Logging

https://campus.barracuda.com/doc/72516608/

The firewall incorporates hardware and software fail-safe mechanisms that are indicated via system alerts and logs. You can inspect the logs to see what is happening with the traffic.

> Do NOT write, rename, or put any files into this directory. Editing the contents of this directory can cause logs to be displayed incorrectly.

Configure Log Streaming

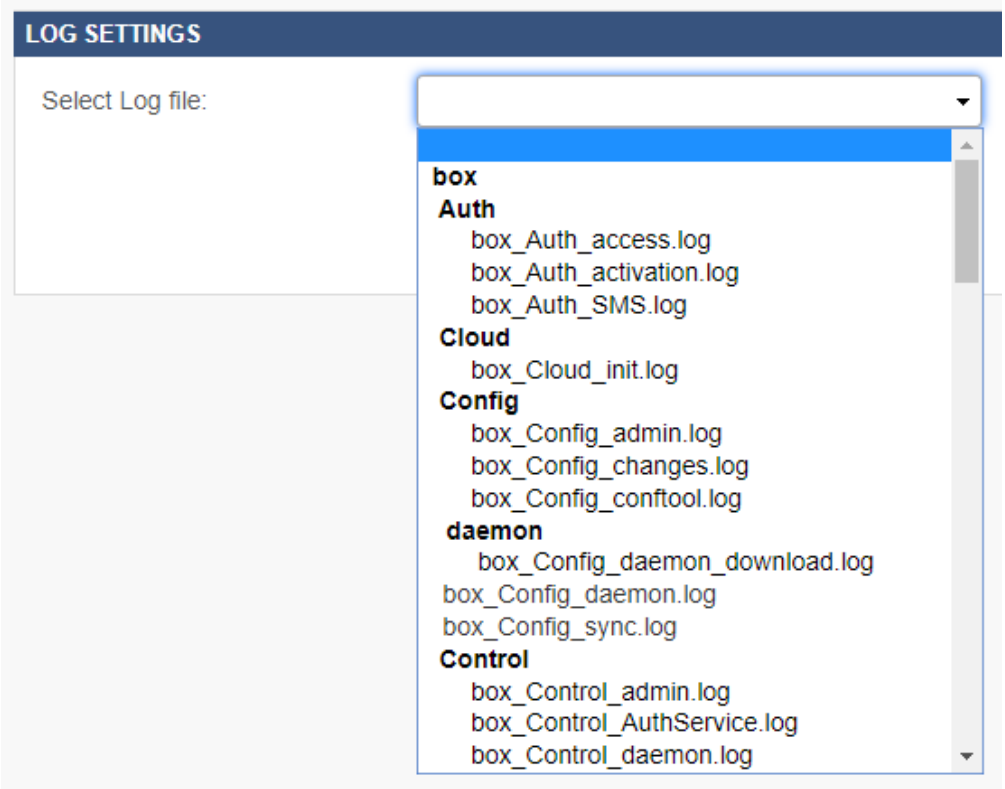
By default, log files are stored on the local file system of the firewall. In addition, log files can be sent to external Syslog servers.

For more information, see Log File Handling.

Viewing Log Files

To access the logs on the CloudGen Firewall web interface:

1. Go to **LOGS**.
2. Expand **Select Log file** drop-down list
3. Choose the log file type.



From the **LOGS** tab, you can view a number of log files to monitor and troubleshoot the firewall.

Authentication Log

The Authentication Log (Auth) displays messages from the authentication service. This includes logins for the web interface and messages from the various authentication methods. For example, if a client cannot access a service, the unsuccessful authentications are written into the log. Successful authentications are also recorded.

Firewall Log

The Firewall Log (NGFW) displays firewall activity, such as rules that have been executed and traffic that has been dropped. It lists all connections on the firewall. You can filter the log by criteria such as a source IP address or network, or the time that the connections occurred.

HTTP Log

The HTTP Log displays the activities of the firewall's connection to the Barracuda Web Security Service. There are several codes in the log. For details on these codes, see the HTTP Log Codes Overview section.

Network Log

Use the Network Log to investigate why network configuration changes are not working properly or cannot be activated. The messages in the Network Log might explain the problem. If not, check the network configuration again for any problems or conflicts.

VPN Log

The VPN Log displays information for all client-to-site and site-to-site VPN tunnels. Use this log to investigate why VPN tunnels and PPTP connections are disconnecting or not being established. To see the messages for specific VPN connections, you can also filter the log by IP addresses.

HTTP Log Codes Overview

The following tables provide details on the codes that you might see on the **LOGS > HTTP Log** page.

TCP Codes

TCP_" refers to requests on the HTTP port (3128)

Code	Description
TCP_HIT	A valid copy of the requested object was in the cache.
TCP_MISS	The requested object was not in the cache.
TCP_REFRESH_HIT	An expired copy of the requested object was in the cache. Squid made an If-Modified-Since request, and the response was "Not Modified."
TCP_REFRESH_FAIL_HIT	An expired copy of the requested object was in the cache. Squid attempted to make an If-Modified-Since request, but it failed. The old (stale) object was delivered to the client.

TCP_REFRESH_MISS	An expired copy of the requested object was in the cache. Squid made an If-Modified-Since request and received a new object.
TCP_CLIENT_REFRESH	The client issued a request with the "no-cache" pragma. ("reload" - handled as MISS)
TCP_IMS_HIT	An If-Modified-Since GET request was received from the client. A valid copy of the object was in the cache (fresh).
TCP_IMS_MISS	An If-Modified-Since GET request was received from the client. The requested object was not in the cache (stale).
TCP_SWAPFAIL	The object was believed to be in the cache, but could not be accessed.
TCP_DENIED	Access was denied for this request.

ERR Codes

Error	Description
ERR_READ_TIMEOUT	The remote site or network is unreachable; it may be down.
ERR_LIFETIME_EXP	The remote site or network may be too slow or down.
ERR_NO_CLIENTS_BIG_OBJ	All clients went away before transmission completed, and the object is too big to cache.
ERR_READ_ERROR	The remote site or network may be down.
ERR_CLIENT_ABORT	Client dropped connection before transmission completed. Squid fetched the Object according to its settings for `quick_abort'.
ERR_CONNECT_FAIL	The remote site or server may be down.
ERR_INVALID_REQ	Invalid HTTP request.
ERR_UNSUP_REQ	Unsupported request.
ERR_INVALID_URL	Invalid URL syntax.
ERR_NO_FDS	Out of file descriptors.
ERR_DNS_FAIL	DNS name lookup failure.
ERR_NOT_IMPLEMENTED	Protocol not supported.
ERR_CANNOT_FETCH	The requested URL cannot currently be retrieved.
ERR_NO_RELAY	There is no WAIS relay host defined for this cache.
ERR_DISK_IO	The system disk is out of space or failing.
ERR_ZERO_SIZE_OBJECT	The remote server closed the connection before sending any data.
ERR_FTP_DISABLED	This cache is not configured to retrieve FTP objects.
ERR_PROXY_DENIED	Access denied. Users must be authenticated before accessing this cache.

Figures

1. select_log.png