Global Information Assurance Certification Paper

Getting the Most out of your Firewall Logs
By Matt Willard
GSEC Practical v1.3

Introduction

A good security solution has many layers or components, commonly referred to as 'Defense in Depth'. Regardless of which types of security solutions are being implemented, logging is critical to ensure their implementation is running smoothly as well to keep tabs on what is happening in an environment. While it is easy to suggest that all logs should be looked on a weekly, if not daily basis, the amount of information commonly logged is so great and often times in a format that is difficult to understand, it becomes a tedious job that more times than not gets overlooked. As a result logs are either not reviewed at all or given a cursory review, which results in the most critical items being missed altogether.

One security solution that nearly every organization deploys is a firewall. Once a firewall has been chosen, much time and effort is dedicated to installing the firewall and configuring its rule-set. A typical firewall will generate large amounts of log information. The goal of this paper is use the logs of CheckPoint FW-1 v4.1 and provide examples of tools that will automate the process of maintaining and monitoring a firewall's logs.

Firewall Log Maintenance

Before any tools can be implemented to monitor and manage the firewall logs, a sound maintenance policy needs to be in place. A good log file maintenance plan is critical so any security breaches or issues can be reviewed days, weeks and even months after they occur. Most organizations will have a log retention policy, whether it is a formal or an informal policy. If a log retention policy hasn't been formally documented, this would be a good time to make sure one is documented and approved by management.

Once a policy has been identified, the rotation and retention methodology can be implemented. An example of a policy I have used in the past requires the log files be rotated on a daily basis and that the last 30 days of logs be available for immediate access. Every log older than 30 days must be available for retrieval within 24 hours and everything 1 year and older can be purged. Based on this policy, scheduled jobs ran nightly rotate the logs. On the last Sunday of every month, additional jobs were run to archive everything older than 30 days to tape. Tapes were stored off-site in a secure location. Tapes greater than 12 months old are recycled. Below is the command used to rotate logs in Firewall-1 (v4.1):

fw logswitch

Firewall logs can be exported to ASCII format – which can be used by several tools to import the logs for reporting purposes. To export the logs to ASCII format use the command:

fw logexport -i fw.log -o fwlog.txt –n

For more detailed information on logging maintenance and configuration (as well as any general information regarding FW-1), visit the web site www.phoneboy.com.

What information am I seeing in my logs?

There is a wealth of excellent information buried inside a firewall's logs. With these logs port scans and un-authorized connection attempts are documented, activity from compromised systems can be identified and much more. Configuring the appropriate levels of logging and implementing a log file maintenance policy is step one. Knowing what to look for and how to identify malicious activity is the next challenge.

Traffic moving through a firewall is part of a connection. A connection has 2 basic components; a pair of IP addresses and a pair of port numbers. The IP addresses identify each computer involved in the communication. The port numbers identify what services or applications are being utilized. More specifically, it is typically the destination port number that will indicate what applications/services are being used.

For example, when I connect to www.sans.org, there will be a log entry in my firewall log that indicates my IP address as the source address and the IP address of www.sans.org as the destination address. The destination port number will likely be port 80 (the standard port used for http).

Knowing what port numbers are associated with what services helps identify malicious activity occurring on the firewall. The Internet Assigned Numbers Authority (IANA) maintains a list of the well-known ports and their applications. These can be found at http://www.iana.org/numbers.htm.

It is also advantageous to have solid knowledge of what Trojans are in circulation, what ports they are using, how they operate and what their general purpose in life is. A nice list of Trojans and their associated ports can be found at http://www.simovits.com/nyheter9902.html.

With a good understanding of the ports logged and their associated applications, it's time to start watching the firewall logs for specific activity. In the article "Read your firewall Logs" (summarized below), Laura Taylor outlines some common items to look for in a firewall's logs:

- IP addresses that are rejected. Although a site will be probed from many places and many times, knowing that a probe is occurring and what is being probed for proves useful information when trying to secure a network.

- Unsuccessful logins. In the same vain as checking for IP addresses that are rejected, knowing when someone is trying to gain access to critical systems proves useful to help secure a network.

- Outbound activity from internal servers. If there is traffic originating from an internal server, having a good understanding of the normal activity on that server will help an administrator determine if the server has been compromised.

- Source routed packets. Source routed packets may indicate that someone is trying to gain access the internal network. Since many networks have an address range that is unreachable from the internet (10.x.x.x), source routed packets can be used to gain access to a machine with a private address since there is usually a machine exposed to the internet that has access to the private address range.

Both of the above topics revolve around gaining a good understanding of what is happening to the firewall. There is an excellent FAQ on this topic maintained by Robert Graham. This can be found at http://www.robertgraham.com/pubs/firewall-seen.html. In this FAQ, Mr. Graham reviews what ports are and why they are important, some of the most common ports used as well as some of the most common Trojans and the ports they use. Beyond that, the FAQ details specific attacks and intrusion attempts and how they work. Overall, this is an excellent source of information, particularly for administrators new to the field.

In addition to the security information documented above, there is another critical use for the information in a firewall's log files that many administrators overlook; normal everyday activity. Knowing how Internet resources are being utilized, the traffic patterns of the firewall (both inbound and outbound traffic), the protocol distribution and load on the firewall, etc., will help the administrator more easily identify when malicious activity is occurring.

To successfully implement a tool that will alert, report on and/or filter firewall logs, having an understanding of what to look for – both what is normal everyday behavior as well as what the 'bad guys' are doing is critical for their successful implementation. With this knowledge in hand, lets take a look at some tools.

