

CHAPTER 20

SysLog/Mail Alert Setup

20.1 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



20.2 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 page titled "System Management > Syslog Access & Mail Alert Setup". It contains two main sections: "SysLog Access Setup" and "Mail Alert Setup".

SysLog Access Setup

- ☐ Enable
- Server IP Address:
- Destination Port:

Mail Alert Setup

- ☐ Enable
- SMTP Server (IP):
- Mail To:
- Return-Path:

At the bottom of the form are three buttons: "Cancel", "Clear", and "OK".

Copyright (c) 2004, DrayTek Corp. All Rights Reserved.

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.

SysLog/Mail Alert Setup

3. **Mail To:** Specify an e-mail address of the recipient's mailbox to which all 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.

20.3 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 DNS and TCP connections from the Vigor router to external servers like hinet.net and messenger.hotmail.com.

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 00:22:43	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire www.hinet.net
Jan 1 00:22:18	Vigor	Local User: 192.168.1.10 DNS -> 194.98.0.1 inquire toolbarqueries.google.com
Jan 1 00:22:16	Vigor	Local User: 192.168.1.10:1599 -> 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 window. At the top, the title bar reads "DrayTek Syslog". Below the title bar, there are several sections:

- Controls:** Includes a dropdown menu set to "192.168.1.1", a "Vigor2900 series" button, and a "LAN Status" section with "TX Packets" (1147) and "RX Packets" (893).
- WAN Status:** Contains two rows of status information:
 - Getway IP (Fixed): 172.16.2.5, TX Packets: 2, RX Rate: 1
 - WAN IP (Fixed): 172.16.2.110, RX Packets: 8, TX Rate: 1
- Log Tabs:** A row of tabs including "Firewall Log", "VPN Log", "User Access Log", "Call Log", "WAN Log" (which is selected), "Budget Log", "Network Infomation", and "NetState".
- Log Table:** A table with three columns: "Time", "Host", and "Message". It contains several log entries for "Vigor" hosts, showing IKE messages with cookies and sequence numbers. The messages are truncated with "N" at the end.
- ADSL Status:** A section at the bottom with fields for "Mode", "State", "Up Speed", "Down Speed", "SNR Margin", and "Loop Att", all showing "...".

SysLog/Mail Alert Setup

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

The screenshot shows the DrayTek Syslog web interface. At the top, there's a 'Controls' section with a red stop button, a green play button, and a gear icon. Below it, 'LAN Status' shows TX Packets (3782) and RX Packets (2987). To the right, 'WAN Status' shows Gateway IP (Fixed) 172.16.2.5, TX Packets 74, RX Rate 1, WAN IP (Fixed) 172.16.2.110, RX Packets 46, and TX Rate 1. A tabbed menu at the bottom includes Firewall Log, VPN Log (selected), User Access Log, Call Log, WAN Log, Budget Log, Network Information, and Net State. The VPN Log tab displays a table of log messages. The table has three columns: Time, Host, and Message. The messages show the establishment of IPsec SA, IKE Quick Mode, and ISAKMP SA, as well as initiating IKE Main Mode and dialing Node1 (VPN). At the bottom, '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