Using the Barracuda Web Security Service Connector

https://campus.barracuda.com/doc/6553601/

The Barracuda Web Security Service Connector can be deployed between your client browsers and the Barracuda Web Security Service to provide transparent and integrated user authentication, application blocking, and web caching. You can centrally manage settings and monitor each Barracuda Web Security Service Connector using the Barracuda Web Security Service Manager interface.For more details see Deployment Options and Barracuda Web Security Service Architectures - Summary.

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

You can deploy a Barracuda Web Security Service Connector in two modes:

- **Service Enforcement Mode** (default mode): proxies all web traffic to the Barracuda Web Security Service (the cloud) for enforcement, or
- **Local Enforcement Mode**: enforce policies locally, only passing reporting information to the Barracuda Web Security Service (the cloud)

Note: If your Barracuda Web Security Service Connector is deployed in Local Enforcement Mode, it still sends logging information to the Barracuda Web Security Service for reporting purposes. See Enforcement Mode to switch modes.

The Barracuda Web Security Service Connector can be deployed in an inline or forward proxy deployment configuration. Both configurations support either enforcement mode. For more information on deployment configurations, refer to Barracuda Web Security Service Connector Deployment Configurations.

In **Local Enforcement Mode**, the Barracuda Web Security Service Connector performs caching, authentication, content filtering, and application blocking locally. Logging information is sent to the Barracuda Web Security Service Manager. You can centrally manage Barracuda Web Security Service Connectors in Local Enforcement Mode from the Barracuda Web Security Service Manager interface.

Service Enforcement Mode is the default mode for the Barracuda Web Security Service Connector. In Service Enforcement Mode, the Barracuda Web Security Service Connector can attach authenticated client information to traffic before proxying it to the Barracuda Web Security Service for policy enforcement. The Barracuda Web Security Service applies user specific policies which you can define on the Rules tab in the Barracuda Web Security Service Manager interface, including content filtering and application blocking, and allows approved web requests to pass through after removing the user information. You can centrally manage Barracuda Web Security Service Connectors from the

Barracuda Web Security Service Manager interface.

Connect to the Barracuda Web Security Service Manager

Use the **System Configuration** utility on the Barracuda Web Security Service Connector interface to connect to the Barracuda Web Security Service Manager. Once connected to the Barracuda Web Security Service, manage Barracuda Web Security Service Connector settings by selecting the Gateway name on the **CONFIGURATION > Gateway** page.

Centralized Management of Barracuda Web Security Service Connectors

The Barracuda Web Security Service Connector automatically receives updated Security Policies when changes are made. The configuration settings you specify in the Barracuda Web Security Service Manager sync with the Barracuda Web Security Service Connector when you accept the prompt to sync your changes or when the Barracuda Web Security Service Connector syncs with the Barracuda Web Security Service Manager when: the Barracuda Web Security Service Connector is first detected by the Barracuda Web Security Service Manager; you restart or reload the Barracuda Web Security Service Connector on the System tab for the selected Barracuda Web Security Service Connector; you make configuration changes and then press the **Sync** button when prompted.

These settings include:

- IP Configuration
- Authentication
- SNMP
- Proxy/Caching
- System (settings for the Barracuda Web Security Service Connector)