



# FortiADC - IPS Deployment Guide

Version 5.3.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



September 03, 2019

FortiADC 5.3.0 IPS Deployment Guide

(Undefined variable: FortinetVariables.Document Number)

# TABLE OF CONTENTS

- Change Log** ..... **4**
- Introduction** ..... **5**
  - 1. Inside FortiADC: Intrusion Prevention System (IPS) ..... 5
- Deployment** ..... **10**
  - 1. GUI ..... 10
  - 2. CLI ..... 15
- Log and Debug** ..... **18**

## Change Log

Date	Change Description
2019-09-03	Initial release.

# Introduction

The FortiADC Intrusion Prevention System (IPS) combines signature detection and prevention with low latency and excellent reliability. With intrusion protection, you can create multiple IPS profiles, each containing a complete configuration based on signatures. Then, you can apply any IPS profile to any L4 VS.

This section describes how to configure the FortiADC Intrusion Prevention settings.

## 1. Inside FortiADC: Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.

### World class next generation IPS capabilities

Today, sophisticated and high volume attacks are challenges that every organization must recognize. These attacks are evolving, infiltrating ever-increasing vectors and complex network environments. The result is an urgent need for network protection while maintaining the ability to efficiently provide demanding services and applications.

### Highlights

- Validated best-in-class security and capacity with proven coverage and high performance.
- Comprehensive protection provided by a signatures-based IPS engine, protocol anomaly scanning.
- Flexible deployment options and actionable implementations for a wide array of network integration and operation requirements.

### Key features & benefits

Best-in-class security with superior coverage	Protects critical digital resources from both internal exploits and external cybercriminals, even if sophisticated attacks are crafted.
Backed by FortiGuard Labs that deliver real-time protection	Maintain up-to-date and proactive protection against latest known threats and newly discovered hacking techniques while allowing time for organizations to patch vulnerable systems.

## Features

### Tested and proven protection

FortiGuard IPS signatures are periodically tested and certified by well-known external labs. Now the IPS has been deployed on FortiADC which has been successfully developed on FortiADC, as the forerunner of the Security Effectiveness.

### Real-time & zero-day protection

The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

## FortiGuard IPS service quick facts

1. Over 10,000 signatures consisting of 18,000 rules (some of the are based on the extended database, which FortiADC is not yet supported, FortiADC has about 6000 signatures originally)
2. Approximately 470,000 network intrusion attempts resisted per minute
3. About 1,000 rules are updated or added per week
4. Over 300 Zero-day vulnerabilities discovered to date

This update service is backed by a team of threat experts and a close relationship with major application vendors. The best-in-class team also uncovers significant zero-day vulnerabilities continuously, providing FortiADC units with advanced protection ahead of vendor patches.

## Protocol decoders and anomaly detection

Protocol decoders are required to assemble the packets and detect suspicious, nonconforming sessions that resemble known attacks or are non-compliant to RFC or standard implementation.

FortiADC offers one of the most comprehensive arrays of protocol decoders in the industry, providing customers with significantly wide coverage in all kinds of environments.

## Pattern & rate-based signatures

The pattern signature matching technique is essential in IPS implementation due to its high level of precision and accuracy. FortiADC offers administrators robust pattern signature selection using filters based on severity, target, operating system, application, and protocol. Each of the signatures has a direct link to its detailed entry on the threat encyclopedia and CVE-ID references. After selection, administrators are able to assign associated actions such as pass, block and default.

Rate-based IPS signatures protect networks against application based DoS and brute force attacks. Administrators can configure 20 rate-based IPS signatures and tune them to their needs. Threshold (incidents per minute) and an action to take when the threshold is reached can be assigned to each signature. If the action is set to block, then a timeout period can be set so that the block is removed after a specified duration.

## Predefined Profiles

Every individual IPS Signature takes effect for a particular type of attack, for an effective detection and protection, a well-considered combination of different IPS signatures plays a key role for the whole IPS system. FortiADC has 8 predefined Profiles in respect to: action, application, severity, target, etc. are ready for customers for a fast security-set-up.

