

Beginner
Guide

Outpost Client Firewall

Personal Firewall Software
from
Agnitum

Abstract

This guide will introduce novice users to Internet and Windows operating system basics, as well as give the users introduction to Outpost Client Firewall software.

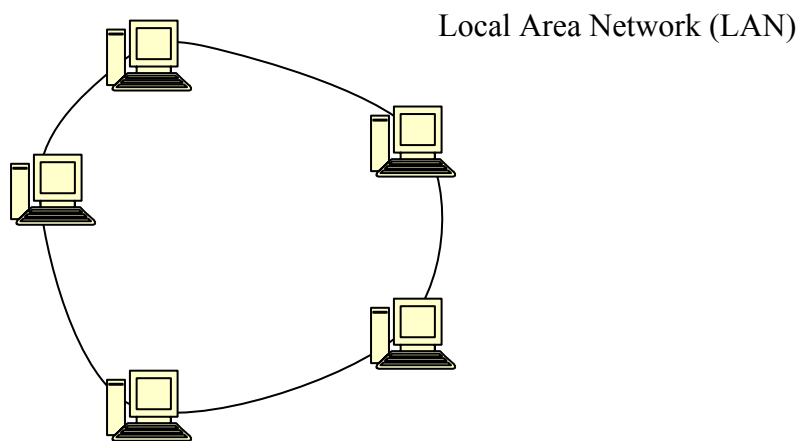
Table Of Contents

1	THE BASICS	4
	1.1 NETWORKING BASICS	4
	1.2 HOW THE INTERNET WORKS	5
	1.3 INTERNET DANGERS	5
	1.4 WINDOWS TERMINOLOGY	7
2	INTRODUCTION TO OUTPOST CLIENT FIREWALL.....	8
	2.1 SYSTEM REQUIREMENTS.....	8
	2.2 OUTPOST CLIENT FIREWALL CAPABILITIES	8
	2.3 GLOSSARY	10
	2.4 TECHNICAL SUPPORT	16

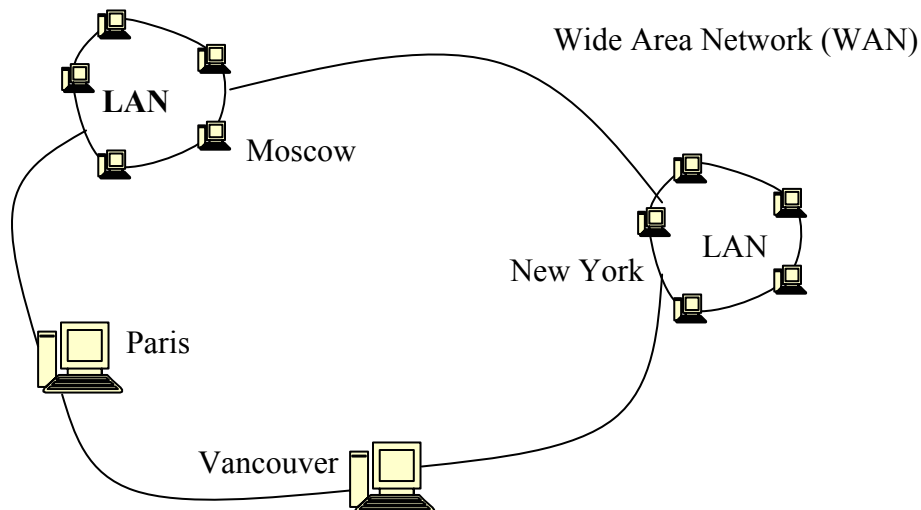
1 The Basics

1.1 Networking Basics

A network is simply two or more computers linked together so their files can easily be shared or transferred from computer to computer. The simplest network is the LAN, the Local Area Network. These computers are in the same office or building. A LAN can have virtually any number of computers. You make a LAN when you connect two computers together in your office or at home.



When computers in different buildings or cities are connected together, the network is called a WAN or Wide Area Network. A WAN can be comprised of individual computers and LAN's.



