FortiGate™-5000 Series

Large Enterprises
Managed Security Service Providers
Carrier Networks

Datasheet

High Performance Modular Multi-Threat Security Solutions

Today's Threats Against Large Networks

Threats against today's networks are complex, blended attacks that infect computers, steal confidential information, create denials of service, or cause costly network outages. Point-based security appliances are inadequately equipped to protect against these attacks because of the multitude of attack vectors used. The FortiGate-5000 Series addresses this problem by tightly integrating multi-threat protection into a purpose-built platform to effectively block today's file-based threats and network-based threats. Examples of critical threats that are blocked by the FortiGate include: viruses, Trojans, worms, phishing schemes, intrusion attempts, denial of service (DoS) attacks and an ever increasing number of attacks that use blended threat vectors.

Leading Edge Chassis-Based Security Platform

The Fortinet FortiGate-5000 Series of Advanced Telecom Computing Architecture (AdvancedTCA or ATCA) security chassis deliver multi-gigabit performance and integrated multi-threat protection ideal for securing high-bandwidth enterprise and service provider networks. Complete Unified Threat Management (UTM) features include: content inspection firewall, VPN, intrusion prevention, web filtering, antispam, antivirus, Instant Messaging (IM) controls and Peer-to-Peer (P2P) controls. These security technologies work together to prevent blended attacks from affecting assets protected by the FortiGate system. The FortiGate-5000 Series features three chassis designs and multiple security modules that meet stringent enterprise and service provider requirements. Highly available configurations with redundant power supplies and fans combined with superior UTM features ensure non-stop availability of mission-critical network applications. The Fortinet FortiGuard™ Security Subscription service makes the FortiGate-5000 Series an affordable and easy-to-manage security solution for large enterprises and service provider customers.

Key Problems	Solutions
High-speed networks require high-performance security systems which will not introduce delays or latency onto the network	The FortiGate-5000 Series provides a scalable platform that is 10 Gigabit Ethernet ready and delivers throughput ranging from 5 Gbps to 70 Gbps while maintaining ulta-low latency for even the most time-sensitive applications.
Virtual server farms need virtualized security solutions to reduce physical space, power and cost	The FortiGate-5000 Series provides an optional high-density virtual domain (VDOM) feature to allow up to 250 VDOMs per FortiGate module and up to 3500 VDOMs per chassis.
Threats against IT systems commonly include attacks that operate at the network and content levels	The FortiGate-5000 Series provides complete threat protection with the ability to tailor the security policy down to the network or even host level. This means that the security policy can adapt to the customer's requirements without requiring changes in hardware or software components.
Data centers require space saving, highly modular, and serviceable networking and security systems for the highest reliability.	FortiGate-5000 provides fully modular chassis systems with complete redundancy features and hot swappable components including blade modules, power supplies, and fan trays to keep mission critical applications running.

