Deployment Options

https://campus.barracuda.com/doc/6553654/

This documentation applies to the Barracuda Web Security Service sold **prior** to April 1, 2017. As of this date, the service is still maintained, while new customers can purchase the new Barracuda Web Security Service cloud based solution powered by Zscaler, the leading cloud web security solution for enterprises. Click here for documentation on the **new** Barracuda Web Security Service.

The Barracuda Web Security Service provides a unified framework which allows you to combine multiple deployment methods. Whichever combination of options you choose, management and reporting is centralized across all users and locations through the central management interface. This makes it simple to customize the solution to fit your exact requirements while providing the freedom to adapt and scale as your organization's needs change.

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

Choose from the three available deployment options or a combination thereof. For illustrations of these different options, see Barracuda Web Security Service Architectures - Summary.

- **Cloud Filtering - Software-as-a-Service (SaaS):** A complete cloud-based web security service providing malware scanning, content filtering and application control. Web traffic from client computers can be directly routed through the cloud service either through proxy settings or firewall rules. This is the simplest deployment option and provides an quick way to use cloud based web security without deploying any additional hardware or software. Administrators can specify global policies through the Barracuda Web Security Service Manager. For more information see Redirecting Traffic Using Proxy Options.

- **Barracuda Web Security Agent**: The Barracuda Web Security Agent (WSA) is a lightweight, tamper-proof client that can be installed on remote off-network computers. Once configured, the Barracuda WSA transparently redirects web traffic from the remote machine to the Barracuda Web Security Service cloud filtering service. The Barracuda WSA also enables user specific browsing policies by securely transmitting local login credentials to the service. The Barracuda WSA is an easy and reliable way to provide the same web security policies to off-network users as are provided to on-network users. The Barracuda WSA supports both Windows and Macintosh OSX devices with the Barracuda Web Security Service as follows:
  - Barracuda WSA for Macintosh UP TO version 2.x. Version 5.x and above does not support the service.
  - Barracuda WSA for Windows UP TO version 4.x. Version 5.x and above does not support the service.

For more information on how to use the Barracuda WSA, refer to Overview.

- **SaaS with Gateway appliances**: The Barracuda Web Security Service framework supports the (optional) use of on-premise gateways wherever required. Gateway appliances, called Barracuda Web Security Service Connectors, provide integration with on-network authentication services (LDAP/AD, NTLM, Kerberos, eDirectory) and local caching for bandwidth optimization. Additionally, these appliances can be configured to enforce security and web usage policies locally or proxy traffic to the cloud filtering service, after authentication, for malware scanning, content filtering and application control. In either case, gateway configuration, policy management and reporting is done through the cloud-based Barracuda Web Security Service Manager interface. This means that administrators can apply and centrally manage policies and generate reports for users filtered through gateway appliances or directly through the cloud filtering service. Since they provide transparent user authentication, Barracuda Web Security Service Connectors enable user or group-specific browsing policies using credentials configured in the corporate directory servers. For more information on using Gateway appliances, refer to Using the Barracuda Web Security Service Connector.