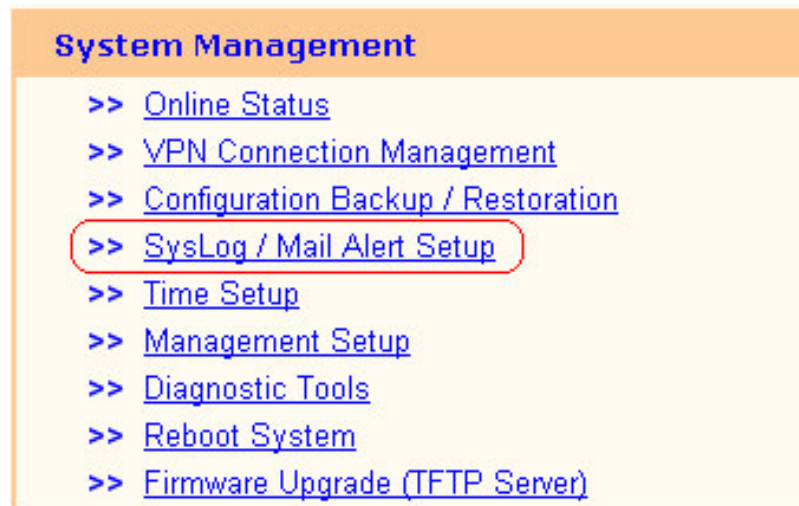

CHAPTER 15

SysLog/Mail Alert Setup

15.1 Introduction

Syslog is a popular utility in Unix world. To monitor router activity, you can run a Syslog Daemon to capture all activities from the router. This Daemon program can run on a local PC or a remote one elsewhere on the Internet. In addition, the Vigor routers provide the Mail Alert facility so that the syslog messages can be packed as an e-mail for someone who wants to receive these messages. In the following, we explain how to setup the syslog and mail alert functions. Use the following setup link on the System Management group of the Setup Main Menu to configure the Syslog/Mail Alert functions.

System Management > Syslog/Mail Alert Setup



15.2 Configuration

After clicking the link of Syslog/Mail Alert Setup, the web configuration will change to another scene, as shown below. In this figure, you can find two functions: one for syslog access setup and another one for mail alert setup.

The screenshot shows a web configuration interface with an orange header bar. The header contains the text "> System Management > Syslog Access & Mail Alert Setup" on the left and "<< [Main Menu](\"#\")" on the right. The main content area has a light yellow background and contains two sections: "SysLog Access Setup" and "Mail Alert Setup". Each section has an "Enable" checkbox, followed by input fields for "Server IP Address", "Destination Port" (with a default value of 514), "SMTP Server", "Mail To", and "Return-Path". At the bottom of the form are three buttons: "Cancel", "Clear", and "OK".

Syslog Access Setup

1. Check the **Enable** box to activate the syslog service.
2. **Server IP Address:** Specify an IP address to which all syslog messages will be sent.
3. **Destination Port:** Specify a UDP port number to which the syslog server is listening. The default value is 514.

Mail Alert Setup

1. Check the **Enable** box to activate the mail alert service.
2. **SMTP Server (IP):** Specify an IP address of the SMTP server which can send mails from your Vigor router to the recipients' mailboxes directly.
3. **Mail To:** Specify an e-mail address of the recipient's mailbox to which all

SysLog/Mail Alert Setup

syslog messages will be sent. The recipient could be an administrator who intends to view or analyze the syslog messages.

4. **Return-Path:** Specify an e-mail address of another mailbox to accept all returned messages if some fatal problems occur at the recipient mailbox.

Notice that the current mail alert function is only used to send syslog messages related to Denial-of-Service (DoS) defense behaviors while you have activated the DoS defense facility.

15.3 Example

Your Vigor router will send many types of syslog messages. Some examples of the syslog messages with their individual formats are shown below.

