SANS Institute
Information Security Reading Room

Configuring Watchguard Proxies: A Guideline to Supplementing Virus Protection and Policy Enforcement

Alan Mercer

Copyright SANS Institute 2020. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Configuring Watchguard Proxies:

A Guideline to Supplementing Virus Protection and Policy Enforcement

By Alan Mercer
GSEC Assignment v. 1.4b
Option 1
Sept 5, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

TABLE OF CONTENTS

TABLE OF FIGURES

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

ABSTRACT:

Recent and well-publicized viral outbreaks and data compromises have raised our awareness of the need to reduce systems exposure to known and unknown dangers. The current state of viral code development is rapid and is beyond the scope of anti-virus (A/V) software alone to prevent new and previously unknown attacks. Additionally, A/V software may fail to function, update, or become disabled on systems behind the firewall. End-users that disregard Acceptable Usage Policies (AUP) may execute or install unauthorized applications. This exposes systems and sensitive data to others, whether intended or not, and may create corporate liabilities and cause systems downtime. Creation of a prophylactic defense is key to reducing risk. This paper focuses upon the layered use of the Watchguard Live Security System (LSS) proxy services to mitigate these risks and reduce exposure. The key to properly configuring LSS proxy services without hampering system function is a strong understanding of organizational policies and these risks. A discussion of the effects and ramifications of using proxied services on the Watchguard and methods of minimizing these effects and weaknesses of the approach are included.

The configuration of commonly used stateful proxy filters on the current Watchguard Firebox II and III appliances using LSS 6.2 SP1 are described. Watchguard released 7.0 during the writing of this paper; changes in this version are not covered. Other Watchguard appliances are not discussed since they lack proxy services or vendor support. Emphasis is placed upon the use of content filters and egress policies that enhance defenses against viral code and support AUPs. Defenses that effectively reduce the impact from new attacks using exploits such as those used by Nimda, Klez, and other blended threats are presented. Other functionality of the Firebox is included for comparative purposes; details of those functions are not topics for this paper. Security concepts contained herein are applicable in part or full to many proxy service devices and applications not discussed in detail in this paper. The use of content filtering proxies in the Firebox units goes beyond simple port filtering; it provides a multi-level defense that effectively supplements other security measures and helps create a defense-in-depth.

MALWARE AND POLICY, THE ISSUES:

In a perfect world, all systems would be fully patched, anti-virus software would automatically detect all malware, and all users would adhere to policy. Unfortunately, this is rarely the case. Deploying patches on hundreds or thousands of systems is time consuming and requires testing before deployment to ensure systems stability and functionality. New viruses are discovered daily, with thousands of systems becoming infected in the hours before new signature files are released and deployed [1]. A/V software and AUPs are the equivalent to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

No Trespassing signs. While most heed the sign, a few seek to violate the sanctity sought by the poster of the sign. Malware authors seek to disrupt or even control data and systems, while some end-users seek to circumvent policies for their own pleasure or benefit, regardless of the impact upon other systems and users. Even responsible users may inadvertently violate policy. Discovery, diagnosis, and correction of vulnerabilities take time. This time increases your risks by benefiting the party that seeks to exploit your vulnerabilities. Both A/V software and users need supplementary assistance to effectively function and adhere to policy [2]. Minimizing risk by layering defenses is one method of improving security.

We can enhance A/V software measures and enforce policy by implementing rules into the proxy services of the Watchguard LSS. Effective rules are based upon organizational business and technology policies, coupled with the concept of minimum required access. Neither can be accomplished unless the business requirements of the organization and its policy are fully understood. Nor can business change be accommodated by a rigid and inflexible solution. Understanding the vulnerabilities and your exposure in the context of your environment is required. Risk assessment must be mandatory and ongoing; change is the only constant we can count on. In addition to the above factors, alternative solutions and available resources must be considered when configuring the proxies in the LSS.

ASSESSMENT:

Identification of key business requirements and policies are the first step towards creation of a rule set for the LSS proxies. What vulnerabilities are exposed due to the access requirements of these needs? Can the Watchguard proxies minimize this risk? Can other existing systems offer a more effective solution? Can an acceptable performance level be maintained? Are there adverse effects upon systems availability, change capacity, or maintenance costs? For demonstration purposes, the following basic considerations are answered for developing a rule set for the Watchguard.

BUSINESS REQUIREMENTS:

Do your users require unrestricted access to the Internet?	No
What specific external access user requirements exist?	Web-browsing, e-mail, DNS.
Do certain users or systems have broader requirements?	Yes, VPN, NTP, FTP
What file types do internal users require for their applications?	Microsoft Word, Excel, Powerpoint Adobe Acrobat files HTML, ZIP files JPEG and GIF images
Of those file types, are any shared or obtained externally?	All permitted
Do external parties require access your systems?	Yes
If so, what is the minimum access required?	E-mail exchange Intranet web use

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Technology Policy:

Does a policy exist?	Yes
Does it define restrictions on types of Internet use?	Yes
Does it restrict downloading of files from the Internet?	Yes
Does it clearly identify permissible downloads?	Yes
Does it restrict the nature or content of Internet sites visited or files transferred?	Yes
Are software application usage standards defined?	Yes
Are unapproved applications prohibited?	Yes
Is an anti-virus policy in place requiring use of current A/V software	Yes
Does the policy provide for monitoring of use and enforcement of restrictions?	Yes
Does the policy provide for exceptions to accommodate business requirements?	Yes

Determining Minimum Required Access:

In this basic example, a strong policy exists that permits the organization to implement and monitor technology use. The right to create restrictive rule sets that limit access and activities is based upon this policy. Next, we examine the business requirements for access. From this we see that internal users and systems require HTTP/HTTPS access (tcp ports 80 and 443). Other services such as SMTP (tcp port 25), FTP (tcp port 21), DNS (tcp and udp ports 53), and NTP (tcp and udp ports 123) are also required by select systems and users. Four of these services may be directly controlled by Watchguard proxies (figure 1). These are HTTP, SMTP, FTP, and DNS. Figure 2 presents the sample network for this demonstration. This network diagram aids in identification of systems requiring specific TCP/IP services other than HTTP.

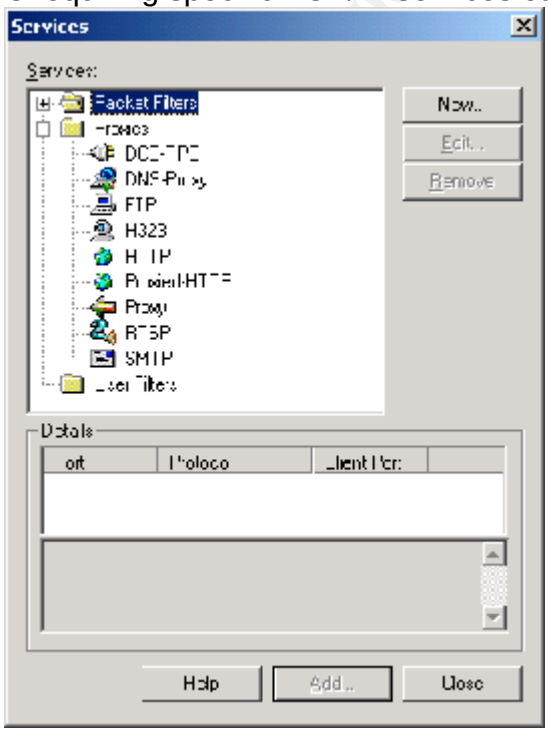

Figure 1 - Watchguard LSS Proxies – Screen capture from Watchguard SMS Utility.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

