

# **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.

PartiGen 1000				- MAMMA Gen L 11 (01-44)	(Creme)
@ Detritoant	Committee 2 life 19 lites 3 lites - Lamb	٩			
- 4 Security Fathers	A Marine		Contracts		Ref.
A Fact/Ver-	at default	All productional signalization with a			
Antoiniti	<ul> <li>all christity press</li> </ul>	All probabilities algorithmets with			
O System	p debuilt	Theorem contract attacks.			
P. Policy & Objects	, Volucionita	Brocks and Collocato High/Mesthania		- 1	
a tenativ Fratien	protect_times	Product applicat talent skele stal			
Contract (	protect, enset, server	Protect against proail parvier of		2	
AND ALL	protant_http://www.	Perhad against UTTP sarrest still		2	
WEFER	with default	Dehailt contguration for office		1	
CM01/84					
Application/Dotrol					
Internation Prevention of					
38./391 (operation					
Web Earth of Overtides.					
West Paulie Doervises					
Comment Transmission					
Ci vini					
User & Cevite:	- 53				
♥ Wili & Switch Controller					
M tog h lopert	- 85				
C Maritan	- FL				

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.



Fortilate 1008				106 Martin	यत्व द्वार्थ 🖉
Derforment     Society Tabrit     Factfolgen     Factfolgen     Society & Depend     Society & Depend     Policy & Depende		Haner Haner Gootstaatte Hoot matte 195 Septetar	isautusta 🗣		
Secretly Profess AvtiVicus Web Filter ONLTRue Avtivitus	*	+ Auto Managements	lgenteren ∰ Dente 2 (2017) Seconda . net Bened SN Second Secondary Teget Service. 25 Active og extrinctional	Ţ.	PacietLoggra
Application Convert SS-SSI Inspection Weil Rating Contribut Weil Protec Constant Control Republic U VPN Later & Davies	0	+ Aust No mette Bornet Gal Scan Dutgo	llar ≠ Loll (Table III (Johns) Pitale (Jessila geodrate for Mellian I Ing Convectione to Mellian United III (Section	Parlor Loging	
With Switch Controller	1	Rate Raned	National Design of Second Second	and the second sec	Aller's Financian Industry
€ Houdan	2		Annu bits services     0     0     0     0       Annu bits services     0     0     0     0	111111	

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.

Furtiliate State				IN MARK Q+		i Carati		
A Deckent	Mar (Theorem )	Author						
@ Security Failure	1	0 Act The						
In Fact/Meet	A second s	Name 7	Interior 1	Target 4	06.2			
+ Parsuarb	Contraction (B)	Xion XDarmer/11/Stever Julie Overface		Window		TORPTP		
bytes		3Can 3COwner/FEShner/Hornettes/Distance		Winters	( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	TOUTE		
Protecy & Chapterte	1711)	X on moleged Merupated Device InternationDiscourse		Wokee	•	TOURNEED		
Seculty Frafilm	A Sartyanan I & See 1 Providence	Wass/West/resurvey. AUSL Wireless Pressal Rocker Dol		1 mar		100 HTTP		
AntifAtta	1	3ConcOfficeConnectUnitysCS(ParnoteCommand.Encodor		Linia		TOUNTIE		
California	Annalysed supersons	Stor MPEGLF in Processing Rather Charlins		Western	e 11	TOUTO		
Application/Control		7. Ballion Selectorepressive Remote Carls Execution		Wester		TOURTR.		
Insides Prevention	C Particul Constant Andres	43708.Cookie.Enned.Authoritication.Bypan		Other		TORNITTE		
158./59H1repactor	Contraction ( ) Andrease of the second	AllShow		.44		TOP		
Web Rathing Overrides	in course of the second of	Alexandre		AL		UDIT.DNS		
Weie Profile Dvertille		AASC Barnet		Att		102		
Convelignation	another and the second se	Antidexe & Suppliers / HP Restante-Cameranal Earn-start		Widow	clinic Bill: Solets M	ALL TOURTS		
TT Auto	· Surdrapping Constructions for another from the	ABSS Audes Multia Player 117 Bullier Overflew		Webb		TOUGHT		
When & Device:	and the second se	Alther Detrait		All		TOUHT19		
<ul> <li>WiFi &amp; Switch Controller</li> </ul>	1 March 1	ACAL another Control Based Automatication Bypen		Weatow	Lines, 160 Sears, 76	ALL TOURTS		
A tag a tagen		Amelian PlaCoste Information Discharen		Linux, BI	D	TOUHTER		
	De l'announces de	AcuthersPTA getStatuser (f), (sealt), takes Demonstalinjection		Linus M	0	TOURT1#		
		ACME renal (Modulation of the Rend		TRUE		TORNITR		
		Act as \$386.5mm:0.4mDeer5av		Weter	•	104		
		ACTLASOCON/L/Configurator Remain Communit Leasaber		Other		10Umm		
	The second se	Active Of Load Matter Fortheoury Correlation		Wedge		IDAHTER.		
		<ul> <li>North Second State Control (North Second State Second Secon</li></ul>		And of the local				

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.