Interested in learning more about security?

SANS Institute
InfoSec Reading Room

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

Using ISA Server Logs to Interpret Network Traffic

Firewalls are necessary for a defense-in-depth strategy. Microsoft entered the firewall market with Internet Security and Acceleration Server (ISA Server). ISA Server was a follow-on release of Microsoft Proxy Server and part of the .Net Family. As with most Microsoft products, logging capabilities are included. ISA Server contains detailed security and access logs. This paper focuses on ISA logs and how you can use them to interpret the types of traffic passed through the network.

Copyright SANS Institute
Author Retains Full Rights

AD

Using ISA Server Logs to Interpret Network Traffic

Introduction

Firewalls are necessary for a defense-in-depth strategy. Microsoft entered the firewall market with Internet Security and Acceleration Server (ISA Server). ISA Server was a follow-on release of Microsoft Proxy Server and part of the .Net Family. As with most Microsoft products, logging capabilities are included. ISA Server contains detailed security and access logs.

This paper focuses on ISA logs and how you can use them to interpret the types of traffic passed through the network. This paper includes the following sections:

- General Log Information
- Configuring Logging
- Interpreting Logs
- Reporting

You can install ISA Server in three different modes: firewall mode, web caching mode, or integrated mode. In firewall mode, you can secure communication between an internal network and the Internet using rules. You can publish internal servers so that their services are available to Internet users. In web caching mode, you can decrease network bandwidth with ISA Server storing commonly accessed objects locally. You can route web requests from the Internet to an internal Web Server. In integrated mode, all of these features are available.

General Log Information

ISA Server provides detailed security and access logs for all traffic that passes through the firewall service and the web caching service. You can generate new logs on a daily, weekly, monthly or yearly basis.

Depending on how ISA Server is installed, there are three types of logs are available:

- **Packet Filter** – contains information about the packets that ISA Server examines. By default, only dropped packets are logged. Disabling packet filtering turns this logging off. You can also disable logging for certain packets that are dropped due to a specific block-mode IP-filter. ISA Server can also log all packets including allowed packets. This greatly increases the amount of logging done on the ISA Server and Microsoft recommends against logging all packets.
- **Firewall** – contains information about all traffic sent through the firewall service, including the client and destination IP address, the ports used, the protocol, and the transport.
- **Web Proxy** – contains the same information as the firewall log, but specific to the web proxy server.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

ISA Server uses two types of logging: text based log files or logging into a database. Two formats are available in the text logging: World Wide Web Consortium (W3C) extended log file format or ISA server file format. For the purpose of this paper, we use ISA Server file format for interpreting the logs.

- The W3C file format contains data and information about the version, date and logged fields. Fields that are not selected in the logging options are not logged since the fields are described in the log files. A tab delimiter is used, and times are recorded in GMT.
- The ISA Server file format contains only data. Unselected fields are recorded as a dash to indicate they are empty. A comma delimiter is used, and date and times are recorded in local time.

These logs are by default recorded in the ISA Server installation directory in a folder called ISALogs (i.e., C:\Program Files \Microsoft ISA Server\ISALogs\). The naming convention for the different log formats in relation to how often new log files are created is detailed below:

Log Format	Daily	Weekly
Packet Filter W3C format	IPPEXTDyyyymmdd.log	IPPEXTDyyyymmw.log
Packet Filter ISA format	IPPDyyyymmdd.log	IPPDyyyymmw.log
Firewall W3C format	FWSEXTDyyyymmdd.log	FWSEXTDyyyymmw.log
Firewall ISA format	FWSDyyyymmdd.log	FWSDyyyymmw.log
Web Proxy W3C format	WEBEXTDyyyymmdd.log	WEBEXTDyyyymmw.log
Web Proxy ISA format	WEBDyyyymmdd.log	WEBDyyyymmw.log

Log Format	Monthly	Yearly
Packet Filter W3C format	IPPEXTDyyyymm.log	IPPEXTDyyyy.log
Packet Filter ISA format	IPPDyyyymm.log	IPPDyyyy.log
Firewall W3C format	FWSEXTDyyyymm.log	FWSEXTDyyyy.log
Firewall ISA format	FWSDyyyymm.log	FWSDyyyy.log
Web Proxy W3C format	WEBEXTDyyyymm.log	WEBEXTDyyyy.log
Web Proxy ISA format	WEBDyyyymm.log	WEBDyyyy.log

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Each log is broken down into numerous fields. Appendix A lists each field and its description for the packet filter log. Appendix B lists fields and their descriptions for the Firewall and Web Proxy Service logs. These fields are described in more detail as we discuss how to interpret the logs.

Configuring Logging

By default, ISA Server performs some minimal logging on the services that you have installed with ISA Server. To gather information that will assist in interpreting network traffic, tweak the logging.

Packet Filter logs:
By default, ISA Server is configured to log every packet that does not match an Allow packet filter rule. While this provides useful information for normal use, administrators who want to know about all of the packets that are seen by the firewall must change this setting.

