Barracuda Web Security Gateway 30 Day Evaluation Guide

https://campus.barracuda.com/doc/23725595/

Where to start

Begin with the Getting Started guide to review deployment types and safely install and configure your Barracuda Web Security Gateway. If you have the Barracuda Web Security Gateway Vx virtual appliance, start with Virtual Deployment, then return to this page for hints and guidelines for your 30 day evaluation process. For hosted web security, see Barracuda Content Shield.

If you have a model 610 or higher, you automatically have a Barracuda Networks sales engineer assigned to help you make the most of your 30 day evaluation of the Barracuda Web Security Gateway. Simply call your reseller or sales representative if you have not yet been contacted by a sales engineer.

Evaluation Methodology

When evaluating the Barracuda Web Security Gateway, it is preferable to address two aspects separately:

- Functional testing
- Sizing for production environment: Size the Barracuda Web Security Gateway based on throughput, concurrent users and active TCP connections. Use the **BASIC > Dashboard** page to view and monitor these statistics.

It is recommended that you first evaluate device functionality on a sub-set of network traffic before deploying the Barracuda Web Security Gateway in a production environment. This will allow you to characterize your network better and familiarize yourself with the product before addressing production concerns.

Common Use Cases

Use Case: Reporting

1. If possible, deploy the Barracuda Web Security Gateway inline as described in Inline Pass-Through (Transparent) Mode Deployment. This deployment does not require setting a proxy in

client browsers. You can either set up the Barracuda Web Security Gateway inline with your computer for initial testing, or follow steps 3 and 4 to configure users and authentication for testing policies.

2. Set the Barracuda Web Security Gateway **Operating Mode** on the **BASIC > Administration** page to *Audit*. This mode logs traffic but doesn't warn or block users from accessing any URL. In *Audit* mode, for inline deployments, HTTP traffic is logged but not blocked, and downloads over HTTP are NOT scanned for viruses or spyware. Use this mode to preview how your currently configured Internet policies would be applied, but without disturbing production traffic. In Forward Proxy deployment, *Audit* mode works just like *Active* mode; traffic is logged and policies are applied.
3. Configure authentication as needed using your LDAP server, Kerberos or NTLM. See How to Choose Your Authentication Mechanisms for more information and to get started.
4. Create a set of Users and Groups if you want to assign block and allow policies to *Authenticated* users.
5. Use the filters on the **BLOCK/ACCEPT** pages to set policies for what you want to block, monitor, warn users about, or allow in web traffic for *Authenticated* or *Unauthenticated* users. See Best Practices in Configuring Policy for guidelines in setting up your traffic filtering policies.
6. After you have had the Barracuda Web Security Gateway running for a while, run reports on user activity, bandwidth usage, most visited domains, and other metrics from the **BASIC > Reports** page.
7. After reviewing reports, you'll have a good idea of what browsing activities or web 2.0 applications you want to warn, monitor, block or allow. Use the **BLOCK/ACCEPT** pages to adjust policies according to your organization's needs.
8. When you are ready to begin blocking specific web traffic, set the Barracuda Web Security Gateway Operating Mode on the **BASIC > Administration** page to *Active.*

Use Case: Social Media Regulation and Monitoring

The Barracuda Web Security Gateway 410 and higher enables granular control over Web 2.0 applications running over HTTPS. For example you can allow access to Facebook messages but block games, chat, posts etc. You can provide safe access to YouTube videos by simply enabling the **Safe Browsing** feature on the **BLOCK/ACCEPT > Content** filter page. Since most social media applications such as Facebook and Google Workspace typically run over HTTPS, you must configure the **SSL Inspection** feature on the Barracuda Web Security Gateway, which is available on the 310 (for Safe Search only), 410 (for granular control) and higher. Barracuda Networks recommends working with your sales engineer to configure SSL Inspection.

With the **Web Application Monitoring** feature and **SSL Inspection**, you can capture and archive the content of social media interactions.

1. For the Barracuda Web Security Gateway 410 and higher, enable SSL Inspection. See Using SSL Inspection With the Barracuda Web Security Gateway for details.
2. Follow steps 2-5 above.
3. See the **BLOCK/ACCEPT > Web App Monitor** page in the Barracuda Web Security Gateway web interface to configure. See How to Configure Web Application Monitoring for more

information and examples.

For schools, using SSL Inspection and Web Application Monitoring provides powerful benefits with common use cases such as these:

- Google Workspace Control Over HTTPS - Granular regulation of Google Workspace tools over HTTPS (Business Gmail as opposed to personal Gmail, and more)
- Facebook Control Over HTTPS - Granular regulation of Facebook applications (chat, posting, games, etc.)
- Alert authorities of emerging cases of cyberbullying, harassment, or loss of confidential data using the Suspicious and Sensitive Keyword Tracking feature. Monitor social messaging in real time, with keyword alert emails to teachers or administrators. This feature does *not* require the use of SSL Inspection unless you want to monitor HTTPS traffic content, and is available on the Barracuda Web Security Gateway 610 and higher.

With the Barracuda Web Security Gateway models 210 and 310, you can block or allow websites and subdomains as well as some applications, but you cannot capture the content of social media interactions as described above. To simply block or allow applications like Facebook Games, Flickr upload, LinkedIn Email and many more, see the **BLOCK/ACCEPT > Web App Control** page in the web interface.

Use Case: Remote Filtering for Students and Offsite Users

Remote Filtering with the Barracuda Web Security Gateway enables your IT department to provide and control content security beyond the perimeter of the IT infrastructure. To learn about options for managing and applying filtering policies to remote laptops, Chromebooks and other computers, see Filtering Traffic for Offsite and Mobile Users.

1. Begin by deploying the Barracuda Web Security Gateway in your network, selecting your authentication mechanism, and testing out policies as described above.
2. After you have configured and tested block and allow policies and authentication, you're ready to test extending this protection to your remote laptop or iPad, for example. If your use case is:
   - Chromebooks - Configure the Barracuda Chromebook Security Extension using your Google Workspace admin console.
   - Remote laptops, PC and Macintosh computers – Install the Barracuda Web Security Agent on one of these devices, which synchronizes them with the Barracuda Web Security Gateway policies. See Filtering Traffic for Offsite and Mobile Users and How to Install the Barracuda WSA with the Barracuda Web Security Gateway to get started.
   - Students with school issued iPads – Set up Global HTTP Proxy on iOS devices to direct traffic from the iOS device to the Barracuda Web Security Gateway.
3. Test your block and allow policies with one remote device before extending to all remote devices.

For use case examples specific to students, see:

- Facebook Control Over HTTPS
- Google Workspace Control Over HTTPS
- Barracuda Web Security Gateway for Education

Creating Exceptions to Policies

If you want to exempt certain users from block and allow policies, such as HR, Finance, Students, Teachers, etc.:

1. Create users and assign them to groups of users on the **USERS > Users and Groups** pages.
2. Set up your authentication mechanism as described above for users and groups.
3. Use the **BLOCK/ACCEPT** pages as described above to create policies.
4. Use the **BLOCK/ACCEPT > Exceptions** page to create exceptions to policies. See Exception Policies for more information and examples.

© 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.