Global Information Assurance Certification Paper

Installation and Configuration of CyberwallPLUS SV

Daren Kinser
January 20, 2003
GSEC Practical
Version 1.4b, Option 1

Abstract

There are many different firewall solutions on the market today. An administrator has the option of network based firewalls, host based firewalls or a combination of the two. Understanding what a firewall is and how the different types work is essential in helping a security professional make important decisions on the type of firewall to implement and how that firewall should be configured.

In this paper I will cover basic information about firewalls then explain the installation and configuration of the host based firewall CyberwallPLUS SV by Network-1. I will also show the benefits of this solution by port scanning the server before the firewall is enabled and after various configurations. I will not spend much time on explaining who needs a firewall. Simply put it's anyone who has their computer or network plugged into a network, especially that big one know as the Internet. I agree with Eugene Shultz when he says, "Firewalls are now so common that failure to deploy them could conceivable constitute failure to exercise 'due care' (that is, reasonable precaution) in one's InfoSec practice."(1)

What Is a Firewall

A firewall is a system, either software, hardware or a combination of the two, that is designed to prevent unauthorized access to and/or from a private network(2).

A host based firewall is a piece of software which is loaded directly on the host machine that it would be protecting. Examples of this would be Network-1 CyberwallPLUS, ZoneLabs Zone Alarm, and ISS BlackIce to name just a few of the many. Host based firewalls are common on home systems, business systems which do not enjoy the protection of a network based firewall or possibly corporate laptop users who work from the road. You might also find host-based firewalls on systems that sit behind a network-based firewall. This would be a good example of an IT security administrator applying security in depth.

Network based firewalls are hardware devices that protect the systems on the trusted network side from the dangers on the untrusted network side. A few examples of network based firewalls are Watchguard Firebox, SonicWall, Netscreen, Check Point and Cisco PIX.

Firewalls fall into four categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls.(3)

Packet filter: A packet filter will look at each individual packet entering and leaving a particular network. Based on a set of preconfigured rules, the packet will either be dropped, forwarded or a message will be sent to the originator of the packet. One benefit of this type of firewall is performance while a disadvantage is IP spoofing. Spoofing involves using one system to impersonate another by forging an IP address.(4) Packet filters are most commonly found as part of a router.(3) Packet filters work at the network level of the OSI model.

Application gateway: These are also called Proxies. These types of firewalls work at the application layer of the OSI model and all communication through the gateway is dependent upon a proxy being setup for that specific service. We can use FTP as an example. If a user wanted to access an external FTP site and a proxy was set up for the FTP protocol with a rule allowing that user to access external FTP then the communication would be allowed. If the proxy for that service was not configured then the connection would be denied. This example would be true for both incoming and outgoing traffic. Application gateways offer the benefit of high security but with the sacrifice of network performance.

Circuit-level gateway: A circuit-level gateway ensures that a trusted client and an untrusted host have no direct contact. A circuit-level gateway accepts a trusted client's requests for specific services and, after verifying the legitimacy of a requested session, establishes a connection with an untrusted host. After the connection is established, a circuit-level gateway copies packets back and forth--without further filtering of them.(5) Circuit-level gateways are advantageous in the fact that they hide the internal network hosts from the internet. All packets appear to come from the gateway and not the individual hosts themselves. On the other hand, a weakness of circuit-level gateways is once the connection is made between a host on the internal network and a resource on the outside, there is no further checking of the packets. Circuit-level gateways work at the transport level of the OSI model.

Stateful: Stateful firewalls work at the network layer but examine packet contents up through the application layer. Each time a connection is made outbound information about source and destination address, port numbers, flags and sequence information is recorded. All Inbound packets are then compared to this record. Only when an appropriate match is made are the inbound packets allowed. Stateful packet filters offer high security but because of their complexity, they can be difficult to setup and maintain properly.

Install

Network-1's CyberwallPLUS contains three separate products: CyberwallPLUS Central Manager Utility (CyberwallPLUS CM), CyberwallPLUS Workstation

Edition (CyberwallPLUS WS) and CyberwallPLUS Server Edition (CyberwallPLUS SV). I will be working with CyberwallPLUS SV.

OS and hardware requirements for CyberwallPLUS SV are as follows.

- Windows 2000 Professional, Server, Advanced Server
- Windows NT 4.0 Workstation and Server
- Windows 98, 98 SE, ME, XP Professional
- 233MHz Pentium or equivalent, 450MHz Recommended
- 65MB RAM minimum, 128MB RAM Recommended
- 25MB Hard Disk Space with additional space needed for local logging
- SVGA display with support for at least 256 colors

The test system this install will take place on is a Windows 2000 Server with service pack 3. It runs a 1.2 GHz AMD Duron processor with 384MB of RAM. Of course this system has also had all the necessary patches and updates applied.

The executable was acquired from http://www.network-1.com\download where it was downloaded and scanned for viruses on a secure system. It was then burned onto a CD ROM.

After placing the CD in the test system, I double clicked on the CyberwallPLUS731.exe icon.

The first window that appears asks where I would like to save my files. I selected the default location and clicked Next. The program begins extracting files to the temporary location and starts the Install Shield installer.

Click Next on the Install Shield welcome screen then answer Yes to the license agreement.

The next screen displays the system requirements. If you are good to go on the hardware as well as the operating system, click the Next button.

Enter the customer information at the next window and click Next.

Next you are asked to choose a destination folder. For this install I will select the default location. Some may find it advantageous on a production system to choose a drive other than the drive that their operating system is on. If this is necessary click the Browse button on this window and select a new location for the install.

At the next window I select the components I want to install. This paper only deals with the firewall product and not the Remote Manager so only the check box for Host Resident Firewall for Enterprise Servers gets checked before clicking Next.

When asked to select a program folder, again I go with the default.

The Start Copying Files window is next (figure1). Give the settings a close look to make sure everything is correct. If necessary make a few notes of this window before clicking Next.