To change this setting:

1. Open the ISA Management MMC.
2. Right click on IP Packet Filters under Access Policies.
3. Select the Packet Filter tab.
4. Enable "Log packets from 'Allow' filters".
5. Select OK to save and update the configuration.

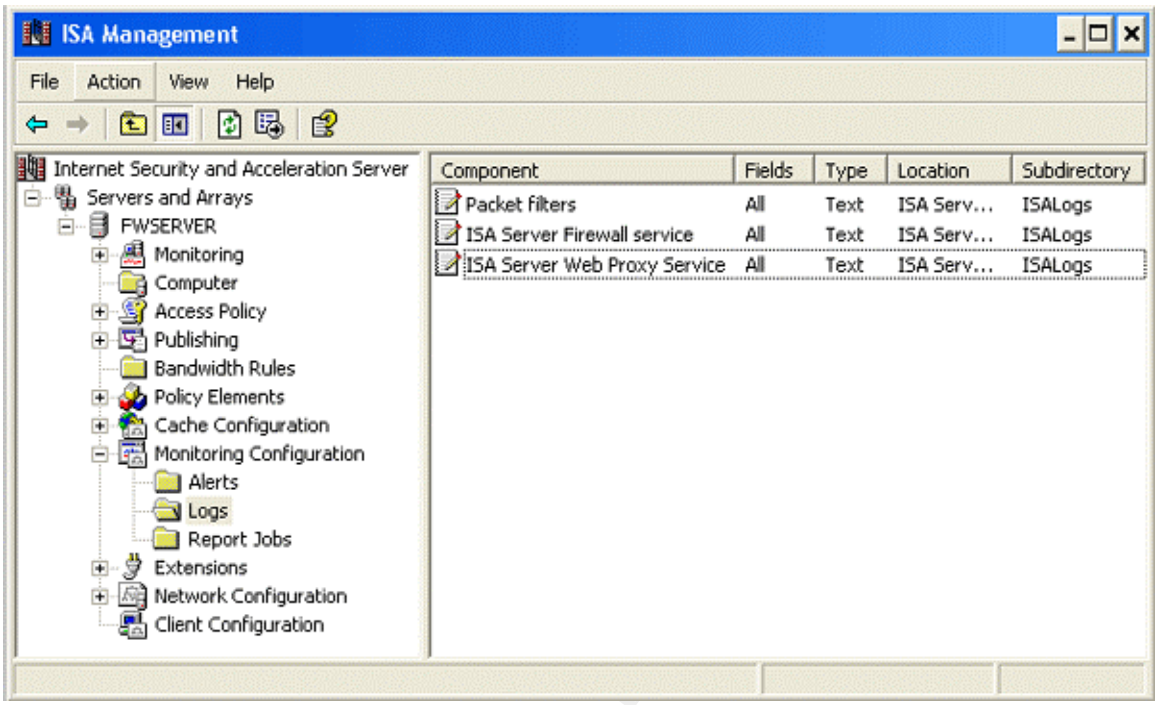
An important note about logging all packets: In high traffic networks, these settings can cause performance degradation and eventually fill the hard drives of the ISA Server. Use caution if you turn on this setting.

Another way to increase the amount of information available in the logs without logging all of the packets that passed filters is to change the fields that are logged. This gives you the ability to see entire packets that were denied, including the header and the payload.

To adjust these settings:

1. Open the ISA Management MMC.
2. Choose Monitoring Configuration | Logs.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



3. Double-click Packet filters to open the Packet filters Properties.
4. Select the Fields tab.
5. Choose all the fields that you want to log. (For this paper, we assume that all fields have been chosen.)
6. Select OK to save and update the configuration

Firewall Service Logs

By default, ISA Server is configured to log connections made through the firewall service. This is good for having a minimum amount of information about your network traffic, but for administrators who want to have more than that baseline, you must extend the logging details. You can adjust the Firewall Service log properties. These settings are adjusted in the same manner as before, except the you must double-click ISA Server Firewall service to launch the appropriate Properties window.

Web Proxy Service Logs

By default, ISA Server is configured to log requests that come through the Web Proxy Service. These logs contain very important information about the Internet traffic that users on your network are creating. While most of the information for interpreting these logs is set to be logged by default, there is information that can be useful for troubleshooting that is not logged, such as the rules that are allowing the traffic to pass through. Including this information in the Web Proxy Service logs can assist an administrator in determining holes in his content rules and access policies. These settings are adjusted in the same manner as the Packet filter logs except you must double-click he ISA Server Web Proxy Service to launch the appropriate Properties window.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Interpreting Logs

More technically savvy administrators can manually open the individual logs and look for suspicious activity. Here are some examples from the different log files and what those entries are telling us.

NOTE: All records and packets were created solely for the purpose of this analysis and modified to protect the IP addresses and Web sites of those involved.