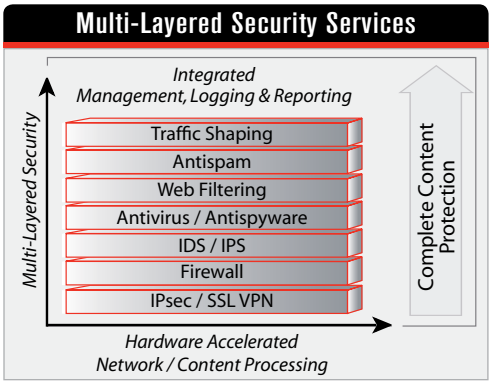
FortiGate-5140
14-slot chassis

FortiGate-5050
5-slot chassis

FortiGate-5020
2-slot chassis

Fortinet's Multi-Layered Security Solution

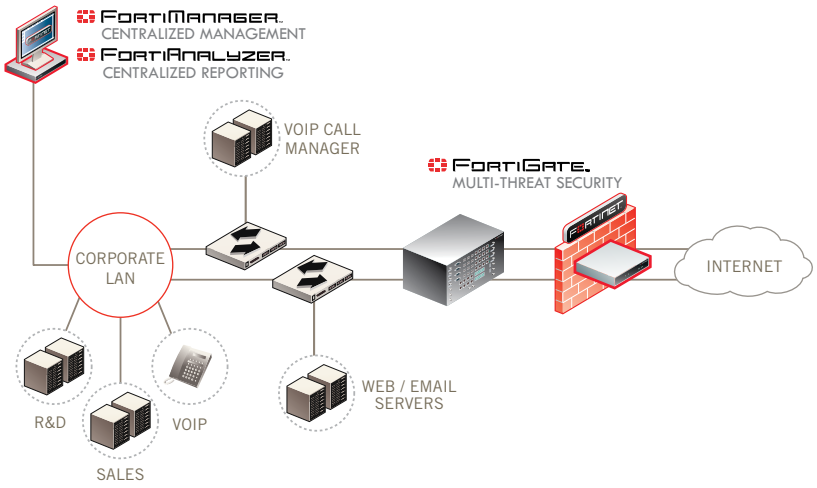
Fortinet's multi-layered security solutions efficiently and economically provide an integrated set of security services in a single, easy-to-manage high-performance appliance that is capable of supporting a wide range of deployment scenarios. In addition, FortiGuard Security Subscription Services include updates for antivirus, antispyware, antispam, and Web filtering services to ensure that your security environment remains current and your corporate resources remain protected against the latest threats. FortiGate systems come with a one-year limited hardware warranty and 90-day limited software warranty.

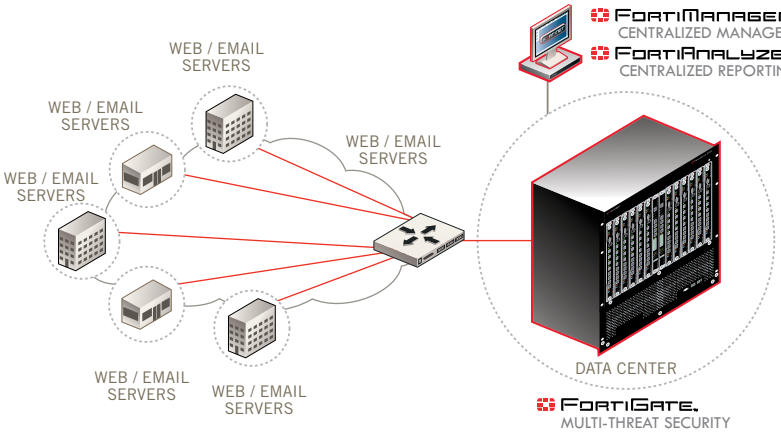


The FortiGate-5000 Series secure large enterprise, service provider and carrier networks.

Next-Generation Perimeter Security

Firewalls alone aren't enough to block today's blended threats. When single packets are examined by point products with no concern for multi-vector attacks, blended threats often pass undetected. Combining content inspection firewall technology with gateway antivirus and intrusion prevention allows packet flows to be tracked. Fortinet multi-layered security technologies examine entire packet flows, from content inspection through reassembly, stopping threats at the perimeter before corporate resources are compromised.



