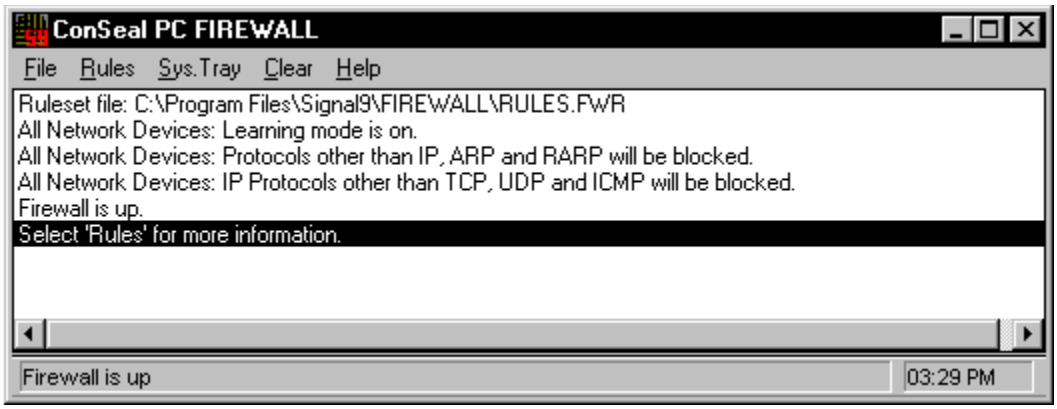


ConSeal PC FIREWALL by Signal 9 Solutions Inc.

Overviews
General overview
Using ConSeal PC FIREWALL
Enough about TCP/IP to get by (and some of the dangers of the Internet)
Glossary

Getting Started
When do I start the firewall?
Can I use another person's ruleset?
Help me build my ruleset: summarized, detailed
What are all those services listed on the Filtering page?
How do I know it's working?
What should I allow?
What should I block?

Becoming an Expert
I want one rule to allow a service for all sites
I thought I wanted one rule to allow all services from one site
Fine tune the ruleset
I have a proxy server/firewall between me and the Internet
I want my system to forward traffic to an internal network
I want to Copy/Paste IP addresses

Commands
File Menu
Rules Menu Item
Clear Menu Item
Help Menu

Registration and Support
Registration
Support

What's new in this version?

Version 1.3 is a no-charge upgrade exclusively for those who have purchased ConSeal PC FIREWALL.

Improvements, v1.3:

Easier licensing method. The licensing method has been changed to make it easier for people who are installing Windows 98.

Group delete of rules. You can now delete many unwanted rules at a time. To do this, select a group and then choose 'Delete'. To select a group of rules, either hold down the 'Shift' key and use the up or down arrow, or hold down the 'Ctrl' key and select rules with the right mouse button. A rule is selected when it is shown with a black background.

Group import and export of rules. You can now import or export a group of rules, to or from a .FWS ("rule subset") file. To export, select a group of rules and left-mouse click to get the popup menu, then select 'Export'. To import, just right-mouse click to get the popup menu, then select 'Import' and choose the correct .FWS file.

Menu item to clear log messages. A menu item has been added to let you clear the messages from the log window.

Improvements, v1.2:

Comments describing each rule. A description field has been added to rules to explain what a rule is supposed to do to protect you and how it does it. You are free to edit this to add your own comments.

Program window size and position is remembered. The next time you run the firewall, it will start in the same place and have the same size. Also, a setting is added on the Rules/Control page to start the firewall in the System Tray (to keep it out of the Task Bar).

No more warnings about non-IP packets. A single log message at the start indicates whether non-IP protocols will be allowed or blocked. Likewise, a log message indicates whether IP protocols other than TCP, UDP and ICMP will be allowed or blocked. These are options that can be set by selecting the Rules menu item, going to the ruleset page and selecting the 'Advanced' button.

An option was added for rules to block incoming fragmented packets. Fragmentation is not common and is the method of several serious denial of service attacks, such as 'teardrop', 'bonk' and 'boink'. The 'basic' ruleset supplied during installation blocks fragments on all incoming packets. Previous versions of ConSeal PC FIREWALL did not filter fragments properly and

typically blocked them.

Version 1.2.1 includes bug fixes for v1.2.

General overview

ConSeal PC FIREWALL is the most comprehensive firewall available for your PC. It sets new standards in PC protection and ease of use. Unlike packet filters built on Winsock wrappers, ConSeal PC FIREWALL catches all network packets, including fileshare activity and other protocols such as ICMP, NetBEUI and IPX.

ConSeal PC FIREWALL runs silently in the background as you work. It blocks unwanted network traffic, in and out, while allowing only authorized data. A set of rules tell the firewall what data to allow and what to block. You can have a single ruleset for all network devices on your system, or you can create a separate rules for each one.
ConSeal PC FIREWALL comes with a pre-configured 'basic' ruleset that protects against most network attacks. Changing your ruleset is made easy by having the firewall create rules automatically based on your normal activities. Modifying rule can be done manually with a user-friendly wizard.

ConSeal PC FIREWALL also logs all activity to the screen and to the log file located in the ConSeal PC FIREWALL directory. The log files are named YYYYMM.LOG, where YYYY is the year and MM is the month. This will give unique file names until the year 11997, by which time our consultants expect to have the Year 10000 problem solved.

To use ConSeal PC FIREWALL, you must first install the product and then create a ruleset.

Using ConSeal PC FIREWALL

ConSeal PC FIREWALL runs silently in the background as you work. It blocks unwanted network traffic, in and out, while allowing only authorized data. Rules define how the firewall filters data packets. A ruleset contains a group of rules. You can have a single ruleset for all network devices on your system, or you can have a different ruleset for each one. For modems, rules can apply when dialed into a specific entry in your "phone book".

ConSeal PC FIREWALL is easy to set up. There are three ways to build a ruleset:
1) Checked Learning Mode - When traffic does not match any existing rule, you are prompted so that you can add it if you choose.

2) Unchecked Learning Mode - When traffic does not match any existing rule, a rule is automatically added to the ruleset to allow it through in the future. This is the fastest way to create a ruleset.

3) Manual Mode - You can create a rule manually, choosing exactly what to allow through.

Regardless of how you create the rules, you can edit them later.

When do I start the firewall?

You can put ConSeal PC FIREWALL in your startup menu so that it will run as soon as you log in. Also, the ConSeal PC FIREWALL icon is added to your desktop. You can double-click on that icon to start the program. Remember you are unprotected when it is not running. If you need firewall protection for accessing the Internet, be sure it is running before you dial. As soon as you are connected to your ISP (Internet Service Provider), your Windows 95 computer will try to broadcast fileshares.

We recommend you leave the firewall running. It will stop itself during shutdown.

Can I use another person's ruleset?

Yes. This is the easiest way to get started. By default, the firewall uses the rules in the file named 'RULES.FWR'. If someone gives you a rules file named 'RULES.FWR', you can replace your current file in your installation directory (probably C:\Program Files\Signal9\Firewall) and the next time the firewall runs, it will use this rules file. It is a safer practice to rename a new rules file to something different so you don't overwrite your old one. You can change the ruleset file that the firewall uses to this file.

What are all those services listed on the Filtering page?

Identification - a simple method for remote servers to get your user identity
- TCP/IP, remote port: Temp. Range, local port: 113

e-mail (POP2) - an email protocol (Post Office Protocol)
- TCP/IP, remote port: 109, local port: Temp. Range

e-mail (POP3) - a popular email protocol (Post Office Protocol)
- TCP/IP, remote port: 110, local port: Temp. Range

e-mail (SMTP) - a popular email protocol (Simple Mail Transfer Protocol)
- TCP/IP, remote port: 25, local port: Temp. Range

HTTP (World Wide Web) - HTTP is for viewing Web pages (HyperText Transfer Protocol)
- TCP/IP, remote port: 80, local port: Temp. Range

HTTPS (Secure HTTP) - HTTP secured with encryption
- TCP/IP, remote port: 443, local port: Temp. Range

News (nntp) - NNTP is for newsgroups (Network News Transfer Protocol)
- TCP/IP, remote port: 119, local port: Temp. Range

IRC - Internet Relay Chat, chat groups
- TCP/IP, remote port: 6667, local port: Temp. Range

Gopher - a tool for gathering distributed information
- TCP/IP, remote port: 70, local port: Temp. Range

DNS - a tool for matching an Internet address to a system name (Domain Name Service)
- UDP/IP, remote port: 53, local port: Temp. Range

RIP - a method of sending routing information (Routing Information Protocol)
- UDP/IP, remote port: 520, local port: 520

Fileshares-UDP - UDP ports for NetBIOS (file and print shares)
- UDP/IP, remote port: 137-138, local port: 137-138

Fileshares-TCP - TCP port for NetBIOS (file and print shares)
you connecting remotely: TCP/IP, remote port: 139, local port: Temp. Range
remote connection to you: TCP/IP, remote port: Temp. Range, local port: 139

Ftp - File Transfer Protocol

- TCP/IP, remote port: 20-21, local port: Temp. Range
active mode - TCP/IP, remote port: Temp. Range, local port: 21

Telnet - a system for remote login sessions
- TCP/IP, remote port: 23, local port: Temp. Range

ICQ - an Internet service that helps people find each other and share information
- UDP/IP, remote port: 4000, local port: Temp. Range

ConSeal VPN - ConSeal Virtual Private Network
- TCP/IP, remote port: 4995-4997, local port: 4995-4997

WINS - Windows Internet Name Server
- UDP/IP, remote port: 1512, local port: Temp. Range

Help me build my ruleset - summarized

1) Make sure the firewall is in Checked learning mode: Select 'Rules' and then the page entitled "All Network Devices" (if you have chosen separate rulesets for each network device, then do the following steps for all device pages).

2) Do your normal network activity (e.g. Email, Web browsing, etc.). The firewall will ask you if you want to allow or block each type of communication. Choose "Allow" unless you know you don't want it. Applications, such as Netscape, will be blocked until you allow them to communicate so expect some lag as you do this setup. Once you are done, you won't feel this slowdown anymore.

3) You can leave the firewall in Checked learning mode and it will keep asking you to allow or block new traffic. When you are able to communicate as usual, turn off Checked learning mode, either on the device page ("All Network Devices") or by selecting "No New Rules" when prompted.

Help me build my ruleset

A basic ruleset is supplied during installation. This ruleset allows the most common (and safe) services, such as email and web browsing.

Before you change your ruleset, you need to understand a bit about networking and TCP/IP. After that, do the following:

1) On the ConSeal PC FIREWALL window, select Rules. You will find yourself at the Control tab where overall functioning of the firewall is defined.

2) The Firewall State box allows you to define whether or not the firewall is to actively filter data, as well as what types of data are to be logged. If you put a check mark in the Logging On box, then messages are generated when network traffic matches rules that have the Log option set. Otherwise, only security related messages are logged.

3) The Ruleset Scope box allows you to decide how many rulesets are to be defined. Decide if you want one ruleset to apply to all devices, or you want to build a separate ruleset for each device. It is easier to have one ruleset and you would choose this if you had just a modem and no network cards. The advantage of separate rulesets for each device is that it is easier and more secure to tailor the ruleset to the activity you do over each device. The systems you reach over a network may be very different from those you reach over a modem. If you change this setting, you must select the <OK> button on the Control menu for the change to take effect.

4) The Ruleset Usage box defines when you want the ruleset to be used. Always is the default and should be used. Advanced users can create rulesets that are invoked when using the ConSeal Virtual Private Network (VPN). (this feature will be supported in the next release of the ConSeal PC FIREWALL)

5) Decide if you want to have password control for ruleset editing. If you share your computer or are an Administrator, you should use password control.

6) Select a ruleset page (they follow the Control page). The default is one page entitled "All Network Devices". If you chose "Separate Rulesets for Each Device", there will be a separate tab for each network device or modem found on your system.

7) There are three ways to build rulesets. Automatic Rule Learning comes in two varieties: Checked (default) and Unchecked. The third method is to create rules manually.

The firewall starts and remains (by default) in **Checked learning mode**. When your system tries to communicate in a way that is not governed by a rule in the ruleset, you will be asked if you want to allow or block it. Information is available to help you make the decision. When you do not want to make any more new rules, select the option, "No New Rules" or turn off

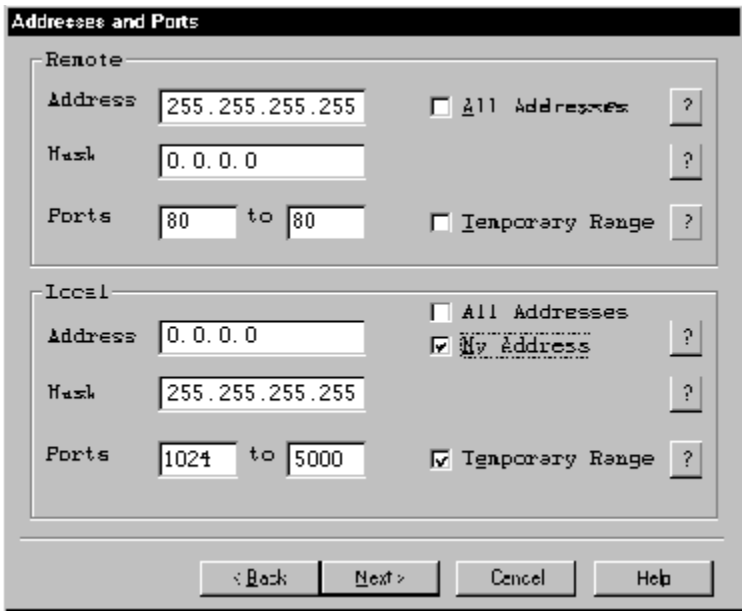
Checked mode on the Ruleset page. Alternately, just leave Checked learning mode on, and you will continue to be informed of any new activity.

If you are experienced with networks and protocols, **creating rules manually** is safe and precise.

If you aren't interested in learning the details, use Automatic Rule Learning, **Unchecked learning mode**. Here, do your normal network activity (e.g. email, Web browsing, etc.). The rules will be created automatically to allow the network traffic. When you have done all that you want to do, choose the OK button. You have made your first ruleset. These rules will be saved and the firewall will allow the same activity the next time. You should check the rules you have created (new rules are flagged with a * in the Options column). Because all activity was allowed during the Unchecked learning mode time, there may have been something allowed that you don't want. Until you remove the rule allowing it, this communication will be allowed to continue.

The next time you access your network or the Internet and the remote service appears to not respond, the reason could be that the firewall is blocking the access. Watch the message window to see if packets are blocked when you are trying to access the service. If they are, go into checked or unchecked learning mode and try again. You are probably doing something new that has not yet been allowed.

