Global Information Assurance Certification Paper

WatchGuard Firewall Appliance & System Software v 5.0

Neil Gesslein GSEC Practical Version 1.3
WatchGuard Firewall Appliance & Firebox System Software v5.0
February, 2002

Introduction
The following paper is intended as a general guide on the Configur ation of the WatchGuard firewall appliance (Also known as a Firebox) & Firebox System Software v 5.0

The axiom ""Good enough" security now, is better than "Perfect" security ...never" [i], more or less sums up the way that many harried Network Administrat ors view Information Security & firewalls in particular.

For the Network Administrator who inherited the firewall as another part of their job description, finding the time to provide the hardware and operating system (and then hardening them) before in stalling the firewall software and then configuring it correctly is a difficult and time consuming task.

The Firebox may be the device they are looking for, allowing them to focus on "keeping the trains running on time".

What is the WatchGuard Firewall appliance ?

According to Craig Simmons,

> "Firewall appliances offer perimeter based network security. Like regular firewalls they can be application gateways, packet filters, or circuit level gateways. In fact firewall appliances are just as diverse as a ny firewall product." [ii]

The Firebox itself is a dedicated network security device (shown below) which gives you the ability to be up and running right out of the box. The firewall operating system does not allow user log-ins and only supports encrypted co nnections to the Firebox.

The WatchGuard Firebox is built on a modified (Hardened) version of the Linux operating system. The fundamental design of Linux has withstood the highest levels of public scrutiny, and the inevitable bug fixes (which any network operating system requires over time) have historically been available far faster than those of the commercial operating systems. All modifications to the modified Linux kernel were released back into the public domain for analysis and comment during th e initial design process.

This process ensures that the actual kernel modifications made to the underlying operating system on which the Firebox runs received the broadest possible scrutiny.

WatchGuard firewall technology combines stateful packet filte rs and sophisticated security proxies to monitor and secure your Internet traffic.

This combination mirrors the statement below taken from "Hacking Exposed – Network Security Secrets & Solutions" [iii].

> "Two types of firewalls dominate the market today: application proxies and packet filtering gateways. While application proxies are widely considered more secure than packet filtering gateways, their restrictive nature and performance limitations have kept their adoption limited to traffic out of the company rather than traffic into a company's web server.
>
> Packet filtering gateways, or the more sophisticated stateful packet filtering gateways on the other hand, can be found in many larger organizations with high performance requirements.
>
> Many believe the "Perfect" firewall has yet to surface perhaps a hybrid of both technologies that offers the security of proxy technology with the performance of packet filtering technology."

Installation

Before installing the WatchGuard Firebox System, you need to decide on how to incorporate the Firebox into your network. This decision will determine what function each of its interfaces will perform.

External Interface

The external interface connects to an external network (most commonly the Internet) which presents a possible threat.

Trusted Interface

This interface connects to the local or internal network which you want to keep secure.

Optional Interface

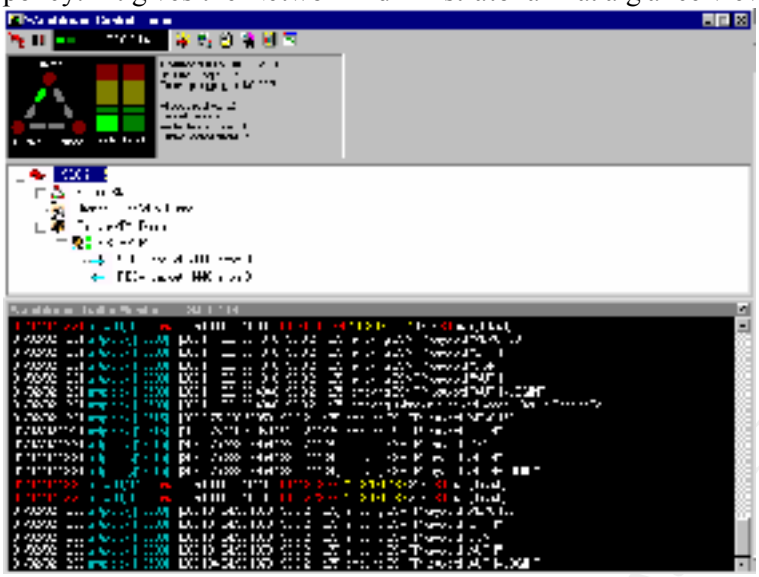
You connect this to the DMZ or to a network with servers which contain externally accessible systems or data that you wish to share with the outside world. Services such as Web, Email, FTP or perhaps dedicated dialup servers are the type of devices you may find on this interface.