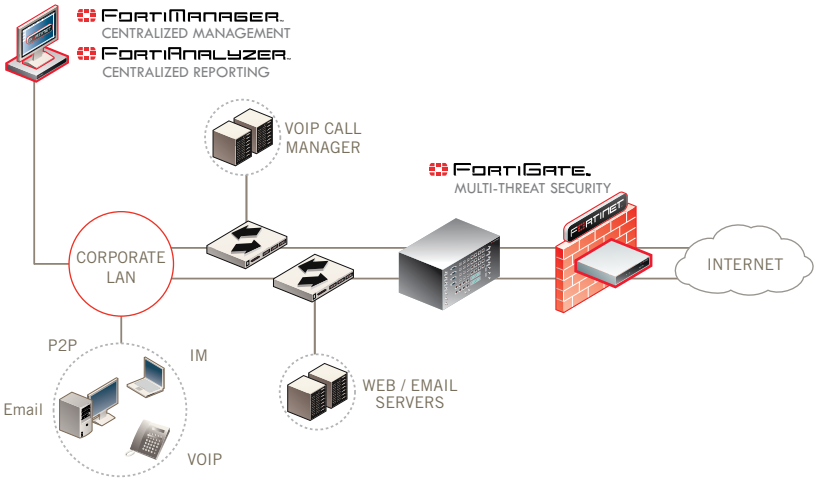


MSSP Core Security

The FortiGate-5000 Series delivers comprehensive security for Managed Security Service Providers (MSSPs). The full suite of ASIC-accelerated security modules allows for customizable features for specific customers, while virtualization features like Virtual Domains (VDOMs) provides up to 3,500 separate security domains. Finally, the full suite of Fortinet integrated management applications—including granular reporting features—offer unprecedented visibility into the security posture of customers while illustrating their highest risks.

Secure Messaging

Email is an essential corporate communication tool. Malware has adapted to this trend and email is now a primary vector of transmission of malcode threats. Instant messaging is quickly becoming a primary propagation vector as IM adoption rate increases. As with any new technology, IM introduces security risks in the form of a new generation of malware that could potentially infect corporate resources. By combining Fortinet antispam technology, IM and P2P controls, antivirus scanning, and web filtering, customers can ensure that email and other messaging remains secure and won't result in lost revenue or lost data.



ATCA Chassis Specifications

HARDWARE SPECIFICATIONS	FortiGate-5020	FortiGate-5050	FortiGate-5140
Available Slots	2	5	14
High Availability Backplane	Built-in	Built-in	Built-in
Dual Switch Module Support	No	Yes	Yes
Max FW Throughput	10 Gbps	25 Gbps	70 Gbps
Max VPN (IPSec) Performance	1.6 Gbps	4 Gbps	11.2 Gbps
Concurrent Sessions	Up to 2M	Up to 5M	Up to 14M
DIMENSIONS (H, W, L, weight)	5.25 inches 17 inches 15.5 inches 35.5 lb (16.1 kg)	8.75 inches 17 inches 15.5 inches 26.75 lb (12.1 kg)	21 inches 19 inches 19 inches 64.5 lb (29.3 kg)
POWER REQUIRED	AC	DC/AC*	DC/AC*
POWER CONSUMPTION (AVG)	Varies based on Configuration	Varies based on Configuration	Varies based on Configuration
ENVIRONMENTAL	Operating temperature: 32 to 104 deg F (0 to 40 deg C) Storage temperature: -13 to 158 deg F (-25 to 70 deg C) Humidity: 5 to 95% non-condensing		
COMPLIANCE	FCC Class A Part 15		
CERTIFICATIONS	ICSA Labs: Antivirus, Firewall, IPSec, SSL-VPN, and IPS NSS Group: UTM Tested and Approved FIPS 140-2, Common Criteria EAL 4+ Firewall (Please contact your Fortinet Sales Representative for a complete list of product certifications)		

* Optional FortiGate-5053 Power Supply Shelf used to provide AC power to the FortiGate-5050 or FortiGate-5140 Chassis.

ATCA Blade Specifications

PERFORMANCE SPECIFICATIONS	FortiGate-5001SX	FortiGate-5001FA2	FortiGate-5005FA2	FortiSwitch-5003	FortiController-5208
SFP Ports	4	4	8	0	8 + 2 x 10GbE (XFP)
10/100/1000 Base-T Ports	4	4	0	3+1 mananagement	1 management
Network Processor Accelerated Ports	N/A	2	2	N/A	N/A
Concurrent Sessions	1M	1M	1M	N/A	N/A
New Sessions / Sec	20,000	20,000	30,000	N/A	N/A
Firewall Throughput	4 Gbps	4 Gbps	5 Gbps	N/A	N/A
VPN (IPSec) Throughput	600 Mbps	600 Mbps	800 Mbps	N/A	N/A
Maximum VPN Tunnels	10,000	10,000	64,000	N/A	N/A
IPS Throughput	2 Gbps	2 Gbps	3 Gbps	N/A	N/A
Antivirus Throughput	250 Mbps	250 Mbps	300 Mbps	N/A	N/A
Unlimited User Licenses	Yes	Yes	Yes	N/A	N/A
Maximum Policies	100,000	100,000	100,000	N/A	N/A
Virtual Domains (VDOMs)	10/250*	10/250*	10/250*	N/A	N/A