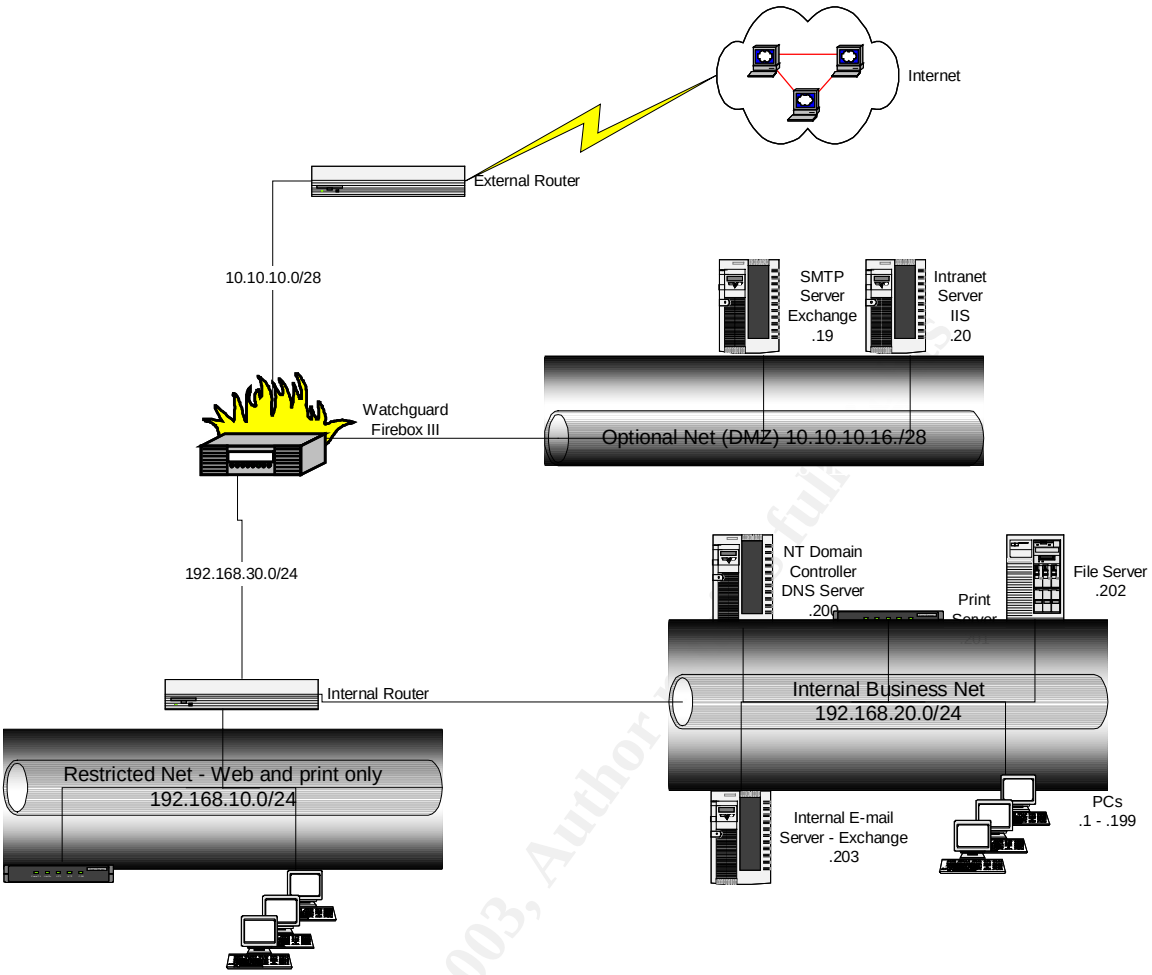

Figure 2 - Sample Network

A common Microsoft network configuration will be used for the demonstration network. The use of Windows servers on two interfaces of the Firebox means that ports commonly used by Microsoft services must pass through the firewall in a controlled manner. Traffic between these servers requires SMB services on tcp ports 139 and 445 and udp ports 137, 138, and 445, and RPC services that originate on port 135. SMB is controlled via a LSS port filtering mechanism. A Watchguard proxy as seen in figure 1, may also control RPC. Other needed services include the POP3 (tcp port 110) and AUTH (tcp port 113) for external e-mail retrieval and authentication may also be controlled via LSS packet filters. Packet filters are not discussed in detail later in this paper, as they do not contain the content-filtering mechanisms of the proxy-filter services of the LSS that are the subject of this paper. However, similar to the proxy filters, access may be restricted on packet filters via IP address permissions and explicit denials to all directional traffic. The following table lists the assessed minimum required access that will be used to apply inbound and egress address filtering by required service along with the inspection and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

process handling rules, in order to support the AUP and protect from malicious code.

Service	External	DMZ (Optional)	Internal
Proxies			
HTTP	Intranet users	Intranet Servers	All clients
SMTP	Mail Servers and clients	SMTP Mail Server	None
DNS	None	SMTP and IIS Servers	None
FTP	None	IIS Server	Select Users
RPC	None	All MS Servers (Internal)	All MS Servers & Select Users (Internal)
Packet Filters			
HTTPS	Intranet users	Intranet Servers	All clients
NTP	None	All MS Servers	Domain Controller
SMB	None	All MS Servers (internal)	All MS Hosts (Internal)
POP3	Mail Clients	SMTP Server	none
Auth	Mail Clients	SMTP Server	none

Vulnerabilities and Risk:

The five proxies to be discussed correlate directly to the five of the top ten successful attack modalities reported by TruSecure for the second quarter of 2002 [3]. Four of these address issues reported in the top five attack vectors of the same report. Gerald Post and David Anderson state that "There are three major security issues: (1) unauthorized disclosure of information, (2) unauthorized modification, and (3) unauthorized withholding of information" [4]. Risk should be assessed within this context when formulating policy and security rules. Each port or service permitted through the firewall will expose an organization to one or more vulnerabilities by exposing an access point to the protected network. As shown above, commonly required services are amongst the most vulnerable to attack. The proper configuration of Watchguard proxies mitigates this risk through controlled access of traffic through the firewall.

Both vendors and security organizations provide warning of vulnerabilities in software and hardware through the issuance of advisories that detail the nature of the flaws. One such advisory was released on July 16, 2003 by Microsoft warning of multiple and critical vulnerabilities in their implementation of RPC [5]. In early August, thousands of computers were compromised at several large universities [6]. On August 11, 2003, less than one month following the Microsoft advisory, the W32.Blaster.Worm ran rampant through the Internet infecting hundreds of thousands of unprotected hosts [7]. Recent research presented by Gerhard Eschelbeck at the Black Hat briefings shows that only 50 percent of vulnerable systems are patched for critical vulnerabilities in each 30-day period subsequent to public knowledge of the issue. Further evidence was presented that exploits become available within 60 days for 80 percent of all vulnerabilities [8]. This "half-life" analogy infers that 25 percent of all systems are still exposed and vulnerable to most critical vulnerabilities even after two months

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

have passed. Furthermore, after the same period, there is a four to one probability that an available exploit exists. Twenty-six percent of respondents reported a virus-related disaster in a 2002 ICSA survey. This survey defined a virus-related disaster as: "an incident in which 25 or more machines experienced a single virus on or about the same time" or "causing their organization significant damage or monetary loss" [9]. These issues demonstrate the need for rapid response tactics to new issues. The proper configuration of Watchguard proxies permits rapid mitigation of this risk through flexible and controlled access of traffic through the firewall.

Other Considerations:

Other alternatives to using Watchguard proxies may exist within an organization and may provide a more effective or efficient solution. Use of proxied services does reduce performance by throttling network throughput. For many organizations, this may not be a concern as limited bandwidth on their Internet connections is the primary bottleneck. Reliance upon a single device creates a single point of failure. Three advantages exist to using the Watchguard LSS proxies to reduce risk by evaluating content when compared to simple port filtering. These are: the logging of content-related actions by the firewall; rapid implementation of new restrictions or filters to address new vulnerabilities; and to provide redundant protection to alternate solutions. By implementing redundant rules on the Watchguard that exist on other devices, exceptions should not occur. If they do occur, this signals a failure of the primary security mechanism to properly block unauthorized or inappropriate network activity. Using the Watchguard as a secondary or tertiary safeguard reduces the load on the Watchguard and minimizes the performance impact of proxied services in the LSS. However, it is the flexibility and ease of configuration that makes the LSS adaptable to rapid change and reduces maintenance costs. The functionality of the LSS provides a rapid and often first response to new vulnerabilities, often without any loss of systems availability. This capacity is best demonstrated in the configuration process.

