Global Information Assurance Certification Paper

Protecting Yourself with Norton Personal Firewall

Mark Greco
Version 1.2b

Introduction

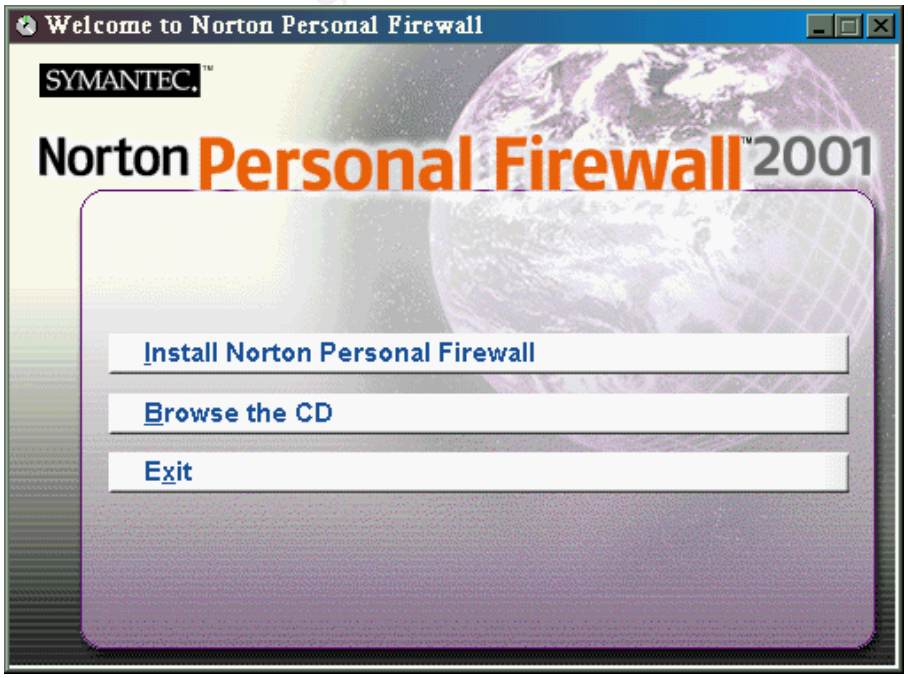
With the boom of the Internet, protection of your PC and the information that it contains has become more and more crucial. Now that personal home users have a full time presence on the Internet with DSL and Cable Modems they too have to worry about protection like the corporations do.

The corporations also have something new to worry about as home user full time connections increase. Those home users are going to want to connect to the office network so they can work from home and spend more time with their families. Without protection and these home users considered a part of the network when their connected to it that's a lot of security holes to worry about. The road warrior connections are also on the rise and those dial-up connections also need to be protected as well.

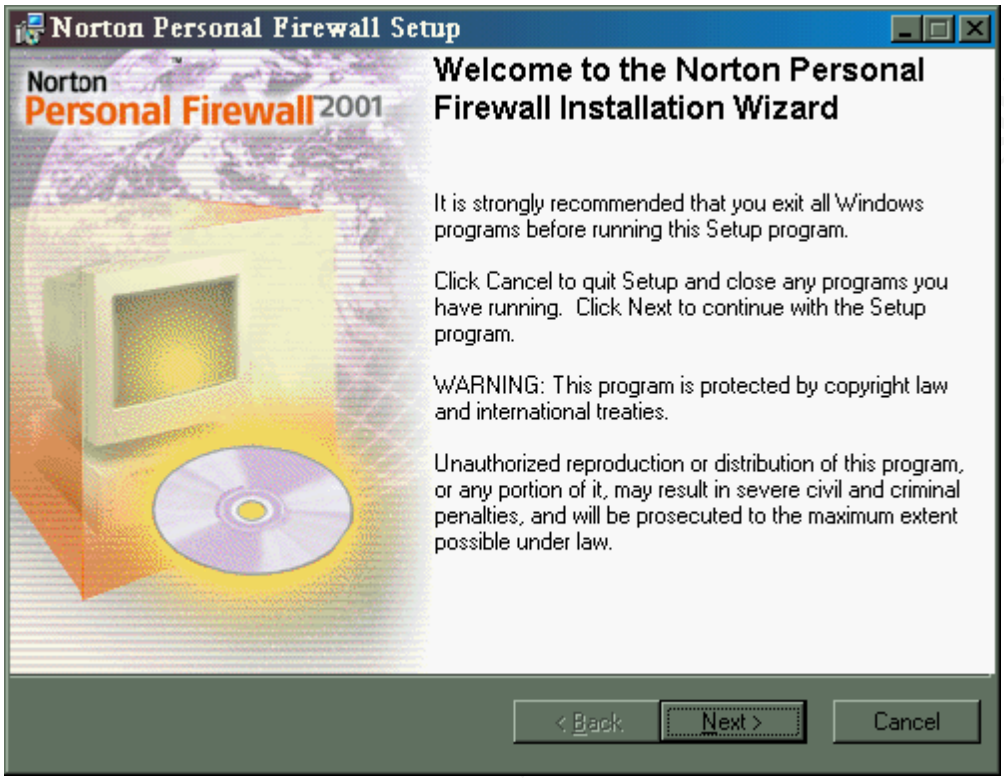
There are many firewalls on the market that can help the home user protect their system and give their system administrators peace of mind. Mcafee's "GuardDog," Zone Labs' "ZoneAlarm," NetworkICE "BlackICE Defender" and Symantec's "Norton Personal Firewall" to name a few. This paper will cover Norton Personal Firewall 2001. I will discuss installation, configuration, and issues that may arise supporting this product.

Installation

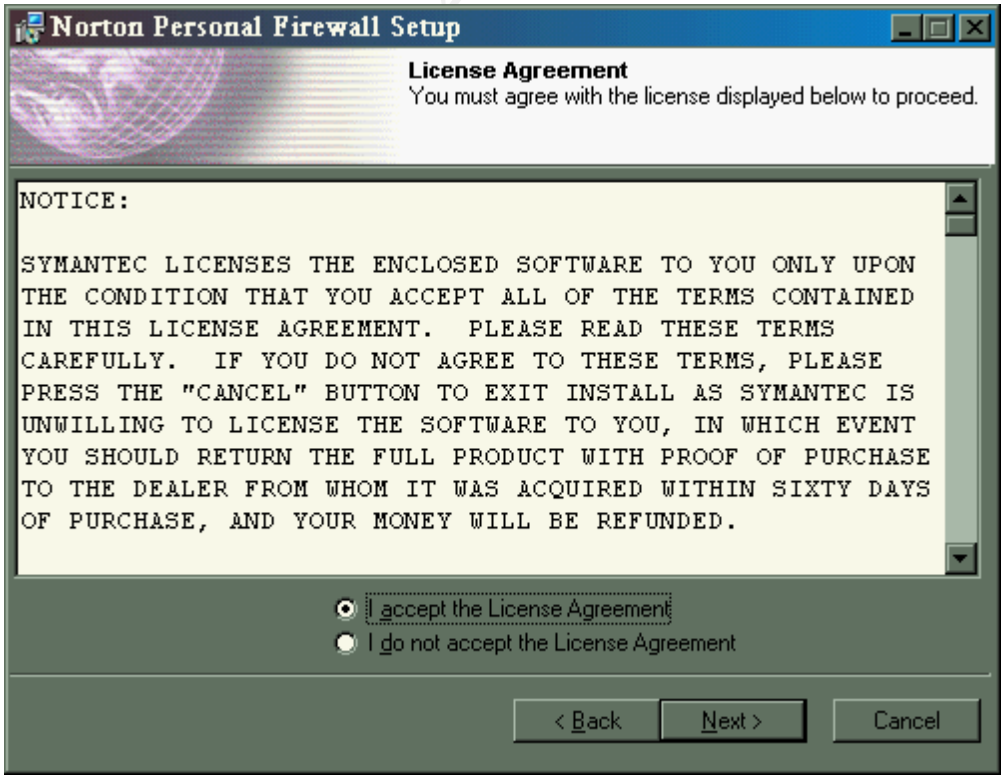
After putting the CD and autorun starts you will be shown the following screen:



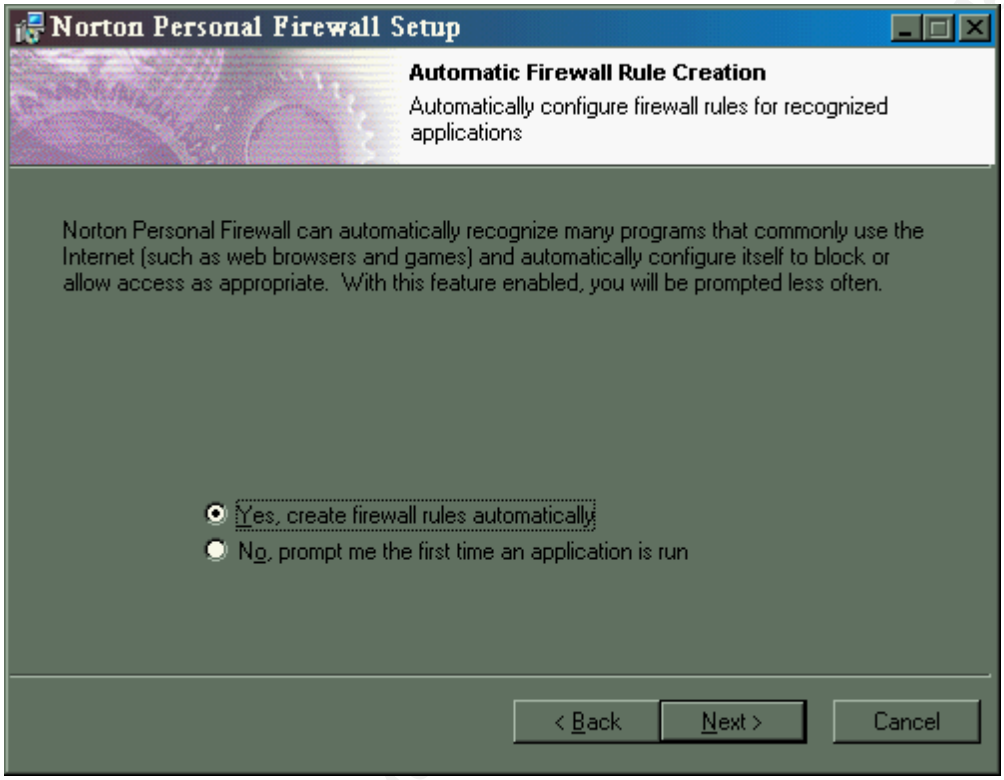
Click Install Norton Personal Firewall and the installation program will begin. The first screen you will be shown is the welcome screen.



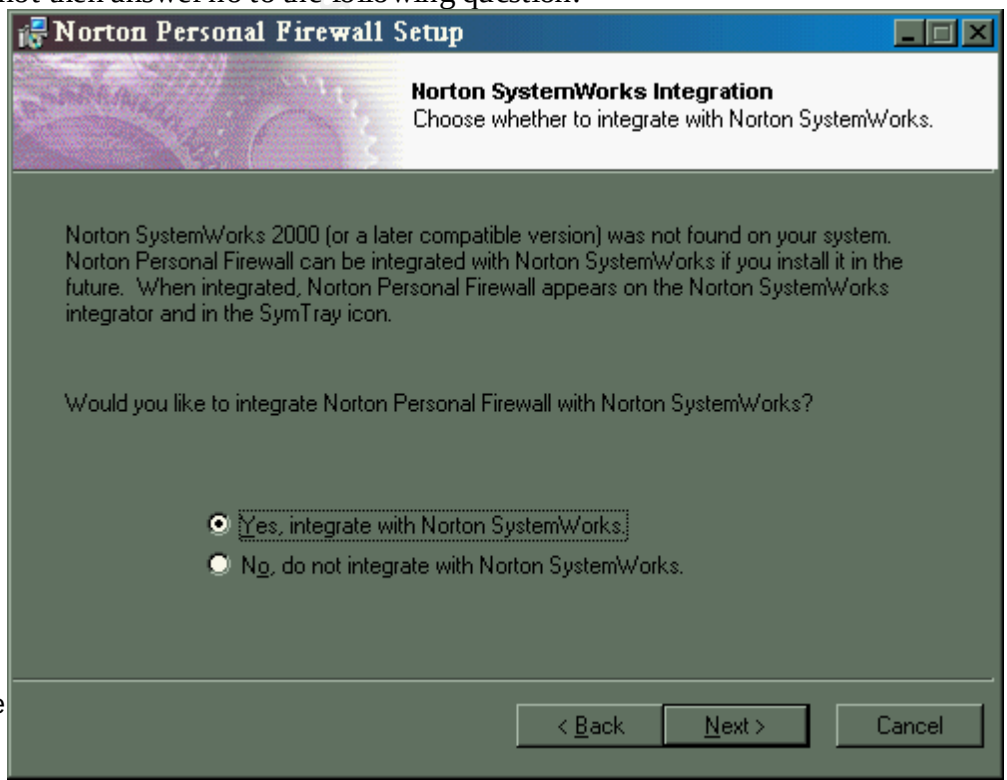
Click yes that you accept the license agreement and then click next to continue.



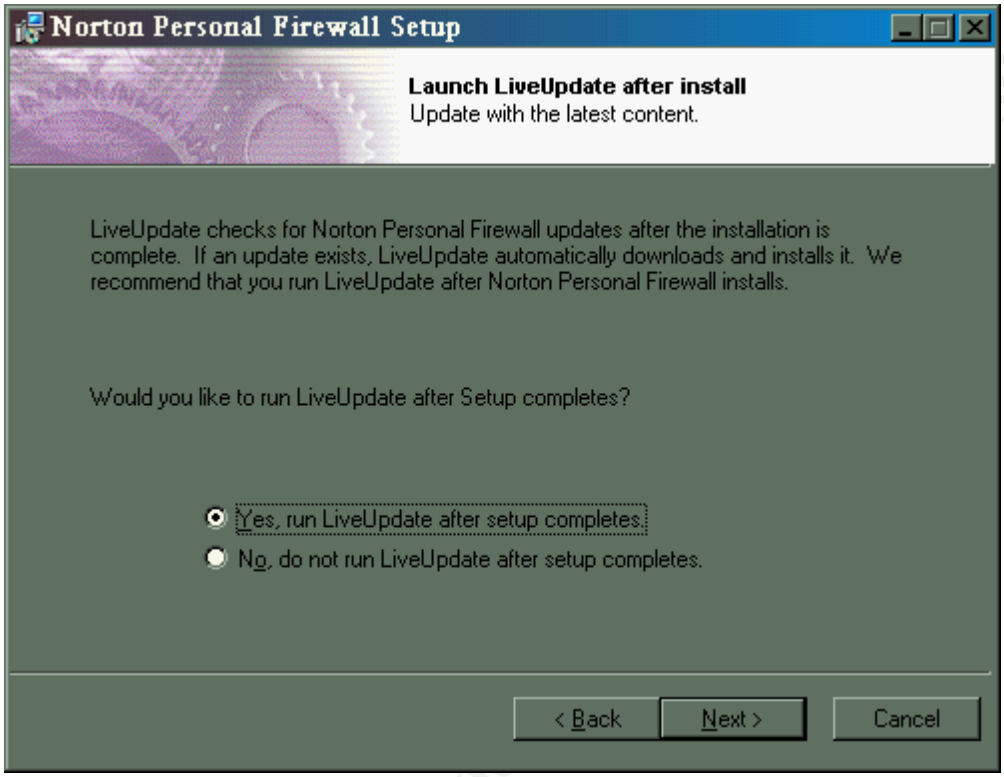
You will then be asked if you want set up to create the firewall rules automatically or if you want the rules added each time an application is ran for the first time. The easiest way to configure the firewall rules is to have set up create them automatically so that the defaults are created and after Norton is installed add any specific rules that you want the firewall to use.