Predefined Profile	Comment
all_default	Signatures with default setting.
all_default_pass	Signatures with PASS action.
default	Prevents critical attacks
high_security	Blocks all Critical/High/Medium and some Low severity vulnerabilities.

Predefined Profile	Comment
protect_client	Protect against client-side vulnerabilities.
protect_email_server	Protect against email server-side vulnerabilities.
protect_http_server	Protect against HTTP server-side vulnerabilities.
sniffer-profile	Monitor IPS attacks.

The coming section will explain how to configure the IPS in detail.

IPS Signatures

+

Add Signature

[-]

Delete

Signature

Severity

Location

OS

Action

No data available in table

Showing 0 to 0 of 0 entries

Show15▼

entries

PreviousNext

IPS Filters

+

Add Filter

[-]

Edit

[-]

Delete

Filter Details

Action

No data available in table

Showing 0 to 0 of 0 entries

Show15▼

entries

PreviousNext

Rate Based Signatures

Status

Signature

Threshold

Track By

Duration (seconds)

Action

OFF

SMB Login Brute Force

500

Destination IP

60

Block

OFF

Digium Asterisk IAX2 Call Number DDoS

275

Source IP

1

Block

OFF

Trinet Login Brute Force

60

Destination IP

60

Block

OFF

POP3 Login Brute Force

200

Destination IP

10

Block

OFF

IMAP Login Brute Force

60

Destination IP

10

Block

OFF

MySQL Login Brute Force

60

Destination IP

60

Block

OFF

FTP Login Brute Force

200

Destination IP

10

Block

OFF

MS XML Core Services Memory Corruption

5

Source IP

10

Block

OFF

DoS Vulnerable Padding Oracle Attack

1000

Source IP

5

Block

OFF

MS Windows SMB NTLM Authentication Lack Of Error

25

Source IP

1

Block

Showing 1 to 10 of 20 entries

Show15▼

entries

Previous12Next

## Signature-based defense

Signature-based defense is used against known attacks or vulnerability exploits. These often involve an attacker attempting to gain access to your network. The attacker must communicate with the host in an attempt to gain access and this communication will include particular commands or sequences of commands and variables. The IPS signatures include these command sequences, allowing the FortiADC unit to detect and stop the attack.

## Signatures

IPS signatures are the basis of signature-based intrusion prevention. Every attack can be reduced to a particular string of commands or a sequence of commands and variables. Signatures include this information so your FortiADC unit knows what to look for in network traffic.

Signatures also include characteristics about the attack they describe. These characteristics include the network protocol in which the attack will appear, the vulnerable operating system, and the vulnerable application.

The FortiGuard Intrusion Prevention Service (IPS) provides customers with the latest defenses against stealthy network-level threats through a constantly updated database of known threats and behavior-based signatures.

This update service is backed by a team of threat experts and a close relationship with major application vendors. The best-in-class team also uncovers significant zero-day vulnerabilities continuously, providing FortiADC units with advanced protection ahead of vendor patches.

The IPS Signatures Database is able to be updated automatically or manually by System > Settings > FortiGuard page

## Protocol decoders

Before examining network traffic for attacks, the IPS engine uses protocol decoders to identify each protocol appearing in the traffic. Attacks are protocol-specific, so your FortiADC unit conserves resources by looking for attacks only in the protocols used to transmit them. For example, the FortiADC unit will only examine HTTP traffic for the presence of a signature describing an HTTP attack.

## IPS engine

Once the protocol decoders separate the network traffic by protocol, the IPS engine examines the network traffic for attack signatures. The engine count is configurable by CLI as well. (The recommendation is configuring the engine count as the same count of CPU of the FortiADC has, an ips-engine per CPU)

## IPS profiles

The IPS engine does not examine network traffic for all signatures. You must first create an IPS profile and specify which signatures are included. Add signatures to profile individually using signature entries, or in groups using IPS filters.

To view the IPS profiles, go to **Security Profiles > Intrusion Prevention**.

