Events

https://campus.barracuda.com/doc/73719592/

The Barracuda CloudGen Firewall is equipped with an elaborate event-based notification model to help you keep track of events and system access on all levels (operating system, Barracuda Networks infrastructure, and Barracuda CloudGen Firewall services). The event system of the Barracuda CloudGen Firewall creates events for special system processes and for all services that are configured on the unit. Some events are generated per default, some as configured according to system and service requirements.

Security and Operational Events

All security and operational events are classified according to their severity and notification type.

For more information, see Operational Events and Security Events.

Viewing and Managing Events

The event monitor lists all events generated on the Barracuda CloudGen Firewall. Icons and fonts indicate the type and importance of the events on the list, helping you determine which actions must be taken. You can view event properties, delete events, filter and refresh the list of events. Some events, such as error events or events that are displayed in black bold text, require acknowledgement. If an event has an alarm, you can also either reset or disable the alarm.

For more information, see the Barracuda Firewall Admin Events tab.

Configure Event Settings

The **Eventing** configuration page in the config tree displays all available event types. From this page, you can assign severity levels and notifications to each event type, edit all available severity levels and add or edit notification types. Each notification specifies a server or client action (such as executing a program or sending emails and/or SNMP traps) to be performed by the firewall when an assigned event occurs. Server actions are performed by the firewall or Control Center, client actions are performed by the Windows client Barracuda Firewall Admin is running on.

For more information, see How to Configure Basic, Severity, and Notification Settings for Events.

Access Control

Each system access attempt poses a potential security risk. By configuring access control notifications, you can keep track of successful or unsuccessful system access attempts. Active notifications make it more difficult than simple log file based accounting for potential intruders to conceal their actions.

For more information, see How to Configure Access Notifications.

Event Propagation

The firewall audit service allows propagating firewall events to the Control Center. Firewall Audit data is stored locally by default, but may be forwarded to the Barracuda Firewall Control Center or to a dedicated Barracuda CloudGen Firewall running the Firewall Audit Log service for central audit log file collection.

For more information, see How to Enable the Firewall Audit Log Service.