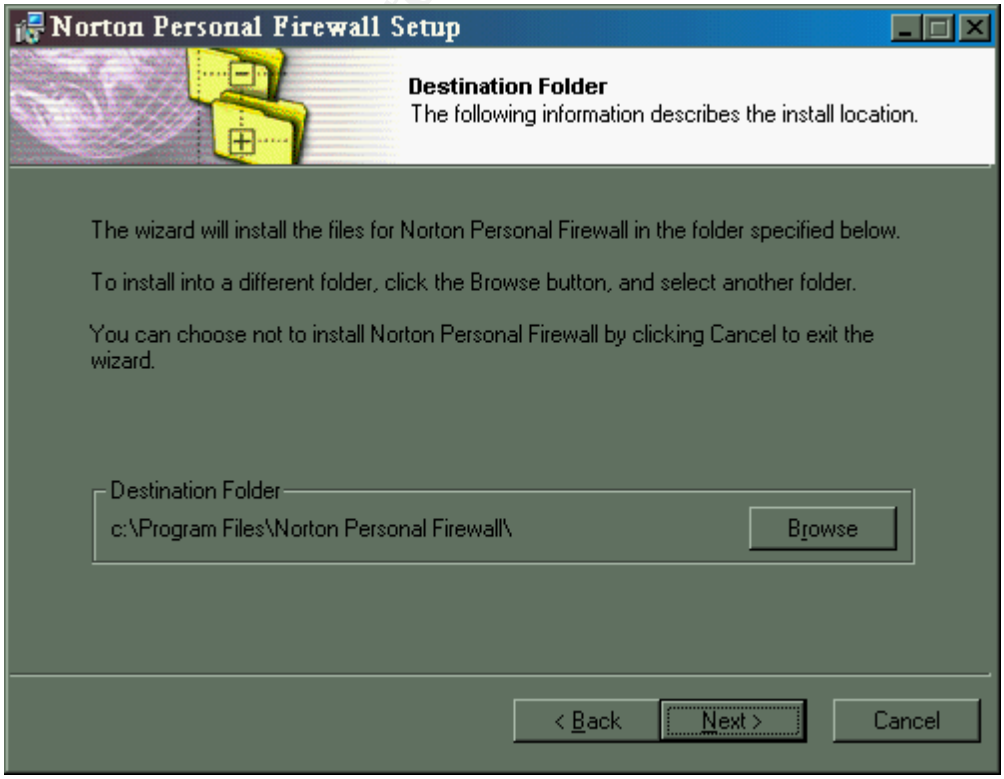
If you are running Norton SystemWorks then you can integrate the firewall. If you are not then answer no to the following question.



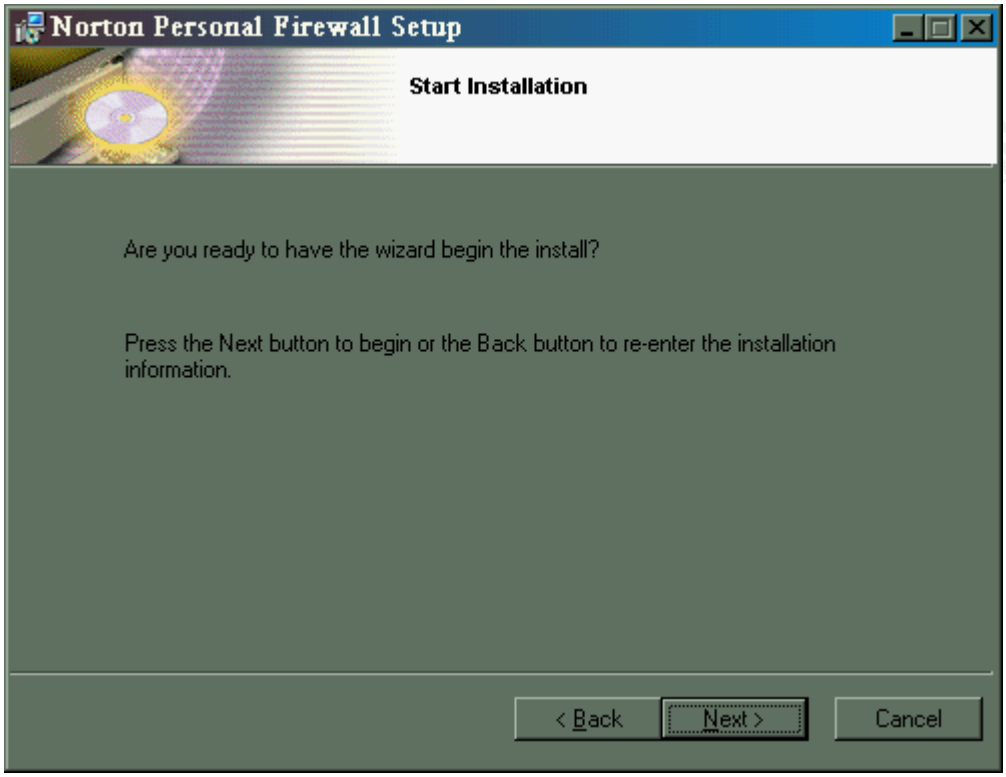
Answer yes to the following question to run Live Update after installation so that your firewall will be running latest version of Norton Personal Firewall.



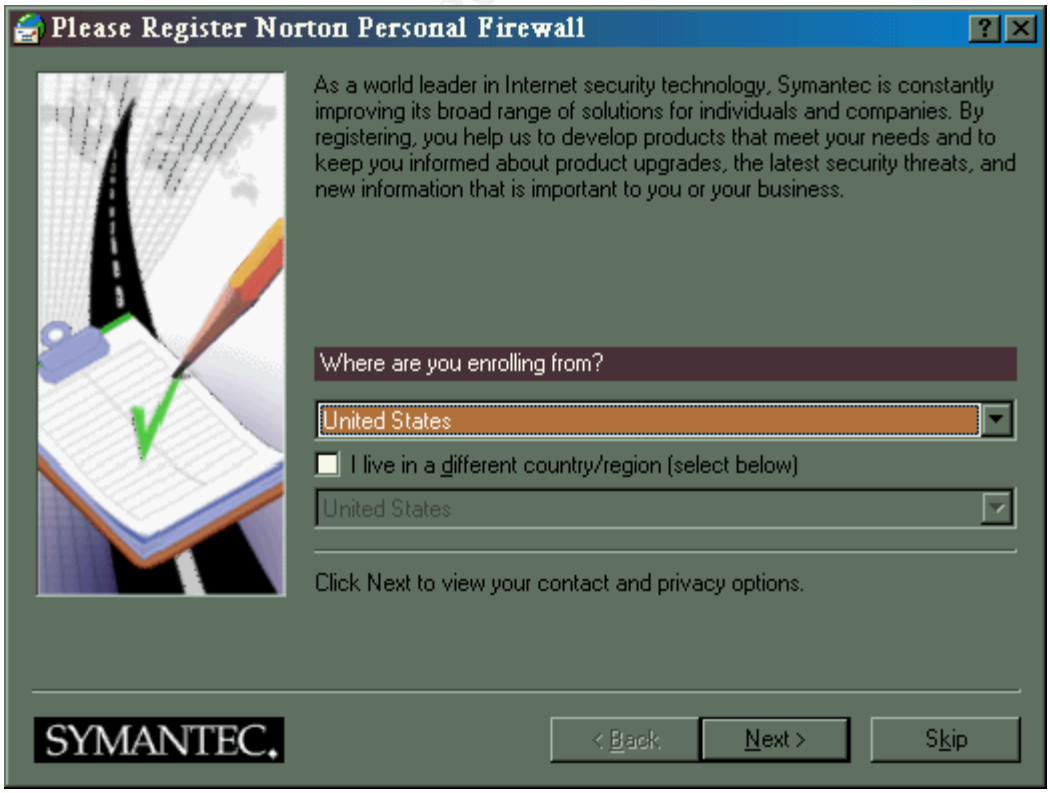
Choose where you want the program installed.



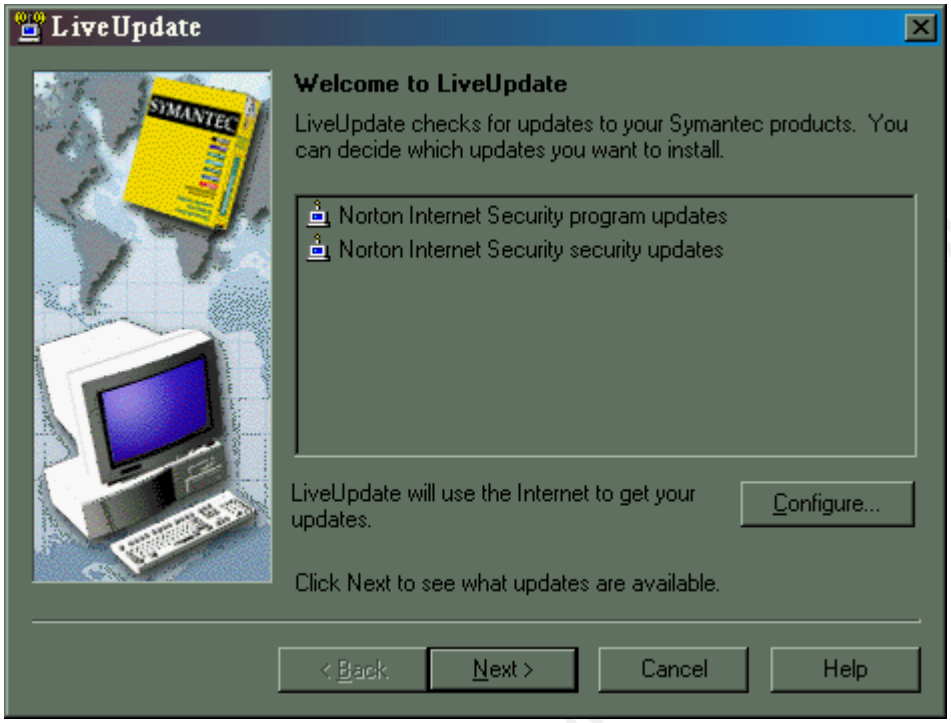
After clicking next the firewall program will be installed and the firewall rules will be set up.



