

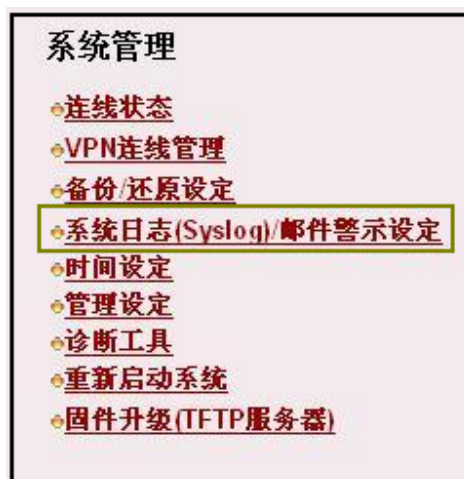
第 19 章

系统日志/邮件警示设定

20.1 简介

系统日志（Syslog）在Unix系统中是一个经常用到的工具。通过运行系统日志后台程序来捕捉路由器的所有活动，用以监视路由器的工作状况。这个后台程序可以运行在一台本地主机上或Internet上的一台远程主机上。另外，Vigor路由器还提供了邮件警示工具，可以将系统日志打包以电子邮件的形式发送给需要接收这些信息的人。下面，我们将介绍如何设置系统日志和邮件警示功能。在**系统管理**组里点击下面的设置链接进入**系统日志/邮件警示功能**页面。

系统管理>系统日志/邮件警示设定



20.2 配置

点击**系统日志/邮件警示设定**进入如下的设置页面。您可以在下图中看到两个功

能，一个是系统日志访问设定，另一个是邮件预警功能设定。

系统管理 > 系统日志(Syslog)/邮件警示设定

SysLog访问设定

☒ 启用

服务器IP地址

目标端口

邮件预警功能设定

☐ 启用

SMTP服务器(IP)

收件人

回信地址

Cancel Clear OK

SysLog访问设定

1. 勾选启用框来启动Syslog服务。
2. **服务器IP地址：**指定用于接收系统日志信息的主机的IP地址。
3. **目标端口：**指定系统日志服务器监听的UDP端口。默认端口为 514。

邮件预警功能设定

1. 勾选启用框来开启邮件预警功能。
2. **SMTP服务器地址：**指定一个邮件服务器的IP地址，可以直接从Vigor路由器发邮件到接收者的邮箱。
3. **收件人：**指定接收者的电子邮件地址，用于接收系统日志信息。接收者

可能是一个管理员，需要查看并分析系统日志。

4. **回信地址：**指定另一个电子邮件地址，在收件人的邮箱出现问题时，用于接收返回的信息。

注意事项：邮件警示功能只能用于发送路由器遭受DoS攻击的信息（在DoS防御功能开启的情况下），

20.3 举例

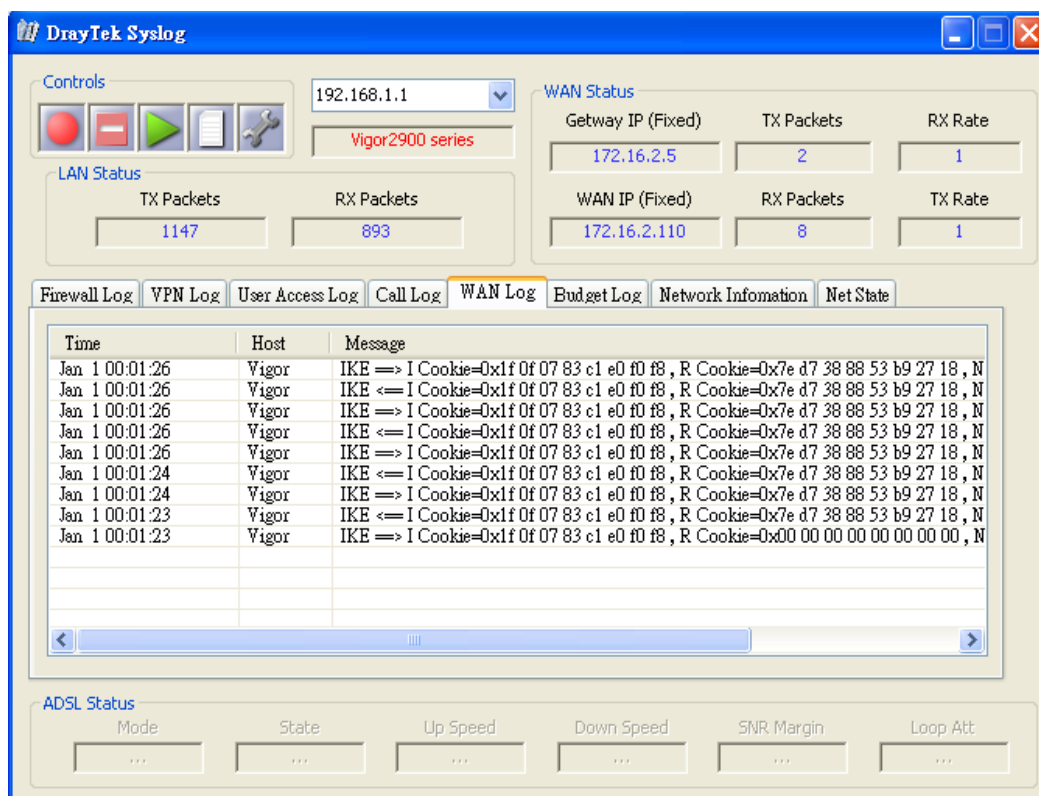
Vigor路由器可以发送很多种系统日志信息。下面举一些例子来说明系统日志信息的格式。

用户访问日志信息的例子

The screenshot displays the DrayTek Syslog web interface. At the top, there's a 'Controls' section with a dropdown menu set to '192.168.1.1' and a 'Vigor2900 series' button. Below this, the 'LAN Status' section shows 'TX Packets' at 5029 and 'RX Packets' at 3983. The 'WAN Status' section shows 'Gateway IP (Fixed)' as 172.16.2.5, 'TX Packets' at 186, 'RX Rate' at 147, 'WAN IP (Fixed)' as 172.16.2.110, 'RX Packets' at 160, and 'TX Rate' at 80. The 'User Access Log' tab is selected, showing a table of log entries. The table has columns for 'Time', 'Host', and 'Message'. The log entries show various DNS and TCP requests from the local user 192.168.1.10 to various hosts like 172.16.2.7, 194.109.6.66, and 194.98.0.1. The 'ADSL Status' section at the bottom shows fields for Mode, State, Up Speed, Down Speed, SNR Margin, and Loop Att, all with '...' values.

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

WAN口日志信息，该例记录了VPN/IPSec隧道的状态的例子



VPN (IPSec) 日志信息用于记录VPN/IPSec隧道的状态的例子

The screenshot shows the DrayTek Syslog application window. The 'VPN Log' tab is selected, displaying a table of VPN-related events. The table has three columns: Time, Host, and Message. The logs show the establishment of IPsec SA, initiation of IKE Main Mode, and dialing of a VPN node.

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