



**Instant Messaging, Peer to Peer,
and Voice over Internet Protocols
Version 3.0 MR5**

FORTINET™

www.fortinet.com

Instant Messanging, Peer to Peer, and Voice over Internet Protocols
Technical Note
Version 3.0 MR5
September 11, 2007
01-30005-0285-20070911

© Copyright 2007 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.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	5
About IM, P2P, and VoIP protocols.....	5
About this document.....	5
Fortinet documentation	5
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation	7
Customer service and technical support.....	7
Instant Messenger Protocols	9
Firewall Control.....	9
IM Aware Firewalls.....	10
Anti-Virus Control.....	13
Detecting New IM Applications	14
Blocking Older Versions of IM Applications	14
IM/P2P Applications Covered by IPS in FortiOS 3.0.....	14
Peer to Peer Protocols.....	17
Rate Limiting	18
Detecting New P2P Applications.....	18
Voice over Internet Protocol	21
Firewall Controls.....	21
VoIP Logging.....	21
VoIP Rate Limiting	21
Statistics.....	22
Viewing overview statistics.....	22
CLI Commands	23

Introduction

This article introduces you to the Instant Messaging (IM), Peer to Peer (P2P) protocols, Voice over Internet Protocol (VoIP) protocols and the options available to control them with the FortiGate Unified Threat Management System. The following topics are covered in this chapter:

- [About IM, P2P, and VoIP protocols](#)
- [About this document](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

About IM, P2P, and VoIP protocols

Instant Messenger (IM), Peer to Peer (P2P), and Voice over Internet Protocol (VoIP) protocols are gaining in popularity as an essential way to communicate between two or more individuals in real time. Some companies even rely on IM protocols for critical business applications such as Customer/Technical Support.

The most common IM protocols in use today include AOL Instant Messenger, Yahoo Instant Messenger, MSN messenger, and ICQ. Although these are the most common currently in use, there are always new protocols being developed as well as newer versions of older ones.

P2P protocols are most commonly used to transfer files from one user to another and can use large amounts of bandwidth.

VoIP is increasingly being used by businesses to cut down on the cost of long distance voice communications.

Some organizations need to control or limit the use of IM/P2P and VoIP protocols in order to more effectively manage bandwidth use.

About this document

This technical note discusses the capabilities of the FortiGate firewall to control various IM, P2P, and VoIP protocols. Although previous versions were IM and P2P aware, the controls appearing in the protection profile are new with FortiOS v3.0.

Fortinet documentation

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

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

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

Fortinet Knowledge Center

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

Comments on Fortinet technical documentation

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

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.

Instant Messenger Protocols

Many IM protocols are in use today. The ones most widely used include:

- AOL Instant Messenger (AIM) - Introduced by AOL as way to allow members to communicate with one another in real-time to avoid the delay of standard email. Latest versions of AIM allow users to not only text chat, but also voice and video chat without using expensive long distance metered services such as the public switched telephone network (PSTN). AIM service is now free to non-paying members as long as they register with AOL.
- Yahoo Instant Messenger (YIM) - Yahoo, wanting to entice users to sign up for its advertiser paid services, offers this popular free IM service which provides all of the same chat capabilities of AIM and provides a nimble client that is capable of discovering holes in firewalls in order to get around blocked ports.
- MSN Messenger - Microsoft offers a similar service to both AOL and Yahoo. In addition to text message exchange, MSN Messenger offers voice and video conferencing with multiple simultaneous users as a way to entice business users to improve communications, display presentations, and reduce travel expense. MSN Messenger is SIP protocol-based which is a well known IP telephony standard.
- ICQ (abbreviated for "I Seek You") - A popular international IM protocol, ICQ is available on many platforms and operating systems to provide the popular IM features offered by AOL, YIM, and MSN Messenger, and is now owned by AOL TimeWarner. Claiming to be the most widely used chat protocol in the world, ICQ offers video chat, dating, lists, and people search capabilities.