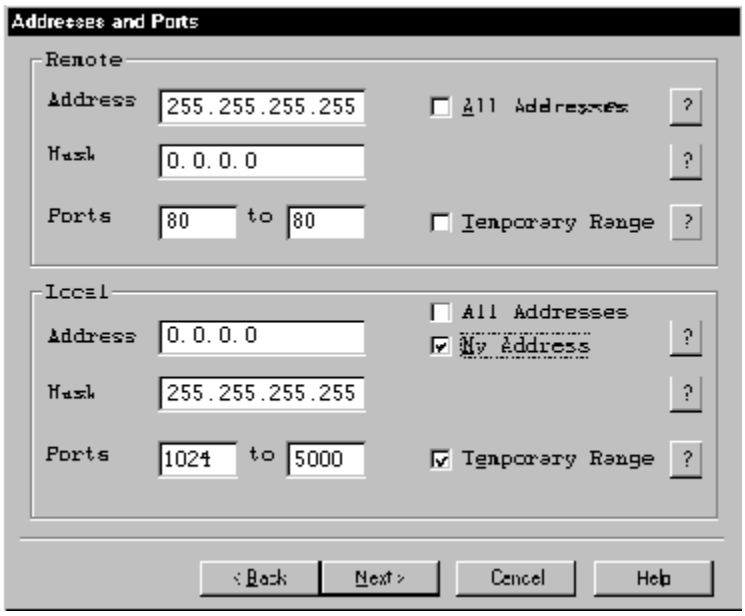
If the ruleset is looking big and repetitive, you may be ready for some expert tailoring.



I want one rule to allow a service for all sites

If your ruleset looks long and you want to condense it, and you feel comfortable allowing a service for all remote addresses, here's how to do it:

1) In the ruleset window, click on the rule you want to change.
2) Click on Manual: Edit.
3) Click on the "Next>" button until you see the "Addresses and Ports" page.
4) Select the "All Addresses" toggle to the right of the "Address" field in the "Remote" group (at the top of the page).
5) Click on the "Next>" and "Finish" buttons to save this change. This rule now applies to all remote addresses. If there are other rules for this service but are for a single remote address, they are now redundant and can be deleted. Remember to <OK> out of the Rules and Control menus to save these changes permanently.



I thought I wanted one rule to allow all services from one site

If there is a system which you trust completely and want to allow all traffic to and from it, you can do it. Before you do, consider the security risk of IP spoofing. Someone can impersonate the trusted machine. If you decide this risk is acceptable, then here's how to change your ruleset.

If you have several rules for this remote address, you will reduce it to one rule for each protocol, e.g. ARP, UDP/IP, TCP/IP. etc.

1) In the ruleset window, click on a rule for the particular IP address
2) Click on Manual: Edit
3) On the Filtering page, make sure it is the protocol you want and that inbound and outbound traffic is allowed, that "Allow" is selected on a match, and you may want to allow incoming connection attempts.
4) Click on the "Next>" button to see the "Addresses and Ports" page.
5) Check or enter port values in the "Remote" group (at the top of the page). It may be sufficient to allow ports 1-1024, if the remote system doesn't use services on your machine.
6) Check or enter port values in the "Local" group (at the bottom of the page). It may be sufficient to select "Temporary Range", if the remote system doesn't use services on your machine.
7) Click on the "Next>" button to see the "Usage" page.
8) Select "Always" so the rule applies always. If another option is more suitable, you may choose it instead.
9) Click on the "Finish" button to save this change. This rule now applies to all services on one remote addresses. If there are other rules for this address and protocol, they are now redundant and can be deleted. Remember to <OK> out of the Rules and Control menus to save these changes permanently.

Fine tune the ruleset

If you are experienced in networking or understand the settings in your automatically created ruleset, you are ready to create and edit rules yourself. If you are just starting, we recommend that you make a list of the services that you want to access, the port numbers they use and the IP addresses of the service providers. Examples of services are:

- DNS server,
- RIP server,
- email server,
- news server,
- Web sites allowed (you may want to allow all IP addresses here)

You can create rules manually or edit existing rules. You can consolidate several rules for the same service by making a more general address range and mask that allows or blocks all of them. Also, you could allow all ports from a specific address (however this isn't recommended for a system on the Internet, since the IP address can be spoofed).

Before you complete the building of your ruleset and use it, please understand your Security Policy (be it written or implied). If security is a serious issue, get a networking expert to review your ruleset.

How do I know it's working?

The firewall reports when it is blocking data (this is the default action). Try to do something that the ruleset does not allow and watch for messages in the firewall window. For example, try to ping a computer, if ping is not allowed. Your computer should report the "Request timed out".

To see a message for data that is allowed to pass, edit a rule, such as #2, "Ping others.", and set the "Warn Always" flag on the "Usage" page. Then ping another system. The firewall will beep and report that data packets are being sent through. (Remember that your system will use the ARP protocol before it tries to ping).

Another way to test the firewall is to have another computer try to access your machine where the firewall ruleset does not allow it. For example, if you block fileshares, have another computer use "Network Neighborhood" to try to view it. If the fileshares are blocked, the other machine will not be able to see your network resources and will not be able to connect.

DO NOT test the firewall by running a port scan on the same system. When a system tests itself, the data packets are not actually sent out before they are received. They are returned internally. This is called 'loopback'. The port scan will not be testing the firewall and will report as if it is not there.

To use a port scanner, run it on a different that the one running ConSeal PC FIREWALL, the system you are testing.

What should I allow?

This is different for every networking environment. The safest approach is to make a list of the network services that you use and create rules to allow just those. These rules can also be created using Unchecked learning mode. You can also use Checked learning mode to create the rules 'on the fly' as activities happen. Whatever method you use, if you want to access another type of network service in the future, you can easily add new rules later.

To understand how to protect yourself, you have to decide who you trust. If the Internet is untrusted, then block all unneeded access to it. If you are on an internal network and your system holds sensitive data, then allow access to only the systems that need it. Also, consider a Virtual Private Network (VPN).

The firewall starts in Checked learning mode, where you are assisted in deciding what to allow or block.

What should I block?

This is different for every networking environment. The default behaviour for ConSeal PC FIREWALL is to block traffic unless a rule allows it. This way, you need only add a rule for each type of traffic you want to allow.

Unchecked Learning mode is the fastest and easiest way to create rules. If you use this method for building rules for your Internet connection, you should immediately review every rule that is created. We recommend that you block NetBIOS rules for the Internet because hackers could try to access your system and do damage. Also, you probably shouldn't do a file share across the Internet because eavesdroppers will get your information easily.

The firewall starts in Checked learning mode, where you are assisted in deciding what to allow or block.

The firewall also offers an Advanced button on the Ruleset device page which allows you to control what happens to protocols which cannot be filtered by the firewall. The firewall lets you filter these IP protocols: TCP, UDP and ICMP. All other IP protocols (e.g. IGMP) are blocked by default. The firewall can also filter non-IP protocols such as ARP and RARP. All other non-IP protocols (e.g. IPX, NetBEUI) are blocked by default. You can change these default actions to allow unfiltered protocols.

I have a proxy server/firewall between me and the Internet

If the proxy server or firewall allows you access to the Internet, it probably translates the port numbers. An example is HTTP (for Web browsing). It is usually available using TCP port 80, but proxies often make it available to you on port 1080.

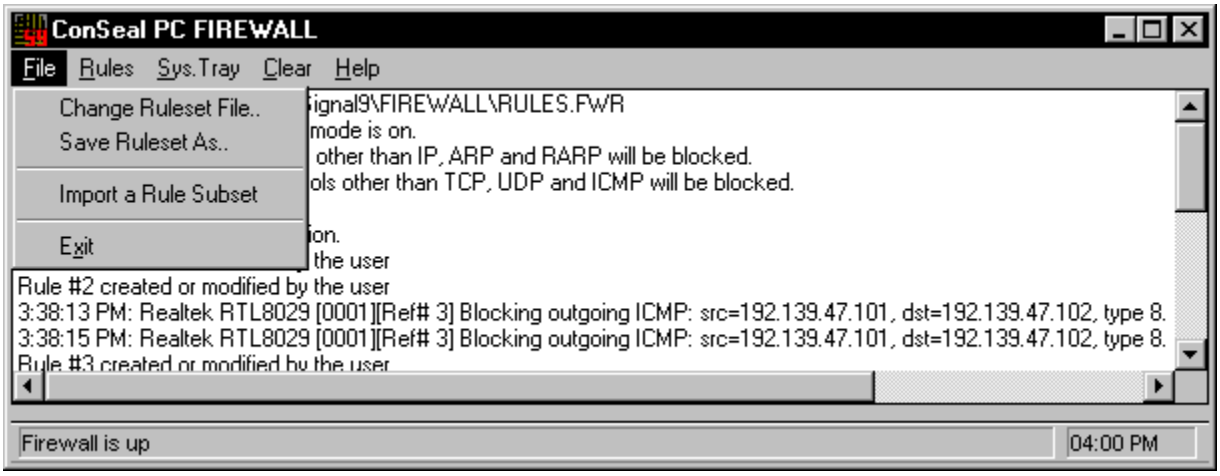
In this case, you must substitute the proxy port number for the standard one. Ask your network administrator for the proxy port numbers or check your application. Netscape users may find the information under Options/Network Preferences/Proxies: View.

I want my system to forward traffic to an internal network

When your PC is routing packets to and from an internal network, this must be reflected in the rules. If the local address in rules is set to "Own Address", then packets are only being allowed to the gateway system running the firewall. You must set the local address and mask to values that allow routing to and from the internal network.

This will be addressed fully in the next release of ConSeal PC FIREWALL, as the grayed-out "Forward" button shows. You can do it with version 1.2, but you must make two rules for each type of traffic you want your gateway to allow or block.

For this explanation, we will assume your internal network uses IP addresses in the range 190.180.170.0 - 190.180.170.255 (a range like this of 256 addresses is called a class C network). One rule you might want is to allow people on your network to do web browsing. This is typically on TCP port 80 (for now, let's assume there is no proxy service to confuse things). You are trying to get traffic from your network out to any address on the Internet and responses to get back in. To do this, you need one rule to allow internal traffic to go to and from your firewall computer and another to allow the firewall computer to relay this same traffic to and from the Internet:



Rule 1 Rule 2
(Internet) ----> In ( ) Out ----> (Internal Network)
(All Addresses) (Firewall) (190.180.170.*)
(Port 80) <---- Out ( ) In <---- (Ports 1024-5000)

Rule 1 allows all Remote Addresses (Address: 255.255.255.255, mask 0.0.0.0) with Remote Port range 80-80 (that is the HTTP service for web browsing, offered on the remote system). The Local addresses will be your internal network (Address: 190.180.170.255, Mask: 255.255.255.0) with Local Port range 1024-5000 (this it the range typically used when accessesing remote services).

Rule 2 is a mirror image of Rule 1, having 'Remote' and 'Local' values reversed. It allows

Remote Addresses on your internal network (Address: 190.180.170.255, Mask: 255.255.255.0) with Remote Port range 1024-5000. The Local addresses will be the Internet (Address: 255.255.255.255, mask 0.0.0.0) with Local Port range 80-80.

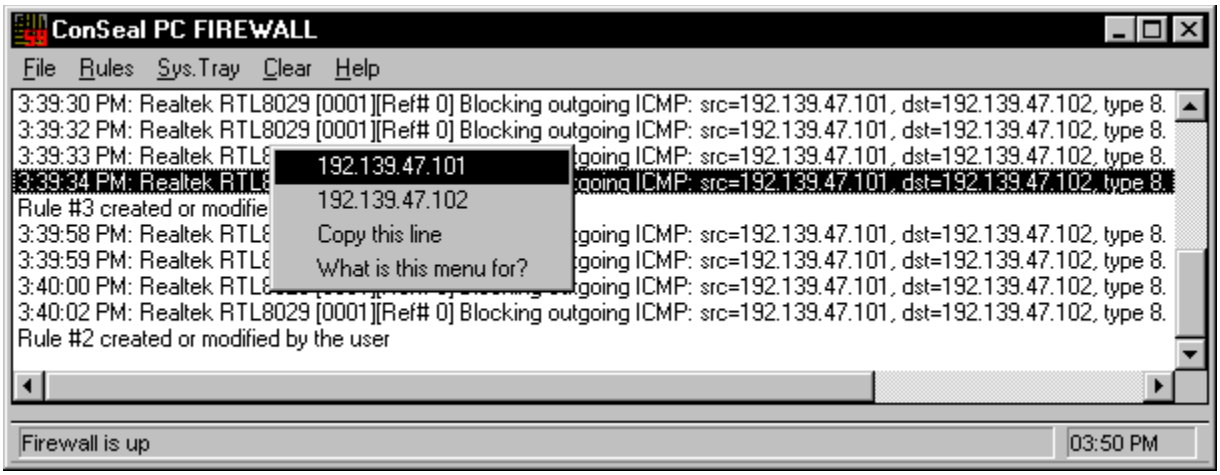
When the 'Forward' option is implemented, it will let one rule be used in either sense (i.e. remote and local can both mean the destination of outgoing data or the source of incoming data).

If your firewall is running proxy software, the systems on the internal network connect to the firewall computer, treating it as if it is the one with the HTTP server (for example, we will assume the firewall proxy uses port 1080 to provide HTTP).

	Rule 1			Rule 2	
(Internet)	----> In	(HTTP Proxy	HTTP Proxy	) Out ---->	(Internal Network)
(All Addresses)		('My Address'	Firewall 'My Address')		(190.180.170.*)
(Port 80)	<---- Out	(Ports 1024-5000	Port 1080	) In <----	(Ports 1024-5000)

You will need Rule 1 to allow all Remote Addresses (Address: 255.255.255.255, mask 0.0.0.0) with Remote Port range 80-80. The Local addresses will be 'My Address', since the connection really goes to the firweall system. The Local Port range 1024-5000.

Rule 2 will allow internal systems to connect to the firewall proxy. It allows Remote Addresses on your internal network (Address: 190.180.170.255, Mask: 255.255.255.0) with Remote Port range 1024-5000. The Local addresses will be 'My Address' with Local Port range 1080-1080.