Packet Filter Logs

Packet 1:

Field	Data
Date	4/24/2002
Time	20:56:12
Source IP	192.168.82.195
Destination IP	10.8.14.78
Protocol	ICMP
Source Port	8
Destination Port	0
TCP Flags	-
Interface	BLOCKED
Interface IP Address	10.8.14.78
Header	45 00 00 3c 2c f8 00 00 6b 01 ed 65 d8 0c e4 63 18 a0 60 53
Payload	08 00 20 5c 02 00 2b 00 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69

Packet 1 shows an ICMP echo request. This is determined by looking at the source port field (which for ICMP traffic is the code used when creating the connection). The ICMP type is also described in the first characters of the payload, 08 (ICMP Type Settings). If we take the last half of payload (starting with 61 62 63…) and convert it to ASCII, we see that it equals `"abcdefghijklmnopqrstuvwabcdefghi"`, which is normally the result of someone using ping.exe from a Windows machine (arachNIDS).

Packet 2:

Field	Data
Date	4/24/2002
Time	20:59:15
Source IP	192.168.82.195
Destination IP	10.8.14.78
Protocol	TCP
Source Port	2876
Destination Port	1
TCP Flags	SYN
Interface	BLOCKED
Interface IP Address	10.8.14.78
Header	45 00 00 30 37 42 40 00 6b 06 a3 22 d8 0c e4 63 18 a0 60 53

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Field	Data
Payload	0b 3c 00 01 65 e9 cf 72 00 00 00 00 70 02 fa f0 12 32 00 00 02 04 05 b4 01 01 04 02

Packet 2 shows a TCP SYN packet being sent to port 1 of the target machine. Seeing numerous packets of this nature being sent to multiple ports (sometimes sequentially) can indicate that a port scan is being run against the destination IP. Another common port scan method is to send FIN packets instead of SYN packets. This type of scan is typically referred to as a stealth scan.

Firewall Logs

Firewall Record #1

Field	Data
Client IP	10.1.1.4
Client Username	smithjd
Client Agent	OUTLOOK.EXE:3:5.1
Authentication Status	N
Date	4/25/2002
Time	16:18:27
Proxy Name	FWSERVER
Destination IP	192.168.11.27
Destination Port	25
Processing Time	48000
Bytes Sent	1323
Bytes received	565
Protocol Name	25
Transport	TCP
Operation	Connect
Rule #1	Mail
Rule #2	Allow Inbound
Session ID	5
Connection ID	26

Firewall Record #1 is from a client that is running the ISA Firewall Client provided with ISA Server. With the client installed, the log is able to record much more information about the traffic the ISA Server is seeing. From this record, the IP address, client username and the agent information is revealed. The agent information contains both the actual executable process that is attempting access through the firewall and a string of numbers that describe the operating system that the client is using. This particular value, 3:5.1, is Windows XP. (For a complete listing of the possible values, see Appendix B.) The destination IP and port of the remote server tell us that the connection was sent to port 25, the standard SMTP port. The rules that allow this traffic both in and out are recorded. Mail is the outbound rule and Allow Inbound is the inbound rule. The session ID is important in tracking an entire communication string for a client.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Firewall Record #2

Field	Data
Client IP	10.1.1.5
Client Username	-
Client Agent	-
Authentication Status	N
Date	4/24/2002
Time	17:09:20
Proxy Name	FWSERVER
Destination IP	192.168.4.9
Destination Port	443
Processing Time	547
Bytes Sent	39
Bytes received	44
Protocol Name	443
Transport	TCP
Operation	Connect
Rule #1	Web Traffic
Rule #2	Allow Inbound
Session ID	64
Connection ID	2010

Firewall Record #2 is from a client that is not running the ISA Firewall Client and shows significantly less information than the record from the client running the ISA Firewall Client. The IP address is the only identifying information of the client that we have. More has to be inferred by using the destination port and the protocol name (which in the firewall log is actually the port that the protocol uses). Communication to port 443 is normally SSL data sent from a web browser. Also seeing that the Web Traffic rule that was setup on the ISA Server is what allowed this communication to occur, it is a bit safer to assume that this is traffic from a web browser.

Web Proxy Logs

Web Proxy Record #1

Field	Data
Client IP	10.1.1.1
Client Username	anonymous
Client Agent	Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Authentication Status	N
Date	4/24/2002
Time	19:20:26
Proxy Name	FWSERVER
Destination name	www.nositename.com
Destination IP	192.168.3.15
Destination Port	80
Processing Time	8953

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Field	Data
Bytes Sent	311
Bytes received	1460
Protocol Name	http
Transport	TCP
Operation	GET
Object MIME	text/html
Object Name	http:// www.nositename.com /
Object Source	Inet
Result Code	200
Rule #1	Web Traffic
Rule #2	Allow Inbound

Web Proxy Record #1 shows an anonymous connection to a website called http://www.nositename.com where the Web Proxy retrieved an HTML page using a http GET command over TCP. Record #1 also reveals the client IP address and that the user was using Internet Explorer 5.01 running on Windows 2000 without being authenticated to the Web Proxy service. The Object Source and Result Code are important in determining if the Web Proxy service is functioning correctly. Inet means that the content came from the Internet and added to the local web cache; while a Result Code of 200 means that the connection was established without problems. Rule #1 shows the rule that allowed the traffic to leave the network and Rule #2 shows the rule that allowed the content back into the network.

