Introduction

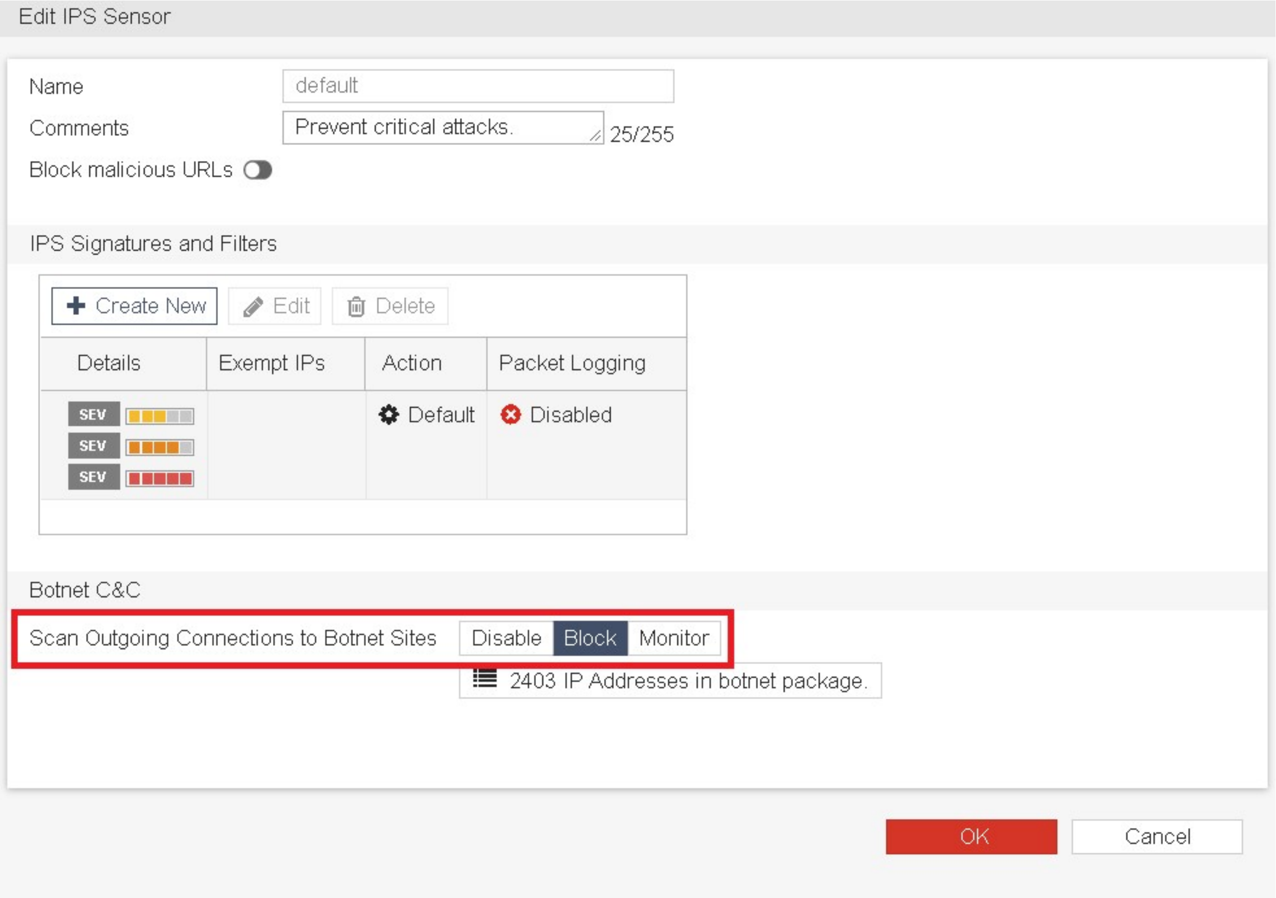
This document is intended to provide guidance on how to enable Botnet detection on FortiGate devices. The information contained in this guide covers all the necessary steps for customers to configure Botnet C&C blocking on the FortiGate.

Botnet C&C IP blocking

The *Botnet C&C* section consolidates multiple botnet options in the IPS profile. This allows you to enable botnet blocking across all traffic that matches the policy by configuring one setting in the GUI, or by the `scan-botnet-connection` command in the CLI.

