User Guide

Reference

Outpost Firewall

Personal Firewall Software

from

Agnitum

1.1 Scope of This Document

This is the complete and detailed reference to the Outpost Firewall PRO 1.0 software.

For an entry-level guide, please see the Quick Start manual. Please note that if you are using Outpost Firewall FREE or a version other than 1.0, then some dialogs and settings will differ.

Table Of Contents

1.2 Welcome

Congratulations on finding and using **Outpost Firewall**, the most powerful yet user-friendly personal firewall software in the world today! Big claims for sure, but easily verified.

This User Guide is arranged in two parts. Part 1 is for all users, but Part 2 is intended only for those users who are technically advanced.

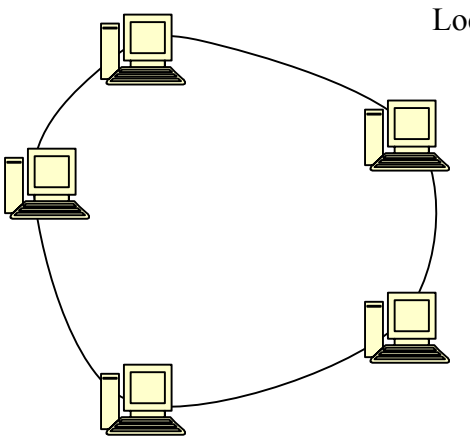
We will start by explaining some of the basics of networking and the Internet. Then we will progress to more advanced topics. Simply skip over those sections you already know about.

Part 1: For All Users

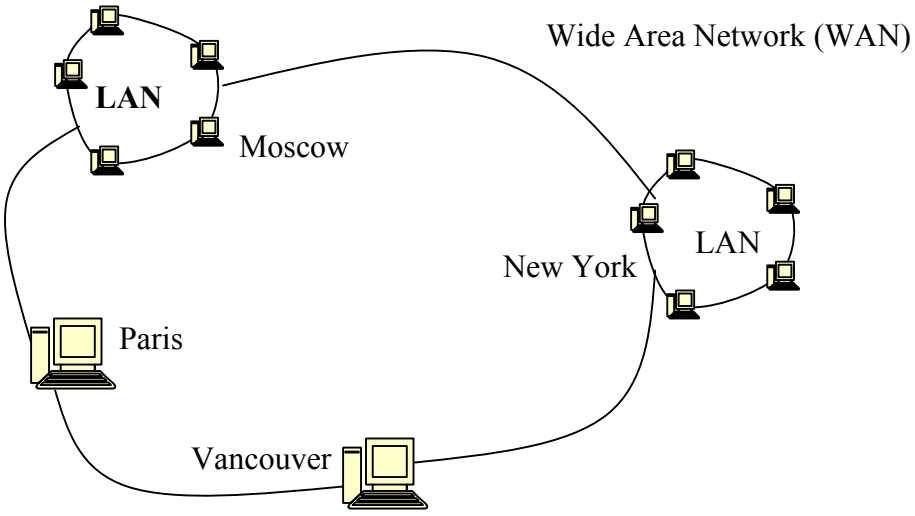
2 The Basics

2.1 Some 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 but the typical size is from 2 to 80 computers. You make a LAN when you connect two computers together in your 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.



2.2 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 the reason a firewall is used. A firewall is simply a 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 exception we know about at this time is **Outpost Firewall**, which was designed from the start to be extremely powerful yet easy to use.

2.3 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 psychotics and criminals (possibly the same thing) who feel compelled to make life difficult for others. Some of these know about computers and how to access files remotely. These are called crackers. To keep them out of our systems we need to use a strong firewall.

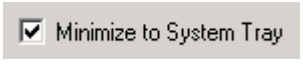
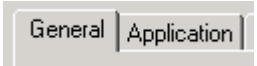
Here are the main dangers:

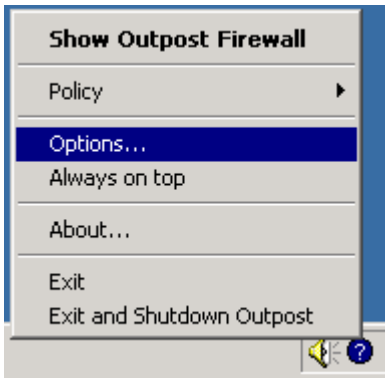
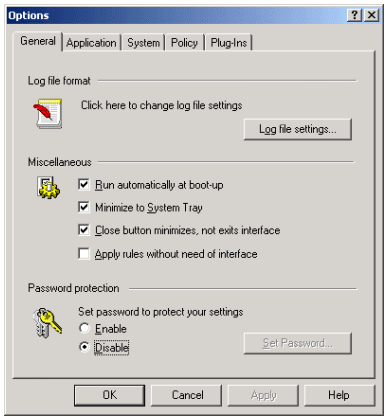
- Unauthorized applications can be delivered to your computer and be executed without your knowledge or control (for example, ActiveX or Java applets embedded in a web page you are browsing). These programs can perform any operation on your computer, including transferring files containing your private information to other computers or simply erasing all the files on your system.
- If your system is incorrectly configured (NetBIOS or Remote Procedure Call, for example, are installed by Windows by default) 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 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 a virus on your computer executes autonomously, whereas a Trojan horse is constructed to be used directly by the intruder who sent it.
- 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 are programs that gather information about you and your interests. Some of America's on-line corporations are placing this software on home computers without the owner's knowledge or permission.

2.4 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 this guide.

Object	Name
	Check box selected
	Check box deselected
	Option button selected
	Option button deselected
	Tab
	Input field

Object	Name
	Button
	Context Menu Generally pops up from a right-click on something or within an area. In this case, it's from a right-click on the **Outpost Firewall** system tray icon (the white question mark in the blue circle).
	Dialog window

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.

3 Introducing Outpost Firewall

3.1 System Requirements

The minimum system requirements needed for **Outpost Firewall** to operate well are:

- 166 MHz Intel Pentium or compatible CPU
- 16 MB RAM
- Windows 95, Windows 98, Windows NT 4.0, Windows 2000 or Windows XP operating system
- 4MB of hard disk space.

Note: There is no special network card or modem needed and there are no special configuration settings of these boards needed for the normal operation of the software.

3.2 Outpost Firewall Capabilities

The **Outpost Personal Firewall** system is the world's most advanced firewall software that combines power and advanced features with a remarkably easy-to-use interface. To effectively use **Outpost Firewall**, you do not need to know the inner workings of Windows. Our engineers specifically configured the default settings for you. You can change any of these many settings at any time, of course. These are covered later in this manual.

A tremendous strength of **Outpost Firewall** is its modular organization. **Outpost Firewall's** capabilities are implemented as modules, files with the `.dll` extension. Each module is independent and can easily be added to an installed system.

These are some of **Outpost Firewall's** many strengths:

- It can be used immediately after installation without any customization.
- It lets you easily create a 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.
- Many 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 so other networked computers cannot even detect your computer.
- 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 95/98/2000/ME/NT and XP.
- It has 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
  - Inappropriate 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 Firewall** does not control or restrict network exchange.
- Check e-mail attachments.
- Warns of any indication of someone attempting an attack of your computer from any other computer and instantly prevents access.

3.3 Technical Support

If you need help with the **Outpost Personal Firewall** system, please visit its support pages at http://www.agnitum.com/support/ for available support options including FAQs, Documentation, Forum, tips-n-tricks and Troubleshooting.

If you are using the free version of **Outpost Firewall**, we cannot also supply free personalized support. If you are unable to find the answer to your question from our web pages, please look through the **Outpost Firewall Forum** and post your question if it has not already been answered there.

4 Getting Started

4.1 Installing Outpost Firewall

Outpost Firewall's installation procedure is similar to that of most Windows programs.

Please Note: To install a newer version of **Outpost Firewall**, you MUST remove the old version first and then **reboot** (very important). See section 5.2 Uninstalling **Outpost Firewall** for details on how to remove older versions. **Also Note:** Be sure to uninstall any other firewall software and **reboot** before installing **Outpost Firewall** to prevent a system conflict of different firewalls fighting to control network access.

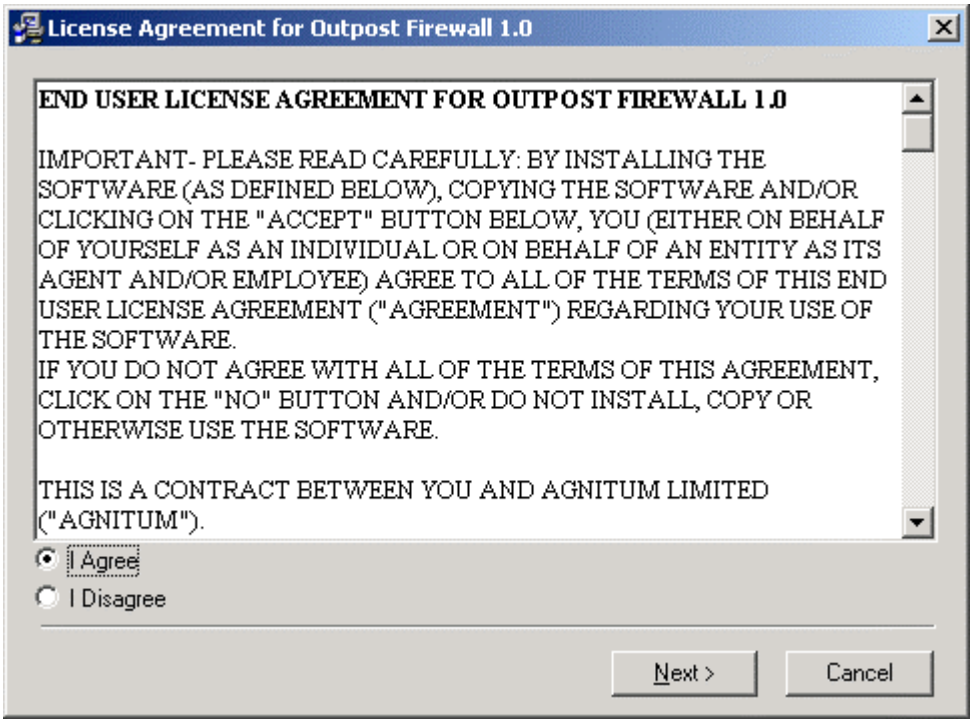
To start the installation program of the **Outpost Firewall** system:

1. **Very Important!** Before installing **Outpost Firewall**, uninstall any other firewall software on your computer, including an earlier version of **Outpost Firewall** and **reboot**.
2. Close all open applications.
3. Click the **Start** button on the Windows Task Bar.
4. Select **Run…** on the Start menu.
5. In the Open field of the Run dialog window, enter the full path to the setup program file (`OutpostProInstall.exe`). For example, if the set up program is on disk **`D:`** in the folder and subfolder `\downloads\outpost\` type into this field:

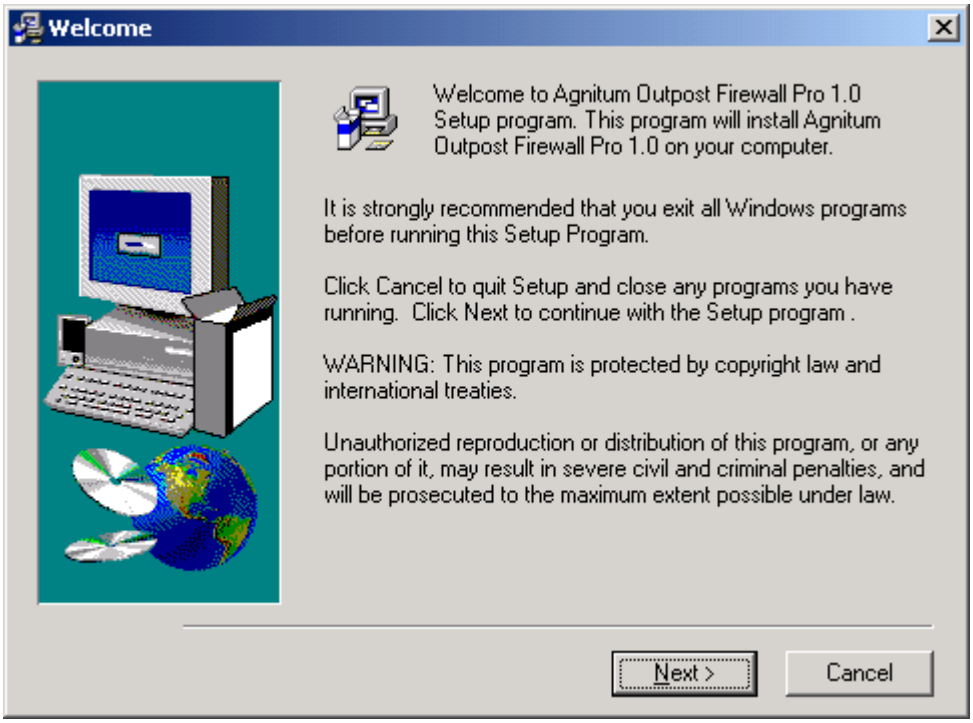
   ```
   D:\downloads\outpost\OutpostProInstall.exe
   ```

6. Click the **OK** button.

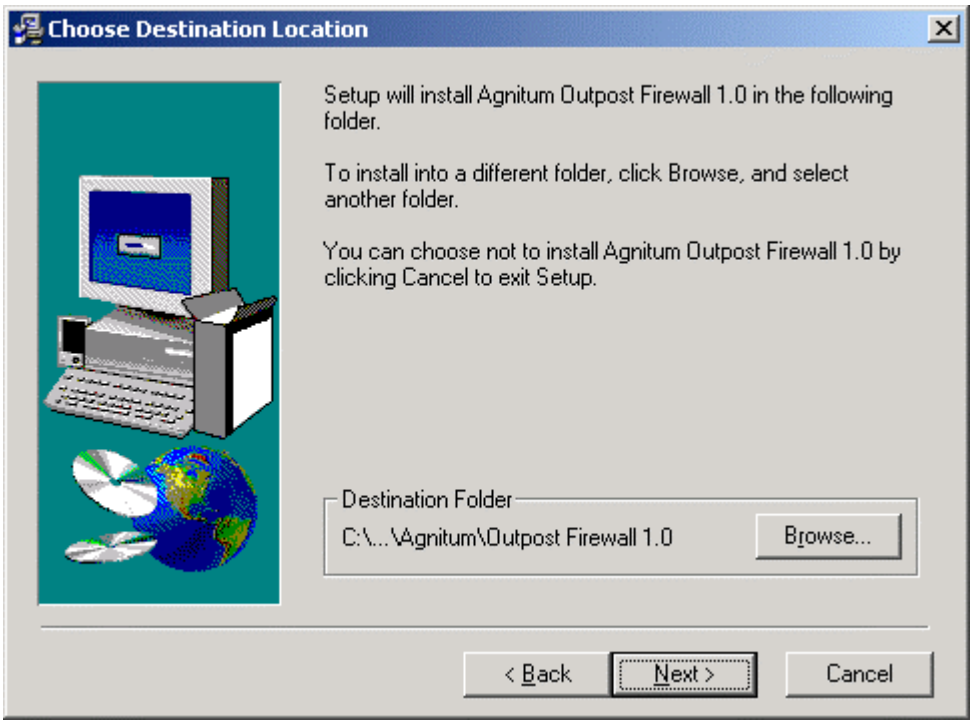
The setup procedure is arranged in several steps. A dialog window appears when each step is completed. The dialog has a **Next** button that takes you to the next step of the procedure, a **Back** button that returns you to the previous step and a **Cancel** button that aborts the entire setup procedure. The installation begins by asking you to accept the License Agreement to use the **Outpost Firewall**. Please read this carefully. This first dialog's **Next** button is enabled only if you select the option button "I Agree" indicating that the License Agreement is acceptable to you.



After you have accepted the License Agreement, the Next button brings you to the following Welcome dialog reminding you to exit all Windows programs:



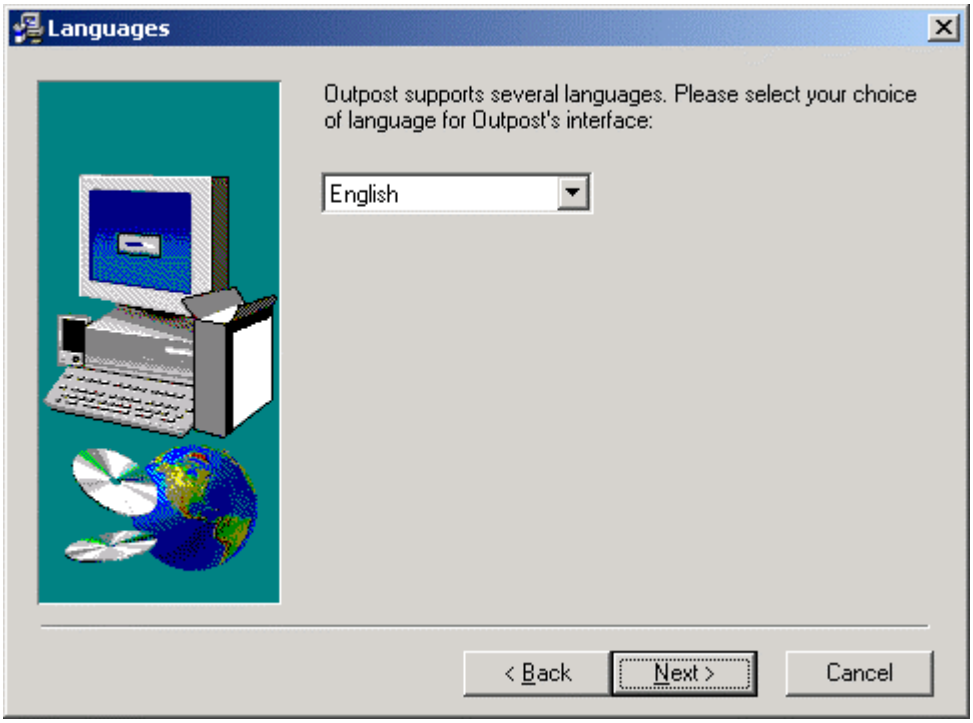
Following this is the Choose Destination Location dialog window shown here:



Specify the folder in which the **Outpost Firewall** components are to be installed. Keep the default folder shown as the Destination Folder if you have no other particular preferences in mind.

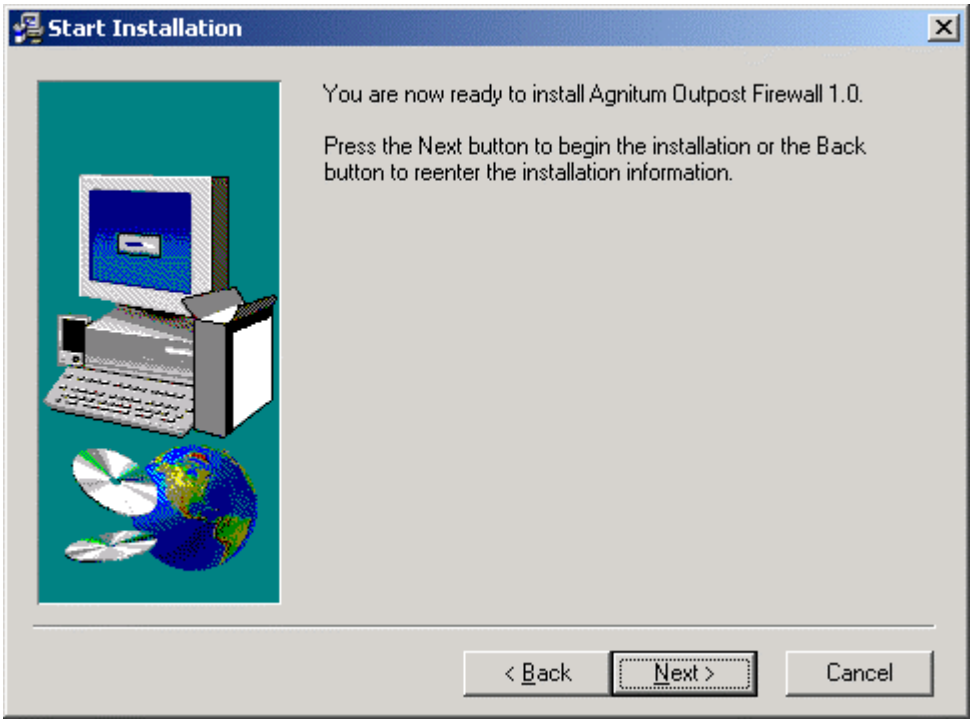
If you want to change the default location, click the **Browse...** button and Windows' familiar Folder Selection dialog is displayed. Select the preferred folder or type the name of a new folder to be created and click the **OK** button.

This dialog's **Next** button takes you to the Select Language dialog:



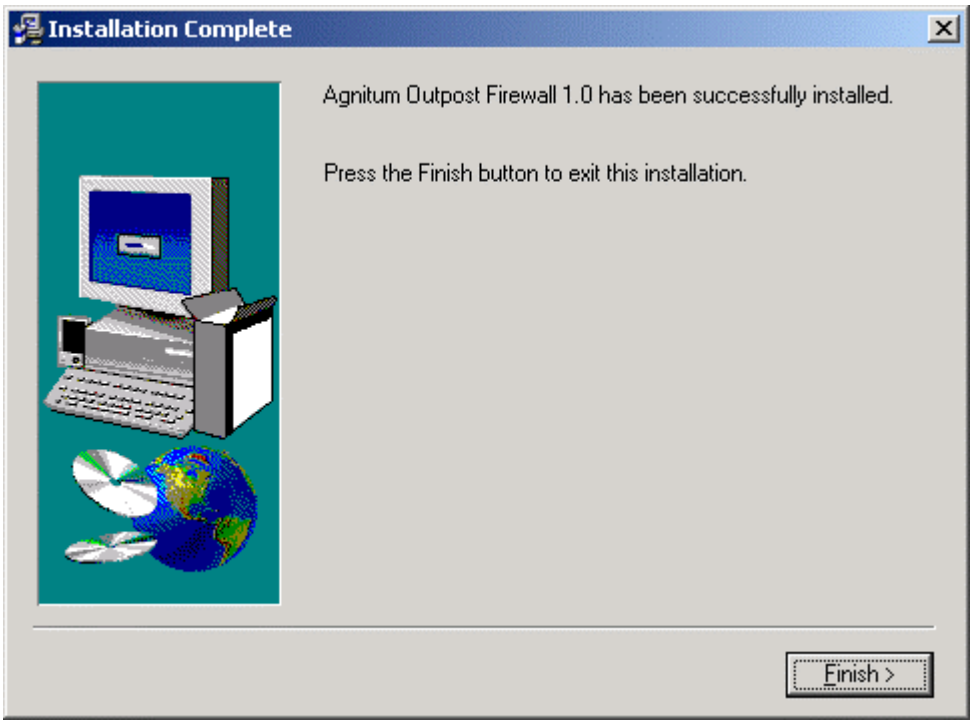
Choose the language for Outpost Firewall interface and press **Next** button.

