Security Policies

https://campus.barracuda.com/doc/98223637/

Configure security policies to filter network and device traffic in order to protect your organization from phishing, malware, and illicit web activity. Security policies always work top down, and explicit policies take precedence over predefined security policies. The default action of a security policy can be either to block all and define exceptions that are allowed, or to allow all and define exceptions that are blocked. You can change the default action for all polices individually.
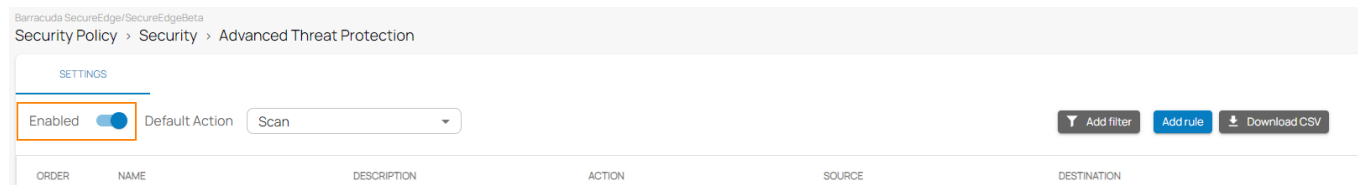
The following security policies are currently available:

- **Advanced Threat Protection** – For more information on Malware Protection, see Advanced Threat Protection.
- **SSL Inspection** – For more information on SSL Inspection, see SSL Inspection.
- **IPS** – For more information on IPS, see IPS.

Enable / Disable Security Features

Certain security features can be enabled or disabled with a switch; other features like web filtering can only be enabled/disabled by specifying the default action.

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control account.
2. Go to **Security Policy**.
3. Expand the **Security** menu on the left and select the security feature you are interested in. The policy settings window opens.
4. Use the switch in the upper-left corner to enable or disable the feature.

Figures

1. enable_sec_90.png