# Configure IPS Sensors on FortiGate

By Elias Georgiou – System Consultant

## What is IPS?

IPS stands for Intrusion Prevention Systems which are network security/threat mechanisms that perform inline scanning to all network traffic in order to detect and ultimately prevent vulnerability exploits or attacks. Such exploits that come in the form of malicious inputs have as a goal to gain control or interrupt applications or machines.

Intrusion Prevention Systems continuously monitor the network looking to identify possible malicious activities, record information about them, report any detected threats to network administrators and take preventative measures to block a threat from causing any harm. Such preventative measures could be closing access points or configuring firewalls to block any future attacks as well. Intrusion Prevention Systems can also be used to identify issues with company security policies discouraging employees or network guest from violating these policies again.

Nowadays network attackers are becoming more and more sophisticated and can penetrate even the most robust security solutions so IPS have become a key component of all major infrastructures in modern organizations.

## How do Intrusion Prevention Systems work?

Intrusion Prevention Systems work by actively scanning all network traffic for known attack patterns or malicious activities which include Denial of Service (DOS) attack, Distributed Denial of Service (DDOS) attack, different types of exploits or viruses. To achieve this Intrusion Prevention Systems are typically placed behind a Firewall, acting as an additional security layer that performs real time packet inspection. Upon detecting any malicious or suspicious packets the below actions will take place:

- Termination of the TCP session that was found to be exploited and proceed with blocking source IP address or user from accessing any hosts or network resources.
- Reconfigure Firewall to block all similar attacks.
- Remove all malicious content within the network by repackaging payloads, removing header information and malicious attachments.

### Types of Intrusion Prevention Systems

Most of the Intrusion Prevention Systems use one of the three methods - Signature based, Statistical Anomaly based or Stateful Protocol analysis detections.

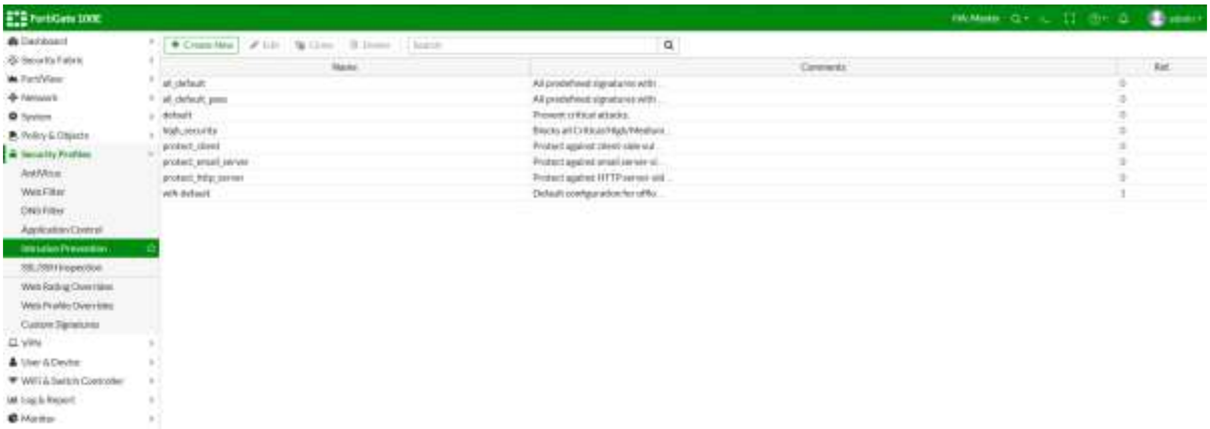
- **Signature based detection:** this approach uses a set of predefined signatures for well-known threats, if an attack is initiated that matches any of these signatures the system will take the necessary action.
- **Statistical Anomaly based detection:** in which the Intrusion Prevention System will scan the network for any unexpected behavioural patterns. If any anomaly is found the system will block access to the affected host.
- **Stateful Protocol detection:** this method requires administrators to create a set of security policies that will apply to the network. If any activity breaks any of these policies an alert is triggered.

### Configure IPS Sensors on FortiGate

Fortinet delivers IPS technology via the industry validated and recognized FortiGate platform. FortiGate security processors provide unparalleled high performance, while FortiGuard Labs informs industry leading threat intelligence, creating an IPS with proven success in protecting from known and zero-day threats. As a key component of the Fortinet Security Fabric, FortiGate IPS secures the entire end-to-end infrastructure without compromising performance.

