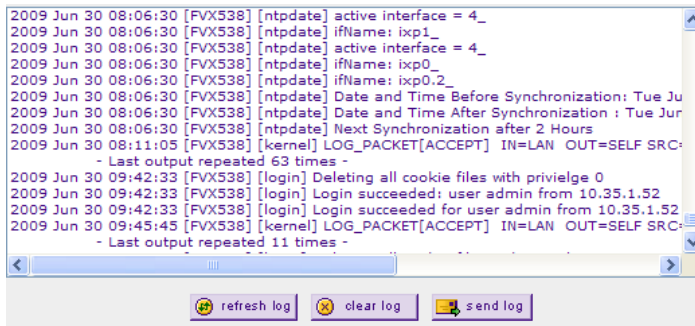


Netgear Router Logs

What are router logs?

Router Logs are a record that a router maintains of events that have occurred on it, which can be very useful for monitoring or troubleshooting a network. It can be viewed in the router web GUI, or automatically emailed to a specified address. The number of events that can be recorded varies from router to router, and when the limit is reached the oldest entries are deleted to allow new entries to be added.

What do router logs look like?



```
2009 Jun 30 08:06:30 [FVX538] [ntpdate] active interface = 4_
2009 Jun 30 08:06:30 [FVX538] [ntpdate] ifName: ixp1_
2009 Jun 30 08:06:30 [FVX538] [ntpdate] active interface = 4_
2009 Jun 30 08:06:30 [FVX538] [ntpdate] ifName: ixp0_
2009 Jun 30 08:06:30 [FVX538] [ntpdate] ifName: ixp0_2_
2009 Jun 30 08:06:30 [FVX538] [ntpdate] Date and Time Before Synchronization: Tue Jun 30 08:06:30
2009 Jun 30 08:06:30 [FVX538] [ntpdate] Date and Time After Synchronization : Tue Jun 30 08:06:30
2009 Jun 30 08:06:30 [FVX538] [ntpdate] Next Synchronization after 2 Hours
2009 Jun 30 08:11:05 [FVX538] [kernel] LOG_PACKET[ACCEPT] IN=LAN OUT=SELF SRC=
- Last output repeated 63 times -
2009 Jun 30 09:42:33 [FVX538] [login] Deleting all cookie files with privilege 0
2009 Jun 30 09:42:33 [FVX538] [login] Login succeeded: user admin from 10.35.1.52
2009 Jun 30 09:42:33 [FVX538] [login] Login succeeded for user admin from 10.35.1.52
2009 Jun 30 09:45:45 [FVX538] [kernel] LOG_PACKET[ACCEPT] IN=LAN OUT=SELF SRC=
- Last output repeated 11 times -
```

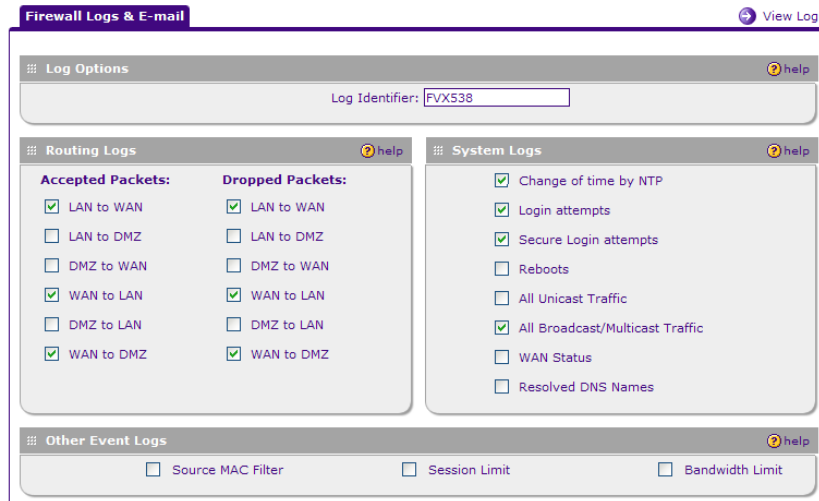
This screenshot shows some typical log entries. These entries show the router successfully synchronizing its local clock to an NTP server, and the administrator successfully logging in to the router.

Clearly, in order for the timestamp on the logged entries to be correct, the system clock on the router must be correct. Automatic syncing to an NTP server is the best way to ensure this.

What events can be logged?

The logging capabilities of routers vary from model to model, and the Prosafe routers provide more detailed control over what gets logged and what doesn't than the consumer products.

This screenshot is from an FVX538 Prosafe router:



The "System Logs" options are self-explanatory.

The "Other Events Logs" options will trigger a log entry if there is an attempt to breach a limit that has been set, such as exceeding a bandwidth limit, exceeding a sessions limit, or using a device that is not on the approved list of MAC addresses.

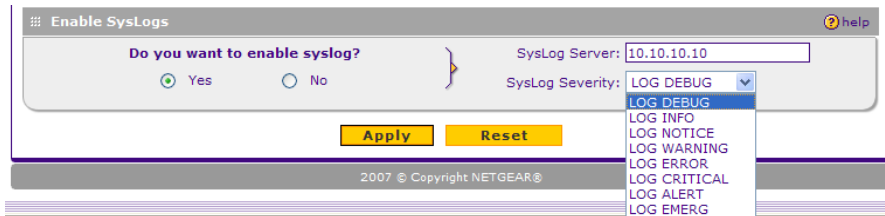
The "Routing Logs" options log when packets are dropped or accepted by firewall rules. When creating firewall rules, "Log:" can be set to "Always" or "Never". If set to Never, packets that match that rule will never be logged, regardless of settings on the screenshot above. Packets that match the default inbound and outbound firewall rules are not logged.

What events should be logged?

In a troubleshooting situation, it is often useful to log almost all activity on the router, to gain a detailed picture of what is happening. However, when a network is operating normally, logging should usually be limited to events that would be considered undesirable or suspicious, such as the WAN link going down, packets being dropped, or a bandwidth limited being exceeded. This is because excessive logging of routine events will adversely impact the performance of both the router and the system administrator.

Are router logs the same as Syslogs?

No, although the logs that they produce are very similar. Syslogging is a standards-based form of logging which sends a real-time record of system events to an external syslog server. Many devices can send logs to the same syslog server, which can act as a central point for monitoring network-wide events.



What events get syslogged is set by the drop-down selection in this screenshot, with “log emerg” only logging the most urgent events, and “log debug” logging every event on the router. In most situations somewhere in between, like “log error” would be chosen.