FortiGate
IPS User Guide
Version 3.0 MR5

FORTINET™

www.fortinet.com

FortiGate IPS User Guide
Version 3.0 MR5
July 24, 2007
01-30005-0080-20070724

Trademarks

Contents

Introduction

This section introduces you to the FortiGate IPS and the following topics:

- The FortiGate IPS
- About this document
- Fortinet documentation
- Customer service and technical support

The FortiGate IPS

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, but 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:

- IPS Overview and General Configuration
- Predefined Signatures
- Custom Signatures
- Decoders
- Traffic anomalies
- SYN Flood Attacks
- ICMP Sweep Attacks

About this document

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, `Central_Office_1`).

Code examples	`F-SBID (--protocol tcp; --flow`
	`established; --content "content here";`
	`--no_case)`

CLI command syntax	`config firewall policy`
	`edit id_integer`
	`set http_retry_count <retry_integer>`
	`set natip <address_ipv4mask>`
	`end`

Document names	*FortiGate Administration Guide*
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
Menu commands	Go to **VPN > IPSEC > Phase 1** and select Create New.
Program output	`Welcome!`
Variables	`<address_ipv4>`

Fortinet documentation

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

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.

- *FortiGate online help*

  Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

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

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

IPS Overview and General Configuration

This section contains the following topics:

- The FortiGate IPS
- Network performance
- Monitoring the network and dealing with attacks
- Using IPS in a protection profile

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

Both the IPS predefined signatures and the IPS engine are upgraded through the FortiGuard Distribution Network (FDN). These upgrades provide the latest protection against IM/P2P and other threats. Anomalies are updated with firmware upgrades. The FortiGate IPS default settings implement the recommended settings for all signatures and anomalies. Signature settings and some anomaly thresholds are adjusted to work best with the normal traffic on the protected networks. Custom signatures can be created for the FortiGate IPS in diverse network environments.

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

Packet logging provides administrators with the ability to analyze packets for forensics and false positive detection.

IPS settings and controls

Configure the IPS using either the web-based manager or the CLI, then enable or disable all signatures or all anomalies in individual firewall protection profiles. If virtual domains are enabled on the FortiGate unit, the IPS is configured globally for all virtual domains. To access the IPS, select **Global Configuration** on the main menu.

Table 1 describes the IPS settings and where to configure and access them in the web-based manager.

Table 1: IPS and Protection Profile IPS configuration

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

See “Using IPS in a protection profile” on page 15 or see the Firewall section in the *FortiGate Administration Guide* for complete protection profile and firewall policy procedures.

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

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

When to use IPS

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

Network performance

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

This section describes:

- Default signature and anomaly settings
- Default fail open setting
- Controlling sessions
- Setting autoupdate
- Restricting IPS processing
- Setting the buffer size

Default signature and anomaly settings

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

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

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.

Change the default fail open setting using the CLI:

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

Controlling sessions

Use this command to ignore sessions after a set amount of traffic has passed. The default is 204800 bytes.

```
config ips global
    set ignore-session-bytes <byte_integer>
  end
```

Setting autoupdate

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

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

Restricting IPS processing

Save system resources by restricting IPS processing to only those services allowed by firewall policies. The default is disable.

```
config ips global
  set ip-protocol {enable | disable}
  end
```

Setting the buffer size

Set the size of the IPS buffer. The size of the buffer is model-dependent.

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

Monitoring the network and dealing with attacks

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

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

This section describes:

- Configuring logging and alert email
- Attack log messages
- The FortiGuard Center

Configuring logging and alert email

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

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

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

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

1 Go to **Log&Report > Log Config > Log Setting**.

2 Select and configure the settings for any logging locations to use.

3 Select Apply.

4 Go to **Log&Report > Log Config > Alert Email**.

5. Select and configure authentication if required and enter the email addresses that will receive the alert email.
6. Enter the time interval to wait before sending log messages for each logging severity level.

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

7. Select Apply.

To access log messages from memory or on the local disk

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

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

Attack log messages

Signature

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

Message ID:	70000
Severity:	Alert
Message:	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]>"
Example:	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: http://www.fortinet.com/ids/ID101318674]"
Meaning:	Attack signature message providing the source and destination addressing information and the attack name.
Action:	Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiGuard Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Attack Encyclopedia.

Anomaly

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

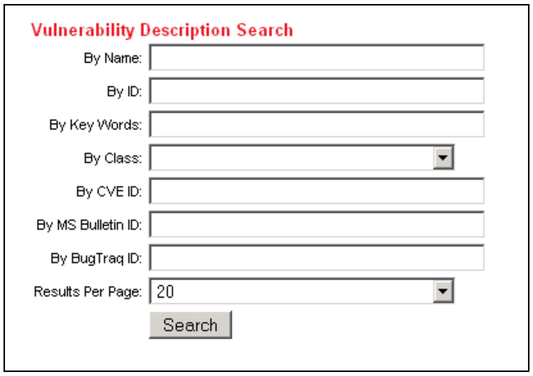
Message ID:	73001
Severity:	Alert
Message:	attack_id=<value_attack_id> src=<ip_address> dst=<ip_address> src_port=<port_num> dst_port=<port_num> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session | detected | dropped | reset} proto=<protocol_num> service=<network_service> msg="<string><[url]>"
Example:	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]"
Meaning:	Attack anomaly message providing the source and destination addressing information and the attack name.
Action:	Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiGuard Center. Copy and paste the URL from the log message into your browser to go directly to the signature description in the Attack Encyclopedia.

The FortiGuard Center

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

Search for attacks in the FortiGuard Attack Encyclopedia by any of the criteria shown in Figure 1.

Figure 1: Searching the FortiGuard Attack Encyclopedia



Vulnerability Description Search

By Name:

By ID:

By Key Words:

By Class:

By CVE ID:

By MS Bulletin ID:

By BugTraq ID:

Results Per Page: 20

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

The Attack Encyclopedia lists the following information for each signature:

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.

This section describes:

- Creating a protection profile that uses IPS
- Adding protection profiles to firewall policies
- Adding protection profiles to user groups

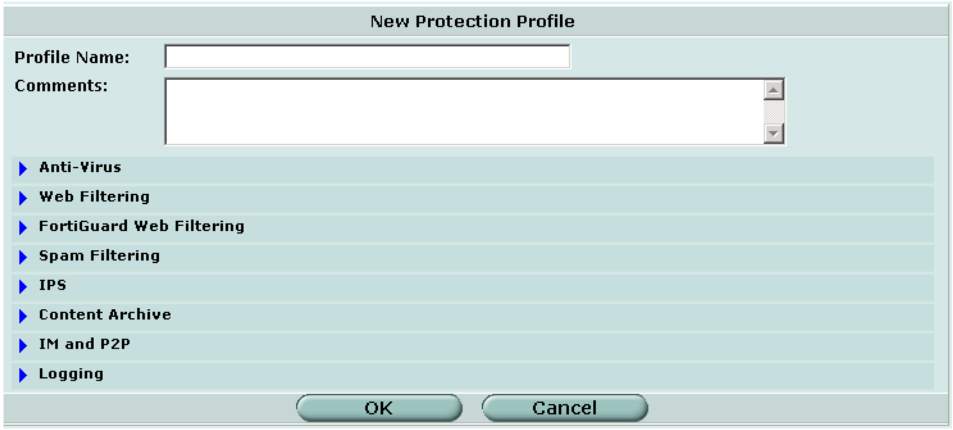
Creating a protection profile that uses IPS

To create a protection profile using the web-based manager

1 Go to **Firewall > Protection Profile**.

2 Select Create New.

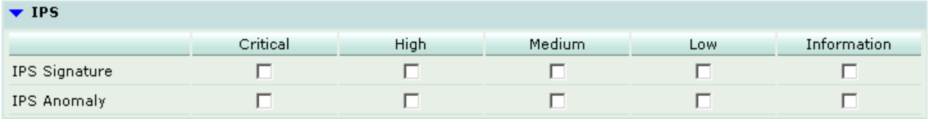
Figure 2: New Protection Profile



3 Enter a name for the protection profile.

4 Expand the IPS option list.

Figure 3: IPS protection profile options



IPS

	Critical	High	Medium	Low	Information
IPS Signature	□	□	□	□	□
IPS Anomaly	□	□	□	□	□

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

IPS Signature Enable or disable signature based intrusion detection and prevention for all protocols.

IPS Anomaly Enable or disable traffic anomaly based intrusion detection and prevention for all protocols.

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 critical and medium severity level signatures and anomalies enabled.

```
config firewall profile
    edit IPS_Special
      set ips-anomaly critical medium
      set ips-signature critical medium
end
```

Adding protection profiles to firewall policies

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

Adding protection profiles to user groups

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

Predefined Signatures

This section describes:

- IPS predefined signatures
- Viewing the predefined signature list
- Predefined signature configuration

IPS predefined signatures

Predefined signatures are arranged in alphabetical order. By default, some signatures are disabled to prevent interference with common traffic, but logging is enabled for all signatures. Check the default settings to ensure they meet the requirements of the network traffic.

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

For each signature, configure the action the FortiGate IPS takes when it detects an attack. The FortiGate IPS can pass, drop, reset or clear packets or sessions. Enable or disable packet logging. Select a severity level to be applied to the signature.

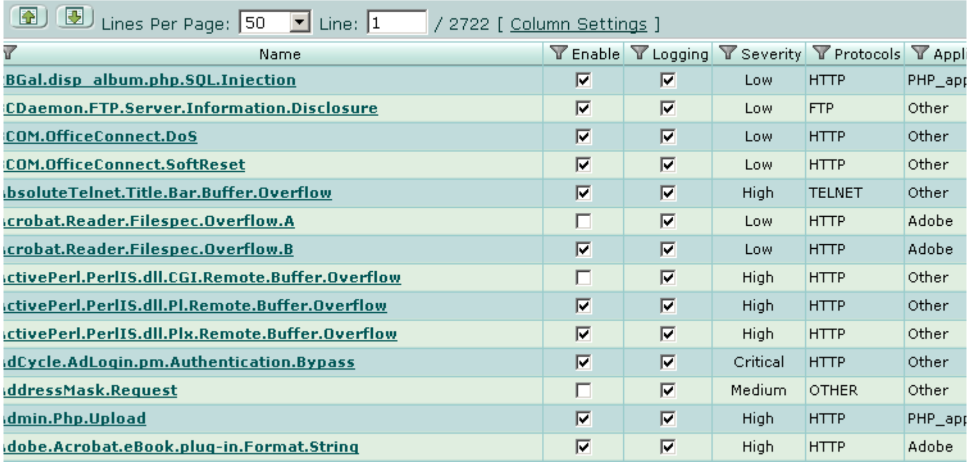
Note: By allowing your IPS signature settings to run on default, you may be slowing down the overall performance of the FortiGate unit. By fine tuning the predefined signature and logging setting, you can ensure maximum performance as well as maximum protection. See “Fine tuning IPS predefined signatures for enhanced system performance” on page 21.

Viewing the predefined signature list

Enable or disable predefined signatures and configure the settings for individual predefined signatures from the predefined signature list. The list can be viewed by signature severity level.

To view the predefined signature list, go to **Intrusion Protection > Signature > Predefined**.

Figure 4: A portion of the predefined signature list



Lines Per Page: 50 Line: 1 / 2722 [Column Settings]

Name	Enable	Logging	Severity	Protocols	Appl
BGal.disp_album.php.SQL.Injection	☑	☑	Low	HTTP	PHP_app
CDaemon.FTP.Server.Information.Disclosure	☑	☑	Low	FTP	Other
COM.OfficeConnect.DoS	☑	☑	Low	HTTP	Other
COM.OfficeConnect.SoftReset	☑	☑	Low	HTTP	Other
bsoluteTelnet.Title.Bar.Buffer.Overflow	☑	☑	High	TELNET	Other
crobat.Reader.Filespec.Overflow.A	□	☑	Low	HTTP	Adobe
crobat.Reader.Filespec.Overflow.B	☑	☑	Low	HTTP	Adobe
ctivePerl.PerlIS.dll.CGI.Remote.Buffer.Overflow	□	☑	High	HTTP	Other
ctivePerl.PerlIS.dll.Pl.Remote.Buffer.Overflow	☑	☑	High	HTTP	Other
ctivePerl.PerlIS.dll.Plx.Remote.Buffer.Overflow	☑	☑	High	HTTP	Other
dCycle.AdLogin.pm.Authentication.Bypass	☑	☑	Critical	HTTP	Other
ddressMask.Request	□	☑	Medium	OTHER	Other
dmin.Php.Upload	☑	☑	High	HTTP	PHP_app
dobe.Acrobat.eBook.plug-in.Format.String	☑	☑	High	HTTP	Adobe

Configure icon Configure settings for the signature.

Reset icon Reset only appears when the default settings for a signature have been modified. Selecting Reset for an individual signature restores the default settings for that signature.

Column Settings Select to customize the signature information to display in the table. You can also readjust the column order.

By default, the signature ID, group name, and revision number are not displayed

The column types are described below.

Name The signature name.

Enable The status of the signature. A check mark means the signature is enabled. An empty box means the signature is disabled.

Logging The logging status of the signature. If logging is enabled, the action appears in the status field of the log message generated by the signature. By default, logging is enabled for all signatures.

Action The action set for individual signatures. Action can be Pass, Drop, Reset, Reset Client, Reset Server, Drop Session, Clear Session, or Pass Session. See Table 2 for descriptions of the actions.

Severity The severity level for each signature. Severity level can be Information, Low, Medium, High, or Critical.

Revision The revision number for individual signatures.

ID The signature's unique ID.

OS The operating system the signature applies to.

Group The group that the signature belongs to such as IM, Backdoor amongst others.

Protocols The protocol the signature applies to.

Location The location that is protected by the signature; Client, Server or both.

Application The applications the signature applies to.

Table 2 describes the action by the predefined signatures.

Table 2: Actions to select for each predefined signature

Action	Description
Pass	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall without further action. If logging is disabled and action is set to Pass, the signature is effectively disabled.
Drop	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The firewall session is not touched. Fortinet recommends using an action other than Drop for TCP connection based attacks.
Reset	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to both the client and the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Client	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the client and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Client action is triggered before the TCP connection is fully established, it acts as Clear Session.
Reset Server	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. The FortiGate unit sends a reset to the server and drops the firewall session from the firewall session table. This is used for TCP connections only. If set for non-TCP connection based attacks, the action will behave as Clear Session. If the Reset Server action is triggered before the TCP connection is fully established, it acts as Clear Session.
Drop Session	When a packet triggers a signature, the FortiGate unit generates an alert and drops the packet. For the remainder of this packet's firewall session, all follow-up packets are dropped.
Pass Session	When a packet triggers a signature, the FortiGate unit generates an alert and allows the packet through the firewall. For the remainder of this packet's session, the IPS is bypassed by all follow-up packets.
Clear Session	When a packet triggers a signature, the FortiGate unit generates an alert and the session to which the packet belongs is removed from the session table immediately. No reset is sent. For TCP, all follow-up packets could be dropped. For UDP, all follow-up packets could trigger the firewall to create a new session.

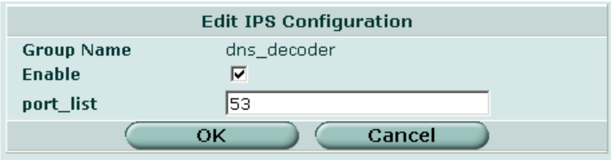
Predefined signature configuration

This section describes:

- Configuring signatures using the web-based manager
- Fine tuning IPS predefined signatures for enhanced system performance
- Configuring predefined signatures using the CLI

Configuring signatures using the web-based manager

Figure 5: Edit IPS Configuration



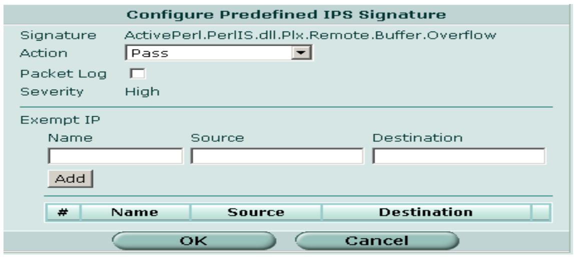
Edit IPS Configuration

Group Name	dns_decoder
Enable	☑
port_list	53

To configure predefined signature settings

1. Go to **Intrusion Protection > Signature > Predefined**.
2. Select the Configure icon for the signature to configure.

Figure 6: Configure Predefined IPS Signature



Configure Predefined IPS Signature

Signature	ActivePerl.PerlIS.dll.Plx.Remote.Buffer.Overflow
Action	Pass
Packet Log	☐
Severity	High

Exempt IP

Name	Source	Destination

#	Name	Source	Destination

3. Select the Action for the FortiGate unit to take when traffic matches this signature. (See Table 2.)
4. If required, enable Packet Log.
5. Select a Severity level for the signature: Information, Low, Medium, High, or Critical.
6. If required create an IP exemption for the signature.
7. Select OK.

To restore the recommended settings of a signature

1. Go to **Intrusion Protection > Signature > Predefined**.
2. Select the Reset icon for the signature to restore to recommended settings.

   The Reset icon is displayed only if the settings for the signature have been changed from recommended settings.
3. Select OK.

Fine tuning IPS predefined signatures for enhanced system performance

By default, the FortiGate unit will have most of the predefined signatures enabled and will log all of them. If left on the default settings, the FortiGate will provide your system with the best protection available. By fine tuning the signatures and log settings you can still provide the best protection available but also free up valuable FortiGate resources. Fine tuning allows you to turn off features that you are not using. By turning off signatures and logs that you do not use, you allow the FortiGate unit to perform tasks faster thus improving overall system performance.

Not all systems require you to scan for all signatures of the IPS suite all the time.

For example. If you have a FortiGate unit that is controlling computers that only have access to an internal database and do not have access to the internet or email, there is no point having the Fortigate unit scanning for certain types of signatures such as email, IM, and P2P.

By telling the FortiGate unit not to look for these signatures, you will maintain a high level of security and increase overall performance.

You should also review exactly how you use the information provided by the logging feature. If you find that you do not review the information, it is best to turn off the logging feature. Logging is best used to provide actionable intelligence.

To disable individual signatures

1. Go to **Intrusion Protection > Signatures > Predefined**.
2. Clear the Enable box for the signatures you want to disable.

To turn off logging for a signature

1. Go to **Intrusion Protection > Signatures > Predefined**.
2. Select the Configure icon on the right hand side of the signature you want to change.
3. Clear the Logging check box.
4. Select OK.

Configuring predefined signatures using the CLI

Note: In the web-based interface, the IPS settings are divided between signatures, protocol anomalies, and traffic anomalies. In the command line interface, protocol anomalies are included with signatures leaving two categories named anomalies and signatures.

idle_timeout	If a session is idle for longer than this number of seconds, the session will not be maintained by tcp_reassembler.
min_ttl	A packet with a higher ttl number in its IP header than the number specified here is not processed by tcp_reassembler.

port_list A comma separated list of ports. The dissector can decode these TCP ports.

bad_flag_list A comma separated list of bad TCP flags.

reassembly_ direction Valid settings are from-server, from-client, or both.

codepoint A number from 0 to 63. Used for differentiated services tagging. When the action for P2P and IM signatures is set to Pass, the FortiGate unit checks the codepoint. If the codepoint is set to a number from 1 to 63, the codepoint for the session is changed to the specified value. If the codepoint is set to -1 (the default) no change is made to the codepoint in the IP header.

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

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

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

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

The `config ips group` command has `1` subcommand.

config rule <rule-name_str>

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

Command syntax pattern

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

Keywords and variables	Description	Default
`group_name_str`	The name of the signature group.	
`bad_flag_list <flag_str>`	A comma separated list of bad TCP flags. This applies to `tcp_reassembler`.	NULL, F, U, P, SF, PF, UP, UPF, UAPSF, UAPRSF
`codepoint <codepoint_integer>`	A number from 0 to 63. Used for differentiated services tagging. When the action for `P2P` and `IM` signatures is set to `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. This applies to `IM` and `P2P`.	-1
`idle_timeout <timeout_integer>`	If a session is idle for longer than this number of seconds, the session is be maintained by tcp reassembly. This applies to `tcp_reassembler`.	30
`min_ttl <ttl_integer>`	A packet with a higher TTL number in its IP header than the number specified here is not processed by tcp reassembly. This applies to `tcp_reassembler`.	1
`port_list <port_integer>`	A comma separated list of ports. The dissector can decode these TCP ports. Default port lists: • `tcp_reassembler` - 21, 23, 25, 53, 80, 110, 111, 143, 513,1837,1863,5050,5190 • `dns_decoder` - 53 • `ftp_decoder` - 21 • `http_decoder` - 80 • `imap_decoder` - 143 • `pop_decoder` - 110 • `rpc_decoder` - 111, 32771 • `smtp_decoder` - 25 • `snmp_decoder` - 161-162 This applies to `tcp_reassembler`, `dns_decoder`, `ftp_decoder`, `http_decoder`, `imap_decoder`, `pop_decoder`, `rpc_decoder`, `smtp_decoder`, and `snmp_decoder`.	Varies.
`direction <direction_str>`	Valid settings are from-server, from-client, or both. This applies to `tcp_reassembler`.	`from-client`
`status {enable | disable}`	Enable or disable this signature group.	`enable`
`The following keywords are specific to the config rule command.`		
`rule_name_str`	The name of the rule.	

Keywords and variables	Description	Default

`action {clear_session	drop	drop_session	pass	pass_session	reset	reset_client	reset_server}`	Select an action for the FortiGate unit to take when traffic triggers this signature. If logging is enabled, the action appears in the status field of the log message generated by the signature.
								`clear_session`
								• The FortiGate unit drops the packet that triggered the signature, removes the session from the FortiGate session table, and does not send a reset.
								`drop`
								• The FortiGate unit drops the packet that triggered the signature. Fortinet recommends using an action other than `drop` for TCP connection based attacks.
								`drop_session`
								• The FortiGate unit drops the packet that triggered the signature and drops any other packets in the same session.
								`pass`
								• 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.
								`pass_session`
								• The FortiGate unit lets the packet that triggered the signature and all other packets in the session pass through the firewall.
								`reset`
								• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear_session`. If the `reset` action is triggered before the TCP connection is fully established it acts as `clear_session`.
								`reset_client`
								• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear_session`. If the `reset_client` action is triggered before the TCP connection is fully established it acts as `clear_session`.
								`reset_server`
								• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear_session`. If the `reset_server` action is triggered before the TCP connection is fully established it acts as `clear_session`.
									Varies.

Keywords and variables	Description	Default
`default_action {clear_session | drop | drop_session | pass | pass_session | reset | reset_client | reset_server}`	The default action for the rule. This option is get only.	
`default_severity {info | low | medium | high | critical}`	The default severity level for the rule. This option is get only.	`critical`
`log {enable | disable}`	Enable or disable logging for the signature. If logging is enabled, the action appears in the status field of the log message generated by the signature.	`enable`
`log_packet {enable | disable}`	Enable or disable packet logging.	`disable`
`rev <rev_integer>`	The revision number of the rule. This option is get only.	`0`
`severity {info | low | medium | high | critical}`	Set the severity level for the rule.	`critical`
`status {enable | disable}`	Enable or disable this signature.	`enable`

Examples

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

```
config ips group DOS
  config rule Newtear
    set action drop
  end
end
```

Use the following command to get information about the rule Echo.Reply.

```
config ips group icmp
  (icmp)# config rule Echo.Reply
  (Echo.Reply)# get
  name                  : Echo.Reply
  action                : pass
  action (default)      : pass
  log                   : enable
  log_packet            : disable
  rev                   : 2.136
  severity              : critical
  severity (default)    : critical
  status                : disable
  status (default)      : disable
```

Custom Signatures

Custom signatures provide the power and flexibility to customize the FortiGate IPS for diverse network environments. This section describes:

- IPS custom signatures
- Viewing the custom signature list
- Custom signature configuration
- Creating custom signatures

IPS custom signatures

The FortiGate predefined signatures cover common attacks. If an unusual or specialized application or an uncommon platform is being used, add custom signatures based on the security alerts released by the application and platform vendors.

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

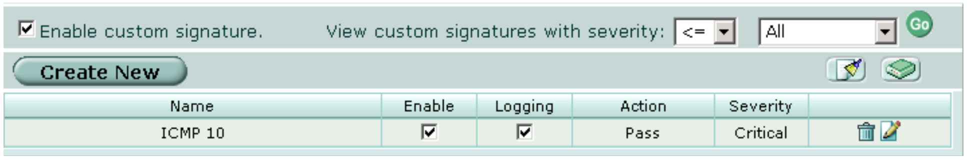
```
F-SBID (--protocol tcp; --flow established; --content "nude
cheerleader"; --no_case)
```

Note: If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select **Global Configuration** on the main menu.

Viewing the custom signature list

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

Figure 7: The custom signature list



☑ Enable custom signature.

View custom signatures with severity: <= All

Name	Enable	Logging	Action	Severity	
ICMP 10	☑	☑	Pass	Critical	

View custom signatures with severity
Select filters then select Go to view only those custom signatures that match the filter criteria. Sort criteria can be <=, =, >= to All, Information, Low, Medium, High, or Critical.

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

Create New
Select to create a new custom signature.

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

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

Name The custom signature name.

Enable The status of each custom signature. A check mark in the box indicates the signature is enabled.

Logging The logging status of each custom signature. A check mark in the box indicates logging is enabled 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.

Severity The severity level set for each custom signature. Severity level can be Information, Low, Medium, High, or Critical. Severity level is set for individual signatures.

Delete icon Select to delete the custom signature.

Edit icon Select to edit the following information: Name, Signature, Action, Packet Log, and Severity.

Custom signature configuration

Add custom signatures using the web-based manager or the CLI. For more information about custom signature syntax, see "Creating custom signatures" on page 29 and "Custom signature syntax" on page 30.

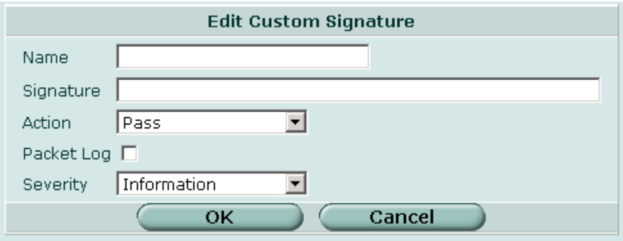
Adding custom signatures using the web-based manager

To add a custom signature

1 Go to **Intrusion Protection > Signature > Custom**.

2 Select Create New to add a new custom signature, or select the Edit icon to edit a custom signature.

Figure 8: Edit Custom Signature



Edit Custom Signature

Name	
Signature	
Action	Pass
Packet Log	□
Severity	Information

3 Enter a name for the custom signature.

4 Enter the Signature.

5 Set the action to Drop Session.

6 If required, enable Packet Log.

7 Select a Severity level for the signature: Information, Low, Medium, High, or Critical.

8 Select OK.

Adding custom signatures using the CLI

After adding the custom signature, configure the settings for it under the signature group named custom. For more information about configuring signature groups, see "Configuring predefined signatures using the CLI" on page 21.

Command syntax pattern

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

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

Example

This example shows how to add a custom signature for ICMP packets set to type 10.

```
config ips custom
    edit ICMP10
      set signature 'F-SBID(--protocol icmp; --icmp_type 10;
  --revision 2; )'
  end
```

Creating custom signatures

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

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

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

Custom signature fields

Table 3shows the valid characters for custom signature fields.

Table 3: Valid characters for custom signature fields

Field	Valid Characters	Usage
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.

Table 3: Valid characters for custom signature fields

KEYWORD	A keyword must start with "--", and be a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by "_". Letters are usually lower case; however, keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature syntax" on page 30 for tables of supported keywords.
VALUE	Double quotes must be used around the value if it contains a space and/or a semicolon. If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: if double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	Set the value for a parameter identified by a keyword.

Custom signature syntax

Table 4: General keywords

Keyword	**Value**	**Usage**
name	A string of greater than 0 and less than 64 characters. Normally, the group name is an English word or English words connected by _. All letters are normally lower case. The name keyword can be different from the signature name.	Because the name identifies the signature for the user, it should be easily readable and unique. The name keyword is optional for custom signatures.
default_action	[pass | pass_session | drop | drop_session | reset | reset_client | reset_server | clear_session]	The recommended action for a signature. The default action is pass.

protocol	ip;
	tcp;
	icmp;
	udp;
		The protocol name.

revision	An integer.	Optional. A revision number for this signature.

Table 5: Content specific keywords

Keyword	Value	Usage
content	[!]"<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(:).
uri	Same as content.	Search for the normalized request URI field. Binary data can be defined as the URI value.
offset	<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.
depth	<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 proceeding "offset", it is equal to a "-offset 0" there.
distance	<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.
within	<number>; An integer (1-65535).	Look for the contents within the specified number of bytes of the payload. Use with the distance tag.
no_case	NULL	Ignore case in the content value.
raw	NULL	Ignore any decoding. Look at the raw packet data.
regex	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.

Table 5: Content specific keywords (Continued)

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

Table 5: Content specific keywords (Continued)

byte_jump	<bytes_to_convert>, <offset> [, [relative,] [big,] [little,] [string,] [hex,] [dec,] [oct,] [align]]; 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.	**bytes_to_convert** - The number of bytes to pick up from the packet. **offset** - The number of bytes into the payload to start processing. **relative** - Use an offset relative to the last pattern match. **big** - Process the data as big endian (default). **little** - Process data as little endian. **string** - The data is stored in string format in the packet. **hex** - The converted string data is represented in hexadecimal. **dec** - The converted string data is represented in decimal. **oct** - The converted string data is represented in octal. **align** - Round the number of converted bytes up to the next 32-bit boundary.

Table 5: Content specific keywords (Continued)

pcre	[!]"(/<regex>/|m<delim><regex><delim>)[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 http://www.pcre.org. The post-re modifiers set compile time flags for the regular expression.	**i** - Case insensitive. **s** - Include newlines in the dot metacharacter. **m** - 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. **x** - Whitespace data characters in the pattern are ignored except when escaped or inside a character class. **A** - The pattern must match only at the start of the buffer (same as ^). **E** - 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). **G** - Inverts the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by "?". **R** - Match relative to the end of the last pattern match (similar to distance:0;). **U** Match the decoded URI buffers (similar to the uri keyword). **B** Do not use the decoded buffers (similar to the raw keyword).
data_at	<value> [,relative];	Verify that the payload has data at a specified location. Optionally look for data relative to the end of the previous content match.

Table 6: IP header keywords

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

Table 6: IP header keywords (Continued)

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

Table 6: IP header keywords (Continued)

dst_addr	[!]<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.
ip_proto	<number>; [!]<number>; ><number>; <<number>;	Check the IP protocol header.

Table 7: TCP header keywords

Keyword	Value	Usage
src_port	[!]<number>; [!]:<number>; [!]<number>:; [!]<number>:<number>;	The source port number.
dst_port	[!]<number> [!]:<number> [!]<number>: [!]<number>:<number>	The destination port number.
tcp_flags	[!|*|+]<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. **S** - Match the SYN flag. **A** - Match the ACK flag. **F** - Match the FIN flag. **R** - Match the RST flag. **U** - Match the URG flag. **P** - Match the PSH flag. **1** - Match Reserved bit 1. **2** - Match Reserved bit 2. **0** - Match No TCP flags set. **+** - Match on the specified bits, plus any others. ***** - Match if any of the specified bits are set. **!** - Match if the specified bits are not set.
seq	<number>;	Check for the specified TCP sequence number.

Table 7: TCP header keywords (Continued)

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

Table 8: UDP header keywords

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

Table 9: ICMP keywords

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

Table 10: Other keywords

Keyword	Value	Usage
same_ip	NULL	The source and the destination have the same IP addresses.
rpc_num	<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.

flow	[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.

Table 10: Other keywords (Continued)

data_size	< 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.

revision	<number>;	The revision number of the attack signature.

Decoders

This section describes:

- Protocol decoders
- Upgrading IPS protocol decoder list
- Viewing the protocol decoder list
- Configuring protocol decoder parameters using the web-based manager

Protocol decoders

The FortiGate IPS uses protocol decoders to identify the abnormal traffic patterns that do not meet the protocol requirements and standards. For example, the HTTP decorder monitors the HTTP traffic to identify any HTTP packets that do not meet the HTTP protocol standards.

Go to **Intrusion Protection > Signature > Protocol Decoder** to set such parameters as port, min_flood_len, and max_callid_len. To set action, packet log, severity, and exempt IP see “Predefined signature configuration” on page 19.

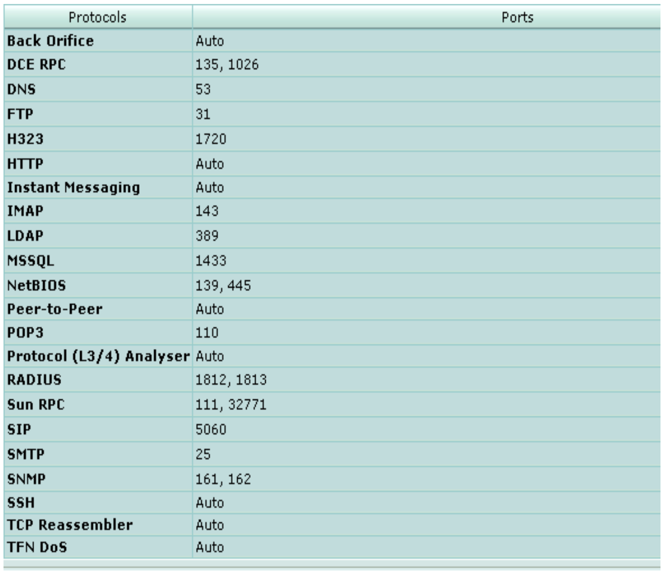
Upgrading IPS protocol decoder list

IPS protocol decoders are included in the IPS upgrade package available through the FortiGuard Distribution Network (FDN). There is no need to wait for firmware upgrades. The IPS upgrade package will keep the IPS decoder list up to date with new threats such as the latest versions of existing IM/P2P as well as new applications.

Viewing the protocol decoder list

To view the decoder list, go to **Intrusion Protection > Signature > Protocol Decoder**.

Figure 9: The protocol decoder list



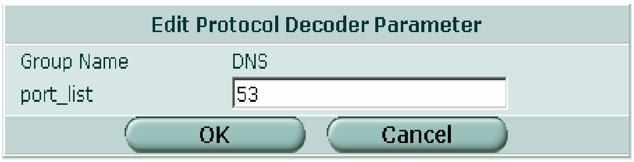
Protocols	Ports
Back Orifice	Auto
DCE RPC	135, 1026
DNS	53
FTP	31
H323	1720
HTTP	Auto
Instant Messaging	Auto
IMAP	143
LDAP	389
MSSQL	1433
NetBIOS	139, 445
Peer-to-Peer	Auto
POP3	110
Protocol (L3/4) Analyser	Auto
RADIUS	1812, 1813
Sun RPC	111, 32771
SIP	5060
SMTP	25
SNMP	161, 162
SSH	Auto
TCP Reassembler	Auto
TFN DoS	Auto

Name	The protocol decoder name.
Port	The port(s) the protocol decoder is using.
Edit icon	Select to edit the port(s) used by the decoder.

Configuring protocol decoder parameters using the web-based manager

Each protocol decoder is configured with a preset configuration. Use the recommended configurations, or modify the port list to meet the needs of your network.

Figure 10: Edit IPS Protocol Decoder: DNS



Edit Protocol Decoder Parameter

Group Name DNS

port_list 53

To configure the parameters of a protocol decoder

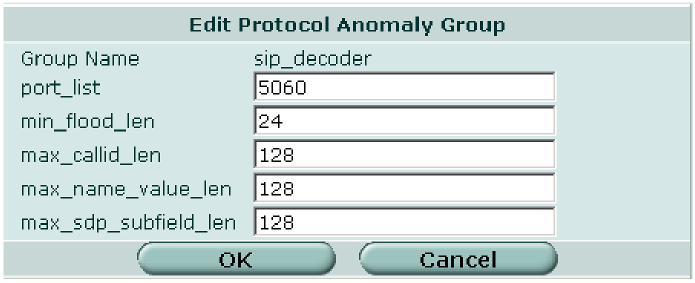
1. Go to **Intrusion Protection > Signature > Protocol Decoder**.
2. Select the Edit icon for the protocol decoder to configure.
3. Configure available parameters.
4. Select OK.