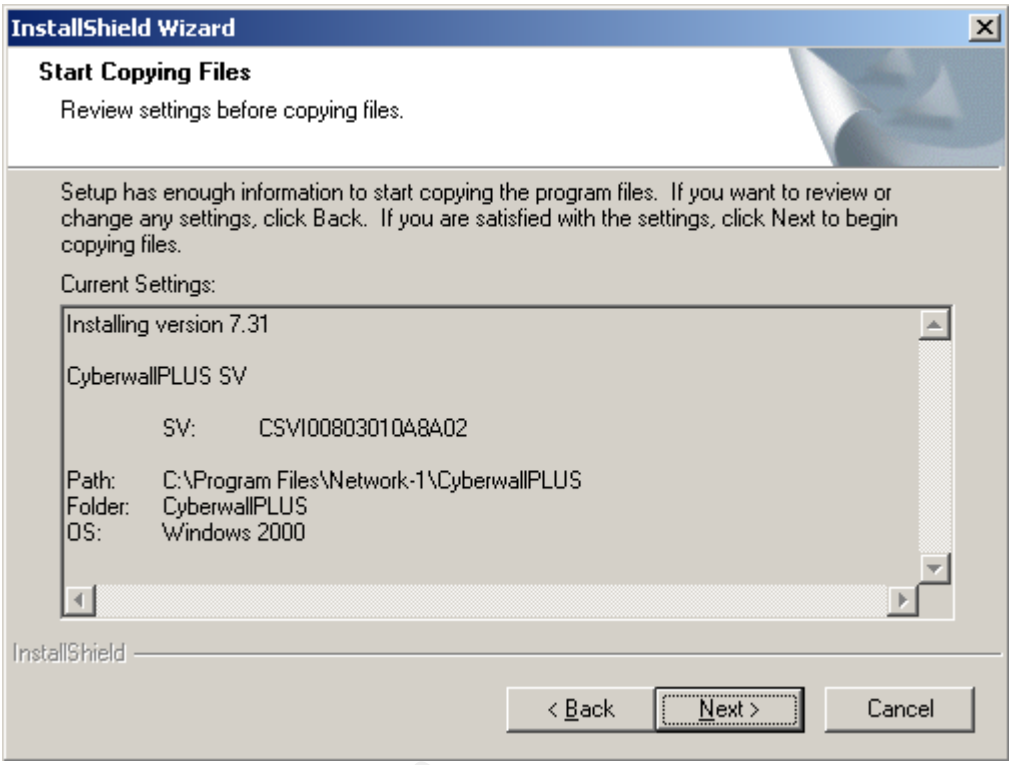


Figure 1

After the program is installed on the system the Automatic Policy Update Configuration window presents itself. Here you can enter the name or IP address of the Central Manager Server and the group that the system is a member of. If we were running Central Manager we would have a policy already built for the group our server is in. This policy would then be automatically applied to this system for us. Again, we are not running Central Manager so we leave these two fields blank and click Next.

At this point a temporary license is granted for approximately 30 days. At anytime during that 30 days if we decide we would like to purchase the product, we can call Network-1, arrange payment and they supply us with a permanent license. Click OK then click Finish to restart the system.

Configuration

After the computer restarts and is logged into, you will notice a new icon in the system tray like the one outlined in Figure 2. To access CyberwallPLUS SV, double click this icon, select localhost and click Connect.

Figure 2

Before you can access CyberwallPLUS you need to authenticate yourself. This keeps would be troublemakers from making unauthorized changes to the firewall configuration. Since many security breaches are from the inside, this is a good feature. Put an administrator username and password along with the domain name and click OK to start CyberwallPLUS.

As the program starts you see the CyberwallPLUS screen. There are nine tabs across the top of the window. I will cover each one of these tabs in this section.

Main Tab

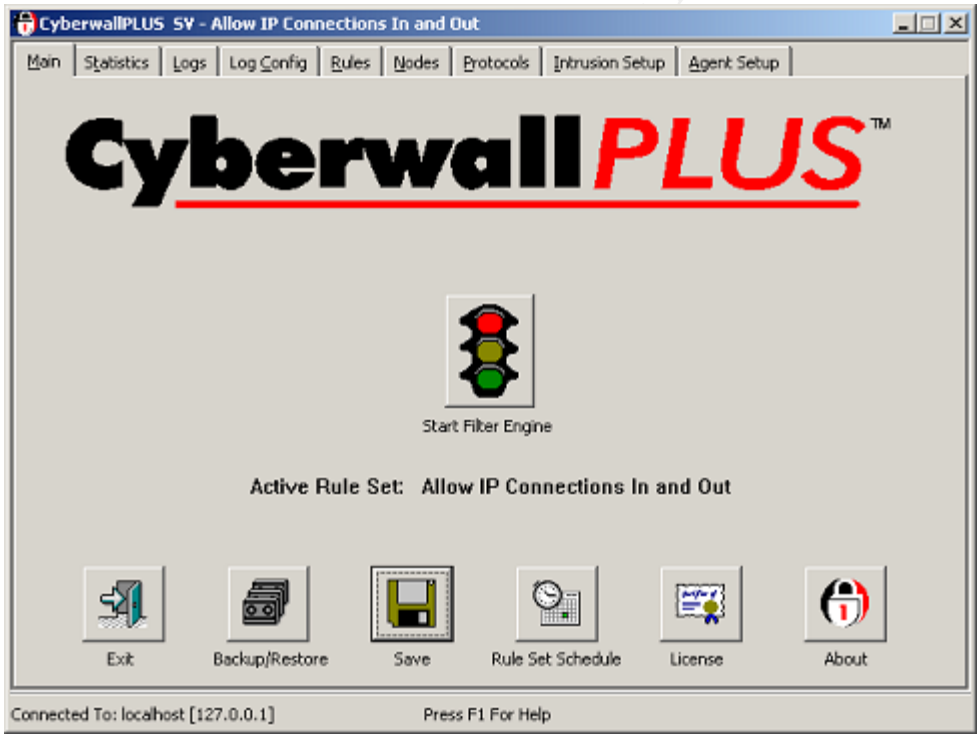


Figure 3

Figure 3 shows a screen shot of the Main tab. You'll notice right away the signal light in the middle of the window. This is a quick and easy way to tell if the firewall is working. If the light is green the firewall is on. If the light is red the firewall is off. To start or stop the firewall, simply click the stoplight. You'll be asked to confirm your request before it is applied. Below the stoplight the active

rule set is given. This tells what rule set is currently being applied. I'll go over rules and rule sets when we get to the rules tab. Along the bottom of the Main window are six buttons.