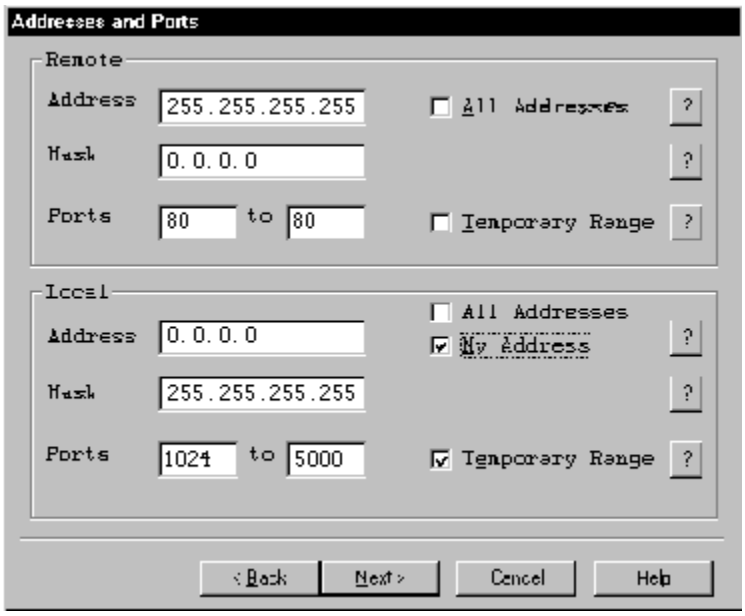


I want to Copy/Paste IP addresses

The log window reports the source and destination IP addresses of packets that caused log or warning messages. You may want to investigate further, to find out more information about a particular address. To do so, move your mouse pointer to the line containing the IP address of interest and click the right-mouse button. A menu will appear containing the IP addresses on the line. If you click on a line without IP addresses, you have only the option of copying the entire line.

When you choose an IP address, it is copied to the system's "Clipboard". This means you can go to another application and "paste" the IP address. If you copy and paste an IP address into network tool like NetLab, you can do functions such as DNS lookup, whois, finger, ping and traceroute without having to remember and type in the IP address yourself.

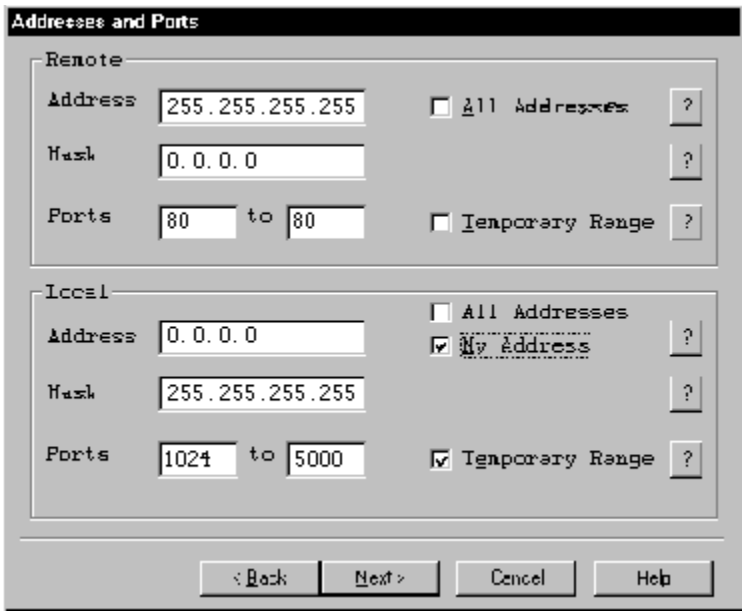
WARNING: This feature may be difficult to use when log messages are coming quickly. The line you are trying to select will move. If this happens, try to wait for a moment when the logging is less frequent. We recognize this as a problem and plan to have it fixed in the next release.



Message Logging to the Screen

Messages that are logged to the log file are also displayed in the ConSeal PC FIREWALL message window. The number of lines is limited to 200, at which point older messages are removed. New messages are shown below older ones, and the lines are scrolled up to display the most current.

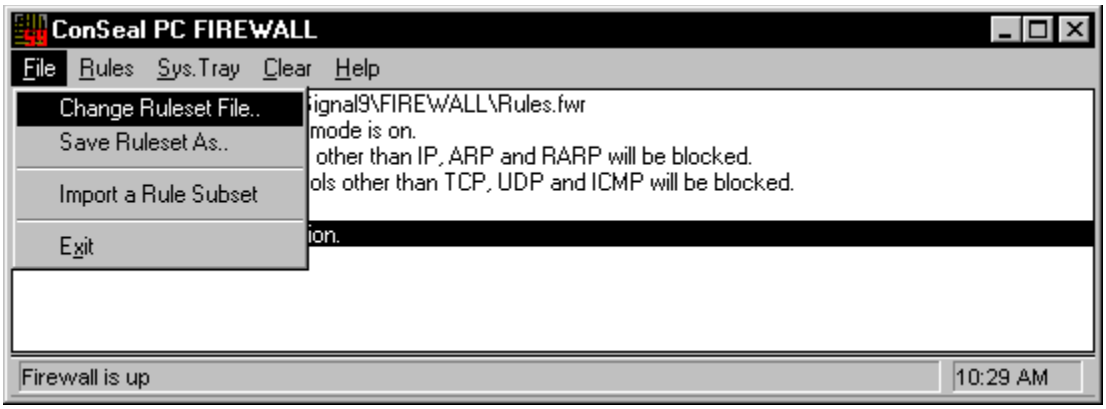
Log messages can be copied to the system 'Clipboard'. Also, messages that contain IP addresses can be used to copy the IP address to the system 'clipboard' for pasting into other applications, such as NetLab (to find DNS, whois, finger information, etc.).



File Menu

Commands

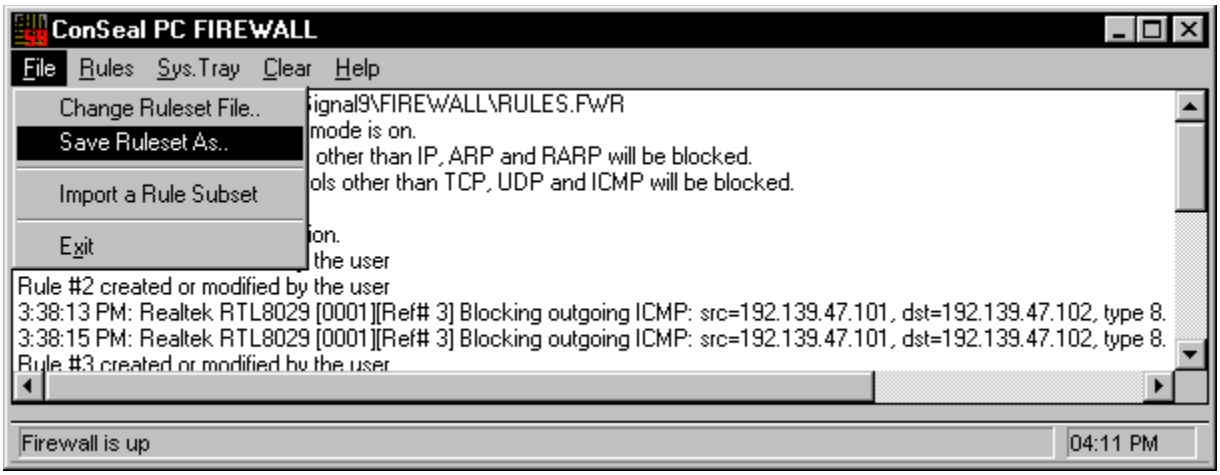
Change Ruleset File.. - Load and use a different ruleset file.
Save Ruleset As.. - Save to another ruleset file (and use it from now on).
Import a Rule Subset - Import a subset of rules into this ruleset.
Exit - Exits ConSeal PC FIREWALL closing any open tunnel connection and unblocking network traffic.



Change Ruleset File..

This command allows you to change the ruleset file that the firewall uses. When you select a new filename, the firewall will continue to use this file instead of the default file, 'RULES.FWR'.

Ruleset files have the extension '.FWR'. You will probably see two in your installation directory: 'RULES.FWR' and 'DEFAULT.FWR'. The file, 'DEFAULT.FWR' contains the 'Basic' ruleset that is offered during installation.



Save Ruleset As..

This command allows you to save the currently loaded configuration (rules and other settings) to a ruleset file on disk. This is useful if you want to keep a copy of your rules or if you want to use different rules at different times.

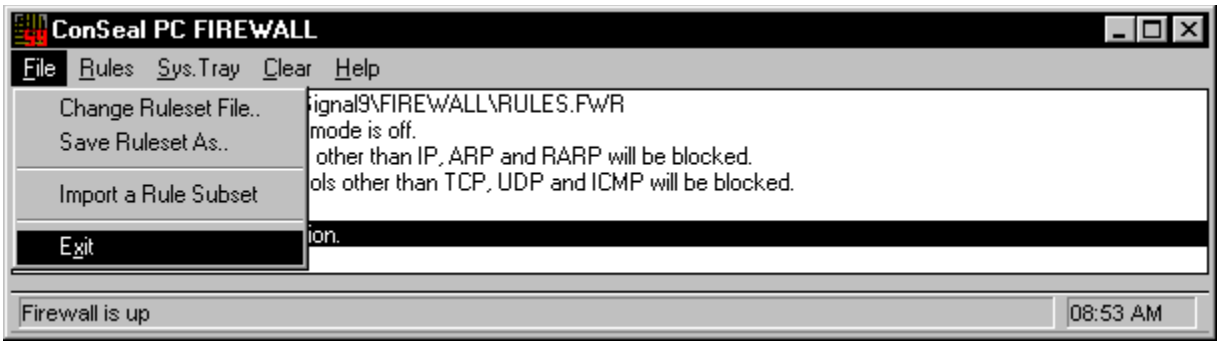
Once you have saved the rules to a file, the firewall will continue to use this file as the default ruleset file. This means until you change the ruleset file or use this command again, the firewall will use this new ruleset file.

Import A Rule Subset

This command allows you to import a rule subset file (.FWS file) into your current ruleset to make an quick addition. This is useful if a ruleset change is being distributed for a new type of threat or to allow an application like ICQ, that requires several rules.

Rule subset files prior to v1.3 were limited to containing one rule. Version 1.3 .FWS files cannot be imported by earlier versions, whoever earlier .FWS files can be imported by v1.3 of the firewall.

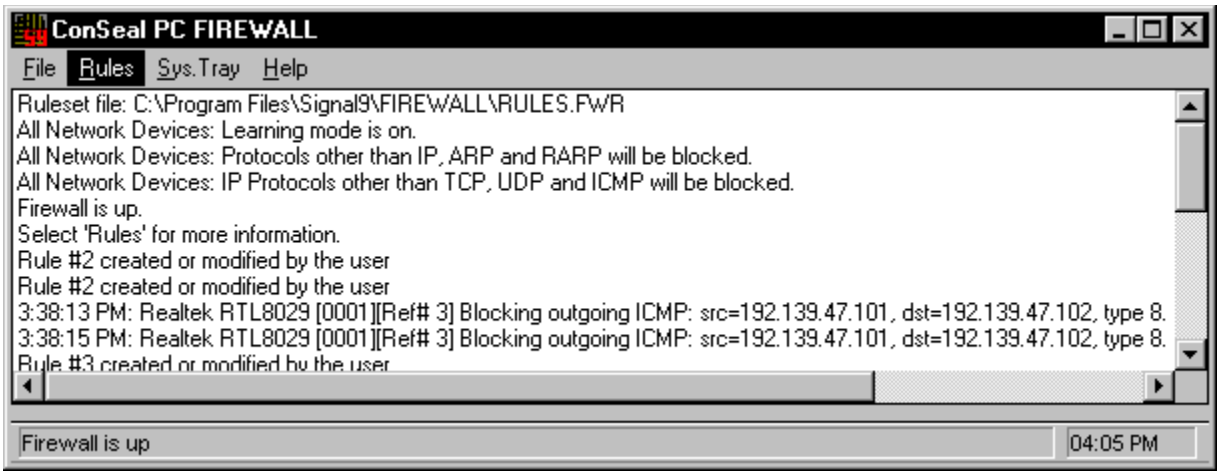
The option to import is also available when editing the rules for a device.



Exit

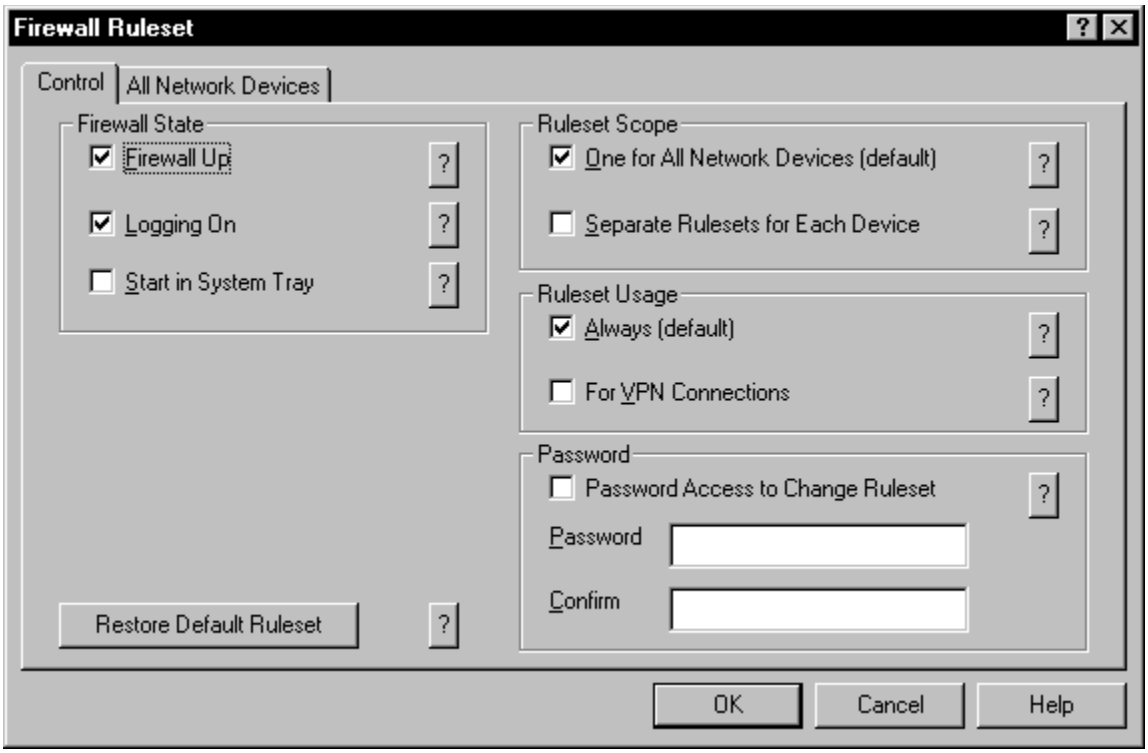
The **Exit** command exits the application. Traffic on modems and network devices is no longer blocked. It is recommended that you run ConSeal PC FIREWALL as part of the bootup sequence, and leave it running. Alternately, click on the ConSeal PC FIREWALL icon on your desktop to bring it up, and leave it running.

