Available Log Files and Structure

https://campus.barracuda.com/doc/79463293/

The CloudGen Firewall creates log files for system processes, box services, and configured services such as Forwarding Firewall, HTTP Proxy, VPN, etc. Logging is processed according to system and service settings.

Box

Service	Log File	Description
Auth	Box\Auth\SMS	Displays informational logs about authentication via SMS notifications concerning configuration processes, updates, and changes.
	Box\Auth\access	Provides informational log files about login and access attempts to the CloudGen Firewall, displaying access source, and opening and closing of sessions.
	Box\Auth\activation	Displays log files concerning process activation and provides information about message board configuration and details.
Azure	Box\Azure\events	Contains events for Azure Event Hub connections.
Cloud	Box\Cloud\control	Provides logs files for the Azure and AWS cloud integration features.
Config	Box\Config\MC-update	Provides informational log files about PAR file processing, updates, and process activation on managed firewalls.
	Box\Config\HA-update	Displays notification logs about HA startup/shutdown and provides information about HA operations, such as configuration, updates, and changes.
	Box\Config\VirusScanner	Provides informational log files about the Virus Scanner updating processes.
	Box\Config\admin	Contains log files about login, authentication, and connection status of administrative session s by displaying IP address and port, and shows the operative processes initiated by the administrative instance.
	Box\Config\changes	Displays informational logs about processes concerning configuration changes such as adding or removing servers and services and activation processes.
	Box\Config\conftool	Display informational logs about processes concerning internal activation and database processes.
	Box\Config\daemon	Contains log files about processes initiated by the configuration daemon such as loading processes, configuration checks, cache generation, and session termination.
	Box\Config\daemon_download	Contains log files about downloading p rocesses initiated by the configuration daemon, providing information concerning progress, changes, and signatures.
	Box\Config\provision	Contains log files concerning Azure Cloud provisioning, if configured .
	Box\Config\shell	Displays notification logs about shell operations, providing information concerning admin permissions and account settings.
	Box\Config\sync	Displays log files concerning synchronization processes, showing connection details, update status, and progress.
Control	Box\Control\AuthService	Contains log files for administration, authentication processes, and access information concerning user groups, access interfaces, and domains of external authentication services.
	Box\Control\AuthService_dcclient	Contains log files for administration, authentication processes, access information concerning user groups, access interfaces, and domains of the Barracuda DC Client.
	Box\Control\Telemetry	Displays the performance and usage data sent to the Barracuda telemetry servers.
	Box\Control\admin	Displays informational logs about connection processes such as login, source address, and box service processes.
	Box\Control\daemon	Contains log files about security status checks initi ated by the control daemon and displays controld processes.

Event	Box\Event\apns	Displays process logs concerning the Apple Push Certificate provider for mobile devices (APNS).
	Box\Event\eventS	Contains log files generated by security events. For more information, see Security Events.
	Box\Event\operative	Contains log files generated by operational events. For more information, see Operational Events.
Firewall	Box\Firewall	Displays log files concerning general firewall configuration changes, ruleset updates, including operation details and time settings.