The next step is the Start Installation dialog window:

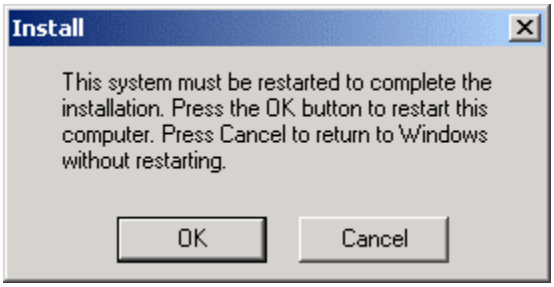


This is the last step before the actual installation of the software takes place. If you decide to change any of the choices you made, you can click on the **Back** button. When you are ready to go ahead with the installation, click the Next button.

After all the components are installed, you will see the Installation Complete dialog window:



After clicking the **Finish** button, the installation procedure is complete and the dialog window prompting you to restart the computer appears:



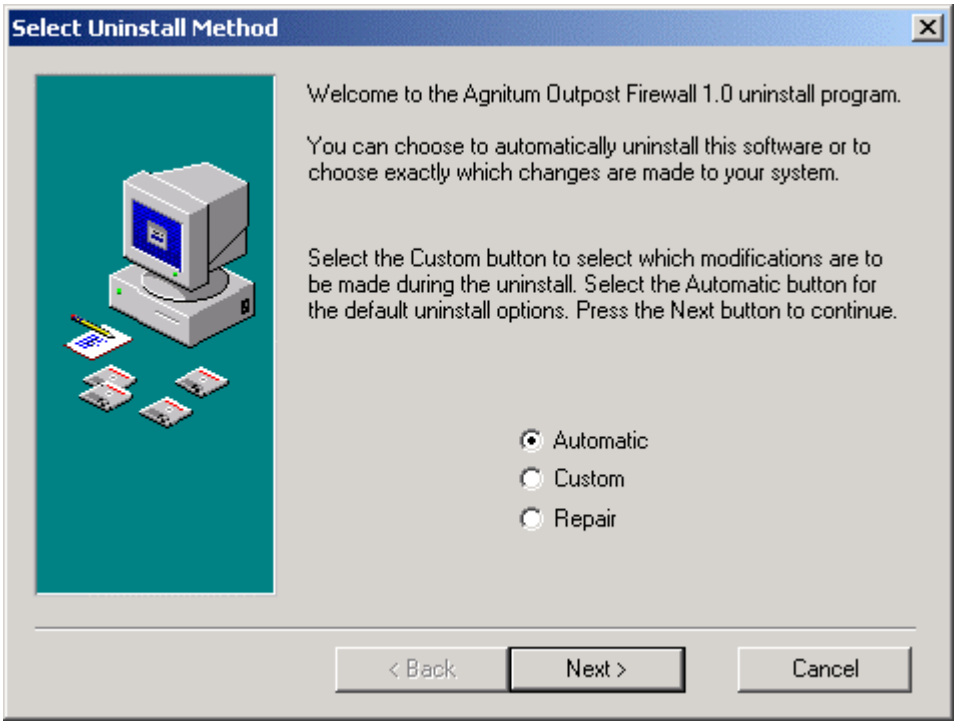
IMPORTANT: Do not launch **Outpost Firewall** manually using the **Start** button or Windows Explorer right after installing it. **You must reboot your computer** before **Outpost Firewall** can start to protect your system.

4.2 Uninstalling Outpost Firewall

Important: Before installing a newer version of **Outpost Firewall**, you **MUST** uninstall an earlier version and **reboot**.

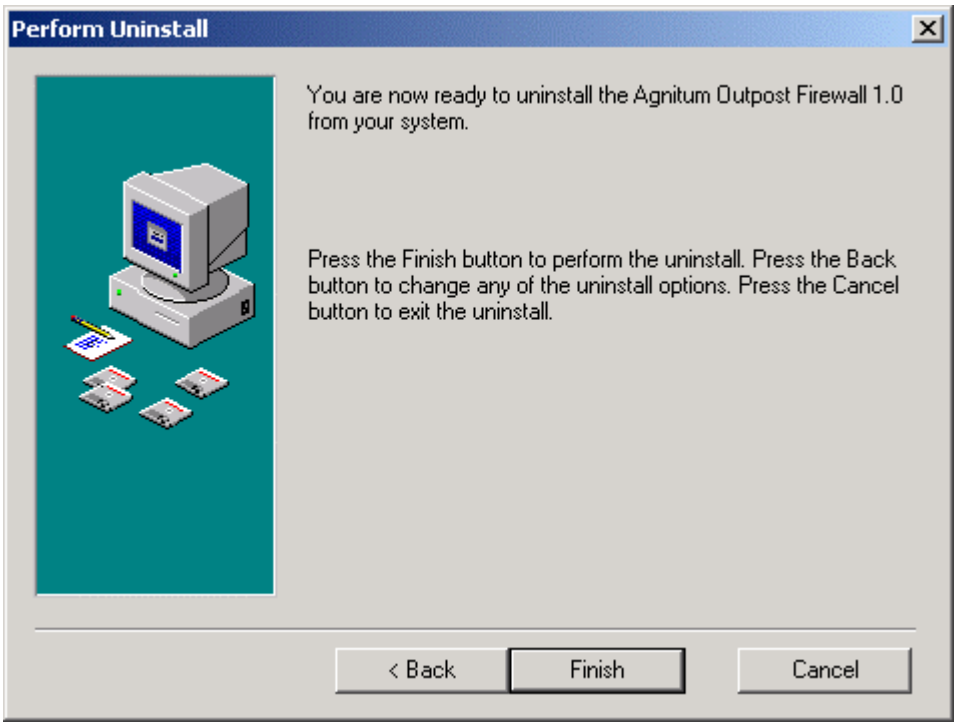
To uninstall **Outpost Firewall**:

1. Right-click on **Outpost Firewall's** system tray icon and select **Exit and Shutdown Outpost Firewall**.
2. Click the Windows' **Start** button and select **Programs**
3. Select **Agnitum**.
4. Select **Outpost Firewall 1.0**.
5. Select **Uninstall Outpost Firewall**.
6. This displays the **Outpost Firewall** Select Uninstall Method dialog window shown here:

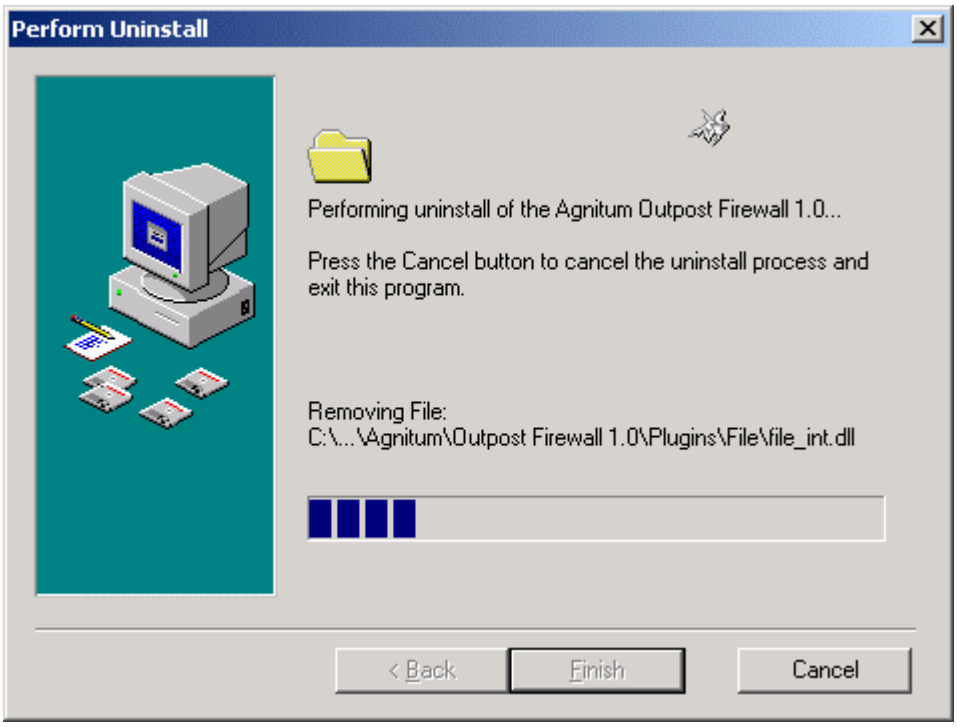


If you are new to Windows, it is recommended that you select **Automatic** then press the **Next** button. This skips the steps that ask you for decisions. If you are familiar with Windows and you want to choose the items to uninstall, select **Custom** before pressing the **Next** button. The **Repair** option is used to reinstall the **Outpost Firewall** system so it is complete and fully operational.

The next dialog window is shown here:



Clicking the **Finish** button of this window starts the uninstall process and displays the following dialog that shows the progress of the uninstall:



Note: To avoid software conflicts, **reboot your system** after the uninstall process completes.

4.3 Starting Outpost Firewall

Once installed, the **Outpost Firewall** starts automatically when Windows is loaded. In this way, **Outpost Firewall** starts protecting your computer immediately before other programs can compromise your system.

When **Outpost Firewall** starts, its icon is placed in the system tray, on the right-hand end of the Windows Task Bar.

If, for some reason, **Outpost Firewall** does not start when Windows loads, you can start it by following these steps:

1. Click the Windows **Start** button and select **Programs**.
2. Select **Agnitum**.
3. Select **Outpost Firewall 1.0**.
4. Select **Outpost Firewall**.

When **Outpost Firewall** is running its icon is displayed in the system tray. If you do not see the **Outpost Firewall** icon in the system tray, then you know that **Outpost Firewall** is not protecting your computer unless you specifically set it up to run in invisible mode. (To do this, turn OFF **Run at start up** and turn ON **Apply rules without need of interface**).

4.4 Stopping Outpost Firewall

Closing **Outpost Firewall's** main window does not shut down the firewall. Its icon remains in the system tray.

There are two ways to shut down **Outpost Firewall**:

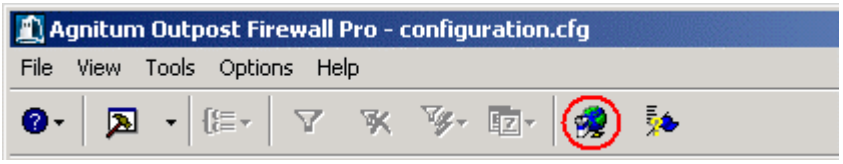
Right-click on its system icon to display the context menu. Select **Exit and Shutdown Outpost Firewall**. This closes the interface and stops the firewall so **Outpost Firewall** is no longer protecting your system.
When **Outpost Firewall's** main window is displayed, go to the **File** menu and select **Exit**. This closes **Outpost Firewall's** interface but leaves the firewall running in memory, blocking connections and banners, etc.

When Outpost Firewall is shut down its icon disappears from the system tray indicating that the firewall is no longer protecting your computer.

4.5 Automatic Update

With **Automatic Update,** you never have to be concerned about the latest Internet threats. **Outpost Firewall** provides you with a convenient way of keeping itself updated via the Internet. Each day, **Automatic update** checks for newer components and plug-ins and if it finds any, it retrieves them for you.

If, for some reason, you would like to check for newer components manually, you could run the **Update** procedure by clicking on the **Update** button on **Outpost Firewall's** toolbar as shown here:



Alternatively, you could manually check for any updated components by:

Clicking the **Start** button on Windows' Task Bar.
Select **Programs**.
Then select Agnitum | Outpost Firewall 1.0 | Agnitum Update.

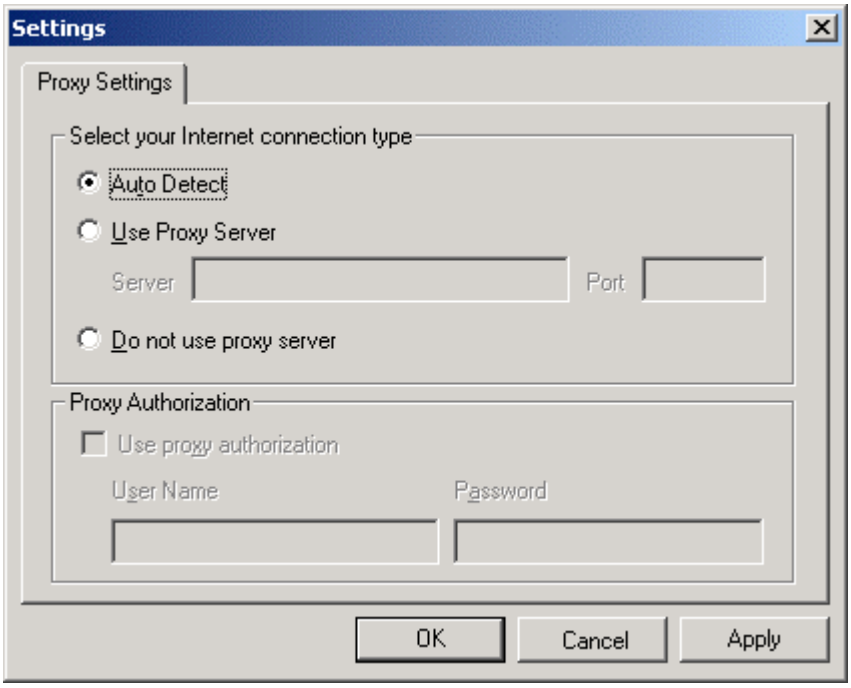
Either of these two methods produces the following dialog:

Select either:

- **Automatic** to have the system find all the components to be updated. **Automatic** is recommended so that all the components that have an update available will be updated together.
- **Custom** for you to specify each component you want to be updated. Only advanced users should use this choice for debug purposes.

Of course, with either **Automatic** or **Custom**, components are updated only if updates are available for them.

Clicking the **Settings** button displays this dialog:

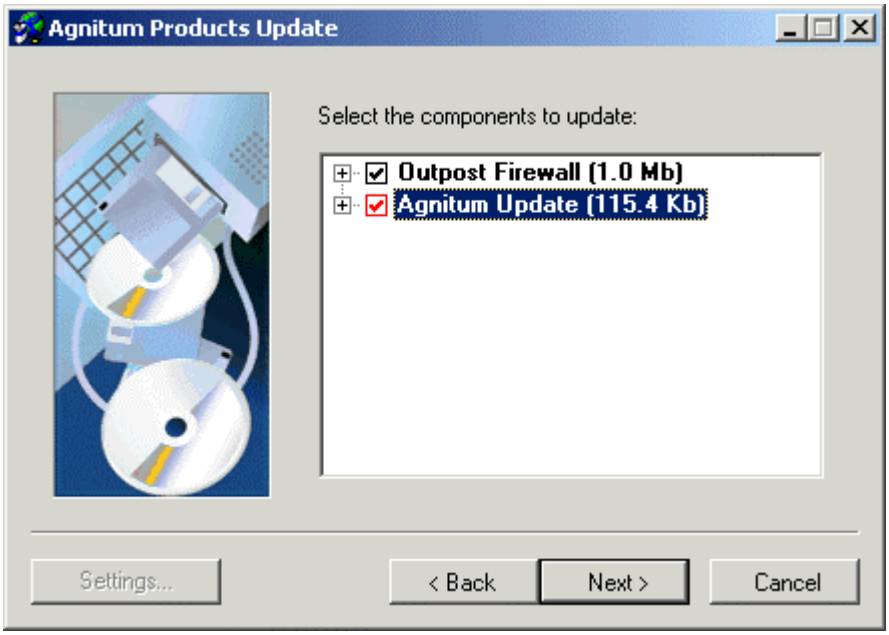


The options are:

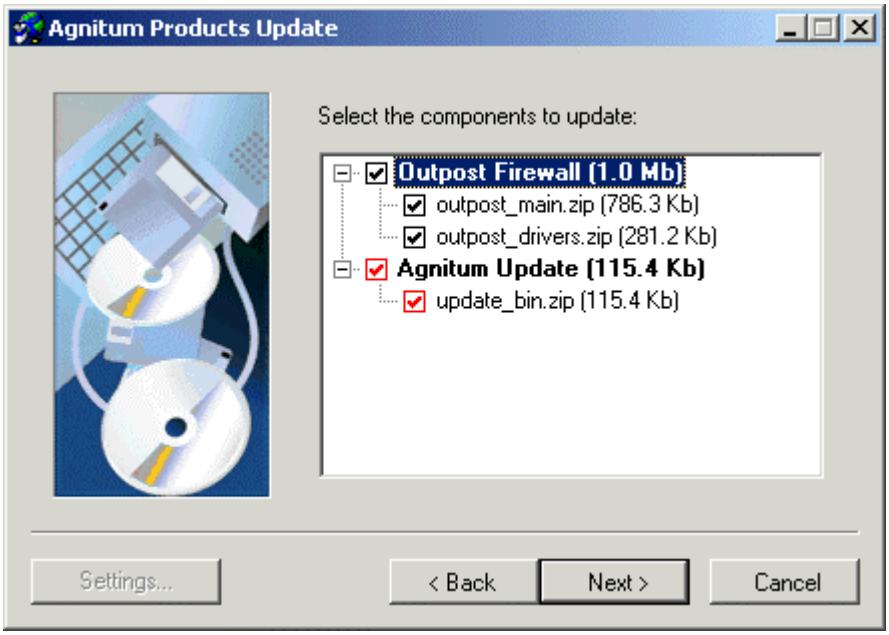
Auto Detect uses the proxy settings already specified in Microsoft Internet Explorer.

- **Use proxy server** lets you specify the parameters of the proxy server that is to be used by **Outpost Firewall's** Automatic Update. The Server and Port fields become visible when you choose this option. Enter the name of your proxy server and its port number (port 8080 is the default). If your proxy server requires authorization, please check the appropriate checkbox and enter your username and password. If you are unsure what type of proxy you use or you do not know your username and password, please consult your system administrator.
- **Do not use proxy server** if your system is not connected to the Internet through a proxy server.

If you selected **Custom update**, you will see this dialog:



Any line in the components list that starts with a **plus sign** is a grouping of components. You can see the listing of these components by clicking on the plus sign. In the picture above, clicking on each plus sign produces the following display:



As you can see, the plus signs were changed to minus signs when they were clicked to show the full listing.

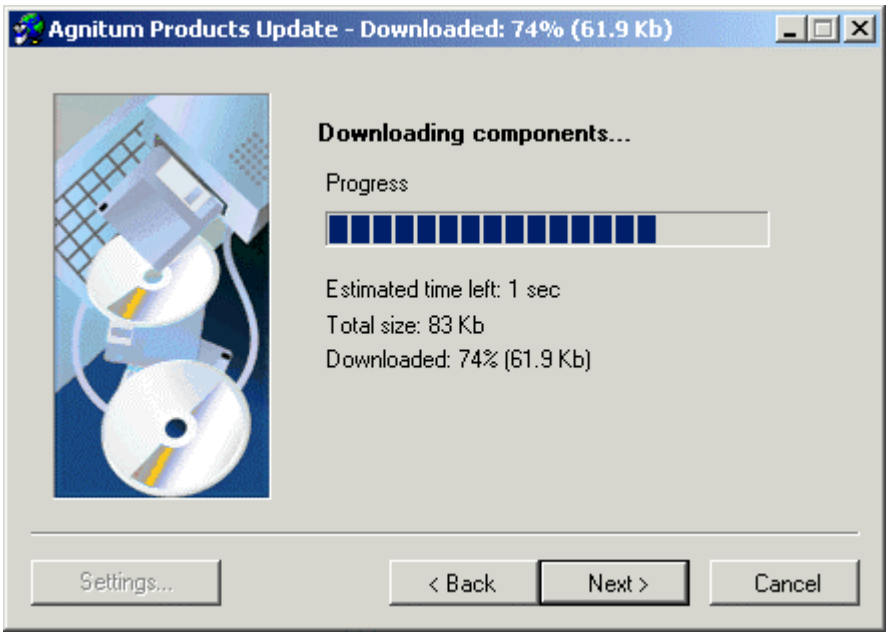
A red checkmark ☑ is a component that our engineers have determined ***must*** be updated for **Outpost Firewall** to avoid compatibility problems between modules and other selected components.

Check the components ☑ you want to update. Deselect the components ☐ you do not want to update. It is recommended to update all components unless you are an advanced user and have some reason not to.

When this dialog window first appears, all the components are checked ☑ by default.