For **Windows 95 only**, if there are any dialup connections active when ConSeal PC FIREWALL exits, Windows 95 may hang them up.



Rules Command

The Rules menu command allows you to display and change all setting to do with the firewall. The Control page has settings that relate to overall firewall settings. The following pages provide control for the ruleset(s). If you have one ruleset that applies to all devices, then you will have a page entitled 'All Network Devices'. Otherwise, you will have a separate page for each network device that the firewall was able to locate on your system.



Control Page

The Control page has settings that relate to the overall functioning of the firewall for all network devices.

Firewall State:

Firewall Up - turns the firewall on or off.
Logging On - logs messages to the message window as well as to the log file.
Start In System Tray - set to make the firewall start with its icon in the System Tray.

Ruleset Scope:

One for All Network Devices - all devices have one ruleset.
Separate Rulesets for Each Device - each network device has its own ruleset.

Ruleset Usage box:

Always (default) - ruleset is in use whenever the firewall is up.
For VPN Connections - ruleset applies only during VPN connections.

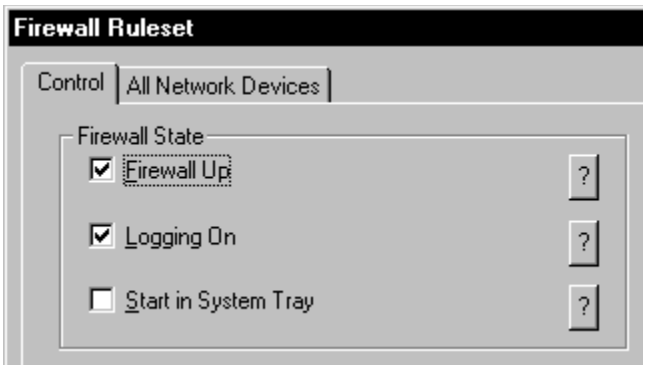
Password box:

Password Access to Change Ruleset - indicates a password is required to change or view the ruleset.

Restore Default Ruleset:

The complete firewall configuration is restored to that of the default supplied during installation. This includes the basic rules defined for specific services and protocols as well as

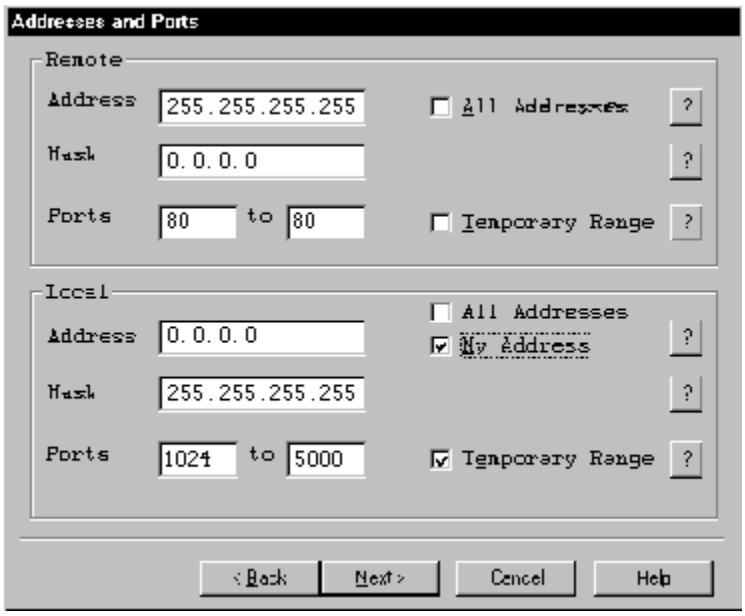
the initial settings of the Control page. Your current firewall configuration is stored in a file called 'RULES.FWR'. The default is in a file called 'default.fwr'. The experienced user may wish to put a different firewall ruleset in the file named default.fwr, in order to 'restore' a ruleset of their own choice.



Firewall Up

This is a toggle to control whether the firewall is on or off. When it is on, it filters packets according to the defined ruleset(s). When it is off, it allows all network traffic. The firewall is 'up' when the box is checked (as in the diagram).

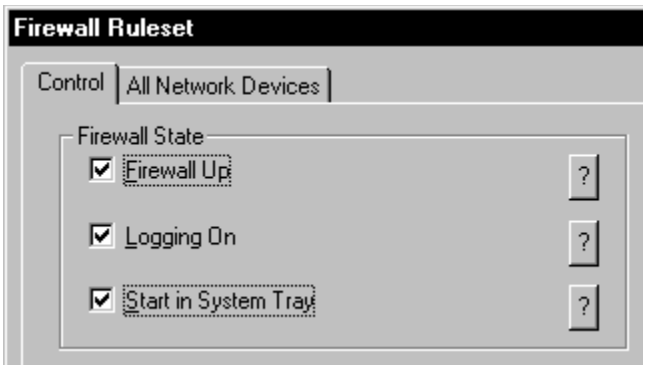
When using a password, this setting cannot be changed before entering the password.



Logging On

This toggle controls whether logging messages are reported or suppressed. When it is on, log messages are reported to the screen and to the log file on disk. When it is off, message logging is suppressed, but warning messages are still allowed.

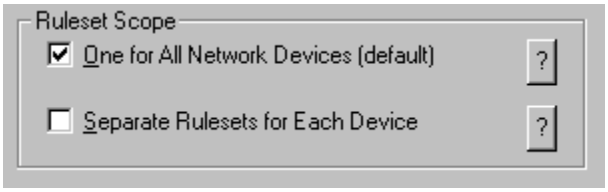
When using a password, this setting cannot be changed before entering the password.



Start In System Tray

This toggle controls whether the firewall puts its icon in the System Tray when it starts, or whether it leaves it in the Task Bar.

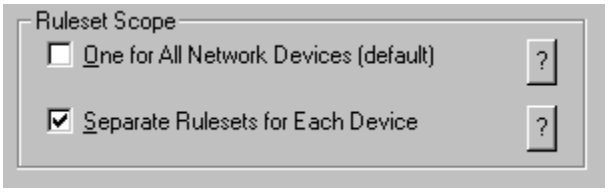
NOTE: This option is not available on Windows NT 3.51.



One for All Network Devices

This is a toggle to control whether the firewall is to create one ruleset for all network devices. When it is on, the same ruleset is applied to all devices (e.g. dialup devices and network devices). You can provide some measure of control when defining a rule by indicating that it should only be in effect when dialed into a certain phone number, or when a certain application is running.

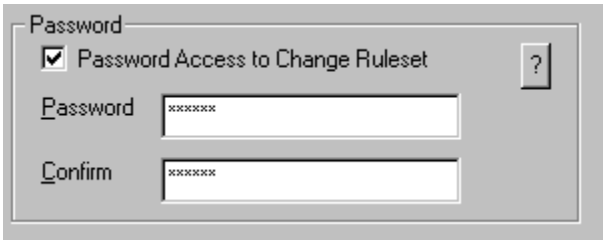
When using a password, this setting cannot be changed before entering the password.



Separate Rulesets for Each Device

This toggle specifies that a separate ruleset is used for each network device. This option gives you greater control over your communications. If you are on a network and have a modem, you can have strict access control to the Internet and freer access to your (trusted) internal network.

When using a password, this setting cannot be changed before entering the password.



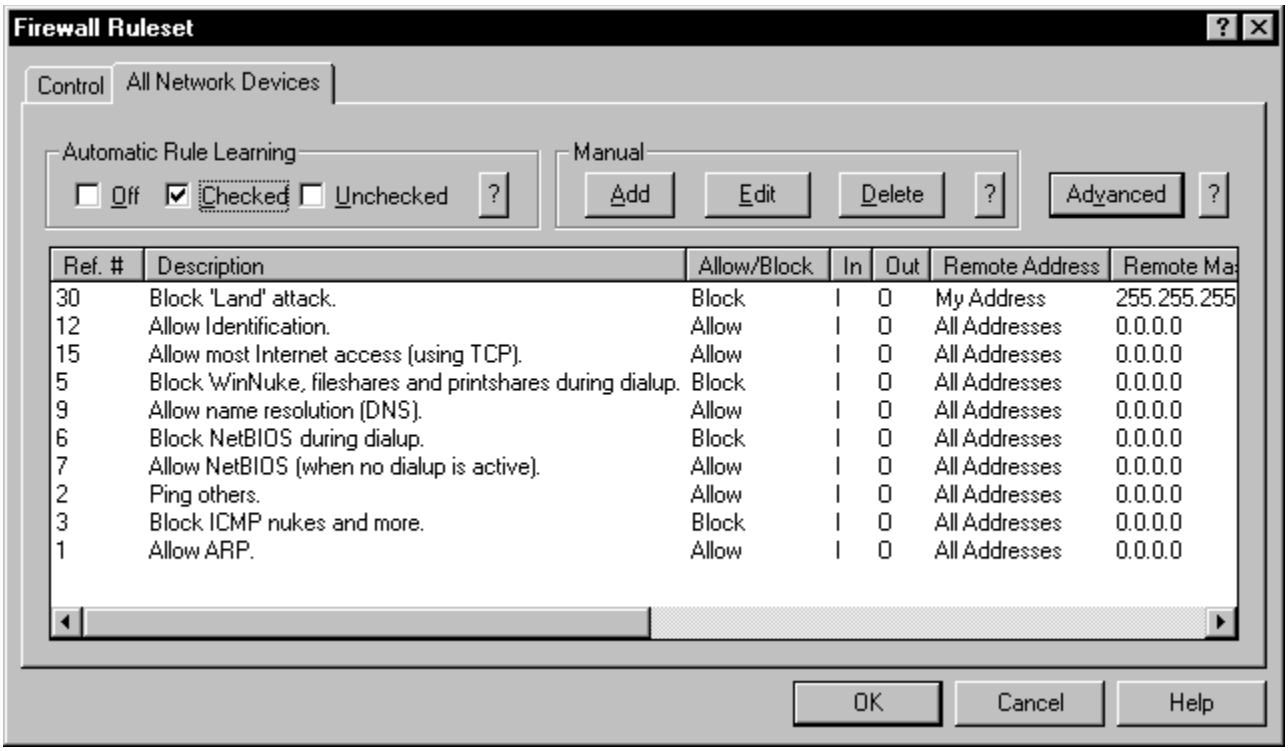
Password

You can impose password access for modifying the firewall ruleset. This is useful where the system is administered for other users. The password is used in two ways to protect the ruleset:

1) A one-way hash is stored to verify the password when it is entered. The password itself is not stored, because a person could read it from disk. You can create the hash from the password but you cannot create the password from the hash. Until the correct password is entered, the user is not permitted to modify any aspect of firewall functioning or to view or alter rules.

2) A checksum of the whole ruleset file is stored in the file. If any part of the ruleset is altered on disk, it can be detected. When the administrator enters the password, the file is checked for tampering using the checksum and if it has occured, it is reported.

For an analysis of the security of password protection, contact Signal 9 Solutions. If a password is used, it is required before the firewall can be turned off.



Rulesets for Network Devices

Each ruleset is shown on a separate page. If you choose, one ruleset will apply to all network devices, modem or dialup.

The rules are displayed in a scrollable list. Buttons and toggles allow you to build and modify the ruleset. You can build the list using unchecked or checked learning mode. Also, rules can be added, edited or deleted using the buttons in the "Manual" grouping.

The Advanced button shows what action the firewall takes if a packet does not match a rule. The standard way a firewall works is to block all traffic that does not match a rule.

The following information is displayed for each rule:

Ref # - a unique identifier of this rule.

Description - a description of the service or the protocol to which this rule applies. This is a comment field that can be modified to better explain the rule. Only the first line is shown in the Ruleset display.
Allow/Block - 'Allow' means data packets will be allowed (in or out) if they match this rule.
In - 'I' indicates the rule applies to incoming data.
Out - 'O' indicates the rule applies to outgoing data.
Remote Address - the address or address range (of remote systems) that this rule matches. The remote address is the destination address of an outgoing data packet or the source address of an incoming data packet.

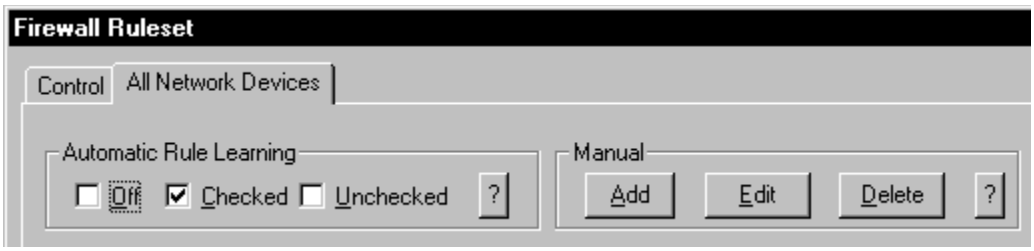
Remote Mask - the address mask that defines how to interpret the Remote Address field.
Remote Port - the remote port or port range that this rule matches.
Local Address - the address or address range (usually of your system) that this rule matches. The local address is the source address of an outgoing data packet or the destination address of an incoming data packet.
Local Mask - the address mask that defines how to interpret the Local Address field.
Local Port - the local port or port range that this rule matches.
Applies - when this rule applies.
Priority - priority (order of precedence) of this rule. Lower numbers indicate higher priority.
Options - information and attributes of this rule:

* - this is a 'new' rule that has never been edited by the user
B - block incoming connection attempts
F - block incoming fragments
L - write a log message when traffic matches this rule
l - write a log message when traffic matches this rule, no more than once every 2 seconds (useful against flooding attacks)
C - log connection attempts
W - warn the user when traffic matches this rule (Warn Always)
w - warn the user when traffic matches this rule, no more than once every 2 seconds (useful against flooding attacks) (Warn Safe)
C - log connection attempts
T - temporary rule, used in this session only (gone the next time you run the firewall)

Advanced - Defaults for Protocols that are not filtered

Some protocols are not filtered in this version of ConSeal PC FIREWALL. These are IP protocols other than TCP, UDP and ICMP, and other protocols such as IPX, SPX, NetBEUI and AppleTalk. Since these protocols cannot be checked, the default setting is to block them. You may choose to allow these protocols while the firewall filters what it knows. The "Advanced" menu lets you control whether the firewall allows other protocols or blocks them.