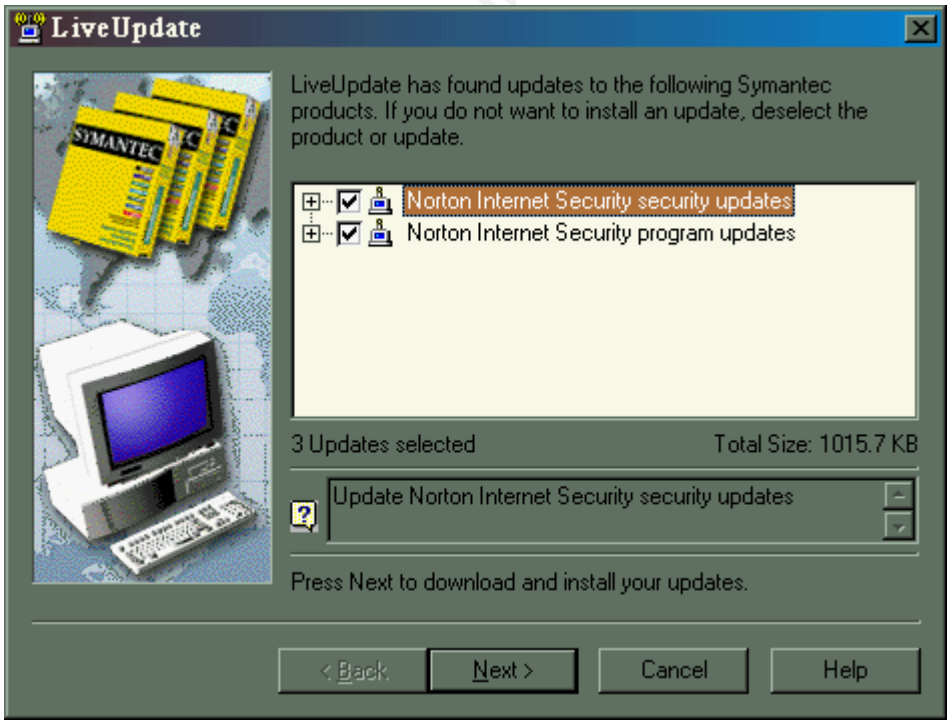
Register the program.



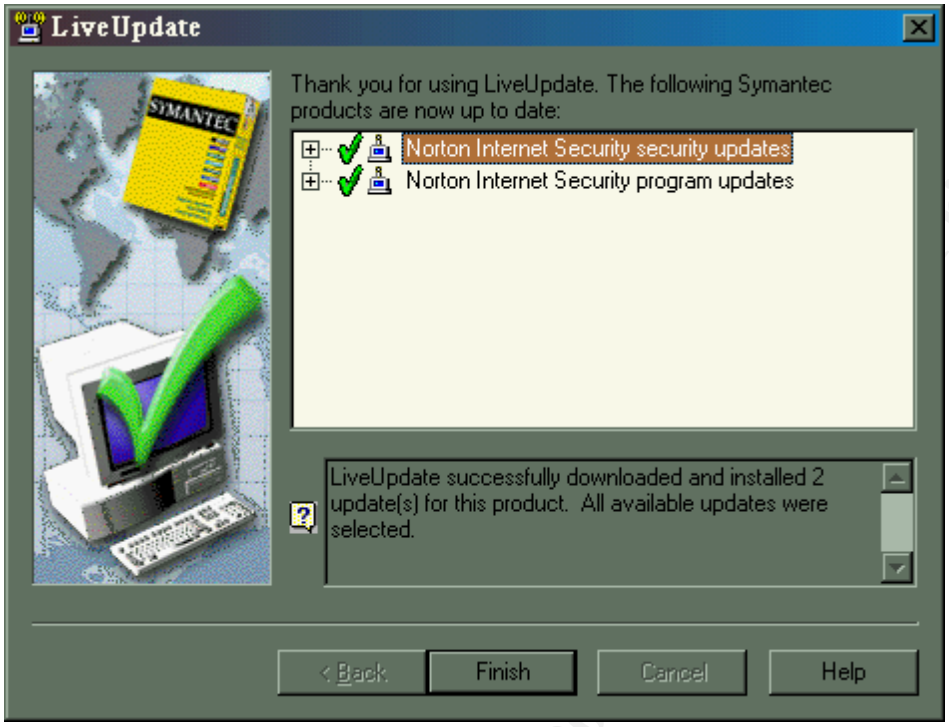
Connect to the Internet if you do not have a full time connection and Live Update will run and check to see if there are any updates for Norton Personal Firewall programs.



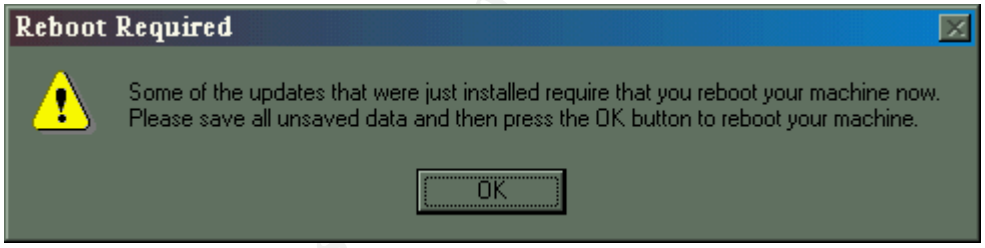
Click next to download and install any updates that are found.



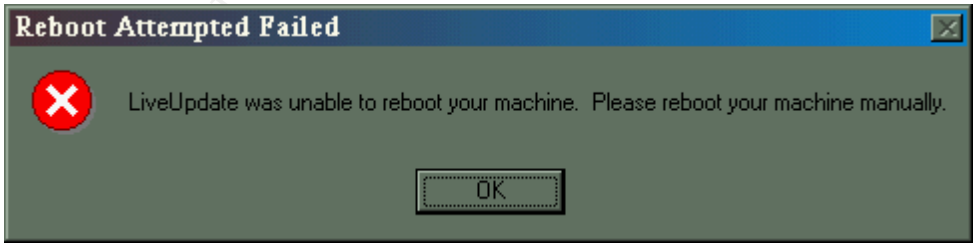
You will receive the following screen after the up dates have been installed.



You will be told that you need to reboot for updates to complete. Click OK.