Configuring parameters for protocol decoders

The following predefined protocol decoders have configurable parameters:

- DCE RPC_decoder
- dns_decoder
- ftp_decoder
- h323_decoder
- http_decoder
- imap_decoder
- ldap_decoder
- mssql_decoder
- NetBIOS_decoder
- pop3_decoder
- radius_decoder
- Sun rpc_decoder
- sip_decoder
- smtp_decoder
- snmp_decoder

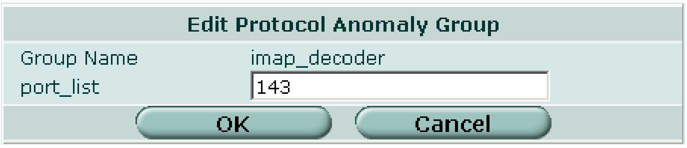
Figure 11: Edit IPS Configuration: sip_decoder



Edit Protocol Anomaly Group

Group Name	sip_decoder
port_list	5060
min_flood_len	24
max_callid_len	128
max_name_value_len	128
max_sdp_subfield_len	128

Figure 12: Edit IPS Configuration: imap_decoder



Edit Protocol Anomaly Group

Group Name	imap_decoder
port_list	143

Traffic anomalies

This section describes:

- IPS traffic anomalies
- Viewing the traffic anomaly list
- Configuring a traffic anomaly using the web-based manager
- Configuring an anomaly using the CLI

IPS traffic anomalies

The FortiGate IPS uses anomaly detection to identify network traffic that does not fit known or preset traffic patterns. For example, if one host keeps sending a number of session within a second, the destination will experience traffic flooding. In this case, the FortiGate IPS uses session thresholds to prevent flooding.

The FortiGate IPS identifies the four statistical anomaly types for the TCP, UDP, and ICMP protocols.

Flooding If the number of sessions targeting a single destination in one second is over a specified threshold, the destination is experiencing flooding.

Scan If the number of sessions from a single source in one second is over a specified threshold, the source is scanning.

Source session limit If the number of concurrent sessions from a single source is over a specified threshold, the source session limit is reached.

Destination session limit If the number of concurrent sessions to a single destination is over a specified threshold, the destination session limit is reached.

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

Note: It is important to know normal and expected network traffic 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.

Use the CLI to configure session control based on source and destination network address.

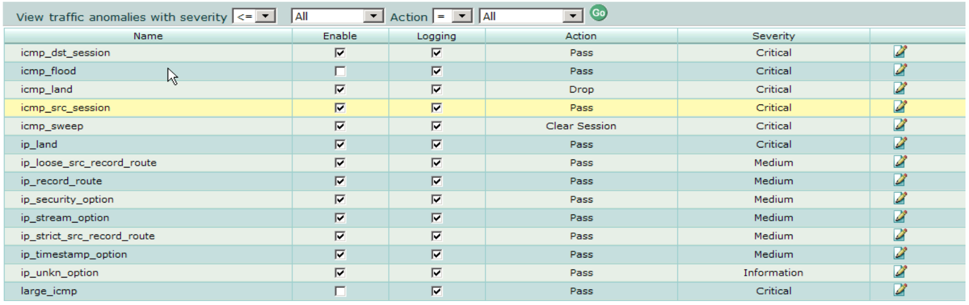
The anomaly detection list can be updated only when the FortiGate firmware image is upgraded.

Note: If virtual domains are enabled on the FortiGate unit, the IPS is configured globally. To access the IPS, select **Global Configuration** on the main menu.

Viewing the traffic anomaly list

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

Figure 13: A portion of the traffic anomaly list



View traffic anomalies with severity <= All Action = All

Name	Enable	Logging	Action	Severity	
icmp_dst_session	☑	☑	Pass	Critical	✎
icmp_flood	□	☑	Pass	Critical	✎
icmp_land	☑	☑	Drop	Critical	✎
icmp_src_session	☑	☑	Pass	Critical	✎
icmp_sweep	☑	☑	Clear Session	Critical	✎
ip_land	☑	☑	Pass	Critical	✎
ip_loose_src_record_route	☑	☑	Pass	Medium	✎
ip_record_route	☑	☑	Pass	Medium	✎
ip_security_option	☑	☑	Pass	Medium	✎
ip_stream_option	☑	☑	Pass	Medium	✎
ip_strict_src_record_route	☑	☑	Pass	Medium	✎
ip_timestamp_option	☑	☑	Pass	Medium	✎
ip_unkn_option	☑	☑	Pass	Information	✎
large_icmp	□	☑	Pass	Critical	✎

View traffic anomalies with severity Select filters then select Go to view only those anomalies that match the filter criteria. Sort criteria can be <=, =, >= to All, Information, Low, Medium, High, or Critical.

Name The traffic anomaly name.

Enable The status of the anomaly. A check mark in a check box indicates the anomaly is enabled. An empty check box indicates the anomaly is disabled.

Logging The logging status for each anomaly. A check mark in the box indicates logging is enabled 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.

Severity The severity level set for each anomaly. Severity level can be Information, Low, Medium, High, or Critical. Severity level is set for individual anomalies.

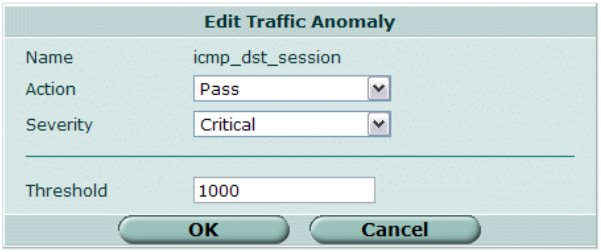
Edit icon Select to edit the following information: Action, Severity, and Threshold.

Reset icon The Reset icon is displayed only if an anomaly has been modified. Use the Reset icon to restore modified settings to the recommended values.

Configuring a traffic anomaly using the web-based manager

Each traffic anomaly is preset with a recommended configuration. Use the recommended configurations, or modify the recommended configurations to meet the needs of your network.

Figure 14: Edit IPS Traffic Anomaly: icmp_dst_session



Edit Traffic Anomaly

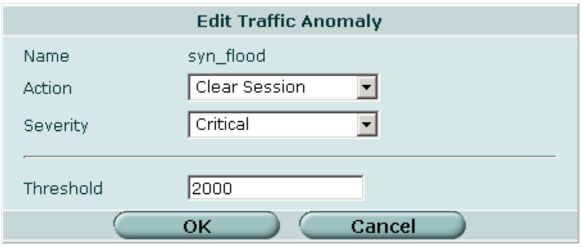
Name icmp_dst_session

Action Pass

Severity Critical

Threshold 1000

Figure 15: Edit IPS Traffic Anomaly: syn_fin



Edit Traffic Anomaly

Name	syn_flood
Action	Clear Session
Severity	Critical
Threshold	2000

To configure the settings of a traffic anomaly

1 Go to **Intrusion Protection > Anomaly**.

2 Select the Edit icon for the signature to configure.

3 Select an action for the FortiGate unit to take when traffic triggers this anomaly.

4 Select a Severity level for the anomaly: Information, Low, Medium, High, or Critical.

5 If required, enter a new threshold value.

6 Select OK.

To restore the default settings of an traffic anomaly

1 Go to **Intrusion Protection > Anomaly**.

2 Select the Reset icon for the anomaly to restore to defaults.

The Reset icon is displayed only if the settings for the anomaly have been changed from defaults.

3 Select OK.

Configuring an anomaly using the CLI

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

The `config ips anomaly` command has 1 subcommand.

config limit

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

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

Command syntax pattern

```
config ips anomaly <name_str>
    set action {clear-session | drop | drop-session | pass
  | pass-session | reset | reset-client | reset-server}
    set log {enable | disable}
    set severity {info | low | medium | high | critical}
    set status {enable | disable}
    set threshold <threshold_integer>
    config limit
      edit <limit_str>
        set ipaddress <address_ipv4mask>
        set threshold <threshold_integer>
    end
  end

get ips anomaly <name_str>
```

Keywords and variables	Description	Default
`name_str`	The name of the anomaly.	

`action {clear-session | drop | drop-session | pass | pass-session | reset | reset-client | reset-server}`	Select an action for the FortiGate unit to take when traffic triggers this anomaly. If logging is enabled, the action appears in the status field of the log message generated by the anomaly.
	`clear-session`
	• The FortiGate unit drops the packet that triggered the anomaly, removes the session from the FortiGate session table, and does not send a reset.
	`drop`
	• The FortiGate unit drops the packet that triggered the anomaly. Fortinet recommends using an action other than `drop` for TCP connection based attacks.
	`drop-session`
	• The FortiGate unit drops the packet that triggered the anomaly and drops any other packets in the same session.
	`pass`
	• 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.
	`pass-session`
	• The FortiGate unit lets the packet that triggered the anomaly and all other packets in the session pass through the firewall.
	`reset`
	• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear-session`. If the Reset action is triggered before the TCP connection is fully established it acts as `clear-session`.
	`reset-client`
	• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear-session`. If the `reset-client` action is triggered before the TCP connection is fully established it acts as `clear-session`.
	`reset-server`
	• 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 this action is set for non-TCP connection based attacks, the action behaves as `clear-session`. If the `reset-server` action is triggered before the TCP connection is fully established it acts as `clear-session`.
		Varies.

Keywords and variables	Description	Default
`default-action {clear-session | drop | drop-session | pass | pass-session | reset | reset-client | reset-server}`	The default action for the anomaly. This option is get only.	
`default-severity {info | low | medium | high | critical}`	The default severity level for the anomaly. This option is get only.	`critical`
`log {enable | disable}`	Enable or disable logging for the anomaly. If logging is enabled, the action appears in the status field of the log message generated by the anomaly.	`enable`
`severity {info | low | medium | high | critical}`	Set the severity level for the anomaly.	`critical`
`status {enable | disable}`	Enable or disable this anomaly.	`enable`
`threshold <threshold_integer>`	For the anomalies that include the `threshold` setting, traffic over the specified threshold triggers the anomaly.	Varies.
`The keywords below are specific to the config limit command.`		
`limit_str`	The name of the limit.	
`ipaddress <address_ipv4mask>`	The ip address and netmask of the source or destination network.	No default.
`threshold <threshold_integer>`	Set the threshold that triggers this anomaly.	No default.

Examples

This example shows how to change the `tcp_land` anomaly configuration.

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

Use the following command to configure the limit for the `tcp_src_session` anomaly.

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

end
```

Use the following command to get information about the anomaly syn_flood.

```
get ips anomaly syn_flood
  name                 : syn_flood
  status               : enable
  status(default)      : enable
  action               : clear-session
  action(default)      : clear-session
  severity             : critical
  severity(default)    : critical
  log                  : enable
  limit:
  == [ default ]
  name: default
```

SYN Flood Attacks

This section describes:

- What is a SYN flood attack?
- How SYN floods work
- The FortiGate IPS Response to SYN Flood Attacks
- Configuring SYN flood protection
- Suggested settings for different network conditions

What is a SYN flood attack?

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

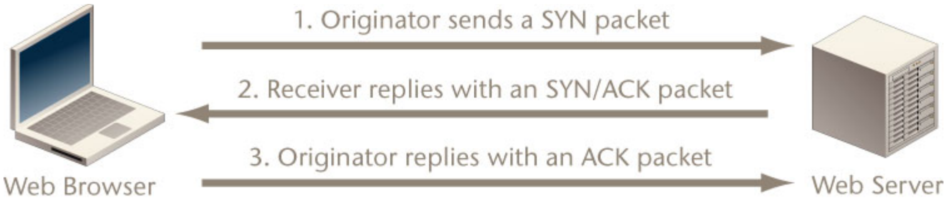
This section provides information about SYN flood attacks and the FortiGate IPS methods of preventing such attacks.

How SYN floods work

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

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

Figure 16: Establishing a TCP/IP connection


1. Originator sends a SYN packet
2. Receiver replies with an SYN/ACK packet
3. Originator replies with an ACK packet
Web Browser
Web Server

1 The originator of the connection sends a SYN packet (a packet with the SYN flag set in the TCP header) to initiate the connection.

2 The receiver sends a SYN/ACK packet (a packet with the SYN and ACK flags set in the TCP header) back to the originator to acknowledge the connection attempt.

3 The originator then sends an ACK packet (a packet with the ACK flag set in the TCP header) back to the receiver to open the connection.

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

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

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

The FortiGate IPS Response to SYN Flood Attacks

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

What is SYN threshold?

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

What is SYN proxy?

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

How IPS works to prevent SYN floods

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

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

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

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

Since the pseudo SYN proxy in the IPS uses a “best effort” 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 17 illustrates the operational behavior of the FortiGate IPS Engine before the SYN Flood threshold is reached. Figure 18 illustrates the operation behavior of the FortiGate IPS Engine after the SYN Flood threshold is reached.

Figure 17: IPS operation before syn_flood threshold is reached

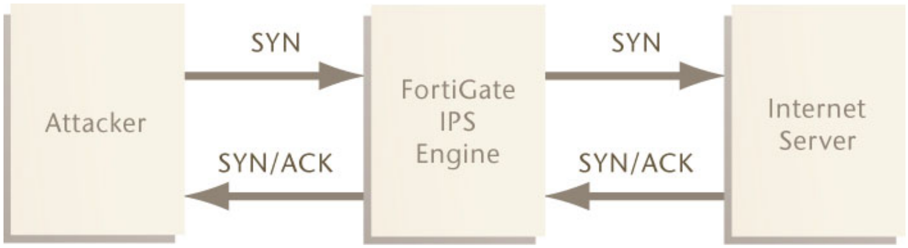
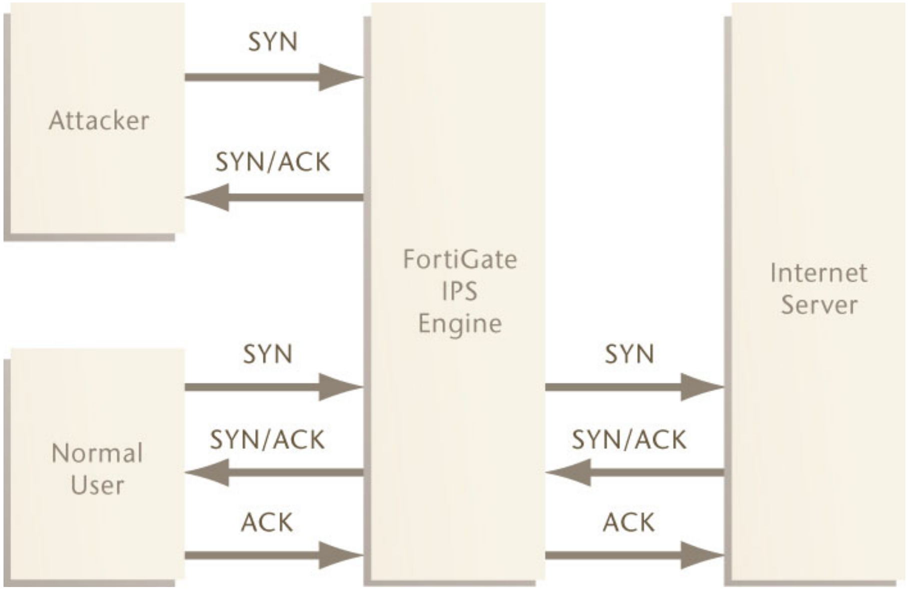


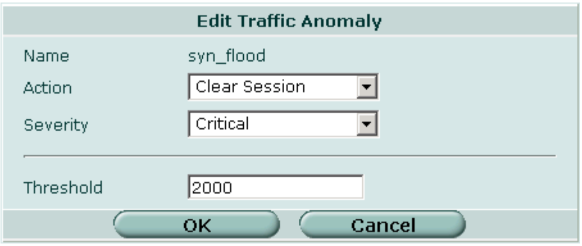
Figure 18: IPS operation after syn_flood threshold is reached



Configuring SYN flood protection

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

Figure 19: Configuring the syn_flood anomaly



Edit Traffic Anomaly

Name	syn_flood
Action	Clear Session
Severity	Critical
Threshold	2000

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

Suggested settings for different network conditions

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

ICMP Sweep Attacks

This section describes:

- What is an ICMP sweep?
- How ICMP sweep attacks work
- The FortiGate IPS response to ICMP sweep attacks
- Configuring ICMP sweep protection
- Suggested settings for different network conditions

What is an ICMP sweep?

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

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

How ICMP sweep attacks work

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

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

The FortiGate IPS response to ICMP sweep attacks

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

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

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

Predefined ICMP signatures

Table 11 describes all the ICMP-related predefined signatures and the default settings for each. See “Configuring signatures using the web-based manager” on page 20 for details about each possible signature action.

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

Table 11: Predefined ICMP sweep signatures

Signature	Description	Default settings
AddressMask.Request	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
Broadscan.Smurf.Echo.Request	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
Communication.Administratively.Prohibited.Reply	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
CyberKit.2.2.Echo.Request	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
DigitalIsland.Bandwidth.Query	Digital Island is a provider of content delivery networks. This company sends ICMP pings so they can better map routes for their customers. Use this signature to block their probes.	Signature enabled Logging enabled Action: Drop
Echo.Reply	This signature detects ICMP echo reply messages responding to ICMP echo request messages.	Signature disabled
ISS.Pinger.Echo.Request	ISS is Internet Security Scanner software that can be used to send ICMP echo request messages and other network probes. While this software can be legitimately used to scan for security holes, use the signature to block unwanted scans.	Signature enabled Logging enabled Action: Drop
Nemesis.V1.1.Echo.Request	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
Oversized.Echo.Request.Packet	This signature detects ICMP packets larger than 32 000 bytes, which can crash a server or cause it to hang.	Signature enabled Logging enabled Action: Pass

Table 11: Predefined ICMP sweep signatures

Signature	Description	Default settings
NMAP.Echo. Request	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
Redirect.Code4. Echo.Request	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
Sniffer.Pro. NetXRay.Echo. Request	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
Superscan.Echo. Request	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
TimeStamp. Request	TimeStamp detects timestamp request messages from a host pretending to be part of the network.	Signature enabled Logging enabled Action: Pass
TJPingPro1.1. Echo.Request	TJPingPro1.1 is a widely-used network tool for older versions of Windows. TJPingPro could be used maliciously to perform an ICMP sweep. ICMP echo request messages sent using this software contain special characters that identify TJPingPro as the source.	Signature enabled Logging enabled Action: Drop
Traceroute.Traffic	Traceroute is a very common network tool available on almost any operating system. This tool could be sued 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
Whatsup.Echo. Request	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

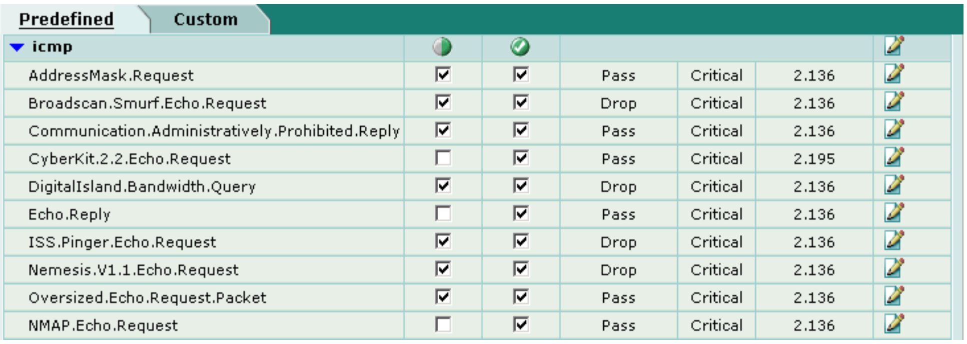
ICMP sweep anomalies

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 **Intrusion Protection > Signatures** and expand the icmp list. Each signature can be configured individually.

Figure 20: Some of the ICMP signatures in the predefined signature list

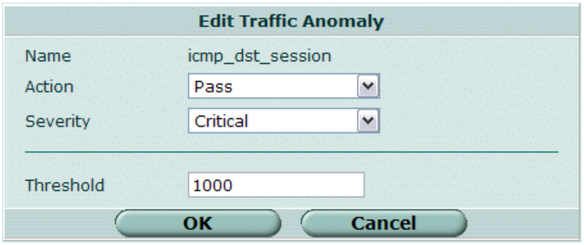


▼ icmp	◐	✓				✎
AddressMask.Request	☑	☑	Pass	Critical	2.136	✎
Broadscan.Smurf.Echo.Request	☑	☑	Drop	Critical	2.136	✎
Communication.Administratively.Prohibited.Reply	☑	☑	Pass	Critical	2.136	✎
CyberKit.2.2.Echo.Request	□	☑	Pass	Critical	2.195	✎
DigitalIsland.Bandwidth.Query	☑	☑	Drop	Critical	2.136	✎
Echo.Reply	□	☑	Pass	Critical	2.136	✎
ISS.Pinger.Echo.Request	☑	☑	Drop	Critical	2.136	✎
Nemesis.V1.1.Echo.Request	☑	☑	Drop	Critical	2.136	✎
Oversized.Echo.Request.Packet	☑	☑	Pass	Critical	2.136	✎
NMAP.Echo.Request	□	☑	Pass	Critical	2.136	✎

See “Predefined Signatures” on page 17 for information about configuring predefined signatures.

To set the configuration for the ICMP sweep anomaly in the web-based manager, go to **Intrusion Protection->Traffic Anomaly**, find icmp_sweep in the anomaly list, and select Edit.

Figure 21: Edit IPS Anomaly: icmp_sweep



Edit Traffic Anomaly

Name	icmp_dst_session
Action	Pass
Severity	Critical
Threshold	1000

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

Suggested settings for different network conditions

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

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

Index

www.fortinet.com

FORTINET™

www.fortinet.com