The Exit button simply exits the program.

The Backup/Restore button takes you through the backup or restore of the Cyberwall program. This is especially helpful if you have had a system go down and you need to restore from scratch. If you have made a backup of your configuration you can load Cyberwall, put the backup disk in the floppy drive and restore. It saves the time of having to reconfigure the entire firewall again.

The Save button will save any configuration changes that have been made and apply them immediately.

The Rule Set Schedule feature is very nice. Some may find it necessary to apply different rules on different days or different times of the day. This can be accomplished easily with this feature. Simply select the day and time you would like a certain rule set applied, select the rule set from the list and click OK.

All the license information can be viewed by clicking the license button. When you decide to purchase Cyberwall Plus, you call technical support and give them the hardware ID and the serial number from the license information. They will give you a new license number and expiration date to enter in the appropriate fields.

Information about Cyberwall and the system that it is loaded on can be obtained by clicking the About button. Most will be pleasantly surprised to find that they are given more information than they normally would see by looking at a programs About information.

Statistics Tab

This tab (figure 4) will show real-time performance information on the firewall. From here you can also monitor network data for both the incoming and outgoing connections. You can also terminate a specific connection, clear the statistics, and view detailed information about each connection. This information gets very granular and is beyond the scope of this paper.

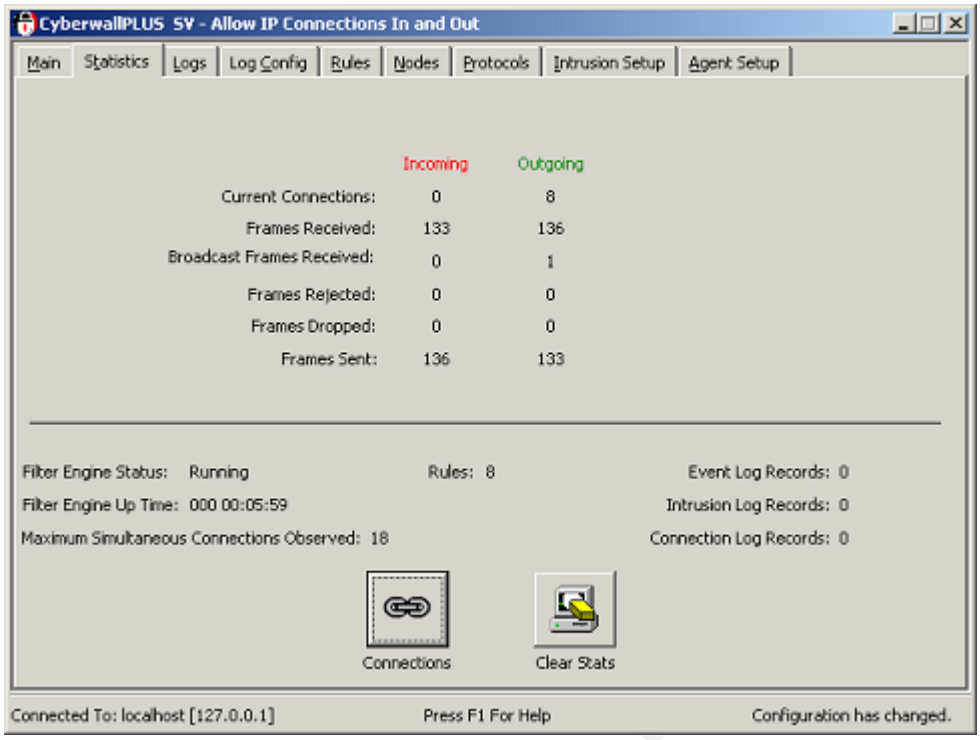


Figure 4

Logs Tab

CyberwallPLUS contains four log types: Event, Connection, Intrusion and Application.

The event log displays a history of all packets that passed or failed to pass through the firewall, depending on how you have your logging configured. The connection log displays the history of all the connections allowed through the firewall. The Intrusion log displays a history of attacks against the firewall. It will also display the source, destination and type of attack. The application log displays information and errors generated by the firewall.

