

The following is the example to how to enable event in the DSR series:

Step1: Make sure the rule that you want to log is enable, we use the firewall rule for example. In the **Log** field, make sure your select **Always**.

The screenshot shows the 'Firewall Rule Configuration' page in a D-Link web interface. The 'Log' field is highlighted with a red rectangle, and its value is set to 'Always'. The page includes a sidebar with navigation options and buttons for 'Save Settings' and 'Don't Save Settings' at the top.

Firewall Rule Configuration	
From Zone:	INSECURE (WAN)
To Zone:	SECURE (LAN)
Service:	HTTP
Action:	Always Allow
Select Schedule:	
Source Hosts:	Any
From:	
To:	
Destination Hosts:	Any
From:	
To:	
Log:	Always
QoS Priority:	Normal-Service

Source NAT Settings	
External IP Address:	WAN Interface Address
Single IP Address:	
WAN Interface:	WAN1

Destination NAT Settings	
Internal IP Address:	192.168.10.10
Enable Port Forwarding:	<input checked="" type="checkbox"/>
Translate Port Number:	80

Step 2. Under the **TOOLS->Log Settings-> LOG CONFIGURATION**, select the direction and dropped/accesspt packet you want to log.

DSR-500N	SETUP	ADVANCED	TOOLS	STATUS	HELP																				
Admin	<div style="border: 1px solid black; padding: 5px;"> <div style="border: 1px solid black; padding: 2px; margin-bottom: 5px;">LOGS CONFIGURATION</div> <div style="text-align: right; margin-bottom: 5px;">LOGOUT</div> <p>This page allows user to configure system wide log settings.</p> <div style="display: flex; justify-content: space-around;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </div> </div>				<p>Helpful Hints...</p> <p>Traffic through each network segment (LAN, WAN, DMZ) can be tracked based on whether the packet was accepted or dropped by the firewall. Denial of service attacks, general attack information, login attempts, dropped packets, and similar events can be captured for review by the IT administrator.</p> <p>More...</p>																				
Date and Time																									
Log Settings																									
System																									
Firmware																									
Firmware via USB																									
Dynamic DNS																									
System Check																									
Schedules																									
<div style="border: 1px solid black; padding: 5px;"> <p>Routing Logs</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th style="text-align: center;">Accepted Packets</th> <th style="text-align: center;">Dropped Packets</th> </tr> </thead> <tbody> <tr> <td>LAN to WAN:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr style="border: 2px solid red;"> <td>WAN to LAN:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>WAN to DMZ:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>DMZ to WAN:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>LAN to DMZ:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>DMZ to LAN:</td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table> </div>							Accepted Packets	Dropped Packets	LAN to WAN:	<input type="checkbox"/>	<input type="checkbox"/>	WAN to LAN:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	WAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>	DMZ to WAN:	<input type="checkbox"/>	<input type="checkbox"/>	LAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>	DMZ to LAN:	<input type="checkbox"/>
	Accepted Packets	Dropped Packets																							
LAN to WAN:	<input type="checkbox"/>	<input type="checkbox"/>																							
WAN to LAN:	<input type="checkbox"/>	<input checked="" type="checkbox"/>																							
WAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>																							
DMZ to WAN:	<input type="checkbox"/>	<input type="checkbox"/>																							
LAN to DMZ:	<input type="checkbox"/>	<input type="checkbox"/>																							
DMZ to LAN:	<input type="checkbox"/>	<input type="checkbox"/>																							
<div style="border: 1px solid black; padding: 5px;"> <p>System Logs</p> <p>All Unicast Traffic: <input type="checkbox"/></p> <p>All Broadcast / Multicast Traffic: <input type="checkbox"/></p> </div>																									
<div style="border: 1px solid black; padding: 5px;"> <p>Other Events Logs</p> <p>Bandwidth Limit: <input type="checkbox"/></p> </div>																									
UNIFIED SERVICES ROUTER																									

Step3:Under **TOOLS->Log Settings-> LOGS FACILITY**, select the Log Facility and the severity of log want to displays.

The screenshot shows the D-Link router's web interface. The top navigation bar includes 'DSR-500N', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar contains a menu with 'Admin', 'Date and Time', 'Log Settings', 'System', 'Firmware', 'Firmware via USB', 'Dynamic DNS', 'System Check', and 'Schedules'. The 'Log Settings' menu item is highlighted with a red box. The main content area is titled 'LOGS FACILITY' and includes a 'LOGOUT' link. Below the title, there is a description: 'This page allows user to set the date and time for the router. User can use the automatic or manual date and settings depending upon his choice.' There are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'Logs Facility' section has a 'Facility:' label and a dropdown menu set to 'Kernel', which is highlighted with a red box. Below this is a 'Display' button. The 'Display and Send Logs' section has two columns: 'Display in Event Log' and 'Send to Syslog'. The 'Display in Event Log' column has checkboxes checked for all severity levels: Emergency, Alert, Critical, Error, Warning, Notification, Information, and Debugging. The 'Send to Syslog' column has unchecked checkboxes for all severity levels.

You can refer the following for more detail:

Logs Facility:

Facility: There are three core components to the router's firmware and the granularity of logging within each can be set independently. Choose between Kernel, System, and Local-0 Wireless.

Kernel: This covers log messages that correspond to the Linux kernel such as logs generated by firewall or network stack traffic.

System: This covers application and management level features such as SSL VPN or administrator changes for managing the unit.

Display and Send Logs

Each of the following type of logs can be sent to the **Event Log** viewer in the GUI and/or the

Syslog server configured to capture remote logging.

When a particular severity level is selected, all events with severity equal to and greater than the chosen severity are captured. The severity levels available for logging are:

EMERGENCY: system is unusable

ALERT: action must be taken immediately

CRITICAL: critical conditions

ERROR: error conditions

WARNING: warning conditions

NOTIFICATION: normal but significant condition

INFORMATION: informational

DEBUGGING: debug-level messages