

The Fortinet logo is displayed in white against a background of abstract, glowing orange and red geometric shapes and grid patterns. The letter 'F' is stylized with a grid pattern inside its vertical bars.

**FORTINET**<sup>TM</sup>

# FortiGate IPS Guide

**FortiGate Antivirus Firewall IPS User Guide**

**Version 2.1**

17 June 2005

01-28010-0080-20050617

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

*FortiGate Antivirus Firewall IPS User Guide*

Version 2.1

FortiOS v2.80 MR10

17 June 2005

01-28010-0080-20050617

**Trademarks**

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

For technical support, please visit <http://www.fortinet.com>.

Send information about errors or omissions in this document or any Fortinet technical documentation to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

# Table of Contents

<b>Introduction .....</b>	<b>5</b>
About the FortiGate Intrusion Prevention System.....	5
About this document .....	5
Fortinet documentation .....	6
Fortinet Knowledge Center .....	7
Comments on Fortinet technical documentation .....	7
Customer service and technical support.....	7
<b>IPS Overview and General Configuration.....</b>	<b>9</b>
IPS overview .....	9
The FortiGate IPS .....	9
When to use IPS .....	10
Network performance.....	10
Default signature and anomaly settings.....	11
Configuring system settings.....	11
Monitoring the network and dealing with attacks .....	12
Configuring logging and alert email .....	13
Attack log messages.....	14
The FortiGuard Center.....	15
Using IPS in a protection profile.....	16
IPS protection profile options .....	16
Creating a protection profile that uses IPS .....	16
<b>Predefined Signatures .....</b>	<b>19</b>
Predefined signatures overview.....	19
Viewing the predefined signature list .....	19
Predefined signature configuration .....	22
Configuring individual signature settings .....	22
Changing the status of predefined signature groups .....	23
Configuring parameters for signature groups .....	23
Configuring signatures using the CLI.....	25
<b>Custom Signatures .....</b>	<b>29</b>
Viewing custom signatures .....	29
Custom signature configuration .....	30
Adding custom signatures using the web-based manager .....	30
Adding custom signatures using the CLI .....	31
Backing up and restoring the custom signature list .....	32
Creating custom signatures .....	33
Custom signature fields .....	34
Custom signature syntax .....	35

- Anomalies..... 43**
  - Anomalies overview ..... 43
  - Viewing the anomaly list ..... 44
  - Configuring an anomaly using the web-based manager..... 44
  - Configuring an anomaly using the CLI..... 46
    - config limit ..... 46
  
- SYN Flood Attacks..... 49**
  - How SYN floods work ..... 49
  - The FortiGate IPS Response to SYN Flood Attacks..... 50
    - What is SYN threshold? ..... 50
    - What is SYN proxy? ..... 50
    - How IPS works to prevent SYN floods..... 50
  - Configuring SYN flood protection..... 52
  - Suggested settings for different network conditions ..... 52
  
- ICMP Sweep Attacks..... 53**
  - How ICMP sweep attacks work ..... 53
  - The FortiGate IPS response to ICMP sweep attacks ..... 53
    - Predefined ICMP signatures ..... 53
    - ICMP sweep anomalies ..... 56
  - Configuring ICMP sweep protection ..... 56
  - Suggested settings for different network conditions ..... 56

# Introduction

This chapter introduces you to FortiGate product name/technology and the following topics:

- [About the FortiGate Intrusion Prevention System](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

## About the FortiGate Intrusion Prevention System

Spam and viruses are not the only threats facing enterprises and small businesses. Sophisticated, automated attack tools are prevalent on the Internet today, making intrusion detection and prevention vital to securing corporate networks. An attack or intrusion can be launched to steal confidential information, force a costly web site crash, or use network resources to launch other attacks.

The FortiGate Intrusion Prevention System (IPS) detects intrusions using attack signatures for known intrusion methods, and detects anomalies in network traffic to identify new or unknown intrusions. Not only can the IPS detect and log attacks, users can choose one of eight actions to take on the session when an attack is detected. This Guide describes how to configure and use the IPS and the IPS response to some common attacks.

## About this document

This document contains the following chapters:

- [IPS Overview and General Configuration](#)
- [Predefined Signatures](#)
- [Custom Signatures](#)
- [Anomalies](#)
- [SYN Flood Attacks](#)
- [ICMP Sweep Attacks](#)

## Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*  
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*  
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*  
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*  
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*  
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*  
Available exclusively from the [Fortinet Knowledge Center](#), the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*  
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*  
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPsec VPN User Guide*  
Provides step-by-step instructions for configuring IPsec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*  
Compares FortiGate IPsec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*  
Explains how to configure a PPTP VPN using the web-based manager.

- *FortiGate Certificate Management User Guide*  
Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*  
Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

### **Fortinet Knowledge Center**

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

### **Comments on Fortinet technical documentation**

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to [techdoc@fortinet.com](mailto:techdoc@fortinet.com).

## **Customer service and technical support**

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.



# IPS Overview and General Configuration

This section describes:

- [IPS overview](#)
- [Network performance](#)
- [Monitoring the network and dealing with attacks](#)
- [Using IPS in a protection profile](#)

## IPS overview

An IPS is an Intrusion Prevention System for networks. While early systems focused on intrusion detection, the continuing rapid growth of the Internet, and the potential for the theft of sensitive data, has resulted in the need for not only detection, but prevention.

### The FortiGate IPS

The FortiGate IPS combines detection using signatures, prevention by recognizing network anomalies, and the ability to block attacks by selecting the action to take when an attack or anomaly is detected. The attack can pass through or the session can be ended in a variety of ways, including sending TCP resets to the client, server, or both. All attacks can be logged regardless of the action applied.

Both the IPS predefined signatures and the IPS engine are upgraded through the FortiResponse Distribution Network (FDN). Anomalies are updated with firmware upgrades. The FortiGate IPS default settings implement the recommended settings for all signatures and anomalies. Signature settings and some anomaly thresholds are adjusted to work best with the normal traffic on the protected networks. Custom signatures can be created for the FortiGate IPS in diverse network environments.

Administrators are notified of intrusions and possible intrusions using log messages and alert email.

Configure the IPS globally using either the web-based manager or the CLI, then enable or disable all signatures or all anomalies in individual firewall protection profiles. [Table 1](#) describes the IPS settings and where to configure and access them in the web-based manager.

**Table 1: IPS and Protection Profile IPS configuration**

Protection Profile IPS options	IPS setting
IPS Signature	IPS > Signature
Enable or disable IPS signatures by severity level.	View and configure a list of predefined signatures. Create custom signatures based on the network requirements.
IPS Anomaly	IPS > Anomaly
Enable or disable IPS anomalies by severity level.	View and configure a list of predefined anomalies.
Log Intrusions	IPS > Signature > [individual signature] IPS > Anomaly > [individual anomaly]
Enable logging of all signature and anomaly intrusions.	Enable packet logging for each signature or anomaly.

See [“Using IPS in a protection profile” on page 16](#) or see the Firewall chapter in the *FortiGate Administration Guide* for complete protection profile and firewall policy procedures.

To access protection profile IPS options, go to Firewall > Protection Profile, select Edit or Create New, and select IPS.

For detailed information on individual signatures and anomalies, see the Vulnerability Encyclopedia in the FortiGuard Center available on the Fortinet web site at <http://www.fortinet.com/FortiGuardCenter/>.

## When to use IPS

IPS is best for large networks or for networks protecting highly sensitive information. Using IPS effectively requires monitoring and analysis of the attack logs to determine the nature and threat level of an attack. An administrator can adjust the threshold levels to ensure a balance between performance and intrusion prevention. Small businesses and home offices without network administrators may be overrun with attack log messages and not have the networking background required to configure the thresholds and other IPS settings. In addition, the other protection features in the FortiGate unit, such as antivirus (including grayware), spam filters, and web filters offer excellent protection for all networks.

## Network performance

The FortiGate IPS is extremely accurate and reliable as an in-line network device. Independent testing shows that the FortiGate IPS successfully detects and blocks attacks even under high traffic loads, while keeping latency within expected limits.

This section describes:

[Default signature and anomaly settings](#)

[Configuring system settings](#)

## Default signature and anomaly settings

The FortiGate IPS default settings implement the recommended settings for all signatures and anomalies. Most signatures are enabled, although some are set to pass but log detected sessions to avoid blocking legitimate traffic on most networks.

Adjust the IPS settings according to the traffic and applications on your network. For instance, if POP3 is not in use, disable the pop3 signature group.

## Configuring system settings

The following CLI commands that are relevant to the IPS have been added. the command `system autoupdate ips` is new for MR10.

### system autoupdate ips

When the IPS is updated, user-modified settings are retained. If recommended IPS signature settings have not been modified, and the updated settings are different, signature settings will be set according to `accept-recommended-settings`.

#### Command syntax pattern

```
config sys autoupdate ips
    set accept-recommended-settings {enable | disable}
end
```

Keywords and variables	Description	Default
accept-recommended-settings {enable   disable}	Enter enable to take new signature settings from the new default settings. Enter disable to retain modified signature settings.	disable

### system global ips-open

If for any reason the IPS should cease to function, it will fail open by default. This means crucial network traffic will not be blocked, and the Firewall will continue to operate while the problem is resolved.

#### Command syntax pattern

```
config sys global
    set ips-open {enable | disable}
end
```

Enable `ips_open` to cause the IPS to fail open, and disable `ips_open` to cause the IPS to fail closed.

Keywords and variables	Description	Default
ips-open {enable   disable}	If for any reason the IPS should cease to function, it will fail open by default. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved.	enable

### system global ip\_signature

Save system resources by restricting IPS processing to only those services allowed by firewall policies.

#### Command syntax pattern

```
config sys global
  set ip_signature {enable | disable}
end
```

Keywords and variables	Description	Default
ip_signature {enable   disable}	Enter one of the following: disable <ul style="list-style-type: none"> <li>only TCP, UDP and ICMP packets are processed by IPS signatures.</li> </ul> enable <ul style="list-style-type: none"> <li>other protocols in addition to TCP, UDP, and ICMP are processed by IPS signatures.</li> </ul>	disable

### system global ips-size

Set the size of the IPS buffer.

#### Command syntax pattern

```
config sys global
  set ips-size <ips_buffer_size>
end
```

Keywords and variables	Description	Default
ips-size <ips_buffer_size>	Set IPS buffer size. The default value is correct in most cases.	model-dependent

## Monitoring the network and dealing with attacks

After configuring IPS and enabling it in protection profiles, it is time to set up tracking and notification of attacks. Enabling logging and alert email maintain user awareness of attacks on the network.

The next step is dealing with attacks if and when they occur. The FortiGuard Center at <http://www.fortinet.com/FortiGuardCenter/> provides a comprehensive Vulnerability Encyclopedia to help decide what actions to take to further protect your network.

This section describes:

- [Configuring logging and alert email](#)
- [Attack log messages](#)
- [The FortiGuard Center](#)

## Configuring logging and alert email

Whenever the IPS detects or prevents an attack, it generates an attack log message that can be recorded or sent as an alert email.

The FortiGate unit categorizes attack log messages by signature or anomaly and includes the attack name in the log message. Enable logging and alert email for attack signatures and attack anomalies.



**Note:** Attack and intrusion attempts occur frequently on networks connected to the Internet. Reduce the number of log messages and alert email by disabling signatures for attacks that the system is not vulnerable to (for example, web attacks when not running a web server).

**Figure 1: Attack log filter options**

Log Filter							
	Check all	Fortilog	Disk	Memory	Syslog	WebTrends	Alert E-mail
▶ Traffic Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Event Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Anti-virus Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Web Filter Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ Attack Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack signature	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attack anomaly	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Spam Filter Log	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### To configure logging and alert email for IPS events using the web-based manager

- 1 Go to **Log&Report > Log Config > Log Setting**.
- 2 Select and configure the settings for any logging locations to use.
- 3 Select **Apply**.
- 4 Go to **Log&Report > Log Config > Alert Email**.
- 5 Select and configure authentication if required and enter the email addresses that will receive the alert email.
- 6 Enter the time interval to wait before sending log messages for each logging severity level.



**Note:** If more than one log message is collected before an interval is reached, the messages are combined and sent out as one alert email.

- 7 Select **Apply**.

- 8 Go to **Log&Report > Log Config > Log Filter**.
- 9 Enable signature and anomaly Attack Filter Log options, and enable logging for the appropriate traffic types to each log location and for alert email.
- 10 Select Apply.

#### To access log messages from memory or on the local disk

View and download log messages stored in memory or on the FortiGate local disk from the web-based manager. Go to **Log&Report > Log Access** and select the log type to view.

See the *FortiGate Administration Guide* and the *FortiGate Log Message Reference Guide* for more logging procedures.

## Attack log messages

### Signature

The following log message is generated when an attack signature is found:

---

<b>Message ID:</b>	70000
<b>Severity:</b>	Alert
<b>Message:</b>	attack_id=<value_attack_id> src=<ip_address> dst=<ip_address> src_port=<port_num> dst_port=<port_num> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session   detected   dropped   reset} proto=<protocol_num> service=<network_service> msg="<string><[url]>"
<b>Example:</b>	2004-07-07 16:21:18 log_id=0420073000 type=ips subtype=signature pri=alert attack_id=101318674 src=8.8.120.254 dst=11.1.1.254 src_port=2217 dst_port=25 interface=internal src_int=n/a dst_int=n/a status=reset proto=6 service=smtp msg="signature: Dagger.1.4.0.Drives [Reference: <a href="http://www.fortinet.com/ids/ID101318674">http://www.fortinet.com/ids/ID101318674</a> ]"
<b>Meaning:</b>	Attack signature message providing the source and destination addressing information and the attack name.
<b>Action:</b>	Get more information about the attack and the steps to take from the Fortinet Vulnerability Encyclopedia in the FortiGuard Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Vulnerability Encyclopedia.

---

## Anomaly

The following log message is generated when an attack anomaly is detected:

---

<b>Message ID:</b>	73001
<b>Severity:</b>	Alert
<b>Message:</b>	attack_id=<value_attack_id> src=<ip_address> dst=<ip_address> src_port=<port_num> dst_port=<port_num> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session   detected   dropped   reset} proto=<protocol_num> service=<network_service> msg="<string><[url]>"
<b>Example:</b>	2004-04-07 13:58:53 log_id=0420073001 type=ips subtype=anomaly pri=alert attack_id=100663396 src=8.8.120.254 dst=11.1.1.254 src_port=2217 dst_port=25 interface=internal src_int=n/a dst_int=n/a status=reset proto=6 service=smtp msg="anomaly: syn_flood, 100 > threshold 10.[Reference: http://www.fortinet.com/ids/ID100663396]"
<b>Meaning:</b>	Attack anomaly message providing the source and destination addressing information and the attack name.
<b>Action:</b>	Get more information about the attack and the steps to take from the Fortinet Vulnerability Encyclopedia in the FortiGuard Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Vulnerability Encyclopedia.

---

## The FortiGuard Center

The FortiGuard Center combines the knowledge base of the Fortinet technical team into an easily searchable database. FortiGuard Center includes both virus and attack information. Go to <http://www.fortinet.com/FortiGuardCenter/>.

Search for attacks in the FortiGuardCenter Vulnerability Encyclopedia by any of the criteria shown in [Figure 2](#).

**Figure 2: Searching the FortiGuard Vulnerability Encyclopedia**

The screenshot shows a search interface titled "Attack Description Search". It contains the following fields and controls:

- By Name:
- By ID:
- By Key Words:
- By Class:
- By CVE ID:
- By MS Bulletin ID:
- By BugTraq ID:
- Results Per Page:
- Search:

Type in the name or ID of the attack, or copy and paste the URL from the log message or alert email into a browser.

The Vulnerability Encyclopedia lists the following information for each signature:

<b>Description</b>	Background information and an explanation of what behavior the signature detects.
<b>Impact</b>	Describes the possible results of the attack.
<b>Vulnerability</b>	Lists operating systems, network equipment, or connection types that are vulnerable to the attack.
<b>References</b>	Links to more information sources about the signature or attack.
<b>Recommended Actions</b>	The actions to take if the signature is triggered.

## Using IPS in a protection profile

IPS can be combined with other FortiGate features – antivirus, spam filtering, web filtering, and web category filtering – to create protection profiles. Protection profiles are then added to individual user groups and then to firewall policies, or added directly to firewall policies.

### IPS protection profile options

Figure 3: Protection profile IPS options

IPS	
IPS Signature	<input type="checkbox"/> Enable (All services)
IPS Anomaly	<input type="checkbox"/> Enable (All services)

The following options are available for IPS through the protection profile:

<b>IPS Signature</b>	Enable or disable signature-based intrusion detection and prevention for all protocols.
<b>IPS Anomaly</b>	Enable or disable anomaly-based intrusion detection and prevention for all protocols.



**Note:** Some popular email clients cannot filter messages based on the MIME header. Check email client features before deciding how to tag spam.

### Creating a protection profile that uses IPS

To create a protection profile using the web-based manager

- 1 Go to **Firewall > Protection Profile**.
- 2 Select Create New.
- 3 Enter a name for the protection profile.
- 4 Expand the IPS option list.
- 5 Enable IPS Signature and IPS Anomaly.
- 6 Configure any other required protection profile options.

**7** Select OK.

The protection profile can now be added to any firewall policies that require it. The protection profile can also be added to user groups and these user groups can be used to apply authentication to firewall policies.

**To create a protection profile using the CLI**

This example creates a protection profile called IPS\_Special with both signatures and anomalies enabled.

```
config firewall profile
  edit IPS_Special
    set ips signature anomaly
  end
```

**Adding protection profiles to firewall policies**

Adding a protection profile to a firewall policy applies the profile settings, including IPS, to traffic matching that policy.

**Adding protection profiles to user groups**

When creating a user group, select a protection profile that applies to that group. Then, when configuring a firewall policy that includes user authentication, select one or more user groups to authenticate. Each user group selected for authentication in the firewall policy can have a different protection profile, and therefore different IPS settings, applied to it.



# Predefined Signatures

This section describes:

- [Predefined signatures overview](#)
- [Viewing the predefined signature list](#)
- [Predefined signature configuration](#)

## Predefined signatures overview

When the FortiGate unit installs an updated attack definition file, it checks to see if the default configuration for any existing signatures has changed. If the default configuration has changed, the changes are preserved.

Signatures are arranged into groups based on the type of attack. By default, all signature groups are enabled, although some individual signatures are disabled.

Enable or disable signature groups or individual signatures. Disabling unneeded signatures can improve system performance and reduce the number of log messages and alert emails that the IPS generates. For example, the IPS detects a large number of web server attacks. If there is no access to a web server behind the FortiGate unit, disable all web server attack signatures.

Some signature groups include configurable parameters. The parameters depend on the type of signatures in the signature group. When configuring these parameters for a signature group, the parameters apply to all of the signatures in the group.

For each signature, pass (let through) or block attacks by configuring the action the FortiGate IPS takes when it detects an attack. The FortiGate IPS can pass, drop, reset or clear packets or sessions.

Configure the FortiGate unit to check automatically for and download an updated attack definition file containing the latest signatures, or manually download the updated attack definition file. Configure the FortiGate unit to allow push updates of new attack definition files as soon as they are available from the FortiGuard Distribution Network. For details, see the *FortiGate Administration Guide*.

## Viewing the predefined signature list

Enable or disable groups of predefined signatures and configure the settings for individual predefined signatures from the predefined signature list.

To view the predefined signature list using the web-based manager:

Go to **IPS > Signature > Predefined**.

**Figure 4: A portion of the predefined signature list**

Name	Enable	Logging	Action	Revision	Modify
▶ apache					
▶ backdoor					
▶ cgi					
▶ coldfusion					
▼ compromise					
OpenSSH.GOBBLER.B			Pass	2.135	
OpenSSH.GOBBLER.Response.*GOBBLE*			Reset Client	2.135	
OpenSSH.GOBBLER.Response.Uname			Pass	2.135	
▶ ddos					
▶ dns					
▶ dos					
▶ exploit					

<b>Group Name</b>	The signature group names.
<b>Enable</b>	The status of the signature group. A white check mark in a green circle indicates the signature group is enabled. A white X in a grey circle indicates the signature group is disabled.
<b>Logging</b>	The logging status for individual signatures. Click on the blue triangle to show the signature group members. A white check mark in a green circle indicates logging is enabled for the signature. A white X in a grey circle indicates logging is disabled for the signature.
<b>Action</b>	The action set for individual signatures. Click on the blue triangle to show the signature group members. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
<b>Revision</b>	The revision number for individual signatures. Click on the blue triangle to show the signature group members.
<b>Modify</b>	The Configure and Reset icons. Reset only appears when the default settings have been modified. Selecting Reset restores the default settings.

[Table 2](#) describes each possible action to take for predefined signatures.

**Table 2: Actions to select for each predefined signature**

<b>Action</b>	Select the action for the FortiGate unit to take when traffic triggers this signature.
Pass	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.

**Table 2: Actions to select for each predefined signature (Continued)**

Reset Client	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the client and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Server	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
Drop Session	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. For the remainder of this packet's firewall session, all follow-up packets are dropped.
Clear Session	When a packet triggers a signature, the FortiGate unit generates an alert and the session to which the packet belongs is removed from the session table immediately. No reset is sent. For TCP, all follow-up packets could be dropped. For UDP, all follow-up packets could trigger the firewall to create a new session.
Pass Session	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall. For the remainder of this packet's session, the IPS is bypassed by all follow-up packets.

**To view predefined signatures using the CLI**

View predefined signature lists one group at a time. This example shows how to view the signatures in the apache signature group.

```
get ips group apache
  name                : apache
rule:
  == [ Apache.DoS.2044 ]
  name: Apache.DoS.2044
  == [ LongSlash ]
  name: LongSlash
  == [ Worm.Infection.Chunked-Encoding ]
  name: Worm.Infection.Chunked-Encoding
status                : enable
```

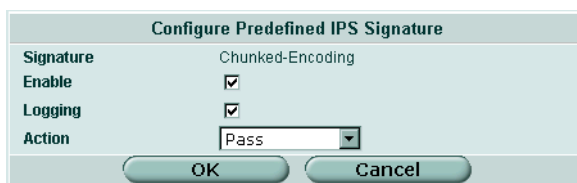
## Predefined signature configuration

This section describes:

- [Configuring individual signature settings](#)
- [Changing the status of predefined signature groups](#)
- [Configuring parameters for signature groups](#)
- [Configuring signatures using the CLI](#)

### Configuring individual signature settings

Figure 5: Configure Predefined IPS Signatures



Configure Predefined IPS Signature	
Signature	Chunked-Encoding
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Pass
OK Cancel	

#### To configure signature settings

- 1 Go to **IPS > Signatures > Predefined**.
- 2 Select the blue triangle next to a signature group name to display the members of that group.
- 3 Select Configure in the Modify column for the signature to configure.
- 4 Select Enable to enable the signature.
- 5 Select Logging to enable logging for the signature.
- 6 Select the Action for the FortiGate unit to take when traffic matches this signature.
- 7 Select OK.

#### To restore the recommended settings of a signature

- 1 Go to **IPS > Signatures > Predefined**.
- 2 Select the blue triangle next to a signature group name to display the members of that group.
- 3 Select Reset for the signature to restore to recommended settings.



**Note:** The Reset icon is only displayed if the settings for the signature have been changed from the default settings.

- 4 Select OK.

## Changing the status of predefined signature groups

Figure 6: Edit IPS Configuration



- Group Name** The signature group name.
- Enable** Select to enable the predefined signature group or clear to disable the predefined signature group.

### To enable predefined signature groups using the web-based manager

- 1 Go to **IPS > Signatures > Predefined**.
- 2 Select Configure next to the predefined signature to enable or disable.
- 3 Select Enable to enable the predefined signature group, or clear Enable to disable the predefined signature group.
- 4 Select OK.

## Configuring parameters for signature groups

The following predefined signature groups have configurable parameters.

- dns\_decoder
- ftp\_decoder
- http\_decoder
- im
- imap\_decoder
- p2p
- pop\_decoder
- rpc\_decoder
- smtp\_decoder
- snmp\_decoder
- tcp\_reassembler

### To configure signature group parameters using the web-based manager

Go to **IPS > Signature > Predefined**, expand a signature group, and select Edit for the signature to configure. When complete, select OK.

Figure 7: Example http\_decoder signature group parameters

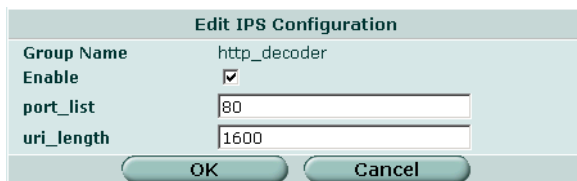


Figure 8: Example im signature group parameters

Edit IPS Configuration	
Group Name	im
Enable	<input checked="" type="checkbox"/>
codepoint	-1
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 9: Example p2p signature group parameters

Edit IPS Configuration	
Group Name	p2p
Enable	<input checked="" type="checkbox"/>
codepoint	-1
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 10: Example rpc\_decoder signature group parameters

Edit IPS Configuration	
Group Name	rpc_decoder
Enable	<input checked="" type="checkbox"/>
port_list	111, 32771
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 11: Example tcp\_reassembler signature group parameters

Edit IPS Configuration	
Group Name	tcp_reassembler
Enable	<input checked="" type="checkbox"/>
idle_timeout	120
min_ttl	10
port_list	21, 23, 25, 53, 80, 110, 111, 1
bad_flag_list	NULL, F, U, P, SF, PF, UP, UPF, I
direction	from-client
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- idle\_timeout** If a session is idle for longer than this number of seconds, the session will not be maintained by tcp\_reassembler.
- min\_ttl** A packet with a higher ttl number in its IP header than the number specified here is not processed by tcp\_reassembler.
- port\_list** A comma separated list of ports. The dissector can decode these TCP ports.
- bad\_flag\_list** A comma separated list of bad TCP flags.
- direction** Valid settings are from-server, from-client, or both.
- codepoint** A number from 0 to 63. Used for differentiated services tagging. When the action for p2p and im signatures is set to Pass, the FortiGate unit checks the codepoint. If the codepoint is set to a number from 1 to 63, the codepoint for the session is changed to the specified value. If the codepoint is set to -1 (the default) no change is made to the codepoint in the IP header.

## Configuring signatures using the CLI

Signatures are arranged into groups based on the type of attack. By default, all signature groups are enabled.

Enable or disable signature groups or individual signatures. Disabling unneeded signatures can improve system performance and reduce the number of log messages and alert emails that the IPS generates. For example, the IPS detects a large number of web server attacks. If there is no web server behind the FortiGate unit, disable all web server attack signatures.

Some signature groups include configurable parameters. The parameters that are available depend on the type of signatures in the signature group. When configured for a signature group, the parameters apply to all of the signatures in the group.

For each signature, configure the action the FortiGate IPS takes when it detects an attack. The FortiGate IPS can pass, drop, reset or clear packets or sessions. Also enable or disable logging of the attack.

The `config ips group` command has 1 subcommand.

### `config rule <rule-name_str>`

Access the `rule` subcommand using the `ips group` command. Use the `config rule` subcommand to configure the settings for individual signatures in a signature group.

### Command syntax pattern

```
config ips group <group_name_str>
  set bad_flag_list <flag_str>
  set codepoint <codepoint_integer>
  set direction <direction_str>
  set idle_timeout <timeout_integer>
  set min_ttl <ttn_integer>
  set port_list <port_integer>
  set status {enable | disable}
  config rule <rule_name_str>
    set action {clear_session | drop | drop_session | pass
  | pass_session | reset | reset_client | reset_server}
    set log {enable | disable}
    set status {enable | disable}
  end
end
```

Keywords and variables	Description	Default
<code>group_name_str</code>	The name of the group.	
<code>bad_flag_list</code> <code>&lt;flag_str&gt;</code>	A comma separated list of bad TCP flags. This applies to <code>tcp_reassembler</code> .	NULL, F, U, P, SF, PF, UP, UPF, UAPSF, UAPRSF

Keywords and variables	Description	Default
codepoint <codepoint_integer>	A number from 0 to 63. Used for differentiated services tagging. When the action for p2p and im signatures is set to <code>pass</code> , the FortiGate unit checks the codepoint. If the codepoint is set to a number from 1 to 63, the codepoint for the session is changed to the specified value. If the codepoint is set to -1 (the default) no change is made to the codepoint in the IP header. This applies to im and p2p signatures.	-1
direction <direction_str>	Valid settings are from-server, from-client, or both. This applies to tcp_reassembler.	from-client
idle_timeout <timeout_integer>	If a session is idle for longer than this number of seconds, the session is be maintained by tcp reassembly. This applies to tcp_reassembler.	30
min_ttl <ttn_integer>	A packet with a higher ttl number in its IP header than the number specified here is not processed by tcp reassembly. This applies to tcp_reassembler.	1
port_list <port_integer>	A comma separated list of ports. The dissector can decode these TCP ports. Default port lists: <ul style="list-style-type: none"> <li>• tcp_reassembler - 21, 23, 25, 53, 80, 110, 111, 143, 513,1837,1863,5050,5190</li> <li>• http_decoder - 80</li> <li>• rpc_decoder - 111, 32771</li> </ul> This applies to tcp_reassembler, http_decoder, and rpc_decoder.	Varies.
status {enable   disable}	Enable or disable this signature group.	enable
The following keywords and variables apply to config rule.		
rule_name_str	The name of the rule.	

Keywords and variables	Description	Default
<pre>action {clear_session   drop   drop_session   pass   pass_session   reset   reset_client   reset_server}</pre>	<p>Select an action for the FortiGate unit to take when traffic triggers this signature.</p> <p><code>clear_session</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature, removes the session from the FortiGate session table, and does not send a reset.</li> </ul> <p><code>drop</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature. Fortinet recommends using an action other than <code>drop</code> for TCP connection based attacks.</li> </ul> <p><code>drop_session</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature and drops any other packets in the same session.</li> </ul> <p><code>pass</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit lets the packet that triggered the signature pass through the firewall. If logging is disabled and action is set to Pass, the signature is effectively disabled.</li> </ul> <p><code>pass_session</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit lets the packet that triggered the signature and all other packets in the session pass through the firewall.</li> </ul> <p><code>reset</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as <code>clear_session</code>. If the <code>reset</code> action is triggered before the TCP connection is fully established it acts as <code>clear_session</code>.</li> </ul> <p><code>reset_client</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as <code>clear_session</code>. If the <code>reset_client</code> action is triggered before the TCP connection is fully established it acts as <code>clear_session</code>.</li> </ul> <p><code>reset_server</code></p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the signature, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as <code>clear_session</code>. If the <code>reset_server</code> action is triggered before the TCP connection is fully established it acts as <code>clear_session</code>.</li> </ul>	Varies.
<code>default_action</code>	The default action for the rule. This option is get only.	
<code>log {enable   disable}</code>	Enable or disable logging for the signature.	enable

Keywords and variables	Description	Default
rev <rev_integer>	The revision number of the rule. This option is get only.	
status {enable   disable}	Enable or disable this signature.	enable

This example shows how to change the action for the AddressMask signature in the icmp signature group to reset.

```
config ips group icmp
  config rule AddressMask
    set action reset
  end
end
```

This example shows how to disable the ftp signature group.

```
config ips group ftp
  set status disable
end
```

This example shows how to change the action for the NAPTHA signature in the dos signature group to drop.

```
config ips group dos
  config rule NAPTHA
    set action drop
  end
end
```

# Custom Signatures

Custom signatures provide the power and flexibility to customize the FortiGate IPS for diverse network environments. The FortiGate predefined signatures cover common attacks. If an unusual or specialized application or an uncommon platform is being used, add custom signatures based on the security alerts released by the application and platform vendors.

Use custom signatures to block or allow specific traffic. For example, to block traffic containing pornography, add custom signatures similar to the following:

F-SBID (--protocol tcp; --flow established; --content "nude cheerleader"; --no\_case)

This chapter describes:

- [Viewing custom signatures](#)
- [Custom signature configuration](#)
- [Backing up and restoring the custom signature list](#)
- [Creating custom signatures](#)

## Viewing custom signatures

To view the custom signature list, go to **IPS > Signature > Custom**.

**Figure 12: Custom signatures**

Name	Revision	Enable	Logging	Action	Modify
ICMP10	2	<input checked="" type="checkbox"/>		Pass	

**Enable custom signature** Select to enable the custom signature group or clear to disable the custom signature group.

**Create New** Select to create a new custom signature.

**Clear all custom signatures** Remove all the custom signatures from the custom signature group.

**Reset to recommended settings?** Reset all the custom signatures to the recommended settings.

**Name** The custom signature names.

<b>Revision</b>	The revision number for each custom signature. The signature revision number is updated when you revise a signature.
<b>Enable</b>	The status of each custom signature. A white check mark in a green circle indicates the signature is enabled. A white X in a grey circle indicates the signature is disabled. Selecting the box at the top of the Enable column enables all the custom signatures. Clearing the box at the top of the Enable column disables all the custom signatures.
<b>Logging</b>	The logging status of each custom signature. A white check mark in a green circle indicates logging is enabled for the custom signature. A white X in a grey circle indicates logging is disabled for the custom signature.
<b>Action</b>	The action set for each custom signature. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
<b>Modify</b>	The Delete and Edit/View icons.

#### To view custom signatures using the CLI

```
get ips custom
```

## Custom signature configuration

Add custom signatures using the web-based manager or the CLI. For more information about custom signature syntax, see [“Creating custom signatures” on page 33](#) and [“Custom signature syntax” on page 35](#).

### Adding custom signatures using the web-based manager

Figure 13: Edit custom signature

<b>Name</b>	Enter a name for the custom signature.
<b>Signature</b>	Enter the custom signature.

<b>Action</b>	Select the action for the FortiGate unit to take when traffic matches this signature.
<b>Pass</b>	The FortiGate unit lets the packet that triggered the signature pass through the firewall. If logging is disabled and action is set to Pass, the signature is effectively disabled.
<b>Drop</b>	The FortiGate unit drops the packet that triggered the signature. Fortinet recommends using an action other than Drop for TCP connection based attacks.
<b>Reset</b>	The FortiGate unit drops the packet that triggered the signature, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Reset Client</b>	The FortiGate unit drops the packet that triggered the signature, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Reset Server</b>	The FortiGate unit drops the packet that triggered the signature, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Drop Session</b>	The FortiGate unit drops the packet that triggered the signature and drops any other packets in the same session.
<b>Clear Session</b>	The FortiGate unit drops the packet that triggered the signature, removes the session from the FortiGate session table, and does not send a reset.
<b>Pass Session</b>	The FortiGate unit lets the packet that triggered the signature and all other packets in the session pass through the firewall.
<b>Logging</b>	Enable or disable logging for the custom signature.

#### To add a custom signature using the web-based manager

- 1 Go to **IPS > Signature > Custom**.
- 2 Select Create New to add a new custom signature, or select Edit to edit a custom signature.
- 3 Enter a name for the custom signature.  
The name of a custom signature cannot be edited.
- 4 Enter the custom signature.
- 5 Select the Action to take when a packet triggers this signature.
- 6 Select the Logging box to enable logging for the custom signature, or clear the Logging box to disable logging for the custom signature.

## Adding custom signatures using the CLI

After adding the custom signature, configure the settings for it under the signature group named custom. For more information about configuring signature groups, see [“Configuring signatures using the CLI” on page 25](#).

```

config ips custom
  edit <name_str>
    set signature <'signature_str'>
  end
end

```

Keywords and variables	Description	Default
name_str	The name of the custom signature.	
signature <'signature_str'>	Enter the custom signature. The signature must be enclosed in single quotes.	No default.

This example shows how to add an example signature called icmp\_10.

```

config ips custom
  edit icmp_10
    set signature 'F-SBID(--protocol icmp; --icmp_type 10; --
revision 2; )'
  end

```


























## Backing up and restoring the custom signature list

The custom signature list can be backed up and restored by going to System > Maintenance > Backup & Restore.



**Caution:** Restoring the custom signature list overwrites the existing file.

**Figure 14: Backup and restore custom signature lists**

Category	Latest Backup	
All Configuration Files	-	 
System settings		
System Configuration	-	 
Debug Log	-	
Web Filtering		
Web Content Block	-	 
Web URL Block List	-	 
Web URL Exempt List	-	 
Spam Filtering		
IP Address	-	 
RBL & ORDBL	-	 
Email Address	-	 
MIME Headers	-	 
Banned Word	-	 
IPS Signatures		
IPS User-Defined Signatures	-	 
VPN Certificates		
All Certificates	-	 

## Creating custom signatures

A custom signature definition should be less than 1000 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.

A custom signature definition begins with a header, followed by a set of keyword and value pairs enclosed by parenthesis [ ( ) ]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE ;)

KEYWORD VALUE ; can be repeated up to 64 times until all the parameters needed for the signature are included.

### Example

The following example signature checks that the ip\_flag header in TCP packets has the Don't Fragment bit set:

```
F-SBID(--name testflag; --protocol tcp; --ip_flag D;)
```

The example signature generates the following traffic:

```
# sendip -p ipv4 -p tcp -is 192.168.5.37 -ifd 1 -ts 5566 -td 1234 -tfs 1 192.168.5.40
```

If logging is enabled, when the signature is triggered the IPS records an attack log message similar to the following:

```
1 2004-09-02 01:19:52 log_id=0420070000 type=ips subtype=signature pri=alert
attack_id=113770497 src=192.168.5.37 dst=192.168.5.40 src_port=5598
dst_port=1234 src_int=ha dst_int=dmz status=detected proto=6 service=1234/tcp
msg="custom: testflag"
```

Set the action to Drop Session.

## Custom signature fields

Table 3 shows the valid characters for custom signature fields.

**Table 3: Valid characters for custom signature fields**

Field	Valid Characters	Usage
<b>HEADER</b>	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.
<b>KEYWORD</b>	A keyword must start with "--", and be a string of greater of 1 to 19 characters. Normally, keywords are an English word or English words connected by "_". Letters are usually lower case; however, keywords are case insensitive.	The keyword is used to identify a parameter. See <a href="#">"Custom signature syntax" on page 35</a> for tables of supported keywords.
<b>VALUE</b>	Double quotes must be used around the value if it contains a space and/or a semicolon. If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: if double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	Set the value for a parameter identified by a keyword.

## Custom signature syntax

**Table 4: General keywords**

Keyword	Value	Usage
<b>name</b>	A string of greater than 0 and less than 64. Normally, the group name is an English word or English words connected by <code>_</code> . All letters are normally lower case. If included, the name must match the name input using the GUI or CLI.	Because the name identifies the signature for the user, it should be easily readable and should be unique. The name keyword is optional for custom signatures.
<b>default_action</b>	[pass   pass_session   drop   drop_session   reset   reset_client   reset_server   clear_session]	The recommended action for a signature. The default action is pass.
<b>protocol</b>	ip; tcp; icmp; udp;	The protocol name.
<b>revision</b>	An integer.	Optional. A revision number for this signature.

**Table 5: Content specific keywords**

Keyword	Value	Usage
<b>content</b>	[!] "<content string>"; A string quoted within double quotes. Optionally place an exclamation mark (!) before the first double quote to express "Not".	The content contained in the packet payload. Multiple contents can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe ( ) character. The following characters in the content string must be escaped using a back slash: double quote ("), pipe sign( ) and colon(:).
<b>uri</b>	Same as content.	Search for the normalized request URI field. Binary data can be defined as the URI value.
<b>offset</b>	<number>; An integer (0-65535).	Start looking for the contents after the specified number of bytes of the payload. This tag is an absolute value in the payload. Follow the offset tag with the depth tag to stop looking for a match after the value specified by the depth tag. If there is no depth specified, continue looking for a match until the end of the payload.

**Table 5: Content specific keywords (Continued)**

<b>depth</b>	<number>; An integer (1-65535).	Look for the contents within the specified number of bytes of the payload. If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched. If depth is used without a preceding "offset", it is equal to a "-offset 0" there.
<b>distance</b>	<number>; An integer (0-65535).	Search for the contents the specified number of bytes relative to the end of the previously matched contents. The distance tag could be followed with the within tag. If there is no value specified for the within tag, continue looking for a match until the end of the payload.
<b>within</b>	<number>; An integer (1-65535).	Look for the contents within the specified number of bytes of the payload. Use with the distance tag.
<b>no_case</b>	NULL	Ignore case in the content value.
<b>raw</b>	NULL	Ignore any decoding. Look at the raw packet data.
<b>regex</b>	NULL	Regular expressions are used in the contents. An asterisk (*) in the content string means any character, any number of times. A question mark (?) means any single character.
<b>byte_test</b>	<bytes_to_convert>, <operator>, <value>, <offset> [, [relative,, [big,] [little,] [string,] [hex,] [dec,] [oct]]; Test a byte field against a specific value (with operator). Capable of testing binary values or converting representative byte strings to their binary equivalent and testing them.	<p><b>bytes_to_convert</b></p> <ul style="list-style-type: none"> <li>- The number of bytes to pick up from the packet.</li> </ul> <p><b>operator</b></p> <ul style="list-style-type: none"> <li>- The operation to perform to test the value (&lt;, &gt;, =, !, &amp;).</li> </ul> <p><b>value</b></p> <ul style="list-style-type: none"> <li>- The value to test the converted value against.</li> </ul> <p><b>offset</b></p> <ul style="list-style-type: none"> <li>- The number of bytes into the payload to start processing.</li> </ul> <p><b>relative</b></p> <ul style="list-style-type: none"> <li>- Use an offset relative to last pattern match.</li> </ul> <p><b>big</b></p> <ul style="list-style-type: none"> <li>- Process the data as big endian (default).</li> </ul> <p><b>little</b></p> <ul style="list-style-type: none"> <li>- Process the data as little endian.</li> </ul> <p><b>string</b></p> <ul style="list-style-type: none"> <li>- The data is stored in string format in the packet.</li> </ul> <p><b>hex</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in hexadecimal.</li> </ul> <p><b>dec</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in decimal.</li> </ul> <p><b>oct</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in octal.</li> </ul>

**Table 5: Content specific keywords (Continued)**

<p><b>byte_jump</b></p>	<p>&lt;bytes_to_convert&gt;, &lt;offset&gt; [, [relative,] [big,] [little,] [string,] [hex,] [dec,] [oct,] [align]];</p> <p>The byte_jump option is used to get a specified number of bytes, convert them to their numeric representation, and jump the doe_ptr up that many bytes for further pattern matching/byte_testing. This allows relative pattern matches to take into account numerical values found in network data.</p>	<p><b>bytes_to_convert</b></p> <ul style="list-style-type: none"> <li>- The number of bytes to pick up from the packet.</li> </ul> <p><b>offset</b></p> <ul style="list-style-type: none"> <li>- The number of bytes into the payload to start processing.</li> </ul> <p><b>relative</b></p> <ul style="list-style-type: none"> <li>- Use an offset relative to the last pattern match.</li> </ul> <p><b>big</b></p> <ul style="list-style-type: none"> <li>- Process the data as big endian (default).</li> </ul> <p><b>little</b></p> <ul style="list-style-type: none"> <li>- Process data as little endian.</li> </ul> <p><b>string</b></p> <ul style="list-style-type: none"> <li>- The data is stored in string format in the packet.</li> </ul> <p><b>hex</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in hexadecimal.</li> </ul> <p><b>dec</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in decimal.</li> </ul> <p><b>oct</b></p> <ul style="list-style-type: none"> <li>- The converted string data is represented in octal.</li> </ul> <p><b>align</b></p> <ul style="list-style-type: none"> <li>- Round the number of converted bytes up to the next 32-bit boundary.</li> </ul>
-------------------------	---	---

**Table 5: Content specific keywords (Continued)**

<p><b>pcre</b></p>	<p>[!]"(/&lt;regex&gt;/ m&lt;delim&gt;&lt;regex&gt;&lt;delim&gt;)[ismxAEGRUB]";                  The pcre keyword allows you to write rules using perl compatible regular expressions (PCRE). For more information on using PCRE, see the PCRE web site at <a href="http://www.pcre.org">http://www.pcre.org</a>.                  The post-re modifiers set compile time flags for the regular expression.</p>	<p><b>i</b>                  - Case insensitive.  <b>s</b>                  - Include newlines in the dot metacharacter.  <b>m</b>                  - By default, the string is treated as one big line of characters. ^ and \$ match at the start and end of the string. When m is set, ^ and \$ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.  <b>x</b>                  - Whitespace data characters in the pattern are ignored except when escaped or inside a character class.  <b>A</b>                  - The pattern must match only at the start of the buffer (same as ^ ).  <b>E</b>                  - Set \$ to match only at the end of the subject string. Without E, \$ also matches immediately before the final character if it is a newline (but not before any other newlines).  <b>G</b>                  - Inverts the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by "?".  <b>R</b>                  - Match relative to the end of the last pattern match (similar to distance:0;).  <b>U</b>                  Match the decoded URI buffers (similar to the uri keyword).  <b>B</b>                  Do not use the decoded buffers (similar to the raw keyword).</p>
<p><b>data_at</b></p>	<p>&lt;value&gt; [,relative];</p>	<p>Verify that the payload has data at a specified location. Optionally look for data relative to the end of the previous content match.</p>

**Table 6: IP header keywords**

Keyword	Value	Usage
<b>ip_version</b>	<number>;	The IP version number.
<b>ihl</b>	<number>; An integer(5-15).	The IP header length.
<b>tos</b>	<number>;	Check the IP TOS field for the specified value.
<b>ip_id</b>	<number>;	Check the IP ID field for the specified value.

**Table 6: IP header keywords (Continued)**

<b>ip_option</b>	{rr   eol   nop   ts   sec   lsrr   ssrr   satid   any}	<p><b>rr</b> - Check if IP RR (record route) option is present.</p> <p><b>eol</b> - Check if IP EOL (end of list) option is present.</p> <p><b>nop</b> - Check if IP NOP (no op) option is present.</p> <p><b>ts</b> - Check if IP TS (time stamp) option is present.</p> <p><b>sec</b> - Check if IP SEC (IP security) option is present.</p> <p><b>lsrr</b> - Check if IP LSRR (loose source routing) option is present.</p> <p><b>ssrr</b> - Check if IP SSRR (strict source routing) option is present.</p> <p><b>satid</b> - Check if IP SATID (stream identifier) option is present.</p> <p><b>any</b> - Check if IP any option is present.</p>
<b>frag_offset</b>	<number>; !<number>; ><number>; <<number>;	Compare the IP fragment field against the specified value.
<b>ip_flag</b>	[!]<[MDR]>[+]*;	<p>Check if IP fragmentation and reserved bits are set in the IP header.</p> <p><b>M</b> - The More Fragments bit.</p> <p><b>D</b> - The Don't Fragment bit.</p> <p><b>R</b> The Reserved Bit.</p> <p><b>+</b> - Match on the specified bits, plus any others.</p> <p><b>*</b> - Match if any of the specified bits are set.</p> <p><b>!</b> - Match if the specified bits are not set.</p>
<b>ttl</b>	<number>; ><number>; <<number>;	Check the IP time-to-live value against the specified value.
<b>src_addr</b>	[!]<ip addresses or CIDR blocks>  You can define up to 28 IP address or CIDR blocks. Enclose the comma separated list in square brackets.	The source IP address.

**Table 6: IP header keywords (Continued)**

<b>dst_addr</b>	[!]<ip addresses or CIDR blocks> You can define up to 28 IP address or CIDR blocks. Enclose the comma separated list in square brackets.	The destination IP address.
<b>ip_proto</b>	<number>; [!]<number>; ><number>; <<number>;	Check the IP protocol header.

**Table 7: TCP header keywords**

Keyword	Value	Usage
<b>src_port</b>	[!]<number>; [!]:<number>; [!]<number>; [!]<number>:<number>;	The source port number.
<b>dst_port</b>	[!]<number> [!]:<number> [!]<number>: [!]<number>:<number>	The destination port number.
<b>tcp_flags</b>	[!*+]<FSRPAU120>[,<FSRPAU120>]; The first part (<FSRPAU120>) defines the bits that must present for a successful match. For example: --tcp_flags AP only matches the case where both A and P bits are set. The second part ([,<FSRPAU120>]) is optional, and defines the additional bits that can present for a match. For example: --tcp_flags S,12 matches the following combinations of flags: S, S and 1, S and 2, S and 1 and 2. The modifiers !, * and + can not be used in the second part.	Specify the TCP flags to match in a packet. <b>S</b> - Match the SYN flag. <b>A</b> - Match the ACK flag. <b>F</b> - Match the FIN flag. <b>R</b> - Match the RST flag. <b>U</b> - Match the URG flag. <b>P</b> - Match the PSH flag. <b>1</b> - Match Reserved bit 1. <b>2</b> - Match Reserved bit 2. <b>0</b> - Match No TCP flags set. <b>+</b> - Match on the specified bits, plus any others. <b>*</b> - Match if any of the specified bits are set. <b>!</b> - Match if the specified bits are not set.
<b>seq</b>	<number>;	Check for the specified TCP sequence number.

**Table 7: TCP header keywords (Continued)**

<b>ack</b>	<number>;	Check for the specified TCP acknowledge number.
<b>window_size</b>	[!]<number>; An integer in either hexadecimal or decimal. A hexadecimal value must be preceded by 0x.	Check for the specified TCP window size.

**Table 8: UDP header keywords**

<b>Keyword</b>	<b>Value</b>	<b>Usage</b>
<b>src_port</b>	[!]<number>; [!]:<number>; [!]<number>;; [!]<number>:<number>;	The source port number.
<b>dst_port</b>	[!]<number>; [!]:<number>; [!]<number>;; [!]<number>:<number>;	The destination port number.

**Table 9: ICMP keywords**

<b>Keyword</b>	<b>Value</b>	<b>Usage</b>
<b>icmp_type</b>	<number>;	Specify the ICMP type to match.
<b>icmp_code</b>	<number>;	Specify the ICMP code to match.
<b>icmp_id</b>	<number>;	Check for the specified ICMP ID value.
<b>icmp_seq</b>	<number>;	Check for the specified ICMP sequence value.

Table 10: Other keywords

Keyword	Value	Usage
<b>same_ip</b>	NULL	The source and the destination have the same IP addresses.
<b>rpc_num</b>	<application number>, [<version number>]*], [<procedure number>]*>;	Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.
<b>flow</b>	[to_client to_server from_client   from_server ]; established; bi_direction; [no_stream only_stream];	TCP only. The to_server value is equal to the from_client value. The to_client value is equal to the from_server value. The bi_direction tag makes the signature match traffic for both directions. For example, if you have a signature with "--dst_port 80", and with bi_direction set, the signature checks traffic from and to port 80.
<b>data_size</b>	< number; > number; < number; number <> number;	Test the packet payload size. With data_size specified, packet reassembly is turned off automatically. So a signature with data_size and only_stream values set is wrong.
<b>revision</b>	<number>;	The revision number of the attack signature.

# Anomalies

This section describes:

- [Anomalies overview](#)
- [Viewing the anomaly list](#)
- [Configuring an anomaly using the web-based manager](#)
- [Configuring an anomaly using the CLI](#)

## Anomalies overview

The FortiGate IPS uses anomaly detection to identify network traffic that does not fit known or preset traffic patterns. The FortiGate IPS identifies the four statistical anomaly types for the TCP, UDP, and ICMP protocols.

<b>Flooding</b>	If the number of sessions targeting a single destination in one second is over a threshold, the destination is experiencing flooding.
<b>Scan</b>	If the number of sessions from a single source in one second is over a threshold, the source is scanning.
<b>Source session limit</b>	If the number of concurrent sessions from a single source is over a threshold, the source session limit is reached.
<b>Destination session limit</b>	If the number of concurrent sessions to a single destination is over a threshold, the destination session limit is reached.

Enable or disable logging for each anomaly, and control the IPS action in response to detecting an anomaly. In many cases, configure the thresholds the anomaly uses to detect traffic patterns that could represent an attack.



**Note:** It is important to estimate the normal and expected traffic on the network before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could miss some attacks.







Configure session control based on source and destination network address. This is a CLI only command available for `tcp_src_session`, `tcp_dst_session`, `icmp_src_session`, `icmp_dst_session`, `udp_src_session`, `udp_dst_session`. For more information, see the *FortiGate CLI Reference Guide*.

The anomaly detection list can be updated only when the FortiGate firmware is upgraded.

## Viewing the anomaly list

To view the anomaly list, go to **IPS > Anomaly > Anomaly**.

**Figure 15: The Anomaly list**

Name	Enable	Logging	Action	Modify
syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	 
portscan	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Clear Session	 
syn_fin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Clear Session	 

<b>Name</b>	The anomaly names.
<b>Enable</b>	The status of the anomaly. A white check mark in a green circle indicates the anomaly is enabled. A white X in a grey circle indicates the anomaly is disabled.
<b>Logging</b>	The logging status for each anomaly. A white check mark in a green circle indicates logging is enabled for the anomaly. A white X in a grey circle indicates logging is disabled for the anomaly.
<b>Action</b>	The action set for each anomaly. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
<b>Modify</b>	The Edit and Reset icons. If you have changed the settings for an anomaly, you can use the Reset icon to change the settings back to the recommended settings.

### To view the anomaly list using the CLI

```
get ips anomaly
```

## Configuring an anomaly using the web-based manager

Each anomaly is preset with a recommended configuration. By default all anomaly signatures are enabled. Use the recommended configurations or modify the configurations to match the requirements of the network.

**Figure 16: Editing the portscan IPS Anomaly**

**Edit IPS Anomaly**

**Name** portscan

**Enable**

**Logging**

**Action**

---

**Parameters:**

threshold

**Figure 17: Editing the syn\_fin IPS Anomaly**

**Edit IPS Anomaly**

**Name** syn\_fin

**Enable**

**Logging**

**Action**

<b>Name</b>	The anomaly name.
<b>Enable</b>	Enable or disable the anomaly in the IPS.
<b>Logging</b>	Enable or disable logging for the anomaly.
<b>Action</b>	Select the action for the FortiGate unit to take when traffic triggers this anomaly.
<b>Pass</b>	The FortiGate unit lets the packet that triggered the anomaly pass through the firewall. If logging is disabled and action is set to Pass, the anomaly is effectively disabled.
<b>Drop</b>	The FortiGate unit drops the packet that triggered the anomaly. Fortinet recommends using an action other than Drop for TCP connection based attacks.
<b>Reset</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Reset Client</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Reset Server</b>	The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
<b>Drop Session</b>	The FortiGate unit drops the packet that triggered the anomaly and drops any other packets in the same session.
<b>Clear Session</b>	The FortiGate unit drops the packet that triggered the anomaly, removes the session from the FortiGate session table, and does not send a reset.
<b>Pass Session</b>	The FortiGate unit lets the packet that triggered the anomaly and all other packets in the session pass through the firewall.
<b>Threshold</b>	Traffic over the specified threshold triggers the anomaly.

#### To configure anomaly settings using the web-based manager

- 1 Go to **IPS > Anomaly > Anomaly**.
- 2 Select Edit for the signature to configure.
- 3 Select Enable to enable the anomaly, or clear Enable to disable the anomaly.
- 4 Select Logging to enable logging for this anomaly. or clear Logging to disable logging for this anomaly.
- 5 Select the Action for the FortiGate unit to take when traffic triggers this anomaly.
- 6 Enter a new threshold value if required.
- 7 Select OK.

#### To restore the default settings of an anomaly

- 1 Go to **IPS > Anomaly > Anomaly**.

- 2 Select Reset for the anomaly to restore to default.  
The Reset icon is displayed only if the settings for the anomaly have been changed from defaults.
- 3 Select OK.

## Configuring an anomaly using the CLI

The list of anomalies can be updated only when the FortiGate firmware image is upgraded.

The `config ips anomaly` command has 1 subcommand.

### config limit

Access the `config limit` subcommand using the `config ips anomaly <name_str>` command. Use this command for session control based on source and destination network address. This command is available for `tcp_src_session`, `tcp_dst_session`, `icmp_src_session`, `icmp_dst_session`, `udp_src_session`, and `udp_dst_session`.

The default entry cannot be edited. Addresses are matched from more specific to more general. For example, if thresholds are defined for `192.168.100.0/24` and `192.168.0.0/16`, the address with the 24 bit netmask is matched before the entry with the 16 bit netmask.

### Command syntax pattern

```
config ips anomaly
  set action {clear_session | drop | drop_session | pass |
  pass_session | reset | reset_client | reset_server}
  set default_action
  set log {disable | enable}
  set status {disable | enable}
  set threshold <threshold_integer>
  config limit
    set ipaddress <address_ipv4mask>
    set threshold <threshold_integer>
  end
end
```

Keywords and variables	Description	Default
action {clear_session   drop   drop_session   pass   pass_session   reset   reset_client   reset_server}	<p>Select an action for the FortiGate unit to take when traffic triggers this anomaly.</p> <p>clear_session</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly, removes the session from the FortiGate session table, and does not send a reset.</li> </ul> <p>drop</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly. Fortinet recommends using an action other than drop for TCP connection based attacks.</li> </ul> <p>drop_session</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly and drops any other packets in the same session.</li> </ul> <p>pass</p> <ul style="list-style-type: none"> <li>The FortiGate unit lets the packet that triggered the anomaly pass through the firewall. If logging is disabled and action is set to Pass, the anomaly is effectively disabled.</li> </ul> <p>pass_session</p> <ul style="list-style-type: none"> <li>The FortiGate unit lets the packet that triggered the anomaly and all other packets in the session pass through the firewall.</li> </ul> <p>reset</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly, sends a reset to both the client and the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as clear_session. If the Reset action is triggered before the TCP connection is fully established it acts as clear_session.</li> </ul> <p>reset_client</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the client, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as clear_session. If the reset_client action is triggered before the TCP connection is fully established it acts as clear_session.</li> </ul> <p>reset_server</p> <ul style="list-style-type: none"> <li>The FortiGate unit drops the packet that triggered the anomaly, sends a reset to the server, and removes the session from the FortiGate session table. Used for TCP connections only. If you set this action for non-TCP connection based attacks, the action behaves as clear_session. If the reset_server action is triggered before the TCP connection is fully established it acts as clear_session.</li> </ul>	Varies.
default_action	The default action for the anomaly.	
log {disable   enable}	Enable or disable logging for the anomaly.	enable

Keywords and variables	Description	Default
status {disable   enable}	Enable or disable this anomaly.	enable
threshold <threshold_integer>	For the anomalies that include the threshold setting, traffic over the specified threshold triggers the anomaly.	Varies.
the following keywords and variables are specific to config limit.		
ipaddress <address_ipv4mask>	The ip address and netmask of the source or destination network.	No default.
threshold <threshold_integer>	Set the threshold that triggers this anomaly.	No default.

This example shows how enable the icmp\_sweep anomaly and change the threshold to 85.

```
config ips anomaly icmp_sweep
    set status enable
    set threshold 85
end
```

This example shows how to change the tcp\_land anomaly configuration.

```
config ips anomaly tcp_land
    set action pass
    set log enable
    set status enable
end
```

This example shows how to change the icmp\_flood anomaly configuration.

```
config ips anomaly icmp_flood
    set action drop
    set log enable
    set status enable
    set threshold 1024
end
```

This example shows how to configure the limit for the tcp\_src\_session anomaly.

```
config ips anomaly tcp_src_session
config limit
    edit subnet1
        set ipaddress 1.1.1.0 255.255.255.0
        set threshold 300
    end
end
```

# SYN Flood Attacks

A SYN flood is a type of Denial of Service (DoS) attack. DoS is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an internet service, for example, a web server. Using SYN floods, an attacker attempts to disable an Internet service by flooding a server with TCP/IP connection requests which consume all the available slots in the server's TCP connection table. When the connection table is full, it is not possible to establish any new connections, and the web site on the server becomes inaccessible.

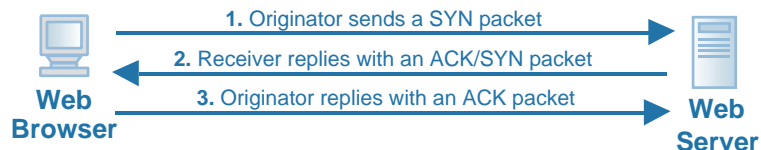
This section provides information about SYN flood attacks and the FortiGate IPS methods of preventing such attacks.

## How SYN floods work

SYN floods work by exploiting the structure of the TCP/IP protocol. An attacker floods a server with connection attempts but never acknowledges the server's replies to open the TCP/IP connection.

The TCP/IP protocol uses a three-step process to establish a network connection.

**Figure 18: Establishing a TCP/IP connection**



- 1 The originator of the connection sends a SYN packet (a packet with the SYN flag set in the TCP header) to initiate the connection.
- 2 The receiver sends a SYN/ACK packet (a packet with the SYN and ACK flags set in the TCP header) back to the originator to acknowledge the connection attempt.
- 3 The originator then sends an ACK packet (a packet with the ACK flag set in the TCP header) back to the receiver to open the connection.

After the handshaking process is complete the connection is open and data exchange can begin between the originator and the receiver, in this case the web browser and the web server.

Between steps 2 and 3 however, the web server keeps a record of any incomplete connections until it receives the ACK packet. A SYN flood attacker sends many SYN packets but never replies with the final ACK packet.

Since most systems have only a limited amount of space for TCP/IP connection records, a flood of incomplete connections will quickly block legitimate users from accessing the server. Most TCP/IP implementations use a fairly long timeout before incomplete connections are cleared from the connection table and traffic caused by a SYN flood is much higher than normal network traffic.

## The FortiGate IPS Response to SYN Flood Attacks

The FortiGate unit uses a defense method that combines the SYN Threshold and SYN Proxy methods to prevent SYN flood attacks.

### What is SYN threshold?

An IPS device establishes a limit on the number of incomplete TCP connections, and discards SYN packets if the number of incomplete connections reaches the limit.

### What is SYN proxy?

An IPS proxy device synthesizes and sends the SYN/ACK packet back to the originator, and waits for the final ACK packet. After the proxy device receives the ACK packet from the originator, the IPS device then "replays" the three-step sequence of establishing a TCP connection (SYN, SYN/ACK and ACK) to the receiver.

### How IPS works to prevent SYN floods

The FortiGate IPS uses a pseudo SYN proxy to prevent SYN flood attack. The pseudo SYN proxy is an incomplete SYN proxy that reduces resource usage and provides better performance than a full SYN proxy approach.

The IPS allows users to set a limit or threshold on the number of incomplete TCP connections. The threshold can be set either from the CLI or the web-based manager.

When the IPS detects that the total number of incomplete TCP connections to a particular target exceeds the threshold, the pseudo SYN proxy is triggered to operate for all subsequent TCP connections. The pseudo SYN proxy will determine whether a new TCP connection is a legitimate request or another SYN flood attack based on a "best-effect" algorithm. If a subsequent connection attempt is detected to be a normal TCP connection, the IPS will allow a TCP connection from the source to the target. If a subsequent TCP connection is detected to be a new incomplete TCP connection request, one of the following actions will be taken: Drop, Reset, Reset Client, Reset Server, Drop Session, Pass Session, Clear Session, depending upon the user configuration for SYN Flood anomaly in the IPS.

A true SYN proxy approach requires that all three packets (SYN, SYN/ACK, and ACK) are cached and replayed even before it is known if a TCP connection request is legitimate. The FortiGate IPS pseudo SYN proxy retransmits every TCP packet immediately from the packet source to the packet destination as soon as it records the necessary information for SYN flood detection.

Since the pseudo SYN proxy in the IPS uses a “best effect” algorithm to determine whether a TCP connection is legitimate or not, some legitimate connections may be falsely detected as incomplete TCP connection requests and dropped. However, the ratio of the pseudo SYN proxy dropping legitimate TCP connection is quite small.

Figure 19 illustrates the operational behavior of the FortiGate IPS Engine before the SYN Flood threshold is reached. Figure 20 illustrates the operation behavior of the FortiGate IPS Engine after the SYN Flood threshold is reached.

Figure 19: IPS operation before syn\_flood threshold is reached

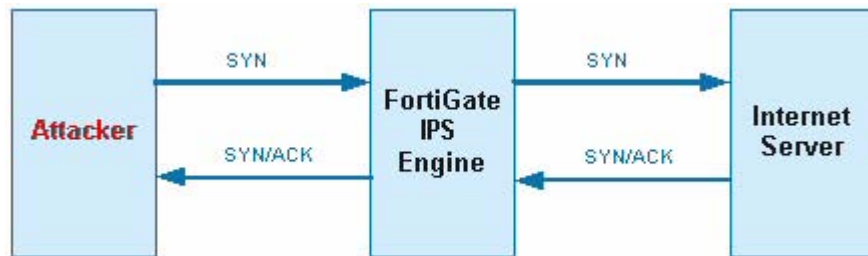
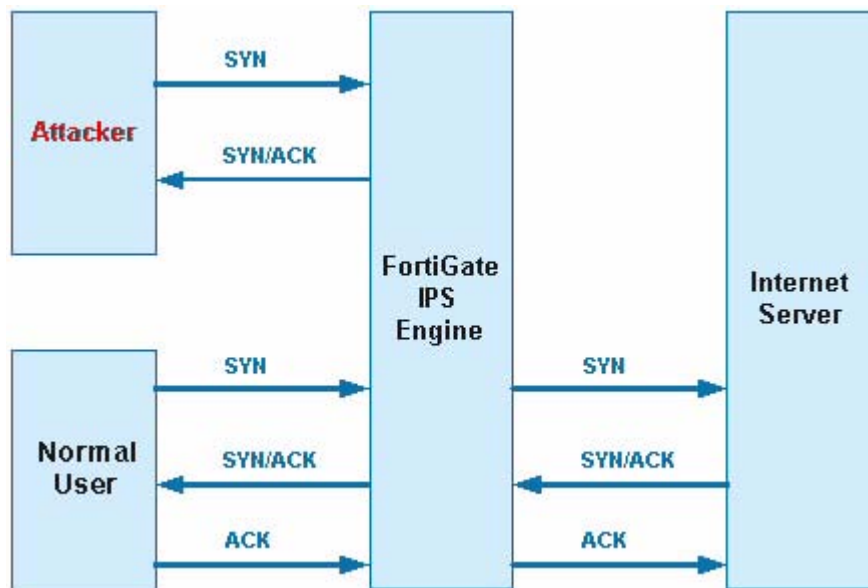


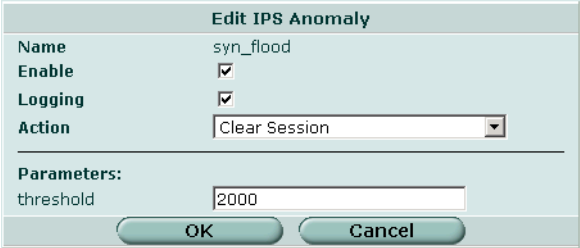
Figure 20: IPS operation after syn\_flood threshold is reached



## Configuring SYN flood protection

To set the configuration for the SYN flood anomaly in the web-based manager, go to **IPS->Anomaly**, find `syn_flood` in the anomaly list, and select Edit.

Figure 21: Configuring the `syn_flood` anomaly



The screenshot shows a web-based configuration window titled "Edit IPS Anomaly". The window contains the following fields and controls:

Edit IPS Anomaly	
Name	syn_flood
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Clear Session
Parameters:	
threshold	2000
OK Cancel	

See [“Anomalies” on page 43](#) for information about configuring anomalies.

## Suggested settings for different network conditions

The main setting that impacts the efficiency of the pseudo SYN proxy in detecting SYN floods is the threshold value. The default threshold is 2000. Select an appropriate value based on network conditions. Normally, if the servers being protected by the FortiGate unit need to handle heavier requests, such as a busy web server, the threshold should be set to a higher value. If the network carries lighter traffic, the threshold should be set to a lower value.

# ICMP Sweep Attacks

ICMP (Internet Control Message Protocol) is a part of the IP protocol and is generally used to send error messages describing packet routing problems. ICMP sweeps are not really considered attacks but are used to scan a target network to discover vulnerable hosts for further probing and possible attacks.

Attackers use automated tools that scan all possible IP addresses in the range of the target network to create a map which they can use to plan an attack.

## How ICMP sweep attacks work

An ICMP sweep is performed by sending ICMP echo requests - or other ICMP messages that require a reply - to multiple addresses on the target network. Live hosts will reply with an ICMP echo or other reply message. An ICMP sweep basically works the same as sending multiple pings. Live hosts accessible on the network must send a reply. This enables the attacker to determine which hosts are live and connected to the target network so further attacks and probing can be planned.

There are several ways of doing an ICMP sweep depending on the source operating system, and there are many automated tools for network scanning that attackers use to probe target networks.

## The FortiGate IPS response to ICMP sweep attacks

The FortiGate IPS provides predefined signatures to detect a variety of ICMP sweep methods. Each signature can be configured to pass, drop, or clear the session. Each signature can be configured to log when the signature is triggered.

Create custom signatures to block attacks specific to the network that are not included in the predefined signature list.

The FortiGate IPS also has an ICMP sweep anomaly setting with a configurable threshold.

## Predefined ICMP signatures

[Table 11](#) describes all the ICMP-related predefined signatures and the default settings for each. See [“Configuring individual signature settings” on page 22](#) for details about each possible signature action.



**Note:** The predefined signature descriptions in [Table 11](#) are accurate as of the IPS Guide publication date. Predefined signatures may be added or changed with each Attack Definition update.

**Table 11: Predefined ICMP sweep signatures**

Signature	Description	Default settings
<b>AddressMask</b>	AddressMask detects broadcast address mask request messages from a host pretending to be part of the network. The default action is to pass but log this traffic because it could be legitimate network traffic on some networks.	Signature enabled Logging enabled Action: Pass
<b>Broadscan.Smurf</b>	Broadscan is a hacking tool used to generate and broadcast ICMP requests in a smurf attack. In a smurf attack, an attacker broadcasts ICMP requests on Network A using a spoofed source IP address belonging to Network B. All hosts on Network A send multiple replies to Network B, which becomes flooded.	Signature enabled Logging enabled Action: Drop
<b>Communication.Administratively.Prohibited</b>	This signature detects network packets that have been blocked by some kind of filter. The host that blocked the packet sends an ICMP (code 13) Destination Unreachable message notifying the source or apparent source of the filtered packet. Since this signature may be triggered by legitimate traffic, the default action is to pass but log the traffic, so it can be monitored.	Signature enabled Logging enabled Action: Pass
<b>CyberKit.2.2</b>	CyberKit 2.2 is Windows-based software used to scan networks. ICMP echo request messages sent using this software contain special characters that identify Cyberkit as the source.	Signature enabled Logging enabled Action: Pass
<b>DigitalIsland.Bandwidth.Query</b>	Digital Island is a provider of content delivery networks. This company sends ICMP pings so they can better map routes for their customers. Use this signature to block their probes.	Signature enabled Logging enabled Action: Drop
<b>Echo.Reply</b>	This signature detects ICMP echo reply messages responding to ICMP echo request messages.	Signature disabled
<b>ISS.Pinger</b>	ISS is Internet Security Scanner software that can be used to send ICMP echo request messages and other network probes. While this software can be legitimately used to scan for security holes, use the signature to block unwanted scans.	Signature enabled Logging enabled Action: Drop
<b>Nemesis.V1.1.Echo</b>	Nemesis v1.1 is a Windows- or Unix-based scanning tool. ICMP echo request messages sent using this software contain special characters that identify Nemesis as the source.	Signature enabled Logging enabled Action: Drop
<b>Packet.Large</b>	This signature detects ICMP packets larger than 32 000 bytes, which can crash a server or cause it to hang.	Signature enabled Logging enabled Action: Pass

Table 11: Predefined ICMP sweep signatures

Signature	Description	Default settings
<b>PING.NMAP</b>	NMAP is a free open source network mapping/security tool that is available for most operating systems. NMAP could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify NMAP as the source.	Signature disabled
<b>Redirect.Code4</b>	This signature detects ICMP type 5 code 4 redirect messages. An ICMP redirect message describes an alternate route for traffic to take. An attacker may use ICMP redirect messages to alter the routing table or cause traffic to follow an unintended route.	Signature enabled Logging enabled Action: Pass
<b>Sniffer.Pro. NetXRay</b>	Sniffer Pro and NetXRay are scanning tools. ICMP echo request messages sent using this software contain special characters that identify them as the source.	Signature enabled Logging enabled Action: Drop
<b>Source.Quench</b>	This signature detects ICMP source quench messages. These messages are generated when a gateway cannot forward packets because the memory buffer is full. The gateway sends a source quench message back to the source to request that the transmission rate be reduced until it no longer receives source quench messages from the gateway. Attackers could use this type of message to slow down the network considerably.	Signature enabled Logging enabled Action: Drop
<b>Superscan.Echo</b>	Superscan is a free network scanning tool for Windows from Foundstone Inc. Superscan could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify Superscan as the source.	Signature enabled Logging enabled Action: Drop
<b>TimeStamp</b>	TimeStamp detects timestamp request messages from a host pretending to be part of the network.	Signature enabled Logging enabled Action: Pass
<b>TJPingPro1.1</b>	TJPingPro1.1 is a widely-used network tool for older versions of Windows. TJPingPro could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify TJPingPro as the source.	Signature enabled Logging enabled Action: Drop
<b>Traceroute</b>	Traceroute is a very common network tool available on almost any operating system. This tool could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify traceroute as the source.	Signature enabled Logging enabled Action: Pass
<b>Whatsup.Gold</b>	WhatsUp Gold is a network scanning tool for Windows from IPswitch. WhatsUp could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify WhatsUpGold as the source.	Signature enabled Logging enabled Action: Drop

## ICMP sweep anomalies

The FortiGate unit also detects ICMP sweeps that do not have a predefined signature to block them. The FortiGate IPS monitors traffic to ensure that ICMP messages do not exceed the default or user-defined threshold.

## Configuring ICMP sweep protection

To set the configuration for the various ICMP sweep attacks, go to **IPS > Signature** and expand the icmp list. Each signature can be configured individually.

Figure 22: Some of the ICMP signatures in the predefined signature list

▶ frontpage	✓						
▶ ftp	✓						
▼ icmp	✓						
AddressMask	✓	✓	Pass	2.1.36			
Broadscan.Smurf	✓	✓	Drop	2.1.36			
Communication.Administratively.Prohibited	✓	✓	Pass	2.1.36			
CyberKit.2.2	✓	✓	Pass	2.1.36			
DigitalIsland.Bandwidth.Query	✓	✓	Drop	2.1.36			
Echo.Reply	✓	✓	Pass	2.1.36			
ISS.Finger	✓	✓	Drop	2.1.36			
Nemesis.V1.1.Echo	✓	✓	Drop	2.1.36			

See “Predefined signatures overview” on page 19 for information about configuring predefined signatures.

To set the configuration for the ICMP sweep anomaly in the web-based manager, go to **IPS->Anomaly**, find icmp\_sweep in the anomaly list, and select Edit.

Figure 23: Configuring the icmp\_sweep anomaly

**Edit IPS Anomaly**

Name	icmp_sweep
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Clear Session

---

Parameters:

threshold	<input type="text" value="100"/>
-----------	----------------------------------

See “Anomalies” on page 43 for information about configuring anomalies.

## Suggested settings for different network conditions

Enable or disable the ICMP predefined signatures depending on current network traffic and the network scanning tools being used.

To use the icmp\_sweep anomaly, monitor the network to find out the normal ICMP traffic patterns. Configure the icmp\_sweep anomaly threshold to be triggered when an unusual volume of ICMP requests occurs.

# Index

## A

- action 27, 47
- alert email
  - configuring 13
- anomalies 43
  - configuring 44
  - log messages 15
  - viewing 44
- attack log messages 14
  - anomalies 15
  - signature 14

## B

- bad\_flag\_list 25

## C

- clear session
  - predefined signature action 21
- codepoint 26
- comments, documentation 7
- config limit 46
- config rule 25
- custom signatures
  - adding 30
  - backing up 32
  - viewing 29
- customer service 7

## D

- default settings 11
- direction 26
- documentation
  - commenting on 7
  - FortiGate 6
- drop
  - predefined signature action 20
- drop sessiondrop
  - predefined signature action 21

## F

- fail open 11

- FortiGate documentation 6
  - commenting on 7
- FortiGuard Center 15
- FortiGuard Vulnerability Encyclopedia 15
- Fortinet customer service 7
- Fortinet Knowledge Center 7

## I

- ICMP attack signatures 53
- ICMP sweep
  - anomalies 56
  - configuring protection 56
- idle\_timeout 26
- introduction
  - FortiGate documentation 6
- ip\_signature 11, 12
- ipaddress 48
- IPS
  - predefined signature action 20
- ips-open
  - system global 12
- ips-size
  - system global 12

## L

- log 27, 47
- logging
  - attack messages 14
  - configuring 13

## M

- messages
  - attack log 14
- min\_ttl 26

## N

- network performance 10

## P

- pass
  - predefined signature action 20

- pass sessiondrop
  - predefined signature action 21
- performance 10
- port\_list 26
- predefined signature
  - actions 20
  - clear session action 21
  - drop action 20
  - drop session action 21
  - pass action 20
  - pass session action 21
  - reset action 20
  - reset client action 21
  - reset server action 21
- predefined signatures 19
  - configuring 22
  - groups 23
  - viewing 19
- protection profiles
  - creating 16
  - options 16

## R

- reset
  - predefined signature action 20

- reset client
  - predefined signature action 21
- reset server
  - predefined signature action 21

## S

- signature 32
- signature attack log messages 14
- signatures
  - configuring predefined 22
  - predefined 19
  - predefined groups 23
  - viewing predefined 19
- status 26, 28, 48
- SYN flood 49
  - configuring protection 51, 52
  - diagrams 51
  - FortiGate response to 50
  - prevention 50
- SYN proxy 50
- SYN threshold 50

## T

- technical support 7
- threshold 48