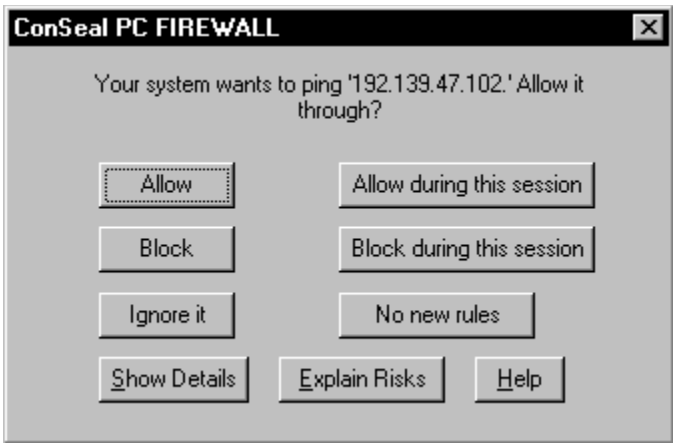
You can allow or block two separate cases: other IP protocols and other (non-IP) protocols.



Checked Learning Mode

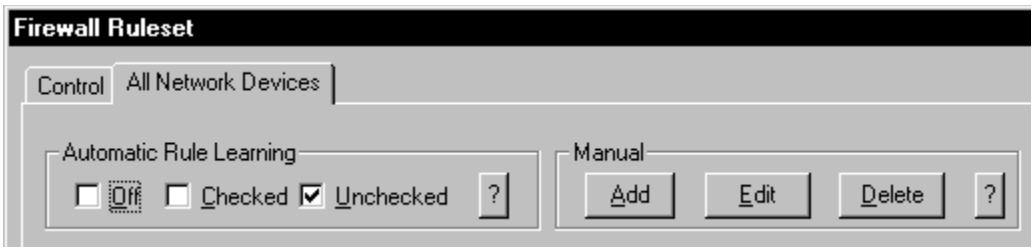
Checked learning mode is a safe and easy way to build your firewall ruleset. No packet is allowed through without being verified.

The firewall starts in this mode and remains so by default. However, you can modify this setting on a per device basis. To change it, select the ruleset page under the Rules menu item and select the Checked mode in the Automatic Learning box. Now, whenever a packet is being sent in or out that does not match a rule in the ruleset, the firewall blocks it and prompts you to add a rule to allow/block it in the future. If you add this as a rule, then that type of packet will be allowed/blocked and gradually your ruleset will grow to filter as you want it to.



Checked Mode Rule Prompt

In Checked learning mode, you are told what type of traffic was trying to get through and you are asked whether to allow, block, ignore or allow or block for this session only. If your ruleset is displayed, you have the option to edit the rule before using it. More information is available by selecting the "Show Details" and "Explain Risks" button.



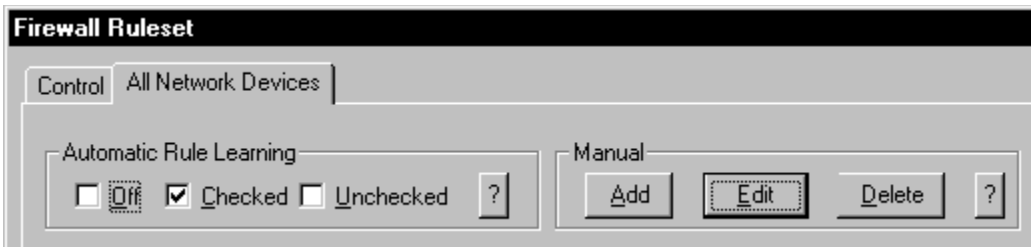
Unchecked Learning Mode

Unchecked learning mode is the easiest and fastest way to build your firewall ruleset. It is safe as long as your system is not attacked while you are in this mode.

To start Unchecked learning mode, set the toggle (a check mark will appear in the box) found in the Automatic Rule Learning box on the device page. Whenever a packet is being sent in or out that does not match a rule in the ruleset, the firewall allows it through and automatically adds a rule to allow it in the future. Once you turn off Unchecked learning mode (by clearing the check mark), you may review the added rules and modify or remove them.

An example of a rule that should be removed is the NetBIOS broadcasts that are done to the Internet (UDP Ports 137 and 138). For reasons of privacy and security, it is recommended that you do not do file shares across the Internet.

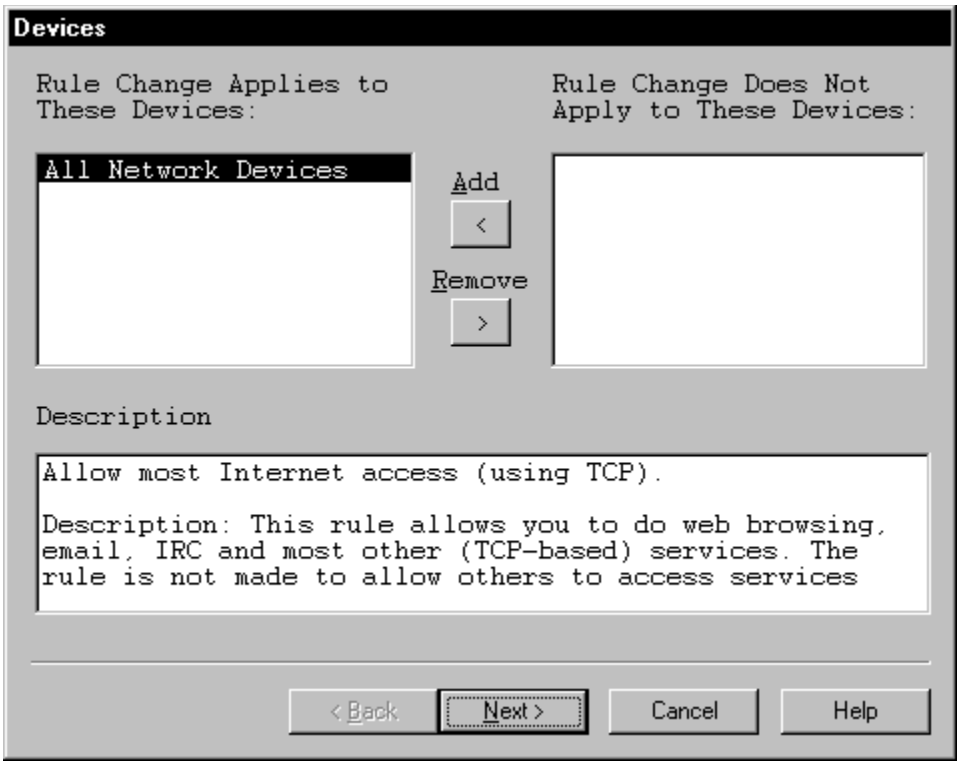
Unchecked learning mode ends when you close the ruleset window, using OK, Cancel or <ESC>. If you do not choose the OK or Apply buttons, the new rules are not added.



Adding and Editing Rules

A convenient edit wizard lets you add new rules or modify existing ones. Each aspect of the firewall rule is presented. Once you are finished the rule is added. Remember you must select the OK button to save the new ruleset permanently.

There are four pages in the edit wizard:
1) Devices - choose the device(s) to which this rule applies. A description is included, which you are free to change. This is to help you understand the purpose of the rule.
2) Filtering - choose what service or protocol is being filtered (when you choose a service, its protocol is set automatically), whether it is to block or allow, direction of traffic (inbound and/or outbound) and the priority to be given to this rule.
3) Addresses and Ports - set the remote and local addresses, masks and ports.
4) Usage - choose when this rule applies. Additionally, you can choose whether you want the firewall to log or warn about packets. There is also an option to log connection attempts (applies to TCP protocols).

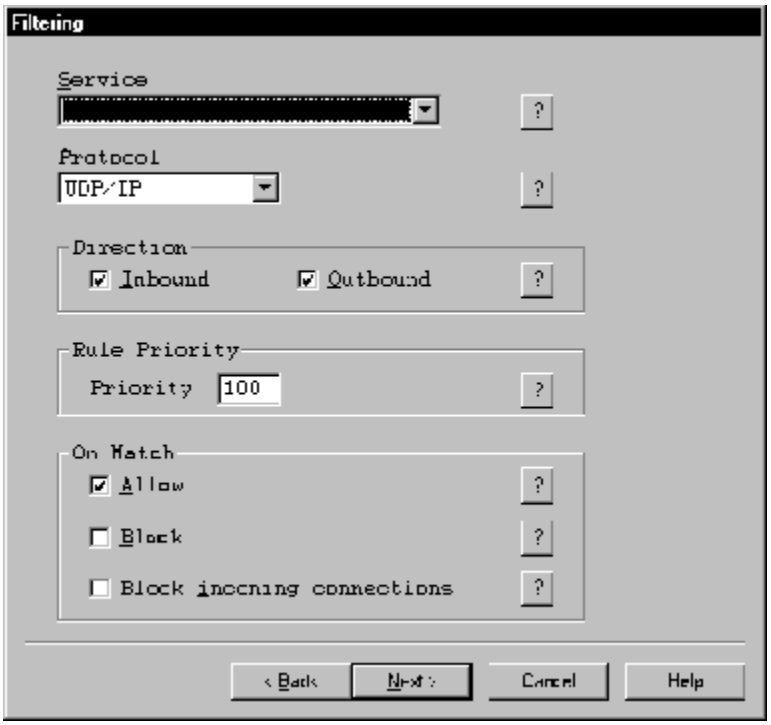


Rule Editing - Device

This page lets you select which of your network devices or modems this rule applies to. If you have selected one ruleset for all devices on the Control Page, then this page does is not automatically shown, because there is nothing to choose. Each device is identified with its device name and unit number, to make it unique. This name corresponds to those shown in the titles or the device pages.

The 'Add' and 'Remove' buttons let you add or remove devices from the list to which the rule applies. The rule applies to devices shown in the list on the left, but does not apply to devices in the list on the right.

A description field is added to describe the purpose of the rule. You are free to write in this comment field. It holds up to 2000 characters.



Rule Editing - Filtering

On this page you select the service or protocol to filter, the direction of data, whether a rule match means block or allow and a priority to be assigned to the rule.

Service - the Service list is a short list of the most common services your system will use. By selecting an item in the list, the protocol is filled in and the port numbers are filled on the Addresses and Ports screen.

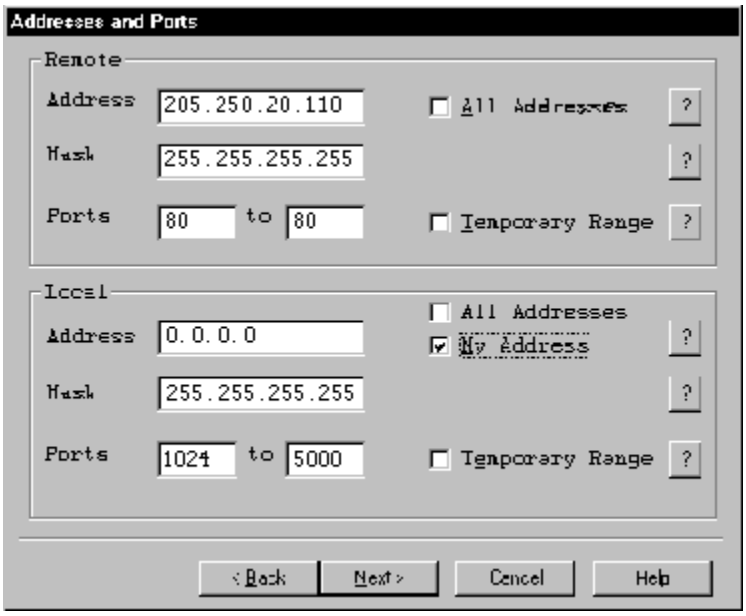
Protocol - the Protocol list contains all the protocols that the ConSeal PC FIREWALL can filter. Any protocol not listed will be classified as "other protocols" in the filtering rules. If you choose an entry in the Service list (above), you don't have to select the protocol.

Direction - in the Direction box, you can select whether the rule applies to inbound or outbound packets or both. In the future, a rule can be set for 'forwarding', which means your system is being used as a gateway between two networks (such as the Internet and your internal network) and the rule is for traffic being forwarded through to and from your network.

Rule Priority - the priority field specifies the order in which rules are checked, and therefore the priority with which they apply (a rule with a lower number is checked before one with a higher number). When rules have the same priority, the order of use is arbitrary (in fact, the order is as shown in the list).

On Match - in the "On Match" box, you specify whether packets matching this rule are to be blocked or allowed. For rules allowing TCP packets, you can choose whether to block incoming connection attempts (when the rule is blocking or when the protocol is not TCP, this

option does not apply and is grayed out). For rules filtering TCP, UDP or ICMP packets, you can choose whether to block incoming fragments (when the rule is blocking, this option does not apply and is grayed out).



Rule Editing - Addresses and Ports

In this page, you specify the network addresses and ports that this rule will filter. Both remote and local addresses and ports are specified. 'Remote' refers to the system your computer is talking to. 'Local' refers to your system.

Address - currently, this is the IP address. To specify all addresses on a subnetwork, set the subnetwork number to 0 and the corresponding part of the mask to 0, e.g. 192.139.46.0 with mask 255.255.255.0 means the rule applies to IP addresses that start with 192.139.46 exactly, but any fourth number will match.

Mask - the mask is a bitwise definition of how the address is to be interpreted. A mask of 255.255.255.255 means the address must match exactly, whereas a mask of 0.0.0.0 means the address can be anything. A mask of 255.255.255.0 means the fourth number can be anything.

Port - the port number is related to the service you are allowing. Typically, when you use a service on a remote machine, such as email or Web browsing, you have a fixed port number on the remote end of the connection and a dynamic number on the local range (here called the Temporary Range), between 1024 and 5000. A list of services is included in the "Rule Editing - Filtering" page.

Rule Editing - IP Addresses

Both a remote and a local address are defined in an IP rule. The address may be an exact IP address or may represent a range.

An exact IP address is the address assigned to a machine. The mask for an exact IP address is 255.255.255.255.

A range of IP addresses may be specified by using the mask field.

ConSeal PC FIREWALL provides an easy way of defining any IP address assigned to your machine: 127.0.0.1 (also called 'localhost'). When this is used, the mask field is unnecessary and is ignored. This representation is useful when specifying your local IP address, because when you connect to the Internet, the IP address you use is likely to be different each time you connect. It also helps a system administrator create one ruleset and copy it to many machines, without change.