Proxy Configuration:

Depending upon the IP service, Watchguard proxies examine more than simple socket information. Each proxy has additional functions that provide enhanced security using content inspection capabilities and process tracking. Of these, the HTTP and SMTP proxies provide the greatest degree of configuration options, permitting rule sets that remove unnecessary or dangerous content and enforcement of egress and usage policies. Many security and anti-virus companies recommend the use of content filters to reduce malicious content from entering networks. MIME Content-types and path patterns are common objects used for content filtering. MIME Content-type usage is defined in numerous IETF RFC documents, particularly 2045 through 2049 [10]. In particular, network policy needs to block executable programs and scripting from

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

entrance, particularly when this content is not needed for organizational goals. Policy also exists to protect organizations from legal liabilities associated with illegal activities, negligent disclosures, sexual harassment issues, and more. Use of content filtering, site restrictions, and reduction of exposure to malicious code all reduce organizational costs of recovery, legal liabilities, and support costs. These filters also protect users who inadvertently visit hostile or inappropriate sites from exposing the organization to these risks by blocking access and unauthorized content. Furthermore, intentional attempts to bypass policy are reduced by frustrating the abuser since fewer attempts to violate policy are successful and through logging of activities.

In order to configure the LSS proxies correctly, an understanding of the terminology used by Watchguard is required. The Firebox is a stateful firewall; it monitors connections by process id (PID) and identifies the connection as incoming or outgoing based upon the initiator of the communication. This PID is assigned at the time of the connection request from the originator of the communication. Figure 3 presents a diagram of incoming and outgoing traffic. All connections originating from the external (public) interface are identified as incoming. Conversely, all connections originating from the trusted (private) interface are always outgoing. Connections originating from the optional (DMZ) interface are outgoing when routed through the external interface and incoming when routed through the trusted interface. This flow is critical to configuring the address restriction portion of LSS proxies and filters.

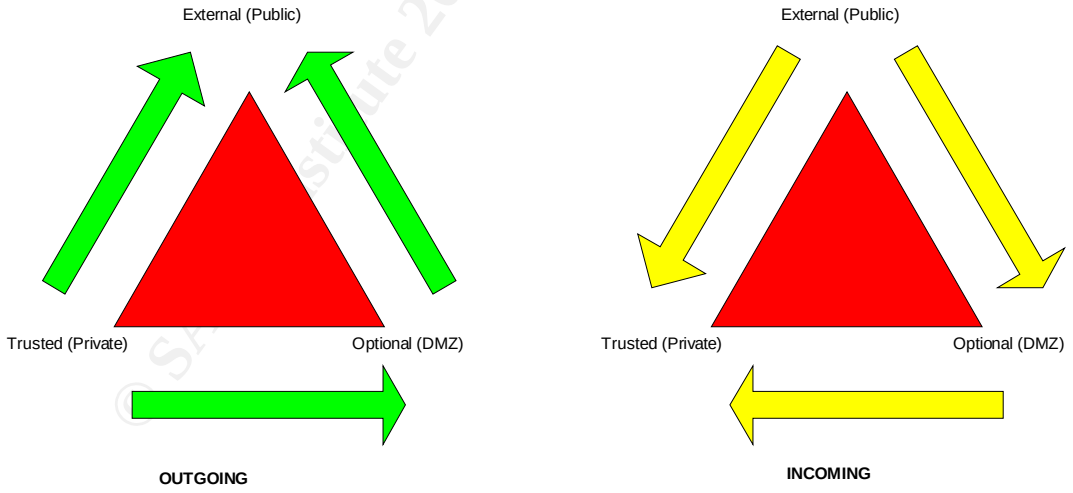

Figure 3 - Watchguard Traffic Flow Diagram

Address restrictions may be aliased to use friendly display names as mnemonics, use IP addresses, and user authentication. The firebox provides six default aliases referring to the three interfaces, the firebox itself, and local and remote DVCP (IPSEC VPN) networks. Authentication is not required, but may

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

be derived from Radius servers, NT Domain groups, CryptoCard server, SecurID server, or the Firebox itself. IP addresses may be listed individually, by range, or by network. Authentication to outside sources is limited to two or less servers or a single domain and is configured under authentication options for the Firebox. This limits the ability to use existing domain structures in multi-master NT domains. The following configurations will only use aliases, NT Groups, IP addresses, or networks.

Watchguard sets precedence of services in two manners, by group preferences and by address specificity. Group precedence is evaluated before address precedence to validate that rules exist addressing traffic on the destination port. This can cause unanticipated results that result in weakened security when the administrator fails to understand rules of precedence. Note that four group types exist: Any, port specific, multi-service, and Outgoing. The multi-service is actually a combination of port specific services combined with Outgoing services that will be discussed later. Multi-services experience a split precedence where the port specific portion of the service has the same precedence as other port-specific services and the non-port specific portion of the service follows the Outgoing rules. It is also important to note that when multiple services exist for a service within the same precedence group, this signals that all rules that process this traffic type are to be evaluated in order of precedence. This evaluation continues until a match occurs that either permits or denies the traffic between the source and destination addresses or until the evaluation of all relevant rules complete without a match. When no match occurs, denial of traffic occurs. Conversely, when only a single service exists for a particular type of traffic, then only that rule is parsed with three possible results: permitted by match, denied by match, or denied by default [11]. The following table shows the LSS order of precedence for both groups and addresses.

Group Precedence Rules*

Service Type Group	Priority
Any	1
Port Specifc	2
Outgoing	3

*Any signifies Any Service

Address Precedence Rules**

From	To	Sort order for Precedence
IP	IP	0
List	IP	1
IP	List	2
List	List	3
Any	IP	4
IP	Any	5
Any	List	6
List	Any	7
Any	Any	8

**Any signifies all IP addresses

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

HTTP Configuration:

The Watchguard Firebox provides eight different services that may be configured to permit HTTP traffic through the firewall. Four are standard packet filtered services that only use address, alias, or authentication mechanisms to permit or deny HTTP traffic. These are the Any, Outgoing, Outgoing-TCP, and Filtered-HTTP services. Each of these services permits all outbound TCP traffic between permitted hosts. The primary differences are that Any and Filtered-HTTP may permit incoming connections, where the Outgoing and Outgoing-TCP services do not open any incoming services. Filtered-HTTP and Outgoing-TCP do not permit UDP port traffic, where the Any and Outgoing services permit both TCP and UDP traffic. Precedence is another concern. None of these services meets the criteria for minimum required access, as all ports are open on either TCP and/or UDP between the listed host addresses. None of these services is recommended for use except when no outgoing restrictions exist or when rule sets become extremely complex and cumbersome. The Any service should never be used except between systems entirely under the control of the organization, either within the immediate network or across a VPN. As a practical limit, approximately 30 to 35 services should be a maximum target configuration, but the firebox can support a greater number of services.

Proxied services and user-filters are generally a better choice for HTTP traffic. With proxied services, HTTP traffic is subject to content inspection rules, unlike filtered services. The user-filter lacks content inspection, is custom definable by the administrator, is restricted by TCP or UDP port, and takes precedence over outgoing filters. The three proxied services are HTTP, Proxied-HTTP, and Proxy. Like the outgoing filters described above, the Proxy service only evaluates outgoing traffic and takes the least precedence when evaluating rules. The Proxy service is an Outgoing-TCP filter with the addition of content inspection capabilities. This provides a higher level of security than the Outgoing-TCP filter, but again should only be used when filters that are more specific cannot provide efficient rule sets due to the complexities of organizational requirements.

Service	Incoming Controls	Outgoing Controls	Content Inspection	Order of Precedence	Added functions
Any	yes - all ports	yes - all ports	no	highest	none
Outgoing	no	yes - all ports	no	least	none
Outgoing-TCP	no	yes - all TCP ports	no	least	none
Filtered-HTTP	yes - TCP port 80	yes - all TCP ports	no	specificity of host rules	none
User-Filter	yes - user defined	yes - user defined	no	specificity of host rules	none
Proxy	no	yes - all TCP ports	yes - all HTTP traffic on any port	least	webblocker - HTTP Controls
Proxied-HTTP	yes - TCP port 80	yes - all TCP ports	yes - all HTTP traffic on any port	specificity of host rules	webblocker - HTTP Controls
HTTP	yes - TCP port 80	yes - TCP port 80	yes - all HTTP traffic on port 80	specificity of host rules	webblocker - HTTP Controls

The intent is to design a rule set based upon the business needs of the organization that enforces acceptable use policies and provides added defenses against malicious code and viruses. Using the sample network and requirements

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

above, the Firebox administrator should select the most restrictive service that does not interfere with business operations in order. As seen in the table above, the HTTP proxied-service provides the minimum required access for web browsing, coupled with content-inspection capabilities. Minimum required access restricts egress from the internal networks adds security and enforces policy by restricting unauthorized network applications that use ports not specifically permitted. Adding the HTTP proxied-service (or any other Watchguard predefined service) to the LSS configuration is simply a matter of selecting it from a list, clicking add, then clicking ok, proceeding through the configuration pages for the service, and clicking ok again.