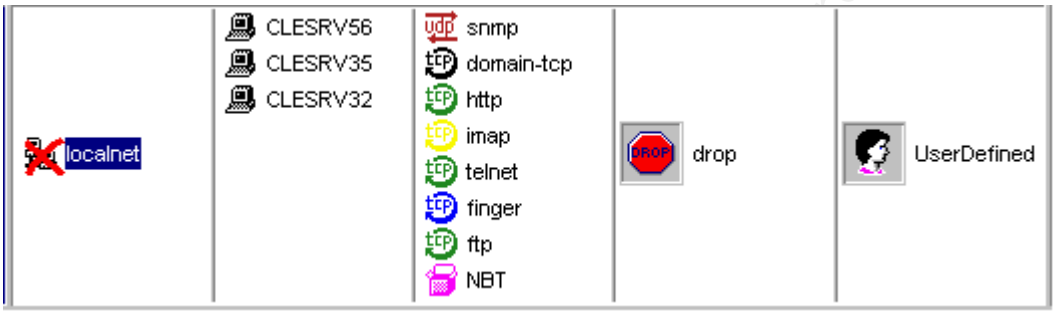
Alert.sh/Alert.vbs

To help administrators know when they are being probed or when unauthorized activity is happening on a firewall, Lance Spitzner developed a script called Alert.sh. The goal of this script is to watch for port scans or any activity defined as important by the administrator, and when they occur notify an administrator via email and save the offending action to a database. This script supports both FW-1 v4.1 as well as FW-1 NG. The script has also been ported to NT via Windows Scripting Host and Perl.

For my installation, I am using the version ported to NT via Windows scripting host by Andrew Roberson. (This version of the script can be download from Lance Spitzner's web site http://www.enteract.com/~lspitz/intrusion.html.) To install the script, I placed the script Alert.vbs in my FW-1 installation directory. A few parameters need to be changed in the script provided before it will work correctly. First, make sure the variable *dir* is set to the directory the script was

copied to. Second, verify that the *fw1dir* variable is pointing to the FW1 installation on the Management Server. There are a few other variables that can be changed – for example email notification can be turned on or off, the recipients of any email notifications can be modified, and the number of times the administrators are notified of a specific occurrence of any incident in any given day can be changed from the default of 5.

Once the parameters of the script are set, the firewall ruleset will need to be modified to put the script in action. Create workstation objects for systems that need monitored – these objects don't need to actually exist, just give the object an IP address in the internal networks address range that are not in use. Next, set the ports for the applications/services that need monitored. To start with, choose some of the most commonly scanned ports (see www.cert.org for a good list). I chose to implement DNS, Finger, Telnet, Http, ftp, Netbios, imap and snmp. Below is an example of what this rule looks like in the FW-1 policy editor.



Be sure to set the *UserDefined* alert to the location of the script. For the Windows Scripting Host version of the script, the user defined alert is set to '*cscript %dir\alert.vbs*'. To set the User Defined action, go to the *Policy* menu, choose *Properties*. Select the *Log and Alert* tab and then put the above command in the section labeled *User Defined Alert Command*.

There are a few other housekeeping items included with this script. When someone scans one of the hosts identified, it will put an entry in a file called unique.log (alert.unique for the Unix version of the script). This log file will list all the unique address that have probed the network for an open port. The Unix version of this script also has a log file alert.archive that details every port ever scanned on the network. The Windows Scripting Host version doesn't have this functionality, but it would be a simple function to add. Both versions of the script also have jobs that can be scheduled to clear out the logs on a daily basis (*rotate.sh* for Unix and *deletefwlog.bat* included with the Windows Scripting Host script). This will keep the log file sizes to a minimum as well as reset the count every day used to determine how many times you are alerted of a scan (the default scan limit is 5, which it gets by counting the occurrences in the file alert.log).

One last note regarding these scripts; since they are written in either Perl or Windows Scripting Host they are relatively easy to customize to fit specific needs. For example, the Windows Scripting Host version uses wsendmail for its mail functionality. This could easily be changed to use MAPI or any other mail provider.

ODBC Database log storage

In the Paper "Security Logs and Checkpoint Firewall1", John Ryan[3] identified the need for a tool that could be used to quickly find specific items in Check Point Firewall-1's logs. The result of his work is an access DB used to store the log files and generate reports based on the data collected. The database formats currently supported are Access 97 or Access 2000. A current copy of this database can be downloaded from http://secure-net.hypermart.net/index.htm. The steps involved in populating the database and generating reports are:

1. Export the log files in ASCII format. Use *fw logexport –d –I input.file –o output.file –n.*
2. Import the log data into an MS-Access database.
3. Run queries to view significant data.

The database designed by John Ryan comes with nine queries pre-built. These queries are designed to quickly identify potential malicious activity on the firewall. Examples include looking for ICMP activity of types 0, 5, 8, 9, 12, identify connections to ports 21, 23, 110, 111, and 143, and monitoring dropped IP connection attempts.

Lance Spitzner has also developed an Access Database with the same principals used as John Ryan. Lance Spitzner's version of the database is available for Access 97 and can be downloaded from http://www.enteract.com/~lspitz/logger.html. This version of the database comes with three queries pre-built; the top ten websites visited by users behind the firewall, the top ten inbound visitors to the companies website, and the top five IP addresses dropped or rejected by the firewall.

Both versions of this database use a single table and maps the fields in Check Point's log files to fields in the database. The queries in both versions of the database will also need to be modified to reflect the IP addressing schema used for a particular network. For example, in the following query from John Ryan's database, the IP address 192.168.0.* represents the internal IP addresses used on that particular network.

```
SELECT [Current Log].*
FROM [Current Log]
WHERE ((([Current Log].[src]) Not Like "192.168.0.*") And (([Current
Log].[s_port]) Like "0" Or ([Current Log].[s_port])="1" Or ([Current
Log].[s_port])="2" Or ([Current Log].[s_port])="3" Or ([Current
Log].[s_port])="4" Or ([Current Log].[s_port])="5"));
```

This query is looking for all activity originating from outside the firewall trying to use the source ports zero through five. If this query is used in a network where the internal clients are using the IP address 10.10.*.*, then the IP address 192.168.0.* would need to changed to 10.10.* in all queries that differentiate between incoming and outgoing traffic.