Web Proxy Record #2

Field	Data
Client IP	10.1.1.1
Client Username	anonymous
Client Agent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Authentication Status	N
Date	4/28/2002
Time	21:04:50
Proxy Name	FWSERVER
Destination name	www.nositename.com
Destination IP	192.168.3.15
Destination Port	80
Processing Time	10938
Bytes Sent	372
Bytes received	185501
Protocol Name	http
Transport	TCP
Operation	GET
Object MIME	http://www.nositename.com/application.zip
Object Name	application/zip
Object Source	Inet
Result Code	200

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Field	Data
Rule #1	Web Traffic
Rule #2	Allow Inbound

Web Proxy Record #2 shows an anonymous connection to the same website as Web Proxy Record #1 except the activity at that website is a little different. The Object MIME and Object Name are important here as it shows that the user downloaded a ZIP file from the Internet. You can track the download habits of users to help enforce company computing policies.

Reporting

ISA Server provides some built-in reporting features, but we will also look at some third-party products that interpret ISA Server logs. First, we can look at the native reporting tool included with ISA Server.

The built-in reporting tool provides the ability to generate summary reports with minimal customization options for users. It generates the following types of reports:

Summary Reports
Data is drawn from both the Web Proxy and Firewall Service Logs pertaining to Network Usage. This is a general report that summarizes the other report types included in ISA Server.

Web Usage
Data is collected from the Web Proxy Logs. These reports include the following information (Shinder, 358):

- Top Web Users
- Top Web Sites
- Protocols used for web traffic
- HTTP Responses
- Object Types delivered by the ISA Server
- Browsers used to connect through ISA Server
- Operating Systems used to connect through ISA Server
- Browsers vs. Operating Systems

The Web Usage reports are beneficial in identifying the type of traffic that is flowing through the web proxy service, including who the top users are and what type of content they are requesting. This information can be used to ensure proper use of the Internet by employees as well as see how effective the ISA server is in caching information.

Application Usage
Data is collected from the Firewall Logs. These reports include the following information (Shinder, 359):

- Protocols used for network traffic passing through the ISA Server

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Top Application Users (by IP address)
- Top Applications that generated the most usage on a per megabyte basis
- Operating Systems used to connect through ISA Server
- Top Destinations (by IP address)

Application Usage reports are useful for determining what and how applications are accessing the Internet. Watching what protocols traffic is communicating through can help determine possible security breaches. For example, a high number of requests coming through a protocol definition that is supposed to see little to no traffic could be a malicious program that has been installed and passing data to the Internet.

NOTE: The Application Usage reports will only show the actual application that is accessing resources outside the firewall if the ISA Firewall Client is installed on individual machines.

Traffic and Utilization Reports
Data is collected from both the Web Proxy and Firewall Service Logs. These reports include the following information (Shinder, 360):

- Protocols
- Traffic that passed through the ISA Server (by date)
- Cache Performance - Objects returned from the Internet, from cache without verification, from cache after verifying that they have not changed, from the Internet, updating a file in cache
- Connections - peak number of simultaneous connections (by day)
- Processing Time of requests
- Daily Traffic (in MB)
- Errors communicating with other computers

Traffic and Utilization reports are useful in understanding the overall flow of traffic through an ISA Server. These reports detail how much data passed through the ISA server on a given day, while also detailing, percentage wise, how much data it was able to return through cache. These reports can help in determining when and if additional ISA servers or additional bandwidth is needed.

Security Reports
Data is collected from the Packet Filter, Web Proxy, and Firewall Service Logs. These reports include the following information (Shinder, 360):

- Authorization Failures - users that failed to authenticate to the ISA Server
- Dropped Packets

Security Reports are useful in seeing which users are having the most packets dropped. This can be used as an indicator that a host is trying to perform some type of communication that is not allowed through the firewall. An unusually high number of dropped packets by one particular host could indicate that the host is infected with a Trojan and is trying to communicate back to the Internet.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

While these reports are useful in most cases, some cases require a more advanced approach to reporting. For example, the reports that include destination and client addresses are only displayed as IP addresses. (This is like giving us the phone number for a list of users, but forgetting to give us their names!) ISA reports can be generated and stored only locally on an ISA Server. You also can only look at reports generated locally from an ISA Server, regardless if the target server is in the same array as the ISA Server at which you are sitting. This presents a problem when it comes to centralized storage, management and reporting of firewall logs.

Generating ISA Server Reports

ISA Server reports are generated through the use of report jobs. Numerous report jobs can be created to generate reports that include different date ranges.

