Security Policies

https://campus.barracuda.com/doc/93194243/

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 security polices individually. For example, URL Filtering is set to allow all and to block only defined exceptions, whereas ACL is set to block all and to allow only defined exceptions.
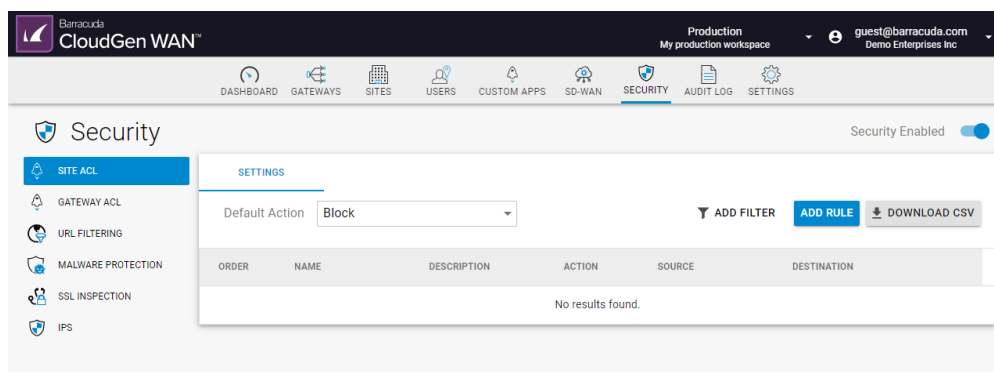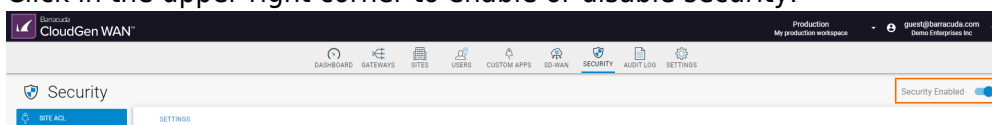

The following security policies are currently available:

- Site ACL
- Gateway ACL
- URL Filtering
- Malware Protection
- SSL Inspection
- IPS

Enable / Disable Security Policies

1. Open https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY**.
3. Click in the upper-right corner to enable or disable security.

Enable / Disable Security Features

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

1. Open https://cloudgenwan.barracudanetworks.com/ and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY**.
3. Click on the security feature you are interested in.
4. Click to enable/disable, if applicable.
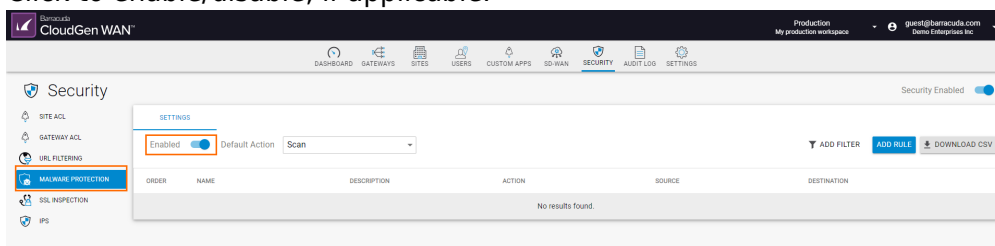
Further Information

- For more information on Site ACL, see Site ACL.
- For more information on Gateway ACL, see Gateway ACL.
- For more information on URL Filtering, see URL Filtering.
- For more information on Malware Protection, see Malware Protection.
- For more information on SSL Inspection, see SSL Inspection.
- For more information on IPS, see IPS.

Figures

1. security_82.png
2. enable_disable_sec_82.png
3. enable_disable_mp_82.png