How to read the logs

Although the exact format of each log entry depends on how your syslog recipient works, most are very much alike. The way in which logs are read is also dependent on how your syslog recipient works. Syslog daemons on UNIX servers usually log to text files, line by line. Most syslog recipients preface each log entry with a timestamp and the IP address of the machine that sent the log data:
Oct 20 2003 09:45:23 gateway
This is followed by the text the sender has chosen to send. All log entries from DFL-1100 are prefaced with "EFW:" and a category, e.g. "DROP:"
Oct 20 2003 09:45:23 gateway EFW: DROP:
Subsequent text is dependent on the event that has occurred.

Usage Event

These events are sent periodically and provide statistical information regarding connections and amount of traffic.
Example:
Oct 20 2003 09:45:23 gateway EFW: USAGE: conns=1174 if0=core ip0=127.0.0.1 tp0=0.00 if1=wan ip1=192.168.10.2 tp1=11.93 if2=lan ip2=192.168.0.1 tp2=13.27 if3=dmz ip3=192.168.1.1 tp3=0.99
The value after conns is the number of open connections trough the firewall when the usage log was sent. The value after tp is the throughput through the firewall at the time the usage log was logged.

Drop Event

These events may be generated by a number of different functions in the firewall. The most common source is probably the policies.
Example:
Oct 20 2003 09:42:25 gateway EFW: DROP: prio=1 rule=Rule_1 action=drop recvif=wan srcip=192.168.10.2 destip=192.168.0.1 ipproto=TCP ipdatalen=28 srcport=3572 destport=135 tcphdrlen=28 syn=1
In this line, traffic from 192.168.10.2 coming from the WAN side of the firewall, connecting to 192.168.10.1 on port 135 is dropped. The protocol used is TCP.

Conn Event

These events are generated if auditing has been enabled.
One event will be generated when a connection is established. This event will include information about protocol, receiving interface, source IP address, source port, destination interface, destination IP address and destination port.
Open Example:
Oct 20 2003 09:47:56 gateway EFW: CONN: prio=1 rule=Rule_8 conn=open connipproto=TCP connrecvif=lan connsrcip=192.168.0.10 connsrcport=3179 conndestif=wan conndestip=64.7.210.132 conndestport=80
In this line, traffic from 192.168.0.10 on the LAN interface is connecting to 64.7.210.132 on port 80 on the WAN side of the firewall (internet).
Another event is generated when the connection is closed. The information included in the event is the same as in the event sent when the connection was opened, with the exception that statistics regarding sent and received traffic is also included.
Close Example:
Oct 20 2003 09:48:05 gateway EFW: CONN: prio=1 rule=Rule_8 conn=close connipproto=TCP connrecvif=lan connsrcip=192.168.0.10 connsrcport=3179 conndestif=wan conndestip=64.7.210.132 conndestport=80 origsent=62 termsent=60
In this line, the connection in the other example is closed.

IDS Event

When an attack has occurred and an email has been, more information about the attack can be found. Copy the attack string and paste it into the **By message** box at the following address: http://www.snort.org/cgi-bin/sigs-search.cgi (you can of course also write the attack

string manually in the box).
Intrusion attacks will always be logged in the usual logs if IDS is enabled for any of the rules.
For more information about how to enable intrusion detection and prevention on a policy or port mapping, read more in the Firewall section below for Policies and Port Mappings.