Filtering HTTP Traffic:

The first configuration page is the incoming rules page. By default, incoming traffic is enabled and denied. In the sample network, an intranet server exists on the optional network and must service requests from external sources. Therefore, this default must be altered to enabled and allowed. Note that this will be required for each service that requires traffic between two or more hosts accessible through different interfaces. This change is assumed throughout the remainder of this paper except where otherwise stated. This change will now permit incoming traffic from any IP address to any IP address on the optional or trusted interface. Further changes are required to restrict access to the minimum level required. In the "To" box of the incoming page, the administrator would then click the add button to add the required hosts, aliases, groups, users, or networks. In this case, inbound HTTP traffic is only required to the Intranet Server, so the administrator would add the host IP address of 10.10.10.20. By selecting the logging button on the incoming page, the administrator sets the logging options. At a minimum denied traffic should be logged for both incoming and outgoing attempts.

The next tab is the Outgoing tab and is configured in the same manner as the incoming tab. Due to the sample network being split between restricted users and business users, the administrator adds the network 192.168.20.0/24 to the from box. To provide web-browsing service to the 192.168.10.0/24 network, a second HTTP proxied service would be added with a new name, this will be done later. Since we are using private IP addresses, Network Address Translation is required, in most cases the default using simple NAT is recommended. Figure 4 presents the screens for incoming and outgoing address restrictions.

Up to this point, configuration of the HTTP proxied-service is identical to any other bi-directional service. Outgoing services use the same configuration concepts as the Outgoing page of the HTTP proxied-service. Discussion of the configuration of address restrictions is important as discussion of other services will mention these settings in the context of the specific address restrictions required for each service. Secondly, the fact that a second HTTP service will be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

configured highlights a quirk of the Watchguard LSS system that could potentially create unexpected results and a potential and unintended security hole. This is the fact that while two icons controlling the same service may be created and nearly all settings may vary between the two icons, the two options "Incoming XXXX connections are…" and "Outgoing XXXX connections are…" must be set the same on all icons based upon the same service. If one HTTP proxied service is set to "enable and allowed" for both incoming and outgoing properties, then all HTTP proxied services must be set to the same values. The addresses listed in the from and to sections of each property can and should be different between each service icon created based upon the same set to avoid conflicts and unintended results.

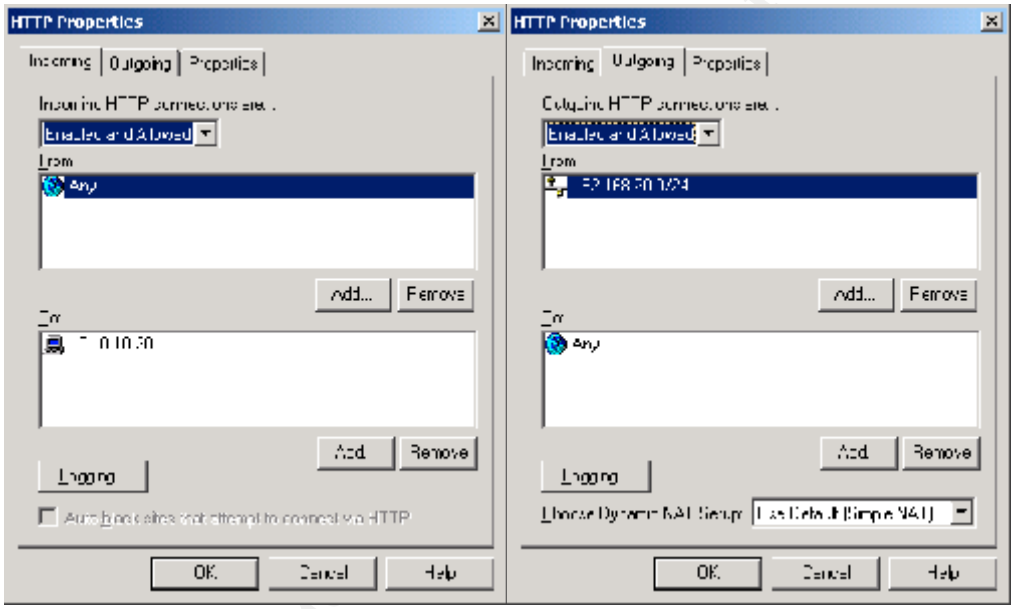

Figure 4 – Watchguard (Screen Capture) HTTP proxied service address permissions

Configuring the HTTP Proxy Content:

The third page of the HTTP configuration shows the ports allowed by the service icon and has a single button titled Settings. This button opens the proxy configuration for HTTP. Use of the HTTP proxy settings is what distinguishes the proxied services from packet-filtered services and provides a mechanism to provide protection from malicious code and enforcement of AUPs. These identical configuration pages are also accessible from the Proxied-HTTP and Proxy services however, it is important to note that each only affects the settings for the outgoing HTTP traffic on the service icon being configured currently. Therefore each service icon can have its own unique settings for the HTTP proxy services regardless of whether it is for one or more instances of the HTTP, Proxied-HTTP, or Proxy services. Configuration of the HTTP proxy consists of setting options on one or more of seven pages of user-configurable options. The

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

first two pages affect HTTP operation and file content evaluation. The subsequent five pages control settings for the Webblocker operation that evaluates web site categories using the SurfControl CyberNot list.

The Settings page contains several options shown in the table below that can restrict the operation of HTTP and help masquerade sensitive client configuration data. Checking the options on this page enables the operation of that option. Commonly used settings to protect networks using HTTP traffic are Remove Client Connection Information, Remove Unknown Headers, Log Accounting/Auditing Information, and Require Content-type. Also of importance is the ability to use a caching proxy server to speed performance since the Watchguard does not provide content caching. Exercise care when selecting this option. To prevent address looping from occurring either, exclude the caching proxy server from the addresses permitted or create a second icon without the caching proxy server option that has higher precedence to service HTTP traffic for the caching proxy server. Other options on this page are frequently disabled as they prevent many websites from being accessed or functioning. They can be enabled when policy specifically prohibits use of Java, ActiveX, Cookies, or use of forms on Web pages. By prohibiting ActiveX and Java applets, malicious code crafted in these formats is blocked from download and execution on client hosts.

Setting	Description	Usage
Remove Client Connection Info	Removes unnessary data such as OS and browser versions	Advised - Common
Remove Cookies	Prohibits use of cookies in HTTP traffic	policy based
Deny Submissions	Prevents clients for using POST or GET data from forms	policy based
Deny Java Applets	Prevents download of Java Applets	Advised - policy based
Deny ActiveX Applets	Prevents download of Active X Applets	Advised - policy based
Remove Unknown Headers	Strips non-compliant MIME headers from Webpages	Advised - Common
Log Accounting/Auditing Info	Records web traffic statistics including URL, size, & source	Advised - Common
Require Content-type	Prevents viewing of webpages that are not MIME compliant	Advised - Common
Use Caching Proxy Server	Redirects web requests to content caching server to improve performance	Advised if caching proxy server is available

The Safe Content page is where primary protection from new malicious code occurs. This page is also present on the SMTP proxy and is configured in the same manner, but may have different settings based upon policy and business requirements. Checking the box labeled, Allow only safe content-types, performs enabling content-type checking. This activates two types of content checking: MIME content-type checking and file path pattern checking. These two checks operate in different manners. MIME content-types are only permitted if explicitly granted, though this permission may be granted by use of wildcards. Only add those MIME types that are required by your organization. Note that Watchguard uses fully compliant MIME content-types, sub-types are required, if missing they are denied. Conversely, file path patterns are only explicitly denied, again wildcards are permitted. The host portion of the URL is not evaluated in path patterns, only the directory structure and file name itself are compared during evaluation. Path pattern lists are long by nature but effective at removing malicious code. Minimum access would dictate that only those MIME Content types that are business necessary or essential for web page viewing be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

permitted. Generally all self executing and executable file types should be denied by file name pattern. Many sources such as www.isi.edu and www.trusecure.com provide lists of MIME content-types or provide recommendations for path pattern exclusion [12] [13].

