
SysLog Setup

Introduction

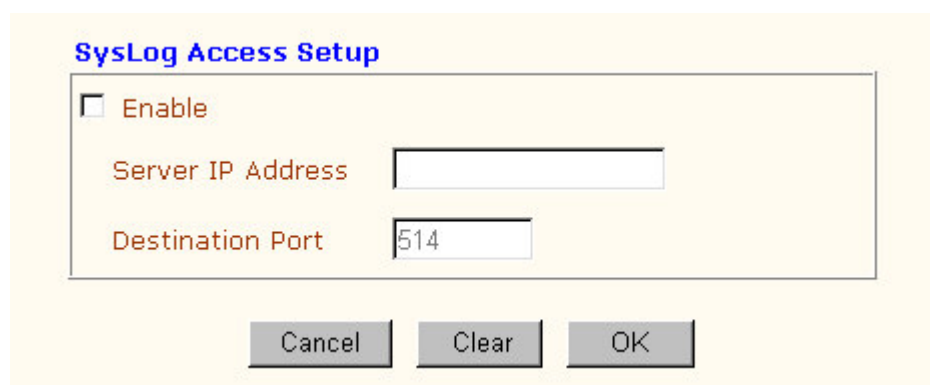
Syslog is a popular utility in Unix world. For monitoring router activity, you can run a Syslog Daemon which will capture the activity output from the router. This Daemon program can run on a local PC or a remote one elsewhere on the Internet.

Configuration

Check the **Enable** box to enable syslog service.

Server IP Address: The IP address which syslog message can be sent to.

Destination Port: The UDP port number which the syslog server is listening. The default value is 514.



The image shows a 'SysLog Access Setup' dialog box. It has a title bar with the text 'SysLog Access Setup'. Inside the dialog, there is a checkbox labeled 'Enable' which is currently unchecked. Below the checkbox, there are two text input fields. The first is labeled 'Server IP Address' and is empty. The second is labeled 'Destination Port' and contains the number '514'. At the bottom of the dialog, there are three buttons: 'Cancel', 'Clear', and 'OK'.

Your Vigor router sends many types of syslog messages. Some examples of the syslog messages with their message format are shown next:

Example of User Access log message:

The screenshot shows the DrayTek SysLog application window. At the top, there's a status bar with icons and a dropdown menu showing '192.168.1.1'. Below this, there are two status sections: 'LAN Status' and 'WAN Status (Static)'. The LAN Status section shows TX Packets: 6350 and RX Packets: 1741. The WAN Status section shows GW IP Addr: 172.16.2.6, TX Packets: 1488, RX Rate: 6, IP Address: 172.16.2.136, RX Packets: 3291, and TX Rate: 29. Below these sections is a tabbed interface with tabs for FireWall Log, VPN Log, User Access Log, Call Log, WAN Log, Client, Local TCP Table, and Local UDP Table. The 'User Access Log' tab is selected, displaying a list of log messages. The messages are in a table with columns: Time, Host, and Message. The messages show local user access for 'vigor2200' with various IP addresses and destinations, including DNS requests and TCP connections. At the bottom, there's a 'Running...' status bar and a clock showing '18:25:41'.

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-cnetadnet.com
Jan 1 00:02:29	vigor2200	Local User: 192.168.1.10 DNS -> gserv-cnetadnet.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

Example of WAN log message while using ISDN connection:

The screenshot shows the DrayTek SysLog application window. At the top, there's a status bar with icons and a dropdown menu showing 'Any'. Below this, there are two status sections: 'LAN Status' and 'WAN Status'. The LAN Status section shows TX Packets: 0 and RX Packets: 0. The WAN Status section shows GW IP Addr: ..., TX Packets: 0, RX Rate: 0, IP Address: ..., RX Packets: 0, and TX Rate: 0. Below these sections is a tabbed interface with tabs for FireWall Log, VPN Log, User Access Log, Call Log, WAN Log, Client, Local TCP Table, and Local UDP Table. The 'WAN Log' tab is selected, displaying a list of log messages. The messages are in a table with columns: Time, Host, and Message. The messages show ISDN data call status for 'vigor2200' at B1 channel, including disconnected, connected, and dialing states. At the bottom, there's a 'Running...' status bar and a clock showing '15:51:58'.

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

Example of VPN (IPSec) log message while the VPN/IPSec tunnel is being used:

The screenshot shows the DrayTekSysLog application window. At the top, there are status sections 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, and RX Rate, all at 0. Below these is a tabbed interface with the following tabs: 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, displaying a list of log messages. The messages are as follows:

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

At the bottom of the window, it says "Running..." on the left and "18:33:29" on the right.