To generate a report:

1. Open the ISA Management MMC.
2. Choose Monitoring Configuration | Report Jobs
3. Right Click on Report Jobs and select New -> Report Job
4. Fill in an appropriate name and description for the report.
5. Select the Period tab and select an appropriate time frame for the report to be generated. ISA offers the following time periods:
    a. Daily
    b. Weekly
    c. Monthly
    d. Yearly
    e. Custom
6. Select the Schedule tab and choose run immediately.
7. Select the Credentials tab and provide an account that has permission to access report information.

Scheduling Reports

Report Jobs have the ability to be scheduled to run in the future and also to run at timed intervals. Reports can be scheduled to recur every day, specific days of the week or on a specific day of the month. This is useful in automating the report generation process.

Report Job Credentials

Credentials can be defined for generating reports. This is necessary when a report job is setup to run against a remote computer, or computers in an array. A report job can be generated with providing credentials on a local standalone ISA Server.

Third-Party Reporting

There are several third-party products with reporting capabilities for ISA Server. One of the most popular is WebTrends Firewall Suite (Firewall Suite).

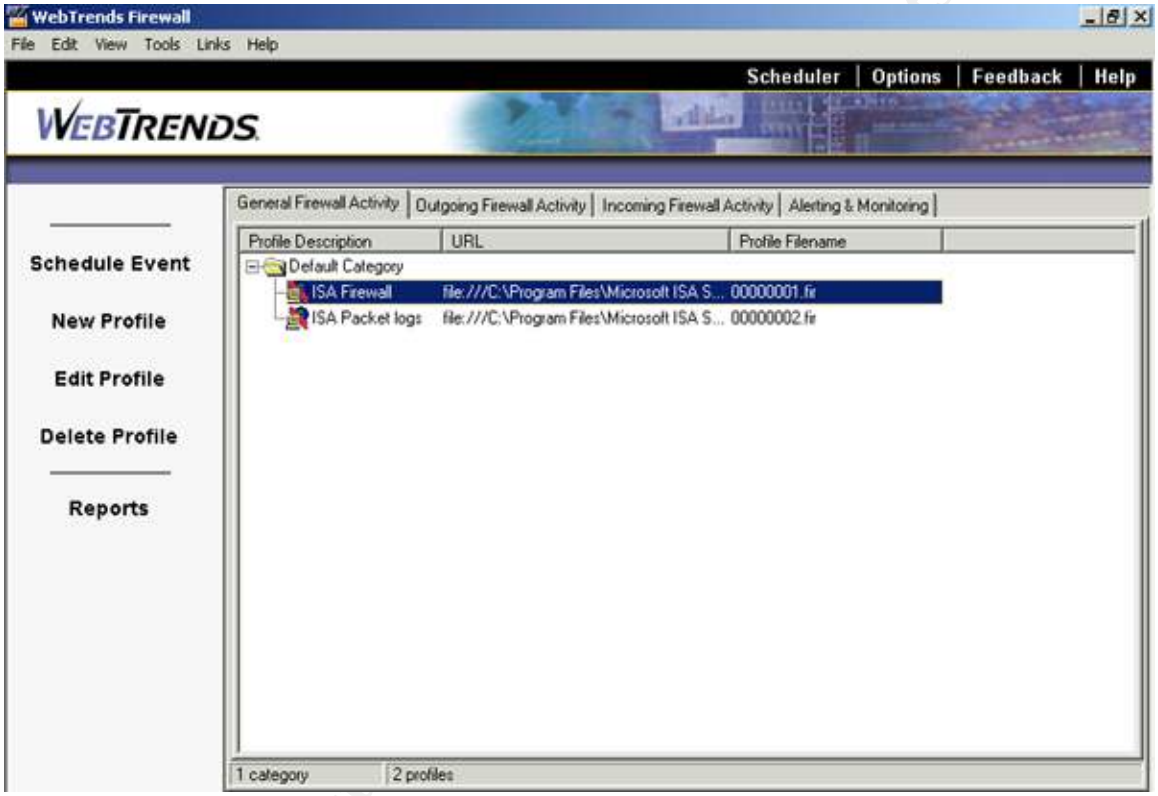
WebTrends Firewall Suite has several key features that make it stand out:

- The ability to consolidate logs from all the firewalls in an enterprise and produce a single set of reports for these products

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The ability to resolve IP addresses that are contained in the firewall logs
- The ability to generate reports on traffic in both directions
- The ability to drill down on events obtaining detailed information.
- Cross-product capabilities that include the majority of the major firewalls in use today

WebTrends Firewall Suite works through the usage of profiles. These profiles contain information about the firewall log that is being analyzed.