Once you have decided on how you will incorporate the Firebox into your network, it's time to install the WatchGuard Firebox System Version 5.0 software. Located on a separate management station, it runs on Microsoft Windows 98, Windows NT 4.0, or Windows 2000 and comes in varying encryption levels from basic encryption (40Bit) all the way to strong (128Bit).

The Firebox System Version 5.0 software comes on the CD provided with the Firebox or can be downloaded from the WatchGuard site once you have registered. Installation is straight forward, simply follow the prompts when you select the wizard, enter the 10 digit license key and it's done. Now it's time for the fun part, configuring your Firebox to meet your requirements.

WatchGuard Control Centre

WatchGuard Control Centre is the heart of the Firebox System, it is a toolkit of applications run from a single location, enabling you to configure, manage, and monitor your firewall policy. It gives the Network Administrator an "at a glance view" of what is happening.



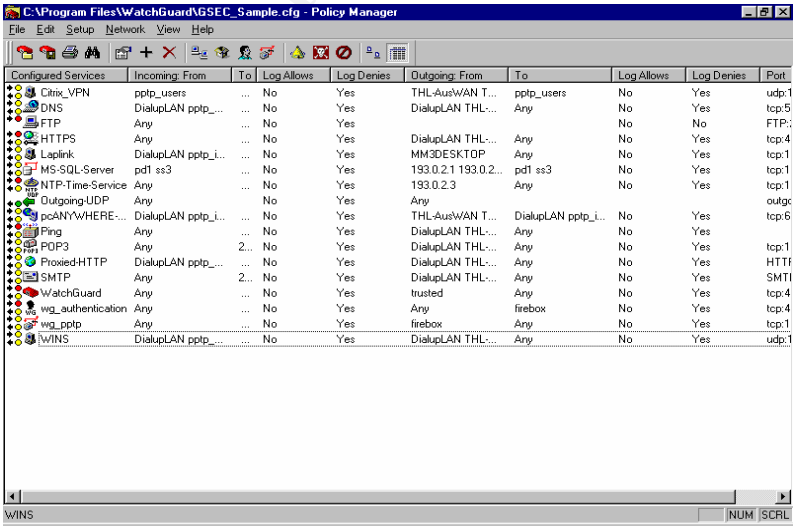
The Control Centre allows you to configure your firewall policy safely from inside and or outside of your secure network. Secure configuration and management of your network is possible because the Firebox uses strong encryption (3DES) to secure your management session. You can manage your network security from anywhere, at any time.

(In the image above you can see at a glance that there is one Remote User VPN user connected, 29 connections in total, that it has been up for over 7 days, there are currently no branch office VPN's in use and that it is currently logging to the log host at 193.0.2.7 **{Note IP addresses in all screen shots have been modified}**).

We will now look at the utilities that come as part of the Control Centre in more detail.

Policy Manager

A firewall policy is only as good as the network or system security policies that drive it. A well-planned security policy specifies which computers can communicate with external entities and by which methods. It ensures that content sent via protocols that can hide potentially destructive content types are examined (See S MTP Proxy section below). It employs encryption where communication could be intercepted (See VPN section below), and secure strong authentication. A combination of well conceived firewall and security policies leaves no holes in the perimeter defenses except for those which are created to allow authorized users and services to pass.



Policy manager has an easy to use interface and includes a large list of predefined filters and proxies and provides for the addition of custom

rules. It is used to design, configure, and manage the electronic portion of a network security policy.

WatchGuard employs a combination of dynamic stateful packet filtering and security proxies to control and monitor the flow of IP packets through the Firebox. The extra security of proxies is applied to the protocols that are the most vulnerable, protocols such as SMTP, FTP and HTTP.

