

FortiGate Firewall Version 3.0 Frequently Asked Questions

FAQ



Firewall Questions

Q: Give me an executive summary of FortiOS version 3.0 new firewall functionality.

A: Major new functionality in FortiOS v3.0 includes:

- IM/P2P protocol integration
- On-the-fly FW policy creation
- Active Directory integration including:
 - Single sign-on
 - Policy-based control on user/group
- Independent VDOMs in Transparent or Route/NAT modes
- GUI based routing protocol control of BGP, OSPF and RIP
- GUI integration of Log and report control from FortiAnalyzer
- Route-based IPSec VPN tunnels
- SSL-VPN support

Q: What are some of the firewall specific enhancements?

A: New 3.0 firewall specific enhancements are:

- Improved user-configurable dashboard layout means faster interpretation of device status
- Microsoft Active Directory support to enable rapid integration with existing authentication services
- On-The-Fly Policy creation. Firewall policies can be created without objects being created first. This enables easier deployment and maintenance for enterprise environments.
- Customizable and sort-able field firewall policy listing feature to easily search and find specific policies through large lists of policies.
- Additional granularity of FTP protocol policy usage including separate FTP-PUT and FTP-GET services.

Q: What are some of the routing and VDOM enhancements?

A: We now have BGP support and GUI configuration for BGP, OSPF and RIP routing protocols. As for VDOMs, you can now specify each individual VDOM on a single FW to operate in either Transparent or Route/NAT mode. We also have more per-VDOM configuration granularity including VDOM specific protection profiles. All FortiGate models now support up to 10 VDOMs in either NAT/Route mode as a standard feature, and the high-end (models 3000 and above) can be upgraded to up to 250 VDOMs for an extra charge.

Q: What specific IM features do we offer?

A: We offer IM antivirus scanning for most common IM protocols (AIM, ICQ, MSN, and Yahoo). We also offer username access controls/monitoring and ability to block IM messages, file transfers, and audio. These features are attractive to MSSPs who can sell this as a service, or to enterprises concerned about the proliferation of viruses or bandwidth control via IM protocols.

Q: What advantages does Fortinet offer over IM “point product” vendors such as FaceTime, Akonix, and IMLogic?

A: Fortinet offers the only complete network security infrastructure solution, combining perimeter and datacenter firewall and VPN functionality, antivirus scanning, intrusion detection and prevention, spam and web filtering, and spyware/greyware filtering. Vendors of “point products” offer only IM scanning and control and must leverage partnerships to offer complete solutions. For example, Akonix offers IM scanning, filtering, and logging, but has no other security features and customers have to integrate it into their existing security infrastructure of Firewalls, antispam gateways, etc.

Q: What P2P protocol enhancements are offered?

A: We now support per protection profile blocking and rate limiting for the most commonly used Peer to Peer protocols including: BitTorrent, eDonkey, Gnutella, KaZaa, and WinNY, plus the ability to block or allow Skype. We can also monitor bandwidth consumption of these major P2P protocols.

Q: What are some of the logging and reporting enhancements?

A: Content Archiving is added which includes Email content logging for SMTP, POP3, and IMAP, web content logging for HTTP and FTP downloads, and IM message content logging, including both text and attachment archiving using the FortiAnalyzer series logging and reporting appliances.

Q: What are the big new VPN features?

A: We now offer Route-based IPsec VPNs where a remote VPN site can be assigned a route as opposed to an interface which allows for more dynamic VPN fail-over capabilities. We have also introduced a new SSL-VPN feature where the FortiGate can be used to support two modes of SSL-VPN clients. The Web Mode supports most SSL enabled web browsers (such as IE or Firefox) and allows a secure tunnel to be terminated on the FortiGate which then proxies the connection to standard non-SSL web server applications such as HTTP, FTP or Telnet. The Tunnel Mode requires either an Active-X or Java client applet be downloaded and installed on the clients web browser, which then allows many more non-web based applications to be accessed from an SSL enabled browser such as custom applications, VoIP, etc.

Q: What are some management enhancements for firewall control?

A: FortiManager now offers new Device and Policy Manager tools which allow better control of configuration files and group policies, and new Deployment Manager and Script Manager tools allow you to more easily roll out configuration changes to a large number of devices. FortiManager is also now more tightly integrated with FortiAnalyzer for improved reporting and analysis. Reporting is emerging as a key feature for increasing regulatory compliance (Sarbox, HIPPA, Basel II). FortiAnalyzer now offers packet capture and alert monitoring to extend real-time troubleshooting capabilities. New Forensic Analysis features provide tools to search through log archives for usernames, email names, or IM names.

Q: What VoIP control features are available?

A: The FortiGate series now supports three major VoIP protocol application layer gateways (ALGs) including H.323, SIP, and SCCP (Skinny). Each ALG allows the FortiGate to provide NAT firewall protection of VoIP devices, monitoring and blocking of unwanted VoIP traffic, and IPS protection of VoIP protocol anomalies, denial of service attacks, buffer overflows, and header manipulation attacks.

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

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

Disclaimer

Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. More specific information is available on request from Fortinet. Please note that Fortinet's product information does not constitute or contain any guarantee, warranty or legally binding representation, unless expressly identified as such in a duly signed writing.

FAQ127 0307 R1