To create a new profile for use with ISA Server:

1. Launch WebTrends Firewall Suite
2. In the General Firewall Tab, right click and select New -> Profile
3. Select whether or not the firewall is located on one or multiple machines (One physical machine in this scenario). Select Next
4. Give the profile a description, choose the Log file format (Microsoft ISA Server Log File in this case) and enter the log file path. Select Next
5. Add the appropriate IP addresses that are behind the firewall. Select Next
6. Choose the Domain Name Resolution Mode. Select Next
7. Specify any filters desired. Select Next
8. Add the cost of Bandwidth per Kilobyte. Select Next
9. Select whether to use the FastTrends™ database to store analysis data. Select Next
10. Enter the store location of the FastTrends™ database. Select Finish

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A profile has now been created to analyze an ISA Server Log. There are several bits of data that are important to bring to attention about information that we provided in the profile. WebTrends Firewall Suite asks if the logs are stored on one or more than one physical machine, giving you the ability to generate reports from numerous ISA Servers all at once. It also asks for the cost of bandwidth per kilobyte providing the ability to perform cost analysis on traffic that is being passed through the firewall. It also has the ability to store information in a database for later analysis.

To run the report, double click on the report and the report selection screen is presented where the choice of both the type of report that is to be generated can be made as well as the format of that report. WebTrends Firewall Suite offers numerous report templates out of the box, and all of the reports can be generated in the following formats:

- HTML
- Microsoft Excel
- Microsoft Word
- Text

WebTrends Firewall Suite also offers the ability to create profiles and reports specifically for data coming from the Internet and separate profiles for data coming from an Intranet. It also offers the ability to monitor network devices. It can detect an event a status change and start recovery actions while notifying the operator. It also offers the ability to generate reports that help in tracking how reliable each monitored device (Firewall Suite, Online Help).

Using the built-in reporting functions of ISA Server provides good information about network traffic, and WebTrends Firewall Suite takes it a step further in the actual analysis of that data providing useful information about network traffic.

Conclusion

Knowing how to interpret the data directly from the logs is an excellent skill. Knowing how to interpret logs is not enough; we must know what to do with the data in those logs. Log data and forensic analysis can assist in troubleshooting ISA Server should something happen to your network.

Running reports on the logs can show when and where the majority of the network traffic takes place so that you can adjust resources to increase the performance of the network. It can also help identify unwanted traffic so that you can take measures to remove that traffic. You can identify violators of company security and Internet usage policies. But the most important reason to know the information that your firewall is passing in each direction is to ensure the safe use of Internet resources in an environment.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

The information in this appendix came from the Microsoft Internet Security and Acceleration Server 2000 Online Help and is available online at the following URL: <http://download.microsoft.com/download/ISAServer2000/ProdDocs/1.0/NT5/EN-US/isa2k.chm>

Packet Filter log fields

Field position	Descriptive name (field name)	Description
1	Date (date)	Date the packet was received.
2	Time (time)	The time the packet was received (service info fields)
3	Source IP (source-ip)	The Internet Protocol (IP) address of the source (remote) computer. The source computer is the computer from which the data packets originated.
4	Destination IP (destination-ip)	The IP address of the destination (local) computer. The destination computer is usually the ISA Server computer.
5	Protocol (protocol)	The particular transport level protocol that is used during the connection, such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), or Internet Control Message Protocol (ICMP).
6	Source port (or protocol type, if ICMP) (param#1)	For TCP and UDP protocols, the remote port used to create a connection. For ICMP protocol, the type used when creating the connection.
7	Destination port (or protocol code, if ICMP) (param#2)	For TCP and UDP protocols, the local port used to create a connection. For ICMP protocol, the code used when creating the connection.
8	TCP flags (tcp-flags)	For a TCP data packet, represents the TCP flag value in the IP header. The possible values are FIN, SYN, RST, PSH, ACK, and URG.
9	Interface (filter-rule)	Indicates whether the packet was accepted (1) or dropped (0). By default, only dropped packets are logged.
10	Interface IP address (interface)	Interface on which the packet was received; usually only one interface.
11	Header (ip-header)	The entire IP header of the data packet that generated the alert event. The IP header is logged in hexadecimal format.
12	Payload (payload)	A listing of a portion of the data packet (after the IP

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

header). The IP packet is logged in hexadecimal format.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix B

The information in this appendix came from the Microsoft Internet Security and Acceleration Server 2000 Online Help and is available online at the following URL: <http://download.microsoft.com/download/ISAServer2000/ProdDocs/1.0/NT5/EN-US/isa2k.chm>

