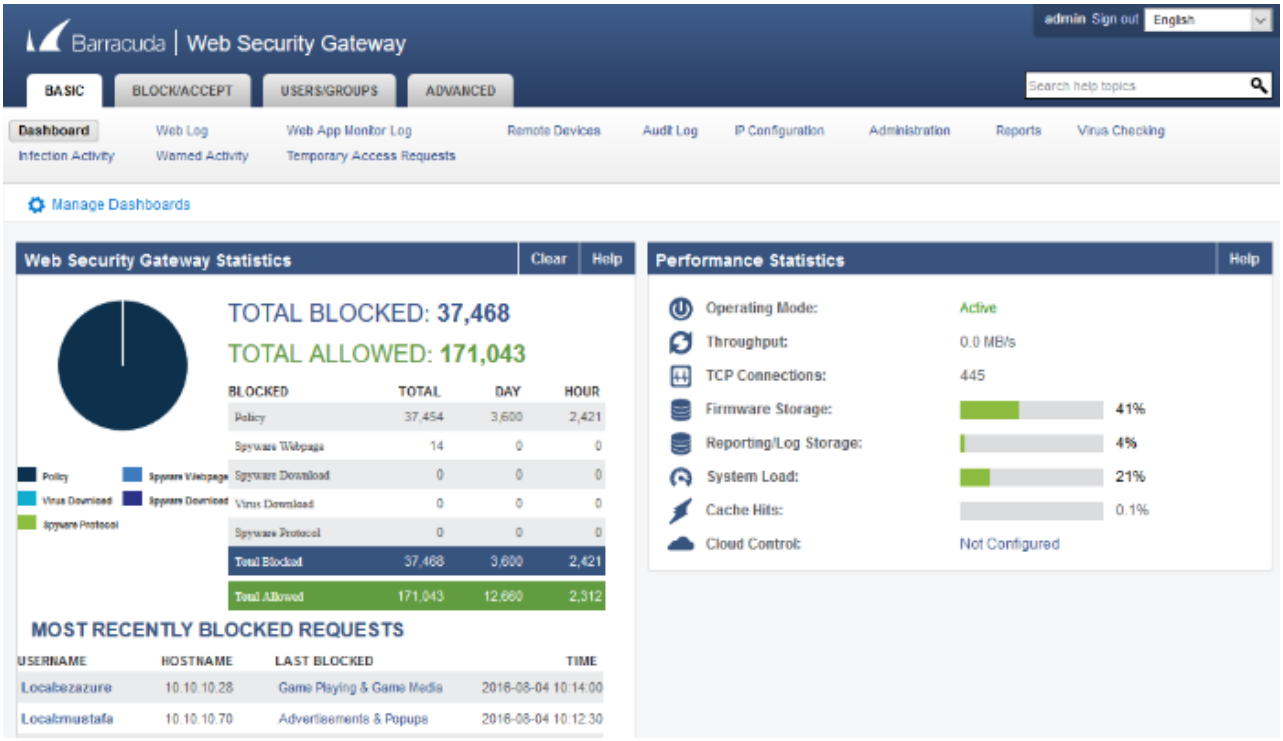
Barracuda Web Security Gateway

Features Brochure



Spyware and Virus Protection

The Barracuda Web Security Gateway uses a continually updated database to identify and block access to sites known to host spyware and viruses. It also detects installed spyware trying to access the Internet. Upon discovery, it blocks the spyware activity and notifies the administrator. By using dual-layer virus blocking, decompressing archives, and blocking file types, the antivirus engine in the Barracuda Web Security Gateway protects networks from aggressive viruses.

Barracuda Central

All Barracuda products are supported by Barracuda Central, a 24x7 advanced security operations centre that works continuously to monitor and block the latest Internet threats. Barracuda Central collects data from more than 150,000 collection points worldwide and analyses it to develop defences, rules, and signatures. As new threats emerge, Barracuda Central is quick to respond to early outbreaks and delivers the latest definitions through Barracuda Energise Updates. These updates require zero administration and ensure that the Barracuda Web Security Gateway provides comprehensive and accurate protection against the latest Internet threats.

Web 2.0 and Social-Media Regulation

The Barracuda Web Security Gateway provides granular control over Web 2.0 sites and web applications, including social media platforms. Scanning and inspecting SSL-encrypted traffic for specific categories and domains enable granular policy enforcement. Administrators can also configure the Barracuda Web Security Gateway to monitor and archive outbound web application communications like Facebook posts, tweets, and web-based email to a message archiving solution, such as the Barracuda Message Archiver. These messages can be indexed and then mined for forensic analysis. Suspicious activity alerts can also be generated using predefined or customised categories.

