Assigning a Security Policy to a Cloud Connection

https://campus.barracuda.com/doc/93196232/

This article describes how to assign a security policy to a cloud connection within Barracuda Cloud Security Guardian. For background on the various types of policies, refer to Understanding Security and Compliance Policies.

After you have created specific security policies in Barracuda Cloud Security Guardian (see Creating a Security Policy), you can assign them to one or more cloud connections. Scanning activities for that cloud connection will then use that policy for its security and compliance.

The procedures described in this article are the same for any of the various types of policies.

> Note that the Default Policy that is already included with Barracuda Cloud Security Guardian includes CIS, NIST, HIPAA, and PCI DSS policies.

To assign a security policy to a cloud connection:

1. Navigate to **Security Policies**.
2. In the **Cloud Connections** section, locate the desired cloud connection. Click **Edit**.
3. The **Cloud Connection Policy** window appears.
4. Click in the **Security Policy** field and select one of the available choices, including the Default Policy and other policies you created. Click **Save Changes**.
5. The policy you chose displays for that cloud connection in the **Cloud Connections** table.