
CHAPTER 16

SysLog Setup

16.1 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.

16.2 Configuration

1. Check the **Enable** box to enable 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.



The screenshot shows a web-based configuration window titled "SysLog Access Setup" under the "System Management > Syslog Access Setup" path. The window contains the following elements:

- An "Enable" checkbox, which is currently unchecked.
- A "Server IP Address" text input field containing the value "192.168.1.10".
- A "Destination Port" text input field containing the value "514".
- Three buttons at the bottom: "Cancel", "Clear", and "OK".
- A footer at the bottom of the window that reads "Copyright (c) 2004, DrayTek Corp. All Rights Reserved."

16.3 Example

Your Vigor router will send many types of syslog messages. Some examples of the syslog messages with their individual format are shown as follows.

SysLog Setup

An example of User Access log message:

The screenshot shows the DrayTekSysLog interface with the 'User Access Log' tab selected. The interface includes status panels for LAN and WAN, and a log table.

LAN Status: TX Packets: 6350, RX Packets: 1741

WAN Status (Static):

GW IP Addr	TX Packets	RX Rate
172.16.2.6	1488	6

IP Address	RX Packets	TX Rate
172.16.2.136	3291	29

User Access Log Table:

Time	Host	Message
Jan 1 00:02:28	vigor2200	Local User: 192.168.1.10 DNS -> a.r.tv.com
Jan 1 00:02:28	vigor2200	Local User: 192.168.1.10 DNS -> a.r.tv.com
Jan 1 00:02:28	vigor2200	Local User: 192.168.1.10:1543 -> 210.57.49.198:80 (TCP)Web
Jan 1 00:02:28	vigor2200	Local User: 192.168.1.10:1544 -> 210.57.49.198:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1545 -> 64.124.237.131:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1540 -> 64.124.237.131:80 (TCP) close connection
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1545 -> 64.124.237.131:80 (TCP) close connection
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10 DNS -> gserv-cnetzd.net.com
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10 DNS -> gserv-cnetzd.net.com
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1548 -> 64.124.237.131:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1549 -> 210.57.49.198:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1550 -> 210.57.49.198:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1551 -> 64.124.237.131:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1552 -> 64.124.237.131:80 (TCP)Web
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10:1553 -> 64.124.237.131:80 (TCP)Web

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

The screenshot shows the DrayTekSysLog interface with the 'WAN Log' tab selected. The interface includes status panels for LAN and WAN, and a log table.

LAN Status: TX Packets: 0, RX Packets: 0

WAN Status:

GW IP Addr	TX Packets	RX Rate
....	0	0

IP Address	RX Packets	TX Rate
....	0	0

WAN Log Table:

Time	Host	Message
May 24 14:22:17	vigor2200	ISDN data call at B1 channel - disconnected, no AOC
May 24 14:22:13	vigor2200	ISDN data call at B1 channel - connected
May 24 11:48:33	vigor2200	ISDN data call at B1 channel - disconnected, no AOC
May 24 11:48:30	vigor2200	ISDN data call at B1 channel - connected
May 24 11:48:29	vigor2200	ISDN data call at B1 channel - dialing
May 24 11:48:25	vigor2200	ISDN data call at B1 channel - disconnected, no AOC
May 24 11:48:22	vigor2200	ISDN data call at B1 channel - connected
May 24 11:48:21	vigor2200	ISDN data call at B1 channel - dialing
May 24 11:48:17	vigor2200	ISDN data call at B1 channel - disconnected, no AOC
May 24 11:48:14	vigor2200	ISDN data call at B1 channel - connected
May 24 11:48:13	vigor2200	ISDN data call at B1 channel - dialing
May 24 11:48:09	vigor2200	ISDN data call at B1 channel - disconnected, no AOC
May 24 11:48:06	vigor2200	ISDN data call at B1 channel - connected
May 24 11:48:05	vigor2200	ISDN data call at B1 channel - dialing
May 24 11:48:02	vigor2200	ISDN data call at B1 channel - disconnected, no AOC

SysLog 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. At the top, there are status indicators for LAN and WAN. The LAN Status section shows TX Packets and RX Packets, both at 0. The WAN Status section shows GW IP Addr, TX Packets, RX Rate, IP Address, RX Packets, and TX Rate, all at 0. Below these are navigation tabs for various logs: Fire Wall Log, VPN Log, User Access Log, Call Log, WAN Log, Client, Local TCP Table, and Local UDP Table. The VPN Log tab is selected, showing a list of log entries. The status bar at the bottom indicates the application is 'Running..' and the time is 18:33:29.

Time	Host	Message
May 24 17:55:16	Vigor	sent MR3, ISAKMP SA established
May 24 17:55:16	Vigor	IPsec SA established
May 24 17:57:34	Vigor	sent MR3, ISAKMP SA established
May 24 17:57:34	Vigor	IPsec SA established
May 24 17:59:30	Vigor	sent MR3, ISAKMP SA established
May 24 17:59:30	Vigor	IPsec SA established
May 24 18:04:10	Vigor	sent MR3, ISAKMP SA established
May 24 18:04:10	Vigor	IPsec SA established
May 24 18:05:10	Vigor	sent MR3, ISAKMP SA established
May 24 18:05:10	Vigor	IPsec SA established
May 24 18:06:51	Vigor	sent MR3, ISAKMP SA established
May 24 18:06:51	Vigor	IPsec SA established
May 24 18:07:33	Vigor	sent MR3, ISAKMP SA established
May 24 18:07:33	Vigor	IPsec SA established
Jan 1 00:00:04	Vigor	sent MR3, ISAKMP SA established