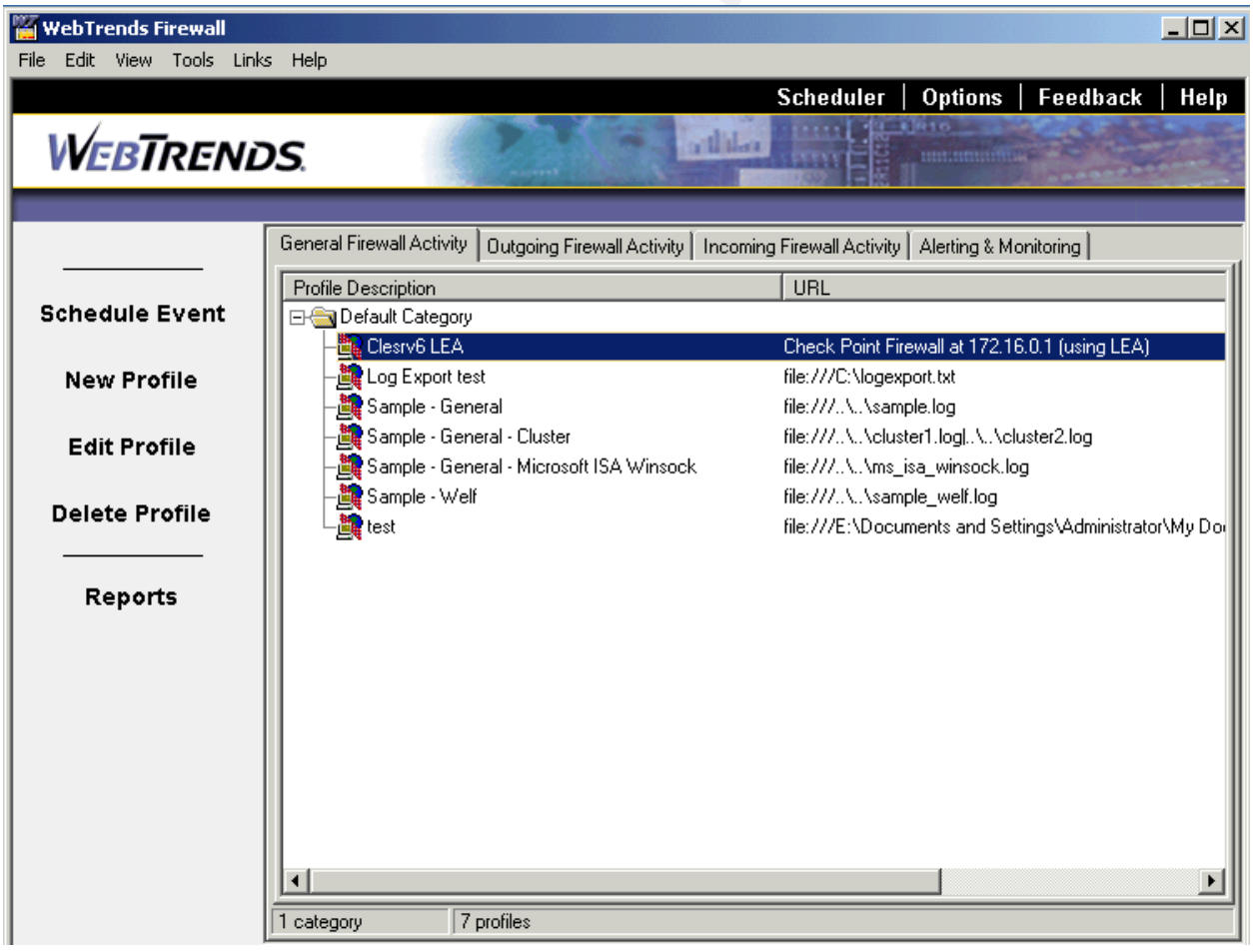
With a little SQL programming knowledge, additional queries could be written to get even more detailed information out of the imported logs. Additionally, the data source could be moved to a more robust database allowing for a more scalable database. Regardless of which version of the database is used, this proves to be a quick method to get valuable data extracted out of the firewall logs.

Firewall Suite

Webtrends Firewall suite (http://www.webtrends.com/products/firewall/default.htm) is another tool that can automate the central storage of firewall logs as well as help the administrator filter through the vast amounts of log data generated. Firewall suite supports over 35 firewalls including Checkpoint FW-1. Firewall Suite comes with 200+ reports built in and can be published in Word, Excel or HTML format. Each of the reports comes with a template so they can be customized to meet individual needs. There are several reports built specifically for security, aimed to assist the admin in identifying any warnings, critical errors logged or rules triggered on the firewall.

To install Firewall suite, a minimum of Windows NT 4.0 workstation is required. Windows 2000 workstation and Windows XP are also supported. Hardware requirements include 1GB of disk space and 512k MB of RAM.

With Firewall suite, reports can be built that will report on all Firewall activity or it can isolate Outgoing and Incoming traffic, depending on the reporting requirements.



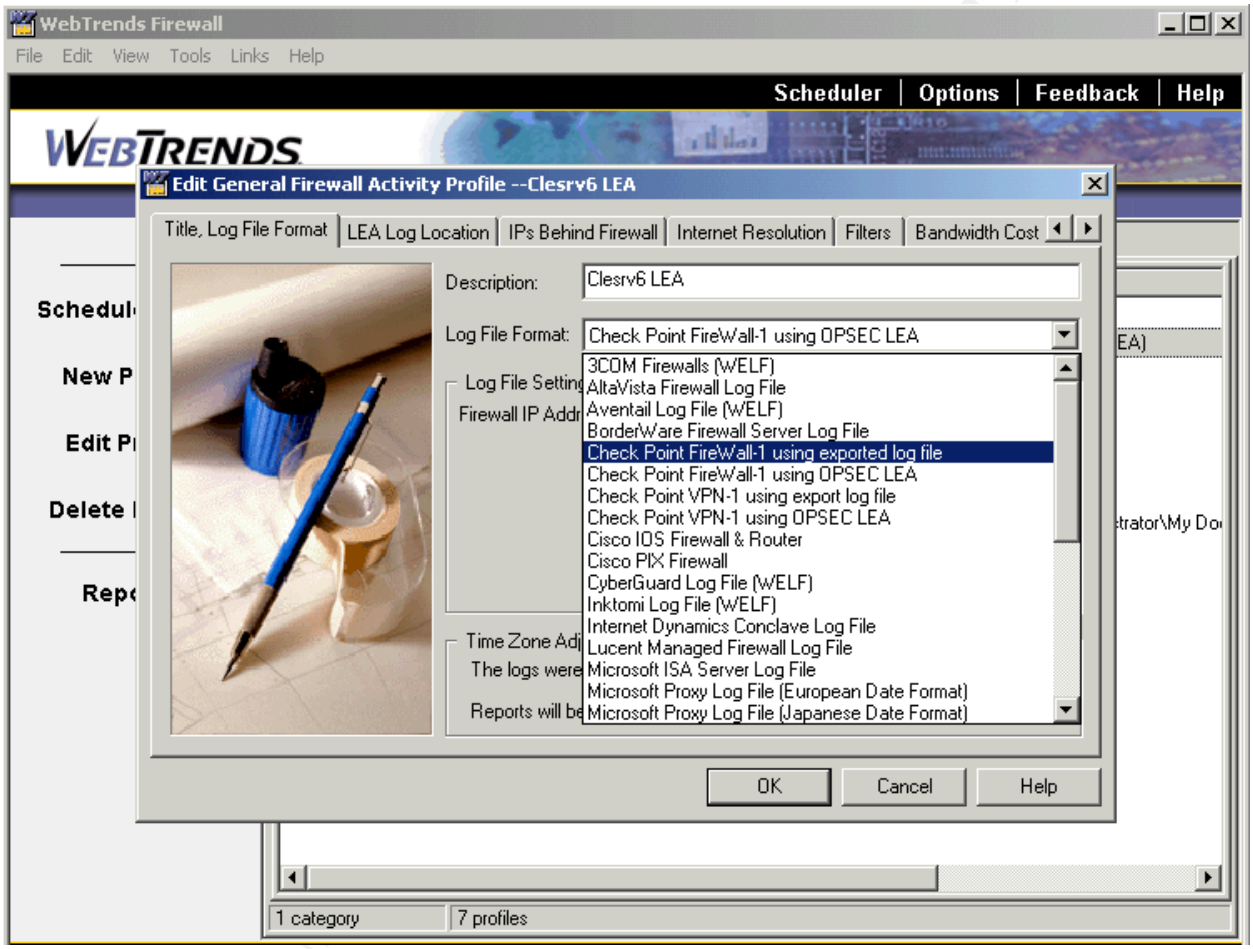
All reporting in Firewall suite is setup through Profiles. Profiles contain all the information

necessary to generate the reports desired. When creating or editing a profile the following information is needed:

- Title, Log File Format: Here the title of the report defined and most importantly, how the log files are collected. For checkpoint FW-1, there are 2 options available:
    - Exported log files: As part of many firewall log file maintenance plans, the firewall logs are exported for archival purposes. If this is the case, these same exports can be used as the input for security reporting in Firewall Suite. Simply indicate the log file path and all reports generated will be based on these log files.
    - OPSEC LEA: Checkpoint has developed the Open Platform for Security (OPSEC). "OPSEC is a single platform architecture designed to allow integration and management of all aspects of network security through an open extensible framework" (Checkpoint, http://cgi.us.checkpoint.com/rl/resourcelib.asp - OPSEC). LEA, Checkpoints Log Export API, allows third parties direct access to the checkpoint logs. With the OPSEC LEA option chosen, the IP address of the management server is required.
- LEA Log Location: The default option is to store the LEA logs on the Firewall suite installation in *%firewall suite installation dir%\LeaCache\%ip_address_of_management_server%.dat*. In this directory there will be a separate log file for every day logs are collected.
- IPs Behind Firewall: Indicate the network portion of the internal IP address schema. This information is used to distinguish between incoming and outgoing traffic.
- Internet Resolution: Use this option to control how the IP addresses are represented in the reports generated. IP addresses can be resolved to host names if desired.
- Filters: Filters can be used to report on specific Protocols, times of day, specific rules, specific firewalls and much more.
- Bandwidth Cost: This section doesn't have a direct security correlation, but it can be used to generate charge back reports for Internet usage.
- Database and Real-Time: By default, all information is stored in a proprietary database format optimized for speed of reporting, the FastTrends database. Optionally, an ODBC data source can be specified.

- Advanced FastTrends: If space on the Firewall suite installation becomes an issue, the FastTrends database can be stored in a different location, which can be specified here.

- Firewall Name(s): This will list all the firewall being reported on in this profile and is auto generated when a report is run.



If the logs are collected using OPSEC LEA, the management server will need to be configured to allow this communication. Two items will need to be added to the management server:

1. Create a rule allowing OPSEC LEA traffic (pictured below):

2. Edit the fwopsec.conf file on the management server and add the following line:
   Lea_server port 18184

Once the previous two items are added, be sure to re-compile the firewall rulesets. Also, on the

Firewall suite installation, stop and restart the *WebTrends Lea Server* service.

Below is an example of the security reports generated with Firewall Suite:

Warnings for External Addresses

This section identifies the top external users responsible for causing an event logged as an error or warning and how many times the event occurred. All errors with the same number for a given address are grouped. Only events that originated outside your firewall are included in this table.

Warnings for External Addresses		
Address	**Description**	**# of events**
10.10.51.215	drop	316
10.10.211.24	drop	177
172.18.21.5	drop	173
10.4.56.3	drop	94
192.168.134.1	drop	27
10.10.9.65	drop	12
192.168.1.1	drop	11
10.10.10.34	drop	9
10.10.5.95	drop	9
192.168.34.5	drop	9

With the profiles in place, reports can be generated on demand or published on an automated schedule. There is a scheduler built in to Firewall suite that can be used for this purpose.

On the housekeeping side of things, if the logs on the Check Point Management server are being rotated using fw logswitch, this will need to be coordinated this with the Firewall suite installation. In the directory configured to store the LEA logs, there will be a text file with a pointer to the last record retrieved from the management server called *lastrecord.txt*. If accounting information is also being logged, there will also be a *lastrecord_a.txt*. Use the following steps if log rotation is part of the log maintenance plan:

1. Stop the *WebTrends LEA Server* service on the Firewall suite installation.
2. Run *fw logswitch* on the management server.
3. Delete *lastrecord.txt* and *lastrecord_a.txt* in the directory storing the LEA firewall logs.
4. Restart the *WebTrends LEA Server* service on the Firewall suite installation.

As discussed earlier, having a solid understanding of the general activity and use of the firewall will go a long way in determining when something abnormal is occurring. Firewall Suite has other reports that detail the general statistics of the firewall; Web/FTP/Telnet usage, Email usage, bandwidth utilization, bandwidth usage trends and much more. All of these reports help complete the overall picture of the health of the firewall.

Security Manager

Another tool that can be used to automate the management and monitoring of firewall logs is

Security Manager by NetIQ. Information regarding Security Manager can be reviewed by. Security Manager provides the following functionality for Check Point FW-1:

- *Central log consolidation*. With multiple log sources to monitor, having all the logs stored in a central location makes the task of monitoring the logs easier for the administrator. Security Manager will consolidate all the logs and store them in a central repository (either MSDE or SQL server). Having the logs stored in a central, secure location - independent of the firewalls and management servers, has the added benefit of making it more difficult for an intruder to cover their tracks by clearing or modifying the logs. This also allows easy archival of the logs for review and inspection days, weeks or months after they were originally recorded.

- *Identify External Attacks*. Any suspicious activity happening on the firewall is recorded in their logs. Trapping things like Port scanning or malformed packets and alerting the administrators when they are occurring makes the job of securing the network and protecting company resources an easier task.

- *Provide automated responses*. When any anomaly is detected, Security Manager can alert the administrators of the activity as well as perform automated responses. For example, in the rules that detect an external attack, a script can be run in response to that attack and the administrators can be emailed and/or paged with details of what happened.

The architecture of Security Manager requires that a central server be configured which is responsible for recording the all events in a single repository. In addition to maintaining this database, this central server also keeps track of all agents deployed in the environment (known as the Consolidator/Agent Manager). Agents are installed on all systems being monitored, in this case the Check Point Management Servers. There is another component on the central server called the Database Access Server (DAS). The DAS is responsible for controlling any communication with the database. For example, when an administrator wants to add monitored systems or change what is being monitored on an existing system, the DAS is responsible for inserting this information into the repository and relaying this information back to the administrator.

To install the Security Manager repository and other central components to monitor 10 systems or less, the following are the minimum requirements:

- Hardware: 300Mhz Pentium, 1.2Gb disk space, 256Mb Ram. Note: The hard disk requirements include 800Mb allocated for the databases used by Security Manager.
- Operating system: Windows 2000.
- Software: Microsoft SQL 2000 Desktop Engine (MSDE), Microsoft Data Access Components (MDAC), and Microsoft Management Console v1.1 (MMC).

In environments that have more than 10 computers to monitor, the setup requirements change slightly. For example, the repository moves from MSDE to SQL v7 Service Pack 3 or SQL 2000 and the Operating System requirements change to include Windows NT 4.0 Service Pack 4 or later as well as Windows 2000. Additionally, in larger environments, the components of the central server can be installed on different machines, providing better performance and fault tolerance. For example, the Repository could be installed on a separate server then the DAS and Agent Manager. The installation documentation provided with Security Manager details the various installation options available.

As mentioned previously, Security Manager uses an agent technology for monitoring servers. Each computer being monitored has an agent installed locally. The requirements for the agent installation are:

- Hardware: 200Mhz Pentium Pro or later, 100Mb of disk space, and 64Mb of RAM.
- Operating System: Windows NT 4 Service Pack 4 or later, or Windows 2000.

The agent is responsible for running any rules or scripts as defined by the administrator and monitoring the log files. For example, when installed on a Check Point Management Server, rules are enabled by default for capturing the firewall logs (using OPSEC LEA) and forwarding these logs to the Agent Manager. The agent also runs any scripts locally on the managed computer. With this architecture the agent will process all scripts and notifications locally and if communication cannot be established with the agent manager, temporarily store all logs locally. When communication is re-established with the agent manager, all log information stored locally will be forwarded to the agent manager and be inserted into the repository.

Prior to agent installation on a Check Point Firewall Management server, two changes need to be made to the policies installed on monitored firewalls. First, the Firewall Management server needs to be able to use the Log Export API service (LEA). To do this, create a rule in the policy rule set that allows LEA service communication using the clear connection port specified *fwopsec.conf* or port 18504 if no clear connection port is specified.

Second, the Agent Manager component of Security Manager needs to be able to communicate with the Firewall Management server. By default, Security has two modes of communication, encrypted and unencrypted communication, which use ports 1270 and 51515 respectively. Both use TCP for communication. Below is an example of these two rules in Policy Editor. SM_AGENT is configured for encrypted communication and sm_agent2 is configured for unencrypted communication.

Once these policies are deployed, the agent can be installed on the Firewall Management Server. In most cases, installing the agent is an automated process. The administrator needs to define what machines are going to be monitored and configure rules in Security Manager that reflects these decisions. Typically, rules are configured which allow an entire domain to be managed and/or specific machines within a domain are targeted for management. Firewalls and the Check Point Management server usually fall into the category of machines that are not a good candidate for automated installation, as they are not normally part of the production domain. (The agent manager can install agents remotely since it is running with privileges in that domain and any domain with the appropriate trusts configured. A typical firewall is installed in a workgroup and the domain doesn't usually have privileges. Therefore the agent needs to be manually installed). To install an agent on a Check Point Management server manually, use the following steps:

1. Run Setup from the *Manual Agent Installation* folder on the Security Manager CD while logged in with administrator privileges.
2. Choose both *Security Manager Agent* and *Check Point Firewall-1 Support*.
3. If displayed, select the IP address that is licensed with Check Point.
4. Enter the name of the *Configuration Group* used by Security Manager. (A configuration group name is entered when the Security Manager server components are initially installed.)
5. Enter the IP address of the Agent Manager (consolidator). To configure advanced items like the use of encrypted or unencrypted communication, click the *Advanced* button.
6. For *Agent Manager Control Level*, select *None*. (The agent manager cannot install and uninstall this agent per the rights issues outlined above.)
7. If there are any locked files or any services need stopped, take the appropriate actions and click *Finish*.

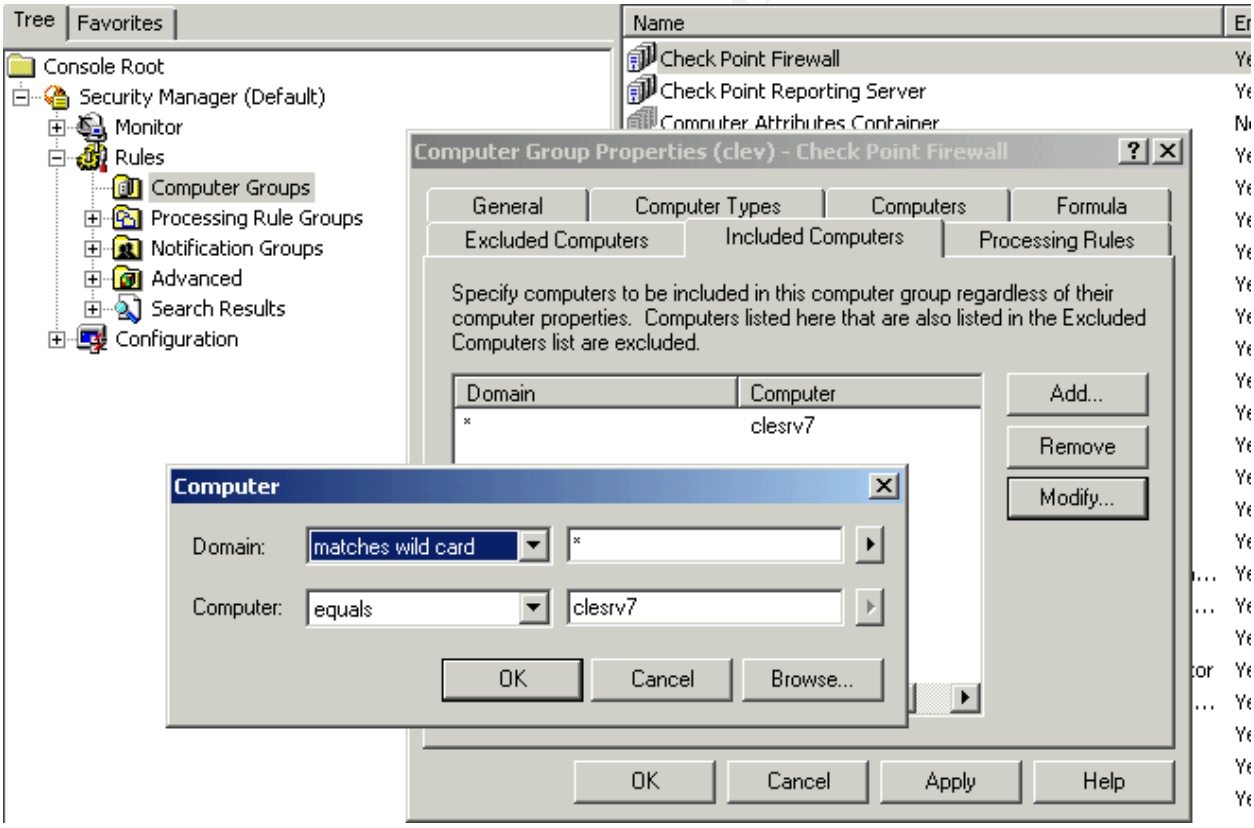
With agents installed manually, the agent manager component of the Security Manager installation needs to know two additional pieces of information: First the Consolidator/Agent Manager needs to know the agent exists. To accomplish this, use the following:

1. Create a text file called *ManualMC.txt* in any text editor.
2. Enter one computer name per line, representing the computers with manually installed agents.
3. Save the text file to the *\MCS onepoint\One point* folder where Security Manager was installed. Typically this directory will be *c:\program files\MCS Onepoint\one point\ManualMC.txt*.

Second, the newly installed agent needs to be associated with the *Check Point Firewall* computer group in Security Manager. Computer groups are used in Security Manager to determine what applications and processes are installed on a server. This functionality allows all agents to run only the rules associated with applications installed on that particular agent. For example, Security Manager has rules to monitor Check Point Firewall-1 as well other application like IIS. If IIS is not installed on the Check Point Management Server, the IIS rule sets will not be running

on that agent. To associate the manually installed agent to the Check Point Firewall computer group:

1. Open the Security Manager administrative tool MMC and expand *Security Manager* in the left pane.
2. Expand *Rules* in the left pane.
3. Select *Computer groups* in the left pane.
4. Right click the *Check Point Firewall* computer group in the right pane and select *Properties*.
5. Click the Included computers tab.
6. In the *Domain* field, select *matches wild card* and enter a wildcard (*). Many times the firewall/management servers are not part of a domain, but a workgroup. Using the wildcard will cover workgroups as well. Alternatively, the name of the workgroup could be entered.
7. In the *Computer* field, select *equals* and enter the name of the Firewall Management Server.

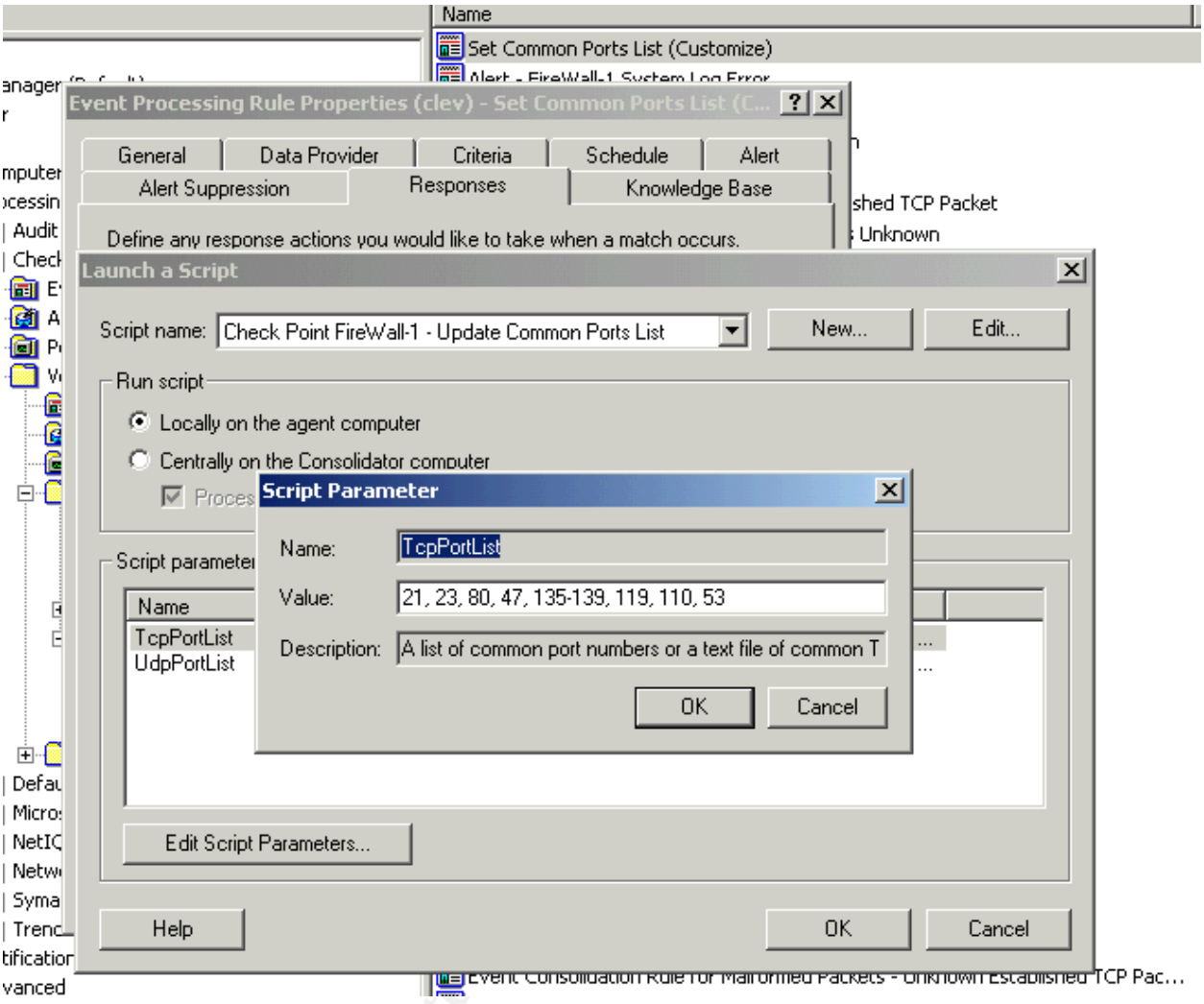


These configuration changes allow the Agent Manger to send the appropriate rules to the agent and allow the Consolidator functionality of Security Manager to receive and process logs and alerts from the Firewall Management Server. With everything in place, Security manager will begin processing and storing the firewall logs.

