
Overview

<https://campus.barracuda.com/doc/6160470/>

The Barracuda Web Security Gateway is an integrated content filtering, application blocking and malware protection solution that is powerful, easy to use and affordable for businesses and educational institutions of all sizes. It enforces Internet usage policies on and off network by blocking access to websites and Internet applications that are not related to business or education, and it easily and completely eliminates spyware and other forms of malware from your organization. Unlimited remote user licenses are included to enforce content and access policies for mobile devices ([such as Chromebooks](#)) outside of the corporate network.

Where to Start

You can deploy the Barracuda Web Security Gateway inline with your core network components or you can deploy the system as a [forward proxy](#). Refer to [Deployment Options](#) for more information.

Device Deployment On-Premises

Supports all Barracuda Web Security Gateway features, and is the only solution that supports inline deployment. With inline deployment, you can filter web-based and non-web based application traffic (e.g. Facebook, Twitter, Skype, BitTorrent, etc.) as well as HTTP/HTTPS traffic.

- [Barracuda Web Security Gateway Quick Start Guide](#) – Download a copy of the Barracuda Web Security Gateway Quick Start Guide that was packed with your appliance.
- [Getting Started](#) – Detailed installation and configuration steps.
- [The 30 Day Evaluation Process](#) – A roadmap for your product evaluation (optional).
- [Managing Policies](#) – Best practices, precedence of block/accept policies, authentication schemes.
- [Integration with Barracuda Content Shield](#) – Optionally integrate the Barracuda Web Security Gateway with the Barracuda Content Shield (BCS) cloud web filtering service to create and manage web filtering policies in the cloud, using the easy-to-use BCS web interface.

Virtual Deployment

Supports only Forward Proxy deployment, which does not support filtering web-based or non-web based application traffic (e.g. Facebook, Twitter, Skype, BitTorrent, etc.); Forward Proxy configuration only supports filtering of HTTP/HTTPS traffic.

- [Barracuda Web Security Gateway Vx Virtual Deployment](#)
- [The 30 Day Evaluation Process](#) – A roadmap for your product evaluation (optional).
- [Managing Policies](#) – Best practices, precedence of block/accept policies, authentication schemes.

Key Features

- Regulates web application activity, including Google Workspace
- Granular, user-aware policies
- Monitor and archive social-network messages (Barracuda Message Archiver required for archival of alert messages)
- Advanced Threat Protection (ATP) service to analyze web traffic for viruses in a secured cloud environment. Subscription-based service detects and blocks advanced malware, zero-day exploits, and targeted attacks.
- Content filtering, with HTTP/HTTPS support and URL filtering by category for various types of users and groups. Simplifies CIPA compliance for schools.
- Comprehensive network threat protection.
- Cloud based URL lookup utilizing Barracuda Network's Web Categorization Service (WCS), featuring dynamic page scanning and classification.
- SSL Inspection of HTTPS traffic with the model 410 and higher, running version 7.1.0 and higher. See [Using SSL Inspection With the Barracuda Web Security Gateway](#) for system requirements.
- LDAP integration, Single Sign-on user authentication – See [How to Choose Your Authentication Mechanisms](#).

Safe Browsing for Schools and Remote Users

- [Barracuda Web Security Gateway for Education](#) – A suite of features to regulate use of social media applications, provide alerts on cyberbullying and to provide safe browsing and content delivery for the classroom
- [Filtering Traffic for Offsite and Mobile Users](#) – A policy enforcement solution for BYOD, campus-issued laptops, Chromebooks and iOS devices

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.