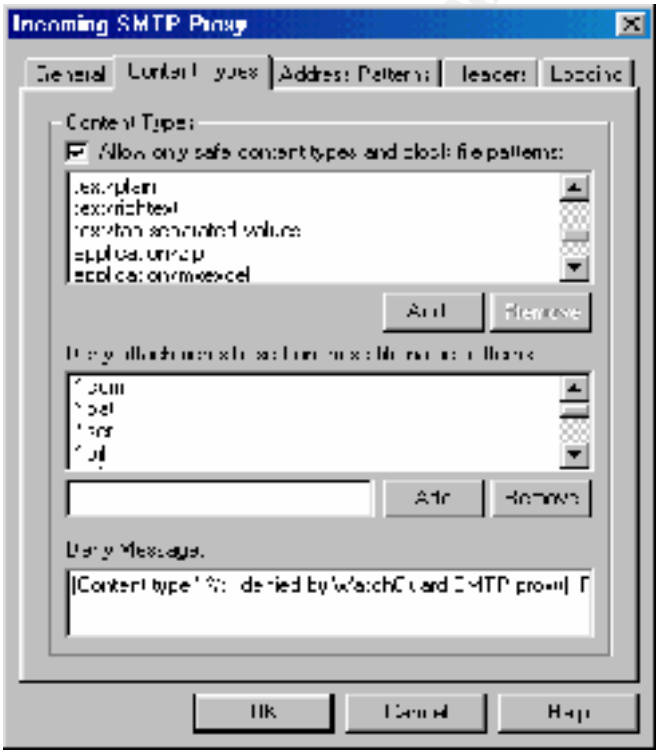
(The policy open in the picture above is more or less a graphical representation of a security policy being enforced. It shows defined rules for DNS, FTP and HTTPS etc.)

Configuring or adding a service
As an example we will examine just one rule from the large range of predefined protocol options in detail, the SMTP Proxy service rule.

Configuring or adding a service, in this case the SMTP Proxy Service is simple. In policy manager select the add services button on the toolbar and scroll down to SMTP Proxy in the Proxies folder.

The way in which the SMTP proxy works is best explained in the 2 paragraphs below taken from the WatchGuard web document titled "Smart and Fast – What to look for in your next Firewall" [iv]

> "A mail proxy examines all SMTP packets to determine whether the payload contains forbidden content types, such as executable programs or items written in scripting languages. The SMTP proxy knows these content types are not allowable; a packet filter does not. Advanced WatchGuard security proxies examine not only one packet at a time, but entire groups of related packets, or data streams, which gives clearer context for deciding whether content is safe or not. Security proxies work at the application level, whereas IP packet filters work at the protocol level. This means that each packet a proxy receives must be stripped of its network wrapping, analyzed, processed, and re-wrapped so it can be forwarded to its destination. This adds layers of complexity and processing well beyond the packet filtering process.



The SMTP proxy limits several potentially harmful aspects of email. The proxy scans the content type and content disposition headers, and then compares them against a user-defined list of known hostile signatures. Email messages containing suspect attachments are stripped of their attachments and then sent to the intended recipient. The proxy can limit message size

and limit the number of message recipients. For example, if the message exceeds preset limits for message size or number of recipients, the Firebox refuses the mail."

Simply put the SMTP Proxy filters all incoming content looking for file types known to be doubtful which will then be stripped before they ever reach the internal network. It acts as another layer of defense before the packet reaches the anti-virus software (You have up to date anti virus software on your hosts don't you?) Specific attachment types such as .exe, .com, .vbs or custom extensions can be added to the denied attachments list. A message is sent to the recipient stating that a particular file type was denied and what content type it was.

The Firebox allows certain headers by default. These are listed on the Headers tab of the Incoming SMTP Proxy Properties dialog box. You can add more headers to this list, create your own custom ones or remove headers from the list. The outgoing SMTP Proxy dialog box is used to set the parameters for traffic going to the outside world.

SMTP masquerading converts an address pattern behind the firewall into an anonymous public address. For example, the internal address pattern might be inside.secinfo.GSECsample.com which would be converted to their public address GSECsample.com.

Enable the check box marked Masquerade MIME boundary strings so that the firewall converts MIME boundary strings in messages and attachments to a string that does not reveal internal host names or other identifying information (A form of egress filtering [v]).

Firebox Monitors

Firebox Monitors combine a set of monitoring tools into a single user interface.

The Bandwidth Meter tab displays current bandwidth usage for the selected interface.

The ServiceWatch tab graphs the number of connections by service. Services can be added or removed as required. (You can see HTTP,SMTP,FTP & Citrix connections shown here on the left hand side.)