Application Control

In addition to standard port/protocol-based policies, the Barracuda Web Security Gateway uses real-time deep packet inspection technology to analyse protocols independent of their port of destination servers. By integrating Layer 7 protocol analysis with policy controls, the Barracuda Web Security Gateway enables complete control over application usage.

Content Filtering

The Barracuda Web Security Gateway provides flexible controls for pinpoint regulation of online activity. Administrators can create policies that control user access to 99.7 percent of commonly visited websites using 95 content categories including pornography, violence, hacking, sports, news, dating, shopping, chat, and more. Content filtering policies can be customised to restrict specific websites or look for patterns in web addresses.

The Barracuda Web Security Gateway's image/multimedia safe search feature prevents search engines such as Google, Yahoo, and Bing from displaying objectionable thumbnail images in search results. Administrators can also create policies that control web-file downloads based on file type.

SSL Inspection

Organisations can control online content normally hidden by SSL. This includes content found in social-media platforms, web-based email, and search engines. Administrators can specify domains and URL categories for which SSL-encrypted traffic will be decrypted and scanned for malware and policy. Not only can organisations restrict entire platforms, it's now possible to enforce granular access for secure websites (e.g.,YouTube).

Intuitive Dashboard Views

The Barracuda Web Security Gateway provides an intuitive dashboard interface for quick understanding of the threats and activities of users on the network. The changes are immediately apparent on the dashboard that features recent infection activity, potentially suspicious activities, a live view of TCP connection usage, and summary data of network usage.

Comprehensive Reporting

To budget computing resources and ensure adherence to corporate policies, IT and HR administrators often require detailed information about how Internet users in the network are spending time online. In addition to its powerful web filtering and malware protection capabilities, the Barracuda Web Security Gateway allows administrators to generate more than 60 different reports on Internet activity.

Interactive reports with multiple layers of drill-down capability can be generated on users' web browsing activity, by domains and content categories, by time spent online, and/or by bandwidth consumption.

Suspicious Activity Alerts

The Barracuda Web Security Gateway includes pre-built English-language dictionaries of keywords and phrases pertaining to harassment, weapons, terrorism, and pornography. Administrators can configure the device to automatically generate alerts when content containing these keywords or phrases is posted to social media portals and search engines. Administrators can also add their own keywords and phrases for monitoring. The alerts are tagged with real network user identities, making it easy to identify the source, independent of online profiles.

Suspicious Activity Alerts

The Barracuda Web Security Gateway includes pre-built English-language dictionaries of keywords and phrases pertaining to harassment, weapons, terrorism, and pornography. Administrators can configure the device to automatically generate alerts when content containing these keywords or phrases is posted to social media portals and search engines. Administrators can also add their own keywords and phrases for monitoring. The alerts are tagged with real network user identities, making it easy to identify the source, independent of online profiles.

The Barracuda Safe Browser

The Barracuda Safe Browser is a full-featured mobile web browser that enforces compliance with the policies configured on the Barracuda Web Security Gateway. Barracuda Safe Browser is currently available for iOS-based devices.

Cloud-Based Centralised Management

Barracuda Web Security Gateways are integrated with the Barracuda Cloud Control (BCC) web-based management portal, which leverages Barracuda's global cloud infrastructure to enable organisations to centrally manage all their devices through a "single pane of glass" interface. Administrators can see a global view of all their devices as well as centrally manage policies and configuration. The intuitive interface makes it easy for small and medium-sized organisations to implement and manage their Barracuda Web Security Gateways with minimal IT overhead.

Easy-to-use Policy Configurations

The intuitive web interface allows for quick and easy configuration and administration of policy rules. Setup takes fifteen minutes or less. System information, logs, powerful policy features and reports are just a few clicks away. Reporting requires no database administration.

Advanced Threat Protection

Barracuda Advanced Threat Protection (ATP) implements full system emulation, providing deep visibility into malware behaviour. Files are checked against a dynamic cryptographic hash database, and any match is immediately blocked. If a match is not immediately found, or in case the file is unknown, it is delivered to our virtual sandbox for detonation where malicious behaviour can be safely discovered.

Barracuda ATP offers Administrators file-type-based control over attachment scanning policies and is used in conjunction with our updated virus scanning engines to maintain complete protection of an organisation? s network.

The Barracuda Advanced Threat Protection is an optional subscription available with WSG firmware 11.

Simple Pricing

The Barracuda Web Security Gateway is delivered with all features and capabilities fully enabled. Content filtering and advanced malware protection is offered as a simple all-inclusive subscription without any per-user fees. The Barracuda Cloud Control management portal is included free of charge.

Chromebook Security Extension

The new Barracuda Chromebook Security Extension is a Chrome browser extension that enables remote enforcement of web security policies. This is especially useful for K-12 environments. The extension works both on- and off-network, providing security for students, even when they take their Chromebook's home.