3.10 Logging Service

SoftEther VPN Server automatically writes logs for operational status and packets flowing over Virtual Hubs as a log file, thereby incorporating a function which enables a simple and sure way to confirm proper operation as well as trace problems and discover any unauthorized access & policy breaches at a later date. This section explains the logging service integrated into SoftEther VPN Server.

3.10.1 Log Save Format & Save Cycle

Types of Logs Saved

The VPN Server automatically writes the Server Log as the log for the entire VPN Server.

Also, in addition to each of the Virtual Hubs writing a security log recording important operating conditions relating to the hub's administration and VPN connection records, they also write packet logs for packets types pre-designated by the Virtual Hub Administrator.

All log files have their own entry and are written one to a line in a text file. When multibyte characters such as hiragana & Chinese characters are used in the log file, the encoding method is unified as UTF-8.

Log File Save Location & Format

All log files create the three subdirectories **server_log**, **security_log** and **packet_log** in the directory containing the vpnserver process (or vpnbridge process in the case of the VPN Bridge) executable files and write each of the server log, security log and packet log there. A further subdirectory is created for the security log and packet log written for each Virtual Hub. These logs are then written to this subdirectory, which is named after its Virtual Hub.

Log File Switch Cycle

Virtual Hub Administrators can set the log file switch cycle of security logs and packet logs. New file names are then generated based on this log file switch cycle. The log file names created when the settable switch cycle and its rules are applied are as follows. Note that the entire VPN Server log is always switched and saved on a daily cycle.

Switch Cycle	Naming convention for file name date portion (Example: 1:45:10 (pm), 7 December 2012)
No Switching	None (perpetually add records to same file)
Every second	20121207_014510
Every minute	20121207_0145
Every hour	20121207_01
Every day	20121207
Every month	201212

Changing the Virtual Hub Log File Settings

The Virtual Hub Administrator can set the switch cycles of the Virtual Hub's security log and packet log by clicking on [Log save settings] in the VPN Server Manager. When not wishing to save a log file, deselect the relevant checkbox prevents any log file from being saved for that type of log. It is also possible to select the details of which types of packet logs should be saved.

All Virtual Hub logs are set with a one day switch save cycle in default.

In the vpncmd utility, use the **[LogEnable]**, **[LogDisable]**, **[LogSwitchSet]** and **[LogPacketSaveType]** commands.

3-10-1.png

Log save settings window.

Measures for Log Files Exceeding 1Gbytes

While the each log file increases in response to the log contents and volume, when exceeding 1Gbytes (or 1,073,741,823 bytes to be precise), that log file is automatically divided and saved approximately every 1Gbytes. The first file keeps the original file name while the second and subsequent files are sequentially named "~01", "~02" and so on. This maximum size can be changed with "LoggerMaxLogSize" in the configuration file.

3.10.2 Server Log

The server log is saved under the **[server_log]** directory. The entire VPN Server operating log is saved in the server log, which saves detailed operating records including

event records upon the launch & termination of the VPN Server and when & what type of connections were received. Therefore, subsequent analysis of this log enables the tracing of unauthorized access and the cause of problems.

In addition, copies of each of the Virtual Hubs' security logs are saved together in the server log so that even if a Virtual Hub Administrator sets the security log not to be saved, it is always saved automatically in the server log. Accordingly, even when the Virtual Hub Administrator does not save the Virtual Hub logs or deletes them, their contents can still be accessed from the VPN Server's server log.

3.10.3 Virtual Hub Security Log

The Virtual Hub security log is saved under the **[security_log/Virtual Hub name]** directory. The security log records information on sessions which connected to the Virtual Hub, records within the Virtual Hub (address table and database updates etc.) and records relating to Virtual Hub administration (user creation etc.).

3.10.4 Virtual Hub Packet Log

The Virtual Hub packet log is saved under the **[packet_log/Virtual Hub name]** directory. The packet log can save all of the headers of packets flowing within the Virtual Hub or their entire payloads.

However, saving all types of packet logs generates a massive amount of log file data. That is why the Virtual Hub Administrator is able to select which types of packets to register in the packet log. The types of packets which can be selected in the [Log save settings] window and their contents are as follows.

Packet Type	Packets saved when this type is selected
TCP Connection Log	Those TCP/IP protocol packets in which a TCP/IP connection between a client and user is established or disconnected.
TCP Packet Log	All TCP/IP protocol packets.
DHCP Packet Log	Those UDP/IP protocol packets which are control data for DHCP protocol.
UDP Packet Log	All UDP/IP protocol packets.
ICMP Packet Log	All ICMP protocol packets.
IP Packet Log	All IP protocol packets.
ARP Packet Log	All ARP protocol packets.
Ethernet Packet Log	All packets.

When set to save packet logs, the Virtual Hub saves the packet log types pre-designated by the Virtual Hub Administrator from among all virtual Ethernet frames flowing within the Virtual Hub. Each Ethernet frame is analyzed with the highest possible layer from layer 2 up to layer 7 using the VPN Server's internal high-level packet analysis engine and important header information is saved as a packet log.

In addition, the Virtual Hub Administrator can write not only the header information but also the entire contents of the packet (bit sequence) to the packet log in 16 decimal format. In this case, note that it is necessary have a high volume disk capacity in proportion to the total size of the packets actually transmitted.