Firewall	Box\Firewall\Activity	Displays firewall log files providing in-depth information about firewall rule processing. All entries of this log file are pipe separated information. Depending on the configured setting, they are in the format **...|key=value|key=value|...** or **...|value|value|...** format. For information how to alter between both formats, see General Firewall Configuration • **Time** – Timestamp of the respective log entry. • **Type** – Information about the Type of log entry. E.g. **Security** or **Info** • **Action** – Information about the action taken according to the firewall ruse set configuration. • **type** – Information about the origin type of traffic and ruleset used. ◦ **LIN** – Local In. The incoming traffic on the host firewall. ◦ **LOUT** – Local Out. The outgoing traffic from the host firewall. ◦ **LB** – Loopback. The traffic via the loopback interface. ◦ **FWD** – Forwarding. The outbound traffic via the forwarding firewall. ◦ **IFWD** – Inbound Forwarding. The inbound traffic to the firewall. ◦ **PXY** – Proxy. The outbound traffic via the proxy. ◦ **IPXY** – Inbound Proxy. The inbound traffic via the proxy. ◦ **TAP** – Transparent Application Proxying. The traffic via stream forwarding. ◦ **LRD** – Local Redirect. Redirected traffic configured in forwarding ruleset. • **proto** –The protocol that was used. For example, TCP, UDP, or ICMP. • **srcIF** – The source network interface of the session. • **srcIP** – The source IP address of the session. • **srcPort** – The source port of the session. • **srcMAC** – The MAC address of the session's source network interface. • **dstIP** – The destination IP address of the session. • **dstPort** – The destination port of the session. • **dstService** – The destination service of the session. • **dstIF** – The destination network interface of the session. • **rule** – The name of the firewall rule processing the session. • **Info** – Operational information for the session. • **srcNAT** – Source NAT address of the session. • **dstNAT** – Destination NAT address of the session. • **duration** – Duration of the session. • **count** – Number of sessions processed. • **receivedBytes** – Received traffic of a session in bytes. • **sentBytes** – Sent traffic of a session in bytes. • **receivedPackets** – Received traffic of a session in packets. • **sentPackets** – Received traffic of a session in packets. • **user** – The name of the user, if the session was handled by a firewall rule that requires authentication. • **protocol** – The protocol of a session. For example, TCP, UDP, or ICMP. • **application** – The application context of a session. • **target** – The application target. • **content** – The application content. • **urlcat** – The URL category the session belongs to.
	Box\Firewall\IPSDownload	Contains log files generated by the Intrusion Prevention System, showing database file download status and information.
	Box\Firewall\Rule-<no-match>	Displays firewall log files providing information about firewall rule processing of traffic not applicable to firewall policies.
	Box\Firewall\appid_stat	Contains log files generated by Application Control, showing system processes related to applications, including configuration and download information.
	Box\Firewall\appid_urlcat	Contains log files generated by Application Control's URL Filter, showing system processes related to Application Control's URL Filter processes, including configuration and download information.
	Box\Firewall\auditop	Contains log files generated by the FWAudit service.
	Box\Firewall\auth	Displays informational log files about processes initiated by the fwauth daemon, providing information concerning authentication, such as listening IP address and port.
	Box\Firewall\sync	Displays log files concerning firewall HA synchronization processes, showing connection details, update status, and progress.
	Box\Firewall\threat	Displays log files generated by ATP, IPS, DNS Sinkhole, and the Virus Scanner.

Logs	Box\Logs\bsyslog	Contains box log files created by bsyslog.
	Box\Logs\logd	Contains box log files created by logd.
	Box\Logs\logstor	Contains box log files created by logstor.
	Box\Logs\logwrapd	Contains box log files created by logwrapd.
	Box\Logs\psyslog	Contains box log files created by psyslog.
Network	Box\Network\QoS	Provides network-related log files about processes such as Quality of Service configuration and traffic shaping.
	Box\Network\activation	Provides log files related to network activation and changes, displaying internal processes such as routing table, cache and interface status and details.
	Box\Network\dhcp	Displays network-related log files created by the dhcp service, such as link detection and worker-related processes.
	Box\Network\dhcpd	Displays log files about the dhcp configuration and provides information about broadcasts and the status and progress of dhcp request.
	Box\Network\shaping	Provides informational log files about processes related to VPN traffic shaping status and processes.
	Box\Network\pppd	Displays network-related log files created by the xDSL service, such as link detection and worker-related processes.
	Box\Network\umts	Displays network-related log files created by the Wireless WAN service, such as link detection and worker-related processes.
REST	Box\REST\control	REST calls to the control daemon.
	Box\REST\firewall	REST calls to the firewall service.
	Box\REST\restd	Log files for the REST daemon.
RESTd	Box\RESTd	REST calls to box level services and queries.
Release	Box\Release\UpdateServer	Contains log files about processes related to Barracuda security subscriptions and Barracuda update server reachability.
	Box\Release\update	Contains log files about processes related to release updates.
	Box\Release\update_hotfix	Displays informational log files about processes related to release updates including hotfixes.
	Box\Release\check	Displays informational log files about processes related to release checks.
SSH	Box\SSH\config	Displays log files about internal processes that are generated by the box ssh daemon, such as startup, read and write operations, etc.
	Box\SSH\sshd	Displays log files about internal processes that are generated by the box ssh daemon, such as connection details, data transfer, and session behavior.
Settings	Box\Settings	Displays log files concerning the box settings configuration, and displays information and error logs in case of box configuration failures.
Settings	Box\Settings\DNS	Displays informational log files about the box DNS settings configuration and notifies about DNS operations such as address assignment and zone-related processes.
	Box\Settings\time	Contains log files related to NTP, displaying information about time server configuration , connection status, and synchronization processes.
	Box\Settings\activation	Provides log files related to box settings configuration activation and changes, displaying the process details.
Snmp	Box\Settings\Snmp	Provides informational log files about startup and working status of the box snmp service and shows the details (pid, etc.).
Statistics	Box\Statistics\cstatd	Displays log files related to cstatd including information about stati stics files collection processes created by cstatd.
	Box\Statistics\distd	Displays log files related to di statd including login information, connection details, and processes created by distatd.
	Box\Statistics\qstatd	Displays log files related to qstatd, showing information about Control Center statistics querying processes.