Firewall and Web Proxy log fields

Field position	Descriptive name (field name)	Description
1	Client IP (c-ip)	The Internet Protocol (IP) address of the requesting client.
2	Client user name (cs-username)	Account of the user making the request. If ISA Server Access Control is not being used, ISA Server uses *anonymous*.
3	Client agent (c-agent)	The client application type sent by the client in the Hypertext Transfer Protocol (HTTP) header. When ISA Server is actively caching, the client agent is *ISA Server*. For Firewall service, this field includes information about the client's operating system.
4	Authentication status (sc-authenticated)	Indicates whether or not client has been authenticated with ISA Server. Possible values are *Y* and *N*.
5	Date (date)	The date that the logged event occurred.
6	Time (time)	The time that the logged event occurred. In W3C format, this is in Greenwich mean time.
7	Service name (s-svcname)	The name of the service that is logged. • **w3proxy** indicates outgoing Web requests to the Web Proxy service. • **fwsrv** indicates Firewall service. • **w3reverseproxy** indicates incoming Web requests to the Web Proxy service.
8	Proxy name (s-computername)	The name of the computer running ISA Server. This is the computer name that is assigned in Windows 2000.
9	Referring server	If ISA Server is used upstream in a chained configuration,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	name (cs-referred)	this indicates the server name of the downstream server that sent the request.
10	Destination name (r-host)	The domain name for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was retrieved from the Web Proxy server cache and not from the destination.
11	Destination IP (r-ip)	The network IP address for the remote computer that provides service to the current connection. For the Web Proxy service, a hyphen (-) in this field may indicate that an object was sourced from the Web Proxy server cache and not from the destination. One exception is negative caching. In that case, this field indicates a destination IP address for which a negative-cached object was returned.
12	Destination port (r-port)	The reserved port number on the remote computer that provides service to the current connection. This is used by the client application initiating the request.
13	Processing time (time-taken)	This indicates the total time, in milliseconds, that is needed by ISA Server to process the current connection. It measures elapsed server time from the time that the server first received the request to the time when final processing occurred on the server—when results were returned to the client and the connection was closed. For cache requests that were processed through the Web Proxy service, *processing time* measures the elapsed server time needed to fully process a client request and return an object from the server cache to the client.
14	Bytes sent (cs-bytes)	The number of bytes sent from the internal client to the external server during the current connection. A hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were sent to the remote computer.
15	Bytes received (sc-bytes)	The number of bytes sent from the external computer and received by the client during the current connection. A hyphen (-), a zero (0), or a negative number in this field indicates that this information was not provided by the remote computer or that no bytes were received from the external computer.
16	Protocol name (cs-protocol)	Specifies the application protocol used for the connection. Common values are HTTP, File Transfer Protocol (FTP), Gopher, and Secure Hypertext Transfer Protocol (HTTPS). For Firewall service, the port number is also logged.
17	Transport	Specifies the transport protocol used for the connection.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	(cs-transport)	Common values are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
18	Operation (s-operation)	Specifies the application method used. For Web Proxy, common values are GET, PUT, POST, and HEAD. For Firewall service, common values are CONNECT, BIND, SEND, RECEIVE, GHBN (GetHostByName), and GHBA (GetHostByAddress).
19	Object name (cs-uri)	For the Web Proxy service, this field shows the contents of the URL request. This field applies only to the Web Proxy service log.
20	Object MIME (cs-mime-type)	The Multipurpose Internet Mail Extensions (MIME) type for the current object. This field may also contain a hyphen (-) to indicate that this field is not used or that a valid MIME type was not defined or supported by the remote computer. This field applies only to the Web Proxy service log.
21	Object source (s-object-source)	Indicates the source that was used to retrieve the current object. This field applies only to the Web Proxy service log.
22	Result code (sc-status)	This field can be used to indicate: • For values less than 100, a Windows (Win32) error code • For values between 100 and 1,000, an HTTP status code • For values between 10,000 and 11,004, a Winsock error code
23	Cache info (s-cache-info)	This number reflects the cache status of the object, which indicates why the object was or was not cached. This field applies only to the Web Proxy service log.
24	Rule #1 (rule#1)	This reflects the rule that either allowed or denied access to the request, as follows: • If an outgoing request is allowed, this field reflects the protocol rule that allowed the request. • If an outgoing request is denied by a protocol rule, this field reflects the protocol rule. • If an outgoing request is denied by a site and content rule, this field reflects the protocol rule that would have allowed the request. • If an incoming request was denied, this field reflects the Web publishing or server publishing rule that denied the request. • If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

		the field is empty.
25	Rule #2 (rule#2)	This reflects the second rule that either allowed or denied access to the request. • If an outgoing request is allowed, this field reflects the site and content rule that allowed the request. • If an outgoing request is denied by a site and content rule, this field reflects the site and content rule that denied the request. • If no rule specifically allowed the outgoing or incoming request, the request is denied. In this case, the field is empty.
26	Session ID (sessionid)	This identifies a session's connections. For Firewall clients, each process that connects through the Firewall service initiates a session. For secure network address translation (SecureNAT) clients, a single session is opened for all the connections that originate from the same IP address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.
27	Connection ID (connectionid)	This identifies entries that belong to the same socket. Outbound TCP usually has two entries for each connection: when the connection is established and when the connection is terminated. UDP usually has two entries for each remote address. This field is not included in the Web Proxy service log. This field applies only to the Firewall service log.

Object source values

Source values	Description
0	No source information is available.
Cache	Source is the cache. Object returned from cache.
Inet	Source is the Internet. Object added to cache.
Member	Returned from another array member.
NotModified	Source is the cache. Client performed an If-Modified-Since request and object had not been modified.
NVCache	Source is the cache. Object could not be verified to source.
Upstream	Object returned from an upstream proxy cache.
Vcache	Source is the cache. Object was verified to source and had not been modified.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

VFInet	Source is the Internet. Cached object was verified to source and had been modified.

