Using Barracuda Content Shield With the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/91132503/

If you are using the Barracuda Web Security Gateway, you can optionally integrate it with the Barracuda Content Shield cloud web filtering service to configure web filtering policies in the cloud with 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. You can then use the BCS web interface to view web traffic statistics, configure web filtering policies and exceptions, and run reports for the Barracuda Web Security Gateway just as you would for any other endpoint.

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

Prerequisites for Integrating Barracuda Content Shield with the Barracuda Web Security Gateway

There are some important prerequisites to be aware of and plan for before you integrate Barracuda Content Shield with your Barracuda Web Security Gateway(s). See the list in Barracuda Content Shield Integration With the Barracuda Web Security Gateway.
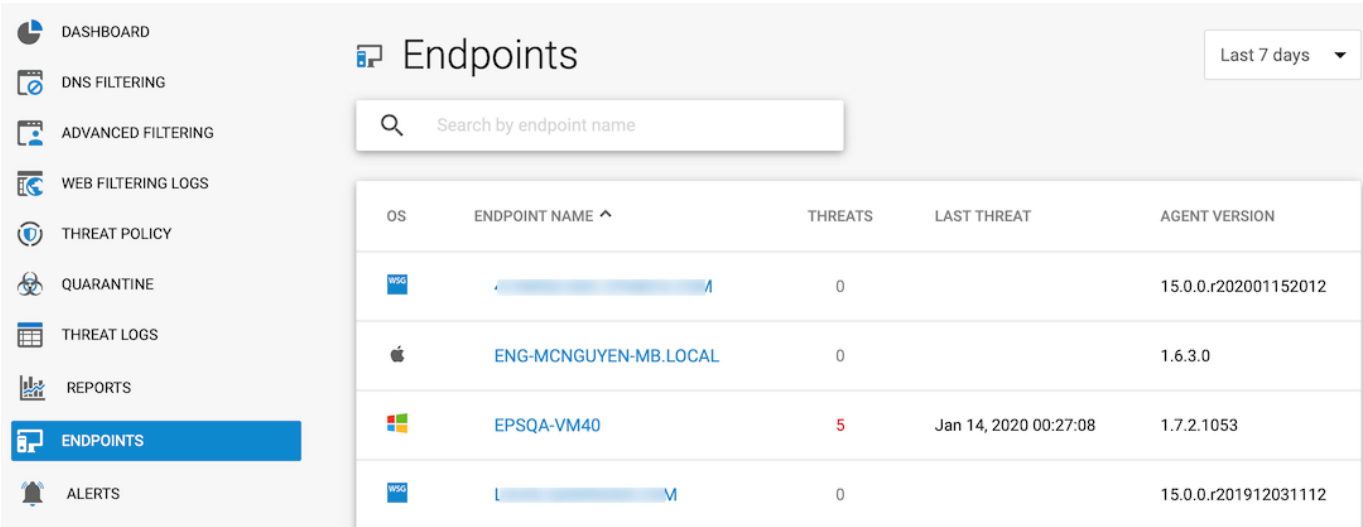
To Integrate Barracuda Content Shield With the Barracuda Web Security Gateway:

1. Log into your BCS plus account. On the **Downloads** page, download and save the Account Configuration (BCS key) file on your system.
2. Continue with instructions in Barracuda Content Shield Integration With the Barracuda Web Security Gateway.
3. 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 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.

After the integration, you will see the **WSG** icon and firmware ('Agent') version of the Barracuda Web Security Gateway in the table on the **ENDPOINTS** page in the BCS web interface as shown in Figure 1. The **Endpoint Name** in the table will show the domain name from the **Domain Configuration** section of the Barracuda Web Security Gateway web interface. You can now configure policies for all

Barracuda Web Security Gateway users using the DNS Filtering and Advanced Filtering tools in BCS.
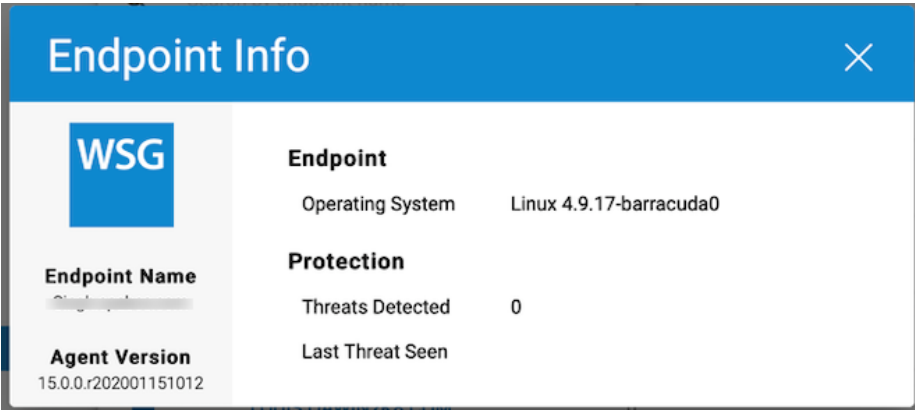
Figure 1. List of endpoints, including 2 Barracuda Web Security Gateways.

If you click on an entry for a Barracuda Web Security Gateway, you'll see the popup as shown in Figure 2 with the firmware ('Agent') version and threat details.

Figure 2. Details about the Barracuda Web Security Gateway as an endpoint.

Web Logs and the Barracuda Web Security Gateway

While the Barracuda Web Security Gateway is integrated with Barracuda Content Shield, look for the web logs on the **WEB FILTERING LOGS** page in the BCS web interface.

Figures

1. EndpointsBCSConnect.png
2. EndpointWSGDetails.png