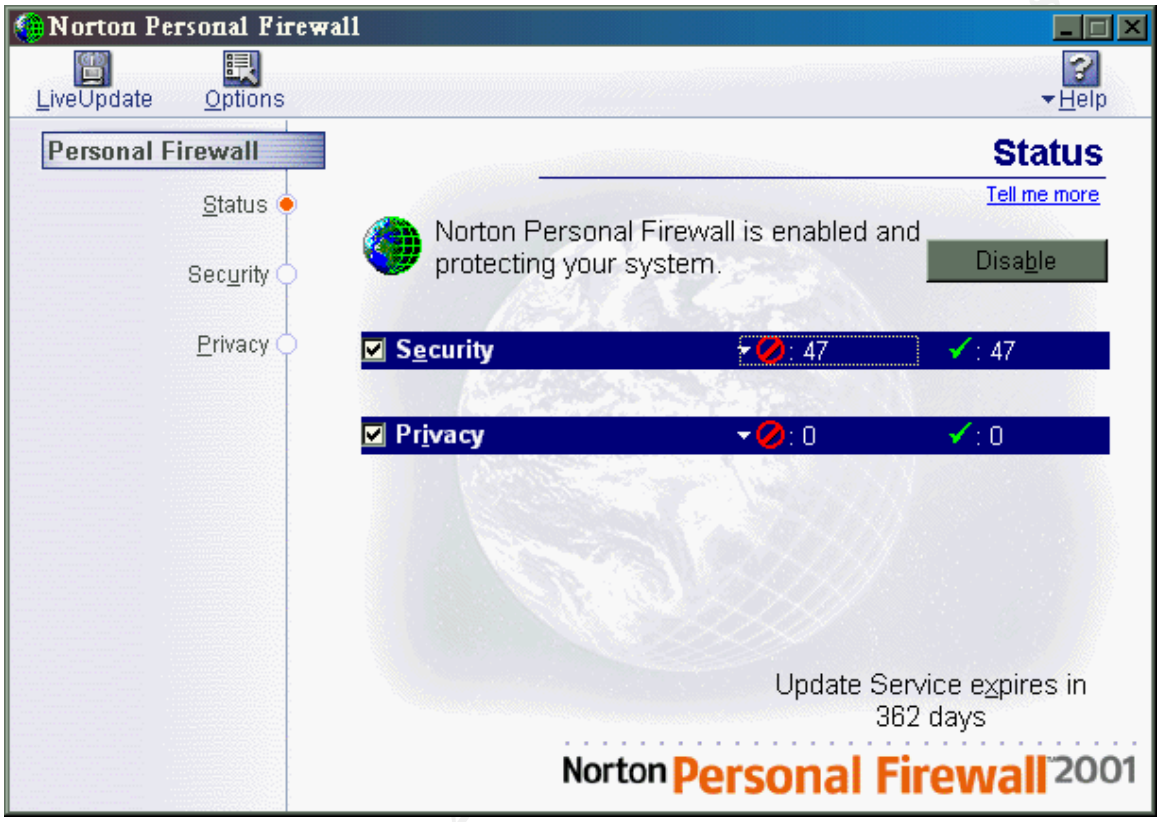
The next window is an error message that the reboot failed, that's ok because the original setup has not completed yet. Click OK.



Next the readme file will be shown, read it and click next when you are finished. Finally the Successful Installation screen will be shown, click finish and you will be prompted to reboot. Click yes and the installation will be complete.

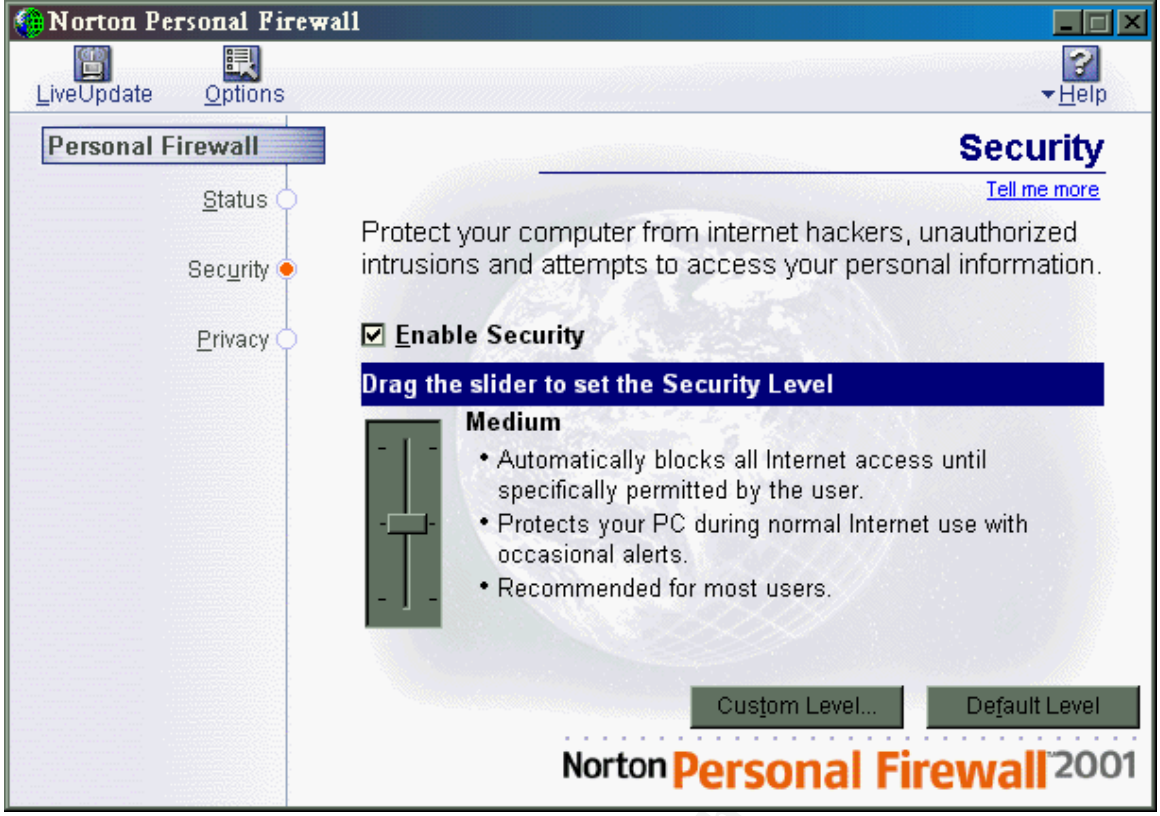
Configuration

The first time you boot your computer after installing Norton firewall the following screen will come up.



This is the status screen. The security line is telling you how many applications and exploits are being blocked access and how many are being allowing access. The privacy line is showing how many cookies and referer fields are being blocked and accepted. Referer fields come into play when you click a link, and your browser tells the web server where the link was that you used to get to it. Later we will go over how you can configure the firewall to handle referer fields so that the web server will believe that you just typed in the URL. This way the web server will not to try to track your information.

On the left hand side of the window there are three options status, security, and privacy. After clicking security you will get the following screen.

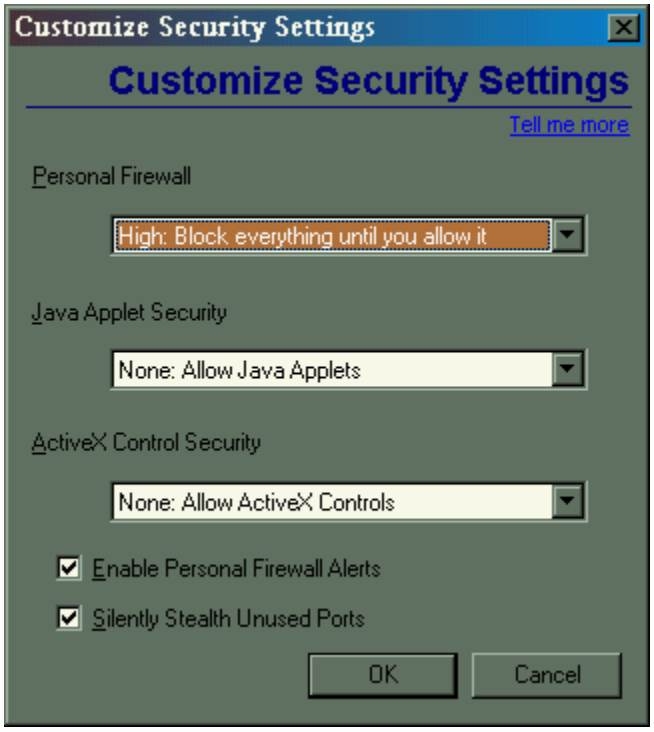


This screen allows you to set what level of security you want the firewall to run with. The minimal level is for users that need only minimal protection, it automatically blocks known threats and closes access ports to hackers. Medium security level is recommended for most users. The previous screen shot shows what it protects against. The High security level is for expert users who are familiar with what type of access they want to allow to their computer. It protects the PC against most attacks with frequent alerts and automatically blocks all Internet access until permitted by the user.