You can group signatures into IPS profiles for easy selection when applying to L4 VS Security. You can define signatures for specific types of traffic in separate IPS profiles, and then select those profiles in profiles designed to handle that type of traffic. For example, you can specify all of the web-server related signatures in an IPS profile, and that the profile can then be applied to a L4 VS Security that controls all of the traffic to and from a web server protected by the unit.

The FortiGuard Service periodically updates the signatures, with signatures added to counter new threats. Since the signatures included in filters are defined by specifying signature attributes, new signatures matching existing filter specifications will automatically be included in those filters. For example, if you have a filter that includes all signatures for the Windows operating system, your filter will automatically incorporate new Windows signatures as they are added.

Each filter consists of a number of signatures attributes. All of the signatures with those attributes, and only those attributes, are checked against traffic when the filter is run. If multiple filters are defined in an IPS profile, they are checked against the traffic one at a time, from top to bottom. If a match is found, the unit takes the appropriate action and stops further checking.

The signatures included in the filter are only those matching every attribute specified. When created, a new filter has every attribute set to all which causes every signature to be included in the filter. If the severity is changed to high, and the target is changed to server, the filter includes only signatures checking for high priority attacks targeted at servers.

## IPS filters

IPS profiles contain one or more IPS filters. A filter is a collection of signature attributes that you specify. The signatures that have all of the attributes specified in a filter are included in the IPS filter.

For example, if your FortiADC unit protects a Linux server running the Apache web server software, you could create a new filter to protect it. By setting OS to Linux, and Application to Apache, the filter will include only the signatures that apply to both Linux and Apache. If you wanted to scan for all the Linux signatures and all the Apache signatures, you would create two filters, one for each.

To view the filters in an IPS profile, go to **Security Profiles > Intrusion Prevention**, select the IPS profile containing the filters you want to view, and select Edit.

## Custom/predefined signature entries



Signature entries allow you to add an individual custom or predefined IPS signature. If you need only one signature, adding a signature entry to an IPS profile is the easiest way. Signature entries are also the only way to include custom signatures in an IPS profile.

Another use for signature entries is to change the settings of individual signatures that are already included in a filter within the same IPS profile. Add a signature entry with the required settings above the filter, and the signature entry will take priority.

### **Security - L4 VS**

To use an IPS profile, you must select it in a L4 VS security options. An IPS profile that is not selected in a policy options will have no effect on network traffic.



IPS does not support NAT46.

---

### **Session timers for IPS sessions**

A session time-to-live (TTL) timer for IPS sessions is available to reduce synchronization problems between the FortiADC Kernel and IPS, and to reduce IPS memory usage.

# Deployment

## 1. GUI

### Quick-Enabling IPS

Refer to the section of Predefined Profiles in [Introduction on page 5](#).

### General configuration steps

For best results in configuring IPS scanning, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Create an IPS Profile.
2. Add signatures and /or filters.  
These can be:
  - Pattern based
  - Rate based
3. In the L4 VS Security Option, Click to select IPS, and choose the IPS Profile from the list.

All the network traffic goes through this L4 VS by this security option -IPS- will be processed according to the configuration of the deployed IPS Profile, these configuration you specify in the IPS Profile.

