

## Barracuda Web Security Service Architectures - Summary

<https://campus.barracuda.com/doc/6553669/>

### Customize Security Coverage to Any Environment

The Barracuda Web Security Service delivers state-of-the-art web security through various deployment options that you administer through one management portal. For corporate and branch office deployments, gateway web security appliances integrate with enterprise directory services such as Active Directory behind the firewall, enabling user and group-based policy control. A pure SaaS web security service provides web security for remote office and home-based users. Software agents extend security to mobile users' Windows and Mac laptops. Administrators can select any deployment option or any combination of deployment options to satisfy their exact web security needs.

### Direct to Service

The simplest way to use Barracuda Web Security Service is to directly proxy your web traffic to the cloud-based content filtering and malware protection service. This can be done with browser proxy settings or by transparently forwarding traffic from any network firewall or proxy that supports forwarding to an upstream proxy.

**Figure 1: Direct to Service.**



The Barracuda Web Security Service currently supports IPv4 (only) for web traffic filtering and reporting.

## Web Security Service Connector

The Barracuda Web Security Service Connector is an on-premises solution that integrates with your directory service for group-based policies, and caches static web content locally to save bandwidth. The Barracuda Web Security Service Connector can be configured either to provide local security and policy enforcement or forward traffic to the cloud-based web filtering service. These appliances are managed and configured through the cloud-based central management and reporting interface. The Barracuda Web Security Service Connector is available as a hardware appliance or as a virtual appliance. See [Using the Barracuda Web Security Service Connector](#) and [Barracuda Web Security Service Connector Deployment Configurations](#) for deployment details and options.

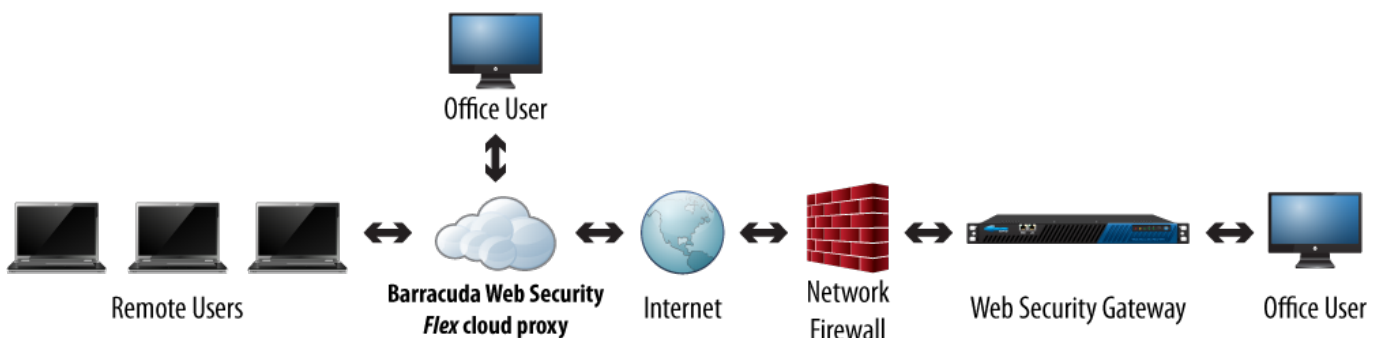
**Figure 2: With the Barracuda Web Security Service Connector appliance.**



## Barracuda Web Security Agent

The Barracuda Web Security Agent protects remote and roaming users by enforcing all web traffic from laptops through the cloud-based content filtering and malware protection service. The Barracuda Web Security Agent is a lightweight, tamper-proof client available for Microsoft Windows and Mac laptops and desktops.

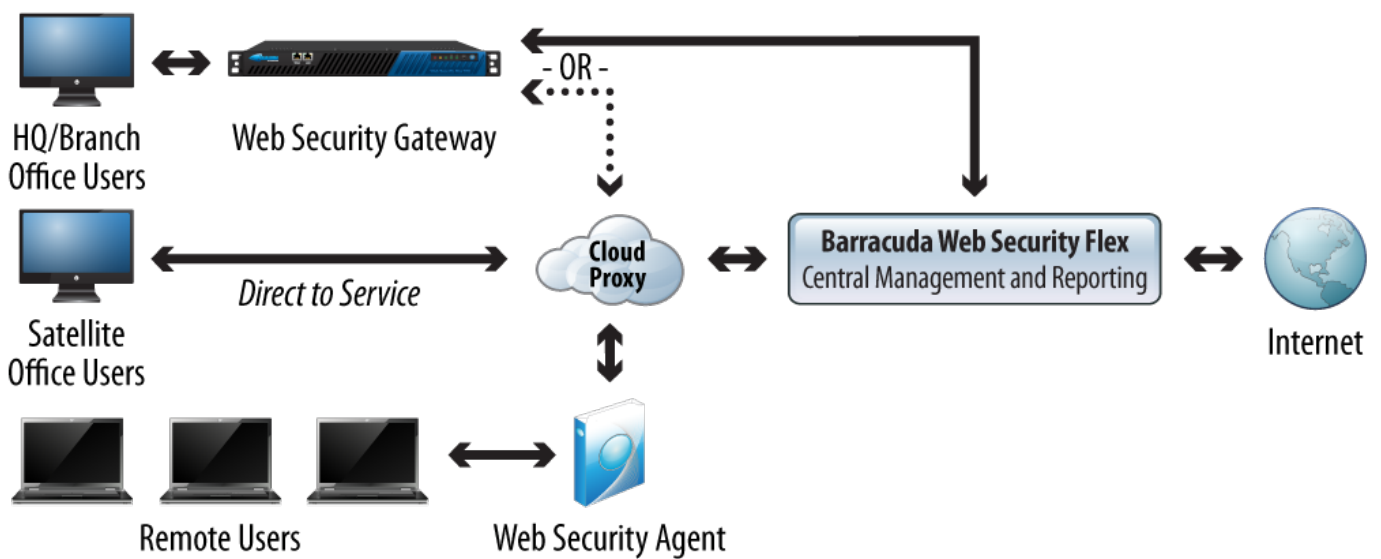
**Figure 3: Barracuda Web Security Agent installed on remote user's machines.**



## Flexible Deployment

The Barracuda Web Security Service allows the flexibility to combine deployment options to suit the specific need of each location. The cloud-based central management and reporting interface makes it easy to specify a uniform web usage policy and monitor web access across all the users.

**Figure 4: Flexible deployment options.**



## Figures

1. Flex Direct TO Service.PNG
2. Flex WSG.PNG
3. Flex WSG WSA.PNG
4. Flex Flexible Comprehensive.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.