Fortinet Unified Security Solutions

All-inclusive, cost-effective security solution	Fortinet offers a lower total cost of ownership with the most complete set of functions including: firewall, VPN, antivirus, intrusion prevention, antispyware, web filtering, and antispam
Automated updates of antivirus/antispyware and IPS security content	Around-the-clock protection against the latest threats. Virus and intrusion encyclopedia covers more than 60,000 different threats
High performance custom hardware	The Fortinet FortiASIC delivers superior performance and reliability, ensuring that the security appliance does not interfere with the flow of mission-critical traffic
Integrated multi-port switch	Eliminates the need for external switches and provides enhanced connectivity options
Secure Web UI for easy deployment and management	Quick and easy configuration wizard walks administrators through initial setup and graphical user interface offers at-a-glance security event and performance monitoring
Security hardened custom Operating System (OS)	Underlying FortiOS™ is ICSA Labs-certified and offers a comprehensive command-line interface

Fortinet's ASIC-Based Advantage

FortiASIC is the foundation of Fortinet's unique hardware technology. FortiASIC is a family of purpose built, high-performance network and content processors that uses an intelligent proprietary content scanning engine and multiple algorithms to accelerate compute-intensive security services. FortiASIC provides the performance required to deliver enterprise and carriers-class UTM services. Coupled with the FortiOS security hardened Operating System, FortiASIC delivers extreme performance and security.

FortiOS: Developed for Security

FortiOS is the software foundation of FortiGate multi-threat security platforms. Developed solely for security, performance and reliablity, it is a purpose-built operating system that leverages power of the the FortiAISC content and network processors. FortiOS enables a comprehensive suite of security services – content inspection firewall, IPS, antivirus, web filtering, antispam, IM/P2P, virtual network security and bandwidth shaping. FortiOS is a complete suite of UTM security services and is certified for Common Criteria EAL 4+.

FortiGate-5000 Series

	FortiGate-5020	FortiGate-5050	FortiGate-5140

FortiGate-5000-series platforms provide the following security features:

FIREWALL
ICSA Labs Certified (Enterprise Firewall)
NAT, PAT, Transparent (Bridge)
Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
User Group-Based Authentication
SIP/H.323 NAT Traversal
WINS Support
Customized Protection Profiles

VIRTUAL PRIVATE NETWORK (VPN)
ICSA Labs Certified (IPSec & SSL)
PPTP, IPSec, and SSL
Dedicated Tunnels
DES, 3DES, and AES Encryption Support
SHA-1/MD5 Authentication
PPTP, L2TP, VPN Client Pass Through
Hub and Spoke VPN Support
IKE Certificate Authentication
IPSec NAT Traversal
Dead Peer Detection
RSA SecurID Support

INTRUSION PREVENTION SYSTEM (IPS)
ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update

ANTIVIRUS
ICSA Labs Certified (Gateway Antivirus)
Includes AntiSpyware and Worm Prevention
HTTP/SMTP/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels
Automatic "Push" Virus Database Update
File Quarantine Support
Block by File Size or Type

WEB FILTERING
URL/Keyword/Phrase Block
URL Exempt List
Content Profiles
Blocks Java Applet, Cookies, Active X
FortiGuard Web Filtering Support

ANTISPAM
Real-Time Blacklist/Open Relay Database Server
MIME Header Check
Keyword/Phrase Filtering
IP Address Blacklist/Exempt List
Automatic Real-Time Updates From FortiGuard Network

