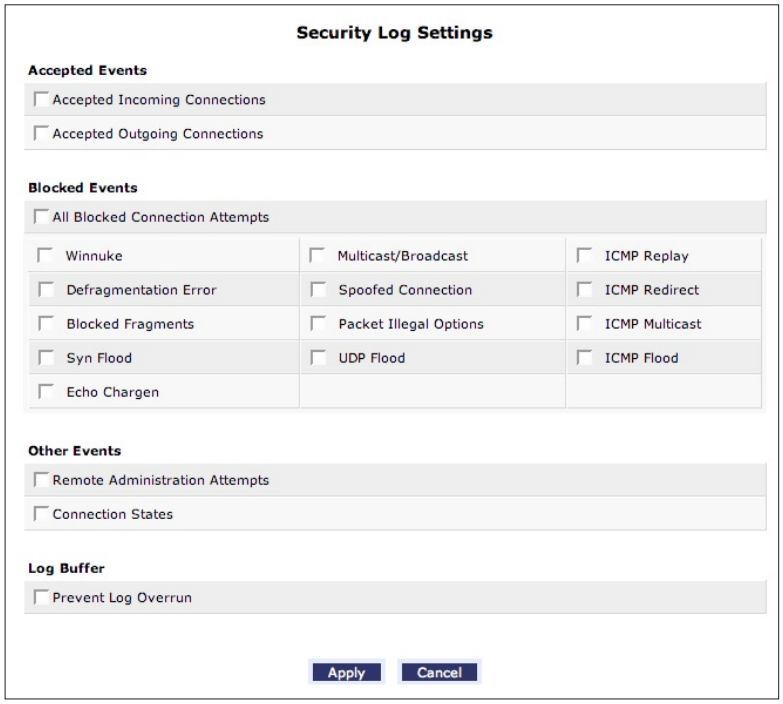
- **Fragmented packet, packet too big** - a packet has been blocked because, after defragmentation, the packet was too big.
- **Fragmented packet, packet exceeds** - a packet has been blocked because, after defragmentation, the packet exceeded.
- **Fragmented packet, no memory** - a fragmented packet has been blocked because there is no memory for fragments.
- **Fragmented packet, overlapped** - a packet has been blocked because, after defragmentation, there were overlapping fragments.
- **Defragmentation failed** - the fragment has been stored in memory and blocked until all fragments have arrived and defragmentation can be performed.
- **Connection opened** - debug message regarding connection.
- **Wildcard connection opened** - debug message regarding connection.
- **Wildcard connection hooked** - debug message regarding connection.
- **Connection closed** - debug message regarding connection.
- **Echo/Chargen/Quote/Snork protection** - a packet has been blocked due to Echo/Chargen/Quote/Snork protection.
- **First packet in connection is not a SYN packet** - a packet has been blocked due to a TCP connection that started without a SYN packet.
- **Error : No memory** - a new connection has not been established because of lack of memory.
- **NAT Error : connection pool is full. No connection created** -a connection has not been created because the connection pool is full.
- **NAT Error: No free NAT IP** - no free NAT IP, so NAT has failed.
- **NAT Error: Conflict Mapping already exists** - a conflict occurred because the NAT mapping already exists, so NAT failed.
- **Malformed packet: Failed parsing** - a packet has been blocked because it is malformed.
- **Passive attack on ftp-server: Client attempted to open Server ports** - a packet has been blocked.

- **FTP port request to 3rd party is forbidden (Possible bounce attack)** - a packet has been blocked.
- **Firewall Rules were changed** - the firewall rule set has been modified.
- **User authentication** - a message arrived during login time, including both successful and failed authentication.

Security Log Settings

To view or change the security log settings:

1. Click **Settings** in the Security Log screen. The "Security Log Settings" screen appears.



2. Select the type of activities that will generate a log message:
   - **Accepted Incoming Connections** - activating this check box generates a log message for each successful attempt to establish an inbound connection to the local network.
   - **Accepted Outgoing Connections** - activating this check box generates a log message for each successful attempt to establish an outgoing connection to the public network.

3. Select the type of blocked events to be listed in the log:

   - **All Blocked Connection Attempts** - activating this check box generates log messages for all blocked events.
   - **Other Blocked Events** - if "All Blocked Connection Attempts" is unchecked, select specific blocked events from this list to generate log messages.

4. Click in the "Remote Administration Attempts" check box to write a log message for each remote-administration connection attempt, whether successful or not.

5. Click in the "Connection States" check box to track connection handling by the firewall and Application Level Gateways (ALGs).

6. Click **Apply** to save changes.

Using Parental Controls

7

The abundance of harmful information on the Internet poses a serious challenge for employers and parents alike - "How can I regulate what my employee/child does on the Internet?" The Wireless Broadband Router's Parental Controls allows users to regulate, control, and monitor Internet access. By classifying and categorizing online content, it is possible to create numerous Internet access policies and easily apply them to networked computers.

Activating Parental Controls

To create a basic access policy for a computer on the Router's network, click **Parental Control** from the top of the Home screen and follow these instructions:

1. The "Parental Control" screen appears. Click in the "Enable" check box to activate the access policy mechanism.

2. Enter a "Rule Name" and "Description" for the access policy in the appropriate text boxes.