How to Configure the Intrusion Prevention System (IPS)

https://campus.barracuda.com/doc/73719234/

IPS policies define how the IPS engine scans traffic. You can create default and custom IPS policies to apply to your access rules. IPS can automatically receive the latest intrusion prevention and security updates from Barracuda Central, an advanced 24/7 security operations center that works to continuously monitor and block emerging Internet threats. Exploit signatures are regularly updated at Barracuda Central and are automatically delivered to your system via Energize Updates. If your system is managed by a Barracuda Firewall Control Center, the IPS pattern updates are done by the Control Center. As soon as the Control Center receives IPS pattern updates, these patterns are delivered to all attached Barracuda CloudGen Firewalls.

Enabling IPS can decrease the overall throughput of your system. By default, all access rules use the default IPS policy. For specific access rules, you can disable IPS.

Before You Begin

To use IPS, make sure that you have a valid Energize Updates subscription.

Enable IPS

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **IPS Policies**.
2. Click **Lock**.
3. Select the **Enable IPS** check box.
4. If you want malicious traffic to be reported without being dropped, select the **Report only** check box.
5. Click **Send Changes** and **Activate**.

View and Edit IPS Signature Policies

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **IPS Policies**.
2. Click **Lock**.
3. In the **Default Policy** section, click **Edit explicit actions** to view the list of IPS signatures and how they are handled.

4. To view the details for an IPS signature, double click it.
5. To edit the settings for an IPS signature, right click it and choose **Edit Selected**.
6. In the **Change Action for Explicit Signatures** window, define how the IPS signature is handled and reported. To use the default IPS policy, select the **Reset to default action** check box.
7. Click **OK** and exit the list.
8. Click **Send Changes** and **Activate**.

Create New IPS Policies

Create new IPS policies to be applied to your access rules.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **IPS Policies**.
2. Click **Lock**.
3. In the **Custom Policies** table, click **+** to add a new entry for your policy.
4. Select an ID for your policy and click **OK**.
5. Enter a **Name** and **Description** for the policy.
6. If you want to apply your settings to the default IPS policy, click **Copy to Default Policy**.
7. Click **Send Changes** and **Activate**.

Create IPS Exceptions

If you want to exempt specific IPS signatures from the default or custom IPS policies, create IPS exceptions.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **IPS Exception Database**.
2. Click **Lock**.
3. Click the **+** icon.
4. In the **Select IPS Signatures** window, select the required IPS signatures and click **Add**. To remove a signature, select it and click **Remove**.
5. Click **OK**. Your override is listed in the table on the **IPS Exception Database** page.
6. Click **Send Changes** and **Activate**.

Apply an IPS Policy to an Access Rule

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **Forwarding Rules**.

2. Click **Lock**.
3. Edit the access rule you wish to apply the policy to.
4. Under **Policy**, select the policy from the **IPS Policy** list. If you want to disable IPS for the rule, select **No Scan**.

Managing IPS on a Firewall Control Center

On the Control Center, IPS pattern version information is displayed in the lower section of the **File Updates** page while successful or failed IPS pattern updates for attached firewalls are listed in the upper section.

Adjusting global file update settings may be necessary if your Control Center uses a system HTTP Proxy for Internet access. If the Control Center is not able to download the IPS patterns, increase the **Log Level** for troubleshooting information.

1. Go to the **CONTROL** tab and click **File Updates** in the ribbon bar.
2. Click the **Set Area Config** button.
3. In the **Time Settings** section, set the **Download Interval** (default: **60**)
4. In the **Proxy Settings** section, specify the settings for the proxy server.
5. Click **OK**.

If a managed Firewall is reinstalled, the IPS pattern database must be updated after the installation process because the database is not stored within the PAR file.