One particular MIME Content-type should never be permitted through, this is Application/Octet-stream that is the designation for a generic binary file and is to be used by applications that cannot evaluate the correct content-type [10]. This often results from incorrectly configured sending hosts, is often the content-type found on new viral code, and can be used by attackers to disguise the true nature of the code. Content-type evaluation has weaknesses that have been highlighted by virus events such as Nimda and Klez that spoof MIME content-types [14] [15]. However, when content-types are permitted only explicitly, only those permitted may be exploited. Using limited lists greatly reduces the chance of malicious code exploiting MIME spoofing. If not required do not add content-types that web browsers will automatically execute such as application/x-wav. Path pattern matching provides added protection from malware by removing files that meet certain path patterns such as *.exe, *.com, *.cmd, *.bat, *.scr, *.vbs, and others [13]. Use of content-types and path patterns will block nearly all newly released viruses and worms distributed by HTTP or SMTP traffic when properly configured in the Watchguard proxies. Figure 5 shows the pages for the HTTP proxy settings and safe content pages.

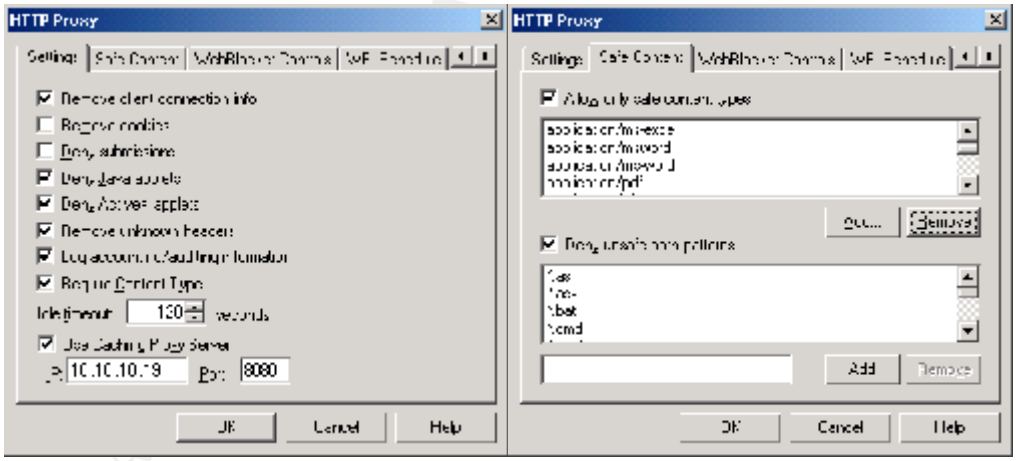

Figure 5 - Watchguard HTTP Proxy Settings and Safe Content

Configuring the Webblocker:

Watchguard includes the Webblocker module with the Firebox II and III series. This software is configured on the next five pages of the HTTP Proxy configuration. Configuration of these pages is straightforward. The first step is to enable Webblocker by checking the box labeled Activate Webblocker. One or more accessible Webblocker servers are required otherwise outgoing HTTP

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

traffic is denied by default. These must be identified by IP address and listed in the order of use desired as this works in a fail over configuration; normally only the first Webblocker server listed is used. If denial of outgoing HTTP traffic is not desired when Webblocker services are not available, check the box labeled Allow Webblocker Server Bypass, this will permit outbound HTTP traffic when the Webblocker server fails to respond.

Next, the operational schedule for Webblocker must be determined. Selecting and activating one-hour blocks for each day of the week configure this schedule. The pages that define HTTP web access during operational and non-operational hours use this schedule. Policies vary on web use, however this demonstration assumes a more restrictive policy applies to non-operational hours for this example. All users require HTTP traffic, so this must be available and the "block all outgoing web access" flag must not be checked on the operational hours page. Select the appropriate web access categories to block, most common blocks include: Sexual Acts, Full Nudity, Partial/Artistic Nudity, Violence/Profanity. Similarly, the non-operational hours access must be configured. If web access is still permitted, again, the flag to block web access must not be checked and each blocked category must be checked. In this case, all non-operational hours web access is to be blocked, so this flag is set. Lastly, certain sites that the organization must access may be blocked by Webblocker category; this can be overridden by inclusion of these sites on the Webblocker Exceptions page. These sites are identified by IP address; verify all IP addresses for the site using NSLookup before inclusion. Content-type checking will still occur on sites exempted from Webblocker rules, but Webblocker categories will be ignored for these sites.

All of the above steps are repeated for secondary and tertiary HTTP proxied-service icons. The same network shows a restricted network. In the example above, this network, 192.168.10.0 was not granted access to HTTP, yet requires HTTP access. This is due to increased restrictions upon the group. Add a second HTTP proxy icon substituting 192.168.10.0 for 192.168.20.0 in the above example. When adding the icon, rename to an appropriate name such as HTTP-Restricted-Net. Configure in the same manner, adding in the increased restrictions such as deny submissions, deny cookies, fewer MIME Content-types, and blocking all Webblocker categories except search engines during operational hours. Similarly, a tertiary icon may be setup that permits access to specific sites with Webblocker disabled and permitting ActiveX and Java Scripts. On the Outgoing page, list the IP addresses or networks of the specific sites required in the To section. Name this icon HTTP-Trusted-Sites or something similar. If as shown in the demonstration a content-caching proxy server is used, another icon is required with the content-caching proxy server flag unchecked, and on the Outgoing tab, the proxy server should be listed its IP address in the From section, with Any in the To section. Remember to consider precedence rules when configuring more than one HTTP icon; address specificity is the only precedence that matters when no other group services HTTP.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Proxied-HTTP service configuration occurs exactly as described above, but reduces the preference evaluation for outgoing traffic other than HTTP to the lowest level. It does add the ability to enforce proxy rules on HTTP traffic on ports other than port 80, but opens egress traffic to all TCP traffic for the permitted addresses. The same applies for the Proxy service icon, except there is no incoming configuration rule set to configure. Note that the HTTP proxied-service does not address HTTPS traffic on port 443. A separate packet filtered service icon must be created. If incoming HTTPS traffic is not required, then the Proxied-HTTP, Proxy, or other Outgoing service will provide for HTTPS traffic. Since inbound HTTPS traffic is required and egress traffic restrictions are needed to minimize access, selection of the HTTPS packet filter is most appropriate.

SMTP Configuration:

Configuration of the firebox for SMTP traffic is similar to that of HTTP traffic. Again, selection of the appropriate filter or proxy and determination of the requirements for content inspection is necessary. Similar to the HTTP protocol, a wide variety of choices exist that permit SMTP traffic flow. Once again the Any, Proxy, Outgoing, Outgoing-TCP, Filtered-SMTP, and user filter options exist. Proxied-HTTP will also permit outgoing SMTP traffic as all outbound TCP traffic is allowed. The last and most restrictive option is the SMTP proxy. Unlike HTTP configuration where three options provided proxy services, only the SMTP proxy offers proxy services to SMTP traffic. Since this demonstration requires both incoming and outgoing SMTP traffic, plus content inspection and filtering, only the SMTP proxy service meets the requirement to provide minimum access.

Configuring host filtering on the SMTP proxy is identical to the configuration of the HTTP proxy. However, the filter list itself is different. Note that a public e-mail server exists on the Optional interface of the firewall. Policy dictates that only organizational mail systems be used on the network. This reduces the need for SMTP traffic to this host alone[1]. Add the address for the e-mail server (10.10.10.19) to the "To" box of the Incoming tab and to the "From" box of the Outgoing tab and set both to "Enabled and Allowed". Leave the default "From" of Any on the Incoming tab and default "To" of Any on the Outgoing tab. This prevents any user or host from bypassing the rules that all SMTP traffic passes through this external e-mail server. It also forces all SMTP traffic to be proxied according to the rule set created for this service icon. Denying users the ability to connect to other SMTP servers strengthens policy. This further strengthens internal e-mail server controls through enforcement of proxy rules on all SMTP traffic.