To configure botnet C&C IP blocking using the GUI:

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. Edit an existing IPS profile, or create a new one.
3. Set *Scan Outgoing Connections to Botnet Sites* to *Block* or *Monitor*.



Edit IPS Sensor

Name: default

Comments: Prevent critical attacks. 25/255

Block malicious URLs ○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging
SEV SEV SEV		Default	Disabled

Botnet C&C

Scan Outgoing Connections to Botnet Sites: Disable [✓ Block] Monitor

2403 IP Addresses in botnet package.

4. Configure the other settings as required.
5. Click *Apply*. Botnet C&C IP is now enabled for the sensor.
6. Add this sensor to the firewall policy.
   The IPS engine will scan outgoing connections to botnet sites. If you access a botnet IP, an IPS log is generated for this attack.
7. Go to *Log & Report* > *Intrusion Prevention* to view the log.

To configure botnet C&C IP blocking using the CLI:

```
config ips sensor
       edit "Demo"
               set scan-botnet-connections {block | monitor}
       next
end
```

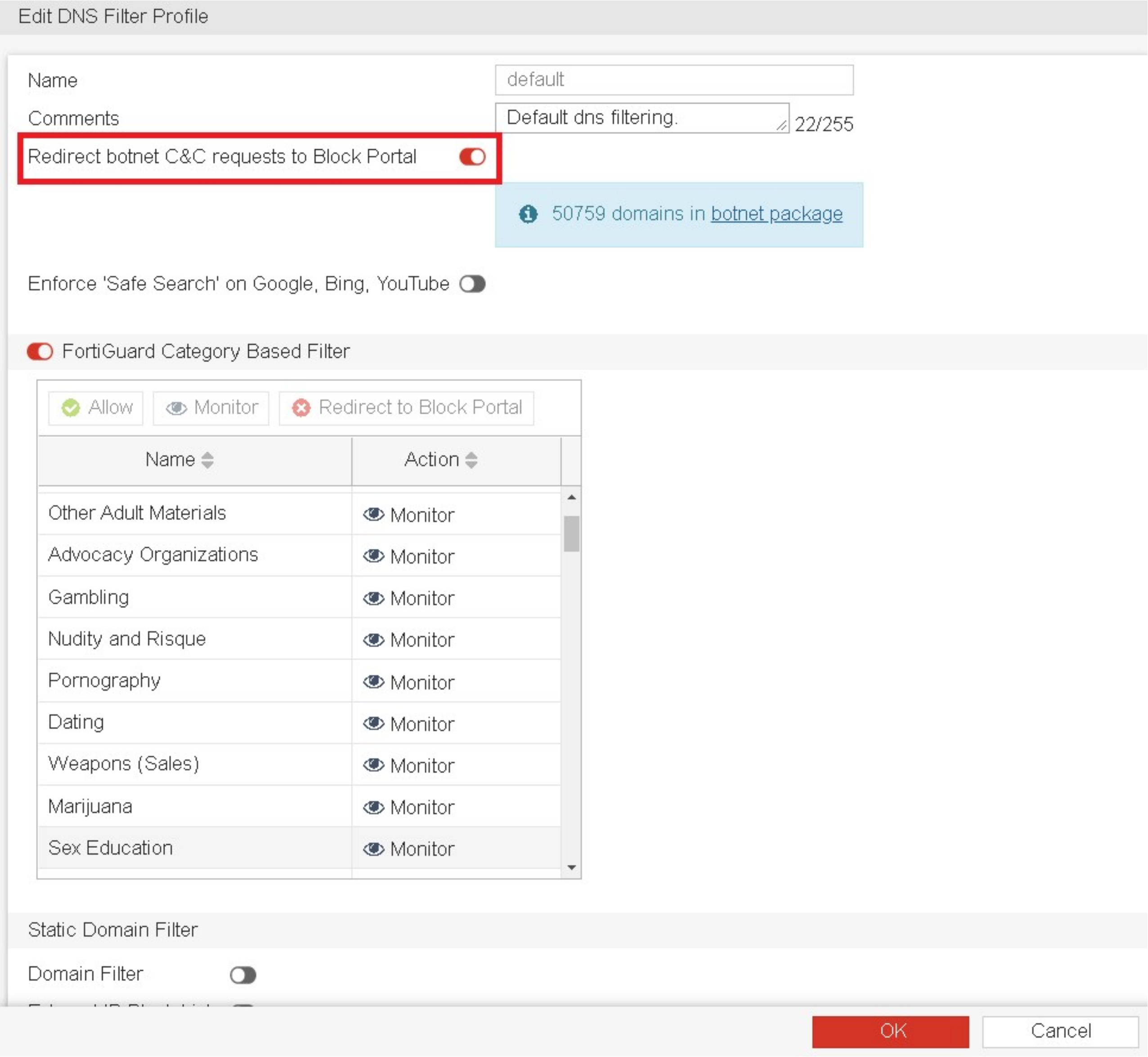
If you are running version 6.0.x or older then it can be configured in under one of the following sections:

- `config firewall interface-policy`
- `config firewall policy`
- `config firewall proxy-policy`

Botnet C&C domain blocking

To block connections to botnet domains using the GUI:

1. Go to *Security Profiles > DNS Filter*.
2. Edit an existing profile, or create a new one.
3. Enable *Redirect Botnet C&C requests to Block Portal*.



Edit DNS Filter Profile

Name: default

Comments: Default dns filtering. 22/255

Redirect botnet C&C requests to Block Portal ●

50759 domains in botnet package

Enforce 'Safe Search' on Google, Bing, YouTube ○

● FortiGuard Category Based Filter

Name	Action
Other Adult Materials	Monitor
Advocacy Organizations	Monitor
Gambling	Monitor
Nudity and Risque	Monitor
Pornography	Monitor
Dating	Monitor
Weapons (Sales)	Monitor
Marijuana	Monitor
Sex Education	Monitor

Static Domain Filter

Domain Filter ○

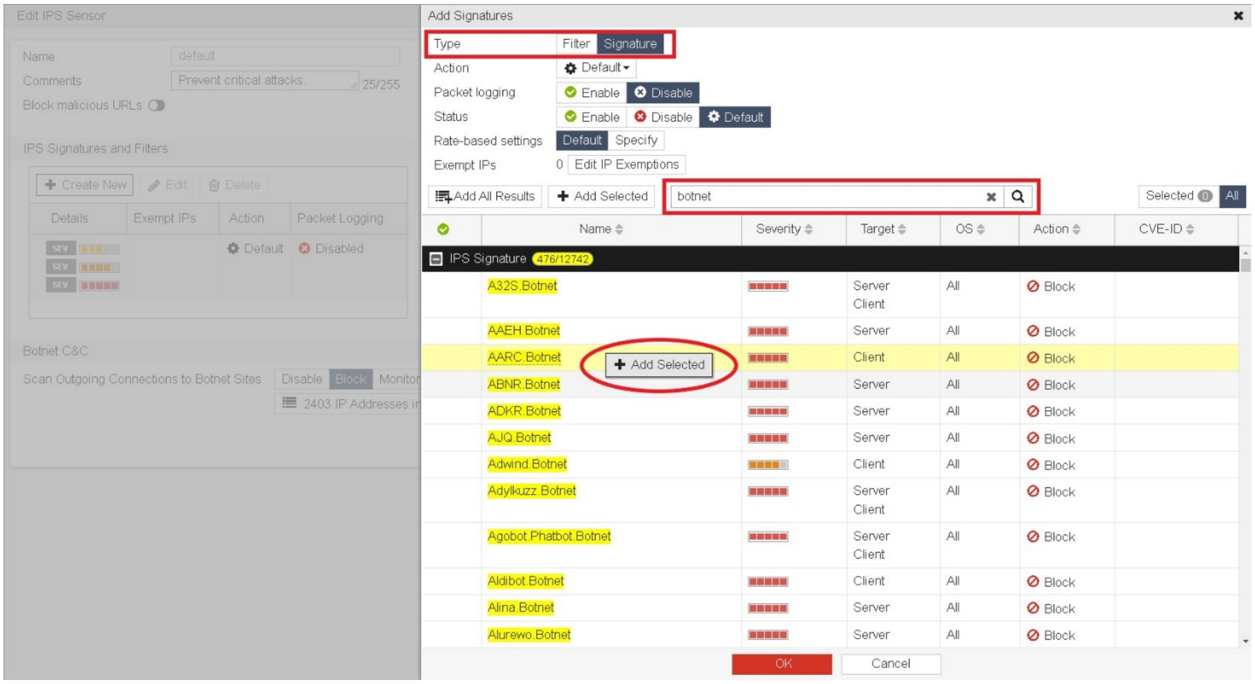
4. Configure other settings as required.
5. Click *OK*.
6. Add this filter profile to a firewall policy.

Botnet C&C signature blocking

To add IPS signatures to a sensor using the GUI:

> One option is to use a predefined default IPS profile to block C&C Signatures. Default IPS profile is pre-configured with default action(block) for severity level 3, 4 and 5 which covers all the C&C signatures.

1. Go to *Security Profiles* > *Intrusion Prevention*.
2. Edit an existing sensor, or create a new one.
3. In the *IPS Signatures and Filters* section, click *Create New*.
4. Set *Type* to *Signature*.
5. Enter *botnet* in the *Search* field to get the list of all available signatures from the database.
6. Right-click the signatures you want to include from the list.
7. Click *Add Selected*.
8. Configure the other settings as required.



Type: Filter | Signature
Action: Default
Packet logging: Enable | Disable
Status: Enable | Disable | Default
Rate-based settings: Default | Specify
Exempt IPs: 0 Edit IP Exemptions

botnet

IPS Signature 476/12742

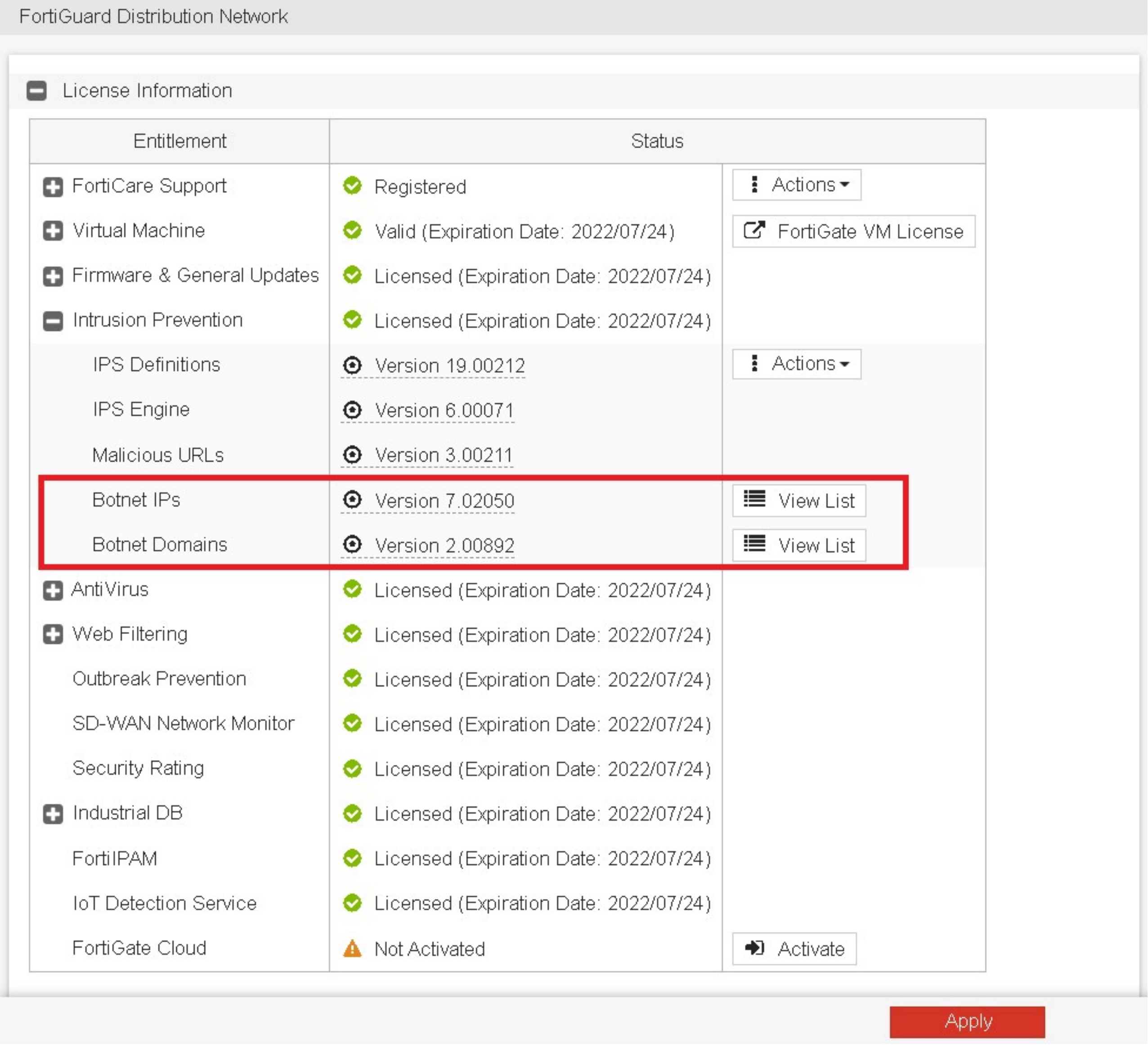
Name	Severity	Target	OS	Action	CVE-ID
A32S.Botnet	▮▮▮▮▮	Server Client	All	⊘ Block	
AAEH.Botnet	▮▮▮▮▮	Server	All	⊘ Block	
AARC.Botnet	▮▮▮▮▮	Client	All	⊘ Block	
ABNR.Botnet	▮▮▮▮▮	Server	All	⊘ Block	
ADKR.Botnet	▮▮▮▮▮	Server	All	⊘ Block	
AJQ.Botnet	▮▮▮▮▮	Server	All	⊘ Block	
Adwind.Botnet	▮▮▮▮	Client	All	⊘ Block	
Adylkuzz.Botnet	▮▮▮▮▮	Server Client	All	⊘ Block	
Agobot.Phatbot.Botnet	▮▮▮▮▮	Server Client	All	⊘ Block	
Aldibot.Botnet	▮▮▮▮▮	Client	All	⊘ Block	
Alina.Botnet	▮▮▮▮▮	Server	All	⊘ Block	
Alurewo.Botnet	▮▮▮▮▮	Server	All	⊘ Block	

9. Click *OK*
10. Configure other settings as required, then click *OK*
11. Add this sensor to a firewall policy to detect or block attacks that match the IPS signatures.

Botnet IPs and domains lists

To view botnet IPs and domains lists using the GUI:

1. Go to *System* > *FortiGuard*. *Botnet IPs* and *Botnet Domains* are visible in the *Intrusion Prevention* section.
2. Click *View List* for more details.



FortiGuard Distribution Network

License Information

Entitlement	Status	
FortiCare Support	✓ Registered	Actions ▾
Virtual Machine	✓ Valid (Expiration Date: 2022/07/24)	FortiGate VM License
Firmware & General Updates	✓ Licensed (Expiration Date: 2022/07/24)	
Intrusion Prevention	✓ Licensed (Expiration Date: 2022/07/24)	
IPS Definitions	Version 19.00212	Actions ▾
IPS Engine	Version 6.00071	
Malicious URLs	Version 3.00211	
Botnet IPs	Version 7.02050	View List
Botnet Domains	Version 2.00892	View List
AntiVirus	✓ Licensed (Expiration Date: 2022/07/24)	
Web Filtering	✓ Licensed (Expiration Date: 2022/07/24)	
Outbreak Prevention	✓ Licensed (Expiration Date: 2022/07/24)	
SD-WAN Network Monitor	✓ Licensed (Expiration Date: 2022/07/24)	
Security Rating	✓ Licensed (Expiration Date: 2022/07/24)	
Industrial DB	✓ Licensed (Expiration Date: 2022/07/24)	
FortiIPAM	✓ Licensed (Expiration Date: 2022/07/24)	
IoT Detection Service	✓ Licensed (Expiration Date: 2022/07/24)	
FortiGate Cloud	⚠ Not Activated	Activate