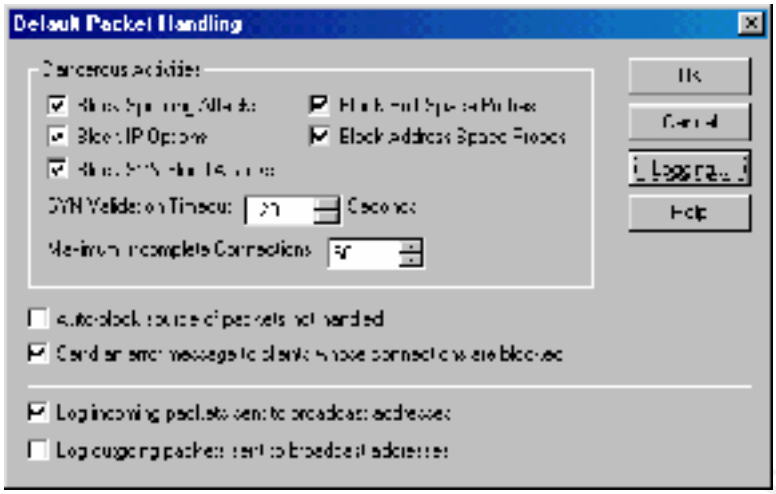
The Status Report tab provides a number of statistics on Firebox activity such as Firebox uptime and Firebox System software version etc.

The Authentication List tab displays the host IP addresses and user names of everyone currently authenticated to the Firebox.

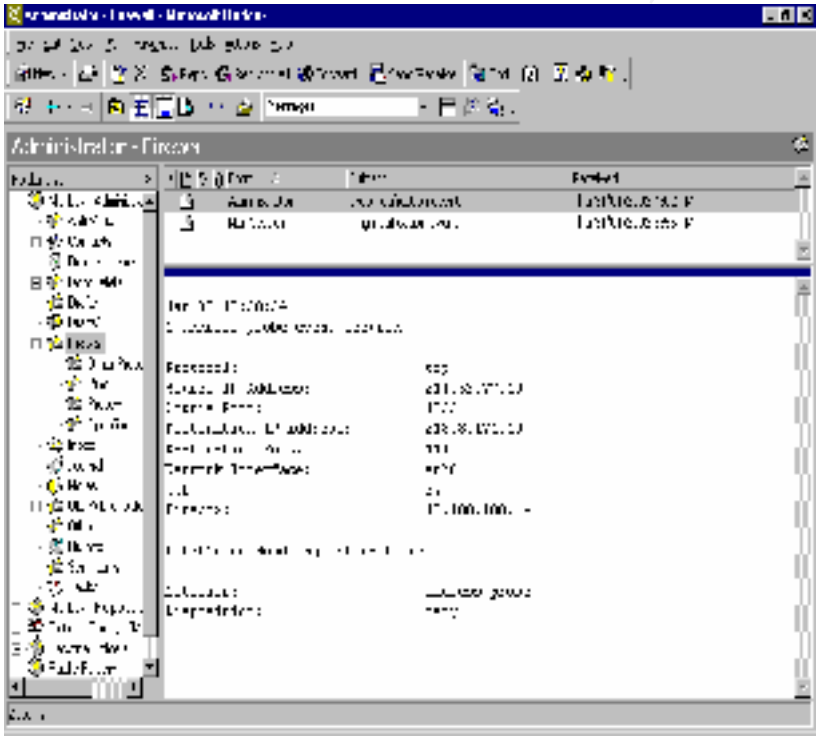
The Blocked Sites List tab lists the IP addresses of any external sites that are temporarily blocked. (Currently showing one blocked site).

Logging & Default Packet Handling

Firebox System software provides the ability to specify which types of events are logged, for each individual service (DNS, SMTP, FTP SQL - Service etc.), and for traffic heading in or out of the network (Egress Filtering logs). Logging parameters can be adjusted depending on the logging host's capacity and the required file size. Logs are not constrained to a set file size that fills up and begins overwriting if unattended or perhaps worse still, not logging at all. You are able to log data by various parameters such as host to host connections, Internet activity, active times of day, User ID or a specific host's activity.



Logviewer is the tool that displays a static view of the lo g data, which you can filter by type, search for keywords and fields, and print and save to a separate file.



An additional option that keeps the harried Network administrator up to date on what is trying to get through the defences is the logging & notification within the "Default packet handling" option (Above).

