Intrusion Prevention System or IPS

https://campus.barracuda.com/doc/28475411/

To report and instantly block suspicious network traffic from passing the Barracuda NextGen Firewall X-Series, the Intrusion Prevention System (IPS) actively scans forwarded network traffic for malicious activities and known attack patterns. The IPS engine analyzes network traffic and continuously compares the bitstream with its internal signature database for known attack patterns. To increase security, the IPS system offers TCP stream reassembly to prevent IP datagram fragmentation before packets are scanned for vulnerabilities. The IPS engine can also inspect HTML requests passing the firewall.

IPS must be globally enabled on an X-Series Firewall. However, you can enable or disable IPS for each firewall rule. Enabling IPS on a per-rule basis lets you select which network traffic is scanned for threats. For example, you can choose to enable IPS scanning only for network traffic that travels from and to the DMZ. When IPS is enabled in a firewall rule, the default IPS policy of Report Mode or Enforce Mode is used. In Report Mode, the X-Series Firewall reports detected attacks instead of immediately blocking network traffic. This mode is recommended after the initial deployment of IPS to prevent traffic from being incorrectly blocked. However, you can prevent false positives when the IPS engine operates in Enforce Mode by creating IPS exceptions.

Enable and Configure IPS

To enable and configure IPS, complete the following steps:

Step 1. Enable IPS

1. Go to the **FIREWALL > Intrusion Prevention** page.
2. In the **Intrusion Prevention** section, set **Enable Intrusion Prevention System** to **Yes**.
3. (Optional) If required, you can choose to enable **TCP Stream Reassembly** and/or **HTML Inspection**.
   These options can decrease the performance of the X-Series Firewall.
4. For **Default IPS Policy**, select either **Report Mode** or **Enforce Mode**.
5. Click **Save**.

Step 2. Adjust the Event Policy

In the **Event Policy** section of the **FIREWALL > Intrusion Prevention** page, define the actions to be taken when the IPS engine detects suspicious network traffic with the following threat levels: **Critical**, **High**, **Medium**, **Low**, and **Information**. When the X-Series Firewall operates in **Report Mode**, you can only adjust the **Log** settings. When the firewall operates in **Enforce Mode**, you can also modify the **Action** for each severity.

Available **Action** settings include:

- **Drop** – Blocks network traffic where malicious activities were detected.
- **Log Only** – Reports network traffic where malicious activities were detected.
- **None** – No action is taken.

Available **Log** settings include:

- **Alert**
- **Warn**
- **Notice**

You can view detected threats on the **BASIC > Recent Threats** page.

Step 3. Configure IPS in Firewall Rules

To configure IPS in a firewall rule:

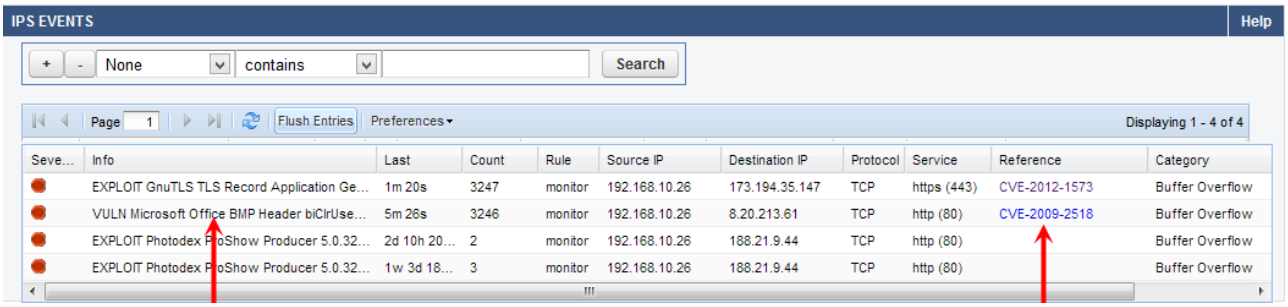
1. Go to the **FIREWALL > Firewall Rules** page.
2. Open an existing rule or create a new one.
3. In the **Add/Edit Access Rule** window, click the **Advanced** tab.
4. Next to **Intrusion Prevention**, select an option to disable or enable IPS:
   - **Default** (Report Mode or Enforce Mode) – Applies the default IPS policy to the rule.
   - **Disabled** – Disables IPS scanning for the rule.
5. Click **Save**.

Configure IPS Exceptions

If you must allow network traffic that the X-Series Firewall has detected as a threat, you can create an IPS exception.

Before you create the IPS exception, get the description or CVE-ID of the threat:

1. Go to the **BASIC > Recent Threats** page.
2. Browse through the list of detected threats or apply filters to locate specific entries.
3. Get the attack description text in the **Info** column, or, if available, the CVE-ID of the detected threat.



To create the IPS exception:

1. Go to the **ADVANCED > IPS Exceptions** page.
2. Click **Add IPS Exception**.
3. In the **IPS Exceptions** window, specify the traffic to be handled and the action to be performed by the exception.
4. Click **Save**.

Figures