Next, the SMTP proxy itself is configured. Distinct from other proxies, the SMTP proxy is split into an incoming proxy and an outgoing proxy, each with

[1] If mail-enabled alerts are configured for Firebox logging events, the Watchguard Security Event Processor server may need to be included in the From section of the Outgoing service.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

different configurations. As opposed to the HTTP Proxy that evaluates content on outgoing traffic, the SMTP proxy evaluates content on incoming traffic. Remember that incoming and outgoing are stateful designations, defined by the direction of the connection initiation, not actual packet flow. The Properties tab of the SMTP proxy provides two buttons, one to open Incoming SMTP proxy configuration, the other to open Outgoing SMTP proxy configuration.

Configuring the Incoming SMTP Proxy Content:

Configuration of the SMTP Proxy focuses mainly upon SMTP and ESMTP restrictions that may also be enforceable upon the e-mail server itself. However, these functions provide a second barrier to abuse of e-mail systems when this redundancy exists. Directionally, incoming SMTP messages and traffic must flow through the firewall before reaching the mail server. Since no restrictions are placed upon source by the firewall, all SMTP traffic bound for the mail server is passed, unless default or imposed restrictions are exceeded. Since the Firebox is not optimized as an e-mail gateway, it may be best to allow traffic to pass and be evaluated by the mail server. At a minimum, the following should be changed on the general tab:

- Maximum Recipients – decrease to an acceptable level for the organization to minimize SPAM.
- Maximum Size – increase or decrease to match policy and e-mail server restrictions.
- Allow Source-Routed Addresses should be disabled.

The ESMTP tab permits configuration of accepted ESMTP command features. Our network shows remote mail clients that use SMTP to send e-mail. Assuming relaying is prohibited without authentication, then AUTH must be allowed and the command AUTH=LOGIN must be permitted to facilitate Microsoft's implementation of AUTH in ESMTP. Similar to the ESMTP tab, the Header tab permits the addition and removal of permitted SMTP message headers. To further reduce the opportunity for relay, the Address Patterns tab option for Allowed To needs to have those e-mail domains that are resolvable to a host behind the firewall. Tracking of removal of ESMTP extensions and unknown SMTP headers should be logged by enabling these options on the Logging tab.

Content inspection primarily occurs as a result of the options on the Content-Types page. Configuring this page is identical in procedure to the Content-Types page of the HTTP Proxy. However, the requirements for file types that are transferred via e-mail most likely differs from those required when web browsing. Often these restrictions include fewer permitted MIME Content-types and more excluded path patterns. As in the HTTP Proxy, SMTP content inspection permits MIME Content-Types explicitly and denies path patterns explicitly. Since most virus distribution has occurred via e-mail during the past

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

few years, it is advisable that policy stipulate that this list be no less restrictive than that of HTTP traffic and preferably more restrictive. The other difference here is not one of policy, but informing users of actions taken. The SMTP proxy provides the opportunity to replace the attachments removed by the proxy rules with a text file that contains a message explaining the removal, a feature not found in the HTTP proxy. These restrictions may also be used to enforce policy on viewing or sharing of pictures via e-mail to reduce systems overhead and prevent sharing of offensive material.

Configuring the Outgoing SMTP Proxy Content:

Configuration of the Outgoing SMTP proxy is comprised of three basic components: general, masquerading, and logging options. The general options page duplicates two items found in the incoming SMTP proxy, the allowed SMTP headers and idle timeout settings. Masquerading allows internal information to be removed or replaced with less identifiable information for security purposes. Domain names, message-ids, and MIME boundary strings may all be masqueraded to reduce disclosure of internal systems information. The last page provides logging options for header removal, masquerading actions, and auditing information.

DNS Configuration:

As is the case with most TCP/IP services, there is more than one manner to permit DNS traffic on the network. DNS requires both TCP and UDP to operate so the options are less than those of SMTP or HTTP are. Five such methods are available: Any, Outgoing, DNS packet filter, DNS-Proxy service, and user-filters. The demonstration network requires both incoming and outgoing DNS traffic due to the use of a DNS server on the Trusted interface of the firebox. This rules out the use of the Outgoing service for our requirements. The Any service does not minimize access and is not advisable. With one exception, the DNS-Proxy service operates exactly as would the DNS packet filter. This exception is the ability to protect DNS servers against buffer overflow attacks from incorrect transaction signature (TSIG) or next (NXT) records, plus other DNS exploits [16].

Selection of the DNS-Proxy is advised due to added capacity to prevent certain buffer overflow attacks upon DNS. Configuration of this proxy has no options that are not available in any regular packet filtered service. The administrator sets the incoming address list, outgoing address list, logging, and auto-block rules. Content filtering is automatic and cannot be altered by the GUI[2]. Manual configuration of query-types and classes from the default configuration is possible by editing the configuration file and saving the new

[2] Configurable options were added to the DNS, FTP, and SMTP proxies in LSS version 7.0 through Protocol Anomaly Detection configuration.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

configuration to the Firebox. This is rarely required and outside the scope of this paper.

The sample network requires all network systems to have access to the internal DNS server. External access is not required as the internal DNS server is not authoritative for hosts on the Internet, nor does it provide resolution services to Internet hosts. Furthermore, all internal hosts should be required to use the internal DNS server to ensure proper resolution of names on the internal network. Some organizations block access to sites banned by policy using internal DNS servers and domain SOA spoofing. This results in redirection of blocked domains to a web page indicating an attempt to access a system blocked by policy. To create this configuration, only the Internal DNS server should have outgoing access and only hosts on the optional network should have incoming access. Add the Firebox and either the specific hosts on the optional network or the Optional alias to the From section of the Incoming properties page and the IP address of the Internal DNS server (192.168.199.200) to the From section of the Outgoing properties page. The Firebox is added to accommodate name resolution for internal hosts during log report generation.

FTP Configuration:

FTP may be permitted through any service that allows TCP and UDP traffic on ports 20 and 21. Like DNS, several options are available to configure services for FTP though no predefined packet filter exists. As shown earlier, the demonstration network only requires Outgoing access for FTP for select users and Incoming access to the Intranet server. Use of the FTP proxied service is recommended given its capacity to layer additional restrictions on inbound and outbound FTP access. Restrict incoming access to only the Intranet server by specifying its address (10.10.10.20) in the To section of the Incoming page. Outgoing access needs to be granted to a select group of users on the internal NT network. Create a NT group called FTP users in the domain, added the required users to this group, and add the NT group to the From section of the Outgoing properties page using the NT group option from Add Other.

Configuration of the proxy restricts user and guest activity by limiting access to read-only, denying the SITE command, setting idle timeout limits, and logging of auditing information. Limiting access to read-only is set separately and independently for incoming and outgoing access by checking the appropriate box. This can prevent guests from modifying internal data or placing data upon external servers and risking disclosure of sensitive information. Denying the Site command on incoming connections reduces the risk of disclosing information about the ftp host that might be used by an attacker. Idle timeout limits restrict vulnerabilities that arise when systems are left unattended, this value is best set to a conservatively low number of seconds such as 300. The final options permit detailed logging information for accounting and auditing purposes to take place

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

on incoming and outgoing connections. This tracks file transfer sizes, source, and destination IP addresses.

RPC Proxy Configuration:

RPC or Remote Procedure Call, also known as Distributed Computing Environment (DCE) is often called a port-mapper service. This is due to the operation of RPC, in which a connection is established on port 135 so that the hosts can negotiate an available port, usually above 1024, for continued inter-process communications [17]. Once this new port is established, port 135 is no longer used and the new port is used for the remainder of the connection. This makes blocking RPC traffic difficult as this expands the need for open ports in the firewall considerably, weakening ingress and egress filters that support policies. The Watchguard RPC-DCE proxy is designed to accommodate this issue without compromising security by opening unnecessary ports. This process uses the PID to track the initial and ongoing communication from its initial port 135 communication to its newly assigned port. Since the PID becomes part of the proxy filter, this eliminates the need to open all traffic to high ports. This port change tracking by PID is what defines this service as a proxy, rather than a packet filter.