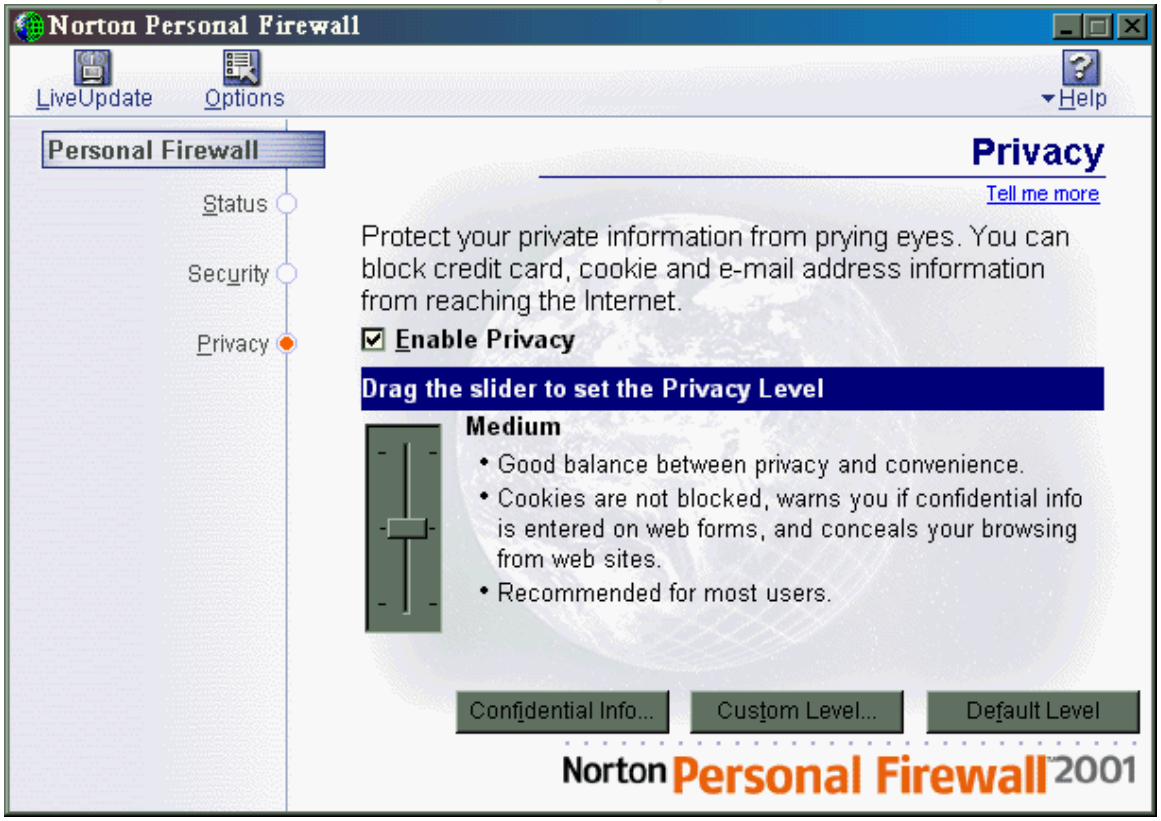
The most secure setting and easiest to administer is medium, this will block all applications that behave like a known malicious program while allowing other applications to run normally. Norton subscription has a list of known, reliable programs that require communication over the Internet. By running Live Update frequently your list of these applications will be up to date and keep the inexperience user out of trouble. Norton will prompt to create a rule when an application is ran that is not in its list and may be a trojan. The Firewall Rule Assistant is a wizard that helps configure these rules.

When Norton Personal Firewall encounters an application for which it has no rules set up the Firewall Rule Assistant appears. The Firewall Rule Assistant helps you decide what to do with the application requesting to access to the Internet. It will show you the name of the application and ask you if you wish to create a rule. It will also give you the option to allow or block it one time only, so you can research the application before creating a rule for it. When setting the security level is set to High, the Firewall Rule Assistant will show up with more frequency and an inexperienced user may not know how to answer the questions. By setting the security level at medium you are going to have the best security with little administration, and avoid having an inexperienced user creating a security hole in the firewall.

You can also create a custom level by clicking the button at the bottom of the screen. You will get the following options.



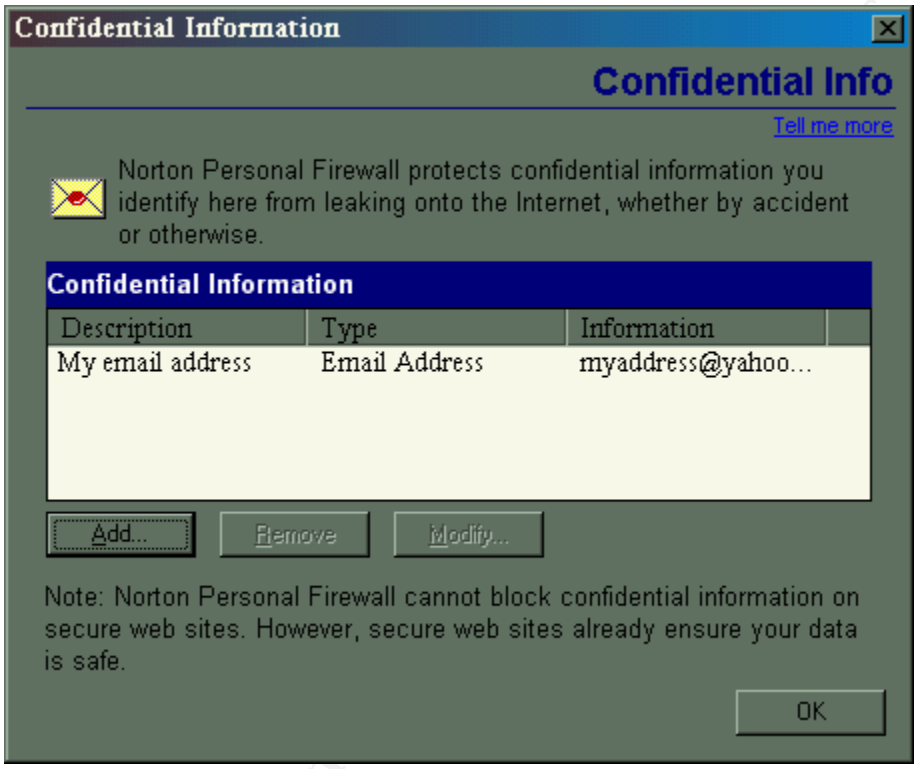
Next click the privacy option to get the following screen.



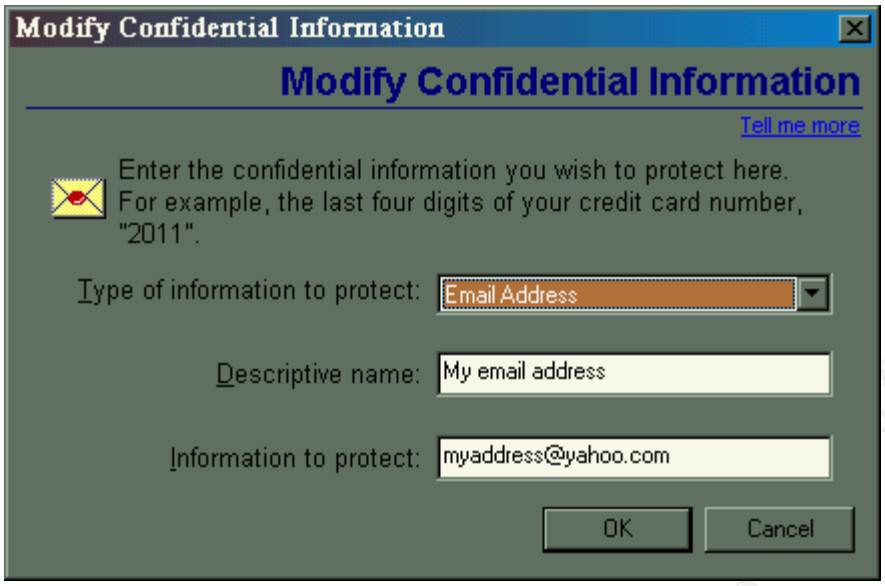
This screen allows you to configure what privacy level you want the firewall to run at. Minimal privacy is for users that want convenience, cookies are not blocked and confidential info may be entered on web forms and your browsing is concealed from web

sites. The medium privacy level is recommended for most users and its settings are shown in the previous picture. For users who are highly concerned about they're personal information there's the high privacy level. High privacy is the safest way to operate, but the least convenient, it blocks all personal and browsing info from the Internet and cookies require special handling. The medium setting is the best balanced, it allows cookies and still allows you to fill out Internet forms. This is the setting that should be used.

By clicking the Confidential Info button at the bottom of the screen you can set up your private information that you which to hide.