System	Box\System\boot	Contains log files related to boot processes including release consistency checks.
	Box\ System \bootloader	Contains informational log files related to boot loader operations such as system startup processes and configuration checks.
	Box\ System \cron	Displays informational log files created by the cron daemon and notifies about executed services and commands.
	Box\ System \klogd	Contains system related log files created by clogd.
	Box\ System \messages	Contains system log files related to messages.
	Box\ System \mgmaccess	Contains system log files related to management access.
	Box\ System \phionrc	Contains system-related log files created by phionrc.
	Box\ System \powersupply	Contains system log files related to power supply.
	Box\ System \syslog	Contains system-related log files created by the syslog daemon.
	Box\ System \tuning	Contains system log files related to system tuning.
Watchdog	Box\Watchdog \config	Contains log files created by Watchdog providing general information about the Watchdog configuration.
	Box\Watchdog \monitor	Contains log files created by Watchdog providing monitoring details.
	Box\Watchdog \repair	Contains log files created by Watchdog providing information about repair processes.
	Box\Watchdog \smartd	Contains log files created by Watchdog providing information about smartd processes.

Reports

These logs are documented with the *Reports_* prefix. They include entries that are carried out in continuous intervals, such as cronjobs.

Service	Log File	Description
Network	Reports\Network\check	Contains reporting log files related to network activity providing information about network checks.
Statistics	Reports\Network\Statistics\statcook	Contains reporting log files related to statistics cooking.
procpar	Reports\procpar	Contains reporting log files created by procpar.
changes	Reports\changes	Contains reporting log files related to configuration changes.
treemigration	Reports\treemigration	Contains log files i ncluding entries that are carried out in continuous intervals, such as cronjobs.

Fatal

All fatal errors that can occur on a CloudGen Firewall are, in addition to the original log file, collected in this section. The original log file is added in the fatal log message text as a prefix.

Server

The virtual server node contains the following log files if the services are present:

Service	Log File	Description
Firewall	<S1>\<FW>\FW	Displays notification logs about Forwarding Firewall startup/shutdown with the location path and provides information about firewall operations, such as configuration loading, updates, and changes. Further logs in this section provide information on installation of updated settings and firewall rules.
	<S1>\<FW>\Content	Provides informational log files about the loading process of the Forwarding Firewall ruleset.
	<S1>\<FW>\CustomExternalImport	Log files containing information about importing and setting the custom external network objects. On cloud firewalls these imports are handled automatically by the cloud-initstart process.
	<S1>\<FW>\SSL	Displays log files concerning SSL Inspection, notifies about the SSL Inspection progress and working state, and displays information and error logs in case of detections, errors, or certificate failures.
	<S1>\<FW>\auth	Contains log files about opening, connection status, and closing of firewall sessions, displaying IP address and port of the connected clients and peers. Information is displayed in case of login failures, file requests, and transactions concerning fwauth, errors or SSL certificate failures.
	<S1>\<FW>\sipproxy	Provides log files concerning startup, activation of child processes, and socket opening of the SIP Proxy, and displays informational log files in case of network interface changes.