Configuration of the RPC-DCE proxy is no different from any packet filter configuration. The incoming and outgoing address restrictions are applied along with the setting of logging options. The demonstration network shows that no external connections require RPC-DCE traffic therefore Incoming options should be set to "Enabled and Denied". Outgoing restrictions are set to "Enabled and Allowed" with the To section list being comprised of the servers residing on the optional interface, 10.10.10.19 and 10.10.10.20. The From section of the Outgoing interface may be left at Any, but should be restricted by interface (Trusted) or by networks. Since the Restricted network has no need to access the servers on the optional interface, adding the network 192.168.20.0/24 to the From list of the Outgoing configuration restricts access to the minimum required levels and provides optimum restrictions upon egress of RPC connections.

Blocking any incoming RPC traffic as presented and restricting outgoing traffic between necessary systems only limits the vulnerability of dangerous protocols that permit execution of processes and commands on remote systems. It also serves to completely block any penetration from the Internet by RPC exploits such as those seen recently in the Blaster and Welchia worms [7] [18]. It also reduces the spread of these exploits by internal systems by limiting egress, reducing damage to systems and promoting good neighbor behavior on the Internet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Other Services:

As previously presented, several other services are required by the organization in the demonstration network. Packet filtered services are the only option for the HTTPS, NTP, SMB, POP3, and Auth services when using a Watchguard Firebox. These are simple configurations, restricted by port(s) and addresses. Each must be configured separately to meet minimum access requirements, since no two services have the same access restrictions; combination of services with user-filters is not achievable without increasing risk. Particular care to restrict egress and incoming traffic on these services is critical to reducing exposure. In particular, SMB services on ports 137, 138, 139, and 445 needs to be blocked from entering or leaving the organizational network if possible. In the demonstration network, there is no cause to open these ports to any interfaces or hosts on the external interface of the Firebox. Configuring these services are not discussed in detail here, as address restrictions are set in the same manner as the proxies discussed above and follow the restrictions shown in the network diagram and required services table.

Benefits and Disadvantages of Watchguard Proxies:

Use of proxies on the Watchguard Firebox provides several benefits over standard packet filtering. Behavior of sessions is monitored by PID, rather than simple review of each packet. This permits multi-packet review to ensure services comply with accepted standards and reassembly and evaluation of fragmented packets and data streams that permits content-inspection using standardized content-type designations and content path pattern matching. By blocking non-compliant behavior, proxies serve to reduce vulnerabilities to exploits that take advantage of software that cannot properly handle or process malformed or unexpected packet configurations. Content inspection permits rapid identification and blocking of potentially malicious code and content not permitted by AUPs. Coupling these proxy capabilities with packet filtering provides a centrally managed egress, ingress, and usage policy with lower cost implementation of perimeter security than many multi-vendor or multi-device options. Site filtering through Webblocker, provides greater capacity to enforce AUPs by restricting access to sites offering unacceptable subject matter.

Most changes in LSS configuration do not require a restart of the Firebox and take effect upon saving the new configuration to the firewall. This permits rapid response to new threats and changing requirements, with virtually no impact upon systems availability. Since changes are often implemented in minutes, entire networks may be secured against new threats far quicker than software patches or virus definition signature files may be distributed. This rapid response provides cost savings when compared to costs of reactionary patching of systems and provides greater protection and time to patch systems in a tested and controlled manner. The Firebox uses a limited and hardened proprietary modification of the Linux kernel running from flash memory to control its

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

operations. This secures the system from Operating System vulnerabilities that often exist in solutions that run on top of standard operating systems such as general distributions of Linux and Microsoft Windows. Finally, nearly all data flow through the Firebox may be logged, permitting integration with Intrusion Detection Systems, usage and abuse reporting, and centralized review of policy.

Use of the proxied services does mean that systems administrators have to find a balance between the benefits and disadvantages of the Firebox system. Using proxied services slows performance and throughput since entire packets are evaluated, rather than only header information. Connections must be tracked and data streams reassembled to perform content removal and replacement under some proxies or to ensure fragmentation does not masquerade the non-compliant behavior of a service. Combining proxy services with packet filters, creates a single point of failure or compromise for attackers, making a failure more critical than a multi-device solution. The former is probably less critical, as hardware or software failures often result in a denial of service since these multiple devices rely upon each other just as the multiple functions of a single device rely upon each other. Compromise by an attacker upon a single device is the more critical issue, once compromised the system is potentially controlled in its entirety by the attacker, rather than only one piece of security being compromised in a multi-device solution.

Further disadvantages lie in the design of the Firebox. Optimization of the kernel secures the Firebox itself and balances the routing, packet filtering, proxy, authentication, and VPN services it provides. When compared to devices specifically designed for single or limited tasks such as routing and packet filtering, its performance lags behind. Combining many functions into a single device also limits resources available to each process and often means more the device is relied upon to control and protect most traffic.

This balance requires a review of the network to optimize performance and determine if alternatives currently exist or may be acquired in order to replace or supplement functionality of the firebox. As previously stated, proxy services slows network throughput. Performance may be improved by moving other services to different devices such as routers or content proxy servers to improve performance. In particular, many routers are more efficient at handling packet-filtering processes. Rule sets should be implemented at routers that block services that are not required anywhere within the organization. This reduces the traffic processed by the Firebox and frees its resources to handle proxied services more efficiently. Placing routers between the firebox interfaces and each network usually provides improved performance on the network by deploying global packet filters at these points. This provides the benefit of having three layers of packet filtering in place to protect the organization. Since all traffic would have to pass through two routers and the firebox, an incorrect configuration of a single device is unlikely to permit a compromise of the protected network. The Firebox as a secondary defense, permits identification of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

primary defense failures through review of detailed logging by the Watchguard. Denials on globally blocked service packets should not occur on the Firebox in this multi-level configuration, when they do occur, the primary defense has been identified as not performing as expected and should initiate further review. Cost is a consideration as the additional hardware and support costs increase with the addition of devices.

Similarly, hosting proxies on another device optimized for proxy services might provide faster throughput than does the Firebox. Again, issues of configuration management, cost, layering of security, and performance must all be balanced. In all cases, distributed security is not without some overhead in addition to each devices processing. Each added device requires some inter-device communication, encapsulation or rewrapping of datagrams, and is reliant upon network traffic and capacity. Adding devices increases the number of times a packet must be transmitted, received, evaluated, and processed. Combining functions in fewer devices does reduce the number of times packet headers must be examined and permits multiple processes to evaluate each connection in fewer steps. This may offset performance losses by combining functions into a single device such as the Firebox, or reduce the performance loss to an acceptable level.

Finally, user impact due to security implementation must be considered. Use of content filtering and subject matter blocking using proxies is likely to generate the most user complaints concerning blocked material. This can be mitigated by communication with the user base as to the actions being taken, the reasons for the actions, and the process for review of requests to permit certain content through the firewall. Just as any restriction creates some additional work in addressing user concerns, use of the LSS proxy content filters is no different. Starting with maximum security and easing restrictions as warranted by business needs and change demand or occur is usually simpler when done initially rather than shutting down previously allowed activities, even though those activities may have violated policy.

Recommendations:

Administrators need to address security issues for their organization, while supporting business requirements and enforcing policy. At the same time, they must be open to consideration and change when business change occurs or users present valid justification to alter the rules of security. The following guidelines are offered to Watchguard Firebox administrators:

- Analyze business requirements and ensure security does not impact critical and normal business operations
- Understand the Acceptable Usage Policy and design the Watchguard Configuration to implement restrictions in accordance with the AUP.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Identify the risks to the organization that are inherent in the systems in use.
- Apply the concept of minimum required access to the LSS configuration
- Use Watchguard LSS Proxies to provide content filtering capabilities to supplement anti-virus protection, and to enforce AUPs.
- Use routers between the Watchguard and each network to provide primary packet filtering to reduce load on the Watchguard, permitting faster proxy service response and secondary intrusion prevention by the Watchguard.
- Use packet filtering at routers and Fireboxes to control ingress and egress traffic on the network in accordance with business requirements and AUPs.
- Use the Watchguard as an initial point of defense to new vulnerabilities to provide greater time to evaluate and deploy more permanent solutions that require time and expense.
- Consider user requests for removal of access controls in light of business needs, justification may exist to change the rule set.