The following topics are included in this section:

- [Firewall Control](#)
- [IM Aware Firewalls](#)
- [Anti-Virus Control](#)
- [Detecting New IM Applications](#)
- [Blocking Older Versions of IM Applications](#)
- [IM/P2P Applications Covered by IPS in FortiOS 3.0](#)

Firewall Control

Firewalls can be used in many cases to block or rate limit certain IM protocols. The FortiGate firewall has predefined services used to block or allow common IM protocols. For example, AIM uses ports 5190-5194, and MSN Messenger uses port 1863 as standard ports for default communications. These IM clients can easily be blocked by closing these ports. Most firewalls are only effective in blocking specific predefined ports so some IM protocols are designed to find other open ports or can be configured to use well known ports such as port 80 to get around the blocked ports.

It is very difficult to block these protocols with standard firewall technology. Because of this, a more effective way of identifying and controlling IM protocols is needed.



Note: If virtual domains are enabled on the FortiGate unit, IM/P2P features are configured globally. To access these features, select **Global Configuration** on the main menu.

IM Aware Firewalls

The FortiGate Unified Threat Management System, an advanced next generation firewall, is IM application aware and uses special protocol decoders to track IM traffic. In FortiOS version 2.80, the FortiGate firewall can block or allow AIM, YIM, MSN, and ICQ individually per protocol by using the Intrusion Prevention System module.

Go to **Intrusion Protection > Signatures > Predefined** to set the IPS action on each of the IM protocols.

Figure 1: Example of IPS signatures in version 2.80

System	Predefined	Custom	Protocol Decoder															
Router	Name																	
Firewall	28Gal_disp_album.php.SQL.Injection			Enable	Logging	Action	Severity	Location	Protocols	OS	Applications	Group						
VPN	3CDaemon.FTP.Server.Information.Disclosure			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Client	FTP	Windows	Other	file_transfer						
User	3COM.OfficeConnect.DoS			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop Session	Low	Server	HTTP	Other	Other	misc						
AntiVirus	3COM.OfficeConnect.SoftReset			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop Session	Low	Server	HTTP	Other	Other	misc						
Intrusion Protection	8Pixel.net.SimpleBlog.SQL.Injection			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	HTTP	All	Other	web_server						
Signature	AA.bot.Botlist.File.Access			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Server	HTTP	Windows	Other	applications						
Anomaly	Aardvark.Topsites.PHP.Arbitrary.Command.Execution			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	HTTP	All	PHP_app	web_app						
Web Filter	Aardvark.Topsites.PHP.Remote.Command.Execution			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	HTTP	All	PHP_app	web_app						
Anti Spam	ABHWhizzy.ABitWhizzy.php.Directory.Traversal			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Medium	Server	HTTP	All	PHP_app	web_app						
IM, P2P & VoIP	Absolute.Image.Gallery.XE.XSS			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Drop	Medium	Server	HTTP	Windows	Other	web_app						
Log&Report	Absolute.Telnet.Title.Bar.Buffer.Overflow			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Client	TELNET	Windows	Other	remote_access						
	ACal.Arbitrary.Command.Execution			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	HTTP	All	PHP_app	web_app						
	Acrobat.Reader.Filespec.Overflow.A			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Client	HTTP	Linux, Other	Adobe	web_app						
	Acrobat.Reader.Filespec.Overflow.B			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Client	HTTP	Linux, Other	Adobe	web_app						
	Acronym.Mod.Admin.Acronyms.PHP.SQL.Injection			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	HTTP	All	PHP_app	web_app						
	Acrowave.Authentication.Bypass			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	TELNET	Windows	Other	remote_access						
	ActionApps.Remote.File.Inclusion			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Medium	Server	HTTP	All	PHP_app	web_app						
	ActiveCampaign.12All.Broadcast.Email.Username.SQL.Injection			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	HTTP	All	Other	web_app						
	ActiveCampaign.KnowledgeBuilder.Remote.File.Inclusion			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Low	Server	HTTP	All	PHP_app	web_app						
	ActivePerl.PerlIS.dll.CGI.Remote.Buffer.Overflow			<input type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	HTTP	Windows	Other	web_app						
	ActivePerl.PerlIS.dll.PL.Remote.Buffer.Overflow			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	HTTP	Windows	Other	web_app						
	ActivePerl.PerlIS.dll.Plx.Remote.Buffer.Overflow			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	High	Server	HTTP	Windows	Other	web_app						

As of FortiOS version 3.0, the FortiGate firewall offers a new IM security module which can also use these special protocol decoders to set up various rules for handling different aspects of IM protocols such as user lists, text messaging, voice/video chat, and file transfers.

