Available Log Files and Structure

https://campus.barracuda.com/doc/41115947/

The Barracuda NG 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.

The Barracuda NG Firewall provides the following structure and log files.

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 Barracuda NG Firewall firewall system, displaying access source, opening and closing of sessions.
	Box\Auth\activation	Displays log files concerning process activation and provides information about message board configuration and details.
Config	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\admin	Contains log files about login, authentication and connection status of administrative sessions, 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 conserning 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 processes initiated by the configuration daemon providing information concerning progress, changes and signatures.
	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, access information concerning user groups, access interfaces, and domains of external authentication sevices.
	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\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 initiated by the control daemon and displays controld processes.
Event	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 including access time, rule action, service and traffic details. • **Allow –** A newly establsihed session was allowed by Firewall based on a policy in the forw*arding firewall* ruleset. • **LocalAllow –** A newly establsihed session was allowed by Firewall based on a policy in the *host firewall* ruleset. • **Fail –** A newly establsihed session was allowed by Firewall based on a policy in the *forwarding firewall* ruleset, but the session failed. • **LocalFail –** A newly establsihed session was allowed by Firewall based on a policy in the *host firewall* ruleset, but the session failed. • **Terminate –** An allowed session was successfully terminated by the administrator, timed out, or was reset by a peer. (Forwarding Firewall) • **LocalTerminate –** An allowed session was successfully terminated by the administrator, timed out, or was reset by a peer. (Host Firewall) • **Block –** A newly establsihed session was blocked by Firewall based on a policy in the *forwarding firewall* ruleset. • **LocalBlock –** A newly establsihed session was blocked by Firewall based on a policy in the *host firewall* ruleset. • **Drop –** A newly established session was silently dropped • **type –** Information about the origin type of traffic and used ruleset. ◦ ■ **LIN** – Local In. The incoming traffic on the box firewall. ■ **LOUT** – Local Out. The outgoing traffic from the box 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, and ICMP. • **srcIF –** The source network interface 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 if the session. • **dstPort –** The destination port of the session. • **dstSevice –** The destination service of the session. • **dstIF –** The destination network interface of the session. • **rule –** The name of the firewall rule processinf 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, and ICMP. • **application –** The application context of a session.. • **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-	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\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.

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 UMTS/3G service, such as link detection and worker related processes.
Release	Box\Release\UpdateServer	Contains log files about processes releated to Barracuda security subscriptions and Barracuda update server reachability.
	Box\Release\update	Contains log files about processes releated to release updates.
	Box\Release\update_hotfix	Displays informational log files about processes releated to release updates including hotfixes.
	Box\Release\check	Displays informational log files about processes releated 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 address assignment and zone related processes.
	Box\Settings\NTPd	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 statistics files collection processes created by cstatd.
	Box\Statistics\distd	Displays log files related to distatd including login information, connection details and processes created by distatd.
	Box\Statistics\qstatd	Displays log files related to qstatd, showing information about Barracuda NG 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 and 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 including entries that are carried out in continuous intervals, such as cronjobs.

Fatal

All fatal errors that can occur on a Barracuda NG 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	\\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.
	\\Content	Provides informational log files about the loading process of the forwarding firewall ruleset.
	\\SSL	Displays log files concerning SSL Interception, notifies about the SSL Interception progress and working state, and displays information and error logs in case of detections, errors or certificate failures.
	\\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.
	\\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	\\access	Contains log files created by the HTTP Proxy service, providing information about access paths of destinations.
	\\cache	Displays log files about the Proxy cache and informs about caching processes, such as cache initialization, starting the Squid cache, adding domain and nameserver, creating sockets and directories, connecting to access cache workers, memory, scanning, etc.
	\\controlSquid	Informs about the Squid cache version at startup, displays parent and child processes with process ID and path, and shows log files about Squid cache operations.
	\\gui	Provides informational log files about Proxy GUI worker startup and shows the maximum fail cache age.
Anti Virus	\\AV	Contains log files created by AVIRA Anti Virus, providing engine and VDF version and displays information about virus scanning, threat detections and actions.
	\\clamav	Contains log files created by the clamAV Anti Virus engine, providing download and update information on database and signatures, safebrowsing, whitelisting, and information about virus scanning, threat detections and actions.
URL Filter	\\Cofsd	Provides log files about the Web Filter service, showing information about licensing, URL filtering processes and actions.
OSPF-RIP-BGP	\\access	Contains log files created by dynamic routing protocols such as OSPF, RIP or BGP.

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.
	\\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.
	\\sslvpn	Contains log files created by SSLVPN, displaying configuration, tunnel transport and keying details.
DHCP	\	Provides log files created by the DHCP service and shows information about DHCP processes, requests and IP address assignment.
DHCP Relay	\	Provides log files created by the DHCP Relay service, displaying processes and packet transmission details.
DNS	\	Contains log files created by the DNS service providing information about DNS configuration, listening interfaces, DNS zone activity and processes.
WIFI	\	Contains log files created by the WIFI service providing information about WIFI configuration including status, keying and driver processes.
FTP Gateway	\	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	\	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	\	Provides log files created by the SNMP service, displaying access control information details and system processes for attached devices.
Spam Filter	\	Contains log files created by the Spam Filter service, providing information about Spam filtering processes and performed actions.
SSH Proxy	\\	Displays log files created by the SSH Proxy service, providing information about SSH configuration and processes, including target access details etc.
	\\sshd	Displays informational log files about SSH Proxy sessions, providing traffic related details such as server listening ports and IP addresses.
Secure Web Proxy	\	Displays log files created by the Secure Web Proxy and informs about web filtering processes and actions such as allowing and denying URL requests if configured.
Access Control Service	\<Access Control>\	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.