### To create a new IPS sensor

1. Go to **Security Profiles > Intrusion Protection**.



| Name | Comments | Ref. |
|---|---|---|
| all_default | All predefined signatures with ... | 0 |
| all_default_pass | All predefined signatures with ... | 0 |
| default | Prevent critical attacks. | 0 |
| high_security | Blocks all Critical/High/Medium ... | 0 |
| protect_client | Protect against client-side vul ... | 0 |
| protect_email_server | Protect against email server vul ... | 0 |
| protect_http_server | Protect against HTTP server-sid ... | 0 |
| wifi-default | Default configuration for offlo ... | 1 |

*Figure 1: depending on the FortiGate model there are many predefined IPS sensors as well*

2. Select the **Create New** icon in the top of the Edit IPS Sensor window.

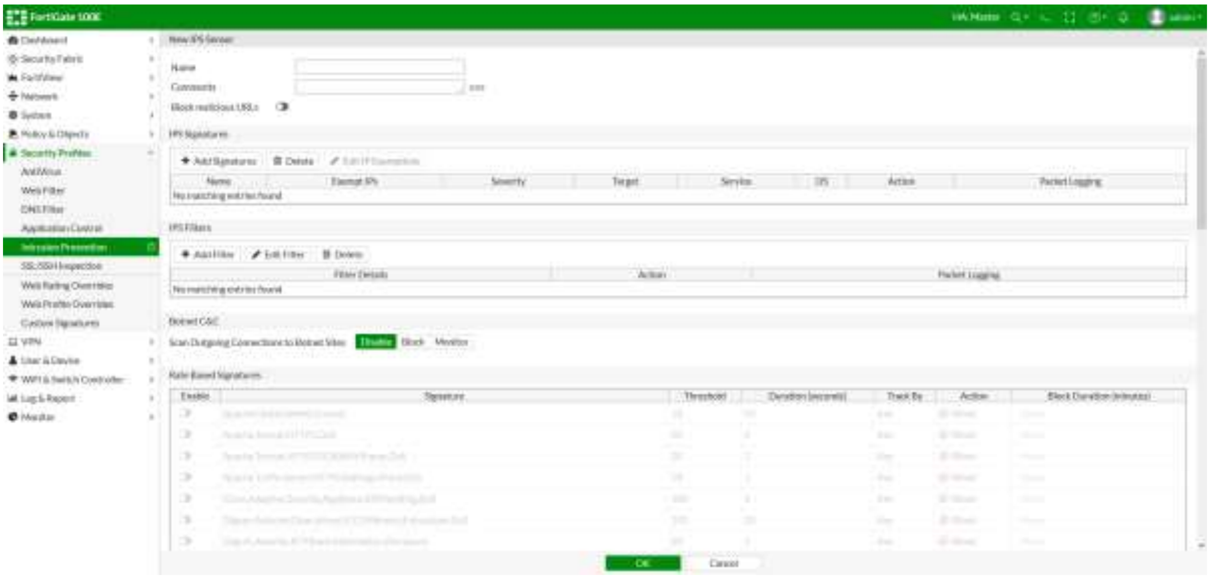


*Figure 2: when creating a new sensor,  you can add IPS signatures, IPS filters or Role Based Signatures*

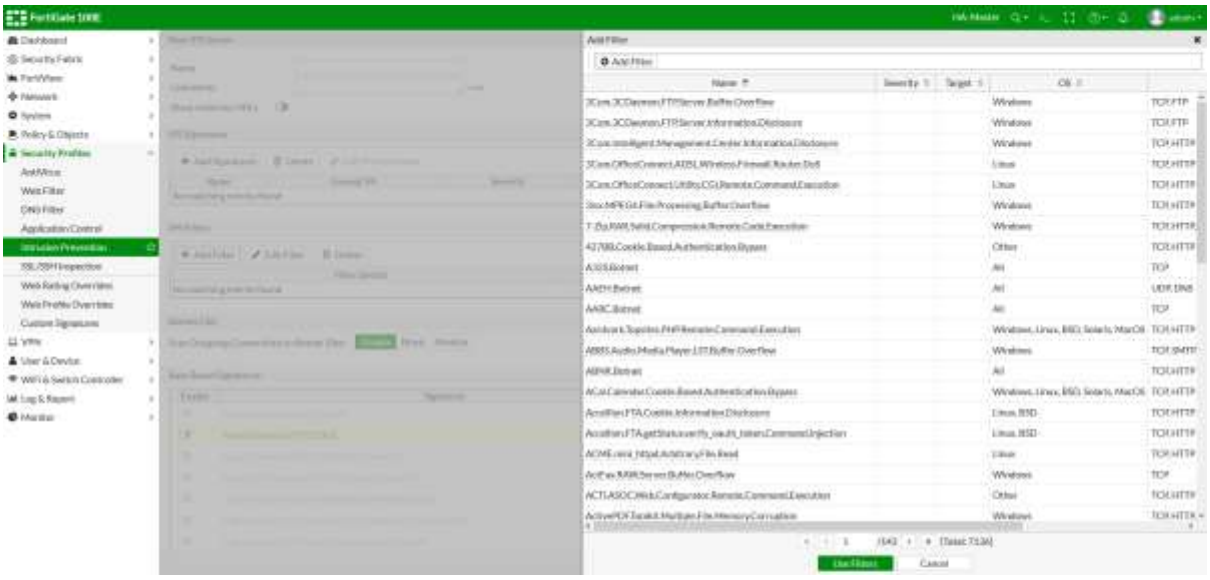
3. Enter the name of the new IPS sensor.
4. Optionally, you may also enter a comment. The comment will appear in the IPS sensor list and serves to remind you of the details of the sensor.
5. Select **OK**.