Rule Editing - Address Masks

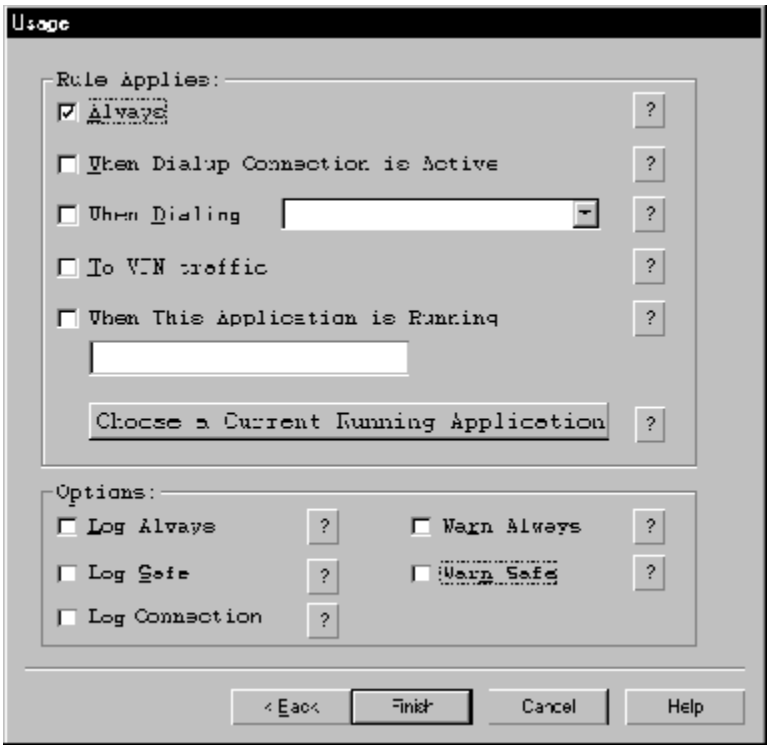
A mask is used to interpret an address. It is a bitwise definition of which bits in the rule's address must match in the corresponding data packet's address. A 1 bit means it must match and a 0 bit means it doesn't have to match. The one exception is when the address 127.0.0.1 is used to represent the local machine's IP address(es). In this case, an exact match is assumed, and the mask is ignored.

An exact IP address should have a mask of 255.255.255.255. This has all bits set to 1.

Allowing any address would be done by using a mask of 0.0.0.0. With all bits in the mask zero, no bits in the address are compared, so anything is a match.

A range of addresses that usually make up a subnetwork is represented by a mask that has 0 bits in the positions of the subnet range. For example, if rule requires a remote address to be in the range of 192.139.46.0 - 192.139.46.255, then the corresponding mask would be 255.255.255.0. The first three 255's require an exact match on the 192, 139 and the 46 parts, and the final 0 means that any fourth number will do.

Any bit pattern is allowed in the mask. You must choose the one that is correct for your rule.



Rule Editing - Usage

In this page, you specify when the rule applies. This gives you precise control over when traffic is allowed. You can also specify how traffic matching the rule is logged and causes warning messages.

Always - this is the default setting, and all that most firewalls offer you. The rule applies as long as ConSeal PC FIREWALL is running. Packets that match the settings in this rule are allowed or blocked, according to the rule's policy.

When Dialup Connection is Active - the rule applies only when you have a RAS connection active. If not, the firewall acts as if the rule does not exist. The rule comes into use when you start a RAS connection, and the rule is removed from use when the connection stops.

When Dialing: - the rule applies only when you have a RAS connection to the specified entry in your default RAS Phone Book. If not, the firewall acts as if the rule does not exist. The rule comes into use when the named RAS connection starts, and the rule is removed from use when the connection stops. This option allows you to have rules that are unique to the different systems you dial in to.

To VPN traffic - the rule applies only to ConSeal PC Virtual Private Network traffic. Unlike other options, this rule does not apply to normal network traffic.

When This Application is Running: - the rule applies only when the named application is running. If not, the firewall acts as if the rule does not exist. The rule comes into use when the

application starts and the rule is removed from use when the application stops. The button labeled "Choose a Currently Running Application" displays the names of the running applications, so you can find the name the system knows them by. This option allows you to have rules that only apply when you are running a particular application. For example you can allow email and WWW access only when your Internet browser is running.

Options
When traffic matches the rule, there are four optional message settings:

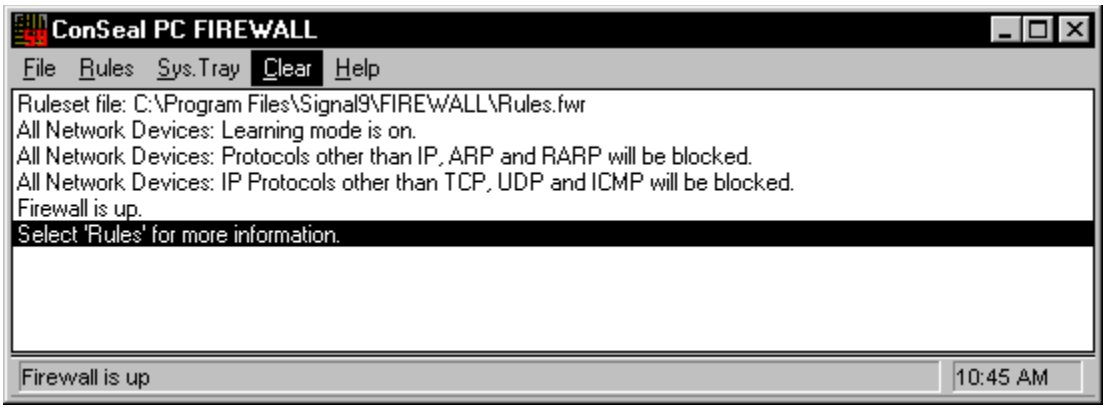
Log Always - this option causes a message to be reported when traffic is blocked by this rule. A log message is written for every data packet blocked. If large amounts of data are blocked, this message logging will affect system performance and 'Log Safe' is a better choice.

Log Safe - this option causes a message to be reported when traffic blocked by this rule, but no more often than once every 2 seconds. This option protects you from a flood of messages created by incoming packets.

Log Connection - this option causes most TCP connection attempts to be recorded in the log file. The message contains the source and destination IP addresses and the source and destination ports. Not all connection attempts are logged because services such as HTTP can send many in a row. A log entry is suppressed when the last connection attempt was between the same two IP addresses and the same (remote) destination port is used (e.g. port 80 when web browsing).

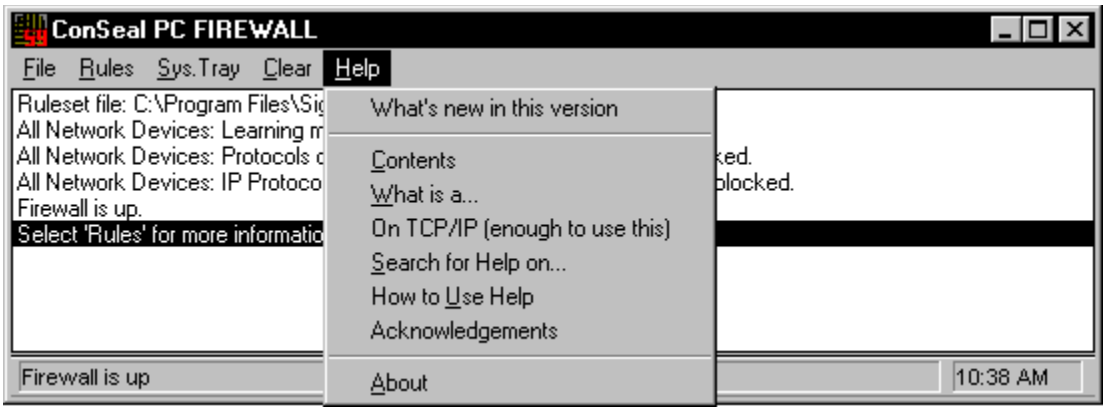
Warn Always - this option causes a message and a warning beep to be generated when traffic matches this rule.

Warn Safe - this option causes a message and a warning beep to be generated when traffic matches this rule, but no more than once every two seconds. This option protects you from a flood of warnings created by a flood of packets.



Clear Menu Item

Choosing this menu item erases all the log messages from the log window. Most log messages are also being written to the log File . Clearing the log window does not cause any messages to be cleared from the log files. It is considered a permanent record.



Help Menu Commands

What's new in this version - New features and improvements in v1.3 (and v1.2).

Contents - displays the contents of the Online Help.

What is a... - provides a comprehensive glossary of terms used by firewalls in general and ConSeal PC FIREWALL in particular.

On TCP/IP (enough to use this) - a simplified explanation of TCP/IP and networking.

Search for Help on.. - displays a list of keywords to search for Online Help topics.

How to Use Help - displays the instructions for using the Online Help facilities.

About - displays product information about **ConSeal PC FIREWALL**.

Product Registration

This product is made available as a 30-day, fully functional trial copy. To use it past the trial period, you must purchase it and complete the registration.

Unlike some shareware, this product stops working after the trial period. You will see messages in the ConSeal PC Firewall window and your log file indicating the trial period has expired. Until you purchase and register the product, the firewall will be 'Down', which means that it will not be blocking anything. By requiring all users to purchase and register, we are able to offer it at an affordable price.

The license allows you to run it on one CPU. The license is not transferrable. If you wish to transfer it to another machine, you will have to re-register. Please visit our web site (www.signal9.com) for instructions on how to re-register.

Product Support

We regret that we cannot provide free support for ConSeal PC FIREWALL. It has been priced to make it affordable for the general public. Pricing it to include telephone support would make the cost prohibitive to many.

There are several options available to you:

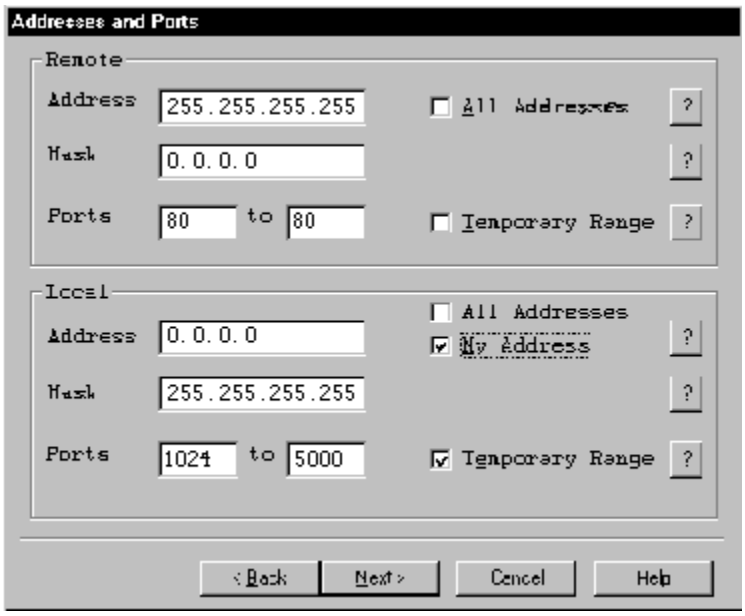
1) Read the online documentation. No kidding. It may take a while, but it contains a lot of information because this is a very technical product.

2) Read the FAQ's (Frequently Asked Questions) posted on our web site: www.signal9.com. The question you have may have been asked and answered.

3) Post your question to a newsgroup, such as comp.security.firewalls or comp.security.misc. Signal 9 technical staff read and contribute to these newsgroups (among others) and will answer your question.

4) Visit Undernet's #firewall chat group. It is dedicated to discussion on this firewall. Signal 9 Solutions usually has a representative in the #firewall channel on Wednesday nights, 8:30 EST. All are welcome to come and ask questions.

5) You can buy technical support from Signal 9 Solutions.



Learning New Rules

ConSeal PC FIREWALL can help you build your ruleset. By default, it reports new types of communication and asks you whether or not to allow it. Five options are given:

1) Allow - this communication is allowed from now on. A rule is added so that the firewall will recognize and allow it.

2) Block - this communication is blocked from now on. A rule is added so that the firewall will recognize and block it.

3) Ignore it - this communication is blocked and you are not prompted again as long as the firewall stays in Checked learning mode. No new rule is added.

4) Allow, this session - this communication is allowed, but only for this session. A "temporary" rule is added so that the firewall will recognize and allow it for this session only. This rule is gone the next time the firewall is run.

5) Block, this session - this communication is blocked, but only for this session. A "temporary" rule is added so that the firewall will recognize and block it for this session only. This rule is gone the next time the firewall is run.

6) Edit - When the Ruleset window is open, you have the option of editing the rule before saving it. This gives you the chance to adjust any of the fields to better suit your purposes.

7) No new rules - clicking on this button stops Checked learning mode for this device. You will not be asked to set any more rules for this device. Any data packets not matching a rule will be blocked and a message will be logged. If you have rulesets for several devices, the learning

mode states for the other devices are not affected. You can return to learning mode by selecting the option in the Firewall Ruleset window.

8) Show Details - detailed information about the attempted communication is displayed. This lets you know what type of communication is being attempted and what the new rule will allow. If a rule is made (allow or block), it can be edited later.

9) Explain Risks - ConSeal PC FIREWALL attempts to explain what type of communication is being attempted and presents to you the effect of allowing or blocking it. Sometimes a recommended path is given to you, although this must be considered in light of your own security policies.

10) Help - displays this help page.

Enough about TCP/IP to get by

This is a simplified explanation of TCP/IP and networking for those whose only interest is using ConSeal PC FIREWALL. It will help you understand the following terms:

Internet, Computer System, TCP/IP, UDP, ARP, Port, Address, Connection, Firewall.

These terms can be easily understood by analogy. If you are familiar with telephone systems, think of the Internet as compared to the world-wide telephone network. Here are analogies for the other terms:

Computer System	A hotel (with phones for staff and guests)
TCP/IP	A person-to-person call
UDP	Voice mail (leaving a message)
Port	A telephone extension number
Address	The telephone number of the hotel
Connection	A telephone call
Firewall	The hotel telephone operator
ARP	Finding a street address

The hotel telephone system is analogous because your computer plays host to the applications you run. Setting up the firewall will be like telling the hotel operator how s/he is allowed to let calls and messages get through. You, the computer user, are both 'hotel manager' and 'VIP guest'.

Concept 1: Applications and Services
Hotels have guests and hire staff that serve the guests.

Firewall: Computers have applications (e.g. email, web browsers) and use operating system services (e.g. DNS, RIP, Identification) to support these applications.

Concept 2: Communication
A person in the hotel wants to phone out. They are calling from a phone with an extension number to another person in a different hotel, also with a phone and an extension number.

Firewall: An application or service in your computer wants to communicate with another application or service on another system. With TCP/IP and UDP/IP, communication uses IP addresses of the computers and port numbers.

Concept 3: Without a Firewall

Without an operator, anyone may call in or out. There may be nobody at that extension. Alternately, the person may or may not answer their phone.

Firewall: Without a firewall, communications are freely attempted, in or out. Not all ports have services using them. Alternately, an application/service may or may not accept a connection attempt.