Result code values

Value	Description
200	OK - Successful connection
201	Created
202	Accepted
204	No content
301	Moved permanently
302	Moved temporarily
304	Not modified
400	Bad request
401	Unauthorized
403	Forbidden
404	Not found
500	Internal server error
501	Not implemented
502	Bad gateway
503	Service unavailable
10060	Connection timed out
10061	Connection refused by destination
10065	Host unreachable
11001	Host not found

Cache info values

Value	Description
0x00000001	Request should not be served from the cache
0x00000002	Request includes the **IF-MODIFIED-SINCE** header
0x00000004	Request includes one of these headers: **CACHE-CONTROL:NO-CACHE** or **PRAGMA:NO-CACHE**
0x00000008	Request includes the **AUTHORIZATION** header
0x00000010	Request includes the **VIA** header
0x00000020	Request includes the **IF-MATCH** header

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

0x00000040	Request includes the **RANGE** header
0x00000080	Request includes the **CACHE-CONTROL: NO-STORE** header
0x00000100	Request includes the **CACHE-CONTROL: MAX-AGE**, or **CACHE-CONTROL: MAX-STALE** or **CACHE-CONTROL: MIN-FRESH** header
0x00000200	Cache could not be updated.
0x00000400	**IF-MODIFIED-SINCE** time specified in the request is newer than cached **LASTMODIFIED** time
0x00000800	Request includes the **CACHE-CONTROL: ONLY-IF-CACHED** header
0x00001000	Request includes the **IF-NONE-MATCH** header
0x00002000	Request includes the **IF-UNMODIFIED-SINCE** header
0x00004000	Request includes the **IF-RANGE** header
0x00008000	More than one **VARY** header
0x00010000	Response includes the **CACHE-CONTROL: PUBLIC** header
0x00020000	Response includes the **CACHE-CONTROL: PRIVATE** header
0x00040000	Response includes the **CACHE-CONTROL: NO-CACHE** or **PRAGMA: NO-CACHE** header
0x00080000	Response includes the **CACHE-CONTROL: NO-STORE** header
0x00100000	Response includes either the **CACHE-CONTROL: MUST-REVALIDATE** or **CACHE-CONTROL: PROXY-REVALIDATE** header
0x00200000	Response includes the **CACHE-CONTROL: MAX-AGE** or **S-MAXAGE** header
0x00400000	Response includes the **VARY** header
0x00800000	Response includes the **LAST-MODIFIED** header
0x01000000	Response includes the **EXPIRES** header
0x02000000	Response includes the **SET-COOKIE** header
0x04000000	Response includes the **WWW-AUTHENTICATE** header
0x08000000	Response includes the **VIA** header
0x10000000	Response includes the **AGE** header
0x20000000	Response includes the **TRANSFER-ENCODING** header
0x40000000	Response should not be cached.

Operating system values

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Value	Description
0:3.95	Windows 95 (16-bit)
2:4.10	Windows 98 (32-bit)
2:4.0	Windows 95 (32-bit)
3:4.0	Windows NT 4.0
3:5.0	Windows 2000
3:5.1	Windows XP

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

BIBLIOGRAPHY

arachNIDS - The Intrusion Event Database. Whitehats Network Security Resource. 25 April 2002. <http://www.activeworx.com/arachnids/IDS169/event.html>.

Firewall Security Services with Microsoft Internet Security and Acceleration Server 2000. 8 June 2001. Microsoft. 16 April 2002. <http://www.microsoft.com/isaserver/techinfo/planning/FirewallSecurity.doc>.

Firewall Suite. 16 April 2002. WebTrends. <http://www.webtrends.com/products/firewall/fws.htm >

Gauci, Sandro. ISA Server IP Packet Filter Logs Interpretation. 22 August 2001. <http://www.isaserver.org/pages/tutorials/isaserver_iplogs.htm>.

ICMP Type Numbers. 16 April 2002. <http://www.e-ther.net/icmptypecodes.html>.

Microsoft Internet Security and Acceleration Server 2000 Online Help. 15 December 2000. Microsoft. 16 April 2002. <http://download.microsoft.com/download/ISAServer2000/ProdDocs/1.0/NT5/EN-US/isa2k.chm>.

Microsoft Internet Security and Acceleration Server 2000 Overview. March 2002. Microsoft. 16 April 2002. <http://www.microsoft.com/isaserver/evaluation/productguide_v1.1.doc>.

Pitsenbargar, Trent. Guide to Secure Configuration and Administration of Microsoft ISA Server 2000. 7 January 2002. National Security Agency. 16 April 2002. <http://nsa1.www.conxion.com/win2k/guides/w2k-11.pdf>.

Schorr, Joesph. Configuring Intrusion Detection in ISA Server. 5 April 2001. <http://www.isaserver.org/pages/tutorials/intrusion%20detection.htm>.

Shinder, Thomas, et al. Configuring ISA Server 2000: Building Firewalls for Windows 2000. Massachusetts: Syngress, 2001.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**