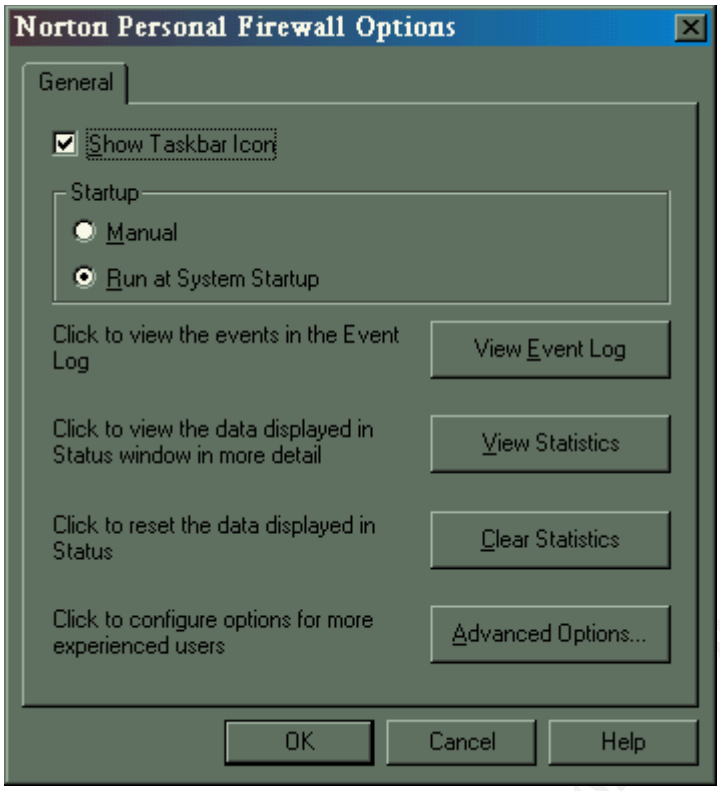


After clicking the Add button you choose what type of information it is, give it a description, and what that information is. Because Norton Personal Firewall blocks the information exactly the way you enter it you should only type in a portion of the information. For example if your protecting a credit card number it can be entered 1234 5678 9012 1234 or 1234567890121234, so by only entering the last four numbers you are protecting those number and the entire number overall. This will prevent that part of the information from always being sent to unsecured web sites.

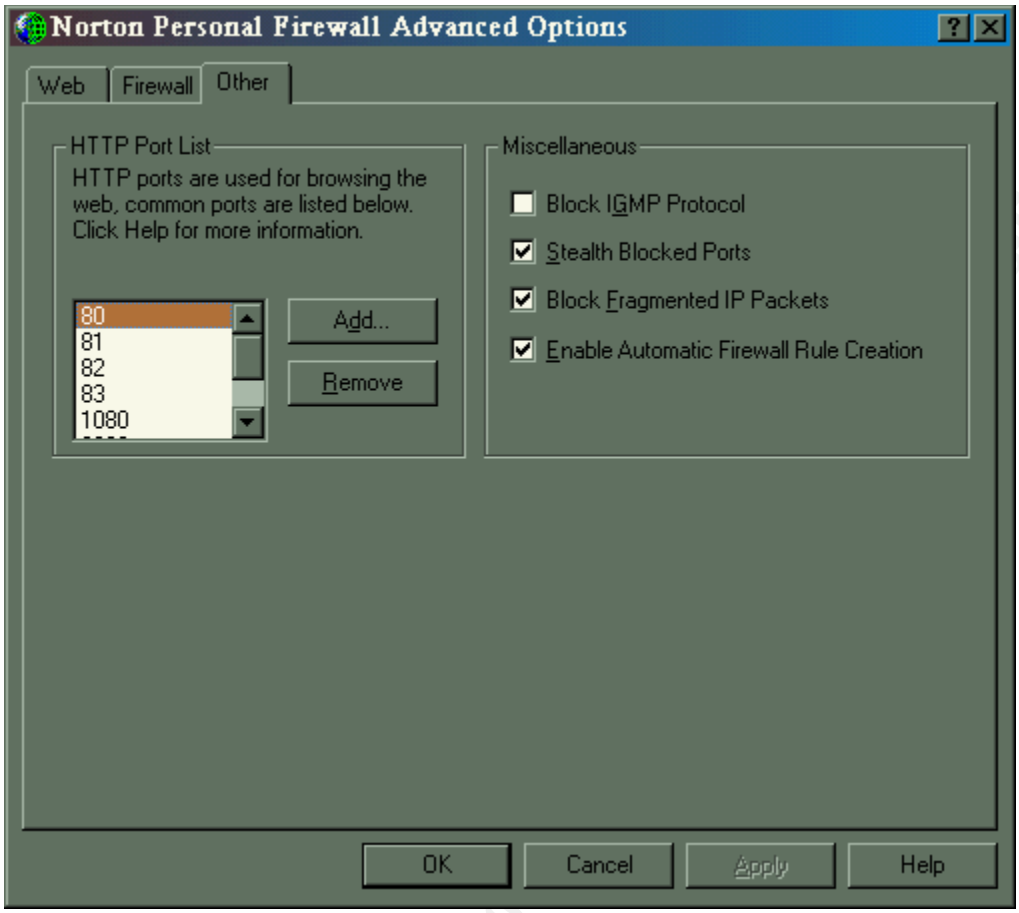


The other option on the privacy screen is creating a custom level just as there was on the firewall configuration screen.

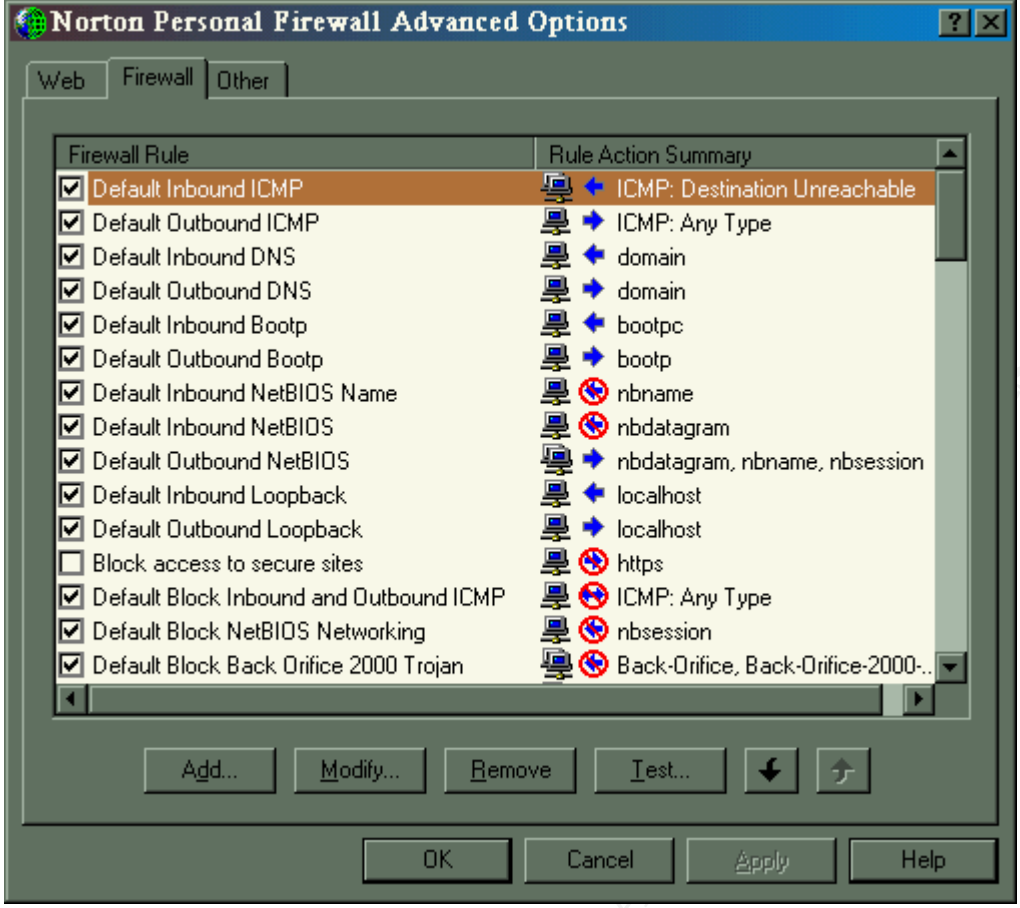
The last part of the configuration of your firewall takes place after you click the options button at the top of the screen.