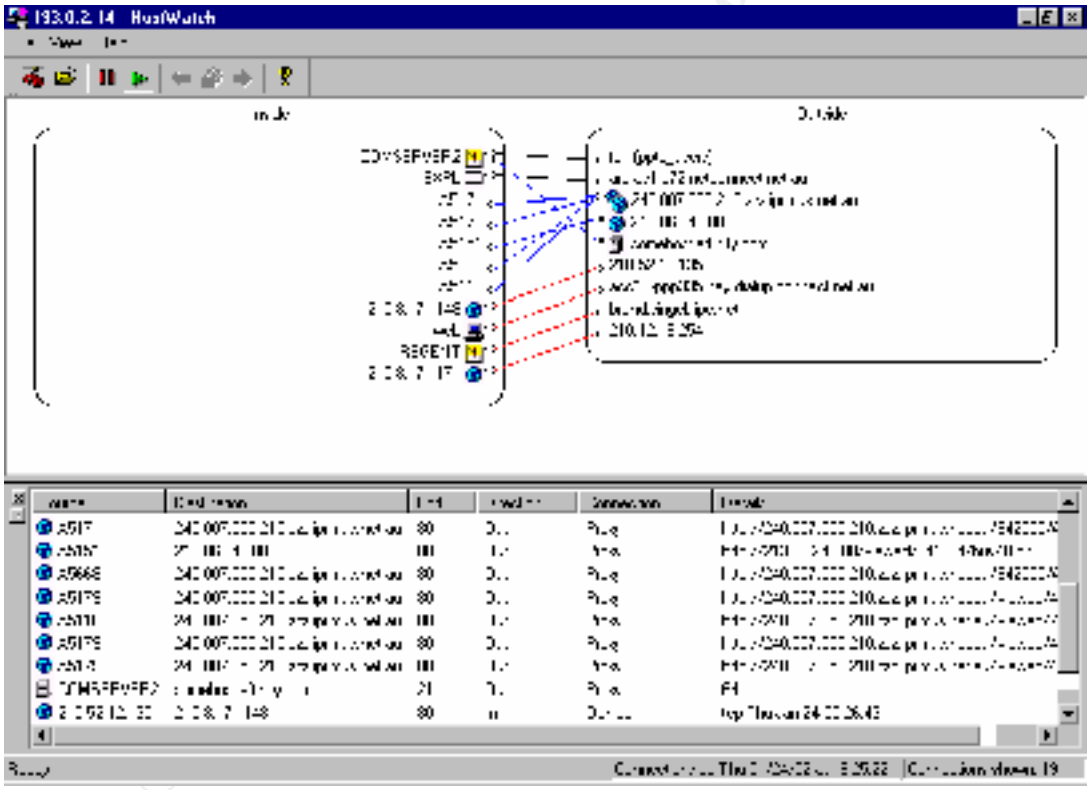
(As an example on average our current Firebox has been averaging approx 150 – 200 port probes and ICMP scans per day over the last 6 months. The screen shot above shows the format of the email alert triggered by a probe attempt. These alerts are logged by default however the email option can be enabled or disabled as required. When you witness how many probe, ping & scan notification events occur, at all hours of the day and night you know the bad guys don't always work normal hours.)

These alert messages are a good metric to show management just what is happening at the perimeter defences and can provide daily, weekly & monthly statistics of the total number of probes.

Be aware that the more options you log the greater the amount and size of log files you generate. To configure alert options, go to **Setup** on the menu and select **Default packet handling** then **Logging** in policy manager.

If you wish to view a log file or data in a period that cove rs more than one log file you can "Roll" them together via the menu options from within the Security Event Processor (Included as part of the default install). The Security Event processor utility provides the ability to schedule reports (See Reports secti on below) define notification settings and to specify when log files "Roll". Log files can be set to "Roll" upon reaching a preset maximum number of entries, by a daily, weekly, monthly or custom time basis or when the file reaches a designated size.

HostWatch
Displays active connections occurring on a Firebox in real time or represents the connections listed in a log file. HostWatch plays back a previous file for review or displays connections in real time, as they are added to the current log file. This tool allows the systems administrator to view and monitor all web traffic in real time.



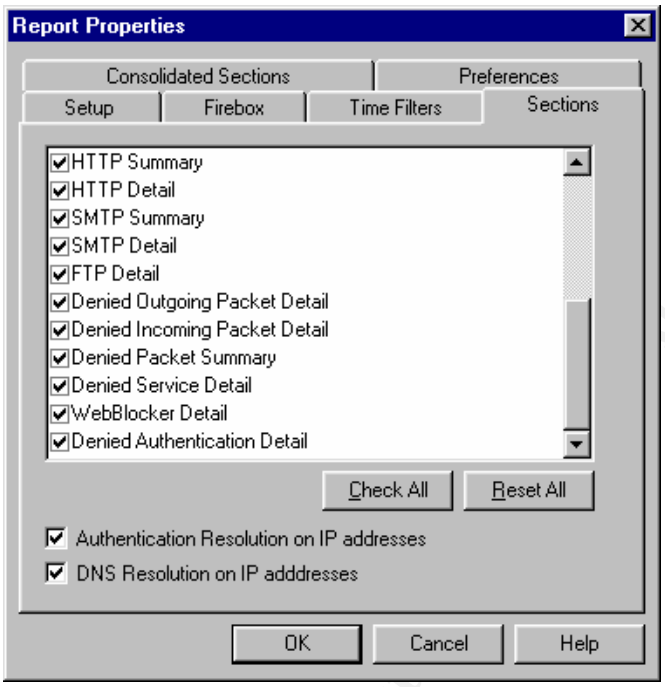
(The screen shot here shows not only allowed and denied (Red) traffic, it's destination and port etc, but in this case highlights the fact that there was a rule misc onfigured. The PPTP user connecting at the top right of picture then has an FTP outbound connection. This is not normal as our policy does not allow FTP traffic outbound.).