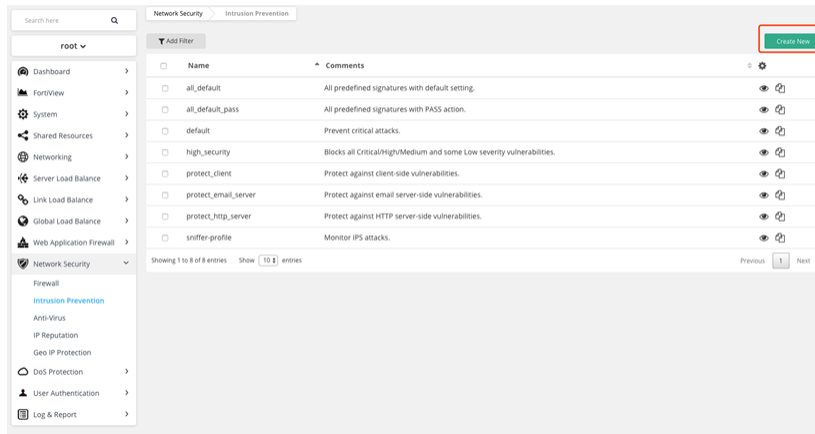
### Creating an IPS Profile

You need to create an IPS profile before specific signatures or filters can be chosen. The signatures can be added to a new profile before it is saved. However, it is good practice to keep in mind that the profile and its included filters are separate things, and that they are created separately. (Predefined Profiles)

#### To create a new IPS Profile

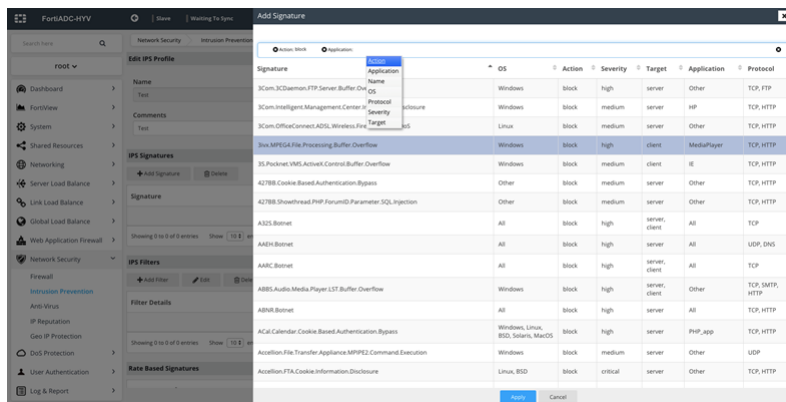
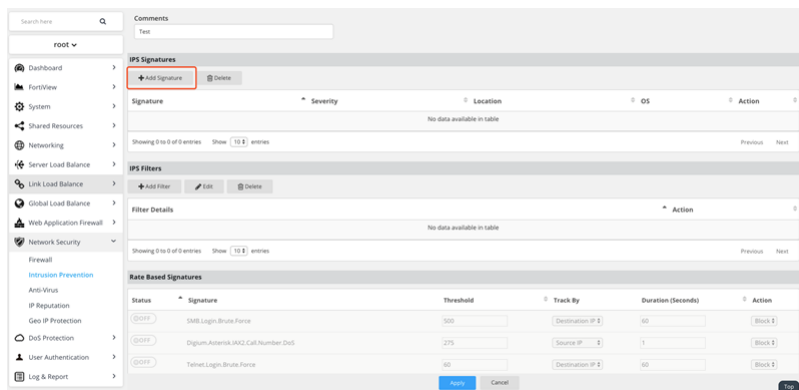
1. Go to **Security Profiles > Intrusion Prevention**.
2. Select the **Create New** icon in the top of the Edit IPS Profile window.
3. Enter the name of the new IPS Profile.
4. Optionally, enter a comment. The comment will appear in the IPS Profile list.
5. Select OK.

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



## Adding IPS signatures to a Profile

1. Go to **Security > Intrusion Prevention**.
2. Select the IPS Profile to which you want to add the signature and click the pencil icon.
3. Under IPS Signatures, select **Add Signature**.
4. Select one or more signatures from the list and click Apply to add them to the sensor.
5. After the selected signature has been added to the IPS Signatures, the drop-down list of Action, which is on the right side of the signature, has Default, Pass and Block, is changeable.
6. Click **Apply** on the bottom of the IPS Profile page



## Adding an IPS filter to a Profile

While individual signatures can be added to a Profile, a filter allows you to add multiple signatures to a Profile by specifying the characteristics of the signatures to be added.

### To create a new pattern based signature and filter

1. Go to Security Profiles > Intrusion Prevention.
2. Select the IPS Profile to which you want to add the signature and click the pencil icon.
3. Under IPS Filters, select Add Filter.
4. Configure the filter that you require. Signatures matching all of the characteristics you specify in the filter will be included in the filter. Once finished, select Apply.

