost.com.hk/support/>的支援頁面，尋求可用的支援選項，包括常見問題解答，文獻彙編，論壇，帖士加竅門以及故障查找。