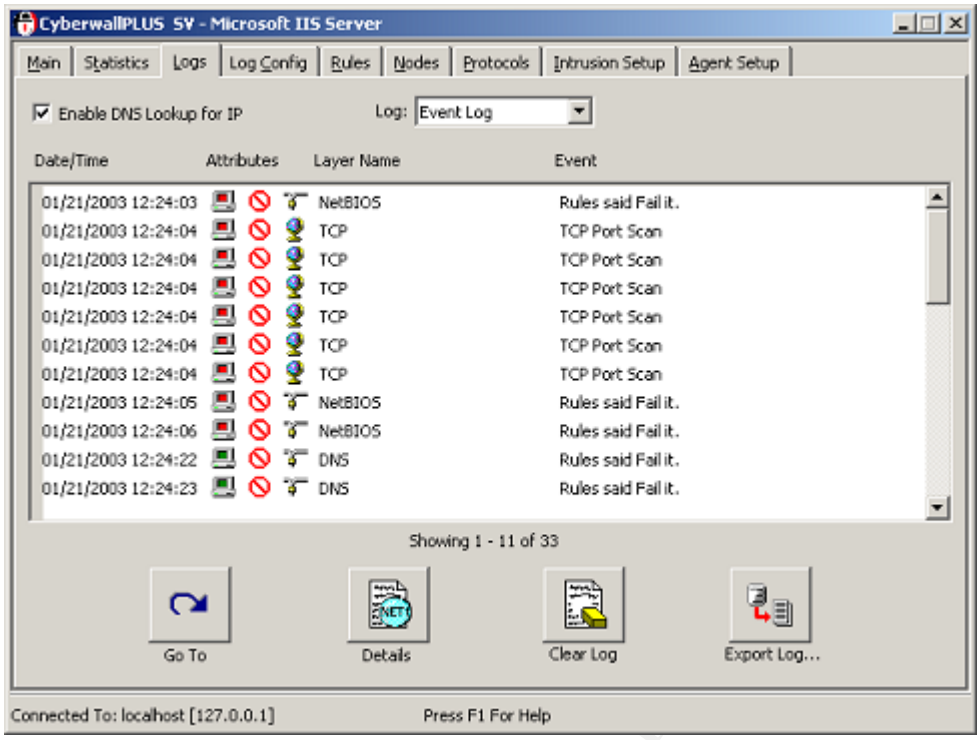


Figure 5

Figure 5 shows what a basic scan of a few ports would look like in the event log. From here you can select any of the events and click the Details button to get some very granular information about the event. You can also export the log files to view or analyze. When exporting the log files you have the choice of exporting into three different formats: comma separated value, Web Trends Enhanced log format or Sniffer format.

Log Config Tab

From the log config tab (figure 6) you can configure what directory you want the log files stored in, what format the file should be and when you want a certain action to be taken. In figure 6 you will notice I have set the log files to be stored in the default directory in native format. I have also configured the log files to be moved to C:/Firewall/Logfiles at midnight every day. After all settings are made the Save button is clicked to apply the configuration immediately.

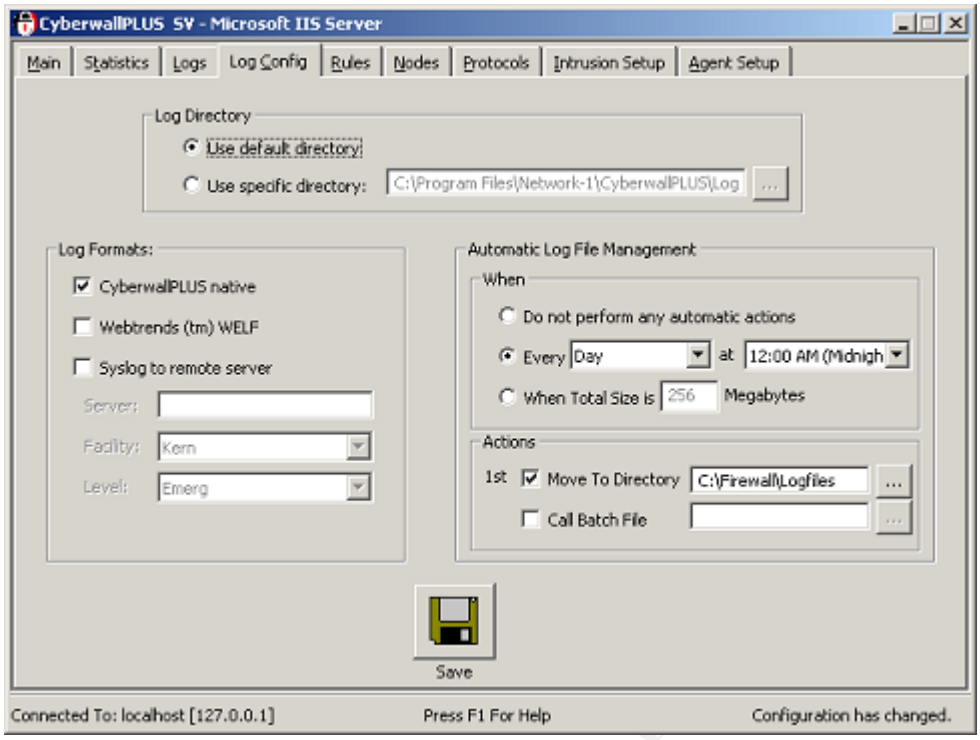


Figure 6

There are more advanced ways to manage CyberwallPLUS log files with third party tools if more advanced logging practices are required.

Rules Tab

Rules are one of the most important aspects of the firewall. As Figure 7 shows I have selected the preconfigured rule set for a Microsoft IIS Server. The rules in the main field show the individual rules that combine to make up the rule set. There are 21 preconfigured rule sets to choose from or you can create your own. I will add a rule to the Microsoft IIS Server rule set to allow "TrustedSystem" to connect via Terminal Services, then save it as a new rule set. It should be noted that TrustedSystem must be created before we add this rule. We will cover this in the Nodes Tab section.

In order to connect to Terminal Services on this machine I will need to open port 3389 to allow a terminal service connection.[6] I will open this port only for TrustedSystem to prevent others from trying to use this port to access my server.

- On the Rules tab click the Add button.
- In the Untrusted field use the drop down list to select TrustedSystem.
- Under Protocol, click the button labeled <undefined>.
- From the protocol list, under TCP, select RDP-Microsoft Terminal Server Protocol.

- Use the drop down list in Allowed Directions under IN and select the green check mark.
- With logging I like to log only Failed events so select Fail from the drop down list under Events. Leave the Connections logging at it's default.
- Click OK

You should now see the new rule appear in the main rules field. We are not done yet because this new setting will not take place until we save it.

- Click the Save button.
- Change Rule Set Name to IIS_TermServ.
- Change Rule Set File Name to IIS_TermServ.
- Leave all other fields at their defaults.
- Click OK.