In default, only the packet header information of two packet types, namely the TCP connection log and DHCP packet log, are saved. While this setting value is sufficient for many environments, change the settings as required to save more detailed packet information. Please note that saving all pockets logs is not practical in view of today's broadened communication lines.

The packet log is recorded in the following format.

Sample of Packet log

2006-08-07,12:00:33.764,SID-THISJUN-6,SID-SECURENAT-5,00ACCF078E3B,00AC1F195AE7,0x0800,62,TCP_CONNECT,SYN,192.168.3.137,1399 130.158.6.56,http(80),3894805527,0,WindowSize=65535,-

????	???	??????????
1	Date	2006-08-07
2	Time	12:00:33.764
3	Source Session ID	SID-THISJUN-6
4	Destination SessionID	SID-SECURENAT-5
5	Source MAC Address	00ACCF078E3B
6	Destination MAC Address	00AC1F195AE7
7	Protocol	0x0800
8	Size of packet	62
9	Packet type	TCP_CONNECT
10	Packet flags	SYN
11	Source IP Address	192.168.3.137
12	Source Port (and the net service name is also described if registered in the etc/services file)	13999

13	Destination IP Address	130.158.6.56
14	Destination Port (and the net service name if known)	http(80)
15	Sequence number	0
16	ACK number	0
17	Detailed information for each protocol	WindowSize=65535
18	Hexadecimal dump for payload (only for full recording mode)	-

3.10.5 Performance Optimization for Log Writing

SoftEther VPN Server writes data to the disk, not immediately nor directly, with using 2 steps shown below. Due to this mechanism, SoftEther VPN Server is able to write all packets log without falling off communication performance, especially in the situation that great amounts of packets exchanging at once.

Generation of Medium Format of Packet Log

All of packets which are logged, which are temporary converted the medium format which computer easily deals with, which are not written to packet log immediately. The packet log data converted to medium format is added to temporary area called "Log Buffer." Thus, communication speed of virtual Hub is not slow down very much because the process of converting to medium format is highly speedy.

Converting from Medium Format to Text Format and Write to Disk

The packet data of medium format added to log buffer is need to be converted to text data before written to disk. However, the process of converting to the text data is high cost and spends much CPU time.

The solution is that logging service program buffers the medium format packet data not to write data to disk when the load of virtual Hub communication service is high. Later, the program converts stocked medium data format to text data when computer has enough CPU time due to virtual Hub packets being decreased. This batch process is quick. At the last, computer flushes a certain mount of text data to disk.

Auto Adjustment of Communication Speed for the lack of Log Buffer Space

The packet log service of virtual Hub with that mechanism automatically assigns virtual Hub with CPU times so that virtual Hub brings out its performance maximally when a great amount of packets saved are occurred at a burst.

However, Due to log buffer which saves medium format data temporarily of course uses main memories, free space is limited. If a great many packets saved are flowed in virtual

Hub for a long time, log buffer which is managed by logging service becomes to be full and new packets may be dropped.

The solution of that logging service automatically adjusts the communication speed of virtual Hub when log buffer has little space in order to keep free space a certain space of log buffer. Because of this function, the logging service makes effort not to decrease the communication speed of virtual Hub when a great many packets saved are exchanged in virtual Hub for a long time.

3.10.6 Obtaining Log Files on a Remote Administration Terminal

The log files written by the VPN Server and Virtual Hubs are saved on the physical computer disk on which the VPN Server is running. However, reading and downloading of the files written to the physical disk is typically limited to that computer's Administrators and users capable of local log in.

The SoftEther VPN Server employs a mechanism which allows log files to be read remotely without having to actually log in locally in consideration of the fact that the VPN Server and Virtual Hub Administrators may not be the System Administrators of the computer running the VPN Server. This is known as the remote log read function.

The remote log read function is very easy to use. Clicking on the [Log File List] button when using the VPN Server Manager displays a list of the log files which can be read with current authority along with their file size and time of last update. Log files can be selected arbitrarily from this list and downloaded to an administration terminal. Data is automatically SSL encrypted to ensure safety when transferring a log file because the administration connection's TCP/IP connection is used.

The **[LogGet]** command can be used in the vpncmd utility.

The VPN Server Administrator can remotely obtain the VPN Server's server log, and the security logs and server logs of all Virtual Hubs. Virtual Hub Administrators can only remotely obtain the security log and server log of the Virtual Hub for which they have authority, and cannot remotely acquire any other log files.

When connected to a cluster controller in a clustering environment, it is possible to collectively enumerate and designate the log files of all cluster member servers including the cluster controller, and download these files.

3-10-2.png

Log file list display window.

3.10.7 Syslog Transmission function

As explained in 3.3 VPN Server Administration, enabling the Syslog Transmission function prevents log data sent by the syslog protocol from being saved to the local hard disk.

See Also

- 3.3 VPN Server Administration
- 6.3.55 "LogFileList": Get List of Log Files
- 6.3.56 "LogFileGet": Download Log file
- 6.4.12 "LogGet": Get Log Save Setting of Virtual Hub
- 6.4.13 "LogEnable": Enable Security Log or Packet Log
- 6.4.14 "LogDisable": Disable Security Log or Packet Log
- 6.4.15 "LogSwitchSet": Set Log File Switch Cycle
- 6.4.16 "LogPacketSaveType": Set Save Contents and Type of Packet to Save to Packet Log