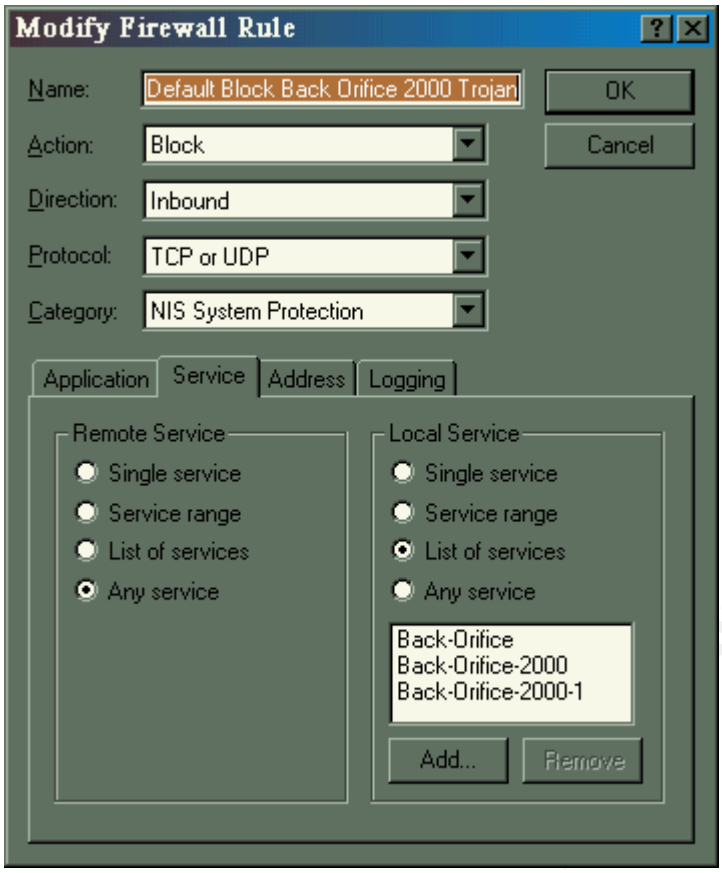
This screen gives you a couple of different options, you can view your event log or statistics, your can clear the statistics, and configure the filter rules that the firewall will use. I'll skip showing the event log and statistics, but let's take a look at the filter rules because this is an important part of the configuration process.



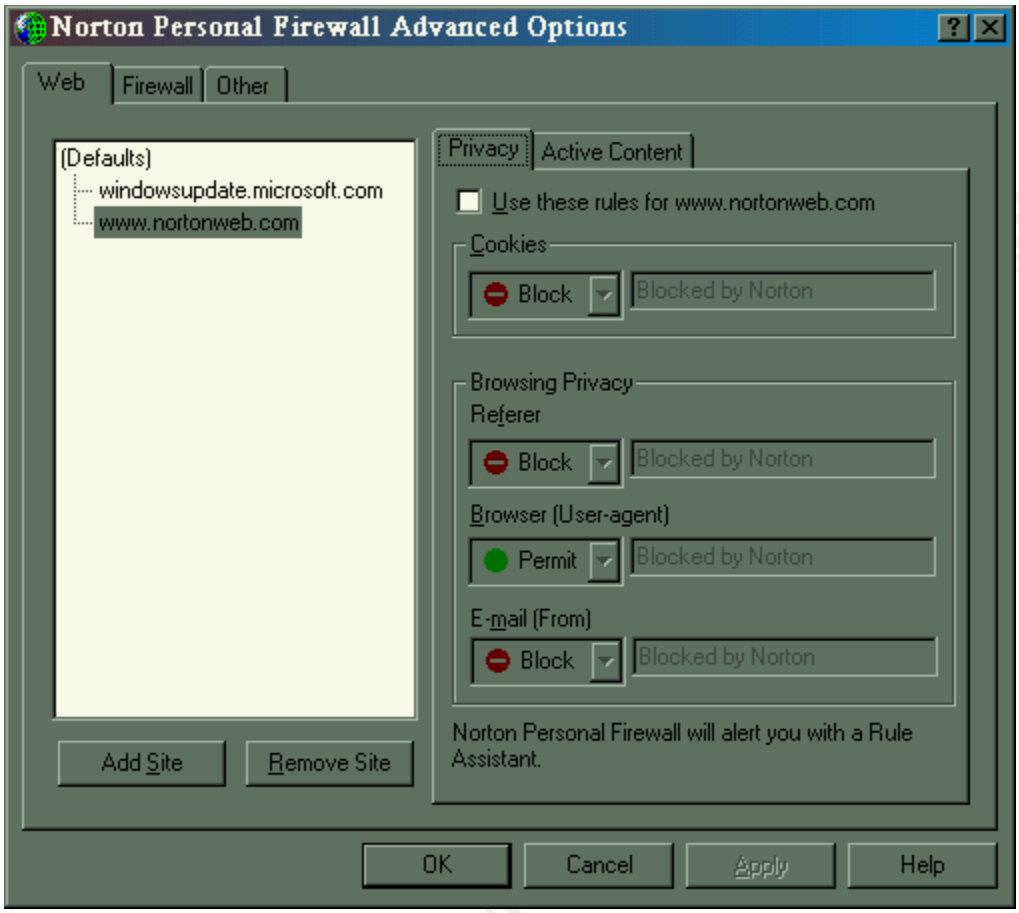
The first screen allows you to set up which ports you want to allow HTTP to use. It also allows you to choose to block IGMP requests to your IP address. If you enable The Stealth Blocked Ports option, than any request made to your ports from the Internet will not respond. This option should be enabled, because if you do not have it enabled than any request made to your ports will respond and pass along an important piece of information to the person making the request, that the IP is live. You also have the option to block fragmented packets. The last option is create firewall rules automatically. This option should be enabled to allow applications that do not have a rule to be created when the application makes a request to access the Internet. Having this option enabled will make support easier because you don't have to create a rule manually every time you add a new application.



This next screen is the filter rules that the firewall uses to protect your system. The screen shows whether the service is incoming or outgoing and whether or not it is allowed or blocked. As you can see Back-Orifice is in the listing as well as a lot of other well-known exploits. These are created for you by default.



The screen above is what will be shown after clicking add. You can name the filter whatever you want. Your action choices are block, allow, or ignore. Next you choose the direction it is suppose to act against inbound, outbound, or either. The protocol is required and your choices are TCP, UDP, ICMP, or TCP and UDP. Next is the category that is used by the service you are blocking, some of your options are email, newsgroup, games, web browsers, etc. The defaults are acceptable for the rest of the configuration and you are now protected against an exploit or service that you were trying to block.



This is the final screen in the configuration process. This screen allows you to configure what the firewall should do when you visit a particular web site. You can block or accept cookies. You can allow or deny ActiveX and Java scripts to run. This is a good feature because it allows you to configure by site. If you run an Intranet site that runs Java scripts, then you can put it in here while still protect yourself from Java scripts on the Internet.

Norton's firewall allows average users protection by allowing them to use the defaults. It automatically updates its rules and protects the user for their occasional Internet use. It also allows advanced user to configure the firewall more to their liking and against more advanced attacks. This is why Norton firewall is a good product to use for remote and home users.

Conclusion

Norton Personal Firewall is an excellent solution for personal users. It should be also be used by corporations that want to provide Internet protection for its road warriors and remote users. It's a product that inexperience users can install and forget about, yet powerful enough for system administrators to configure for their corporate networks. For those of you who are going to use this product I hope this document helps with your installation and configuration.

Bibliography

Zych, Tina. "Personal Firewalls: What are they, how do they work?" SANS Institute 22 August 2000. URL: http://www.sans.org/infosecFAQ/homeoffice/personal_fw.htm. 12 May 2001

Symantec, URL: http://service1.symantec.com/SUPPORT/nip.nsf/docid/2000011014313436 12 May 2001

Norton Personal Firewall User's Guide v2.5 2000 ed. ftp://ftp.symantec.com/public/english_us_canada/products/norton_internet_security/manuals/npf25.pdf 12 May 2001

Symantec Service and Support. Knowledge Base. "Default Firewall Rules" 8 May 2001 http://service1.symantec.com/SUPPORT/nip.nsf/ddb3f5ca22507b08852569370052afd6/42e37d490c68820a85256a3f006a349a?OpenDocument 13 May 2001

Symantec Service and Support Knowledge Base "How to "stealth" a port with Norton Internet Security or Norton Personal Firewall" 12 February 2001 http://service1.symantec.com/SUPPORT/nip.nsf/ddb3f5ca22507b08852569370052afd6/2d50a9f9d1f4b3fa882569290064a60a?OpenDocument 13 May 2001