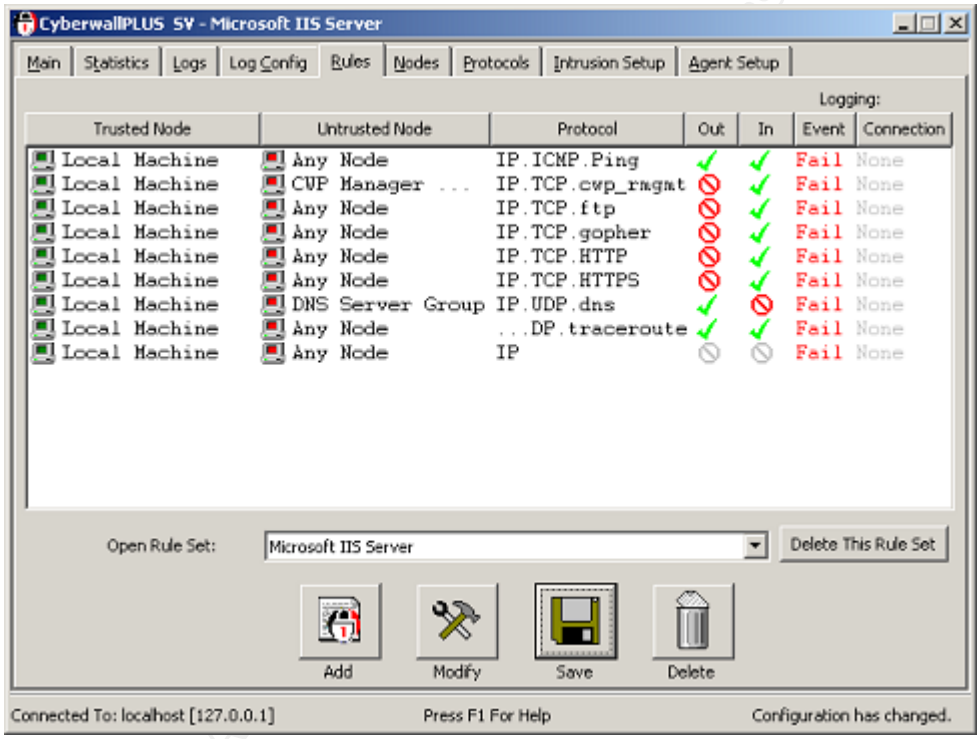


Figure 7

Now on the rules tab in the Open Rule Set field you should see the entry IIS_TermServ. Since we saved this rule set, it has immediately been applied. If you drop down the Open Rule Set list you will also notice we have not changed the original Microsoft IIS Server rule set but instead created a whole new rule set. We can now connect to terminal services on the Test system from our TrustedSystem host.

Nodes Tab

On the Nodes tab (Figure 8) we configure who the untrusted nodes are. A node is any system connected to a network, usually a workstation or server. You can group nodes into groups for easier administration or leave them identified individually. As an example, if you had many users, you may want to create a group called Users and add all the individual nodes under this group. CyberwallPLUS has created a few node groups in advance but most will need to be created. Any system wishing to access resources on this server will need a Node ID added for that system.

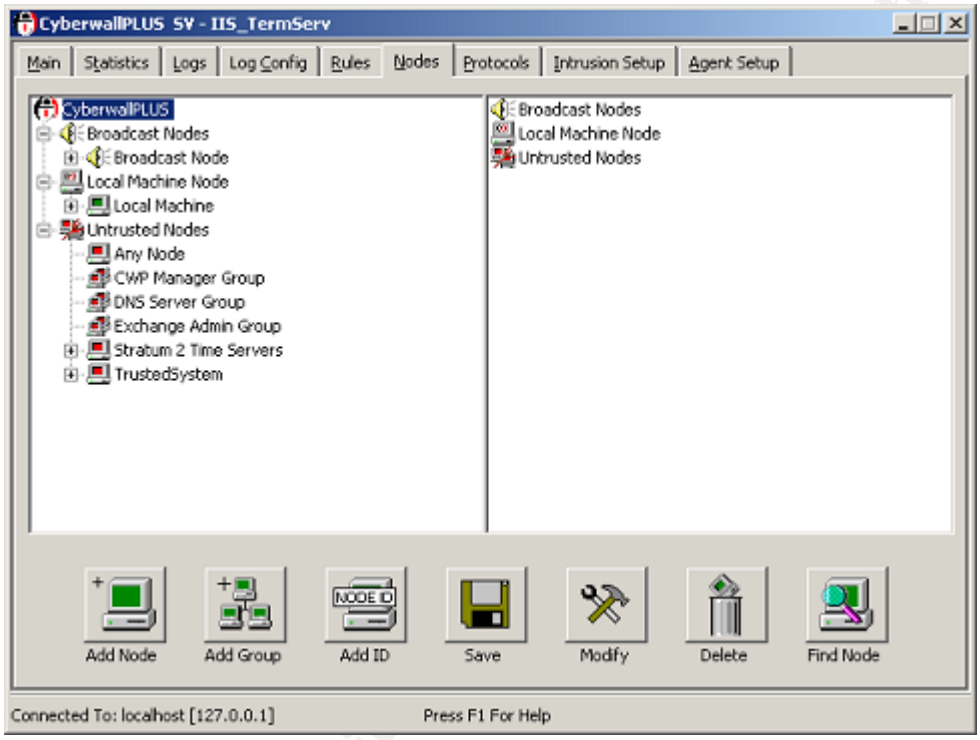


Figure 8

Earlier we configured a new rule so TrustedSystem could access terminal services on this server. This would not have been possible if we had not first added this node here on the Nodes tab. Adding a node is fairly simple.

- Select Untrusted Nodes (single click) in the left pane.
- Click the Add Node button.
- Enter TrustedSystem in the Node Name field.
- Click Add ID button.
- Under Node ID Type select Individual Address.
- In the address field enter the IP address of TrustedSystem.
- Click OK.
- Click OK.