An example of User Access log message:

The screenshot displays the DrayTek Syslog application window. The 'User Access Log' tab is selected, showing a table of log entries. The table has three columns: Time, Host, and Message. The log entries show various network activities, including DNS queries and TCP connections. The interface also includes sections for LAN Status, WAN Status, and ADSL Status.

Time	Host	Message
Jan 1 00:22:54	Vigor	Local User: 192.168.1.10:1617 -> 172.16.2.7:3128 (TCP)
Jan 1 00:22:51	Vigor	Local User: 192.168.1.10 DNS -> 194.109.6.66 inquire www.hinet.net
Jan 1 00:22:47	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan 1 00:22:47	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire www.hinet.net
Jan 1 00:22:43	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan 1 00:22:18	Vigor	Local User: 192.168.1.10:1599 -> 172.16.2.7:3128 (TCP)
Jan 1 00:22:16	Vigor	Local User: 192.168.1.10:1598 -> 172.16.2.7:3128 (TCP)
Jan 1 00:18:03	Vigor	Local User: 192.168.1.10:1405 -> 172.16.2.7:3128 (TCP)
Jan 1 00:17:56	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan 1 00:17:52	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com
Jan 1 00:17:48	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire messenger.hotmail.com

SysLog/Mail Alert Setup

An example of WAN log message to record the status of VPN/IPSec tunnel:

The screenshot displays the DrayTek Syslog application interface. At the top, the title bar reads "DrayTek Syslog". Below the title bar, there are several sections:

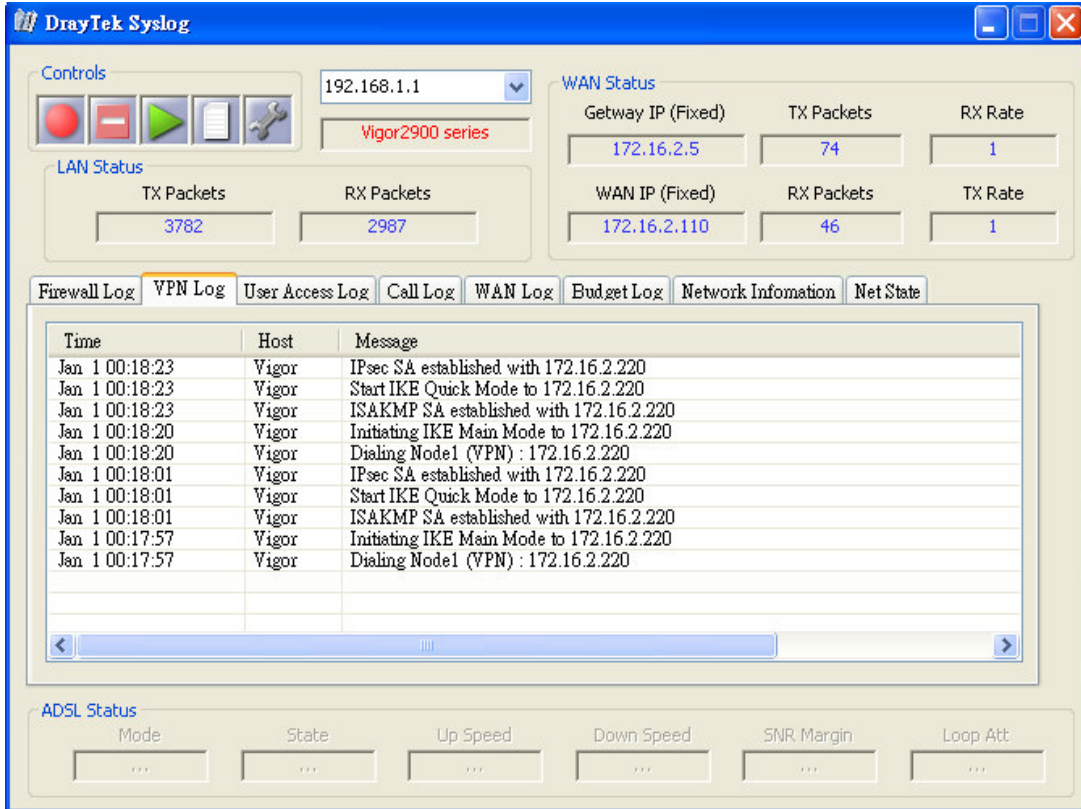
- Controls:** Includes a red stop button, a green play button, a document icon, and a gear icon. A dropdown menu shows "192.168.1.1" and a text box displays "Vigor2900 series".
- LAN Status:** Shows "TX Packets" as 1147 and "RX Packets" as 893.
- WAN Status:** Shows "Gateway IP (Fixed)" as 172.16.2.5, "TX Packets" as 2, "RX Rate" as 1, "WAN IP (Fixed)" as 172.16.2.110, "RX Packets" as 8, and "TX Rate" as 1.
- Log Tabs:** Includes "Firewall Log", "VPN Log", "User Access Log", "Call Log", "WAN Log" (selected), "Budget Log", "Network Information", and "Net State".
- Log Table:** A table with columns "Time", "Host", and "Message". It contains several entries for "Vigor" with timestamps and IKE messages.
- ADSL Status:** Includes fields for "Mode", "State", "Up Speed", "Down Speed", "SNR Margin", and "Loop Att", all showing "...".