Concept 4: Role of a Firewall
When the operator is working, s/he decides which extensions may make calls and which other hotel and extension they may call.

Firewall: When the firewall is running, it decides what systems may communicate and what port numbers may be used.

Concept 5: Other PC-based Firewalls
Older operators cannot block calls to some of the key hotel staff, such as the accountant. Your hotel has an operator that can screen all calls.

Firewall: Other PC-based firewalls that are Winsock-based cannot block connections to some key Windows services such as file shares. ConSeal PC FIREWALL intercepts all data packets, including fileshares.

Concept 6: Other Protocols (IPX, NetBEUI, etc.)
Older operators don't know that hotels can have fax machines or Morse Code, and can't screen them at all. Your hotel has an operator that knows the hotel can have fax machines, Morse code, etc. Soon the operator will be taught how to screen them, but for now you tell the operator whether these other media should be allowed or blocked (they are blocked by default).

Firewall: Other PC-based firewalls don't intercept data packets of other protocols such as IPX or NetBEUI, and can't screen them at all. ConSeal PC FIREWALL intercepts all data packets of these protocols. In the future, ConSeal PC FIREWALL will be able to screen these protocols, but for now, you can choose whether to allow or block them (they are blocked by default, see the Advanced button on the ruleset page).

Concept 7: Blocking Incoming TCP/IP Connections
An operator can block an incoming telephone call to a person while allowing that person to make outgoing calls.

Firewall: A firewall can block incoming connection attempts on any particular TCP/IP port while allowing the same port to be used for outgoing connections.

Concept 8: This Firewall is a "Packet Filter"
The operator can block a call, but s/he does not censor what is said. A security guard or chaperon might help.

Firewall: A (packet filter) firewall can block communication but does not inspect the contents of the data packets. Anti-virus software or NetNanny might help.

Concept 9: TCP/IP compared to UDP/IP
Some people always make "person-to-person" calls and others leave a message. When you leave a message you are never quite sure that the other person got it.

Firewall: Applications either use TCP/IP to make a connection or they use UDP/IP to send a single "datagram". With UDP/IP, you are never quite sure that the other application got it.

Concept 10: Blocking UDP/IP Data
If the operator is instructed to allow a guest to leave messages for another person, (in another hotel), then the operator will also allow that other person to leave a message for the guest.

Firewall: If ConSeal PC FIREWALL has a rule to allow applications/service to send UDP/IP to another system(s) on certain ports, that other system(s) may send to you using the same ports. The reason is that it is not clear when a system is replying to you and when it is taking the initiative.

Concept 11: How Ports are Used (1)
The white courtesy phone in the lobby is available for all guests to make outgoing calls. Typically, hotel staff can be reached at extensions 1 to 1023. Courtesy phones have extensions 1024 to 5000. This way, guests don't tie up extensions assigned to hotel services (room service, front desk, etc.).

Firewall: A range of (local) ports is available for applications that communicate with services on other systems. Typically, services are available on ports 1 to 1023. Ports for temporary use range from 1024 to 5000. This way, applications/services don't tie up a port assigned to your system's services (file shares, identification, etc.).

Concept 12: How Ports are Used (2)
A convention in the hotel business is that the Lounge is at ext. 80, the Concierge is at ext. 53, a Bellman is at ext. 23, etc. This way, guests know how to reach staff in other hotels. Guests are kindly requested not to use the staff's extensions for personal calls.

Firewall: A convention in the TCP/IP and UDP/IP protocols in that particular services are available at particular ports, e.g. Web servers are at port 80, DNS is at 53, telnet is at 23, etc. This way, your applications know how to reach services on other systems. Applications should not to use these extensions inappropriately (as stated in Concept 11, applications usually access services in the range 1 to 1023 and use a local port from 1024 to 5000).

Concept 13: Rule Usage
This hotel has an operator that can be instructed to allow certain calls through only under certain circumstances, such as 1) only when a certain guest is in the hotel, 2) when cell phones are in use, 3) when the call is going through the hotel's secure phone lines, etc.

Firewall: With ConSeal PC FIREWALL, you can make a rule that allows certain communications only under certain circumstances, such as 1) when a certain application is running, 2) when a dialup connection is active, 3) when communication is through a ConSeal PC VPN (Virtual Private Network) connection, etc.

Concept 14: Priority of Rules
Some instructions for the operator are more important than others. By assigning a priority to each one, you control the order in which the operator reads and applies the instructions.

Firewall: Some rules take precedence over others. By setting the priority (default: 100), you can control the order in which rules are used and applied. Lower numbers assign a higher priority and are checked first.

Concept 15: Total Paranoia and Info Wargames:
This hotel is on the same block as some others. One peculiar detail is that you can't make any call to another hotel without knowing its street address. Today's hotel staff forget easily, so they keep asking each other their address every few minutes. If the operator stops the hotel staff from exchanging street addresses, people won't talk at all.

Firewall: Your computer is on the same network as some others. One peculiar detail is that you can't communicate with another computer without knowing it's Ethernet Address (this is done through ARP). Your computer drops that information if it is not constantly used, so it keeps asking others for their Ethernet Address every few minutes. If you block ARP, the systems won't talk at all. (Strangely, ARP applies to dialup in a rather rhetorical form).

<u>The following concepts have to do with security, which is the whole reason you need a firewall. You will need to understand the hotel analogy (above) before reading this.</u>

Concept 16: IRC Chat and Nuking
Guests who chat on the phone tend to invite harassing interruptions from guests at other hotels. These guests tell your hotel front desk to hang up. Blindly, front desk does it. Without an operator to block this, the guests at the Gates Motel get really annoyed.

Firewall: People who use chatgroups (IRC) tend to invite harassing interference from other malicious chatters. These 'lamers' send 'ICMP nukes' and other datagrams to tell your system that it can no longer reach the chat server. Without ConSeal PC FIREWALL to block this, IRC chat on Windows systems can be really annoying (currently, no other desktop firewall can block ICMP).

Concept 17: Eavesdropping
Even though your hotel staff and guests are calling a person in another hotel, hotels talk on a party line so other people in other hotels can listen to the call.

Firewall: Even though your system is communicating with another computer, it is travelling on a shared network so other computers can access the information that is sent.

Concept 18: Authentication
People in the Listen Inn could claim to be in the Share-It Inn and fool your operator into letting a call go through. It is up to the guests to identify the caller, or to insist on a secure phone line.

Firewall: Computers can alter their IP address and pretend to be another (trusted system) and fool a firewall. It is up to applications to authenticate the remote system, or to use a VPN connection.

Concept 19: TCP connection hijacking
It's possible for a caller at the Listen Inn to intercept a call from the Share-It Inn, hang up the person at the Share-It Inn and pretend to be them. Without a secure phone line, your people would never know.

Firewall: It's possible for a hacker to intercept a TCP connection you have, tell the other system the connection has closed, then pretend to be them. Without a secure connection (e.g. VPN), your system would never know.

Concept 20: DNS Spoofing
If a guest at the Listen Inn could pretend to be Directory Assistance (411), they could supply incorrect phone numbers and make you talk to the wrong hotel.

Firewall: If a hacker can interfere with DNS (Domain Name Service), they can supply you with incorrect IP address and make your system talk to the wrong computers.

Concept 21: Altering of Data
If a guest at the Listen Inn can intercept your phone call, they can alter what is said. A secure phone line solves this problem.

Firewall: If a hacker can intercept your communication, they can alter the data. A VPN connection solves this problem.

Concept 22: Intercepting Data (1)
One amazing aspect of the hotel telephone system is that phone calls get passed from hotel to hotel until they reach the final destinations. That means a lot of people can listen to your call: watch what you say, or use a secure line.

Firewall: One amazing aspect of the Internet is that data is passed from computer to computer until it reaches the final destinations. That means a lot of people can see your data: watch what you send, or use a VPN link.

Concept 23: Intercepting Data (2)
Some links between hotels are broadcast over a microwave link.

Firewall: Some phone calls are routed through microwave relays and cell phones broadcast to the nearest tower. This makes the data more accessible.

Concept 24: Network Security
Guests at the Mac Inn Lodge wake up refreshed, knowing that their operator has earned an excellent reputation. As a guest of the Gates Motel, you can rest easier knowing that you have brought in an operator to screen your calls.

Firewall: Mac's have earned an excellent reputation in network security. As a Windows user, you can rest easier knowing that ConSeal PC FIREWALL is protecting your network connections.

Glossary

Address
Address Mask
Administrator
Allow/Block
All Addresses
ARP
Authentication
Broadcast
Button
cc:mail
Cookie
Connection
Connection Attempt
ConSeal
Default
Dialog Box
DNS
Email
Ethernet
Fileshare
Filter
finger
Firewall
FTP
Gopher
Hacker
HTTP
HTTPS
Identification
Incoming Connection
ICMP
ICQ
inbound packet
IP
IPX
IRC
ISP
Learning Mode
Local
Log File
match
Menu
Message Box
Modem
NetBEUI
NetBIOS
Netware-IP
Network
Network Device
News (NNTP)
NeWS
NNTP
ntp
Operating System
Options
outbound packet
Packet
Packet Filter
Password
Phone Book
ping
POP2
POP3
Port
Printshare
Priority
Protocol
RARP
RAS
Reference Number
Remote
RIP
Rule
Ruleset
Running Application
Service
SMTP
snmp
TCP
tcpmux
Telnet
Temporary Range
tftp
Toggle
Tunnnel
UDP
VPN
WINS
Winsock
Wizard

Address - a data field in a packet header that specifies either the sender or the intended receiver of the packet. Note that computers can often see data packets that are not intended for them.

Address Mask - a value that describes how to interpret an address. Masks are often used to help identify a range of addresses.

Administrator - the person responsible for computer configurations and support.

Allow/Block (rules) - the action to take on a packet if it matches a rule. Block means the packet is not sent/received. Allow means it is sent/received.

All Addresses (rules) - a value for an address field that means any address is a match.

ARP - Address Resolution Protocol, an Ethernet protocol for matching IP addresses to Ethernet addresses.ARP is an essential tool for telling your system how to reach other computers. If you block it, you will not be able to reach other systems for any service. Likewise, they will not be able to reach you, nor will they know you are on the network. Don't, however, rely on ARP alone to protect you. It is just one step.

Recommendation: Allow from all addresses to all addresses, unless you are in a particularly insecure environment, then allow to and from systems or subnets that you do trust.

Authentication - the property of knowing that a person or system is who they say they are. This can be achieved by Virtual Private Networks.

Broadcast (networks) - a message that is addressed to all computers on a specified subnetwork.

Button - an item on a window that causes an action to be performed when it is "pressed", (usually by clicking the mouse button when the cursor is on it).

cc:mail - an email system by Lotus. Uses TCP port 3264.

Connection - a method of data exchange that allows a reliable transfer of data between two computers.

Connection Attempt - the data transfer that requests the opening of a connection. Firewalls often block incoming connection attempts, since it is usually your local machine that should be making them. FTP is an exception. In active mode, the remote machine will make a connection attempt in order to send a file. In passive mode, only your machine makes connection attempts.

ConSeal - the name of Signal 9's suite of network security products. Many products call themselves "VPN's" or "firewalls", but when you compare features, performance, price and service, ConSeal wins. ConSeal is a trademark of Signal 9 Solutions Inc.

Cookie - a file placed on your hard drive by a web site you visit. The original intent was for cookies to contain information about your preferences about you, so they can tailor the appearance to your wants. They can also save you time when you next visit the site.

The security risk with cookies is that since they are written directly to the hard drive, they can store something dangerous (viruses) or private (a password). There is also concern that one website can get a cookie created by another website. It appears that cookies cannot be used to get other data from a user's hard drive (such as, applications used, database, address book, personal files, etc.). Cookies can, on the other hand, be used to track where a user has been within a web site.

Netscape Navigator can be set to ask you whether or not you will accept a cookie.

Default (rulesets) - the action to be taken when no rule in the ruleset is matched.

Dialog Box - a window used to help the user enter information.

DNS - Domain Name Service, a service for mapping computer names to their IP addresses.
DNS usually uses UDP port 53, but may use TCP.

If you don't allow DNS, you won't be able to reach any system by name.

Email - electronic mail, a method of sending messages to other people via computer networks.

Ethernet - the most common type of local area network (LAN).

Fileshare - a file system resource available through a network connection. Uses UDP ports 137 and 138 and TCP port 139.

Your system uses UDP broadcasts to announce its presence on a network and listens to see who is out there. This is alright in a trusted office environment, but is completely inappropriate for an Internet connection.

Allow inbound if you want to receive broadcasts and see people in your 'Network Neighborhood'. Block outbound to the Internet. If it is not allowed to internal networks, you will not see or be seen in 'Network Neighborhood'.

The Operating Systems provides some protection for this type of access, so you should learn about it and use it. If you block TCP port 139, no fileshares are allowed.

Recommendation: Block during dialup connections. File and printshares during Internet access is not a good idea. When allowed, block incoming connections unless you want to share your system resources. Allow outgoing connections if you want to share another system's resources.

Filter (firewalls) - a tool used to intercept all incoming and outgoing network traffic and block all that is unwanted.

Finger - a service that finds information about a user. It uses port 79.

Recommendation: Allow inbound if your system runs a finger daemon (probably doesn't). Allow outbound if you need it.

Firewall - a service that controls the transfer of data between a computer or network and the surrounding network(s). The firewall is responsible for filtering all packets and often provides proxy services to protect internal computers.

When the ConSeal PC FIREWALL was introduced on Sept. 2, 1997, we knew of no other PC-based firewall that could protect your fileshares or ICMP nukes. For more information on how ConSeal PC FIREWALL and other ConSeal security products surpass the competition, see www.signal9.com or call us at (613) 599-9010.

FTP - File Transfer Protocol, a high-level protocol for file transfer. FTP uses TCP/IP, ports 20-21.

Providing ftp as a service invites hacking attempts. Use the security of your Operating System to control access (e.g. usernames, passwords, file access control). In the firewall, decide if you can filter by remote IP and allow only to the local IP address of your ftp server.

Recommendation: Block inbound connection attempts unless you have an ftp server. If you are accessing an ftp server, try to use passive mode.

Ftp is generally safe when you are the client. The risk is mainly related to the files you tranfer: they may have viruses. The risk with 'active' ftp is that you are allowing another system to initiate TCP connections to you and it is not explicitely within your control. 'Passive mode' ftp does not do this, which means you can block incoming ftp connection attempts.

Recommendation: Allow ftp if you use it. Use passive mode (block incoming connections). Check all files for viruses.

Gopher - a program used to access information that is often widely spread across the Internet. It uses port 70.

Recommendation: Allow if you need it.

Hacker - a person who misuses computer resources, often finding or damaging information.