At this writing RFCs 2045 through 2049 are in either draft or best practice status, but have not been adopted as Internet standards [19]. Standardization of MIME Content-types, addition of cross validation, and acceptance would further enhance the use of MIME content-type filters. The Internet community should push the adoption of RFCs 2045 through 2049 into Internet standards, thus defining the rules of compliance. Meanwhile vendors need to integrate new content-type validation rules to minimize the impacts of content spoofing as seen with recent viral code. Currently, many vendor products, Watchguard included, only validate either the MIME Content-type or the file extension to determine the handling and processing of the file or attachment. No cross validation is performed to verify that the MIME Content-type matches the file extension of the attachment, though many systems contain the references necessary to accommodate this type of cross-referencing. This issue exposed Microsoft Windows systems to the Nimda Virus. The Windows registry contains the necessary information to perform cross validation tests that identify the spoofed content-type. Yet, no cross-validation routines existed in the Windows operating system. The result was the exposure of millions of systems to exploits of this vulnerability.

Conclusion:

Proper selection, use, and configuration of Watchguard proxies are key to creating a layered defense that supplements other security controls and enforces AUPs. This process requires an understanding of the business operations, usage policy, and the processing rules of the Watchguard to create an effective and efficient security tool. In particular, the Watchguard provides robust content filtering that removes potentially malicious code as traffic attempts entry into the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

secured network. By carefully controlling the content permitted or denied, the Firebox system provides a first line of defense against new exploits. Using guidelines developed by security firms and software developers, most malicious code cannot enter the network. This prophylactic defense occurs even though detection definitions are not yet available from anti-virus vendors. Content and subject matter filters and restrictions that match AUPs, enforce the policy through active means and log transgressions that can be used to further isolate and correct policy violations, regardless of user intent.

The rapid configuration tool permits reconfiguration of proxied and packet filtering services, permitting entire networks to be secured in minutes through by use of a single device. In most cases, systems availability is not impacted. This reduces organization costs through the reduction of response time while minimizing the impact upon business operations. By providing an immediate response to new attacks, it becomes less critical to effect emergency patching of individual systems as the primary means of protection. This does not exclude the need to patch systems or update virus definitions; exploits and malicious code can and do enter networks by alternative means. While the Watchguard may be a primary defense against Internet based attacks, it is not a sole defense against all attacks. What often occurs is a grace period that permits proper testing and evaluation of patch deployment and impact upon existing systems in a coordinated and controlled manner. This resulting structure reduces cost to the organization and provides the means to deploy permanent corrective action in a systematic approach. The result is the mitigation of negative impacts, duplicative efforts, and delay of other work due to emergency response efforts. The result is a cost-effective, rapid-response solution to new and developing external threats coupled with an effective mechanism to enforce Acceptable Usage Policies.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References:

1. Dougherty, Chad and Householder, Allen. "Malicious Code Propagation and Anti-Virus Software Updates." CERT Incident Note IN-2003-01. 2 July 2003. URL: http://www.cert.org/incident_notes/IN-2003-01.html (5 July 2003).
2. Tippet, P. " Building 'Synergistic' AV". Information Security Magazine. (May 2002) URL: http://infosecuritymag.techtarget.com/2002/may/synergisticav.shtml (28 July 2003).
3. TruSecure. "2002 Q2 Top 10 Successful Electronic Attack Modalities". 2002. URL: http://www.trusecure.com/knowledge/threats/ (28 July 2003).
4. Post, Gerald V. and Anderson, David L. Management Information Systems 2nd Ed. Boston: The McGraw-Hill Companies, Inc. 2000. 611
5. Microsoft Corporation. "Buffer Overrun In RPC Interface Could Allow Code Execution (823980)". Microsoft Security Bulletin MS03-026. 16 July 2003. URL: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp (17 July 2003).
6. Hurley, Edward. "Windows RPC Flaw Exploited in Campus Hacker Attacks" Security Wire Digest. 11 August 2003. URL: http://infosecuritymag.techtarget.com/ss/0,295812,sid6_iss63,00.html#news3 (12 August 2003).
7. Messmer, Ellen. "Update: Blaster worm infections spreading rapidly". Network World Fusion. 13 August 2003. URL: http://www.nwfusion.com/news/2003/0812blastinfect.html (15 August 2003).
8. Fisher, Dennis. "Black Hat: Moderate Flaws Threaten Networks". e-Week. 30 July 2003. URL: http://www.eweek.com/article2/0,3959,1207932,00.asp (15 August 2003).
9. Bridwell, Larry. "ICSA Labs 8th Annual Computer Virus Prevalence Survey". TruSecure. 2003. URL: http://www.trusecure.com/download/dispatch/VPS2002.pdf?ECDE=W0107 (PDF Pg. 5) (8 August 2003).
10. Freed, N. and Borenstein, N. "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies". IETF Network Working Group Request for Comments: 2045. November 1996 URL: http://www.ietf.org/rfc/rfc2045.txt?number=2045 (24 August 2003).
11. Watchguard Technologies, Inc. "Watchguard Firebox System User Guide Firebox System 4.6" 2001 URL: http://www.watchguard.com/help/docs/v461UserGuide.pdf (PDF pg. 56) (17 August 2003)
12. Information Sciences Institute. "Media Types". 16 October 2001 URL: http://www.isi.edu/in-notes/iana/assignments/media-types/media-types (28 July 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

13. TruSecure. "Automatic launching of applications or scripts via email". TruSecure Alert - TSA-01-008. 20 June 2002. URL: http://www.trusecure.com/knowledge/hypeorhot/2001/tsa01008.shtml (28 July 2003)
14. Network Associates. "Exploit-MIME.gen". 21 November 2001. URL: http://vil.nai.com/vil/content/v_99273.htm (28 July 2003).
15. Microsoft Corporation. "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment". Microsoft Security Bulletin (MS01-020). 29 March 2001. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-020.asp (28 July 2003).
16. Watchguard Technologies, Inc. "Watchguard Firebox System User Guide Firebox System" 2003 URL: http://www.watchguard.com/help/docs/v461UserGuide.pdf (PDF pg. 123-124) (17 August 2003)
17. Microsoft Corporation. " HOWTO: Configure RPC Dynamic Port Allocation to Work with Firewall". Microsoft Knowledge Base Article – 154596. 14 May 2003 URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;154596 (27 August 2003).
18. Nahorney, Benjamin; Knowles, Douglas; Perriot, Frederic. " W32.Welchia.Worm". Symantec Security Response. 18 August 2003. URL: http://www.symantec.com/avcenter/venc/data/w32.welchia.worm.html (18 August 2003).
19. Reynolds, J.; Braden, R.; Ginoza, S.; De La Cruz, A.; " Internet Official Protocol Standards". IETF Network Working Group Request for Comments: 3300. November 2002 URL: ftp://ftp.rfc-editor.org/in-notes/std/std1.txt (28 July 2003).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: January 25th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Las Vegas 2020	Las Vegas, NVUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Vienna January 2020	Vienna, AT	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Security East 2020	New Orleans, LAUS	Feb 01, 2020 - Feb 08, 2020	Live Event
SANS New York City Winter 2020	New York City, NYUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Northern VA - Fairfax 2020	Fairfax, VAUS	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS London February 2020	London, GB	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Dubai February 2020	Dubai, AE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Cairo February 2020	Cairo, EG	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Training at RSA Conference 2020	San Francisco, CAUS	Feb 23, 2020 - Feb 24, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure India 2020	Bangalore, IN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Dallas 2020	Dallas, TXUS	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Prague March 2020	Prague, CZ	Mar 09, 2020 - Mar 14, 2020	Live Event
Wild West Hackin Fest 2020	San Diego, CAUS	Mar 10, 2020 - Mar 11, 2020	Live Event
SANS Doha March 2020	Doha, QA	Mar 14, 2020 - Mar 19, 2020	Live Event
SANS Secure Singapore 2020	Singapore, SG	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS Norfolk 2020	Norfolk, VAUS	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS London March 2020	London, GB	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS San Francisco East Bay 2020	OnlineCAUS	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced