

The Fortinet logo is displayed in white, bold, uppercase letters. The letter 'O' is replaced by a red square containing a white grid pattern. The background of the top half of the page is a complex, abstract composition of red and orange geometric shapes, including triangles and polygons, some of which are semi-transparent, creating a sense of depth and movement. The overall aesthetic is high-tech and dynamic.

**FORTINET**

# FortiGate IPS Guide

**Intrusion Prevention System Guide**

**Version 1.0**

30 November 2004

01-28007-0080-20041130

© Copyright 2004 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.

*Intrusion Prevention System Guide*

Version 1.0

FortiOS v2.80 MR7

30 November 2004

01-28007-0080-20041130

**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>
FortiGate documentation .....	6
Fortinet Knowledge Center .....	6
Comments on Fortinet technical documentation.....	6
Customer service and technical support.....	7
<b>Configuring and Using the IPS .....</b>	<b>9</b>
What is an IPS? .....	9
The FortiGate IPS .....	9
When to use IPS.....	10
IPS configuration.....	10
Predefined signatures .....	10
Custom signatures .....	16
Anomalies .....	19
Network performance.....	23
Using IPS in a protection profile.....	23
IPS protection profile options .....	24
Creating a protection profile that uses IPS .....	24
Monitoring the network and dealing with attacks .....	25
Configuring logging and alert email .....	25
Attack log messages.....	26
The FortiProtect Center .....	27
<b>SYN Flood Attacks.....</b>	<b>29</b>
How SYN floods work .....	29
The FortiGate IPS Response to SYN Flood Attacks.....	30
What is SYN threshold?.....	30
What is SYN proxy? .....	30
How IPS works to prevent SYN floods.....	30
Configuring SYN flood protection.....	32
Suggested settings for different network conditions .....	32
<b>ICMP Sweep Attacks.....</b>	<b>33</b>
How ICMP sweep attacks work .....	33
The FortiGate IPS response to ICMP sweep attacks .....	33
Predefined ICMP signatures .....	33
ICMP sweep anomalies .....	36
Configuring ICMP sweep protection .....	36
Suggested settings for different network conditions .....	36

<b>Custom Signatures .....</b>	<b>37</b>
Creating custom signatures .....	37
Example .....	37
Custom signature fields .....	38
Custom signature syntax .....	39
<b>Glossary .....</b>	<b>47</b>
<b>Index .....</b>	<b>51</b>



# Introduction

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.

This Guide describes:

- [Configuring and Using the IPS](#)
- [SYN Flood Attacks](#)
- [ICMP Sweep Attacks](#)
- [Custom Signatures](#)

## FortiGate documentation

Information about FortiGate products is available from the following guides:

- *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 Guide*  
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference Guide*  
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability Guide*  
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate VPN Guide*  
Explains how to configure VPNs using the web-based manager.

### Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much 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

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet technical support web site at <http://support.fortinet.com>.

You can also register FortiGate Antivirus Firewalls from <http://support.fortinet.com> and change your registration information at any time.

Fortinet email support is available from the following addresses:

- |                                  |                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>amer_support@fortinet.com</b> | For customers in the United States, Canada, Mexico, Latin America and South America.                            |
| <b>apac_support@fortinet.com</b> | For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia. |
| <b>eu_support@fortinet.com</b>   | For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.                 |

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiGate unit serial number
- FortiGate model
- FortiGate FortiOS firmware version
- Detailed description of the problem



# Configuring and Using the IPS

This section describes:

- [What is an IPS?](#)
- [When to use IPS](#)
- [IPS configuration](#)
- [Using IPS in a protection profile](#)
- [Monitoring the network and dealing with attacks](#)

## What is an IPS?

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.

You can upgrade both the IPS predefined signatures and the IPS engine 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. You can adjust signature settings and some anomaly thresholds to work best with the normal traffic on the protected networks. You can also create custom signatures for the FortiGate IPS in diverse network environments.

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

The IPS is configured globally in the FortiGate unit but can be enabled separately in each firewall protection profile. See [“Using IPS in a protection profile” on page 23](#) or see the Firewall chapter in the *FortiGate Administration Guide* for complete protection profile and firewall policy procedures.

For detailed information on individual signatures and anomalies, see the Attack Encyclopedia in the FortiProtect Center available on the Fortinet web site at <https://www.fortinet.com/FortiProtectCenter/>.

## 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.

## IPS configuration

This section describes:

- [Predefined signatures](#)
- [Custom signatures](#)
- [Anomalies](#)
- [Network performance](#)

### Predefined signatures

The FortiGate IPS matches network traffic against patterns contained in attack signatures. Attack signatures reliably protect your network from known attacks. Fortinet's FortiProtect infrastructure ensures the rapid identification of new threats and fast deployment of new attack signatures.

The FortiGate IPS contains an ever-increasing number of predefined signatures divided into groups. For information about individual signatures visit the [Attack Encyclopedia](#) in the FortiProtect Center.

This section describes:

- [Signature updates](#)
- [Signature groups](#)
- [Attack responses](#)
- [Logging attacks](#)
- [Viewing the predefined signature list](#)
- [Configuring individual signature settings](#)
- [Changing the status of predefined signature groups](#)
- [Configuring parameters for signature groups](#)

## Signature updates

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

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.

## Signature groups

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

You can 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 you do not provide access to a web server behind your FortiGate unit, you should 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 you configure these parameters for a signature group, the parameters apply to all of the signatures in the group.

## Attack responses

For each signature, you can 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. IPS actions are described in [“Configuring individual signature settings” on page 13](#).

## Logging attacks

You can also enable or disable logging of the attack. See [“Configuring logging and alert email” on page 25](#).

## Viewing the predefined signature list

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

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

Figure 1: 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					

- Group Name** The signature group names.
- Enable** 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.
- Logging** 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.
- Action** 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.
- Revision** The revision number for individual signatures. Click on the blue triangle to show the signature group members.
- Modify** The Configure and Reset icons. Reset only appears when the default settings have been modified. Selecting Reset restores the default settings.

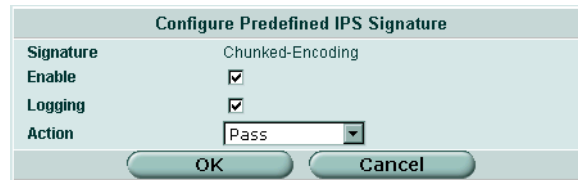
**To view predefined signatures using the CLI**

You can 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
```

## Configuring individual signature settings

Figure 2: Configure Predefined IPS Signatures



<b>Signature</b>	The predefined signature name.
<b>Enable</b>	Select to enable the predefined signature or clear to disable the predefined signature.
<b>Logging</b>	Select to enable logging for the predefined signature or clear to disable logging for the predefined signature.
<b>Action</b>	Select the action for the FortiGate unit to take when traffic triggers 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 you set this action 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 you set this action 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 you set this action 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>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>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.

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

- 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 you want 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 configure signature settings using the CLI

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
```

### 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 you want 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 3: Edit IPS Configuration

Edit IPS Configuration	
Group Name	apache
Enable	<input checked="" type="checkbox"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

**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 that you want 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.

### To enable/disable a predefined signature group using the CLI

This example shows how to disable the ftp signature group.

```

config ips group ftp
    set status disable
end

```

## Configuring parameters for signature groups

The following predefined signature groups have configurable parameters.

- http\_decoder
- im
- p2p
- rpc\_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 you want to configure. When you are done, select OK.

Figure 4: Example http\_decoder signature group parameters

Edit IPS Configuration	
Group Name	http_decoder
Enable	<input checked="" type="checkbox"/>
port_list	80
uri_length	1600
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Figure 5: 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 6: 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 7: 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 8: 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, !
direction	from-client
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

<b>idle_timeout</b>	If a session is idle for longer than this number of seconds, the session will not be maintained by tcp_reassembler.
<b>min_ttl</b>	A packet with a higher ttl number in its IP header than the number specified here is not processed by tcp_reassembler.
<b>port_list</b>	A comma separated list of ports. The dissector can decode these TCP ports.
<b>bad_flag_list</b>	A comma separated list of bad TCP flags.
<b>direction</b>	Valid settings are from-server, from-client, or both.
<b>codepoint</b>	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.

### To configure signature group parameters using the CLI

This example shows how to change the idle-timeout setting to 180 seconds and the direction to from-server for the tcp\_reassembler signature group.

```
config ips group tcp_reassembler
    set idle_timeout 180
    set direction from-server
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 you are using an unusual or specialized application or an uncommon platform, you can add custom signatures based on the security alerts released by the application and platform vendors.

See [“Custom Signatures” on page 37](#) for information on custom signature syntax.

This section describes:

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



**Note:** Custom signatures are an advanced feature. This document assumes the user has previous experience creating intrusion detection signatures.

## Viewing custom signatures

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

Go to **IPS > Signature > Custom**.

**Figure 9: Custom signatures**

<input checked="" type="checkbox"/> Enable custom signature.					
<b>Create New</b>					
Name	Revision	<input checked="" type="checkbox"/> Enable	Logging	Action	Modify
ICMP10	2	<input checked="" type="checkbox"/>	<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 Create New 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.
- Revision** The revision number for each custom signature. The signature revision number is updated when you revise a signature.
- Enable** 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.
- Logging** 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.
- Action** The action set for each custom signature. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
- Modify** The Delete and Edit/View icons.

## To view custom signatures using the CLI

```
get ips custom
```

## Adding custom signatures

Figure 10: 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 you set this action 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 you set this action 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 you set this action 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 an existing custom signature.

- 3 Enter a name for the custom signature.  
You cannot edit the name of an existing custom signature.
- 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.

### To add a custom signature using the CLI

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

For information on backing up and restoring the custom signature list, see the *FortiGate Administration Guide*.



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

## Anomalies

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.

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



**Note:** It is important to estimate the normal and expected traffic on your 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.

You can also 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.

This section describes:

- [Viewing the anomaly list](#)
- [Configuring an anomaly](#)

### Viewing the anomaly list

#### To view the anomaly list using the web-based manager

Go to **IPS > Anomaly**.

**Figure 11: The Anomaly list**

Name	Enable	Logging	Action	Modify
syn_flood			Clear Session	
portscan			Clear Session	
syn_fin			Clear Session	

- Name** The anomaly names.
- Enable** 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.
- Logging** 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.
- Action** The action set for each anomaly. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session.
- Modify** 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

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

Figure 12: Editing the portscan IPS Anomaly

Edit IPS Anomaly	
Name	portscan
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Clear Session
Parameters:	
threshold	2048
OK Cancel	

Figure 13: Editing the syn\_fin IPS Anomaly

Edit IPS Anomaly	
Name	syn_fin
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Clear Session
OK Cancel	

- Name** The anomaly name.
- Enable** Enable or disable the anomaly in the IPS.
- Logging** 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 you set this action 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 you set this action 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 you set this action 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**.
- 2 Select Edit for the signature you want 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 configure anomaly settings using the CLI

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
```

### To restore the default settings of an anomaly

- 1 Go to **IPS > Anomaly**.
- 2 Select **Reset** for the anomaly you want to restore to default.  
The **Reset** icon is displayed only if the settings for the anomaly have been changed from defaults.
- 3 Select **OK**.

## 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.

### 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.

You can adjust the IPS settings according to the traffic and applications on your network. For instance, if you are not using POP3 you can disable the pop3 signature group.

### Default fail open setting

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.

You can change the default fail open setting using the CLI:

```
config sys global
    set ips-open [enable | disable]
end
```

## 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 14: 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 your 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, you can also select a protection profile that applies to that group. Then, when you configure a firewall policy that includes user authentication, you select one or more user groups to authenticate. Each user group you select for authentication in the firewall policy can have a different protection profile, and therefore different IPS settings, applied to it.

## Monitoring the network and dealing with attacks

Once you have configured IPS and enabled it in protection profiles, it is time to set up the FortiGate unit to keep track of attacks and notify you if they occur. Enabling logging and alert email will keep you aware of attacks on the network.

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

### 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. You can enable logging and alert email for attack signatures and attack anomalies.



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

Figure 15: 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"/>

Apply

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 you want 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

You can 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 you want 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 Attack Encyclopedia in the FortiProtect Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Attack 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 Attack Encyclopedia in the FortiProtect Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Attack Encyclopedia.

## The FortiProtect Center

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

You can search for attacks in the FortiProtect Attack Encyclopedia by any of the criteria shown in [Figure 16](#).

**Figure 16: Searching the FortiProtect Attack Encyclopedia**

**Attack Description Search**

By Name:

By ID:

By Key Words:

By Class:

By CVE ID:

By MS Bulletin ID:

By BugTraq ID:

Results Per Page:

You can type in the name or ID of the attack, or copy and paste the URL from the log message or alert email into your browser.



# 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, such as a web server. SYN floods are a type of DoS attack in which 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.

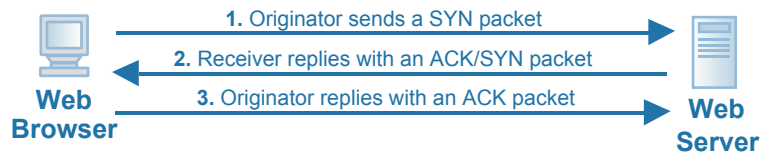
This section provides information about SYN flood attacks and the FortiGate IPS methods of preventing such attacks.

## How SYN floods work

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

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

**Figure 17: 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.

Once 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

FortiGate 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 receiver.

### How IPS works to prevent SYN floods

The FortiGate IPS uses a defense method that is similar to but not a complete SYN proxy to prevent SYN flood attack. This pseudo SYN proxy 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 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 18 illustrates the operation behavior of FGT IPS Engine before the SYN Flood threshold is reached. Figure 19 illustrates the operation behavior of FGT IPS Engine after the SYN Flood threshold is reached.

Figure 18: IPS operation before syn\_flood threshold is reached

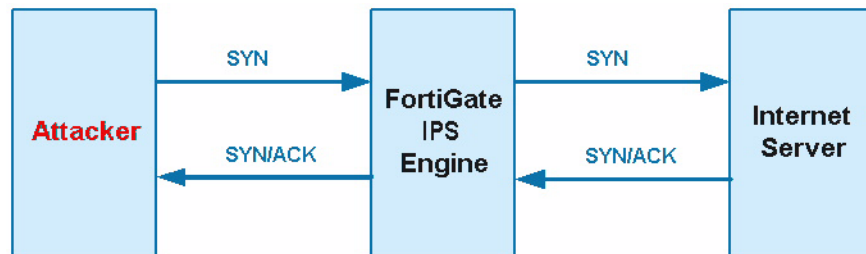
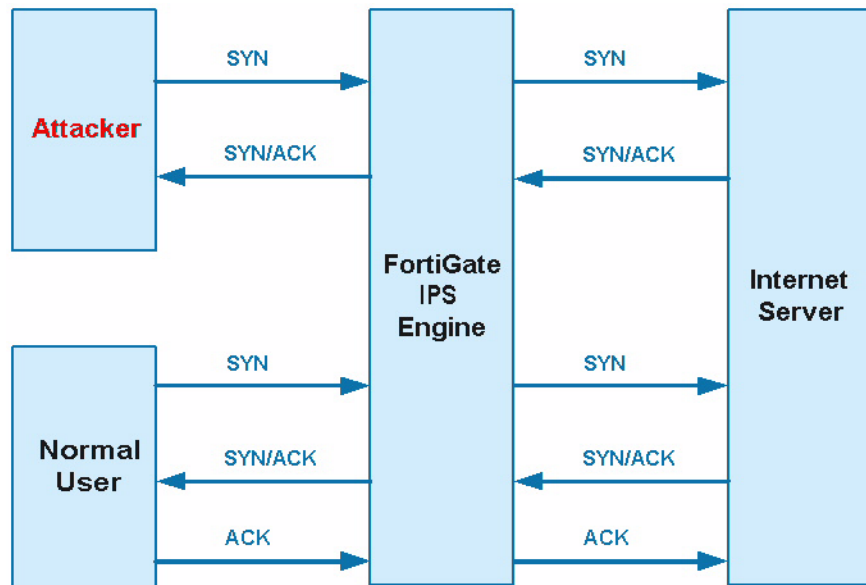


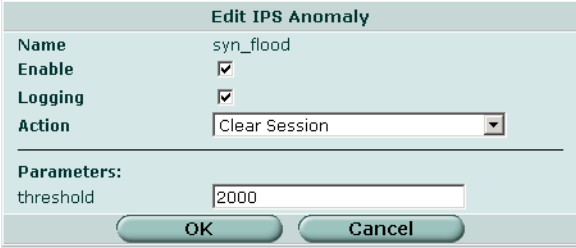
Figure 19: IPS operation after syn\_flood threshold is reached



## 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 20: 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:

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

At the bottom of the window are two buttons: "OK" and "Cancel".

See [“Anomalies” on page 19](#) 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. You should select an appropriate value based on your network conditions. Normally, if the servers being protected by the FortiGate unit need to handle heavier requests, such as a busy web server, then the threshold should be set to a higher value. If your 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 that 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.

You can create your own custom signatures to block attacks specific to your 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 1](#) describes all the ICMP-related predefined signatures and the default settings for each. See [“Configuring individual signature settings” on page 13](#) for details about each possible signature action.



**Note:** The predefined signature descriptions in [Table 1](#) are accurate as of the IPS Guide publication date. Predefined signatures may be added or changed with each Attack Definition update.

**Table 1: 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. If you are not a customer of Digital Island 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, you can 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 1: 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>	<b>TJPingPro1.1 is a widely-used network tool for older versions of Windows.</b> 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 21: 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” on page 10 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 22: Configuring the icmp\_sweep anomaly

**Edit IPS Anomaly**

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

---

**Parameters:**

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

See “Anomalies” on page 19 for information about configuring anomalies.

## Suggested settings for different network conditions

You can enable or disable the ICMP predefined signatures depending on your current network traffic and the network scanning tools that you are using.

To use the icmp\_sweep anomaly, you should monitor your network to find out the normal ICMP traffic patterns. You can then configure the icmp\_sweep anomaly threshold to be triggered when an unusual volume of ICMP requests occurs.

# 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 you are using an unusual or specialized application or an uncommon platform, you can add custom signatures based on the security alerts released by the application and platform vendors.

You can also use custom signatures to block or allow specific traffic.

## Creating custom signatures

Each 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.

Each 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 2 shows the valid characters for custom signature fields.

Table 2: 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>	The keyword must start with --, and be a string of greater than 0 and less than 20 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 39</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 3: 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.	Optionally include a revision number for this signature.

**Table 4: 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 4: Content specific keywords**

<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.	<b>bytes_to_convert</b> - The number of bytes to pick up from the packet. <b>operator</b> - The operation to perform to test the value (<, >, =, !, &). <b>value</b> - The value to test the converted value against. <b>offset</b> - The number of bytes into the payload to start processing. <b>relative</b> - Use an offset relative to last pattern match. <b>big</b> - Process the data as big endian (default). <b>little</b> - Process the data as little endian. <b>string</b> - The data is stored in string format in the packet. <b>hex</b> - The converted string data is represented in hexadecimal. <b>dec</b> - The converted string data is represented in decimal. <b>oct</b> - The converted string data is represented in octal.

**Table 4: Content specific keywords**

<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 4: Content specific keywords**

<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 5: 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 5: IP header keywords**

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

**Table 5: IP header keywords**

<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 6: 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 6: TCP header keywords**

<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 7: UDP 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.

**Table 8: ICMP keywords**

Keyword	Value	Usage
<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 9: 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.

# Glossary

**Connection:** A link between machines, applications, processes, and so on that can be logical, physical, or both.

**DMZ, Demilitarized Zone:** Used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

**DMZ interface:** The FortiGate interface that is connected to a DMZ network.

**DNS, Domain Name Service:** A service that converts symbolic node names to IP addresses.

**Ethernet:** A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

**External interface:** The FortiGate interface that is connected to the Internet. For the FortiGate-60 the external interface is WAN1 or WAN2.

**FTP, File transfer Protocol:** An application and TCP/IP protocol used to upload or download files.

**Gateway:** A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

**HTTP, Hyper Text Transfer Protocol:** The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**HTTPS:** The SSL protocol for transmitting private documents over the Internet using a Web browser.

**Internal interface:** The FortiGate interface that is connected to an internal (private) network.

**Internet:** A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

**ICMP, Internet Control Message Protocol:** Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

**IKE, Internet Key Exchange:** A method of automatically exchanging authentication and encryption keys between two secure servers.

**IMAP, Internet Message Access Protocol:** An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

**IP, Internet Protocol:** The component of TCP/IP that handles routing.

**IP Address:** An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

**L2TP, Layer Two (2) Tunneling Protocol:** An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

**IPSec, Internet Protocol Security:** A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

**LAN, Local Area Network:** A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

**MAC address, Media Access Control address:** A hardware address that uniquely identifies each node of a network.

**MIB, Management Information Base:** A database of objects that can be monitored by an SNMP network manager.

**Modem:** A device that converts digital signals into analog signals and back again for transmission over telephone lines.

**MTU, Maximum Transmission Unit:** The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

**Netmask:** Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

**NTP, Network Time Protocol:** Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

**Packet:** A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

**Ping, Packet Internet Grouper:** A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

**POP3, Post Office Protocol:** A protocol used to transfer e-mail from a mail server to a mail client across the Internet. Most e-mail clients use POP.

**PPP, Point-to-Point Protocol:** A TCP/IP protocol that provides host-to-network and router-to-router connections.

**PPTP, Point-to-Point Tunneling Protocol:** A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

**Port:** In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

**Protocol:** An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

**RADIUS, Remote Authentication Dial-In User Service:** An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

**Router:** A device that connects LANs into an internal network and routes traffic between them.

**Routing:** The process of determining a path to use to send data to its destination.

**Routing table:** A list of valid paths through which data can be transmitted.

**Server:** An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

**SMTP, Simple Mail Transfer Protocol:** In TCP/IP networks, this is an application for providing mail delivery services.

**SNMP, Simple Network Management Protocol:** A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

**SSH, Secure shell:** A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

**Subnet:** A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

**Subnet Address:** The part of the IP address that identifies the subnetwork.

**TCP, Transmission Control Protocol:** One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

**UDP, User Datagram Protocol:** A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

**VPN, Virtual Private Network:** A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

**Virus:** A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

**Worm:** A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.



# Index

## A

- alert email
  - configuring 25
- anomalies 19
  - configuring 20
  - log messages 27
  - viewing 20
- attack log messages 26
  - anomalies 27
  - signature 26
- attacks
  - logging 11
  - responses 11

## C

- custom signatures 16
  - adding 18
  - backing up 19
  - viewing 17
- customer service 7

## D

- default settings 23

## F

- fail open 23
- firewall profiles 23
- Fortinet customer service 7
- FortiProtect Attack Encyclopedia 27
- FortiProtect center 27

## G

- groups 11

## I

- ICMP
  - definition 47
- ICMP attack signatures 33
- ICMP sweep
  - anomalies 36
  - configuring protection 36

## L

- logging
  - attack messages 26
  - configuring 25

## M

- messages
  - attack log 26

## N

- network performance 23

## P

- performance 23
- predefined signatures 10
  - configuring 13
  - groups 14
  - viewing 11
- protection profiles 23
  - creating 24
  - options 24

## S

- signature attack log messages 26
- signatures
  - configuring predefined 13
  - custom 16
  - groups 11
  - predefined 10
  - predefined groups 14
  - updates 11
  - viewing predefined 11
- SYN flood 29
  - configuring protection 31, 32
  - diagrams 31
  - FortiGate response to 30
  - prevention 30
- SYN proxy 30
- SYN threshold 30

## T

- technical support 7

**U**

updates 11