Managing Content Filtering Services

https://campus.barracuda.com/doc/6553658/

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 various Content Filtering Services which you can configure and enable using the **CONFIGURATION > Content Filtering Services** page, including:

- Safe Browsing
- URL Blocking

You can also configure the Failure Response of the following **Content Filtering Services** to **Fail Open** or to **Fail Closed** if the service becomes unavailable:

- Anti-Virus Protection
- Malware Protection
- URL Filtering

Configure URL Blocking Global Settings

The Barracuda Web Security Service provides global settings governing URL Blocking which you can configure on the **CONFIGURATION > Content Filtering Services > URL Blocking page**. On a per rule basis, you can override the global block page setting by creating custom blocking messages; but if you do not configure custom block messages for a rule, these global settings will apply to any access blocked by that rule.

- **Block Page Selection**: You can choose between displaying: a **Default Global Block Page** for all users who attempt access of blocked content, which contains the default blocking message indicating the category of the blocked content; or a **Custom Global Block Page** with a custom message you compose.**Save Blocking Changes** after changing your selection.
- **Change Global Bypass Password**: Enter a password which you can provide to users who need to bypass block pages. After entering the bypass password, a user is allowed access to otherwise blocked content.**Save Password Changes** after setting the password.
- **Change Default Bypass Timeout (min)**: Enter the time in minutes, after which a bypass block page expires. **Change Default Coaching Timeout (min)**: Enter the time in minutes, after which a coaching block page expires. **Save Timeout Changes** after setting new timeouts.

Configure Failure Response for Services

You can configure how the Barracuda Web Security Service responds to a filtering service being unavailable using the following **CONFIGURATION > Content Filtering Services** Configure pages:

- **URL Configure**: Select **Fail Open** (Recommended) to allow all traffic, or **Fail Closed** to block all traffic if URL Filtering is not possible.
- **Virus Configure**: Select **Fail Open** (Recommended) to allow all traffic, or **Fail Closed** to block all traffic if Virus checking is not possible.
- **Malware Configure**:Select **Fail Open** (Recommended) to allow all traffic, or **Fail Closed** to block all traffic if Malware checking is not possible.