TRAFFIC SHAPING
Policy-based Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth

NETWORKING/ROUTING
Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
Multi-Zone Support with Routing Between Zones
Route Between Virtual LANs (VDOMS)
Multi-Link Aggregation (802.3ad)

MANAGEMENT/ADMINISTRATION OPTIONS
Console Interface (RS-232)
WebUI (HTTP/HTTPS) and Command Line Interface
Telnet / Secure Command Shell (SSH)
Role-Based Administration
Multi-language Support
Multiple Administrators and User Levels
Upgrades and Changes Via FTP and WebUI
System Software Rollback
Central Management via FortiManager (optional)

LOGGING/MONITORING
Internal Logging
Log to Remote Syslog/WELF server
Graphical Real-Time and Historical Monitoring
SNMP
Email Notification of Viruses And Attacks
VPN Tunnel Monitor
Optional FortiAnalyzer Logging

USER AUTHENTICATION OPTIONS
Local Database
Windows Active Directory (AD) Integration
External RADIUS/LDAP Integration
IP/MAC Address Binding
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support

VIRTUAL DOMAINS (VDOMs)
Separate Firewall/Routing domains
Separate Administrative domains
Separate VLAN interfaces
10 VDOMs (standard)
Up to 250 VDOMs (optional license - models 3000 and higher)

HIGH AVAILABILITY (HA)
Active-Active, Active-Passive
Stateful Failover (FW and VPN)
Device Failure Detection and Notification
Link Status Monitor
Link failover

INSTANT MESSENGER / PEER-TO-PEER ACCESS CONTROL

AOL-IM	Yahoo	MSN	
ICQ	Gnutella	BitTorrent	
WinNY	Skype	eDonkey	KaZaa

FortiGuard Security Subscription Services

With FortiGuard™ Security Subscription services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security intelligence. FortiGuard services deliver the latest security content directly to Fortinet products. Fortinet offers four standard subscription services: Antivirus, Intrusion Prevention, Web Filtering and Antispam services to protect against multiple types of new and emerging threats. FortiGuard services are updated by the Fortinet Global Threat Research Team, a team of experts working around the clock and around the world to keep Fortinet customers secure. The Fortinet Global Threat Research Team enables Fortinet to deliver comprehensive multi-threat protection, including zero-day protection from new and emerging threats. The FortiGuard Network is a network of global data centers that automatically deliver updates quickly and reliably to Fortinet products.

For customers requiring guaranteed response time to suspicious malware threats, Fortinet offers a premier version of the FortiGuard Antivirus Security Subscription service. Along with Service Level Agreements (SLAs), the premier service provides the customer with a direct conduit to the Fortinet Global Threat Research Team.

Fortinet also offers a premier version of the FortiGuard Web Filtering Security Subscription service. This higher-tier service offering includes guaranteed SLAs and a larger quota for rating URLs submitted to the Fortinet Global Threat Research Team.

FortiCare Support Services

Includes:

- 24/7/365 FortiCare Web-based support
- Technical account management service available
- 8x5 telephone-based technical support (24x7 - optional)
- Professional services available
- 1-Year limited hardware warranty
- 90-day limited software warranty

FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com/sales

EMEA SALES OFFICE-FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33-4-8987-0510
Fax +33-1-5858-0025

APAC SALES OFFICE-HONG KONG
Fortinet Incorporated
Room 2429-2431, 24/F Sun Hung Kai Centre
No.30 Harbour Road, WanChai, Hong Kong
Tel +852-3171-3000
Fax +852-3171-3008

©2006-2008 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are trademarks or registered trademarks of the Fortinet Corporation 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. Licensed under U.S. Patent No. 5,623,600. Although Fortinet has attempted to provide accurate information in these materials, Fortinet assumes no legal responsibility for the accuracy or completeness of the information. Please note that no Fortinet statements herein constitute or contain any guarantee, warranty or legally binding representation. All materials contained in this publication are subject to change without notice, and Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

DAT136-0408-R9