HTTP - Hypertext Transfer Protocol, a powerful tool used primarily for browsing the World Wide Web. It uses TCP port 80. Web sites often want to send you cookies, which can be sent by different channels.

Recommendation: If you block it, you won't be able to 'web surf'. Allow, but check files for viruses. Understand and use the security features in your web browser. Use Java with caution and don't use ActiveX.

HTTPS - Secure HTTP. This is a variation of HTTP that uses encryption to add privacy. It uses TCP port 443.

ICMP - Internet Control Message Protocol, a maintenance protocol that handles error messages and helps network debugging (see ping). ICMP is carried in IP packets.

ICMP is easily abused and has become a serious annoyance to IRC Chatgroup users. Because other people can find out information about you, such as your IP address, they can easily send false ICMP messages to your system which promptly drops your IRC connection. ConSeal PC FIREWALL is currently the only firewall to block ICMP to your Windows computer.

ICMP Types are:

0 - Echo Reply (ping reply)
3 - Destination Unreachable (the most abused)
4 - Source Quench
5 - Redirect
8 - Echo Request (ping request)
9 - Router Advertisement
10 - Router Solicitation
11 - Time Exceeded (used by Traceroute)
12 - Parameter Problem
13 - Timestamp Request
14 - Timestamp Reply
15 - Information Request
16 - Information Reply
17 - Address Mask Request
18 - Address Mask Reply

Recommendation: Block ICMP incoming type 3 (destination unreachable).

ICQ - an Internet service that helps people find each other and share information. Uses UDP port 4000. ICQ is made difficult for firewalls to filter because it uses a UDP port in the temporary range. Information can be faked.

Recommendation: Allow if you use ICQ, but remember that the information you receive could be sent falsely by a third party.

Identification - a service that provides user information to another system, so they can try to verify your identity. If you block it, other systems may refuse you their services, such as email. Uses TCP port 113.

Incoming Connection - a connection established by a remote computer to you. This is easily identifiable in the TCP protocol.

inbound packet - a packet arriving from a remote computer or network.

IP - the essential network protocol of the Internet. It supports TCP, UDP, ICMP and many others. ConSeal PC FIREWALL filters TCP, UDP and ICMP, and the Advanced button on the Ruleset page can be used to allow or block other protocols.

IP Spoofing - altering the source address in an IP header so the packet appears to have come from a different (trusted) system. Doing this leads to many forms of attack (which can be prevented with authentication).

IPX - a network protocol, most commonly used by Novell. It supports SPX. Also, it can be tunneled over IP.

ConSeal PC FIREWALL can block IPX and other non-IP protocols. See the Advanced button on the Ruleset page to allow or block other protocols, collectively.

IRC - Internet Relay Chat. A service that lets people on the Internet share a typed conversation. Whatever a person typed is sent to other people in the "chat group". IRC usually use TCP ports in the range 6660-6669.

The biggest risk here is that people might become hostile and try to 'nuke' you or send you unpleasant email. Consider NetNanny to screen the messages that are sent in IRC.

Recommendation: Allow inbound connections only if you are running an IRC server. Allow outbound if you use IRC, but block incoming ICMP.

ISP - Internet Service Provider, the company that sells you access to the Internet.

Learning Mode (firewalls) - a setting where the firewall helps the user build new rules for the ruleset.

Local (Address or Port) - refers to your machine, as opposed to a remote machine.

Log File - a record kept by the firewall to track activity. The log file helps monitor breakin attempts. An entry might look like this:

Dial-Up Adapter [0000][Ref# 4] Blocking incoming TCP: src=154.11.111.155, dst=192.134.5.124, sport=1029, dport=139.

This log message reports:
- the device name on which traffic was intercepted,
- the device unit number [0000],
- the firewall rule has Reference Number 4,
- incoming TCP traffic was blocked,
- the (remote) source IP address was 154.11.111.155,
- the (local) destination IP address was 192.134.5.124 (this is probably your dynamically assigned IP address),
- the (remote) source port number was 1029,
- the (local) destination port number was 139 (NetBIOS: fileshares)

match (firewall rules) - a packet matches a rule when the values in its data fields are within the range specified by the rule. Typical packet fields specified in a rule are protocol, address and port number.

Menu - a list of commands that are available. If a command is in gray, it is not available.

Message Box - a message window that appears to briefly tell the user information.

Modem - device that carries a data signal, typically over a telephone or ISDN line.

NetBEUI - NetBIOS Extended User Interface. A local-area protocol that operates underneath the NetBIOS interface.

ConSeal PC FIREWALL does not currently filter NetBEUI. If you allow it through, it will be unchecked. If you block it, applications that rely on it will not be able to communicate.

Recommendation: Block unless you need it. See the Advanced button on the Ruleset page to allow or block these other protocols collectively.

NetBIOS - a protocol that supports file and print shares. This protocol can be carried over TCP and UDP or IPX.

If you block NetBIOS, you will not be able to share system resources such as file and printshares. We recommend that you block NetBIOS (UDP ports 137-138, TCP port 139) when connected to the Internet.

Netware-IP - Netware protocol sent using the IP protocol. Port 396 is assigned to it.

The Netware protocol is not currently filtered by ConSeal PC FIREWALL. You can either allow or block Netware-IP altogether.

Network - a channel used to support communication between computers, e.g. Ethernet or Internet.

Network Device - a hardware computer component that connects your computer to a network, such as Ethernet or Internet

News (NNTP) - a service available through most ISP's where thousands of newsgroups discuss specific topics, and users may post relevant articles. The most prominent risk is that if you post using your real email address, you WILL receive an unending stream of 'spam' (junk email). Uses TCP port 119.

Recommendation: Allow inbound connections only if you are running a news server. Allow to your news server. If you block it, you won't be able to access news. Corrupt your email address before posting. The news server may require authentication before allowing you access.

NeWS - Network Window System. Uses port 144.

This probably doesn't apply to you.

Recommendation: Leave it blocked.

ntp - Network Time Protocol, a service that supplies the time. Uses port 123.

This is a risk is if your system has time-sensitive services or applications and it uses the time that is supplied.

Recommendation: Leaved it blocked unless you need it.

Operating System - the low-level program that supports the running of all other programs on a computer. OS/2, Windows 95 and UNIX are Operating Systems.

Options - information and settings of a firewall rule:

* - this is a 'new' rule that has never been edited by the user

B - block incoming connection attempts

F - block incoming fragments

L - write a log message when traffic matches this rule

l - write a log message when traffic matches this rule, no more than once every 2 seconds (useful against flooding attacks)

C - log connection attempts

W - warn the user when traffic matches this rule

w - warn the user when traffic matches this rule no more than once every 2 seconds (useful against flooding attacks)

T - temporary rule used in this session only (gone the next time you run the firewall)

outbound packet - a packet leaving your computer or network to a remote destination.

Packet - a block of data sent over a communication medium, such as the Internet.

Packet Filter - a function of a firewall that checks incoming or outgoing packets, and allows or blocks them, depending on the rules in the ruleset.

Password - a secret character sequence used for authentication. ConSeal PC FIREWALL supports password control over changes to a ruleset.

Phone Book - a set of dial-up services available on your system (look on your system for Dial-Up Networking).

ping - an ICMP-based service used to verify the availability of computers on a network.

POP2 - Post Office Protocol, version 2. Used to transfer email. Uses TCP port 109.

This is an older version of an email service. It is not considered a risk for PCs. Risks related to email are the spreading of viruses in files that are attached, and 'spam', the junk-mail of the Internet. Use a virus checker on all files (programs and documents) you receive. For spam, there are spam filters, but the real solutions is to get your ISP to reject the email and not deliver it to you.

Recommendation: Allow inbound connections only if you are running a POP2 mail server. Allow outbound to your POP2 mail server.

POP3 - Post Office Protocol, version 3. Used to transfer email. Uses TCP port 110.

This is one of the most popular email services. It is not considered a risk for PCs. Risks related to email are the spreading of viruses in files that are attached, and 'spam', the junk-mail of the Internet. Use a virus checker on all files (programs and documents) you receive. For spam, there are spam filters, but the real solutions is to get your ISP to reject the email and not deliver it to you.

Recommendation: Allow inbound connections only if you are running a POP3 mail server. Allow outbound to your POP3 mail server.

Port - a number used to identify a communication instance.

Printshare - a printer resource available through a network connection. Uses TCP port 139.

The Operating Systems provides some protection for this type of access, so you should learn about it and use it. If you block it, no printshares are allowed.

Recommendation: Block during dialup connections. File and printshares during Internet access is not a good idea. When allowed, block incoming connections unless you want to share your system resources. Allow outgoing connections if you want to share another system's resources.

Priority - a part of the firewall rule that sets the order of use. A rule with a lower number is checked before rules with higher numbers. This way, one rule can take precedence over another. When rules have the same priority, the order of use should be considered arbitrary.

Protocol - a standardized method of communication, e.g. IP

Two main types of protocols are connectionless and connection-based. A connectionless (or datagram-oriented) protocol sends packets without a method of checking that it was received. Packets may get lost during transit. Examples of connectionless protocols are IP, UDP and IPX.

A connection-based protocol provides a mechanism for reliable delivery. Correctly received packets are acknowledged and lost or corrupted packets will be resent. Examples of connection-based protcols are TCP and SPX.

RARP - Reverse Address Resolution Protocol, an Ethernet protocol used to resolve IP addresses.

RARP typically doesn't apply to Windows computers. It is more for network computers and devices that are booted over the network. If you block RARP, your system won't be able to reach others using any other protocol except broadcasts.

Recommendation: Don't make any rule for RARP (which will leave it blocked) unless you need it, then allow.

RAS - Remote Access Service, a service that supports dialup connections.

Reference Number - a ID number for a firewall rule. This number is reported in message logs to tell the user which rule caused data to be blocked, e.g.

Dial-Up Adapter [0000][Ref# 4] Blocking incoming TCP: src=154.11.111.155, dst=192.134.5.124, sport=1029, dport=139.

This log message reports:
- the device name on which traffic was intercepted,
- the device unit number [0000],
- the firewall rule has Reference Number 4,
- incoming TCP traffic was blocked,
- the (remote) source IP address was 154.11.111.155,
- the (local) destination IP address was 192.134.5.124 (this is probably your dynamically assigned IP address),
- the (remote) source port number was 1029,
- the (local) destination port number was 139 (NetBIOS: fileshares)

Messages that refer to 'Ref #0' have a special meaning. They are reported when a packet did not match any rule and was blocked by default.

Remote (Address or Port) - refers to another machine you might communicate with, as opposed to your (local) machine.

RIP - Routing Information Protocol, a UDP-based protocol used to send routing information to systems on a network. Uses UDP port 520.

One danger with RIP is if the information is falsified, it could interfere with your connections.

Recommendation: Block inbound unless it makes systems unreachable. Allow outbound, but don't abuse it.

Ruleset (firewalls) - a set of rules that, together, describe how to filter all packets.

Rule (firewalls) - a set of parameters that define a type of data packet to look for, and what to do when it is found, e.g. allow it or block it.

Running Application - an application, such as a web browser or word processor, that is currently running.

Service - an application or function often considered part of the operating system.

SMTP - Simple Mail Transfer Protocol. Uses TCP/IP port 25.

This is one of the most popular email services. It is not considered a risk for PCs. Risks related to email are the spreading of viruses in files that are attached, and 'spam', the junk-mail of the Internet. Use a virus checker on all files (programs and documents) you receive. For spam, there are spam filters, but the real solutions is to get your ISP to reject the email and not deliver it to you.

Recommendation: Allow inbound connections only if you are running an SMTP mail server. Allow outbound to your SMTP mail server.

snmp - Simple Network Management Protocol. A protocol used to manage networks and routing. This should not be a concern to PC users. Uses UDP port 161.

Recommendation: Block.

tcpmux - TCP Port Service Multiplexer (uses port 1), rare for PCs if ever.

This service is risky because it can randomly assign ports to applications. This means you might be required to allow all ports on your system, thus leaving yourself unprotected.

Recommendation: Block or ask an expert on how to allow it.

TCP - a connection-based Internet protocol carried in IP packets. Examples of TCP-based applications and services are FTP, web browsing, email, and IRC.

Telnet - a TCP-based service that supports remote logins (usually to UNIX systems). Telnet uses port 23.

One risk with telnet is that you are sending your username and password over a network and they may be stolen by someone and used to break in.

Recommendation: Allow if needed, but consider a VPN for privacy.

Temporary Range - the local port range that applications use for TCP- or UDP-based services. Also called the "ephemeral ports". Applications such as ICQ (UDP port 4000) are more difficult for firewalls to filter because they use a port within this range.

Recommendation: treat with suspicion the information from UDP-based applications that are available in the "ephemeral" range.

tftp - trivial file transfer protocol, a UDP-based file transfer protocol, using port 69. tftp is a security risk because it involves no interaction with the user - it can occur without you knowing about it

Recommendation: Block.

Toggle - a setting that switches between two positions or values.

Tunnel - encapsulating one protocol or data stream within another. A Virtual Private Network (VPN) tunnels data by encrypting it and then encapsulating it within a protocol such as TCP (better) or UDP (worse).

UDP - a connectionless (datagram) Internet protocol carried in IP packets. It is harder for a firewall to block UDP-based attacks than it is to block TCP-based attacks. Examples of services and applications that use UDP are ICQ, DNS, RIP, NetBIOS (for broadcasts etc.), RIP.

VPN - Virtual Private Network. A secure private connection, usually through an untrusted network. You can link the LAN's of two offices through the Internet using a VPN, and systems in either office can access those in the other, as if they were on the same LAN. The route through the Internet is invisible. Hackers or snoopers on the Internet just see encrypted traffic and cannot get your private information.

Another configuration of a VPN is "client/server", where computers, such as laptop PCs connect to a VPN server which gives access to a protected network. Home or mobile workers can connect to the office and have the same secure link and can access office systems.

Here at Signal 9, we have connected a PC to the Internet, started a VPN link to the office network, and then used the PC to get an office computer to send a fax. The PC could be anywhere in the world, and it sent a fax local to the office.

To learn how Signal 9's ConSeal VPN product line beats the others, look at www.signal9.com or contact us at (613) 599-9010.

WINS - Windows Internet Name Service, a protocol similar to DNS. Uses port 1512.

If your system is configured to use WINS, then blocking it will result in you not being able to contact other systems.

Recommendation: Allow to your WINS servers only.

Winsock - a part of the Windows operating systems that handles most network connections (it does not handle file or printshares) or ICMP.

Wizard - a tool that helps you use an application.

WWW - World Wide Web, a graphical medium for accessing the Internet. Uses HTTP.