The selected "WAN Log" tab shows the following log messages:

Time	Host	Message
Jan 1 00:01:26	Vigor	IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:26	Vigor	IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:26	Vigor	IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:26	Vigor	IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:26	Vigor	IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:24	Vigor	IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:24	Vigor	IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:23	Vigor	IKE <== I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x7e d7 38 88 53 b9 27 18 , N
Jan 1 00:01:23	Vigor	IKE ==> I Cookie=0x1f 0f 07 83 c1 e0 f0 f8 , R Cookie=0x00 00 00 00 00 00 00 , N

SysLog/Mail Alert Setup

An example of VPN (IPSec) log message to record the status of the VPN/IPSec tunnel:



The screenshot displays the DrayTek Syslog application window. The interface includes a top bar with the title "DrayTek Syslog" and standard window controls. Below the title bar, there are several sections:

- Controls:** Contains a red stop button, a green play button, a document icon, and a gear icon. A dropdown menu shows "192.168.1.1" and a text field displays "Vigor2900 series".
- LAN Status:** Shows TX Packets (3782) and RX Packets (2987).
- WAN Status:** Displays Gateway IP (Fixed) as 172.16.2.5, TX Packets as 74, RX Rate as 1, WAN IP (Fixed) as 172.16.2.110, RX Packets as 46, and TX Rate as 1.
- Log Tabs:** Includes Firewall Log, **VPN Log** (selected), User Access Log, Call Log, WAN Log, Budget Log, Network Information, and Net State.
- Log Table:** A table with columns Time, Host, and Message. It lists several log entries related to IPsec SA establishment and IKE Quick Mode initiation.
- ADSL Status:** Shows Mode, State, Up Speed, Down Speed, SNR Margin, and Loop Att, all with "..." values.

Time	Host	Message
Jan 1 00:18:23	Vigor	IPsec SA established with 172.16.2.220
Jan 1 00:18:23	Vigor	Start IKE Quick Mode to 172.16.2.220
Jan 1 00:18:23	Vigor	ISAKMP SA established with 172.16.2.220
Jan 1 00:18:20	Vigor	Initiating IKE Main Mode to 172.16.2.220
Jan 1 00:18:20	Vigor	Dialing Node1 (VPN) : 172.16.2.220
Jan 1 00:18:01	Vigor	IPsec SA established with 172.16.2.220
Jan 1 00:18:01	Vigor	Start IKE Quick Mode to 172.16.2.220
Jan 1 00:18:01	Vigor	ISAKMP SA established with 172.16.2.220
Jan 1 00:17:57	Vigor	Initiating IKE Main Mode to 172.16.2.220
Jan 1 00:17:57	Vigor	Dialing Node1 (VPN) : 172.16.2.220