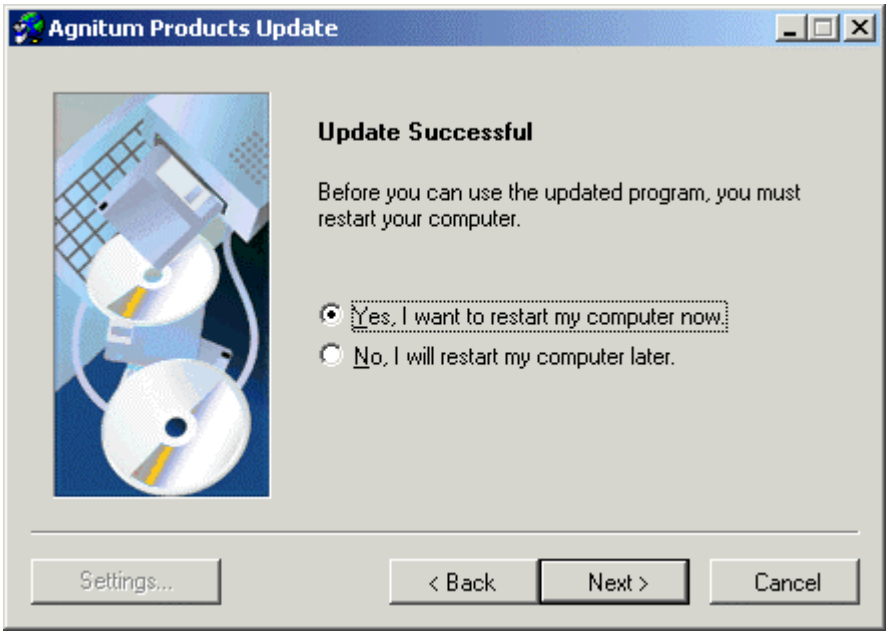
After all the components to be updated are selected, click the **Next** button.

Here is the next dialog showing the downloading progress:



When the download is complete, this dialog is automatically replaced without your having to click the **Next** button.

This is the last dialog that is displayed during the **Update** process:

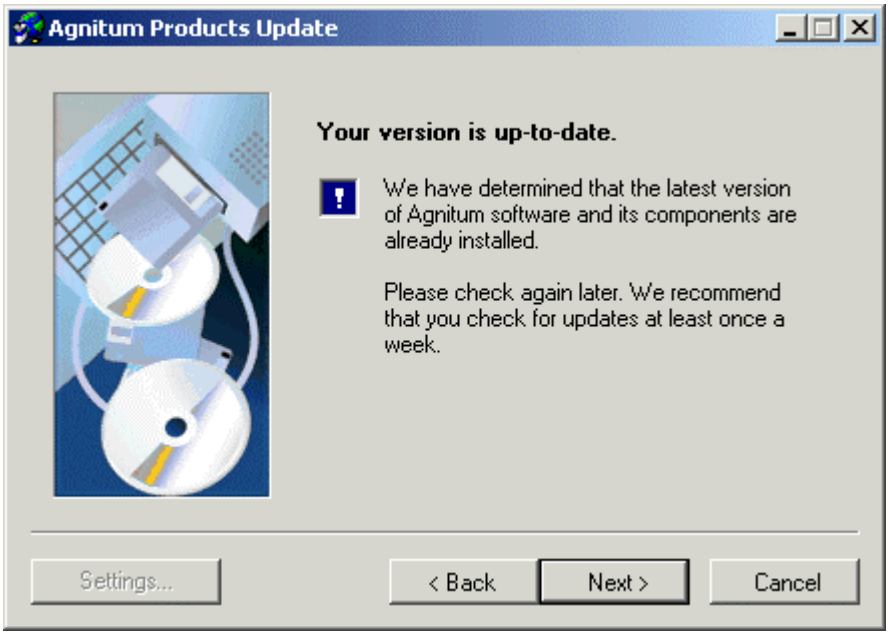


This dialog gives you the following choices:

- **Yes, I want to restart my computer now** to restart your computer immediately.
- **No, I will restart my computer later** gives you the opportunity of saving any incomplete work before restarting your computer. Be sure to restart your computer as soon as possible to take advantage of the increased protection afforded by the updated components you just downloaded.

Please note: The Outpost version is changed only after a reboot of your computer. If you simply restart Outpost, it will be the same version. To see what version is active, select from the menus **Help –> About**.

If there are no updates available, this dialog window is shown:



5 An Orientation

5.1 The System Tray Icon

The system tray is the right most part of the Windows task bar that generally looks like this:

The blue circle with the question mark is **Outpost Firewall's** icon.

This icon is one of the primary ways you can access **Outpost Firewall's** many controls, settings and logs. This icon changes with each of **Outpost Firewall's** major modes so you can see which mode is being used to protect your system at any time.

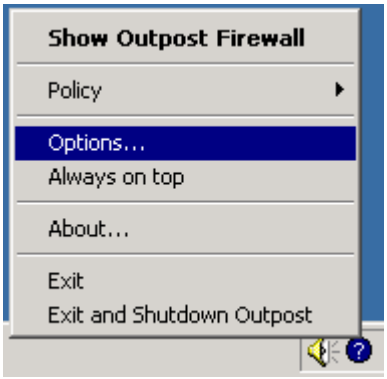
Here are the icons and the modes they represent:

Icon	Mode	Description
	Stop all	All network connections are blocked.
	Block most	All network connections are blocked except those you explicitly allowed.
	Rules Wizard	Helps you determine how an application will interact with the network the first time each application is run.
	Allow most	All network connections are allowed except those you explicitly blocked.
	Disable	All network connections are allowed.

These modes are covered in **Selecting a Policy**.

When you right-click on **Outpost Firewall's** system tray icon you get its context sensitive menu.

Here is a picture of **Outpost Firewall's** context sensitive menu from the system tray icon:



You can select any of these items on this menu by clicking its name with your mouse:

- **Show Outpost Firewall—**displays **Outpost Firewall's** main window.
- **Policy ▸ —**opens a sub-menu where you can change **Outpost Firewall's** Selecting a Policy to: **Disable mode**, **Allow most mode**, **Rules Wizard**, **Block most mode** or **Stop all**.
- **Options…—**displays the **Options** dialog window.
- **Always on top—**when selected, keeps **Outpost Firewall's** current window on top of all other windows.
- **About…—**shows the current version of **Outpost Firewall** and lists each module in the package and their individual versions.
- **Exit—**Closes **Outpost Firewall's** GUI but leaves the firewall running in memory blocking connections and banners, etc.
- **Exit and shutdown Outpost Firewall—**Closes the GUI and stops the firewall so **Outpost Firewall** is no longer protecting your system.

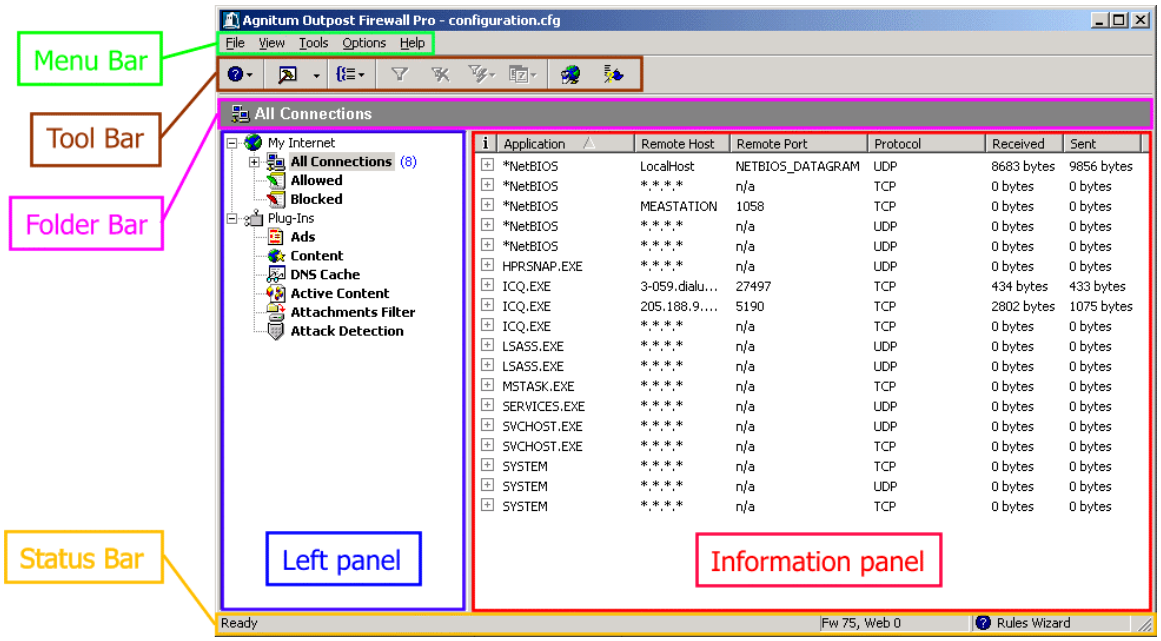
5.2 Outpost Firewall's Main Window

The main window is your central control panel of **Outpost Firewall.** It is used to monitor the network operations of the computer and to modify the firewall settings.

To display **Outpost Firewall's** main window:

1. Right-click on the **Outpost Firewall** icon in the system tray to get the context menu.
2. Select **Show Outpost Firewall**.

This is what the **Outpost Firewall** main window looks like right after **Outpost Firewall** is installed:



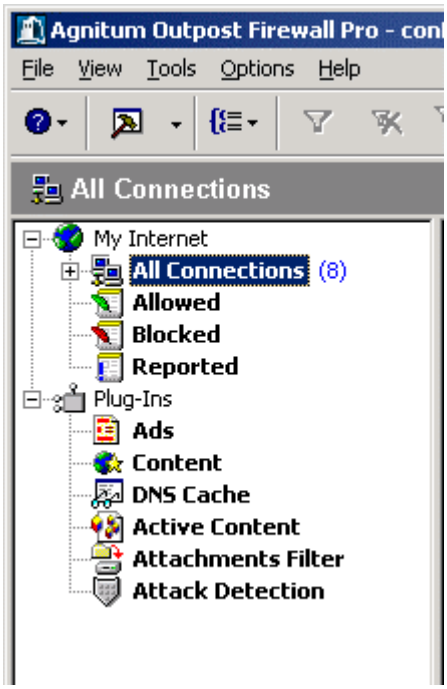
The main window contains:

- **Outpost Firewall's** menu
- The tool bar
- Folder bar
- Left panel
- Information panel
- Status bar.

5.3 The Panels

The Left panel and Information panel are similar to the left and right panels of Windows Explorer. The Left panel is a listing of the components secured by **Outpost Firewall** on your computer and the Information panel gives specific data about any component highlighted in the Left panel.

Here is the Left panel:



Under **My Internet** are the items:

- **All Connections**—shows every application and protocol that currently has an active connection to the Internet or LAN as well as all open ports.
- **Allowed**—shows a log of all the applications and connections that **Outpost Firewall** allowed, whether the connection is still active or not. The listing is arranged most recent first (reverse date/time order).
- **Blocked**—shows the log of all the applications and connections that **Outpost Firewall** blocked, listed most recent first.
- **Reported**—is the log of all the attempts by applications and connections to access the Internet or LAN that you specified **Outpost Firewall** to report to you.

Although the details of the logs are intended for advanced users, the above items are important when you need to see exactly what applications are accessing the Internet or are trying to establish connections. You can also use these lists to make certain that **Outpost Firewall** is correctly configured and is doing the job you need and want of it.

Some **Outpost Firewall** plug-ins are included in the setup package that you downloaded from Agnitum's web site. Plug-ins are independent from the primary **Outpost Firewall** engine and you may install or uninstall any or all of them. You can even get third-party plug-ins from other vendors and web sites. The second part of the listing of the Left panel shows the plug-ins that are installed.

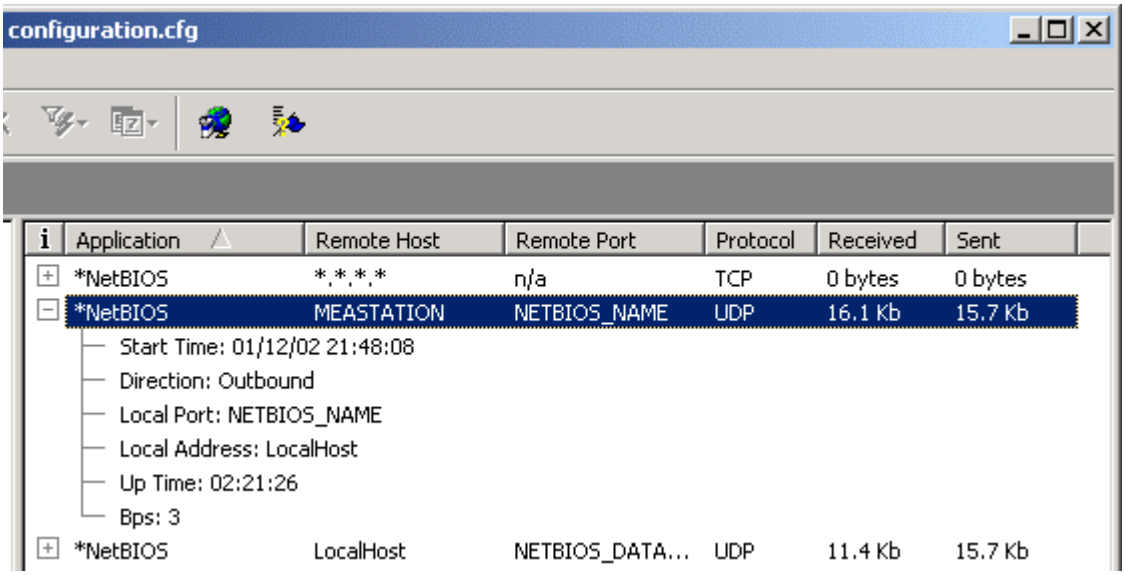
Each plug-in has its own icon in the Left panel and the log of its activity is displayed in the Information panel. When **Outpost Firewall** is first installed the **Plug-Ins** list contains the following modules:

- **Ads**—displays a list of all the ads that were blocked.
- **Content**—displays all the web sites or pages that were blocked by this plug-in and the reason why.
- **DNS Cache**—displays the web addresses saved by **Outpost Firewall** to speed up your Internet connection to those sites.
- **Active Content**—displays the sites that had some of its active content blocked based on the settings for Java, VB Script, Active X and other active content elements.
- **Attachments Filter**—shows all the e-mail file attachments that were neutralized and quarantined from your computer.
- **Attack Detection**—shows any suspected attacks on your computer from the Internet, the ports involved and where the attacks are from.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcategories. In the picture above, the **All Connections** line can be expanded by clicking on the plus sign at the start of that line.

Any line starting with a minus sign (**-**) shows that the line has already been expanded. By clicking on the minus sign, all of its subcomponents can be hidden so only the type of component is displayed to conserve screen space.

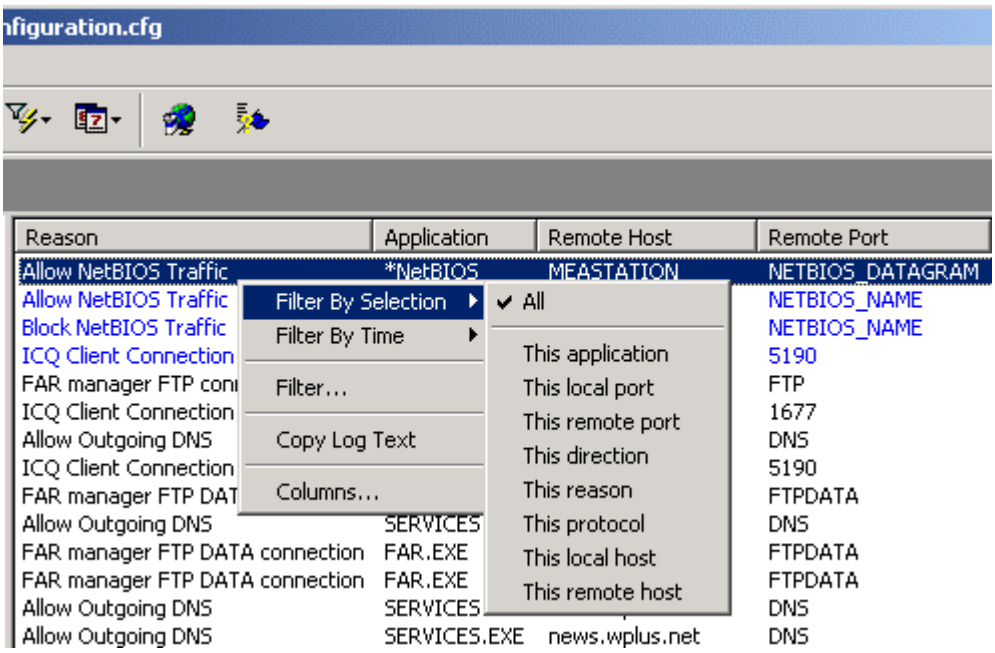
Here is an example of the Information panel showing some of the many data it displays:



Each of the lines is preceded by a plus sign (+) except the one highlighted, which has a minus sign (-), so is expanded to show its individual data. To hide this extra data, click on the category's minus sign. A line without a plus or minus sign preceding it has no extra data to be shown or hidden.

For advanced information about customizing the Information Panel, see section 8.3 Columns.

As with most elements of **Outpost Firewall**, a right-click in the Information panel produces a context sensitive menu. In the picture below, the menu is pertinent to the highlighted line. If no line was highlighted and the right-click was over some of the white space below the lines, then all the menu items starting with "This" would not be applicable and so would be grayed out.



The menu shown in the above picture is for displaying the data in the Information panel in a way that is most useful to you. This is mainly for professionals like system administrators who need to rapidly track down some particular datum. Even though **Outpost Firewall** is easy enough for a home computer user, it is also very sophisticated to meet the needs of advanced users.

The choices in the menus shown above are self-explanatory to those users who would need to use them. **Outpost Firewall** makes extensive use of context sensitive menus for all of its different items, categories, panels, and icons. A little experimenting will help you discover all of them and is far more instructive than reading detailed descriptions of each item.

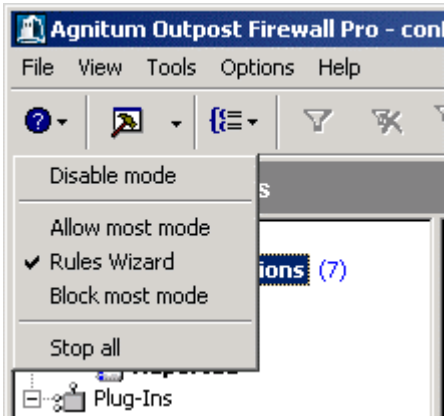
For advanced information about filtering, see section 8.2 Filter.

5.4 The Toolbar

The toolbar is close to the top of the main window and looks like this when **Outpost Firewall** is first installed:

You can see what each button does by holding your cursor over it for a second or so. This presents that button's tool tip, shown in the picture as "Options".

The icon in the left end of the toolbar shows **Outpost Firewall's** current Selecting a Policy. Clicking on this icon gives a menu you can use to quickly change usage modes. The menu looks like this:



Here are all the buttons found on the **Toolbar:**

Only some of these buttons are visible (active) at any one time, depending on what is highlighted in the Left panel or the Information panel.

Each button on the toolbar is a shortcut to a menu item except the update button. These buttons are simply an easy and direct path to their functions rather than having to go through several different menus or dialog windows to access these same functions.

Outpost Firewall's Toolbar Buttons

Button	Function	Corresponding Menu Path
	Changes **Outpost Firewall's** overall Selecting a Policy	**Options** | **Policy**
	Accesses the Options dialog window	**Options**
	Changes the items a listing is grouped by	**View** | **Group by**
	Filters a log listing of data inapplicable to your search	**View** | **Filter**
	Cancels filtering of a log listing	**View** | **Filter** | **Show all events**
	Narrows a log listing to a specific data type and value	Right click on **Allowed, Blocked** or **Reported** for context menu then select **Filter By Selection**
	Narrows a log listing to events within a specified time	Right click on **Allowed, Blocked** or **Reported** for context menu then select **Filter By Time**
	Checks for an update of **Outpost Firewall**'s plug-ins or software	(No other way to access this function directly) To have **Outpost Firewall** automatically check for updates whenever Windows starts, use **Help** | **Automatically check for Update**
	Displays **Outpost Firewall's** About screen	**Help** | **About Outpost Firewall**

6 Setting Up Outpost Firewall

6.1 Basic Information

A firewall for your computer is like the lock on a door of your home. In most cities, we usually lock the front door of our homes when we leave. This is not because the majority of people are criminals or because we cannot trust our neighbors to mind their own business. We generally lock our doors to prevent criminal types from snooping, stealing or doing damage.

The Internet is similar. Most web sites are unobtrusive and benign. Only a small percentage holds any threat to our privacy. However, because there are such a huge number of Internet users, even a small percentage of them with an impulse to vandalize adds up to a very significant number of people. For this reason, leaving your computer unprotected is just not prudent.

Outpost Firewall is engineered to detect a suspicious connection. It is recommended that you keep the firewall in either **Rules Wizard** or **Block most** modes for several days use. **Rules Wizard** is the easiest for you to use if you are unfamiliar with how firewalls work.

NOTE: If you have any doubt or confusion about changing any default setting, it is recommended that you DO NOT MAKE THE CHANGE. Even if you do understand the change, it is advisable to save or record the setting before changing it.

When **Outpost** alerts you to a suspicious connection request from an application on your computer or from the Internet, **Outpost** gives you some information about the request, such as the DNS or IP address of the remote computer, the application making the request and other data to help you decide if you want to allow the connection or not. If in doubt, simply disallow the connection **this one time**. See what happens. If you are prevented from doing something you wanted to do, then just try doing it again and this time **allow** the connection when prompted. In this way, you can learn what your applications are doing and which ones you need to be careful of or even uninstall completely from your system. It will also alert you to the presence of a Trojan horse!

Note: A good rule of thumb when using **Outpost** is to keep the settings **Outpost** suggests if you do not have a particular reason and the knowledge to change them.

In **Outpost Firewall** an access setting is basically a rule that you set regarding how much of your information you want to let other computers access or how much information you want to allow other computers to send to yours.

Outpost Firewall uses various security settings to keep your computer protected from unwanted access from other computers on the Internet or any type of network connection. It also restricts the flow of information coming into your computer as you see fit. You

might set a rule about file sharing, for example, so that your computer shares your files only with other computers you trust on your local network. A common use for a firewall is to restrict the amount of information your computer gives out while it is connected to the Internet.

Some applications and web sites do not need to be monitored or restricted. In **Outpost Firewall** the term "trusted" is used for these. Although the same word, "trusted" is used for both applications and web sites, **Outpost Firewall's** internal control devices deal with these two categories very differently as covered in **Advanced Settings**. An example of a trusted web site is one made by your company to keep its employees informed of daily activities. Other computers on your local network could also be trusted.

