Barracuda Content Shield Integration With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/91131409/

You can optionally integrate the Barracuda Web Security Gateway with the Barracuda Content Shield (BCS) cloud web filtering service to create and manage web filtering policies in the cloud, using the easy-to-use BCS web interface. Simply proxy all of your client web traffic to the Barracuda Web Security Gateway, or connect clients inline with it, and then enable the BCS integration on the Barracuda Web Security Gateway. The BCS web interface then provides views of web traffic statistics, configuration of web filtering policies, exceptions, and reporting.

- Policies can be quickly configured by categories, super categories, urls and / or specific domains
- Traffic statistics, web logs and reporting are provided in the BCS web interface
- LDAP, NTLM and Kerberos user authentication methods are still configured on the Barracuda Web Security Gateway

When you enable the BCS integration with the Barracuda Web Security Gateway, some tabs or pages no longer appear in the web interface, as some of the functions they provide will be available in BCS.

For this integration, you must configure your LDAP in your Barracuda Cloud Control (BCC) account, even if you are using NTLM or Kerberos on the Barracuda Web Security Gateway. This provides BCS with access to your users and groups information.

Prerequisites for Integration with Barracuda Content Shield

- Be existing Barracuda Web Security Gateway customer with valid subscriptions
- Must initiate a Barracuda Content Shield trial account, or have an existing account
- Must uninstall any Barracuda Web Security Agents on remote devices, and install the Barracuda Content Shield suite on those machines.
- Must not be using Network / IP based policies on the Barracuda Web Security Gateway
- Must not be using Application or Web Application policies on the Barracuda Web Security Gateway
- If you are using Barracuda Cloud Control with your Barracuda Web Security Gateway, go to the **ADVANCED > Cloud Control** page. Set **Connect to Barracuda Cloud Control** to *No*.
- If you have clustered your Barracuda Web Security Gateways, you must disable the cluster by deleting all settings on the **ADVANCED > Linked Management** page.
- If you are using Barracuda Reporting Server, go to the **BASIC > Administration** page and set **Connect to Barracuda Reporting Server** to *No*.

To integrate with Barracuda Content Shield:

1. Log into your BCS plus account. On the **Downloads** page, download and save the Account Configuration (**bcs.key**) file onto your system.
2. Log into the Barracuda Web Security Gateway as *admin*.
3. Go to the **ADVANCED > Configuration** page. In the **Barracuda Content Shield** section, click **Browse**. Select the file **bcs.key** that you downloaded in step 1.
4. After opening the **bcs.key** file, click **Upload Now**.   The **ADVANCED > Configuration** page then reloads and displays a new feature titled **Enable BCS Connector**.
5. Clic*k Yes* to enable this feature. Click **Save**.
6. The Barracuda Web Security Gateway will reboot and display the Barracuda Web Security Gateway login screen. Log in as *admin*.
   After the Barracuda Web Security Gateway reboots, note that the **Dashboard** page is greatly reduced, and many of the tabs and pages are no longer present in the web interface.
7. Proxy all of your client web traffic to the Barracuda Web Security Gateway IP address, or place them inline with the Barracuda Web Security Gateway.
8. To configure your authentication mechanism, go to the **USERS/GROUPS > Authentication** page. LDAP, NTLM and Kerberos are supported with BCS integration. As noted above: You must configure your LDAP in your Barracuda Cloud Control (BCC) account, even if you are using NTLM or Kerberos on the Barracuda Web Security Gateway. This provides BCS with access to your users and groups information.
9. If you are using LDAP, you can configure the Barracuda DC Agent as usual.

For Endpoint Machines off Network

If you are filtering traffic for endpoints *outside* the network, you need to also install the Barracuda Content Shield Suite on those endpoints. If you have installed the Barracuda Web Security Agent (WSA) on those machines in the past, you must uninstall the Barracuda WSA and then install the Barracuda Content Shield Suite in order to filter traffic for those machines. See Barracuda Content Shield Suite for Endpoints.

Web Logs and the Barracuda Web Security Gateway

While BCS integration is enabled on the Barracuda Web Security Gateway, look for the web logs on the **WEB FILTERING LOGS** page in the BCS web interface.

Configuring Policies in BCS

Now you can configure policies for all Barracuda Web Security Gateway users using the **ADVANCED FILTERING** page in BCS. The Barracuda Web Security Gateway now appears in BCS like any other endpoint. See Using Barracuda Content Shield With the Barracuda Web Security Gateway for illustrations.