HTTP Proxy	<S1>\<HTTP>\access	Contains log files created by the HTTP Proxy service, providing information about access paths of destinations.
	<S1>\<HTTP> \cache	Displays log files about the proxy cache and i nforms about caching processes, such as cache initialization, starting the Squid cache, adding domain and name server, creating sockets and directories, connecting to access cache workers, memory, scanning, etc.
	<S1>\<HTTP> \controlSquid	Informs about the Squid cache version at startup, displays parent and child processes with process ID and path, and s hows log files about Squid cache operations.
	<S1>\<HTTP> \gui	Provides informational log files about proxy GUI worker startup and shows the maximum fail cache age.
Anti Virus	<S1>\<VIR> \AV	Contains log files created by AVIRA antivirus, providing e ngine and VDF version, and displays information about virus scanning, threat detections, and actions.
	<S1>\<VIR> \clamav	Contains log files created by the clamAV antivirus engine, providing download and update information on database and signatures, safe browsing, whitelisting, and information about virus scanning, threat detection, and actions.
URL Filter	<S1>\<URL> \Cofsd	Provides log files about the Web Filter service, showing information about licensing, and URL filtering processes and actions.
OSPF-RIP-BGP	<S1>\<DYNBO2>\access	Contains log files created by dynamic routing protocols such as OSPF, RIP, or BGP.

VPN	<S1>\<VPN>\VPN	Provides informational log files about the status of VPN sessions, showing tunnel transport, keying, and updates, and displays notifications in case of tunnel and transport failure.
	<S1>\<VPN>\ikev2	Contains notification log files created by the VPN service, providing debugging information related to IPsec if debugging mode for IKEv2 is enabled in the VPN settings.
	<S1>\<VPN>\ike	Contains notification log files created by the VPN service, providing debugging information related to IPsec if debugging mode for IKE is enabled in the VPN settings.
	<S1>\<VPN>\pptpd	Contains notification log files created by the VPN service, providing information related to pptpd.
	<S1>\<VPN>\sslvpn	Contains log files created by SSLVPN, displaying configuration, tunnel transport, and keying details.
	<S1>\<VPN>\wanopt	Contains informational log files created by the VPN service, providing information related to wanopt protocol handling processes.
	<S1>\<VPN>\wanopt-comp	Contains informational log files created by the VPN service, providing additional information related to wanopt processes .
DHCP	<S1>\<DHCP>	Provides log files created by the DHCP service and shows information about DHCP processes, requests, and IP address assignment.
DHCP Relay	<S1>\<DHCP-Relay>	Provides log files created by the DHCP Relay service, displaying processes and packet transmission details.
DNS	<S1>\<DNS>	Contains log files created by the DNS service providing information about DNS configuration, listening interfaces, and DNS zone activity and processes.
Wi-Fi	<S1>\<Wi-Fi>	Contains log files created by the Wi-Fi service providing information about Wi-Fi configuration including status, keying, and driver processes.
FTP Gateway	<S1>\<FTP-GW>	Contains log files created by the FTP Gateway service, displaying information about the FTP gateway, FTP sessions, traffic, and file transfer actions and details.

Mail Gateway	<S1>\<MAIL-GW>	Contains log files created by the Mail Gateway service, displaying Mail Gateway traffic details such as mail operations, data size limits, redirection, and file attachment processing.
SNMP	<S1>\<SNMP>	Provides log files created by the SNMP service, d isplaying access control information details and system processes for attached devices.
Spam Filter	<S1>\<Spam Filter>	Contains log files created by the Spam Filter service, providing information about spam filtering processes and performed actions.
SSH Proxy	<S1>\<SSH>\<SSH>	Displays log files created by the SSH Proxy service, providing information about SSH configuration and processes, including target access details etc.
	<S1>\<SSH>\sshd	Displays informational log files about SSH Proxy sessions, providing traffic related details such as server listening ports and IP addresses.
Secure Web Proxy	<S1>\<S-PROXY>	Displays log files created by the Secure Web Proxy and i nforms about web filtering processes and actions such as allowing and denying URL requests if configured.
Access Control Service	<S1>\<Access Control>\<SSH>	Provides log files created by the Access Control service and shows information about access control policy processing and monitored actions and registry checks according to the configured log level.
	<S1>\acs\acs	Provides log files created by the Access Control service and shows information about access control policy processing and monitored actions and registry checks according to the configured log level.
	<S1>\acs\gui	Displays informational log files about Access Control service eventing processes.
	<S1>\acs\matcher	Displays informational log files about access control policy changes.