**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.**

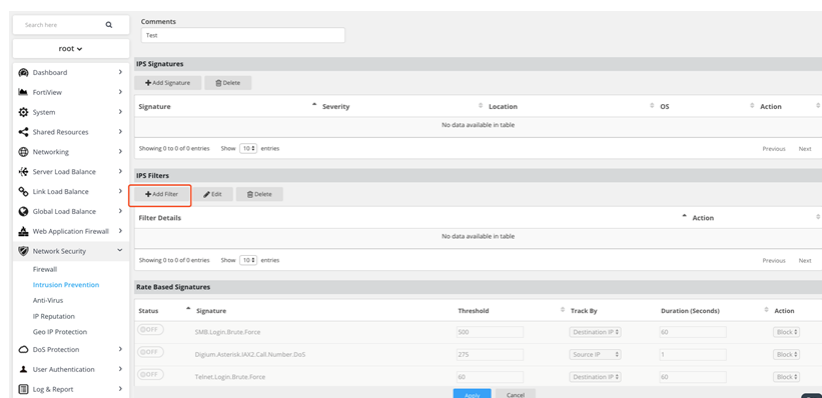
**Protocol** refers to the protocol that is the vector for the attack; filter options include over 35 protocols, including "other."

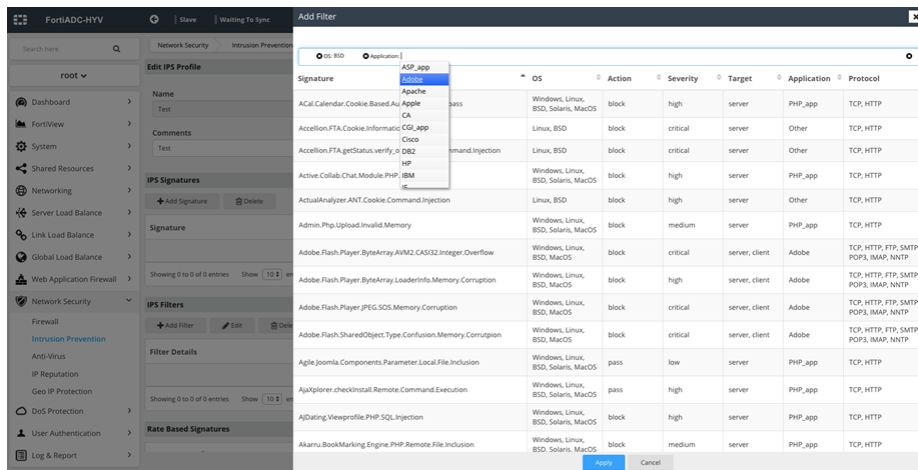
**Severity** refers to the level of threat posed by the attack. The options include **Critical, High, Medium, Low, and Info.**

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

Action	Description
Pass	Select Pass to allow traffic to continue to its destination. Note: to see what the default for a signature is, go to the IPS Signatures page and enable the column Action, then find the row with the signature name in it.
Block	Select Block to drop traffic matching any signatures included in the filter.
Default	Select Default to use the default action of the signature.

5. After the selected signature has been added to the IPS Signatures, the drop-down list of Action, which is on the right side of the Filter, has Default, Pass and Block, is changeable
6. Click **Apply** on the bottom of the IPS Profile page

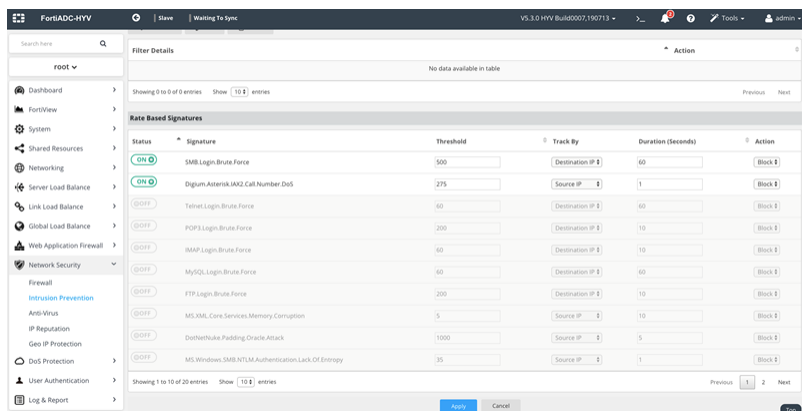




## Adding rate based signatures

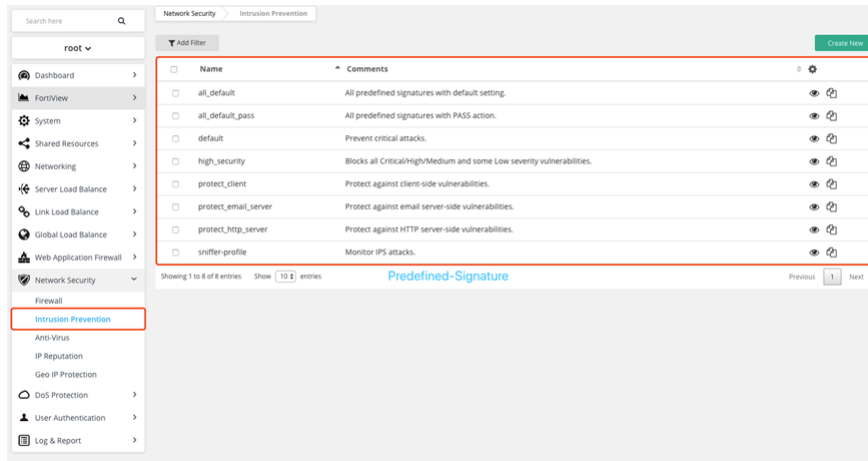
These are a subset of the signatures that are found in the database. This group of signatures is for vulnerabilities that are normally only considered a serious threat when the targeted connections come in multiples, like DoS attacks.

Adding a rate based signature is straight-forward. Select the enable button in the Rate Based Signature table that corresponds with the desired signature.



## Predefined IPS Profile

FortiADC has 8 predefined IPS Profiles for the convenience and fast-set-up of users to enable IPS more quickly. Each predefined profile is created under the attributes of each signature. For users demanding a wide protection but not yet ready to create a particular customized profile, predefined IPS profiles are highly recommended. They will be routinely updated resulted from a periodical database update by the FortiGuard Service. These Profiles are available by directly selecting from **Security -> IPS** in L4 VS options. They can be considered a Quick-Enabling-IPS.

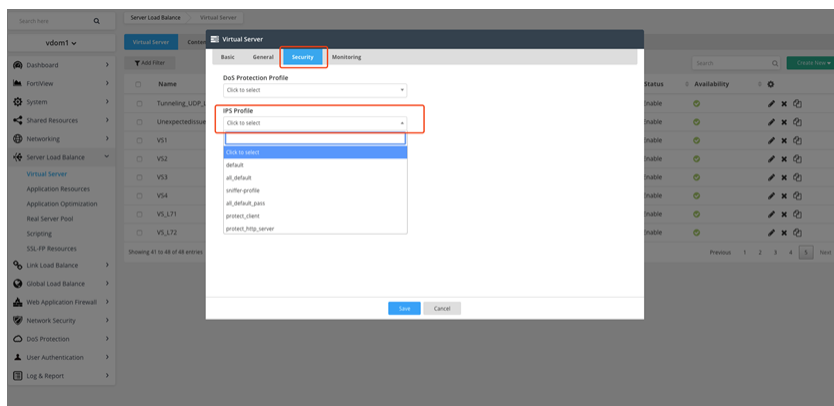


## Enabling IPS

Currently, the IPS Scanning only supports L4VS traffic

- The IPS Profile contains filters, signature entries, or both. These specify which signatures are included in the IPS Profile.

When an IPS Profile is selected in a security option, all network traffic matching the policy will be checked for the signatures in the IPS Profile.



## Configuring Engine Count

In consideration of performance differences on different platform, and for other various demands, the Engine-Count of IPS in FortiADC can be configured. The more Engine-Count that a FortiADC has, the better the IPS performs. However, this will require more CPU and memory.

The default value of the Engine-count is 1.

Eg: 4-Engine for a 4-Core device.

## CLI Syntax

```
config global
config system ips
set engine-count {1-256}
next
end
```

## Enabling IPS

Currently, IPS Scanning only supports L4VS traffic

- The IPS Profile contains filters, signature entries, or both. These specify which signatures are included in the IPS Profile.

When an IPS Profile is selected in a security option, and all network traffic matching the policy will be checked for the signatures in the IPS Profile.

Virtual Server

Basic General **Security** Monitoring

DoS Protection Profile

Click to select

IPS Profile

Click to select

Click to select

- default
- all\_default
- sniffer-profile
- all\_default\_pass
- protect\_client
- protect\_http\_server

Save Cancel

## 2. CLI

### Config IPS Profile

```
config security ips profile
edit <profile>
set comment {comment}
config entries
edit {id}
set rule {id1 id2 ...}
set status {disable | enable | default}
set log {disable | enable}
set action {pass | block | default}
set location {loc1 loc2...}
set severity {sev1 serv2...}
set protocol {proto1 proto2...}
set application {app1 app2...}
set os {os1 os2...}
set rate-count {count}
set rate-duration {duration}
set rate-mode {periodical | continuous}
set rate-track {field}
next
end
```

### IPS profile option in VS

```
config load-balance virtual-server
```

```
set type l4-load-balance
set ips-profile {name}
next
end
get security ips info rule
FortiADC-VM (root) # get security ips info rule
rule-name: "MS.SMB.Client.Memory.Allocation.Code.Execution"
rule-id: 20900
rev: 2.855
date: 1398326400
action: block
status: enable
log: disable
severity: 4.critical
service: TCP, NBSS
location: client
os: Windows
application: Other
rate-count: 0
rate-duration: 0
rate-track: none
rate-mode: continuous
vuln_type: Resource Management Errors
cve: 20100269

rule-name: "MS.Windows.MPEG.Layer3.Audio.Decoder.Stack.Overflow"
rule-id: 20903
rev: 3.095
date: 1398240000
action: block
status: enable
log: disable
severity: 4.critical
service: TCP, HTTP, FTP, SMTP, POP3, IMAP, NNTP
location: server, client
os: Windows
application: MediaPlayer
rate-count: 0
rate-duration: 0
rate-track: none
rate-mode: continuous
vuln_type: Buffer Errors
cve: 20100480
```

## Quick Creating a new L4 VS with IPS

1. Create a new L4 VS.
2. Go to **Server Load Balance** and click **Virtual Server**.
3. Click **Create New > Advanced Mode**.
4. Create a L4 VS named as Test VS, for example.
5. Create a new IPS Profile.
6. Go to **Network Security** and click **Intrusion Prevention**.
7. Click **Create New** to create a customized IPS Profile, named as Test IPS for example.

