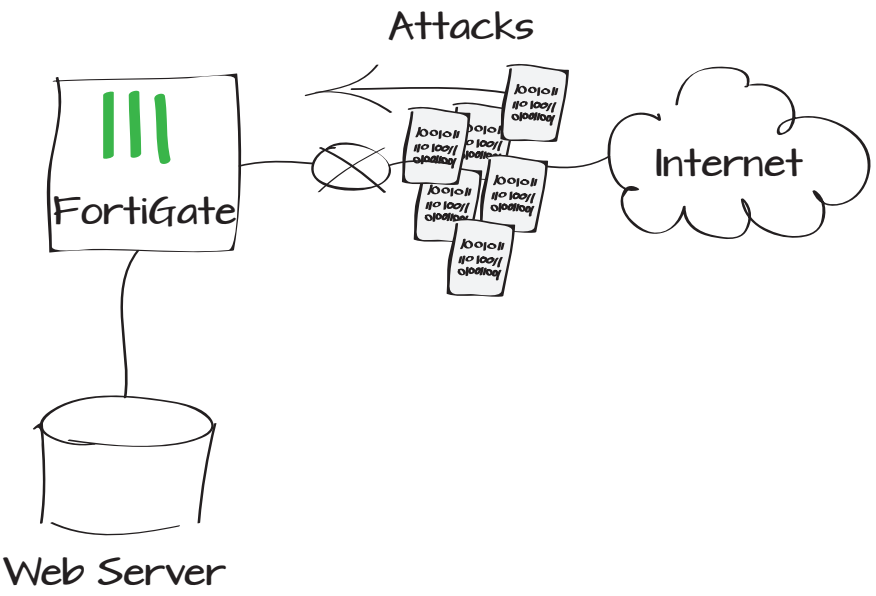
Protecting a web server from external attacks

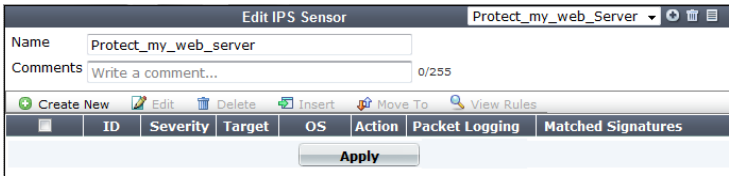
This example uses the FortiOS intrusion protection system (IPS) to protect a web server by configuring an IPS sensor to protect against common attacks and adding it to the policy which allows external traffic to access the server. A denial of service (DoS) security policy is also added to further protect the server against that specific type of attack.

1. Configuring an IPS sensor to protect against common attacks
2. Adding the IPS sensor to a security policy
3. Adding a DoS security policy
4. Results

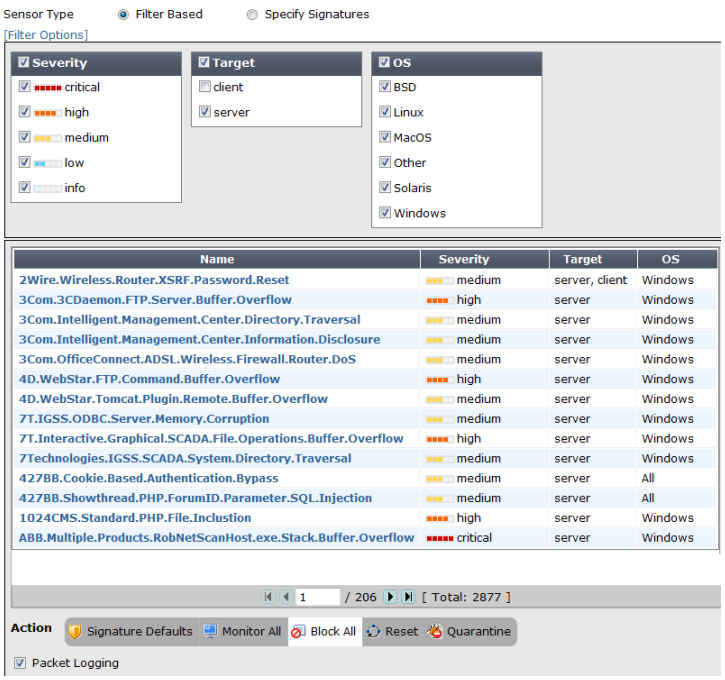


Configuring an IPS sensor to protect against common attacks

Go to **Security Profiles > Intrusion Protection > IPS Sensors**. Select the plus icon in the upper right corner of the window to create a new sensor.



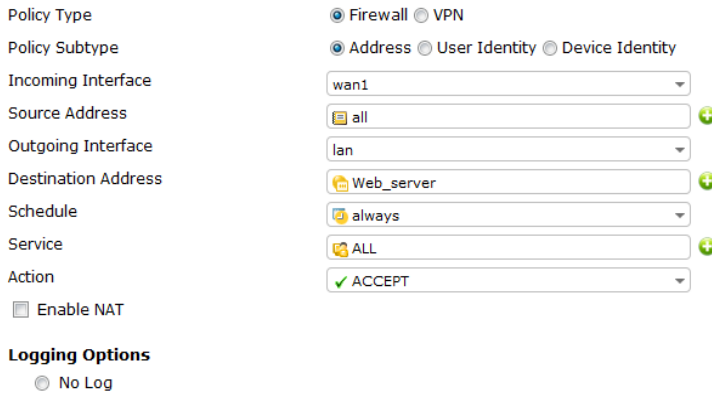
Create a new IPS filter. Set the **Target** to **server** and set the **Action** to **Block All**.



Adding the IPS sensor to a security policy

Go to **Policy > Policy > Policy**. Edit the security policy allowing traffic to the web server from the Internet.

Enable **IPS** and set it to use the new sensor.

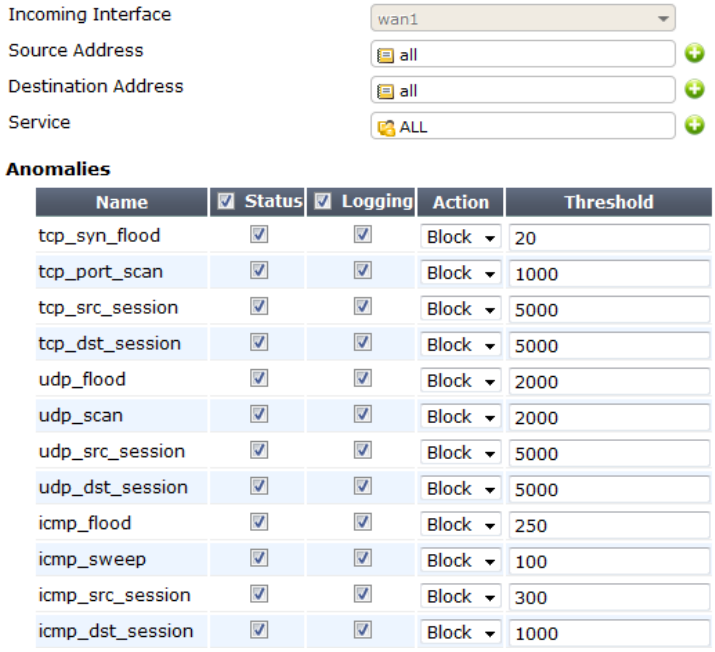


Adding a DoS security policy

Go to **Policy > Policy > DoS Policy**.

Create a new policy. The **Incoming Interface** is your Internet-facing interface.

In the **Anomalies** list, enable **Status** and **Logging** and set the **Action** to **Block** for all types.



Results

WARNING: Causing a DoS attack is illegal, unless you own the server under attack. Before performing an attack, make sure you have the correct server IP.

Perform an DoS tcp_sync_flood attack to the web server IP address. IPS blocks the TCP sync session when it reaches the **tcp_syn_flood** threshold, in this case 20.

Go to **Log & Report > Security Log > Intrusion Protection** to view the results of the DoS policy.

Select an entry to view more information, including the severity of the attack and the attack name.

wnload Raw Log

Severity	Src	Protocol	Count	Attack Name	Attack ID	Level	
	172.20.120.123	tcp	4	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	3	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	2	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	1	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	5	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	9	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	2	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	7	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	3	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	4	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	2	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21
	172.20.120.123	tcp	11	tcp_syn_flood	100663396		anomaly: tcp_syn_flood, 21

Dst	172.20.120.24	**Virtual Domain**	root
Protocol Number	6	**Severity**	critical
Service	http	**Protocol**	tcp
Identity Index	0	**Message**	anomaly: tcp_syn_flood, 21 > threshold 20, repeats 4 times
Dst Port	80	**Reference**	http://www.fortinet.com/ids/VID100663396
roll	65522	**Status**	clear_session
Timestamp	Wed Apr 24 16:04:33 2013	**Sequence Number**	0
Policy ID	0	**Src Interface**	wan1
Src	172.20.120.123	**Count**	4
Level	alert	**Sensor**	DoS-policy1
pcap_id	100663396	**Src Port**	62132
Log ID	18432	**Sub Type**	anomaly
Attack ID	100663396	**Attack Name**	tcp_syn_flood
Date/Time	04-24 16:04 (Wed Apr 24 16:04:33 2013)		