Once again this is an excellent metric for highlighting to management just what is happening at the gateway. During the CodeRed outbreak in 2001 the denied listing was consistently going off the scale.

Hostwatch can be used to replay events. Within Hostwatch select a log file for the period you want to replay (If necessary Roll several files into one) and select open. You can now replay events as they happened giving the Network Administrator an opportunity to review what has been happening. As in the screen shot above it can be utilised to confirm that something out of the norm (Outside the boundaries of the defined security or firewall policy) has in fact happened.

Historical Reports

The Historical reports tool creates HTML reports from the log files provided. It provides a visual representation of log data useful for reviewing, monitoring and troubleshooting Internet access and usage. It is an excellent tool for providing metrics to upper management on bandwidth usage, most active host, most active site etc.



It can report on which user has been browsing sites outside the boundaries of the corporate acceptable use policy (WebBlocker covered in next section). The Historical Reporting tool offers custom and standardized reporting options to summarize your network activity. Create custom reports or select one of a large variety of standardized predefined reporting options. The Security Event processor utility provides the ability to schedule reports on a daily, weekly, monthly or custom time basis and they can be saved to file or launch Internet Explorer automatically on completion. As with the Logviewer once again you can specify that multiple logs can be "Rolled" and these can then be directed to the output of your choice, HTML chart, graph, text file, or an export file for integration directly into WebTrends. [vi]

A cross section of predefined reports supplied include but is not limited to the following;

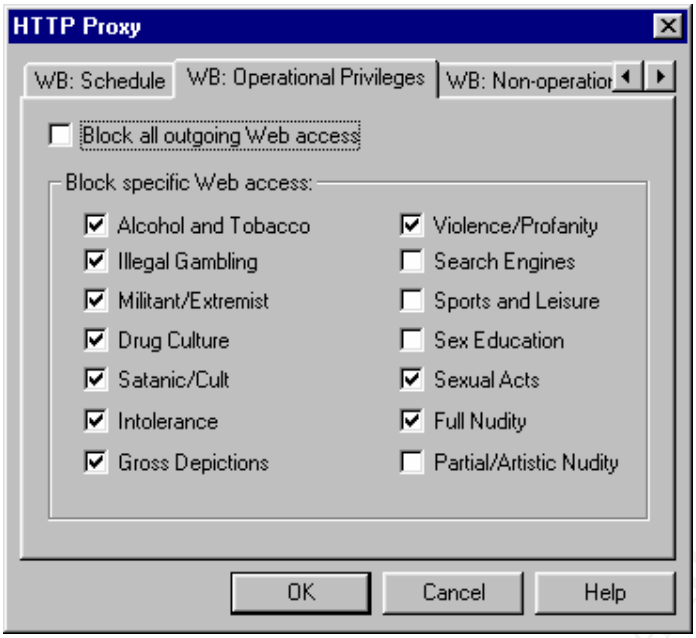
Authentications Denied Service Detail, Denied Service Summary, Firebox Statistics
FTP Detail, FTP Summary, HTTP Detail, Host Summary, Service Summary
Session Summary, Denied Authentications, Denied Packet Detail or Denied Packet Summary.

WebBlocker

WebBlocker URL filtering enables the Network Administrator to prevent users from squandering organization time and resources on Web-based entertainment inappropriate to your corporate goals or in contradiction of your corporate acceptable use policy. An administrator can restrict Web surfing based on type of content (e.g. Illegal gambling or Satanic sites) and time of day, and to assign those rules to groups or individuals.

WebBlocker relies on a URL database built and maintained by SurfControl. [vii] This database is segregated into 14 distinct groups or operational privileges and are applied within the

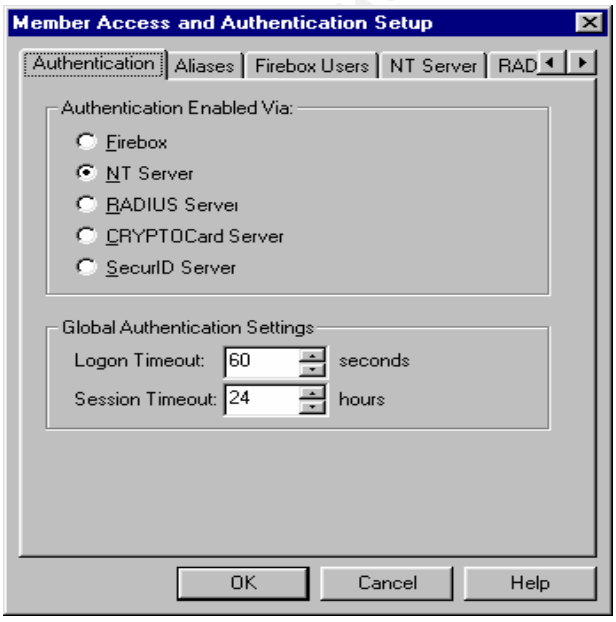
HTTP Proxy rule. It also contains a scheduling function for operational and non operatio nal hours.



The database is copied to the WatchGuard WebBlocker site at regular intervals. The WatchGuard Security Event Processor is automatically configured to download the most recent version of the database from the WatchGuard WebBlocker site over an authorized channel. In turn, the Firebox regularly queries the WatchGuard Security Event Processor for changes and, when appropriate, downloads a new version and generates a log entry to show the transfer.

If the database is either corrupted, incompletely retrieved, or in any other way incomplete, the Firebox does not load it. It repeats the attempt until it completes a successful transfer. When you restart your Firebox, all Web access is blocked for a brief period of time. Users might receive the error message "Database not loaded" until the Firebox downloads a database.

You can manually force a download of the latest blocked URL database from WebBlocker.WatchGuard.com using a DOS utility called dbfetch which is part of the default install. (Note when the "Database not Loaded" event occurs , WatchGuard goes into fail over mode - **NO** web access is permitted until it is successfully downloaded or WebBlocker is disabled from within the HTTP rule via the Policy manager.)



Along with WebBlocker the Firebox h as the option to selectively block sites and ports and also allows specific exceptions should you need to do so. These options are also available via the Policy Manager toolbar.

VPN and Authentication

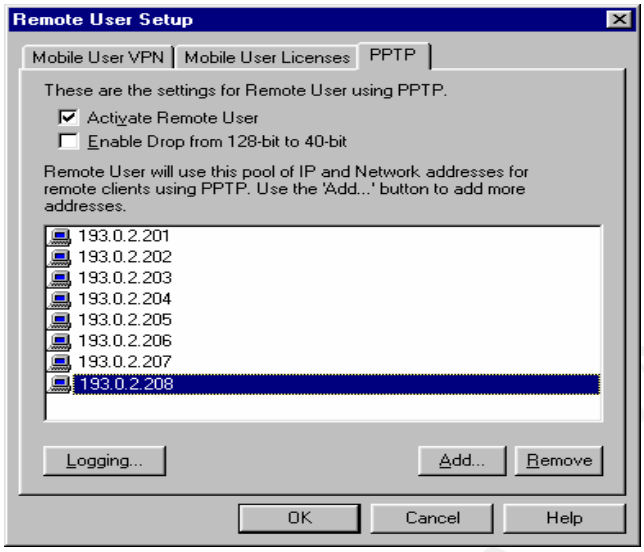
WatchGuard is built around the basic premise that unle ss an external user has authorization for a specific activity, then that external user is denied an inbound connection.

WatchGuard has the ability to authenticate a user against different types of authentication servers such as SecurID or RADIUS or it's o wn built in authentication service (See picture).

The WatchGuard VPN's are managed by the Firebox as it ensures that the VPN is in step with the security policy and ensures that a VPN tunnel, for example, does not clash with any rules in the firewall policy, that specifies what service is accepted or denied.

It provides consistency of services by ensuring that adding a service or a tunnel does not breach security.

It applies the Firewall policy to all VPN connections. For each VPN you can limit access to servers, services, and the networks available to those tunnels to the minimum level necessary to meet your needs. This granular application of rules is necessary as you are assigning an implicit trust to every user coming through a VPN tunnel. As far as the network is concerned the VPN user is no different than an employee working on the LAN.



By default WatchGuard comes with an unlimited license for the PPTP Remote VPN users. These VPN tunnels are kept secure by using 128Bit encryption (See picture) but you have the option of purchasing the Mobile User VPN client license which supports the IPSec protocol.

Alternatively it is also possible to connect multiple Fireboxes together using the Branch VPN option (Once again a license is required).

Livesecurity Subscription – Keeping WatchGuard up to date

Over time both the Firewall policy and software ages, and therefore becomes more vulnerable to new threats and exploits. The busy Network Administrator must somehow divide his or her time between local administration tasks, and the effort to keep the network and perimeter secure by obtaining patches, disabling vulnerable services and keeping abreast of current trends and threats. Ideally, a Firewall appliance will have an auto updating mechanism which downloads software updates and patches and information about emerging security threats to keep the entire networked environment current and therefore, more secure.

This is the where the Livesecurity subscription comes in (It is free for the first year with the purchase of a Firebox).

The paragraphs below taken from the official WatchGuard site [viii] details the advantages of this service.

> **LiveSecurity Broadcasts.** WatchGuard's Rapid Response Team constantly monitors the Internet to identify emerging threats, and then delivers alerts that tell you specifically what you can do to address each new menace.

Threat Responses. Detailed information on the largest and most far -reaching security vulnerabilities as they happen and what WatchGuard is doing to help you keep y our network secure.

Virus Alerts. Our strategic alliance with McAfee gives you real -time virus alerts and specific information on how to protect your systems.

Information Alerts. Timely analysis of breaking Internet security events combined with instructions on how to keep your network secure.

Expert Editorials. A network of top security experts offer their views on Internet security and provide a source of continuing education.

Support Flashes. Technical tutorials offer tips for managing your Watch Guard products.

Summary

While by no means being an exhaustive review of the WatchGuard Firewall Appliance, it is hoped that this paper provides the reader with sufficient information on the features of the Firebox and it's associated software. With its c ombination of stateful packet filters and sophisticated security proxies for monitoring and securing your Internet traffic it is an effective tool to control access into and out of your network/s.

Not all companies and sites can afford the luxury of or ha ve the necessary resources to have a full time firewall or information security professional.

For the busy Network Administrator that inherits the responsibility of protecting the corporate perimeter, the WatchGuard Firebox may be just what the doctor or dered.

References

"Top Eleven Reasons" The Firewall Systems top 11 reasons to consider using the WatchGuard Firebox as your internet protection appliance.
URL http://www.firewalls.com .au/default.asp?P=eleven.inc (Febuary 2002)

WatchGuard V5.0 User Guide. A White Paper Prepared by WatchGuard Technologies, Inc. (PDF Format)
URL http://www.WatchGuard.com/products/wgls.asp
(Available from the Brochures option, requires free registration) (Febuary 2002)

---

[i] Fred Avolio is a member of WatchGuard Technologies LiveSecurity Advisory Council, a nd writes a column for their LiveSecurity Service. This is his "Security Axioms Page"
URL http://www.avolio.com/axioms.html (Febuary 2002)

[ii] "Firewall Network Appliance" Simmons, Craig
URL http://rr.sans.org/firewall/fw_netapp.php (October 10, 2000)

[iii] Mcclure, Stuart & Scambray, Joel & Kurtz, George
Hacking Exposed Network Security Secrets & Solutions

Osborne / McGraw-Hill
Berkley, California 94710 USA (1999) : 314

[iv] "Smart and Fast – What to look for in your next Firewall" A White Paper Prepared by WatchGuard Technologies, Inc. (PDF Format)
URL http://www.WatchGuard.co m/products/wgls.asp (Available from the white papers option "requires free registration") (August 2001)

[v] "Egress Filtering" Global Incident Analysis Centre – Special Notice
URL http://www.sans.org/y2k/ egress.htm (Febuary 29, 2000)

[vi] URL http://www.netiq.com/support/default.asp for further information regarding this add on product called Webtrends Firewall Appliance Analyzer v4.0 (Febuary 2002)

[vii] URL http://www.surfcontrol.com/oem/test_a_site/ SurfControl supplies the WatchGuard WebBlocker database. It contains more than 65,000 IP addresses and 40,000 directories and this page allows you to test if a site is on the list. (Febuary 2002)

[viii] "LiveSecurity Service"
URL http://www.WatchGuard.com/products/lsservice.asp
("Requires free registration") (Febuary 2002)

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event