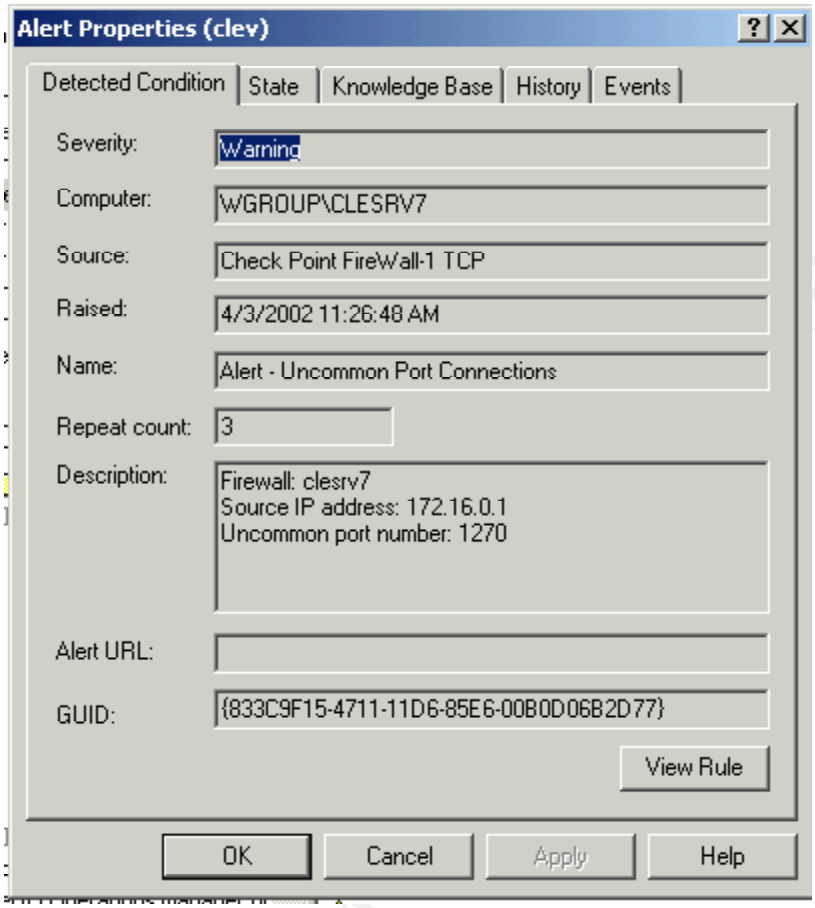
By default, the rules to alert on potential port scans and malformed packets are enabled in Security Manager. To detect Port Scanning, Security Manager requires that the Check Point Malicious Activity Detector (CPMAD) be enabled on the Check Point Firewall-1 installations. CPMAD can identify attacks like: SYS flooding, anti spoofing, land attacks, port scanning and more. When CPMAD detects a port scan it will add an entry to the firewall logs. Securtiy Manager will pick up this entry, generate an alert and optionally notify the administrator of its occurrence.

Another nice feature is the ability to alert the administrator when any unexpected port is allowed a connection. To implement this, a list of what is considered 'common ports' needs to be configured in Security Manager. Edit the rule *Set Common Port List (Customize)* and enter a list of common ports, or optionally enter a path to a file containing the same information. To edit the Set Common Port List scripts:

1. Double click on the *Set Common Ports List (Customize Script)*.
2. Click the *Responses* tab, highlight the only response listed – *Check Point Firewall-1 Update Common Ports List* and click *Edit*.
3. Highlight *TcpPortList* under Script parameters and click *Edit Script Parameters*.
4. Enter the ports considered as common (or enter the file with the same listing).
5. Optionally add a list of ports for *UdpPortList*.



Here is an example of an alert generated on the detection of an uncommon port connection – port 1270. Notice that port 1270 is not listed in the *TcpPortList* above.



Port 1270 is the encrypted port used by the agent to communicate with the Agent Manager. To keep from being alerted on this port as it is expected to be a normal part of the communication stream on a Check Point Management Server with the Security Manager agent installed, add port 1270 to the common port list TcpPortList.

In addition to the specific examples provided above, Security Manager can be configured to alert or report on any traffic patterns on a specific firewall or group of firewalls. Alerts can also be generated on control messages logged by the management server. Additionally, custom rules can be developed for any special considerations or services the administrator determines to be important.

Conclusion

In most organizations, the Firewall is the first layer of defense and needs to be closely monitored. With the amount of logs a correctly configured Firewall will generate, keeping a close eye on intrusion attempts and malicious activity can be a daunting task.

While there are many tools available designed to monitor these logs with a wide range of functionality, choosing the right tools for a particular environment has many variables including specific functionality, firewalls supported and budget. The tools presented here represent a

subset of the tools available and can serve as a starting point for any administrator wanting to automate the process of monitoring and managing a firewall's logs.

References

Welch, D. "PhoneBoy's Firewall-1 FAQ's". URL: http://www.phoneboy.com/ (29 Feb. 2002).

Internet Assigned Numbers Authority. "Protocol Numbers and Assignment Services". 27 March 2002. URL: http://www.iana.org/numbers.htm#P (6 April 2002).

Simovits Consulting. "Ports used by Trojans". 30 June 2001. URL: http://www.simovits.com/nyheter9902.html (5 April 2002).

Taylor, Laura "Read Your Firewall Logs", 10 July 2001. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2782699,00.html (29 Feb. 2002)

Graham, Robert. "FAQ: Firewall Forensics (What am I seeing?)." 20 June 2000. URL: http://www.robertgraham.com/pubs/firewall-seen.html (2 April 2002).

Spitzner, Lance. "Intrusion Detection for FW-1." 22 Dec. 2001. URL: http://www.enteract.com/~lspitz/intrusion.html (5 April 2002).

Ryan, John. "Security Logs and Checkpoint Firewall1". 4 June 2001. URL: http://rr.sans.org/firewall/logs.php (5 April 2002).

Ryan, John. "An MS Access database to analyze Checkpoint Firewall-1 logs". 5 June 2001. URL: http://secure-net.hypermart.net/index.htm (2 March 2002).

Spitzner, Lance. "Welcome to Logger". URL: http://www.enteract.com/~lspitz/logger.html (4 March 2002).

Webtrends. "Firewall Reporting". URL: http://www.webtrends.com/products/firewall/default.htm (6 March 2002).

Checkpoint. "OPSEC". URL: http://cgi.us.checkpoint.com/rl/resourcelib.asp - OPSEC (6 March 2002).

NetIQ. "Products: Security Manager". URL: http://www.netiq.com/products/sm/default.asp (8 March 2002).