We have now added TrustedSystem to our untrusted nodes.

From the nodes page it is also possible to add, delete or modify rules. If you right click on Local Machine under Local Machine Node and select Rule Inheritance, you can view the rules applied to the untrusted nodes. Select TrustedSystem in the left pane. In the right pane drill down to RDP-Microsoft Terminal Server Protocol under TCP and you will notice a green checkmark in the Allowed IN column. In this window you can double click any of the protocols and add or delete a rule for that untrusted node.

Protocols Tab

The Protocols tab (Figure 9) displays all the protocols that are available to CyberwallPLUS. From this tab you can view, add and modify a protocol. The default view only shows the most popular ports. If you need to see more ports, put a check in the Show Full Protocol List box.

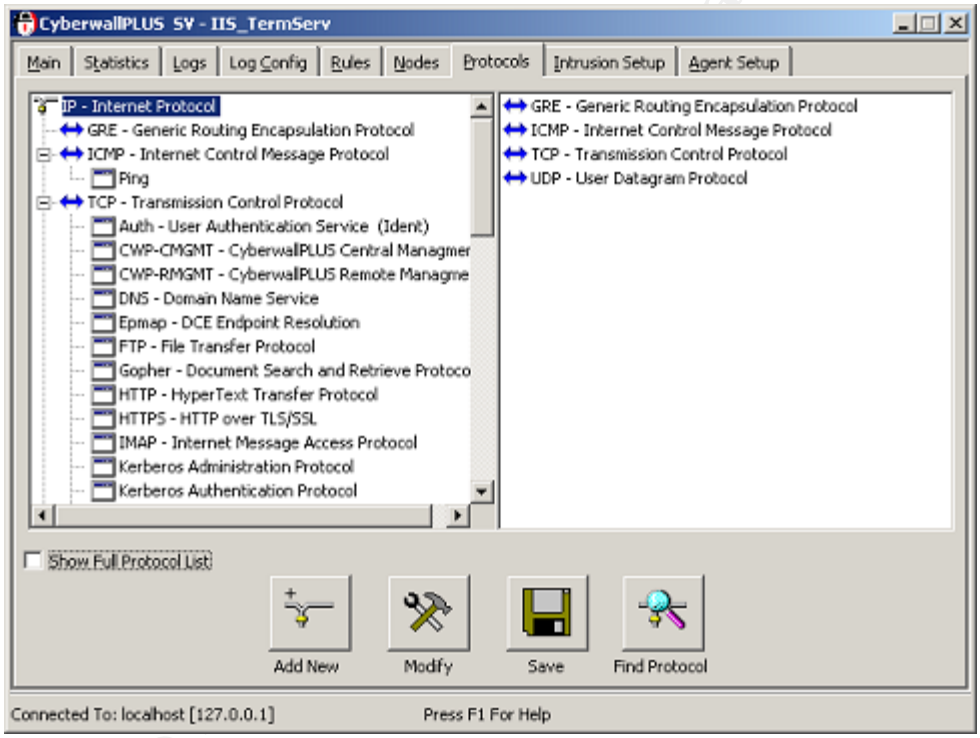


Figure 9

For security reasons some administrators find it advantageous to change the default port a protocol operates on. In an earlier example I configured a new rule set to allow Terminal Service access to the server. There are some security issues with doing this. The tool TSEnum.exe from http://www.hammerofgod.com is used to enumerate Terminal Servers. One counter measure to this tool is to change the default port that Terminal Server listens on.[7]

After changing the default listening port on the server and modifying the destination port on the client you will need to modify the port number in CyberwallPLUS. To do this, select RDP-Microsoft Terminal Server Protocol from the protocol list. Click the Modify button and in the values field change the port number to match the server and client configurations. Save the changes and you have just added some defense in depth.

Intrusion Setup Tab

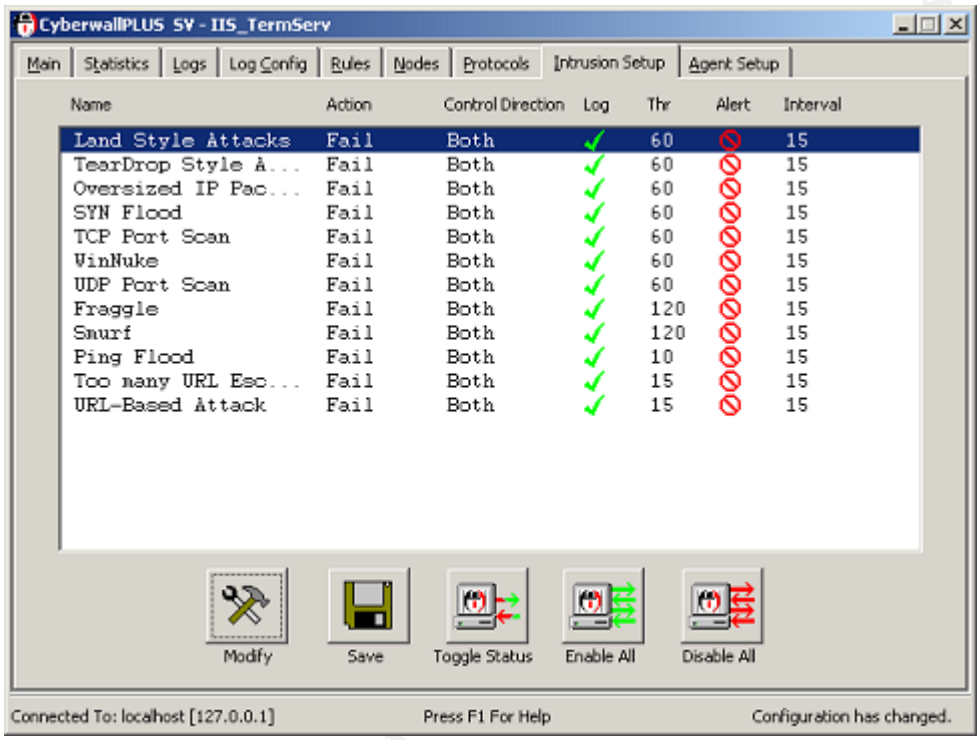


Figure 10

The Intrusion Setup tab (Figure 10) is used to control how the firewall reacts to know attack signatures. There are 12 intrusion attack names configured into CyberwallPLUS. For each intrusion there is a column for action, control direction, log, threshold, alert and interval. To modify any of the components of an intrusion, select the intrusion name and click the Modify button. I selected Ping Flood for an example (Figure 11).

The action field tells CyberwallPLUS what it should do with the packet when that intrusion is detected. Control Direction indicates if the firewall is configured to filter for incoming packets, outgoing packets, packets traveling both incoming and outgoing or to filter none of the packets. If the Send events to the Intrusion Log box is checked then this intrusion will be logged. The Threshold field indicates how many seconds the firewall will wait after it has logged an intrusion before it will log that same intrusion again. The Alerting area is for configuring email alerts for that particular intrusion. Set the interval field to the number of minutes you

desire between each alert. Be careful here because it would be easy to set this too low and create a flood of unnecessary emails in your inbox.

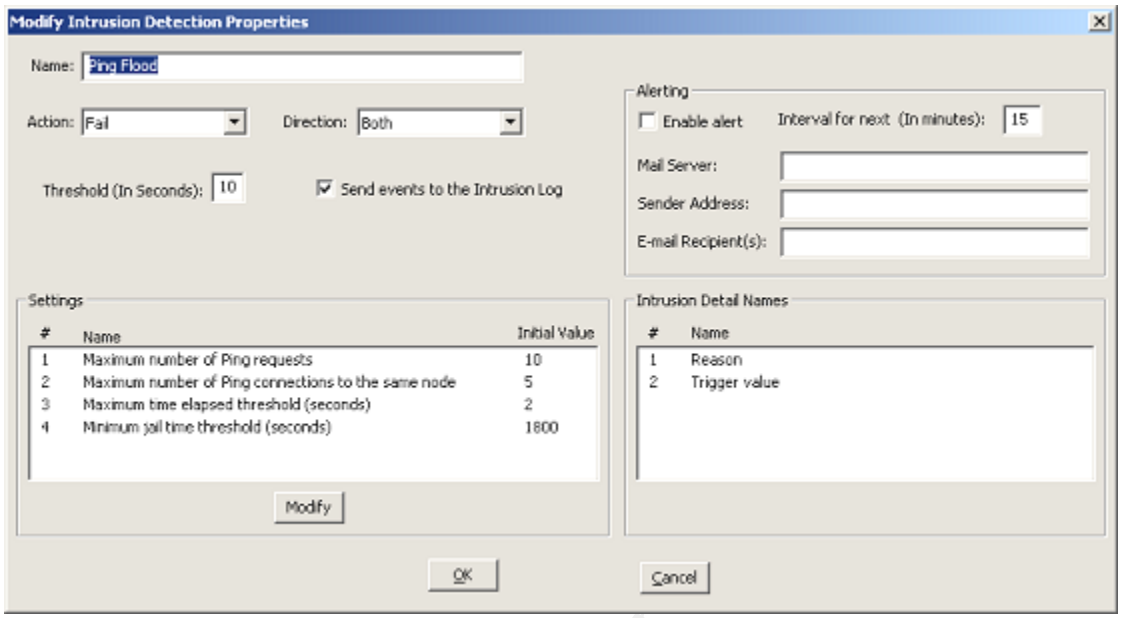
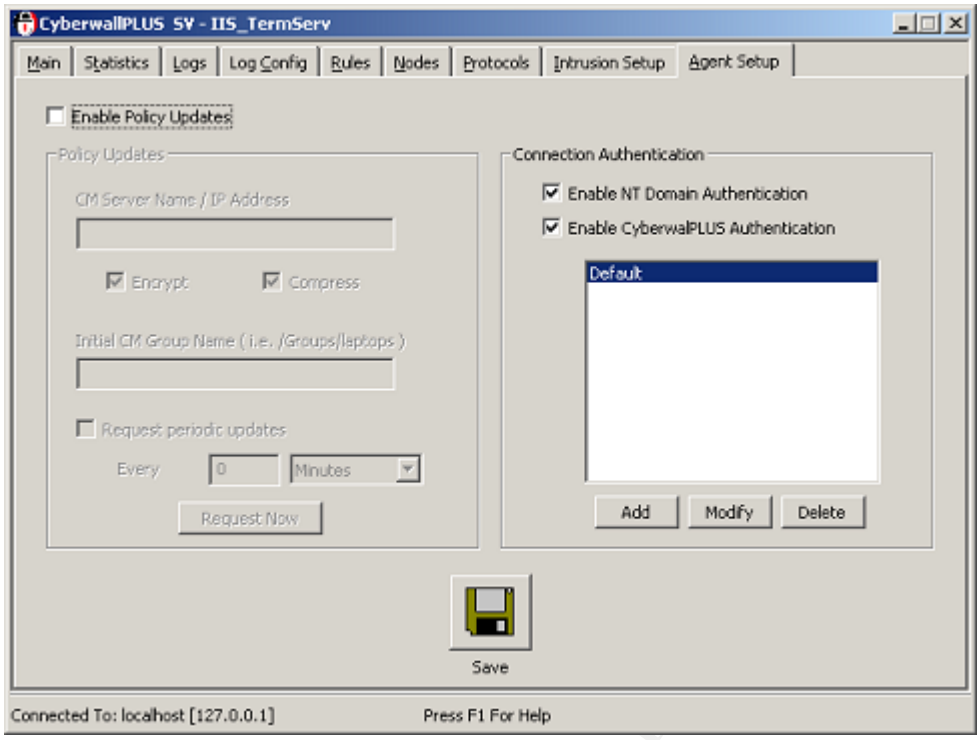


Figure 11

Back at the Intrusion Setup tab there are buttons for Toggle Status, Enable All and Disable All. The Toggle Status button will change the Direction setting for whatever intrusion you have selected. The Enable All and Disable All buttons will either select or deselect the Send event to the Intrusion Log setting for all the intrusions in the list.