A newly created sensor is empty and contains no filters or signatures. You need to add one or more filters or signatures before the sensor will be of any use.

### To create a new Pattern Based Signature and Filter

1. Go to **Security Profiles > Intrusion Protection**.
2. Select the IPS sensor to which you want to add the filter using the drop-down list in the top row of the Edit IPS Sensor window or by going to the list window.

3. Under **IPS Filters**, select **Add Filter**.



| Name | Severity | Target | OS | |
|---|---|---|---|---|
| 3Com.3CDaemon.FTPServer.Buffer.Overflow | | | Windows | TCP, FTP |
| 3Com.3CDaemon.FTPServer.Information.Disclosure | | | Windows | TCP, FTP |
| 3Com.Intelligent.Management.Center.Information.Disclosure | | | Windows | TCP, HTTP |
| 3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS | | | Linux | TCP, HTTP |
| 3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution | | | Linux | TCP, HTTP |
| 3ivx.MPEG4.File.Processing.Buffer.Overflow | | | Windows | TCP, HTTP |
| 7-Zip.RAR.Solid.Compression.Remote.Code.Execution | | | Windows | TCP, HTTP |
| 427BB.Cookie.Based.Authentication.Bypass | | | Other | TCP, HTTP |
| A311.Botnet | | | All | TCP |
| AAEH.Botnet | | | All | UDP, DNS |
| AABC.Botnet | | | All | TCP |
| Aardvark.Topsites.PHP.Remote.Command.Execution | | | Windows, Linux, BSD, Solaris, MacOS | TCP, HTTP |
| ABBS.Audio.Media.Player.LST.Buffer.Overflow | | | Windows | TCP, SMTP |
| [illegible].Botnet | | | All | TCP, HTTP |
| ACal.Calendar.Cookie.Based.Authentication.Bypass | | | Windows, Linux, BSD, Solaris, MacOS | TCP, HTTP |
| Accellion.FTA.Cookie.Information.Disclosure | | | Linux, BSD | TCP, HTTP |
| Accellion.FTA.getStatus.verify_oauth_token.Command.Injection | | | Linux, BSD | TCP, HTTP |
| ACME.mini_httpd.Arbitrary.File.Read | | | Linux | TCP, HTTP |
| ActFax.RAW.Server.Buffer.Overflow | | | Windows | TCP |
| ACTi.ASOC.Web.Configurator.Remote.Command.Execution | | | Other | TCP, HTTP |
| ActivePDF.Toolkit.Multiple.File.Memory.Corruption | | | Windows | TCP, HTTP |

1 /542 [Total: 7536]

*Figure 3: create a custom filter or select one of the predefined filters*

4. Configure the filter that you require. Signatures matching all the characteristics you specify in the filter will be included in the filter. Once finished, select **Use Filters**.

**Application** refers to the application affected by the attack and filter options include over 25 applications.

**OS** refers to the Operating System affected by the attack. The options include **BSD**, **Linux**, **MacOS**, **Other**, **Solaris**, and **Windows**.

**Protocol** refers to the protocol that is the vector for the attack; filter options include over 35 protocols, including "other."

**Severity** refers to the level of threat posed by the attack. The options include **Critical**, **High**, **Medium**, **Low**, and **Info**.

**Target** refers to the type of device targeted by the attack. The options include **client** and **server**.

5. Once you have selected the filters you wish to add, right-click the filters and choose an action for when a signature is triggered:

**Pass** to allow traffic to continue to its destination.

**Monitor** to allow traffic to continue to its destination and log the activity.

**Block** to drop traffic matching any the signatures included in the filter.

**Reset** to reset the session whenever the signature is triggered.

**Default** to use the default action of the signature.

**Quarantine** to refuse traffic based on the attacker’s IP Address.

**Packet Logging** to enable packet logging for the filter.

6. Select **Apply**.

The filter is created and added to the filter list. The same process can be followed in order to create or add an IPS Signature to an IPS sensor.

Elias Georgiou is working for IBSCY for the last 4 years. He is working in the implementations department which consist of 4 people. His team is fully responsible for the implementations of new and existing clients in Cyprus and internationally. He holds several certifications from Microsoft, HPE, VMWare and other vendors.