

Filtering Traffic for Offsite and Mobile Users

<https://campus.barracuda.com/doc/6160468/>

Remote Filtering enables your organization to enforce content and access policies for mobile and desktop devices outside of the corporate network. For students, satellite offices, remote and mobile workers, the Remote Filtering feature allows secure web browsing access from laptops, Chromebooks, remote desktops, iPhones and iPads from any location. Web traffic from these devices is subject to the web access and security policies of the organization. This feature is available for use with the Barracuda Web Security Gateway model 410 and higher, and is also available with the [Barracuda Web Security Service](#) cloud solution.



Barracuda provides the following solutions for filtering remote traffic so you can choose how you protect your remote and mobile users online:

- **Laptops and desktops** – On each remote Windows desktop, laptop or Macintosh OS X computer, deploy the [Barracuda Web Security Agent](#) (WSA) to do one of the following:
 - Proxy all web traffic over the Internet through a specific Barracuda Web Security Gateway, which can monitor traffic and apply web security policies before routing that traffic to the internet. [SSL Inspection](#) is available for these deployments on the Barracuda Web Security Gateway 410 and higher running version 10 and higher.
 - Look up and apply company policies to client web traffic before routing it to the internet, without passing traffic through the Barracuda Web Security Gateway. For this option, see [Policy Lookup Only Mode With the Barracuda Web Security Agent](#).

When **Policy Lookup Only** mode is enabled, traffic is not routed through the Barracuda Web Security Gateway, so **SSL Inspection** cannot be applied to HTTPS traffic from remote computers. See also [Client-side SSL inspection with the Barracuda WSA](#).

- **Chromebooks**– The Barracuda Chromebook Security Extension can be installed on Chromebooks to enforce security policies provided by the Barracuda Web Security Gateway. The extension provides control and visibility over both HTTP and HTTPS traffic, and does not send any user generated traffic through the Barracuda Web Security Gateway, but instead, synchronizes policy and report data between the Chromebook and the Barracuda Web Security Gateway. You can configure Barracuda Chromebook Security Extension on the **ADVANCED > Remote Filtering** page. See [How to Get and Configure the Barracuda Chromebook Security](#)

[Extension.](#)

- **iOS Devices** - To protect the user's Internet traffic, configure Global HTTP Proxy on iOS devices. Enforcing Global HTTP proxy enables you to route and control internet bound traffic through Barracuda Web Security Gateway.

Figures

1. RemoteFiltering.png

© Barracuda Networks Inc., 2019 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.