Agent Setup Tab

The Policy Updates area of the Agent Setup tab (Figure 12) is not used for this setup. It is used to configure CyberwallPLUS SV to communicate with a Cyberwall Central Manager so policy changes can be pushed out.



Under the Connection Authentication area of this tab, settings for authentication type can be set. The NT Domain Authentication and the CyberwallPLUS Authentication are enabled by default. If you needed a user who was not an administrator on the local machine to configure CyberwallPLUS you could click the Add button and add a user to the CyberwallPLUS Authentication group.

Testing

To test the firewall I used a program called SuperScan v3.0. This is a simple and free program that can be downloaded from http://www.foundstone.com/knowledge/scanning.html. I scanned from my SecureSystem host which had an IP address on the same internal subnet as my test server.

I first scanned the server with no firewall enabled to show just how many ports are open on a basic install of Windows 2000 Server. I only scanned the first 10,000 ports for this demonstration. Appendix A shows the results of this scan. As you can see there were 30 open ports, some of which where giving out information that a hacker might find somewhat valuable.

My next scan was with CyberwallPLUS SV firewall enabled for a Microsoft IIS Server. Again I scanned the first 10,000 ports with the results shown in appendix B. Because the firewall was set for a web server the only ports shown as open are 80 and 443. Port 80 is for http and port 443 is for secure http.[6]

The results of my third and final scan can be seen in appendix C. Here the firewall was configured with the IIS_TermServ rule set. Since I was scanning from TrustedSystem it was allowing access to Microsoft Terminal Services which runs on port 3389.

Conclusion

According to CERT there were 52,658 incidents reported in 2001.[8] These are frightening numbers proving a properly configured and well maintained firewall is essential to any serious security effort. Because of it's ease of installation and maintenance, CyberwallPLUS is a practical choice if a security administrator is looking for a robust host based firewall. Whether it be for a stand alone server, bastion host or sitting behind a network firewall as part of a companies security in depth implementation, CyberwallPLUS may help fill a gap.

Appendix A:

```
* + 192.168.2.5   TestServer
        |___    25  Simple Mail Transfer
                  |___ 220 kramer.testdomain.com Microsoft ESMTP MAIL Service,
Version: 5.0.2195.2966 ready at  Tue, 21 Jan 2003 08:50:22 -0800 ..
        |___    53  Domain Name Server
        |___    80  World Wide Web HTTP
                  |___ HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Date: Tue, 21 Jan
2003 16:50:27 GMT..Connection: Keep-Alive..Content-Length: 1270..
        |___    88  Kerberos
        |___   119  Network News Transfer Protocol
                  |___ 200 NNTP Service 5.00.0984 Version: 5.0.2195.2966 Posting
Allowed ..
        |___   135  DCE endpoint resolution
        |___   139  NETBIOS Session Service
        |___   389  Lightweight Directory Access Protocol
        |___   443  https  MCom
        |___   445  Microsoft-DS
        |___   464  kpasswd
        |___   563  snews
        |___   593
                  |___ ncacn_http/1.0
        |___   636  ssl-ldap
        |___  1026
        |___  1029
                  |___ ncacn_http/1.0
        |___  1042
        |___  1053
        |___  1057
        |___  1058  nim
```

|___ 1068 Installation Bootstrap Proto. Cli.
|___ 1075
|___ 1080 Socks
|___ 3268
|___ 3269
|___ 3372
|___ 3389
|___ 3730
|___ 4447 N1-RMGMT
|___ 6101

Appendix B:

* + 192.168.2.5 [Unknown]
|___ 80 World Wide Web HTTP
|___ HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Content-Location: http://192.168.2.5/Default.htm..Date: Wed, 22 Jan 2003 04:29:04 G
|___ 443 https MCom

Appendix C:

* + 192.168.2.5 [Unknown]
|___ 80 World Wide Web HTTP
|___ HTTP/1.1 200 OK..Server: Microsoft-IIS/5.0..Content-Location: http://192.168.2.5/Default.htm..Date: Wed, 22 Jan 2003 05:51:20 G
|___ 443 https MCom
|___ 3389

List of References

1. Schultz, Eugene. Windows NT/2000 Network Security. MacMillan Technical Publishing, 2000. 219.

2. Webopedia. “Firewall.” September 24, 2002. URL: http://www.webopedia.com/TERM/F/firewall.html (Jan. 15, 2003).

3. Viconsoft. “What different types of firewalls are there?” Firewall White Paper. (Jan. 15, 2003). http://www.firewall-software.com/firewall_faqs/types_of_firewall.html

4. Sharma, Kapil. “IP Spoofing.” Linux Gazette. February, 2001. URL: http://www.linuxgazette.com/issue63/sharma.html (Jan. 16, 2003).

5. Snell, Mark. Hutchinson, Michelle. “Types of Firewalls.” Firewall Appliances. December 20, 2001. URL: http://www.zdnet.com.au/newstech/communications/story/0,2000024993,20262375-2,00.htm (Jan. 18, 2003).

6. Microsoft. “Appendix B-Ports and Protocols”. Exchange Server 2000 Resource Kit. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/reskit/resguide/appendb.asp. (Jan. 20, 2003).

7. McClure, Stuart *et al.* Hacking Exposed: Network Security Secrets and Solutions, Third Edition. Berkeley: Osborne/McGraw-Hill, 2001. 545-546.

8. CERT. “CERT/CC Statistics 1988-2002.” January 21, 2003. URL: http://www.cert.org/stats/ (Jan. 21, 2003).