User lists can be managed to allow or block certain users. Each user can be assigned a policy to allow or block activity for each IM protocol. Each IM function can be individually allowed or blocked providing the administrator the granularity to block the more bandwidth consuming features such as voice chat while still allowing text messaging. There is also an option to block older versions of the IM protocol if our protocol decoders can only recognize the latest version.

Figure 2: Example of IM user list under IM, P2P&VoIP > User > User List

Protocol	Username	Policy	
AIM	user_1	Block	[Delete] [Edit]
MSN	user5	Allow	[Delete] [Edit]
Yahoo!	user5	Block	[Delete] [Edit]

Figure 3: Example of user policy

User Policy
When unknown IM users connect through the FortiGate, the following action should be taken:

	MSN	Yahoo!	AIM	ICQ
Automatically Allow:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Automatically Block:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

List of Temporary Users Protocol: All

#	Protocol	Username	Policy	Permanent Allow	Permanent Block
1	Yahoo!	block7test	Allow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	MSN	block6test@hotmail.com	Allow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	ICQ	346040689	Allow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4	AIM	block6test	Allow	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Protocol decoders are also used to provide statistical monitoring of IM usage as well as content logging of actual message traffic on a FortiGate unit's hard drive or a FortiAnalyzer appliance.

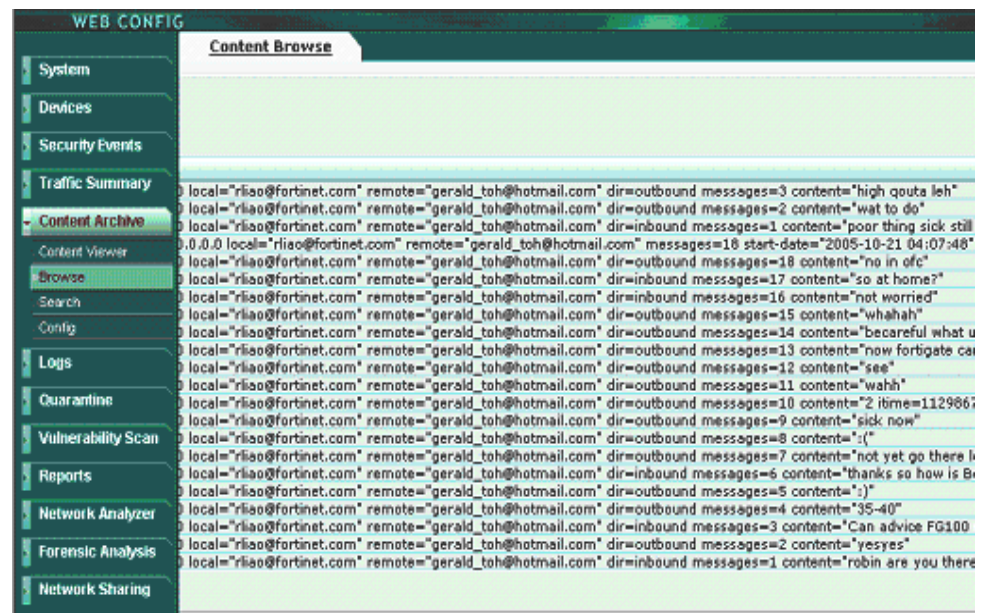
Figure 4: Example of IM usage statistics under IM, P2P&VoIP > Statistics > Protocol

Automatic Refresh Interval: none Refresh Protocol: AIM

Usage Since: 2005-06-06 10:01:32

Category	Item	Value
Users	Current Users	0
	Since Last Reset	0
	Blocked	0
Chat	Total Chat Sessions	0
	Server-based Chat	0
	Group Chat	0
	Direct/Private Chat	0
Messages	Total Messages	0
	Sent	0
	Received	0
File Transfers	Since Last Reset	0
	Sent	0
	Received	0
	Blocked	0
Voice Chat	Since Last Reset	0
	Sent	0
	Blocked	0

Figure 5: Example of IM content logging on a FortiAnalyzer unit

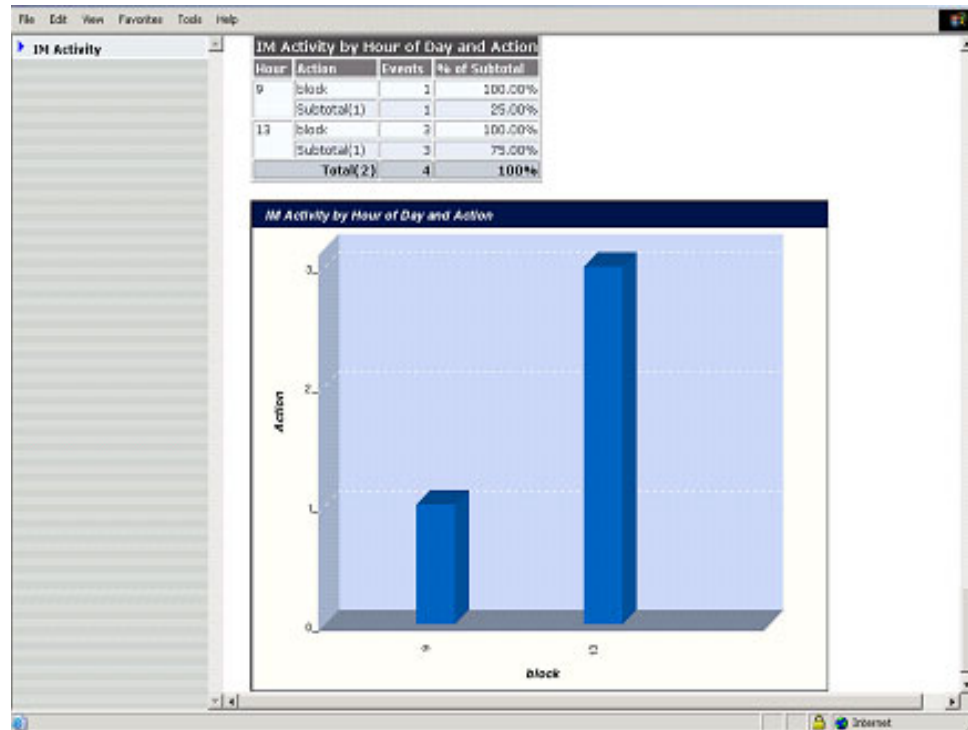


Using the FortiAnalyzer system, you can even generate usage reports by IM username in order to track usage over time. You can log IM chat information and its limitations by enabling **Archive full IM chat info to Fortianalyzer** in the protection profile. You can also generate a variety of different report types, including:

- IM activity by date and action
- Top permitted sources by date
- Top blocked sources by date
- Top permitted destinations by date
- Top blocked destinations by date
- IM activity by month and action
- Top permitted sources by month
- Top blocked sources by month
- Top permitted destinations by month
- Top blocked destinations by month
- IM activity by day of week and action
- IM activity by hour of day and action

For more information, see the FortiAnalyzer documentation.

Figure 6: Example of FortiAnalyzer report.



Note: IM users who are already logged on before changes are made to the IM protection profile, will not be affected until their next login. You cannot disconnect users who have already logged on by enabling logon blocking.

Anti-Virus Control

Virus writers are constantly adapting to get around common antivirus defense methods. IM protocols are becoming a new vehicle for spreading viruses. Another benefit of having IM protocol decoders is the ability to proxy the protocol through the FortiGate antivirus engine. This allows any IM file transfers to be scanned in real-time to prevent the spread of these new viruses. The FortiGate firewall can now be used to configure IM scanning per protection profile.

Figure 7: Example of AV protection profile.

Anti-Virus	HTTP	FTP	IMAP	POP3	SMTP	IM	NNTP	Option
Virus Scan	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
File Pattern	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	-- None --
Pass Fragmented Emails			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
Comfort Clients	<input type="checkbox"/>	<input type="checkbox"/>						
Interval (1 - 900 seconds)	10	10						
Amount (1 - 10240 bytes)	1	1						
Oversized File/Email	Pass	Pass	Pass	Pass	Pass	Pass	Pass	
Threshold (1 - 25 MB)	10	10	10	10	10	10	10	
Add signature to outgoing emails	<input type="checkbox"/> Enable							(SMTP only)

Detecting New IM Applications

New versions of current IM/P2P applications are constantly being produced. In some cases, new applications are readily available.

Although most IM/P2P controls are under **Firewall > Content Profile**, the detection of IM/P2P applications is done by IPS. To detect new IM/P2P applications or new versions of the existing applications, users only need to update the IPS package. By upgrading the IPS package, the user is upgrading the protocol decoders, making IPS more effective. No firmware upgrade is needed.

Blocking Older Versions of IM Applications

Use the following command, `config imp2p old-version`, in the CLI to block IM applications that are older than the following versions:

- MSN 6.0
- ICQ 4.0
- AIM 5.0
- Yahoo 6.0

IM/P2P Applications Covered by IPS in FortiOS 3.0

The table below is a list of IM/P2P applications that are currently recognized by FortiOS 3.0. The table includes the decoders, the applications associated with the decoders and the location of the decoders in the FortiGate interface.



Note: Applications marked as **bold** can connect to multiple P2P networks. Turning **on** IM and P2P decoders and signatures will help improve IPS performance. For example, If the you want to use IPS, but you do not want to block IM or P2P applications, you should leave IM/P2P decoders and signatures enabled. Normally, if you turn off other signatures, the performance will be better, but for IM/P2P, it's the opposite.

Table 1: IM applications covered by IPS in FortiOS 3.0

IPS	Applications
Instant Messaging	
AIM (Protection Profile > IM/P2P)	AIM, AIM Triton
ICQ (Protection Profile)	ICQ
MSN (Protection Profile > IM/P2P)	MSN Messenger
im_decoder:qq	QQ
Yahoo! (Protection Profile > IM/P2P)	Yahoo Messenger
im_decoder:msn_web_messenger	MSN web Messenger
im_decoder:google_talk	Google Instant Messenger
im_decoder:rediff	Rediff Instant Messenger



Note: If you encounter an IM/P2P applications that is not listed above, make sure that you have the latest upgrade for the IPS.
If you have the latest upgrade and the IM/P2P application is still unrecognized, use Custom Signatures.

Peer to Peer Protocols

Peer to Peer (P2P) protocols also have some of the same capabilities as IM protocols, such as live text chat and file transfers. P2P differs from IM however in that instead of having a sponsor controlled central server system, you can set up as many servers as you want independent of the sponsor. P2P is typically used to set up file sharing networks, where the files can be hosted by anyone willing to install the P2P server software. Skype is a popular new P2P protocol which can be used for text message and voice chat over the Internet for free. The FortiGate firewall does have protocol decoders for most popular P2P protocols including Skype, Gnutella, eDonkey, Bit Torrent, KaZaa and WinNY. However at this time it only provides allow, block, or rate limiting capabilities since file transfers are normally encrypted by the individual protocol, which prevents the FortiGate from being able to analyze or scan the content for viruses.

Figure 8: Example of IPS control of KaZaa in version 2.80

Configure Predefined IPS Signature	
Signature	kazaa
Enable	<input checked="" type="checkbox"/>
Logging	<input checked="" type="checkbox"/>
Action	Pass
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

In FortiOS 3.0, the FortiGate firewall can also monitor statistics on P2P usage. For each protocol, you can view average bandwidth consumption in bytes per second.



Note: Note that due to the encrypted nature of Skype, the FortiGate firewall is unable to monitor usage for that particular protocol.

Figure 9: P2P usage statistics under IM, P2P&VoIP > Statistics > Summary

Automatic Refresh Interval: none		Usage Since: 2007-08-16 22:00:06				Reset Stats
IM Usage						
	MSN	Yahoo!	AIM	ICQ		
Users						
Current Users	0	0	0	0		
Since Last Reset	0	0	0	0		
Blocked	0	0	0	0		
Chat						
Total Chat Sessions	0	0	0	0		
Total Messages	0	0	0	0		
File Transfers						
Since Last Reset	0	0	0	0		
Blocked	0	0	0	0		
Voice Chat						
Since Last Reset	0	0	0	0		
Blocked	0	0	0	0		
P2P Usage						
	BitTorrent	eDonkey	Gnutella	KaZaa	WinNY	
Total Bytes	0.00 B	0.00 B	0.00 B	0.00 B	0.00 B	
Average Bandwidth	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	0.00 B/s	
VoIP Usage						
				SIP	SCCP	
Sessions						
Active Sessions (phones connected, etc)				0	0	
Voice Calls						
Total Calls (since last reset)				0	0	
Calls Failed/Dropped				0	0	
Calls Succeeded				0	0	



Note: If virtual domains are enabled on the FortiGate unit, IM/P2P features are configured globally. To access these features, select **Global Configuration** on the main menu.

Rate Limiting

Another advanced capability of FortiGate firewalls is P2P rate limiting. Rate limiting can be used to block or limit the amount of bandwidth consumed by P2P protocols and more effectively manage limited Internet resources.

Rate limiting is also done in the firewall policy protection profile so that it can be enabled on a per-policy basis. You can limit each protocol to a maximum amount of bandwidth consumed in kilobytes per second.



Note: Due to the encrypted nature of Skype, the FortiGate firewall is unable to rate-limit for that protocol. Only the Block and Pass options are available for that protocol.

Figure 10: Example of P2P rate limiting in a protection profile

IM / P2P					
	<input checked="" type="checkbox"/> AIM	<input type="checkbox"/> ICQ	<input checked="" type="checkbox"/> MSN	<input checked="" type="checkbox"/> Yahoo!	
Block Login	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Block File Transfers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Block Audio	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Inspect Non-standard Port	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	BitTorrent	eDonkey	Gnutella	KaZaa	Skype
Action	Rate Limit	Rate Limit	Block	Rate Limit	Pass
Limit (KBytes/s)	40	45	0	50	0

Detecting New P2P Applications

New versions of current IM/P2P applications are constantly being produced. In some cases, new applications are readily available.

Although most IM/P2P controls are under **Firewall > Content Profile**, the detection of IM/P2P applications is done by IPS. To detect new IM/P2P applications or new versions of the existing applications, users only need to update the IPS package. No firmware upgrade is needed.



Note: Applications marked as **bold** can connect to multiple P2P networks. Turning **on** IM and P2P decoders and signatures will help improve IPS performance. For example, if you want to use IPS, but you do not want to block IM or P2P applications, you should leave IM/P2P decoders and signatures enabled. Normally, if you turn off other signatures, the performance will be better, but for IM/P2P, it's the opposite.

Table 2: P2P applications covered by IPS in FortiOS 3.0

IPS	Application
P2P	
BitTorrent (Protection Profile > IM/P2P)	BitComet Bitspirit Azureus Shareaza
eDonkey (Protection Profile > IM/P2P)	eMule Overnet Edonkey2K Shareaza BearShare MLdonkey iMesh
Gnutella (Protection Profile > IM/P2P)	BearShare Shareaza LimeWire Xolox Swapper iMesh MLdonkey Gnucleus Morpheus Openext Mutella Qtella Qcquisition Acquisition NapShare gtk-gnutella
KaZaA (Protection Profile > IM/P2P)	KaZaA
Skype (Protection Profile > IM/P2P)	Skype
WinNY (Protection Profile > IM/P2P)	WinNY
p2p_decoder:ares	Ares Galaxy
p2p_decoder:direct_connect	DC++



Note: If you encounter an IM/P2P applications that is not listed above, make sure that you have the latest upgrade for the IPS.
If you have the latest upgrade and the IM/P2P application is still unrecognized, use Custom Signatures.

Voice over Internet Protocol

With FortiOS v3.0 MR4 firmware, you can control and monitor the usage of VoIP protocols.

The VoIP menu provides statistics for network VoIP usage.

FortiOS supports two VoIP protocols: Session Initiation Protocol (SIP) and Skinny Client Control Protocol (SCCP).

The following topics are included in this section:

- [Firewall Controls](#)
- [Statistics](#)
- [CLI Commands](#)

Firewall Controls

In the Firewall Protection Profiles, you are able to control two functions within the VoIP protocols: logging and rate limiting. Logging allows you to enable tracking of information available in the Statistics section.

The VoIP options allow you to set the rate limiting for each of the VoIP protocols supported by the FortiGate unit.

VoIP Logging

You can log VoIP calls.

To enable VoIP logs

- 1 Go to **Firewall > Protection Profile**.
- 2 Select create New to create a new protection profile or the Edit icon to edit a profile.
- 3 Select the blue arrow to expand the Logging options.
- 4 Select Log VoIP Activity.
- 5 Select OK.

VoIP Rate Limiting

You can configure VoIP rate limiting for Session Initiated Protocol (SIP) and Skinny Client Control Protocol (SCCP) or Skinny protocol. SIP and SCCP are two types of VoIP protocols. Rate limiting is generally different between SCCP and SIP. For SIP, rate limiting is for that SIP traffic flowing through the FortiGate unit. For SCCP, the call setup rate is between the FortiGate unit and the clients because the call manager normally resides on the opposite side of the FortiGate unit from the clients.

To configure VoIP rate limiting

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

- 2 Select create New to create a new protection profile or the Edit icon to edit a profile.
- 3 Select the blue arrow to expand the VoIP options.
- 4 Select the SIP and SCCP checkboxes.
- 5 Enter a number for requests per second in the Limit REGISTER request (requests/sec) (SIP only) field.
- 6 Enter a number for requests per second in the Limit INVITE request (requests/sec) (SIP only) field
- 7 Enter a number for the maximum calls per minute in the Limit Call Setup (calls/min) (SCCP only) field.
- 8 Select OK.

Statistics

You can view the VoIP statistics to gain insight into how the protocols are being used within the network. Overview statistics are provided for all supported VoIP protocols.



Note: If virtual domains are enabled on the Instant Messaging, Peer to Peer, and Voice over Internet Protocols unit, IM, P2P and VoIP features are configured globally. To access these features, select **Global Configuration** on the main menu.

Viewing overview statistics

The **IM, P2P&VoIP > Statistics > Summary** page provides a summary of statistics for all VoIP protocols.

Figure 11: VoIP statistics summary

VoIP Usage	SIP	SCCP
Sessions		
Active Sessions (phones connected, etc)	0	0
Voice Calls		
Total Calls (since last reset)	0	0
Calls Failed/Dropped	0	0
Calls Succeeded	0	0

VoIP Usage	For SIP and SCCP protocol
Active Sessions (phones connected)	Number of sessions that are currently active
Total calls (since last reset)	Total VoIP calls since the last FortiGate unit reset.
Calls failed/Dropped	Number of VoIP sessions that failed during the reporting period.
Calls Succeeded	Number of VoIP sessions that were successfully completed during the reporting session.

CLI Commands

The CLI commands to configure SIP and SCCP settings are under:

```
config firewall profile
```

The TCP and/or UDP port that the SIP proxy will listen on can be set per VDOM:

```
config system settings
    set sip-tcp-port
    set sip-udp-port
end
```

For details, see the config firewall chapter of the *FortiGate CLI Guide*.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com