1.2 How The Internet Works

The Internet is a network of networks. There are two fundamental types of computers on the Internet, servers and clients. A server is a computer specifically set up to serve its files (make its files available for viewing or download) to client computers. A client is any computer you use to access the Internet: desktop, laptop, handheld, cell phone, etc. The files a server makes available to your computer can be web pages, videos, sounds, images, etc. For your home computer to be able to receive files or any data from a server, your computer must request this information. This happens when you enter an URL in your browser or when you receive e-mail.

Any computer can be set up as a server or a client. Without the proper safeguards, anyone can access the files on your personal computer when it is connected to the Internet. This is why a firewall is used. A firewall is a simple way to protect your computer from having its files accessed without your permission. There are many different kinds of firewalls and they have different capabilities. As with most software, the most powerful firewalls are the hardest to operate. The only known exception at this time is **Outpost Client Firewall**, which was designed from the start to be extremely powerful yet easy to use.

1.3 Internet Dangers

We have all heard of the dangers of the Internet and cyberspace. Although some of these have been greatly exaggerated, it does not alter the fact that a computer connected to the Internet is liable to very real attacks. Unfortunately, there are mads and criminals (often combined in one person) who feel compelled to make life difficult for others. Some of these know about computers and how to access files remotely. These are called hackers or [crackers](#). To keep them out of our systems we need to use a strong firewall.


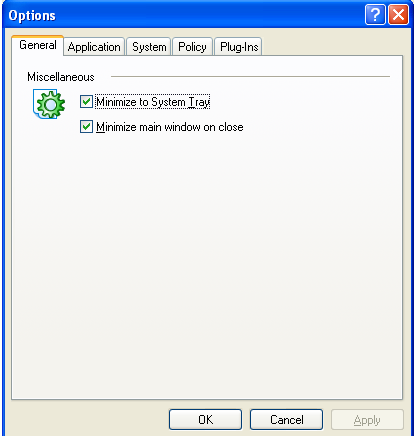
Here are the main dangers:

- Unauthorized applications can be delivered to your computer and be executed without your knowledge or control (for example, [ActiveX](#) or [Java applets](#) embedded in a web page you are browsing). These programs can perform any operation on your computer, including transferring files containing your private information to other computers or simply erasing all the files on your system.
- If your system is not properly configured other computers can access your files directly without someone having to surreptitiously load special software on your computer.

- Some information (in the form of [cookies](#) or [referrers](#)) can be placed on your computer, so advertisers and others can track the sites you visit and what your interests are.
- [Trojan horses](#) can be placed on your computer. Trojans are programs used by hackers ([crackers](#)) that open the door to your private information, such as passwords, banking data and credit card numbers. One of the fundamental differences between a Trojan and a virus is that a virus on your computer executes autonomously, whereas a Trojan horse is constructed to be used directly by a remote intruder.
- Internet [worms](#) can get to your computer as attachments to e-mail messages. Some e-mail programs open attachments without asking for permission. Some users, unaware of threats, open all attachments manually. Once opened, the worm executes and rapidly infects your system.
- Unnecessary data in the form of [banners](#) and other advertisements use up your bandwidth. Although these objects cannot directly access or damage the data on your computer, they can significantly slow your connection, especially on a dial-up.
- [Spyware](#) is in many ways similar to Trojans. These programs gather information about you and your interests (such as your surfing habits, what other software you have on your PC, etc.) without your knowledge or consent. Spyware is mostly used by on-line or software corporations for marketing purposes.

1.4 Windows Terminology

There are many different objects in the Windows environment, which are shown and named in the table below so there is no misunderstanding or confusion when these items are referred to in Outpost documentation.

Object	Name
<input checked="" type="checkbox"/> Minimize to System Tray	Check box selected
<input type="checkbox"/> Close button minimizes, not exits interface	Check box cleared
<input checked="" type="radio"/> Inbound.	Option button selected
<input type="radio"/> Outbound.	Option button cleared
General Application	Tab
Width: 100	Text box
OK	Button
	<p>Shortcut menu</p> <p>Generally pops up from a right-click on something or within an area. The picture shows menu that appears if you right-click the Outpost Client Firewall system tray icon (the white question mark in the blue circle).</p>
	Dialog box

In Windows, many objects, such as files, dialog boxes, etc. can be moved by dragging them with the mouse.

To drag an object:

1. Move the cursor to the object you want to drag.
2. Click the left mouse button and keep it pressed while moving the cursor to where you want to drag the object.
3. Release the left mouse button.

2 Introduction to Outpost Client Firewall

2.1 System Requirements

The minimum system requirements for **Outpost Client Firewall** are:

- 233 MHz Intel Pentium or compatible CPU
- 32 MB RAM
- Windows 98/2000/XP or 2003 Server operating system
- 30MB of hard disk space.

Note: No special network adapter or modem as well as no special network configuration settings needed for the normal operation of the software.

2.2 Outpost Client Firewall Capabilities

The **Outpost Client Firewall** system is advanced firewall software that combines power and advanced features with a remarkably easy-to-use interface. To effectively use **Outpost Client Firewall**, you do not need to know the inner workings of Windows. Our engineers specifically configured the default settings for you. Of course, you can change any of these many settings at any time. See the Outpost User Guide for details.

An indubitable strength of **Outpost Client Firewall** is its modular organization. **Outpost Client Firewall's** capabilities are implemented as special modules called [plug-ins](#), files with the **.ofp** extension. Each module is independent and can easily be added to an installed system.

These are the major benefits of **Outpost Client Firewall**:

- **Outpost Client Firewall** protects you against the number of security threats from privacy issues to data leaks and exploits.
- It can be used immediately after installation without any customization.
- It can auto-configure for the best protection or will let you easily create your custom secure configuration very quickly using system prompts and default settings without interrupting your work.
- The interface performs very complicated adjustments to the security of your system with just a few keystrokes.
- Multi-language: **Outpost Client Firewall** supports 7 languages.

And here are some of **Outpost Client Firewall's** many strengths:

- A number of settings can be used to restrict network access both to your computer and from your applications. Advanced users can also adjust service [protocols](#) and create special security facilities as required.
- Stealth mode makes your computer invisible to hackers while letting you browse the Internet as usual.
- The modular structure of the system lets you add new protective modules in the form of plug-ins.
- The system is compatible with all versions of Windows 98/2000/XP and 2003 Server.
- Impressively minimal system requirements.
- You can restrict a list of applications having access to the network and specify acceptable [protocols](#), [ports](#) and directions of access (incoming or outgoing) for each of these applications.
- Block or restrict non-requested information being sent to your computer, in particular:
 - Banner advertisements
 - Pop-up windows on web pages
 - Objectionable content data from specific web pages.
- Restrict or prohibit the action of program components built into web pages, such as [Java applets](#), [ActiveX](#) scripts and [JavaScript](#).
- Restrict or prohibit the use of [cookies](#).
- Specify a zone of “friendly” [IP addresses](#), your own LAN for example. In this zone, **Outpost Client Firewall** does not control or restrict network exchange.
- Can quarantine e-mail attachments to protect your system from Internet worms.
- Warns of any indication of someone attempting an attack of your computer from any other computer and instantly prevents access.
- Advanced database driven Log System supports custom queries for data mining tasks.
- Successful on all known “leak-tests”.

2.3 Glossary

ActiveX - is a technology of creating active web pages. This technology is implemented with the ActiveX control element—a dedicated program, for which the browser allocates an area of rectangular form, where this program is completely responsible for the interface with the user. The ActiveX technology supports fully automated installation. When the browser encounters an [HTML](#) link to the control element, it first checks if this element is already on the user's computer (i.e. if it was used before). If the control element is found, the browser starts it and transfers the data necessary for operation to it. If this component is not already available on the computer, the browser accesses the web address specified in the HTML document body, then downloads, installs, and registers the new control element with Windows. This technology is rigidly bound to the specific operational environment of Windows 9x/NT.

Banner - is generally a rectangular, graphic representation of an advertisement in GIF or JPG format located on a web page with a hyperlink to the advertiser's server.

Broadcast - is a special kind of [IP address](#) used to dispatch a message to all nodes of a network. There are two forms of broadcasting messages:

Broadcast or **broadcasting message** - if every binary bit in the IP address is a 1, the package is dispatched to all network nodes from where the source of the package is.

Limited broadcast or **limited broadcasting message** - if every binary bit in the node number in the address is a 1, then the package having such an address is dispatched to all network nodes with the specified number.

Client – is a computer that accesses the Internet, as opposed to a [server](#).

Cookie - is a small piece of information transferred by the server to a browser and saved on the user's computer. The browser stores this information and sometimes transfers it to the server. Some cookies are stored only during one session and deleted when the browser is closed. Other cookies are installed for an extended period.

Cracker – is someone who gains unauthorized access to a computer.

Datagram - is the unit of data, or packet, transmitted in a [TCP/IP](#) network. Each datagram contains source and destination addresses and data.

DHCP (Dynamic Host Configuration Protocol) - is a [protocol](#) intended for dynamic assignment of [IP addresses](#). In addition to dynamic assignment, DHCP supports simpler methods of static assignment of addresses allowing addresses to be assigned both manually

and automatically. DHCP can cause problems. First is the problem of coordinating the address database in DHCP and [DNS](#) services. Second is a frequent change of the IP addresses that complicates network control procedures.

DNS (Domain Name System) - is a system of names officially assigned to individual networks and servers on the Internet as an easier method of remembering those names than a string of IP numbers. For example: www.agnitum.com is easier to remember than the IP address 207.44.236.84. The DNS service automatically translates the name to its corresponding IP address. The DNS system requires a static configuration of its tables, which define the one to one correspondence of computer names and IP addresses. The DNS protocol is an auxiliary service protocol at the application level. This protocol is an asymmetric one - DNS servers and DNS clients are defined in it. DNS servers store a part of the distributed database that contains the correspondence of names and IP addresses. This database is distributed according to administrative domains on the Internet. Clients of the DNS server know the IP address of the server of their administrative domain and they transfer a request with the DNS name according to the IP protocol, and then wait for the IP address that corresponds to this name. If the requested information is stored in the DNS server's database, the server immediately transfers the answer to the browser. Otherwise, the server transfers a request to the DNS server of another domain, which can either process the request itself or transfer it to another DNS server. All the DNS servers are integrated in the hierarchical structure according to the domain hierarchy of the Internet. A client (browser) interrogates these name servers until it finds the necessary correspondence. The DNS database has a tree structure called a domain area of names, in which each domain (a node of the tree) has a name and can contain sub-domains. The name of a domain identifies its position in this database in relation to the parent domain, and points in the name separate parts corresponding to the domain nodes.

DNS address - is a network address of a character type, in which the names of different domains are separated from each other by a dot (.). This address corresponds to the network address in the DNS database. For example, www.agnitum.com.

DOS (Denial of Service) attack - is an attack on one's computer from other computers on a network or the Internet. This type of attack takes advantage of errors in network software or protocols and results in a disturbance of the normal operating conditions of your computer.

Flash animation – Multimedia clip made with Macromedia Flash technology. Delivers interactive Web page content that greatly extends Web pages functionality and appearance to the user.

FTP (File Transfer Protocol) - is an Internet service for transferring files from one computer to another.

Gateway - is a computer connecting two networks and transmitting packages from one network to another (the same as a router).

GGP (Gateway to Gateway Protocol) - is a protocol two gateways use to interact with one another, specifically in executing control tasks.

GRE (Generic Routing Encapsulation) - is a way to connect very different computer systems so they can exchange data.

GUI (Graphics User Interface) – is the type of software interface most computer users have come to expect in the last decade. It uses button images, icons, desktop analogy, etc. Apple's Macintosh computer is one of the first popular computers with a GUI. Microsoft Windows is a later GUI.

Page navigation scripts – These are scripts that handle web page load and unload events—that is when the user navigates to or from that web page. Since this is the most common action the user performs while surfing the Internet, these scripts are executed most often and may perform annoying actions such as displaying popup windows or banner ads.

Hidden frame – A frames page, also called a frameset, is a web page that is divided into two or more frames, each of which points to a separate web page. A frame on a frames page can also point to another frames page. Frames can be hidden so they are not displayed in the browser window—not visible to the user—but are loaded and processed by the browser. A hidden frame can contain elements that operate without the user being aware of them and this may result in compromised security and lower privacy.

HTML (HyperText Markup Language) - is a language of tags that can be embedded into a text file that a browser uses to make a fancy web page and makes it easy to browse here and there over the Internet. With HTML a web page author can combine graphics with text, enhance that text appearance and add links in the page that can supply an interaction with the person viewing that page in a browser.

ICMP (Internet Control Message Protocol) - allows Internet nodes to report on errors or submit information on unusual operating conditions. ICMP messages are transferred via the Internet in the data field of [IP datagrams](#). The ultimate goal of ICMP messages is not an

application program or the user on a machine-target, but IP software on one's computer. Any computer can send an ICMP message to any other computer.

IGMP (Internet Group Management Protocol) - is used by nodes and [routers](#) to support group dispatch of messages. It informs the physical network of the nodes that are currently combined into groups and to what groups those nodes belong.

IP (Internet Protocol) - is a network-level set of Internet [protocols](#).

IP address - is an address comprised of 4 bytes, usually represented as 4 decimal numbers separated by a dot (.). For example: 64.176.127.178. The IP address is used at the network level. A network manager assigns it when configuring computers and routers. The IP address consists of two parts: the network number and the node number. The manager can select the network number arbitrarily if the network is not connected to the Internet. Otherwise, the IP address is assigned according to recommendations made by the special Internet subdivision (Network Information Center, NIC).

IP datagram - is the unit of data or packet, transmitted in a [TCP/IP](#) network. Each datagram contains source and destination addresses and data.

Java applet - is a computer program written in the Java programming language and is embedded in a web page. Although the program is integrated directly with a web page, it is stored as a separate file.

JavaScript - is a program embedded within a web page, generally with the purpose to enhance the viewer's experience when browsing that web page.

Loopback - is a special IP address (127.0.0.1) reserved for feedback when testing software on a node without having to dispatch the packets on the network.

Multicast - is a special group of [IP addresses](#) beginning with the sequence 255. If a multicast address is specified as an assignment address in a packet, all nodes having that address will receive that packet. The nodes identify themselves by which groups they belong to. The same node can be included in several groups. Such messages are called group messages. A group address is not divided into network and node number fields and is processed by a router in a special way.

NetBIOS (Network Basic Input/Output System) - is a basic network [protocol](#) developed by IBM for sharing files and printers over a network. NetBIOS is supported by IBM (IBM

PC LAN), Novell NetWare, Microsoft Windows networks and the networks of other companies.

Plug-in - is an independent component that can be added or removed from a software package to extend the capability of that software. The software must be designed and built to support plug-ins. Plug-in technology allows third-party developers to create plug-ins specific to that software enabling the software to do many more things than the software was originally designed.

Pop-up window – Browser instance created without the user interference with the purpose to display unwanted content like banners or ads, which decreases web surfing speed, comfort, and may also compromise the browsing security.

Port – is a number corresponding to data types so that different types of data can be efficiently sent to their appropriate application programs. A port is not a physical plug or socket. It is assigned in software only.

PPTP (Point-to-Point Tunneling Protocol) - is a technology that enables very secure communications over the Internet so they cannot be intercepted.

Preset - a preset in Outpost Client Firewall is a pre-defined setting or group of settings for an event or action. A preset can apply many settings simultaneously with one mouse click. This saves time for users who would otherwise need to apply each setting manually.

Protocol – is a set of accepted rules for a particular type of communication interchange. When two computers are programmed to use the same protocol when transferring data between them, that data will be correctly relayed. Otherwise, if two different protocols are being used, then the transfer of data will not occur.

Proxy server - is software that manages the connection between a sender and a receiver. All input is redirected to a different [port](#), which prevents a cracker from accessing a private network.

Referrer - is part of the HTTP request that contains the URL of the last page visited before the request.

Router - is a computer connecting two networks and transmitting packages from one network to other (the same as a [gateway](#)).

RPC (Remote Procedure Call) - supports distributed applications (those apps having components located on different computers). An application issues an RPC when it needs to use a function running on another computer in the same network. It is used in client/server applications that run on Microsoft Windows.

Scripting ActiveX elements – ActiveX elements not directly built into HTML page code, but created from scripts running on that page. Though the user that browses the page is not always able to view associated scripts, these ActiveX elements may expose threats to the user's system.

Server – is a computer that sends files and web pages to [client](#) computers over a network.

SMB (Service Message Block) - is a method of sharing network files that is used with NetBIOS. SMB works mainly through a series of client requests and server responses. SMB client and server software exists in all versions of Microsoft Windows.

Spyware - is hidden software or a concealed part of some software that is secretly or unknowingly installed on your computer. Spyware collects information (usually for marketing purposes) and sends it—without the user's knowledge—to the author or organization that originated the spyware.

SSL (Secure Sockets Layer) - is a special [protocol](#) designed to support safe access to web servers. This is a dominating protocol for encoding exchange between a client and server.

TCP (Transmission Control Protocol) - is a main traffic protocol ensuring reliable delivery of information. TCP connection is always carried out between two points.

Telnet (Telecommunications Network Protocol) - is a program for linking Internet tools, such as browsers, with databases, library directories and other world-wide information resources.

Trojan horse - is a program surreptitiously placed on your computer that establishes a connection to a remote intruder. The Trojan operates under the instructions arriving from the attacker's computer or automatically transmits the information the intruder programmed it to transmit. This information is generally passwords or other confidential data stored on the user's computer.

UDP (User Datagram Protocol) - is a [protocol](#) that provides simple, low-level tools of transmission and reception of network packets directly to applications. The UDP protocol does not control the data transfer and does not define a correlation between the individual

messages received or sent. Since UDP does not guarantee a reliable data transfer, applications using this protocol usually number each package and, if necessary, initialize a data retransmission. All applications that require a broadcasting or group function of [IP](#) connections should operate only with the UDP protocol.

URL (Universal Resource Locator) - is a World Wide Web universally recognized address for the identification and retrieval of resources such as a web site, a web page, an image, a video, a file, etc. A URL has the following appearance:

[protocol]://host[: port][path], where:

- Protocol is a protocol name such as http, ftp etc. If no protocol is specified, http is assumed.
- Host is the IP address or DNS address.
- Port is an optional parameter specifying the port number of the server. For example, with the http protocol, port 80 is generally used and is assumed if no port is specified with the http protocol.
- Path is the full path to the file, including its name. If the path is not specified, the server transmits its main (home) page.

VBScript - is a program embedded within a web page, generally with the purpose to enhance the viewer's experience when browsing that web page.

Web - is an abstract Internet space, in which a user can access multiple file types and archives connected by hyperlinks. See also [HTML](#).

Worm (also known as I-Worm or Internet Worm) - worm is a self-replicating program that reproduces itself over a network. They can damage file systems and/or simply use up bandwidth. Worms generally use e-mail clients to replicate themselves over networks. Worms became infamous when Robert Morris at Cornell created one that shut down many Unix computers on the Internet in 1988. Recent worms are: MyDoom and its derivatives – NetSky and Bagel.

2.4 Technical Support

If you need assistance in using Outpost Client Firewall, visit its support pages at <http://www.agnitum.com/support/> page for available support options including FAQs, Documentation, Forum, Tips-n-tricks and Troubleshooting.