Server CC

The virtual server node on the Control Center contains the following log files if the services are present:

Service	Log File	Description
CC-Access-Control-Service	<S1>\ACCESS	Contains information about access to the Control Center via several connection methods, e.g., login, file access, or GUI.
CC-Audit-Service	<S1>\AudLog	Container directory for logs that are created on managed boxes and transferred to the Control Center.
	<S1>\AudLog\AudLog	Contains information from the worker process that handles auditing logs from boxes managed by the Control Center.
	<S1>\AudLog\admin	Contains information about administrative events relating to auditing tasks on CC level.
Firewall	<S1>\CCFW	Displays notification logs about Forwarding Firewall startup/shutdown with the location path and provides information about firewall operations, such as configuration loading, updates, and changes. Further logs in this section provide information on installation of updated settings and firewall rules.
	<S1>\CCFW\Content	Provides informational log files about the loading process of the Forwarding Firewall ruleset.
	<S1>\CCFW\SSL	Displays log files concerning SSL Inspection, notifies about the SSL Inspection progress and working state, and displays information and error logs in case of detections, errors, or certificate failures.
	<S1>\CCFW\auth	Contains log files about opening, connection status, and closing of firewall sessions, displaying IP address and port of the connected clients and peers. Information is displayed in case of login failures, file requests, and transactions concerning fwauth, errors, or SSL certificate failures.
	<S1>\CCFW\sipproxy	Provides log files concerning startup, activation of child processes, and socket opening of the SIP Proxy, and displays informational log files in case of network interface changes.

CC-VPN-Service	<S1>\ CCVPN	Container directory for VPN log files fed during VPN connections between the CC and the managed boxes.
	<S1>\ CCVPN\CCVPN	Provides informational log files about the status of VPN sessions, showing tunnel transport, keying, and updates, and displays notifications in case of tunnel and transport failure.
	<S1>\ CCVPN\ vpnstat	Contains information about the health state of open tunnels served by the tunnel server process.

CC-Configuration-Service	<S1>\CONF	Container directory for logs that are created by processes part of the Control Center's configuration system for managed boxes.
	<S1>\CONF\CONF	Contains information about configuration sessions that were initiated on the Control Center.
	<S1>\CONF\admin	Contains information about login, authentication, and connection status of administrative session s, displaying IP address and port, and shows the operative processes initiated by the administrative instance. Information relates to CC level.
	<S1>\CONF\boxupdate	Contains information about update processes that were initiated on managed boxes from the Control Center.
	<S1>\CONF\c3d	Contains information about configuration updates, state, and delivery of firmware updates between the Control Center and SCAs. In case no SCAs are connected, this log file is empty.
	<S1>\CONF\changes	Contains information about changes made on the Control Center that affect configuration of managed firewalls.
	<S1>\CONF\download	Contains information about downloads that were initiated on the Control Center.
	<S1>\CONF\exec	Contains information about triggering the execution of external processes initiated by the Control Center.
	<S1>\CONF\licupdate	Contains information about license updates.
	<S1>\CONF\masterd	Contains information about the master daemon running on the Control Center.
	<S1>\CONF\softwarestatus	Contains information created by the software update daemon on the Control Center.
	<S1>\CONF\status	Contains status information about the managed boxes.
	<S1>\CONF\sync	Contains information about synchronization processes.

CC-Event-Service	<S1>\EVENT	Container directory for logs that contain information about events.
	<S1>\EVENT\eventS	Contains information about security events. For more information, see Security Events .
	<S1>\EVENT\operative	Contains information about operational events. For more information, see Operational Events.
CC-Statistic-Collector	<S1>\STCOLL	Contains information created by the engine responsible for collecting statistical information.
CC-Statistics-Viewer	<S1>\STVIEW	Contains information created by the engine responsible for displaying statistical information.
CC-Syslog-Service	<S1>\Syslog	Container directory for logs that contain information about different processes and daemons that run with system privileges on CC level.
	<S1>\Syslog\Syslog	Contains system-related log information created by the syslog daemon on CC level.
	<S1>\Syslog\csslsrv	Contains system-related log information created by the SSL service daemon on CC level.
	<S1>\dstats	Contains information collected from managed boxes by the daemon for statistics.
	<S1>\mdist2	Contains information about authentication syncs, e.g., synchronization between Virus Scanner versions etc.