

## How to Configure IPS Policies

<https://campus.barracuda.com/doc/41116020/>

IPS policies control the behavior of the IPS when an attack is detected. You can define multiple IPS policies and apply them to individual firewall rules as needed.

### In this article:

## Default IPS Policy

By default all firewall rules use the default IPS policy. All traffic is scanned according to this policy while the IPS is enabled. To turn off IPS scanning for an individual firewall rule, choose **No Scan Policy** from the **IPS Policy** dropdown. This makes sense for connections for which you want to avoid being blocked in case of a IPS misconfiguration.

### Custom Policy Section

Within the **Custom Policy** section it is possible to create and manage user created IPS policies. Each of the created policies can be individually applied to firewall rules. The configuration interface for IPS policies is identical for the default policy and custom policies.

## Policy Configuration

1. Open the **IPS Policies** page (**Config > Full Config > Virtual Servers > your virtual server > Assigned Services > Firewall**).
2. Click **Lock**.
3. Select **Enable IPS**.
4. If you want malicious traffic to be dropped, disable the **Report only** check box.  

Barracuda Network recommends to use **Report only** mode and to monitor the log files for false positives for an initial deployment phase and then disable **Report only** mode later.
5. Select **Scan SSL-Intercepted Traffic** if decrypted SSL traffic should be scanned. Only available with enabled [Application Control 2.0 with SSL Interception](#).
6. Configure the settings described in the following sections:

Enable IPS  Report only [Download Options for IPS Signatures](#)

**Default Policy**  
[Clone Default Policy](#)

Name: Default  
 Description: Default Policy

Scan:  ON  OFF

	Critical	High	Medium	Low	Informational
from Client	Drop  Alert	Drop  Warn	Log  Alert	Log  Warn	Log  Warn
from Server	Drop  Alert	Drop  Warn	Log  Alert	Log  Warn	Log  Warn

Scan only for explicit signatures [Edit explicit actions \(0\)](#)

---

**Custom Policies**

ID	Scan	Name
1	OFF	No Scan Policy

**No Scan** [Copy to Default Policy](#)

Name: No Scan Policy  
 Description: This is a system policy. Used to not scan for IPS Signatures. This Policy is read only.

Scan:  ON  OFF

	Critical	High	Medium	Low	Informational
from Client	None	None	None	None	None
from Server	None	None	None	None	None

Scan only for explicit signatures [Show explicit actions \(0\)](#)

**From Client/From Server** - Allows different actions for data streams of a session. Streams initiated from the host are classified as *From Client*, while answers from the target host are classified as *From Server*.

It may be necessary for system administrators to configure different IPS policy settings for the traffic source and destination.

- **Action** - Describes the protection behavior of the IPS engine in case of detection of malicious traffic:
- **Drop** - Drops malicious network traffic.
- **Log** - Only informs about malicious network traffic according to the defined Notification.
- **None** - Malicious network traffic will be neither reported nor dropped.

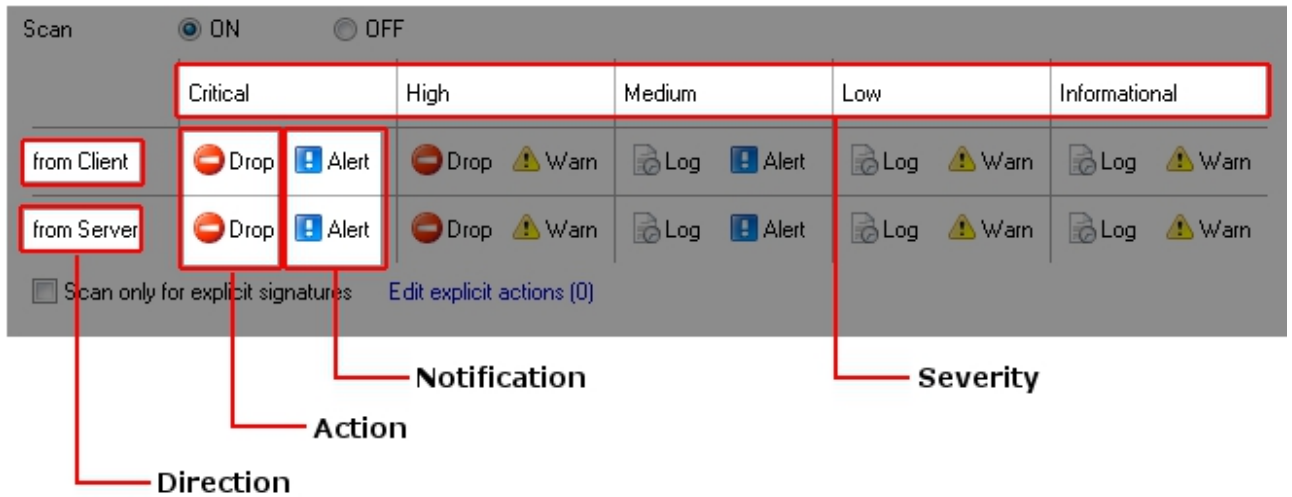
**Notification** - Describes the warning behavior (Eventing) of the IPS engine in case of detection of malicious traffic:

- **Alert** - An Alert Event will be generated.
- **Warn** - A Warning Event will be generated.
- **Notice** - A Notice Event will be generated.

**Severity** - Detected malicious network traffic is classified by the IPS engine into the following severities:

- **Critical**
- **High**
- **Medium**
- **Low**
- **Informational**

### IPS Policy Management



### Custom Policies

- Click **Add** to create an IPS Policy with custom settings.
- Click **Delete** to remove the selected IPS Policy.
- Click **Clone** to copy the selected IPS Policy.

**Copy to Default Policy** - Changes the currently selected policy to the default policy.

**Explicit Signatures** - For each IPS Policy, a set of custom signature actions can be defined and IPS scanning can be limited to this user defined set.

**Scan only for explicit signatures** - If enabled, the IPS scanning will only be performed for IPS signatures that have been edited via the explicit action link.

**Edit explicit actions** - Click this link to modify the action of a IPS signature.

### IPS Signatures - Explicit Actions:



- **Edit** - Select the desired IPS signature and click **Edit Selected** to modify the according action. Click **Edit All** to change actions for all currently signatures displayed.
- **Severity Filter** - Select the desired severity to filter for.
- **Policy Filter** - Select the desired policy type:
  - **All** - Display all available IPS signatures.

- **Overwritten** - Display only IPS signatures with custom actions.
  - **Default only** - Display only IPS signatures with default actions.
7. Click **Send Changes** and **Activate**.

### **Assign IPS Policy to Firewall Rules**

---

As soon as a custom IPS Policy is configured, it is selectable within a firewall rule. Open a firewall rule and select the desired IPS Policy. Now traffic that is handled by this firewall rule will be scanned according to the selected policy.

## Figures

1. ips\_policy.png
2. ips\_conf.png
3. ips\_conf2.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.