An application can be marked as trusted if you are absolutely certain that it does **only** what it says it does. An example is an application that you create yourself.

Note: It is **very important** that you do not give an application or web site the trusted designation unless you are sure it can and should be trusted. Giving this label to an application that has malicious code prevents **Outpost Firewall** from doing its job of protecting your system.

To add an application to **Outpost Firewall's** trusted list, please see these instructions in **Advanced Settings**.

To add a web site to the trusted list, please see these instructions in **Advanced Settings**.

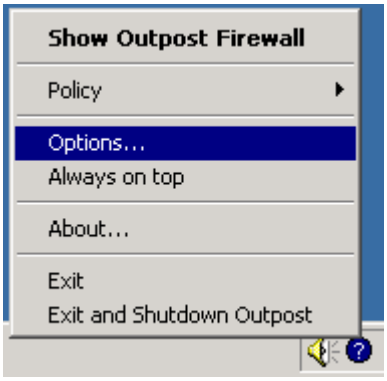
6.2 Initial Settings

Outpost Firewall is ready for operation as soon as it is installed. Its default settings are more than adequate for most purposes and are recommended until you become fully acquainted with how **Outpost Firewall** operates. Once you are familiarized, you can customize **Outpost Firewall** in many ways to best suit your particular needs.

This section gives a brief overview on how to customize the system. You can change these settings at any time.

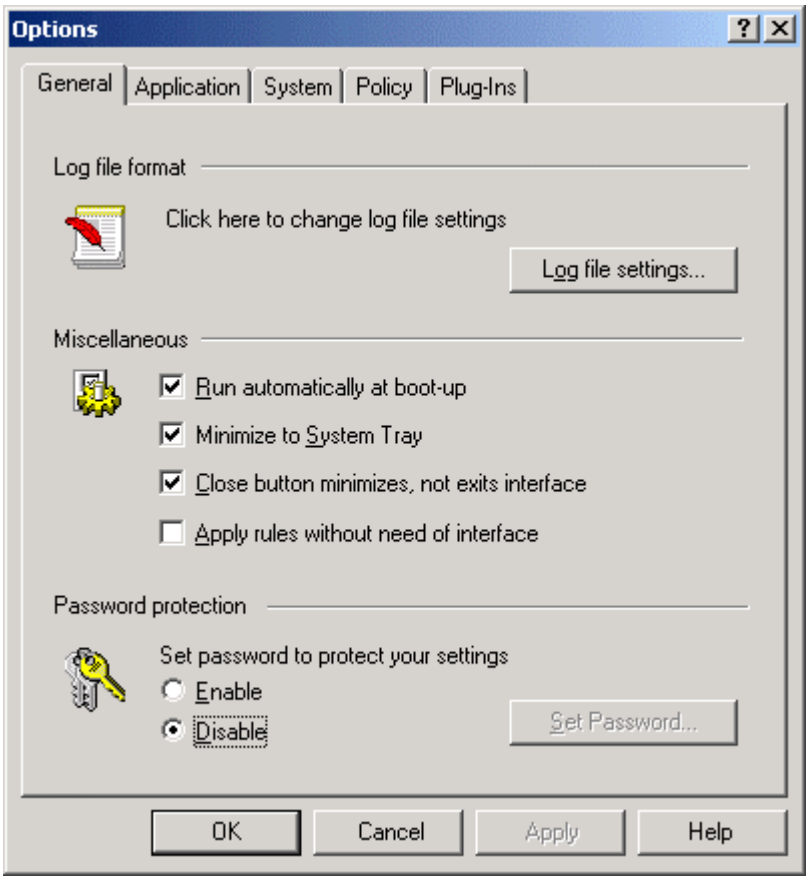
To display the **Outpost Firewall** settings dialog window:

Right click on the **Outpost Firewall** system tray icon to get the **Outpost Firewall** context menu shown here:



Select Options as shown in the picture.

The settings dialog looks like this:



The first section is **Log file format**. Clicking on the **Log file settings…** button lets you set the maximum size of the log file and how long you want to keep the log entries before overwriting them. These settings are provided for users with limited disk space.

In the **Miscellaneous** area of the dialog is where you can select or deselect to have **Outpost Firewall** start automatically whenever your computer first starts. Select **Minimize to System Tray** to not have a button placed on the task bar for **Outpost Firewall's** main window whenever it is minimized. Instead of this, to see **Outpost Firewall's** main window, simply double-click on **Outpost Firewall's** system tray icon or right click on it and select **Show Outpost Firewall**.

If **Close button minimizes, not exits interface** is selected, then whenever you click on the close button only **Outpost Firewall's** dialog window will close, not the firewall. In this case, to close **Outpost Firewall**, right-click on **Outpost Firewall's** system tray icon and select **Exit** or **Exit and Shutdown Outpost Firewall**.

Select **Apply rules without need of interface** if you want **Outpost Firewall** to run in invisible mode, without its system tray icon or any of its dialog windows. This option is provided for two reasons: to save system resources and for a parent or Systems Administrator to block unwanted traffic or content in a way that's completely hidden from a user. In order for this option to take effect you must disable the **Run automatically at boot-up** option.

The **Password protection** section lets you choose to have your **Outpost Firewall** settings protected by password so only you can change its configuration.

6.3 Selecting a Policy

One of the most useful and important features of **Outpost Firewall** is its usage modes. A usage mode is the basic attitude you want **Outpost Firewall** to have in doing its job of policing your computer's access to and by the Internet or any other network your computer may be connected to. The usage mode of **Block most**, for example, gives **Outpost Firewall** a particularly nasty attitude but **Allow most** makes **Outpost Firewall** very trusting.

Here are the different usage modes:

Icon	Mode	Description
	Stop all	All network connections are blocked.
	Block most	All network connections are blocked except those you explicitly allowed.
	Rules Wizard	Helps you determine how an application will interact with the network the first time each application is run.
	Allow most	All network connections are allowed except those you explicitly blocked.
	Disable	All network connections are allowed.

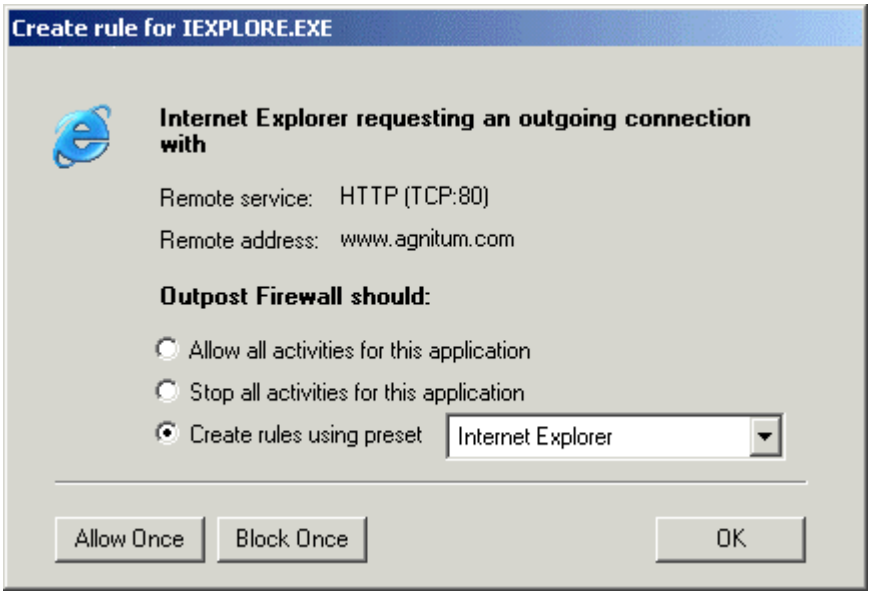
The icon shown for each mode is what is displayed in the system tray as the **Outpost Firewall** icon. You can tell at a glance what mode **Outpost Firewall** is in by looking at its system tray icon.

When **Outpost Firewall** is installed, the default mode is **Rules Wizard** mode. This mode helps you decide whether an application should be allowed a network connection. **Rules**

Wizard facilitates the specifying of applicable network parameters for each type of application.

Rules Wizard mode makes your life a little easier. Instead of having to create a new and often complex rule each time a new application is run, **Rules Wizard** does the work for you by basing its presets on all well-known applications. **Rules Wizard** even recommends the best selection for you. Unless you **know** of a better choice, simply okay **Outpost's** recommendation.

Here is the **Rules Wizard** dialog window that pops up whenever a new application requests a network connection:



Outpost Firewall has a database of the more commonly used applications. Our engineers programmed the optimum settings for each type of application so the decisions you have to make are very few.

The **Outpost Firewall** system groups applications into three groups.

1. **Blocked—**distrusted applications for which all connections are blocked.
2. **Partially allowed—**applications granted limited network access by having their protocols, ports and directions specified by policies (rules).
3. **Trusted—**applications for which all connection requests are allowed.

In the picture of the dialog window above, you can see what application is attempting a network access, "Internet Explorer", what manner of access is being attempted, the basic parameters of the connection and the choices you can make regarding the request.

The choices you can make for an application in **Rules Wizard** mode are as follows:

Choice	Purpose	Result
Allow all activities for this application	For applications you trust completely.	All network requests by this application are allowed and the application is given the status Trusted Application.
Block all activities for this application	For applications that should not be allowed network access	All network activities for this application are disabled. The application is given the status Blocked application.
Create rules using preset	For applications that can obtain network access under specific protocols, via specific ports, etc.	Creates a rule for the application that limits network access to specific ports and protocols using presets worked out by our engineers that are optimum for most purposes. This application will be included in the Partially allowed applications list.
Allow once	For applications that you are doubtful of but want to see what they do with the connection.	This network connection is allowed this time. The next time this application tries to establish a network connection, this same dialog window appears. No rule is created for the application.
Block once	For applications that you do not trust but do not want to block totally.	This network connection will be blocked this time. The next attempt by this application to establish a network connection results in this same dialog window. No rule is created for the application.

Outpost Firewall will detect most of the applications that regularly access the network after working a day or so in **Rules Wizard** mode. Once **Outpost Firewall** has registered most of your applications, you can switch to **Block most** mode.

You can also create your own rule for an application rather than select one of the presets. To create a rule, click on the down arrow at the right side of the **Create rules using preset** pull down. Go right to the last selection at the bottom of the pull-down list, **Other**, and click the **OK** button. This brings up the **Rules** dialog where you can create any rule for this application.

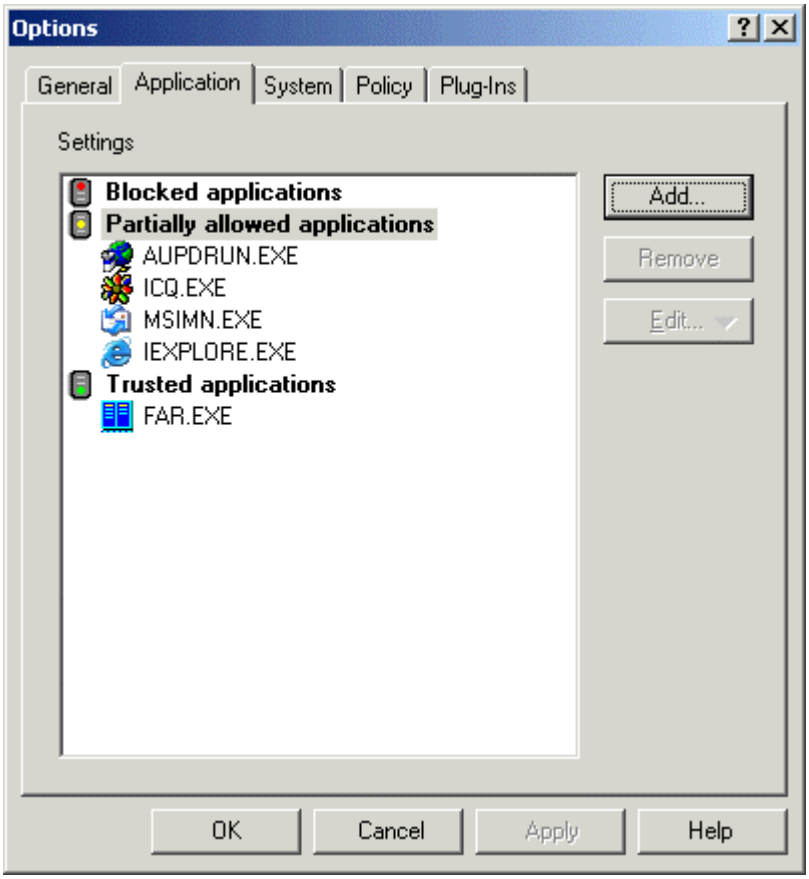
NOTE: The Allow Once and Block Once buttons are available only for some connections (outgoing TCP connections). When these functions are unavailable, their buttons are grayed out.

6.4 Application Level Filtering

One of Outpost's most important features is application level filtering. This lets you decide which applications should have access and which should not.

The dialog window to control application is accessed from a right-click on the system tray icon and selecting **Options…** and then the **Application** tab. You can also access this dialog from the main window using the menu **Options**, then selecting **Application**.

This is the **Application** dialog window:



Outpost Firewall divides all applications into three categories:

- **Blocked**—All activity of this group is blocked. We recommend that you add to this group all applications that do not need Internet access, such as text editors, calculators, etc.
- **Partially Allowed**—Outpost allows access to the Internet for these applications based on the rules that were created by you manually or from presets. Only specified application activity is allowed. We advise that you put most of your applications in this group.

- **Trusted**—All activity for these applications is allowed. It is not recommended that you include an application in this group unless you trust it absolutely.

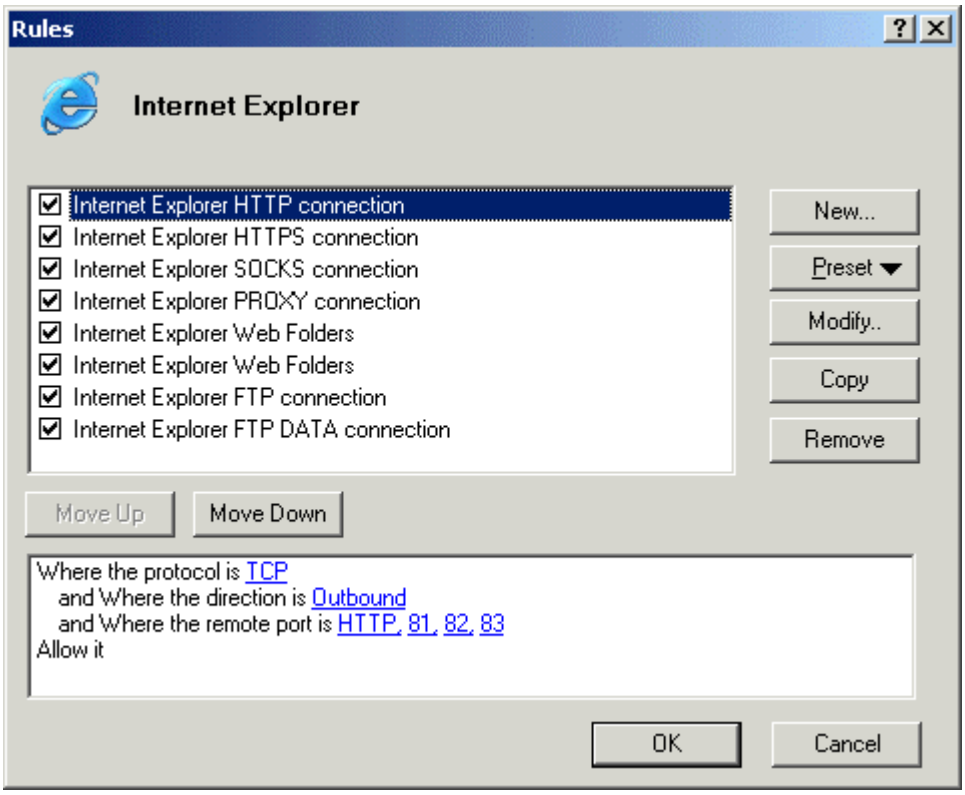
There is no need to add your applications to these groups manually. Rules Wizard automatically does this for you.

You can change an application's status from **Blocked** to **Partially allowed** to **Trusted** at any time. Applications can simply be dragged and dropped from one category to another.

You can also directly add an application by dragging its icon from Windows Explorer or your desktop into the **Options | Application** dialog or by clicking on the **Add** button, then browsing to the location of the application's **`.exe`** file and clicking on the **Open** button. If the same application is already listed in another category, it will be deleted from that other category.

The **Edit** button lets you change any of the detailed settings for whatever application is highlighted.

Whenever an application is dragged to the **Partially allowed applications** category of the **Options' Application** tab, or is in any other way added to this category, the following dialog box with its list of rules is displayed:

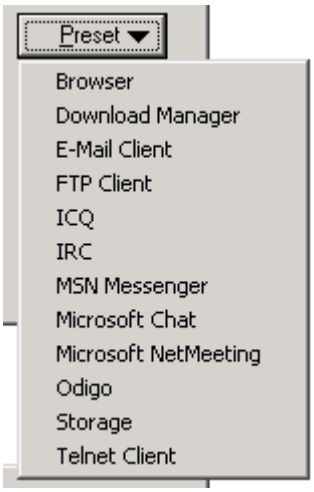


Using this dialog, advanced users have full control of each of the different protocol settings by highlighting one and pressing the **Modify** button. This is covered in detail in the advanced section, Creating Rules for Applications.

A simpler approach is to use the **Preset** button to select the general type of application that best applies. The settings for these presets were worked out by our engineers and are optimum for most purposes. Even advanced users are recommended to use these presets, and then tweak their settings later as needed. In using the **Rules** dialog, an empty checkbox in the list of rules means that rule will not be applied.

Note: It is possible to create several different rules for the same application. Be aware that **Outpost Firewall** uses the first instance of a rule having criteria that match the application's activity and ignores all subsequent ones. The rules in the firewall rules list are processed in the order in which they are listed. Once a rule is matched, searching of the rules list stops. In other words, any other rules that match this type of communication are ignored, if they are further on the list than the first rule that matches. The buttons **Move Up** and **Move Down** are used to change the sequence of rules so you can determine which **Outpost** will use. If no rule is found, **Outpost Firewall** displays the **Rules Wizard** dialog or simply blocks the connection, depending on whether you are running **Outpost** in **Rules Wizard** or **Block Most** mode.

Clicking the **Preset** button in the above dialog gives you a choice that looks like this:



The choices on the **Preset** list will very likely be added to as time goes on or otherwise modified. This will be included in any updates of the **Outpost Firewall** software as covered earlier. For advanced information about rule creation, see section 7.4 Creating Rules for Applications.

7 Plug-Ins

7.1 Introduction

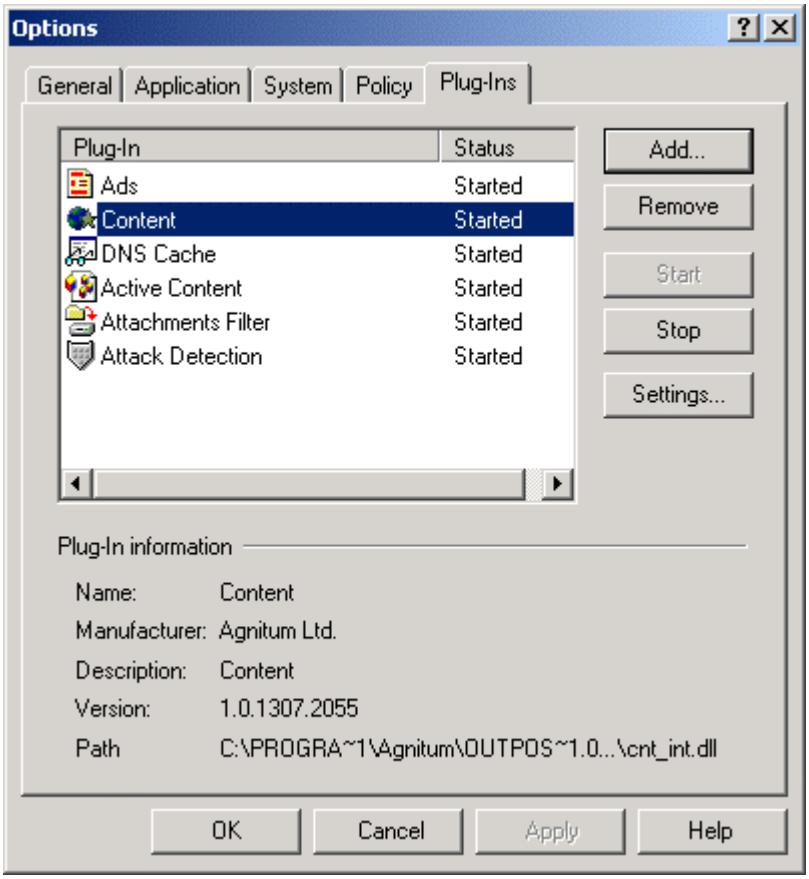
One of **Outpost Firewall's** most useful and effective design strategies is the employment of plug-ins. These modules can be created by third party developers and easily added to increase **Outpost Firewall's** capabilities.

If you are interested in developing **Outpost Firewall** plug-ins, please visit http://www.agnitum.com/products/outpost/developers.html for samples, tutorials and the developer's forum.

Please note that plug-ins are absolutely independent from each other and the main **Outpost Firewall** module. Any rules that you create for an application in **Outpost Firewall**, such as the **Trusted Zone** settings, will not influence or apply to any plug-in's functionality.

The dialog window to control these plug-ins is accessed from a right-click on the system tray icon and selecting **Options…** and then the **Plug-Ins** tab. You can also access this dialog from the main window using the menu **Options**, then selecting **Plug-Ins Setup**.

This is the **Plug-Ins** dialog window:



The right-side buttons are:

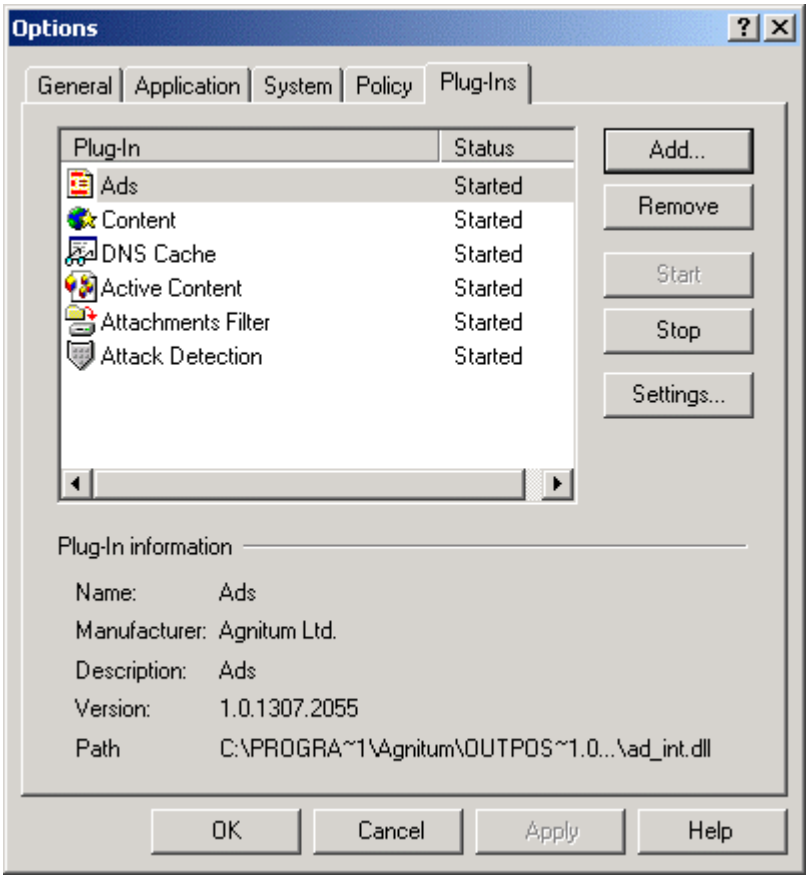
- **Add…—**used to add a new plug-in to **Outpost Firewall** using Windows' file open dialog.
- **Remove—**used to delete a plug-in that is highlighted on the list.
- **Start—**restarts a highlighted plug-in that is stopped.
- **Stop—**used to stop a highlighted plug-in from operating, but not to delete the plug-in from **Outpost Firewall**.
- **Settings…—**used to modify any of the settings for a highlighted plug-in. The types of settings vary with the different plug-ins. **Note:** Only those plug-ins having the status of "Started" can have their settings modified. The settings dialog for any started plug-in can also be accessed by clicking on that plug-in in the main window's Left panel and selecting **Properties…** in the context sensitive menu that pops up. The settings dialog for each started plug-in can also be accessed using the  button on the toolbar of **Outpost Firewall's** main window.

The **Plug-In information** section, in the lower half of the above dialog, shows the most important properties of a highlighted plug-in and where, on your system, the plug-in's `.dll` file is located.

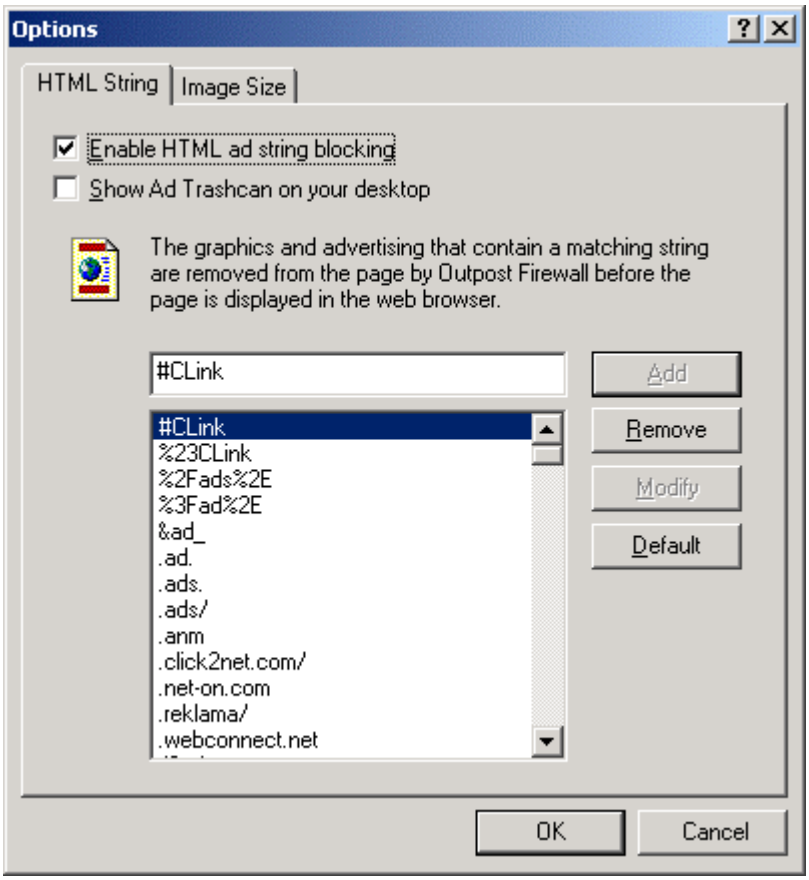
7.2 Ad Blocking

More and more web sites are becoming filled with ads. With a fast connection these are generally not a problem but often it's nice just to surf without the distraction of blinking, moving ads.

To change the settings of **Outpost Firewall's** Ad Blocking, right-click on the system tray icon to get the context menu, then select **Options…**. You will see the following dialog window:



Click on **Advertisement Blocking** to highlight it and then click on the **Settings** button to get the following dialog:



Outpost Firewall can block the display of banner ads from certain advertisers. **Outpost Firewall** comes with a large list as shown in the above screenshot. As you can see from the picture, all the entries on the list are single "words", each having no spaces in them. These are the most common "words" in Internet advertisement URLs located in the HTML tags "**<IMG SRC=**" and "**<A HREF=**". To add another word to the list, simply start typing it in the text field above the list and press the **Add** button. **Outpost Firewall** replaces these banners with the text: **[AD-IMG]**.

Be sure that **Enable HTML ad string blocking** is selected (check marked). This activates the **Add** and **Modify** buttons. Click **Add** to add the new entry to the list or **Modify** to change it.

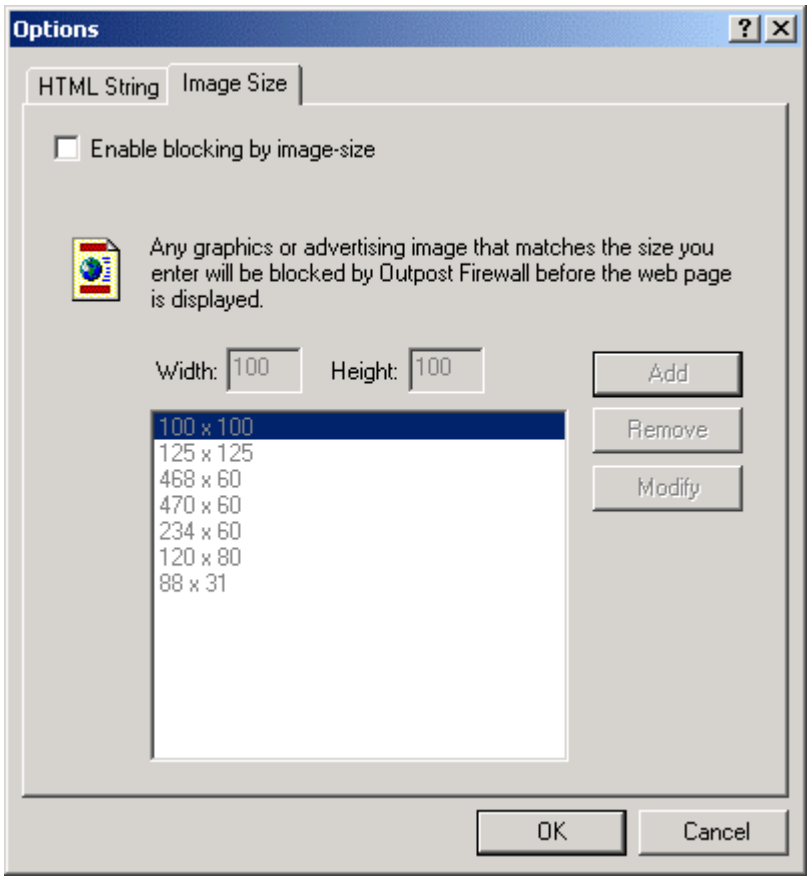
Enabling "**Show Ad Trashcan on your desktop**", then pressing "**OK**" puts this on your desktop:

With this little window present, to remove an ad from the web page you are viewing, simply drag the ad over to this **Ad Trashcan**.

This will give you the following dialog:

Select **A portion of the string** if you want to trim the URL down as shown in the above picture. Then click on the **OK** button to save the ad's URL into **Outpost Firewall**.

Outpost Firewall can also block all banner ads having standard sizes. To do this, select the **Image Size** tab near the top of the **Options** dialog. You will get the following display:



Outpost Firewall lets you block all specific sized graphic images that have a link. Be sure to select **Enable blocking by image size**.

Immediately after installation, **Outpost Firewall** is set to block all images with a link (images inside an **<a** tag) of 100 x 100, 125 X 125, 468 x 60, 470 x 60, 234 x 60, 120 x 80, and 88 x 31 pixels. **Outpost Firewall** replaces the designated banners it with the text **[AD-SIZE]** in the web page.

To allow all graphics to be displayed on the screen, deselect **Enable blocking by image size**.

To add to the list of image sizes to be blocked, select **Enable blocking by image size**, then type in the size of the image to be blocked and press the **Add** button.

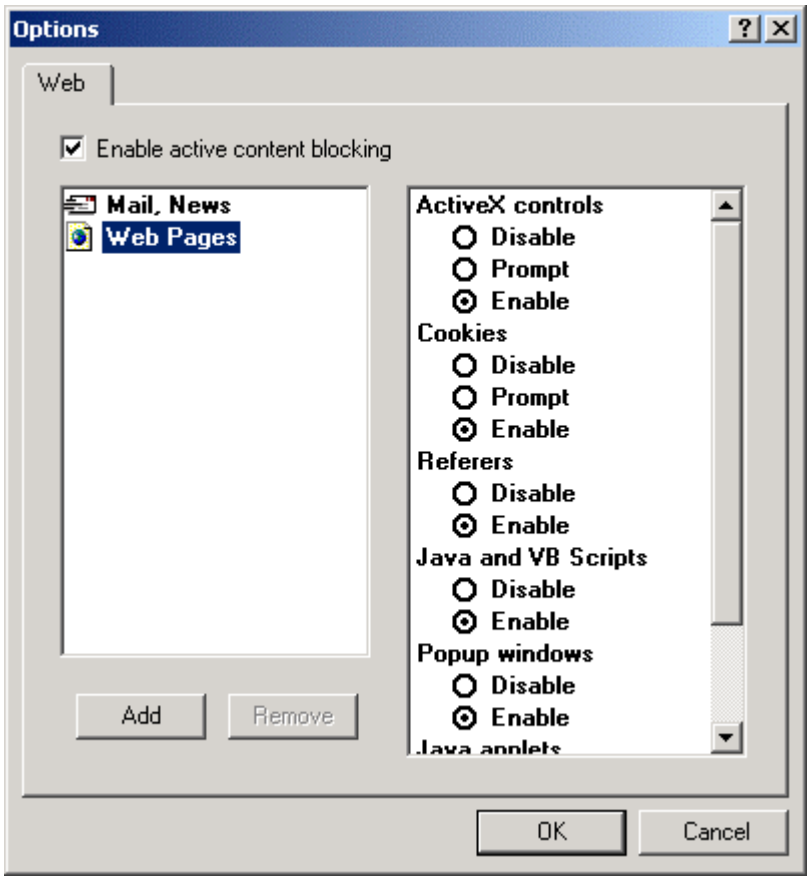
Please note that **Outpost Firewall** blocks banner ads according to the settings you specify. Some legitimate images could be blocked if the setting is too strict, such as adding the word “image” to the list of blocked words. In addition, a few ads will not be blocked with this plug-in’s default settings.

7.3 Active Content Blocking

The **Active Content Filtering** plug-in controls the operation of the following active elements:

- ActiveX.
- Java applets.
- Programs based on Java Script and VBScript.
- Cookies.
- Pop-up windows.
- Referrers.

This plug-in lets you independently allow or block any of these elements that might be contained in the web pages you are browsing.



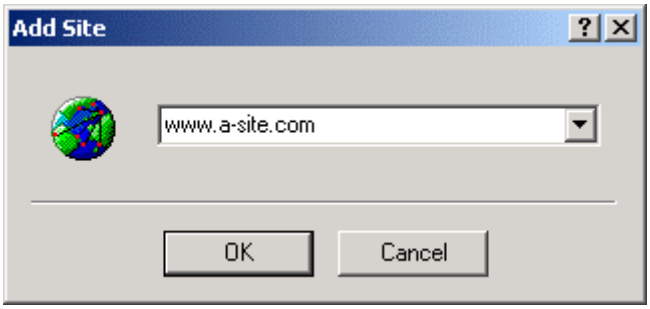
Enable active content blocking must be selected (checked) for this plug-in to function. Once you have fully configured this plug-in, you can activate it or de-activate it simply by clicking on this checkbox.

Control of active elements can be individually set for e-mail and news or web pages. Select either "**Mail, News**" or "**Web Pages**". The right-panel listing shows the settings for each selection. The choices are:

- **Disable—**blocks the element's action.
- **Prompt—**asks you each time this element tries to activate.
- **Enable—**allows the element to function.

When the system is installed, the use of all active elements is enabled for all web pages, except pop-up windows and referrers.

Individual web sites can be added to the listing in the left panel so that each site can be configured separately. To do this, highlight **Web Pages**, as shown in the picture above, and click the **Add** button. This gives the following dialog:



Type in the web page you want to give individualized settings for its active content and press the **OK** button. The use of all active elements is set to **Enable** for that site by default. To modify these settings, highlight the web site in the left-panel and change each element as you see fit.

To remove a site from the list of DNS addresses in the left part of the dialog window highlight it and press the **Remove** button.

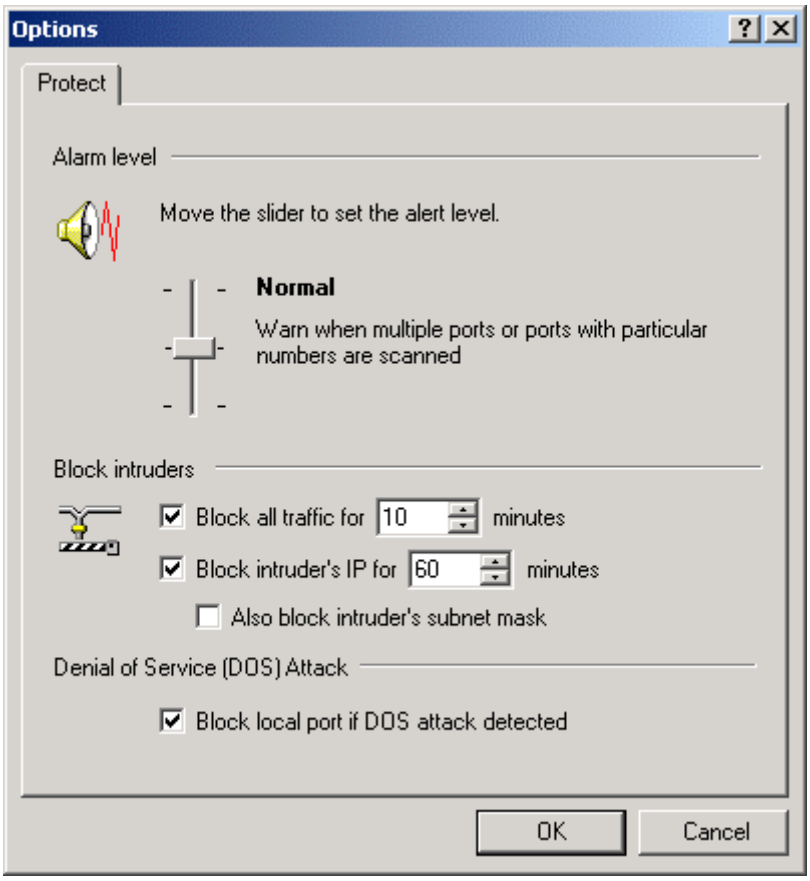
Please note that some sites require that all or several of its active content elements be active for their pages to display or function correctly. If you make very strict settings for all sites, you can experience the following problems: images not being displayed, a web page not displayed at all, a web page displayed incorrectly or some useful services contained in applets not working. If this happens, just change this plug-in's settings for all sites or that particular site.

7.4 Attack Detection

This plug-in informs you of a possible attack on your computer from the Internet or the network your computer is connected to. It recommends the steps to be taken as well, in order to prevent damage to your computer.

The **Attack Detection** plug-in lets you specify the conditions in which a warning is to be displayed. It also has response settings that will be used if a specified security level is exceeded.

Here is the plug-in's **Options** dialog window:



In the section named **Alarm level**, you move the slider up for a higher level of security or lower as follows:

- **Maximum**—a "Port Scanned" warning is displayed even if a single scanning of your port is detected.
- **Normal**—a "Port Scanned" warning is displayed if several ports are scanned or if a specific port is scanned that **Outpost Firewall** recognizes as one that is commonly used in attacks.
- **Minimum**—a "Port Scanned" warning is displayed if a multiple attack is definitely detected.

The lower half of the window lets you specify the steps **Outpost Firewall** is to follow if an attack on your computer is detected:

- **Block all traffic for**, if selected, blocks all network exchanges to and from your computer for the specific number of minutes you set (10 minutes is the default).
- **Block the intruder's IP for**, if selected, blocks all network exchanges from the computer attacking yours for the number of minutes you set (60 minutes is the default).
- **Also block intruder's subnet**, if selected, blocks all network exchanges from the entire subnet to which the intruder belongs.
- **Block local port if DOS attack is detected**, if selected, blocks the local port if a DOS (Denial Of Service) attack is detected.

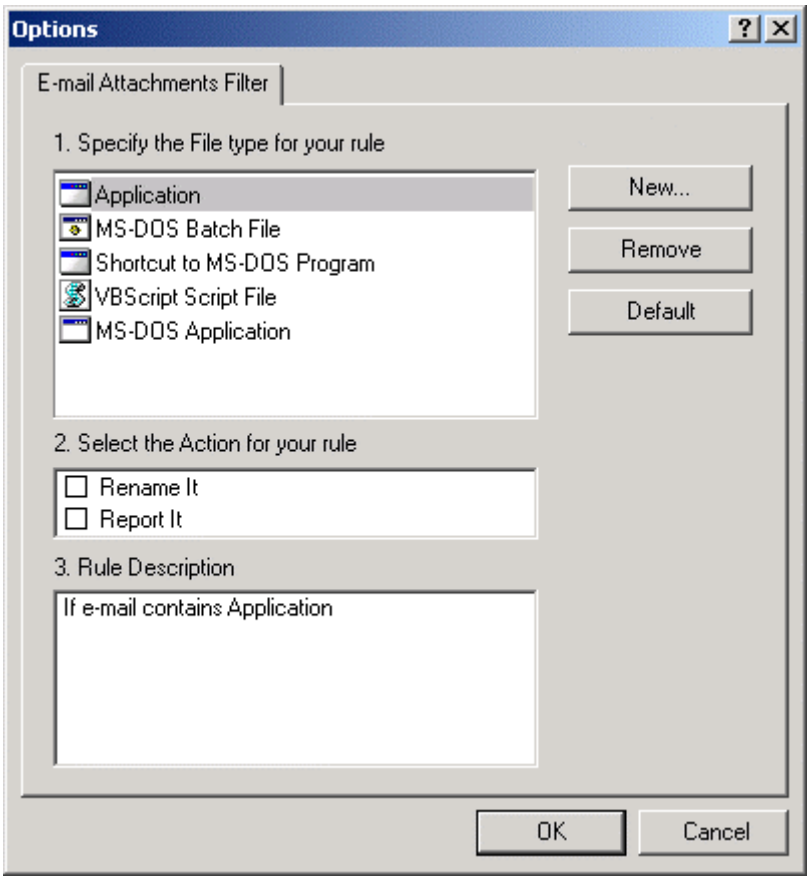
We highly recommend that you do not enable "Block all traffic for" after a port scanning because disabling regular port scans can result in your inability to work on the Internet after an innocuous port scan.

For more information about fine-tuning this plug-in, read the **`protect.lst`** file in **Outpost Firewall's** install folder.

7.5 Incoming Files Guard

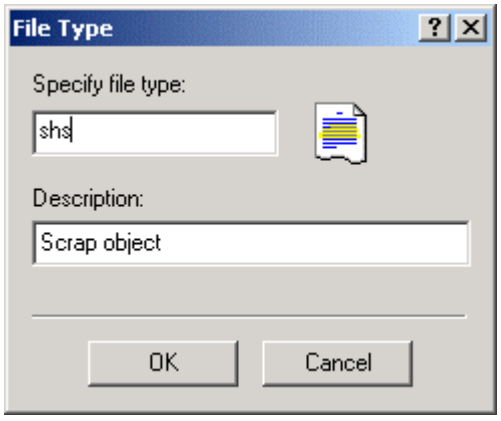
This plug-in checks the file attachments of e-mail arriving at your computer. With this plug-in, you can specify that attached files are to be renamed so they cannot harm your computer as well as to alert you with appropriate messages. Different modes of file checking can be set in this plug-in according to the file type of each attachment.

The settings of this plug-in can be modified in its **Options** dialog shown here:

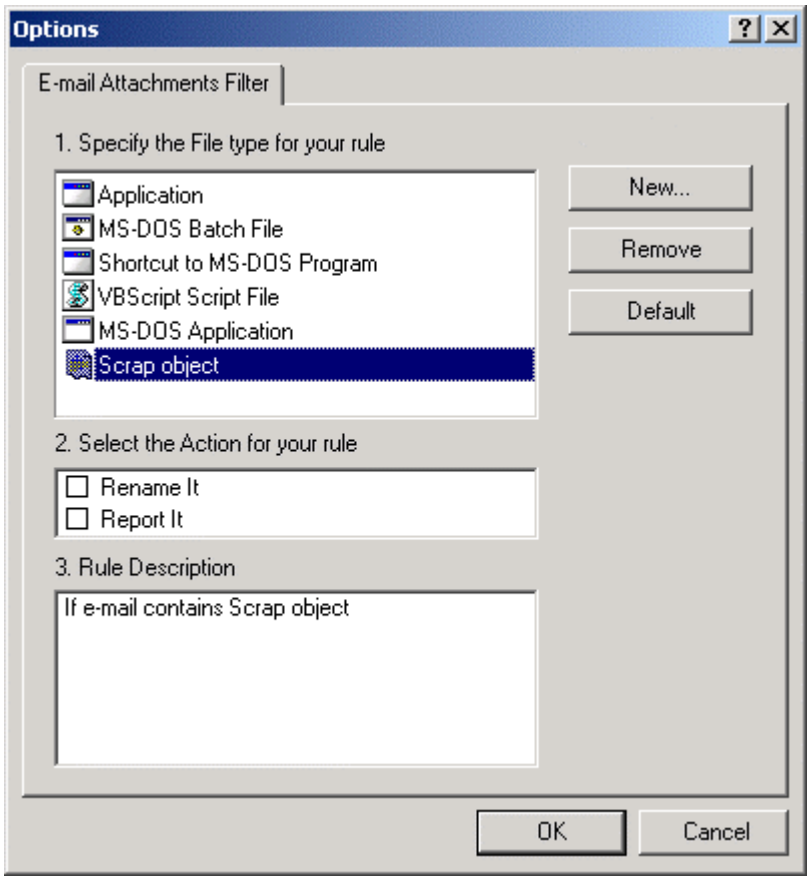


The dialog comes with the most popular file types already configured by our engineers. If you do not see the file type you want to set rules for, you can create a new rule for that file type by clicking on the **New…** button. This presents a dialog in which you can specify the extension of the file type. The description of it is automatically supplied by **Outpost Firewall** and added to the list in the above picture.

Here is the dialog that is presented:



Clicking the **OK** button brings you back to the plug-in's **Options** dialog. As you can see in the picture below, the new file type and its description has been added to the list of file types **Outpost Firewall** is set to monitor.



Add a checkmark to **Rename It** and/or **Report It** as you prefer and click the **OK** button.

Here is an example of the message that is displayed by **Outpost Firewall** whenever your computer receives an e-mail containing a file type that you specified to **Rename It** and **Report It**:

As you can see in the picture, the dialog box containing the message is displayed for a certain length of time, indicated on the button near the bottom-right corner of the message box. Clicking this button closes the message immediately.

7.6 Domain Name Cache

The Internet works by assigning a series of numbers to each computer connected to it. This is called the computer's IP address. An example of an IP address is: 64.176.127.178. You can simply type in this series of numbers into your browser's location field (near the top of your browser's window) and press your keyboard's Enter key and your browser will go to that computer's web pages.

Although these numerical IP addresses are easy for a computer to use, they are difficult for us humans to remember. So an address system was invented that uses words or letters called the DNS (Domain Name System). A DNS name is what you are probably more familiar with than IP numbers. An example of a DNS name is: www.agnitum.com .

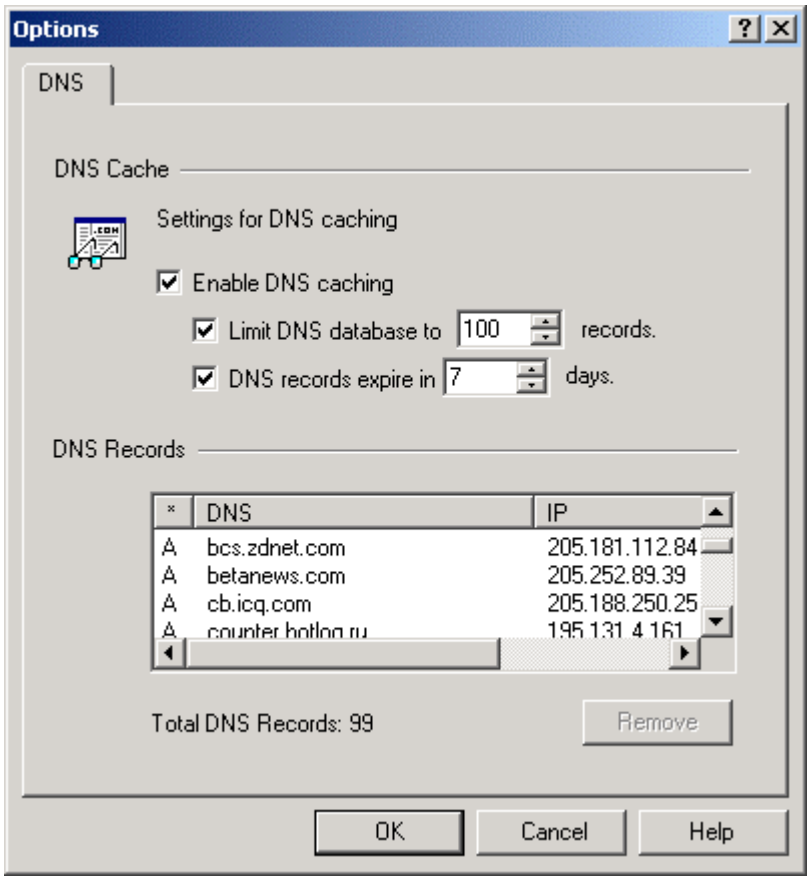
DNS names are much easier for us to remember, but our browsers still need to use the IP address to find and transfer files on the Internet. Therefore, there are databases throughout the Internet that keep track of what IP address goes with what DNS name. To find the IP address that corresponds to a DNS name, sometimes your browser has to consult several different databases located at different places on the Internet and this often takes time.

To speed things up, **Outpost Firewall** provides a personalized look-up table of DNS addresses on your own computer. This is called a domain name cache and you can customize it however you like.

Outpost Firewall maintains the DNS cache automatically within your specifications to include those addresses that are most recently used by you. The amount of time that a DNS address is saved in the DNS cache depends on the time you specify as one of the settings for this plug-in. It also depends on how many DNS names you want **Outpost Firewall** to keep track of. Only the most recently used names are kept up to the maximum number of entries you specify.

To modify the settings of the **DNS Cache** plug-in, use the **Options** menu of **Outpost Firewall's** main window. Select **Plug-Ins Setup**, highlight **DNS Cache** and press the **Settings** button. Another way to get this same settings dialog window is to right-click on **DNS Cache** in the main window and select **Properties…**.

Here is the **DNS Cache** settings dialog window:



The **Enable DNS caching** option must be selected (check marked) for **Outpost Firewall** to provide this speed up. You can limit the DNS database to a specific number of entries and have them be automatically deleted if they are not used within a certain number of days. . To not limit the database to only those entries that are used within a certain number of days, deselect the **DNS records expire** option box.

We strongly recommend that you do not increase the limits of the DNS database, change the expiry period or limit the database by unchecking any of these checkboxes.

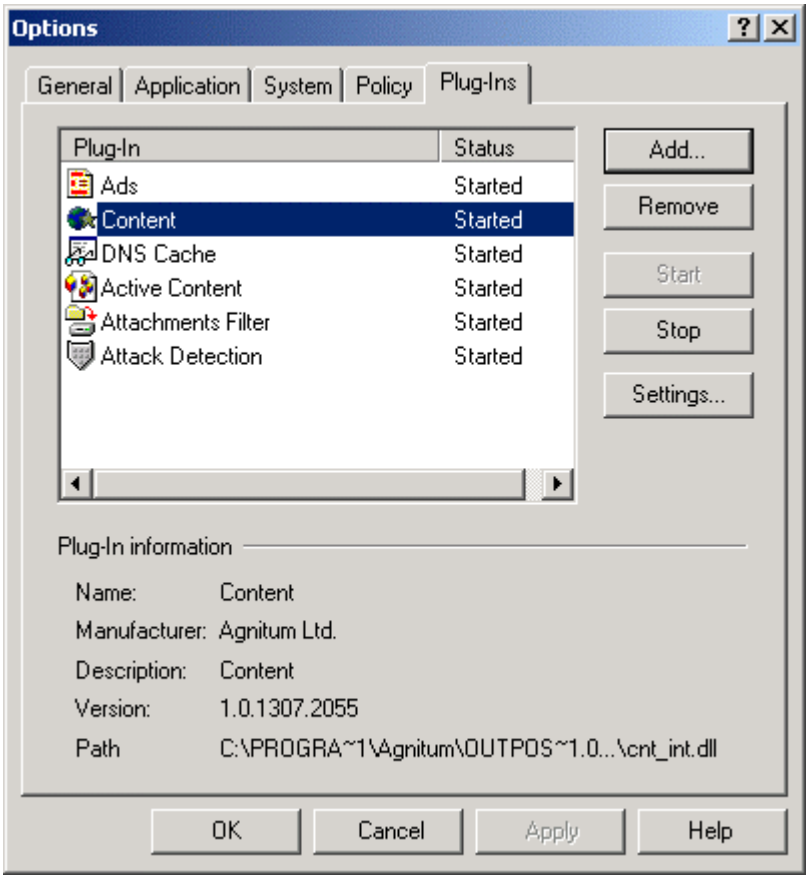
You can delete particular DNS entries from the list by highlighting the line and pressing the **Remove** button.

The list of entries can be sorted by DNS name or IP address by clicking on either of these column names.

The total number of DNS entries is shown just below the list.

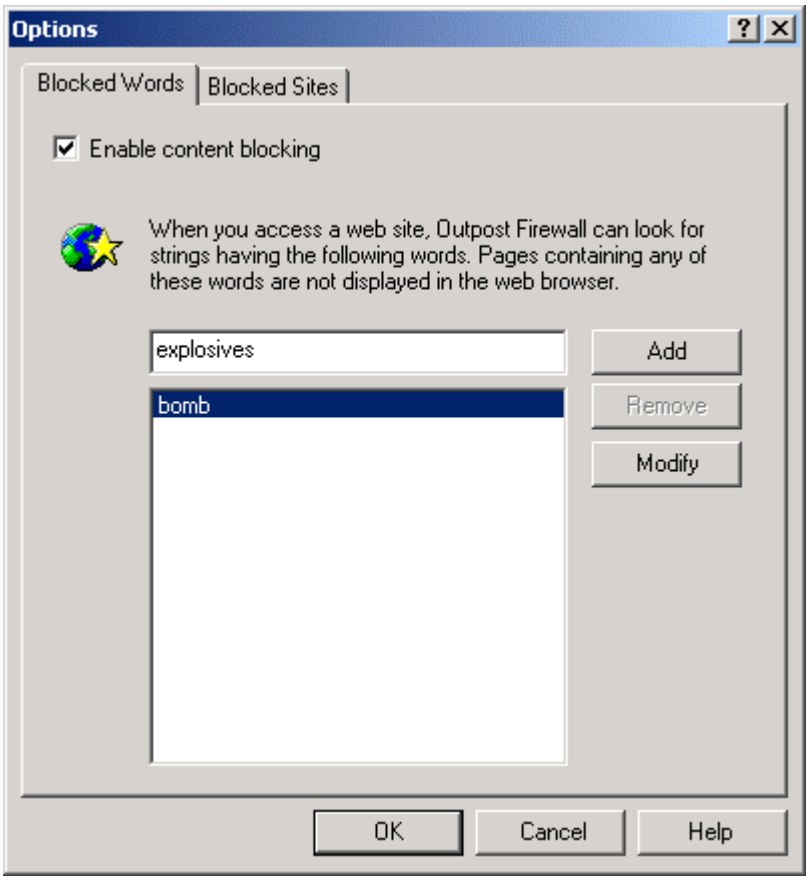
7.7 Content Blocking

You can block the display of particular web sites or pages containing objectionable material. To do this, right-click on the icon in the system tray, then select **Options** to get this dialog:



Highlight **Content Filtering** and click on the **Settings** button.

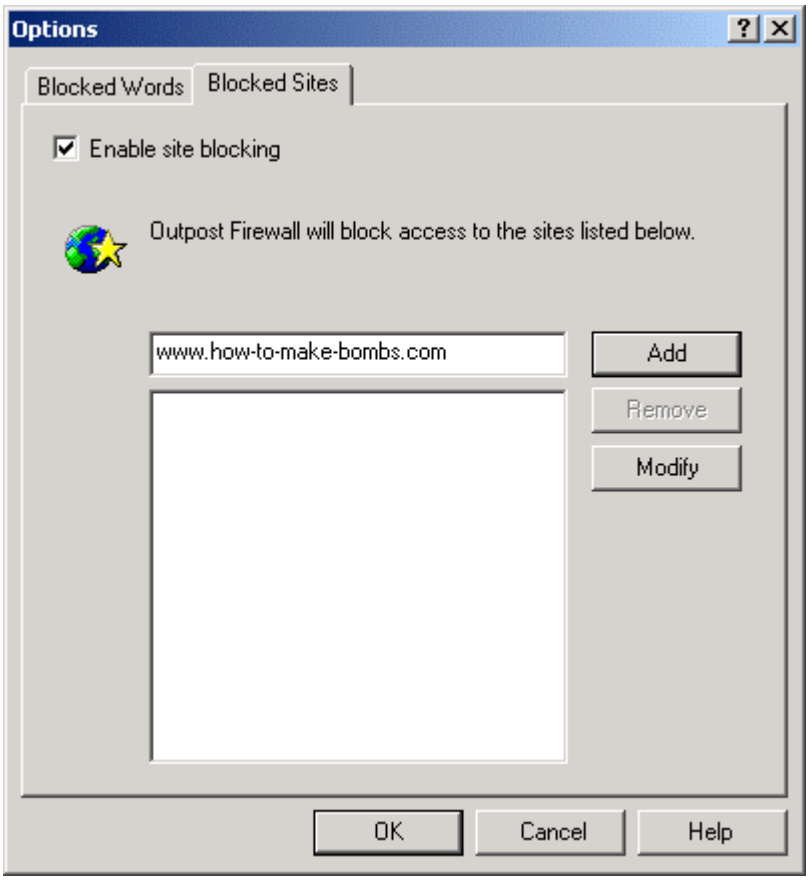
This displays the following dialog:



Select **Enable content blocking** as shown in the picture above, then start typing into the text field above the listing area all the words you do not want shown in a web page. As soon as you start typing, the **Add** button is activated. Click the **Add** button for each word or phrase. Any web page containing any of the words on this list will not be displayed.

To list particular web sites you do not want displayed on your computer, select the **Blocked Sites** tab near the top of the dialog window.

This gives you the following dialog window:



Select **Enable site blocking** so it has a check mark as shown in the picture. Type in the URL of the site you do not want displayed on your computer. As soon as you start typing the **Add** button is activated. Click the **Add** button after you finish typing in the URL of each site to be blocked. Then click the **OK** button to have **Outpost Firewall** save the list.

Part 2: For Advanced Users Only

8 Advanced Settings

8.1 Introduction

Our engineers configured **Outpost Firewall's** default settings to give optimum protection for most computer systems and networks. **Outpost Firewall** was designed from the start to be effectively used in its pre-configured state even by computer novices who need not know about network protocols to have their computer system safeguarded against malicious applications or web sites.

However, we also wanted **Outpost Firewall** to be fully configurable to advanced users, those individuals who understand networking technology.

This chapter is provided so advanced users can effectively tweak **Outpost Firewall** and learn about its most powerful features.

Note: A good rule of thumb when using **Outpost Firewall** is to keep the settings **Outpost Firewall** suggests if you do not have a particular reason and the knowledge to change them.

8.2 Saving and Loading Configurations

Outpost Firewall has very many settings. Being able to save several different configurations of these settings lets you:

- Create different configurations for you and your family or colleagues.
- Prevent your children from accessing unwanted sites (sex, games, bomb making), from playing online games or chatting.
- Switch, using one mouse click, between "Work", "Rest", "I am away", "Block Everything", and "Children" configurations.
- Back up your configurations.

A configuration is the state **Outpost Firewall** is in at any time. To create a new configuration, just change whatever settings you want and then go to the **File** menu, select **Save Configuration as…** and then enter the name you want to give that configuration. The **File** menu item **New configuration** is simply the default settings that **Outpost Firewall** had when first installed. This is given as a convenience for you when making new configurations but is not needed to create a new configuration.

The default configuration file **Outpost Firewall** uses is named **`configuration.cfg`**, located in the **Outpost Firewall** directory. You can create several different configuration files simply by giving each a different name.

A configuration file can be protected by password. To do this, use the **Options** menu and select **General** then click on **Enable** in the **Password protection** area of the dialog.

To change to a new configuration use the **File** menu, select **Load configuration…** and choose the configuration file you want or simply selecting the configuration name in the **File** menu between **Save configuration as…** and **Always on top**.

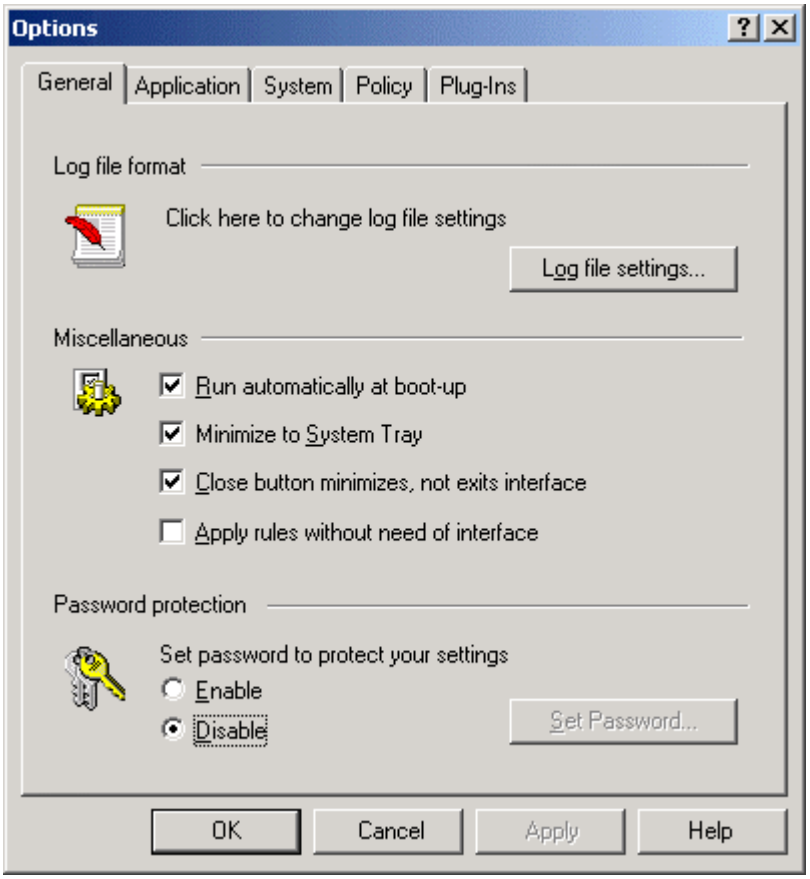
Note: Save the current configuration if you have made any changes to it before loading a new one, otherwise all your changes will be lost.

When exiting **Outpost Firewall,** the configuration file that is currently in use is saved so it will be automatically loaded the next time **Outpost Firewall** is started.

8.3 Setting a Password

You can safeguard the settings you give **Outpost Firewall** by selecting a password. This will prevent all the data you entered into **Outpost Firewall** from being changed. You can, for example, block access to objectionable sites for your children and know that your settings cannot be tampered with.

To set a password or change an old one, right-click on the icon in the system tray, then select **Options**. You will see this dialog:

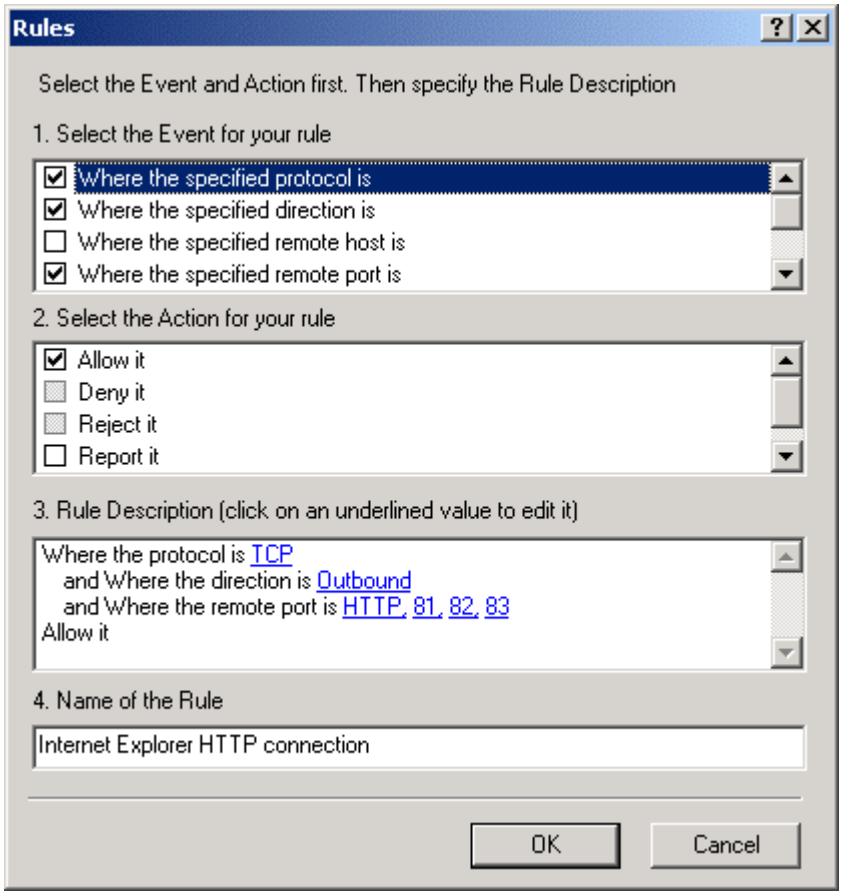


Select **Enable** under **Set password to protect your settings**. This brings up a small window in which you can enter the password you want. When you have entered in your password, click the **OK** button, then click the **Set Password** button in the above dialog window.

Note: Remember your password!

8.4 Creating Rules for Applications

This section is an extension of what was covered earlier in Application Level Filtering. The rules for applications can be set by the following **Rules** dialog window accessed from the **Options** menu, the **Application** tab, highlighting an application on the list and clicking on the **Modify** button. The dialog looks like this:



Use of this dialog is recommended only for people who know about networking protocols. A little experimentation with this dialog's interface will show the advanced user far more than a few paragraphs written here could relate.

First, describe the Event to which the rule applies. You can select from the following criteria for your rule in **Select Event** window:

- Protocol
- Direction
- Remote host and port
- Local host and port

- Time interval

Selecting a checkbox, in the **Select Event** window, adds its message to the **Rules Description** field. If a rule is listed as *undefined*, you should click on it and select one of its options.

Then select an action for your rule in the **Action field**. It can be:

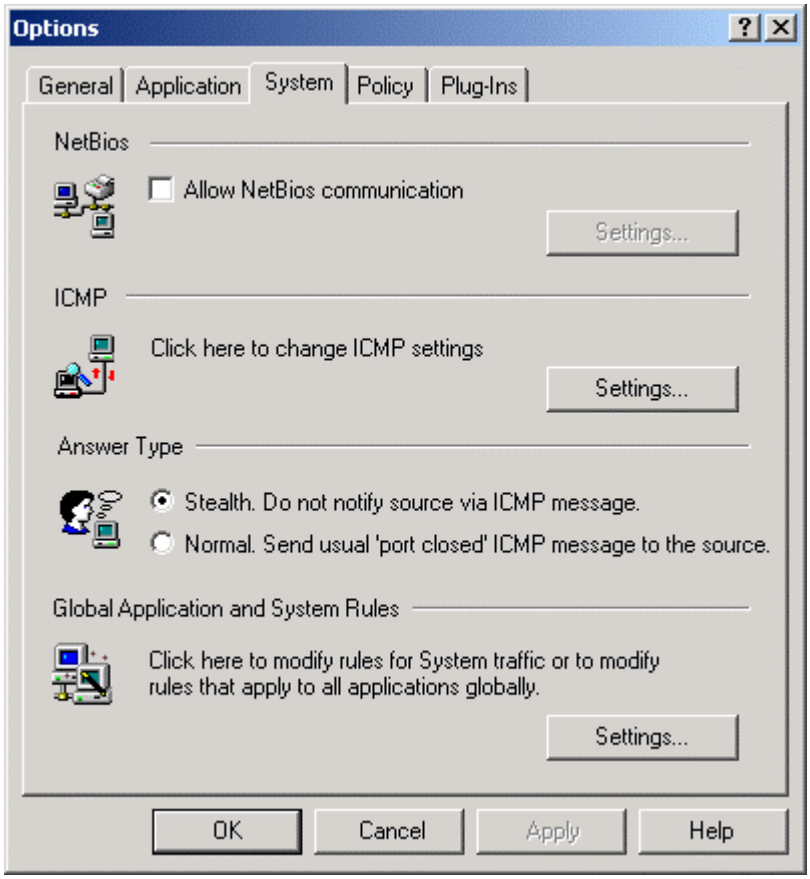
- Allow it—Allows this communication.
- Deny it—Drops the packet. The source is not notified so it appears that the packet never arrived at the destination.
- Reject it—Drops the packet and sends "the host (or port) unreachable" message to the source.
- Report it—Displays a message box when a rule is triggered.
- Run application—Runs any application when a rule is triggered.

The final step is to assign a name to the rule. We recomend that you give an understandable name to the rule, so it will be easy for you or others to recognize it in the future. In addition, the name you give your rule appears in the **Allowed** or **Blocked** log as the **Reason** for allowing or blocking this communication.

It is prudent to save the present configuration before making changes to it.

8.5 System Level Filtering

Here is the System tab of the Options dialog window accessed from the **Options** menu in the main window or the context menu of the system tray icon:



Note: These settings are for advanced users only. If any are incorrectly changed for your system or network, it could result in your firewall not working as expected.

NetBIOS—lets you allow or disallow the NetBIOS protocol for specific DNS addresses, IP addresses and/or IP ranges. **NetBIOS** is what Windows uses as the protocol for transferring shared files between computers and/or printers on a network. NetBIOS is useful on a LAN with trusted computers but it can leave your computer open to attack if NetBIOS is allowed for general Internet connections.

ICMP—lets you specify the types and directions of ICMP messages allowed. The different types of ICMP messages are listed in Types of ICMP Messages. It is recommended that you do not change the ICMP settings unless you are certain that you are making the right

changes. The **Default** button on the ICMP settings dialog resets all the ICMP settings to what they were when **Outpost Firewall** was first installed.

Answer Type—to switch **stealth mode** on of off. Normally, when your computer receives a connection request from another computer it lets the other computer know that this port is closed. In **stealth mode,** your computer will not respond, making it seem like it is not turned on or not connected to the Internet. It is recommended that you keep **Outpost Firewall** in **stealth mode** unless you have some reason not to.

Global Application and System Rules—lets you specify global rules for each of the following:

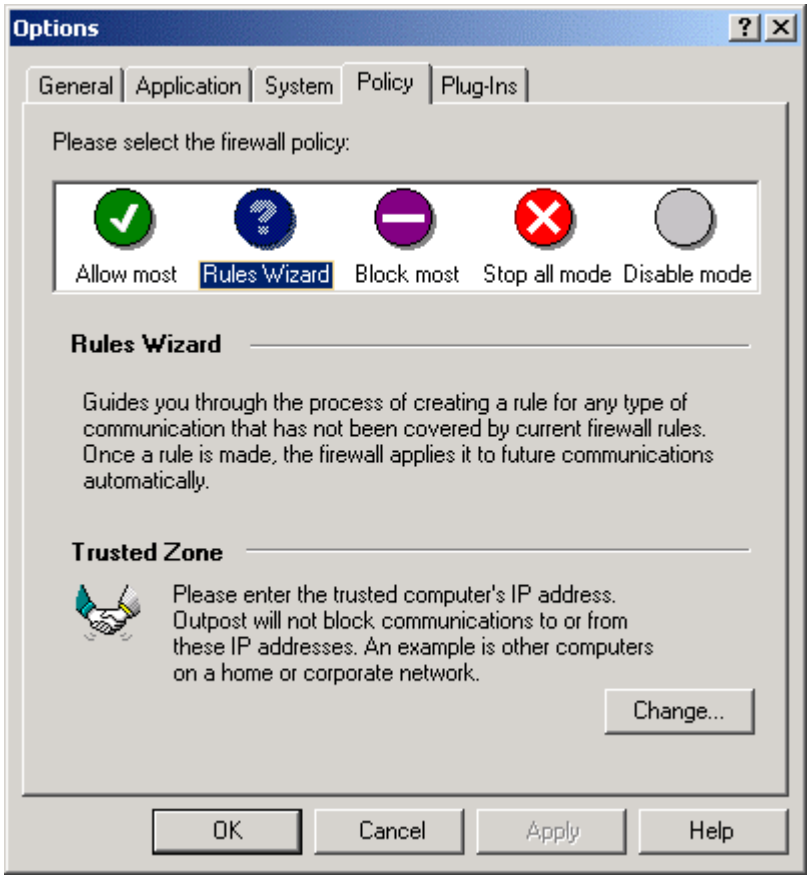
- Outgoing DNS
- Outgoing DHCP
- Deny Unknown Protocols
- Inbound Identification
- Broadcast/Multicast
- Inbound/Outbound loop back

The user can create system rules as well by clicking the **Settings…** button; very similar to how application based rules are created. Стр: 73
For more information, see section 7.4 Creating Rules For Applications.

8.6 Settings For a Home or Office Network

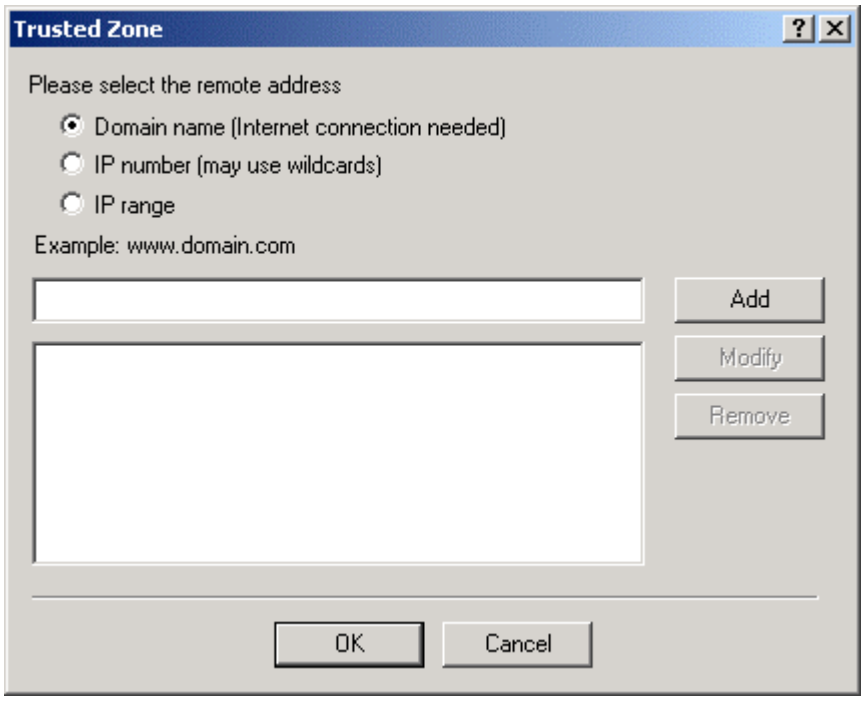
A fundamental difference between a local area network (LAN) and the Internet is the level of trust you can have in each. A LAN used in the home or an office is generally comprised of "friendly" computers, computers belonging to or operated by other family members or fellow workers. Computers on a LAN can be called a **Trusted Zone**.

To add a web site to the trusted list, right-click **Outpost Firewall's** icon in the system tray to get the context menu, then select **Options**. Select the **Policy** tab to get the following dialog:



In the **Trusted Zone** section near the bottom of the dialog window is the **Change** button. Click it to display the **Trusted Zone** dialog window.

This is the dialog you will see:



Choose one of the selections near the top of the dialog and enter in the data about the address into the input field. An example is given below the selection area for each type of address designation. An active Internet connection is required for **Domain name (Internet connection needed)** because the IP address needs to be looked up directly over the Internet. The IP address is saved along with the domain name you enter and it is this IP address that is mostly used by **Outpost Firewall**.

Click the **Add** button to add your entry to **Outpost Firewall's Trusted Zone** listing.

An entry on the trusted list can be modified at any time by highlighting it and clicking the **Modify** button.

To remove an entry, highlight it on the list and click the **Remove** button.

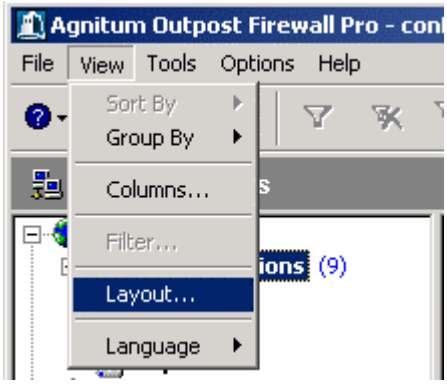
Please note that plug-ins are independent from the **Trusted Zone** settings. For example, if we add www.agnitum.com to **Trusted Sites**, **Outpost Firewall** plug-ins will block banners, active content and other things from this site regardless.

In addition, it is very important to remember that **Trusted Zone** rules are given the highest priority possible. Even restricted applications can communicate with **Trusted Zone** hosts. We advise you to put ONLY your absolutely trusted computers into this zone. If you only need file and printer sharing, please use NetBios Settings rather than **Trusted Zone**.

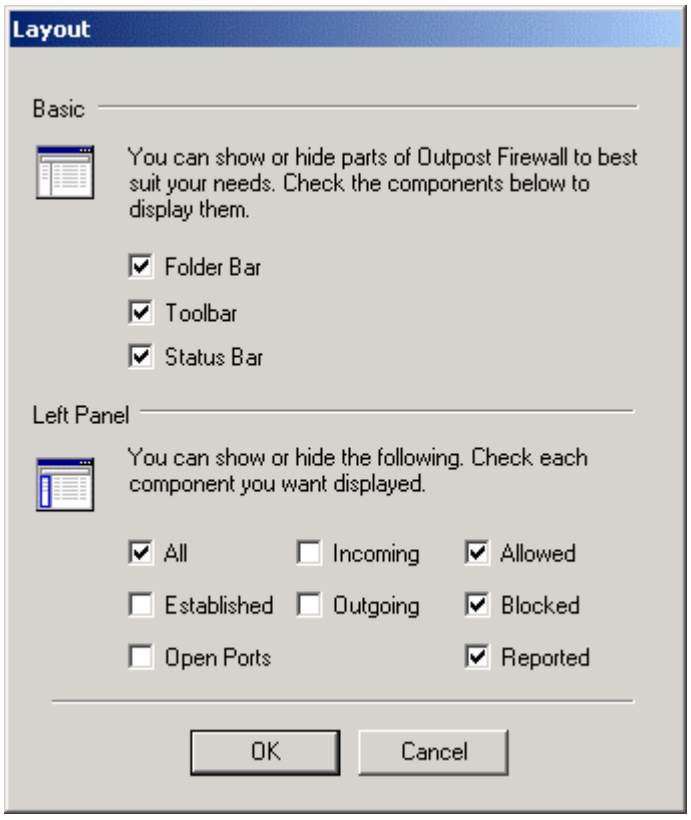
9 The View Menu

9.1 Layout

You can choose not to display the folder bar, tool bar and/or the status bar in order to increase the amount of viewing space of the Information panel. To do this, click on the **View** menu and select **Layout** as shown here:



The following dialog box lets you deselect these bars as shown:



In the section labeled **Left panel** in the above picture are the categories that can be displayed or hidden in the Left panel's listing by selecting or deselecting them in this dialog. These are:

- **All**—all objects having a network connection.
- **Established**—all objects with an established network connection.
- **Open Ports**—all objects with an open port for a network connection.
- **Incoming**—all remote objects that are connected to your computer.
- **Outgoing**—all objects that opened a connection to a remote network node.
- **Allowed**—all applications with a protocol that is supported and allowed for network operation.
- **Blocked**—all applications with network connection attempts that were blocked.

- **Reported**—all applications for which a report on their network operations must be made according to **Outpost Firewall's** settings.

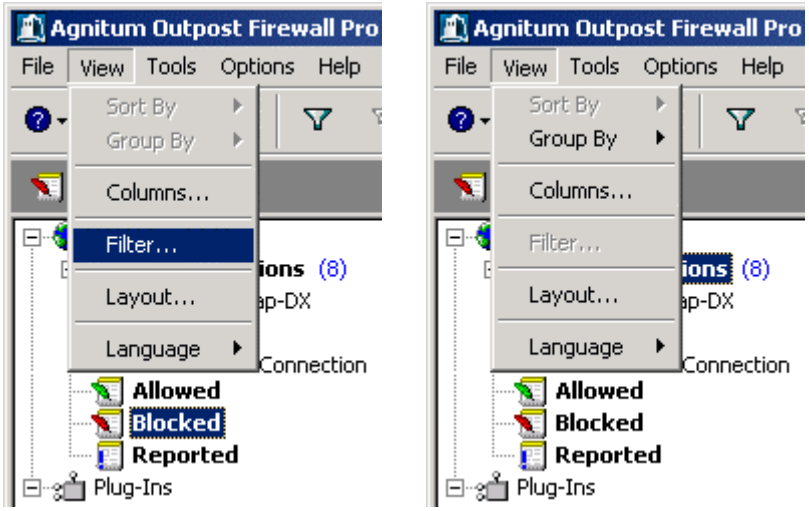
Note: The same object can be in several lists as applicable.

9.2 Filter

This filters out the data you are not interested in so you can more easily find the data you ***are*** interested in. **Filter** limits the amount of information displayed for the **Allowed**, **Blocked** and **Reported** items of the Left panel so you do not have to search through data inapplicable to the analysis you are conducting.

Using **Filter**, you can narrow your search to only the data within a specific time span and/or only the data about a particular application, port, etc.

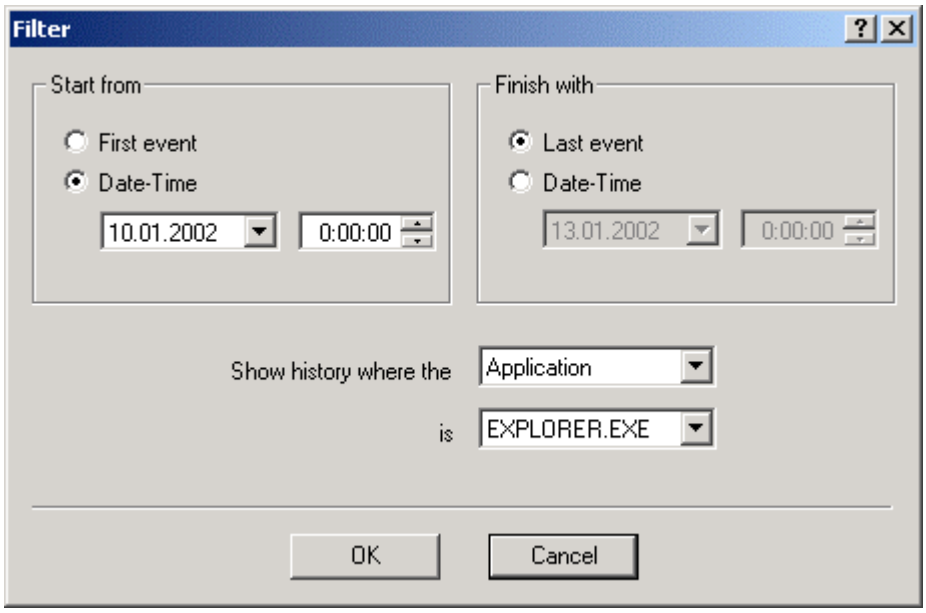
Filter is only available on the **View** menu when one of the Left panel items **Allowed**, **Blocked** or **Reported** is highlighted as shown here**:**



An alternate way to access the **Filter** dialog window is from **Outpost Firewall's** toolbar.

The **Filter** button  that is accessible only when one of the Left panel's **Allowed**, **Blocked** or **Reported** items is highlighted.

Here is the **Filter** dialog available only for the Left panel's **Allowed**, **Blocked** or **Reported** items:



Use this dialog to limit the Information panel's listing according to:

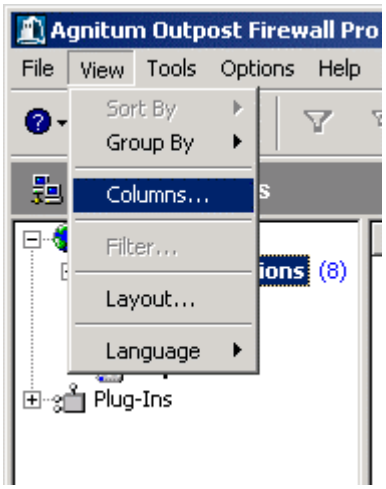
- **Start from**
  - **First event**—starts the listing from the first event that was logged.
  - **Date/Time**—starts the listing from the first event at or after the date and time you specify here.
- **Finish with**
  - **Last event—continue the listing up to the last event that was logged.**
  - **Date/Time—continue the listing up to the last event before the date and time you enter.**
- **Show history where the**—type of object to be reported in the listing is one of the following:
  - **Show All Events—do not limit the listing to any particular object.**
  - **Application—limit the listing to applications only.**
  - **Block Reason—limit the listing to one of the reasons given in the pull-down choices.**
  - **Protocol—limit the listing to one of the protocol choices.**
  - **Direction—limit the listing to inbound (coming to your computer) or outbound (leaving your computer) traffic only.**

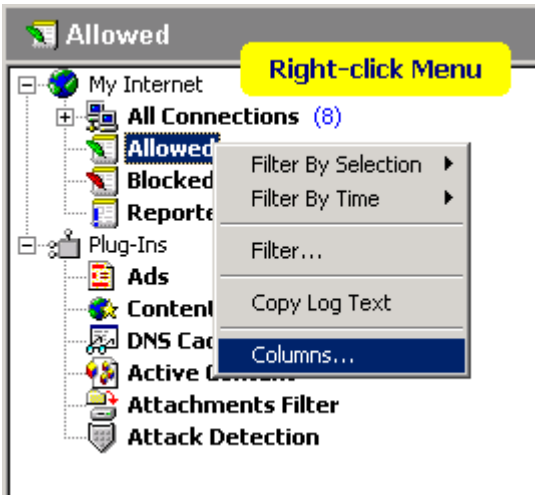
    - **Local Port—limit the listing to a specific port on your computer.**
    - **Remote Port—limit the listing to a specific port on remote computers.**
    - **Remote Address—limit the listing to a particular network address.**
- **Is**—one of the choices pertinent to the type of object selected in Show history where the selection.

After pressing the **OK** button, the filter is applied. To show all events and cancel the filter, press the **Show All Events** button on the task bar.

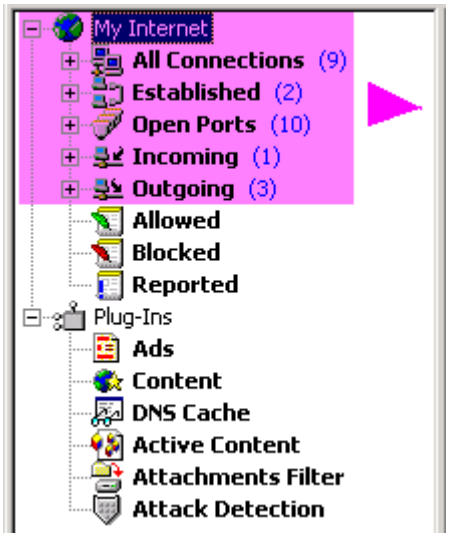
9.3 Columns

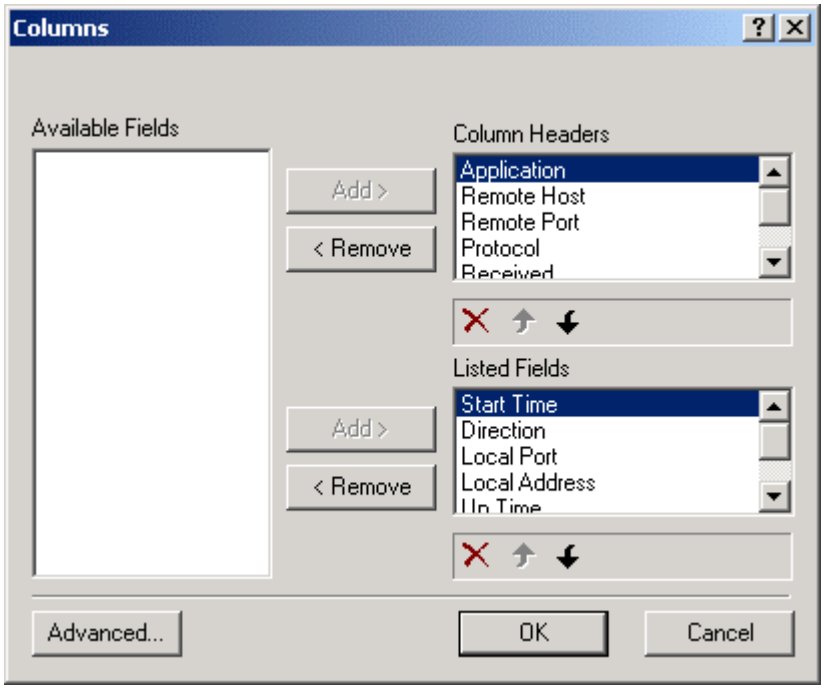
With the **View** menu's **Columns** option, you can configure **Outpost Firewall** to show you only those data you are interested in. This is also available by highlighting the line in the Left panel and right-clicking on it to get its context sensitive menu.



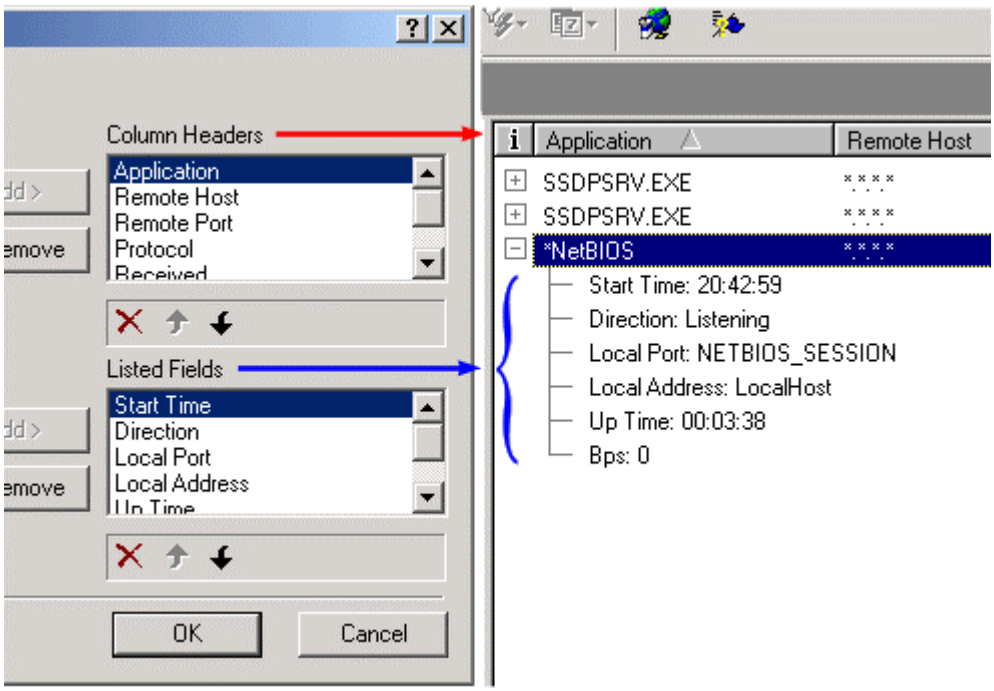


If you select an item in the pink area, then click on the **Columns** option from the **View** menu, the following **Columns** dialog is displayed:





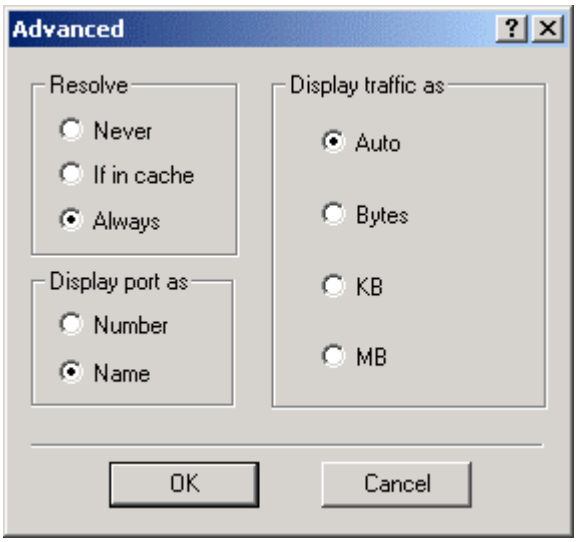
The **Column Headers** and **Listed Fields** in this dialog correspond to those in the Information panel as shown here:



You can customize the listings by removing an item on the list using the **< Remove** button or adding a previously removed item back to the list using the **Add >** button. The  button below each listing does the same as the **< Remove** button.

You can re-arrange the sequence of the items for each listing also. To move an item in either the Listed Fields or Column Headers list, use the up arrow button  to move the item one line up or the down arrow button  to move the item one line down. These buttons are located under the listing they influence.

At the bottom left corner of the dialog window is the **Advanced** button. Clicking this displays the Advanced dialog:



The **Resolve** section gives you the choice of displaying network addresses as DNS (example, www.agnitum.com)

- **Never**—always display these addresses as IP addresses (example, 64.176.127.178). However, this is not recommended as it can result in a great number of DNS requests.
- **If in cache**—convert these to their DNS addresses if the information for the address conversion is stored in the DNS Cache module.
- **Always**—always convert and display these addresses as DNS addresses.

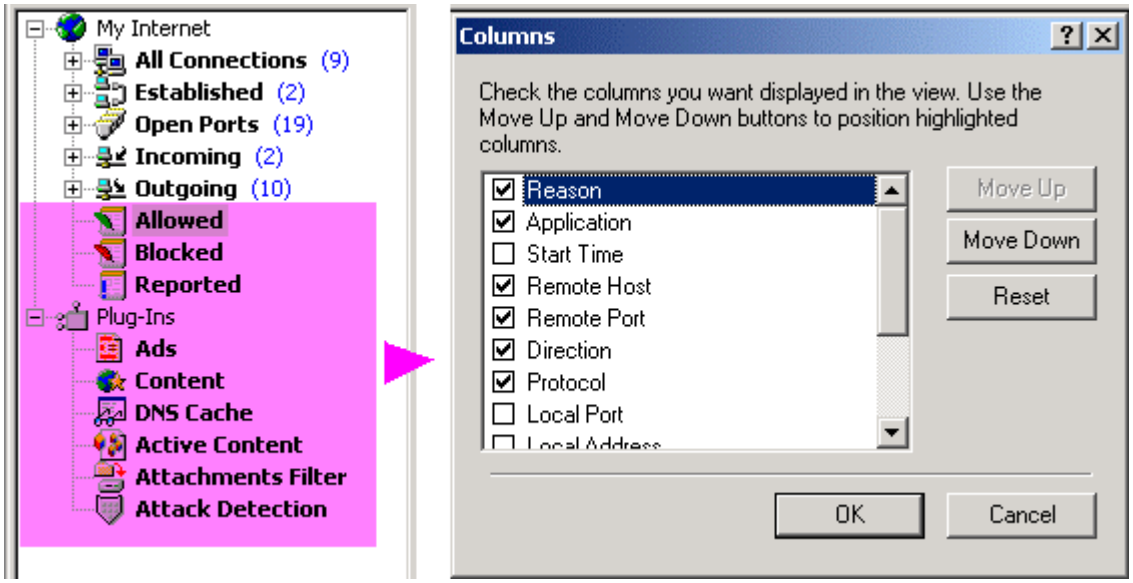
The **Display port as** section lets you display the Local Port (on your computer) and Remote Port values as:

- **Number**—ports are displayed as numbers.
- **Name**—ports are displayed as names describing their task, if the information is available in the system for that port (for example, “www” rather than “80”).

The **Display traffic as** section lets you specify the base measure of the amount of transferred information in the Sent and Received fields as:

- **Auto**— displays traffic in the most suitable measurement.
- **Bytes**—displays traffic in number of bytes sent or received.
- **KB**— displays traffic in kilobytes.
- **MB**— displays traffic in megabytes.

If you select an item in the pink area, then click on the **Columns** option from the **View** menu, the following **Columns** dialog is displayed:



Select the columns you want displayed in your log by putting a checkmark in its square. An empty square means that item will not be displayed. Different columns are displayed for different logs.

You can arrange the sequence of the columns in your log by using the **Move Up** and/or the **Move Down** buttons. The highlighted line will move up or down depending on which of these buttons is pressed.

The **Reset** button brings the entire list back to the way it was before you made any changes to it.

Click the **OK** button when you have the list to your liking. This saves your formatting. Otherwise, click the **Cancel** button to exit this dialog without saving your changes.

9.4 Group By

Group By is a very useful selection on **Outpost Firewall's View** menu. Using it, you can get the information you need very quickly. Normally, the information is grouped by application, which is generally the most useful grouping of information. For example, you can **Group By Application**, then click on the application you are investigating in the Left panel and **Outpost Firewall** lists all the connections of this particular application and nothing more. Another example is, if you run a web or FTP server, select **Group By Local Port**, then click on the port name in the Left panel ("www", for example) and the Information panel shows you how your computer is exactly connected to your server.

If you are looking for applications sending data to a particular computer on the Internet you can do this almost immediately if you use the **Group By** selection of the **View** menu.

Group By can be used on the following Left panel items:

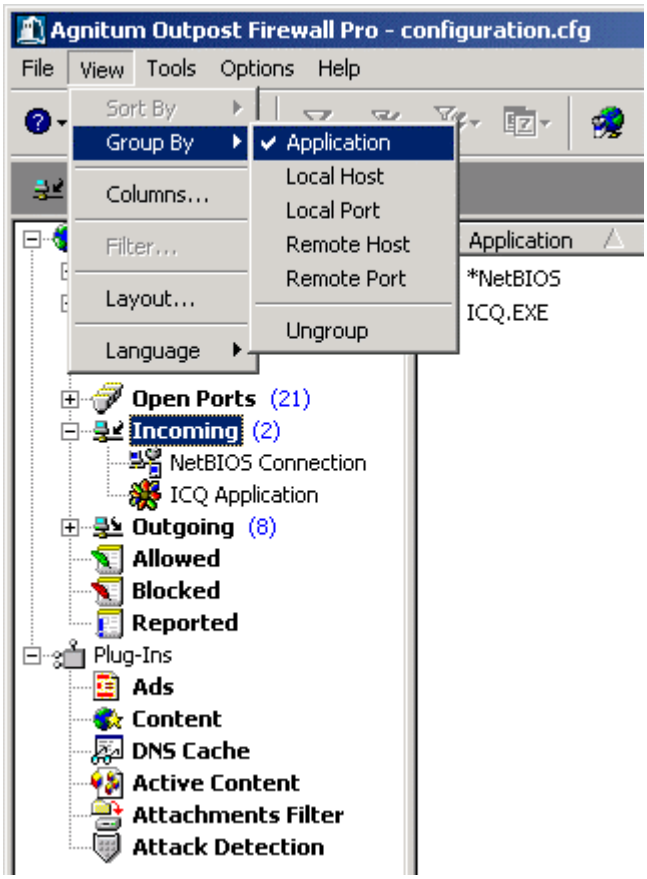
All Connections
Established
Open Ports

- Outgoing (connection established by your computer)
- Incoming (connection established to your computer by a user on another computer)

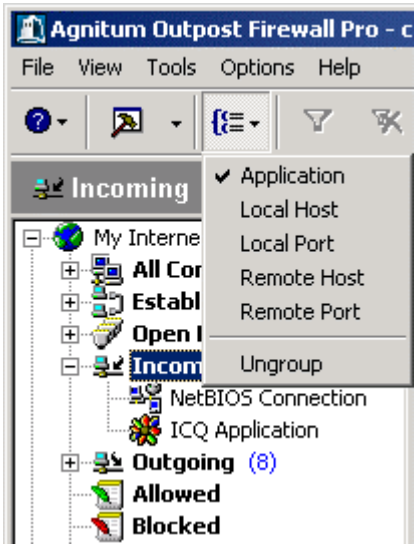
Group By changes the type of objects shown in a listing to:

Application
Local Host (your computer)
Local Port (on your computer)
Direction (incoming or outgoing)
Remote Host (another computer than yours)
Remote Port (on the other computer)

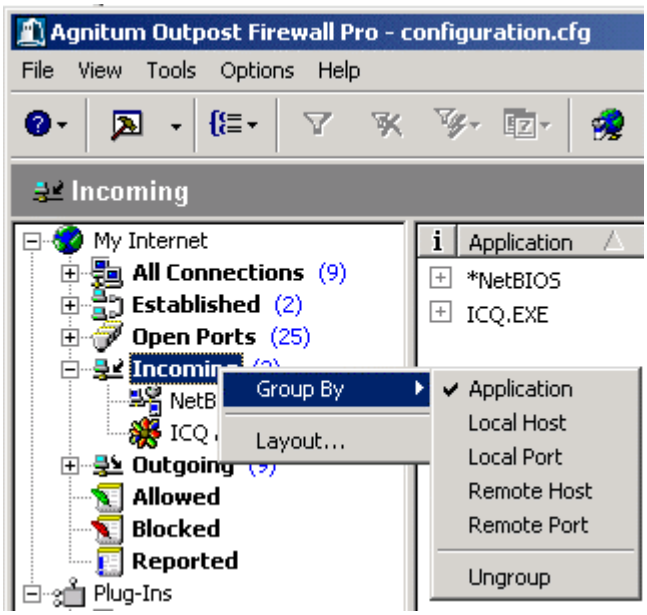
To access the Group By selection of the View menu, highlight one of the Left panel items listed above, click on the View menu and select Group By to see the following:



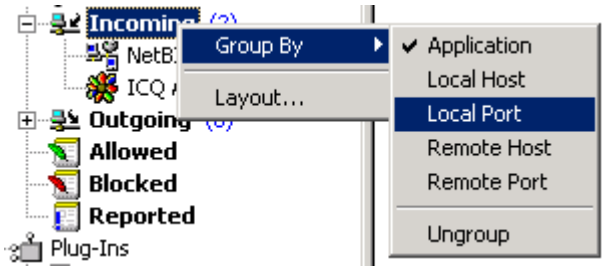
You can also get this same display by highlighting the Left Panel category, **All Connections** in our picture, and then pressing the **Group By** button  in the tool bar as shown here:



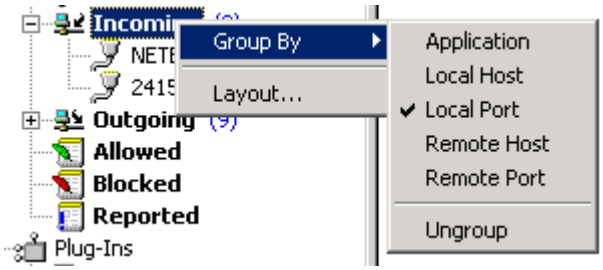
Another way you can access the **Group By** menu is by highlighting the Left panel category and right-clicking on it to get this context sensitive menu:



Clicking on an item in the **Group By** menu selects that item to be listed.



This moves the checkmark from the older item to the one just selected as shown here:



Appendix

9.5 Types of ICMP Messages

Field Value	Description
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect
8	Echo Request
10	IP Announcement
11	Time Exceeded For Datagram
12	Parameter Problem On Datagram
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

Echo Request is one of the simplest methods of checking operating conditions of a network node. Once an echo signal is received, any network node generates an **Echo Reply** and returns it to the source. If the source receives a reply to the echo request, this indicates that the main components of the traffic system are in good condition.

Destination Unreachable is generated by a gateway when it cannot deliver an IP datagram. This is the unit of data, or packet, transmitted in a TCP/IP network. Each datagram contains source and destination addresses and data.

A **Source Quench** ICMP message is transmitted from the node to the datagram source in the event that the input queue is overcrowded. In this case, the datagram is removed from the queue.

A **Redirect** ICMP message is transmitted when a gateway detects that an un-optimal route is used, then the gateway sends a request for a change of route in the routing table.

An **IP Announcement** ICMP message transmits a broadcast to announce its IP address.

The **Time Exceeded For Datagram** ICMP message is sent when a datagram is transferred from one gateway to another more times than it is allowed (normally this indicates route cycling).

A **Parameter Problem On Datagram** ICMP message is sent by a gateway if a problem occurs during the transmission of a specific datagram that is not in the range of the above messages. The datagram must be abandoned due to this error.

The **Timestamp Request** and **Timestamp Reply** ICMP messages are used to synchronize the clocks in a network's nodes.

The **Information Request** and **Information Reply** ICMP messages are obsolete. They were used earlier by network nodes to determine their inter-network addresses, but are now considered outdated and should not be used.

The **Address Mask Request** and **Address Mask Reply** ICMP messages are used to find out the mask of a subnet (i.e. what address bits define a network address). A local node sends an **Address Mask Request** to a gateway and receives an **Address Mask Reply** in answer.

9.6 The Menu System

Menu	Menu item	Description
File	New Configuration	Make a new configuration of settings based on **Outpost Firewall's** default settings.
File	Load Configuration…	Load a previously saved file of configuration settings.
File	Save Configuration	Save **Outpost Firewall's** current configuration to the same file that was earlier loaded. If no configuration file was loaded earlier, then this menu item is the same as **Save Configuration as**…
File	Save Configuration as…	Save **Outpost Firewall's** current configuration to a file of your choosing.
File	Always On Top	Keep **Outpost Firewall's** main window on top of all other dialog windows
File	Exit	Close the main window (does NOT mean to shut down the firewall)

Menu	Menu item	Description
View	Sort by ▸	Specify the column and sorting order of the lines in the Information panel (the right-side panel of **Outpost Firewall's** main window).
View	Group By ▸	Specify the types of connections in the Left pane.
View	Columns…	Specify the columns of data to be displayed and their sequence in the Information panel.
View	Filter…	Filter unwanted data from the display of a log file in the Information panel to help narrow down a search for specific network activities.
View	Layout…	Specify the kind of elements in the My Internet list to be displayed in the Left panel
View	Language ▸	Set the language of **Outpost Firewall's** interface

Menu	Menu item	Description
View ▸ Group By	Application	Group by names of applications
View ▸ Group By	Local address	Group by names of local hosts
View ▸ Group By	Local port	Group by names of local ports
View ▸ Group By	Direction	Group by direction (listening or outbound or open port)
View ▸ Group By	Remote address	Group by names of remote hosts
View ▸ Group By	Remote port	Group by names of remote ports
View ▸ Group By	Ungroup	Do not group

Menu	Menu Item	Description
Tools	Clear All Log Information	Clears all log information from **Outpost Firewall's** logs
Tools	Export log files…	Exports all plug-ins and firewall log files into text format

Menu	Menu Item	Description
Options	General…	Display the system settings window with the General tab activated.
Options	Application…	Display the system settings window with the Application tab activated.
Options	System…	Display the system settings window with the System tab activated.
Options	Policy…	Display the system settings window with the Policy tab activated.
Options	Plug-Ins Setup	Display the system settings window with the Plug-Ins tab activated.

Menu	Menu Item	Description
Help	Contents and Index	Display **Outpost Firewall's** main help files.
Help	Context Help	Display help for a main window element.
Help	Read me	Display **Outpost Firewall's** readme file.
Help	Automatically Check for Updates	Select this to automatically update **Outpost Firewall** as updates become available.
Help	Outpost Firewall on the Web ▸	Display the sub-menu of online support options.
Help	About Outpost Firewall	Display the dialog window containing the current version of **Outpost Firewall** and each of its components.
Help ▸ Outpost Firewall on the Web	Outpost Firewall Overview	Display the web page containing a brief description of **Outpost Firewall**.
Help ▸ Outpost Firewall on the Web	Online Support	Display the web page containing the various choices of online support.
Help ▸ Outpost Firewall on the Web	Outpost Firewall Home Page	Display **Outpost Firewall's** home page of its web site.
Help ▸ Outpost Firewall on the Web	Agnitum Home Page	Display **Agnitum's** home page of its web site.

9.7 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:
Limited broadcast or **limited 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.
Broadcast or **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 can support 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 an instability 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. Example: www.agnitum.com is easier to remember than the IP address 216.12.219.12. 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. 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.

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.

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. MS Windows is a later GUI.

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 Group Management Protocol) - allows Internet nodes to report on errors or submit information on unusual operating conditions. ICMP messages are transferred via the Internet to 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 (.). 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 package 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 package, all nodes having that address will receive that package. 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 for Workgroups networks and the networks of other companies.

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.

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).

Server – is a computer that sends files and web pages to client computers over a network.

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. 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.