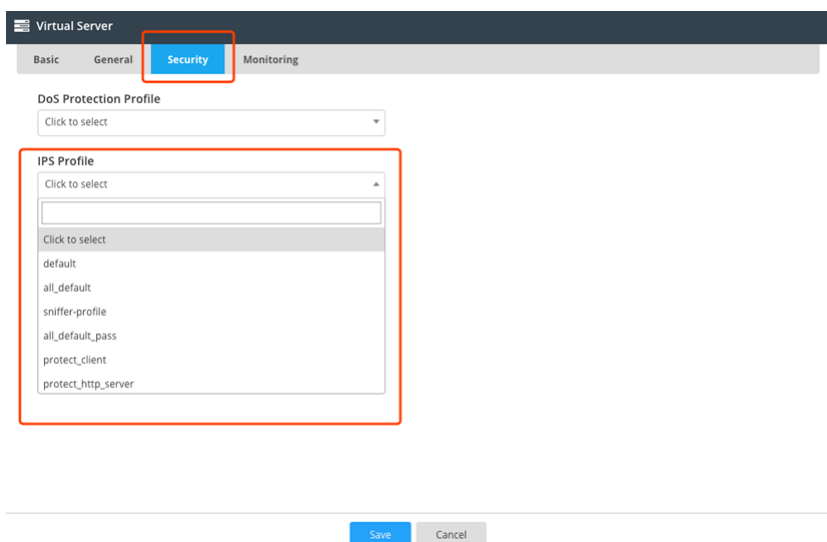


8. Select the necessary IPS Signatures / filters / Rete based Signatures
9. **Apply**
10. Enable the IPS Profile for L4 VS.



IPS does not support NAT46.

11. Go back to the L4 VS - Test VS.
12. Click the pencil icon and click **Security**.
13. The created IPS profile can be selected in the drop down list.



Virtual Server

Basic General **Security** Monitoring

DoS Protection Profile

Click to select

IPS Profile

Click to select

Click to select

- default
- all\_default
- sniffer-profile
- all\_default\_pass
- protect\_client
- protect\_http\_server

Save Cancel

# Log and Debug

## Syslog and statistics

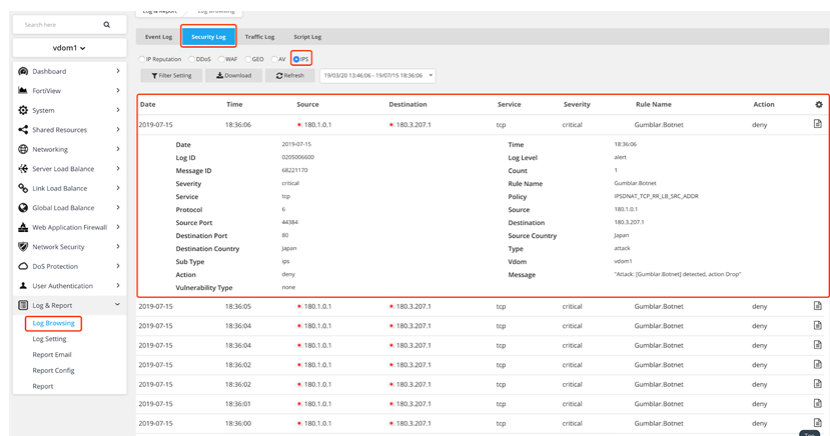
Log header	
date	The year, month and day of when the event occurred in yyyy-mm-dd format
time=(12:55:06)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
log_id	A five or ten-digit unique identification number
type	Attack for IPS
subtype	The subtype category of the log message(IPS)
level	The priority level of the event.
vd	The name of the virtual domain where the action/event occurred in.

## Log body fields

Log body	
source	Source IP address
dstination	Destination IP address
proto	Protocol
policy	Virtual server name
service	Service
action	Policy action
sigid	Attack signature ID
srccountry	Location of the source IP address
dstcountry	Location of the destination IP address
msg	Security profile name, category, subcategory, and description of the attack.
count	Rule match count

## Browsing Log over GUI

1. Go to **Log Report > Log Browsing**.
2. Select the **Security Log** and then click **IPS**.
3. All the traffic triggered IPS will be listed.
4. Click the **Detail** icon; the details of the traffic are according to the format provided above.



## Debug

#diagnose debug module ips-engine

Option	Content
show	show ips engine debug status
packet	ips engine packet debug info
packet-detail	ips engine packet detail debug info
timeout	ips engine timeout debug info
cfg	ips engine config debug info
cfg-delay	ips engine config delay debug info

#diagnose ips session

Option	Content
clear	clear all sessions in ips engine
content	show ips session content statistics
list	list all sessions in ips engine
performance	show ips session performance statistics
status	show ips session status



**FORTINET®**



Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.