

FortiGate-5000 Series

For Large Enterprises and Managed Security Service Providers

Datasheet

High Performance 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 content 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 Solution Features and Benefits

<ul style="list-style-type: none"> Industry proven, multi-threat security architecture for large enterprises and service providers 	Delivers powerful, integrated application security ideal for protecting against today's complex blended threats
<ul style="list-style-type: none"> Extremely high price-to-performance ratio 	Low total cost of ownership, ultra high-performance, and wide range of deployment options matches complex network security requirements
<ul style="list-style-type: none"> Easy to deploy ATCA-based chassis 	ATCA-based design allows for rapid deployment to quickly secure mission-critical networks
<ul style="list-style-type: none"> Modular software and hardware architecture 	Enables rapid support of new technologies, such as VoIP, IM, and P2P, to be secured without unnecessary interruptions
<ul style="list-style-type: none"> Customized and detailed logging and reporting tools 	FortiGate systems combined with FortiAnalyzer and FortiManager offer extensive reporting, logging, and data archiving options for regulatory compliance, trending, or baselining



FortiGate-5140
14-slot chassis



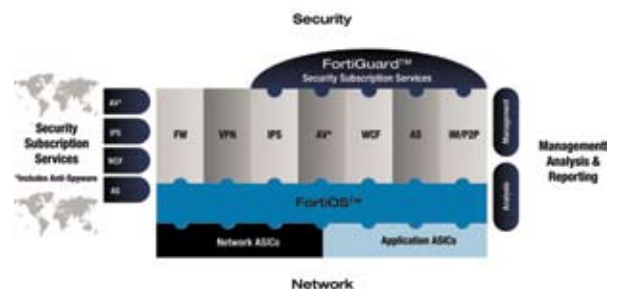
FortiGate-5050
5-slot chassis



FortiGate-5020
2-slot chassis

The Fortinet Security Solution

The Fortinet market-leading suite of security modules offer unparalleled protection from today's blended threats. Ultra-high performance is achieved by combining custom content processing ASICs with the FortiOS security-hardened operating system. Coupling these with FortiGuard Security Subscription Services enables up-to-the-minute network protection against viruses, spam, inappropriate web content, and blended threats that propagate via applications like IM, P2P, email, Web, and VoIP.

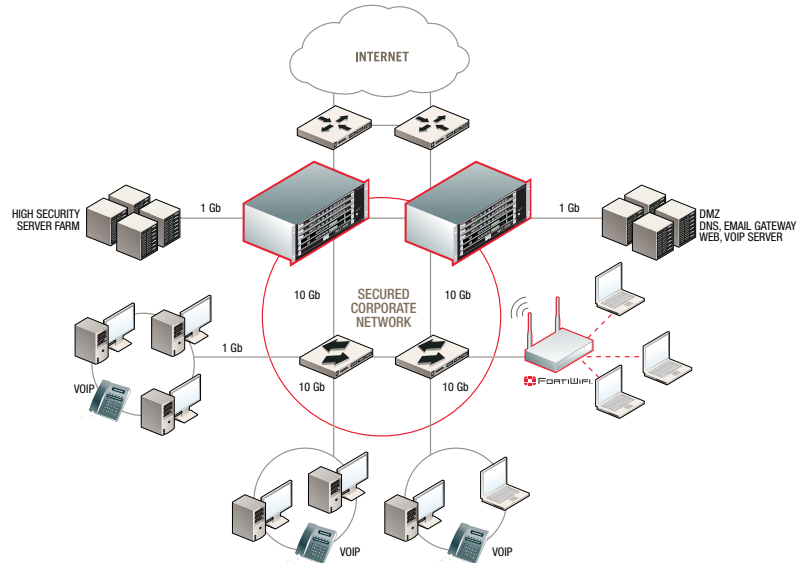


The Fortinet FortiGate-5000 Series is designed to secure large enterprise and service provider networks.

Next-Generation Perimeter Security

Firewall + Intrusion Prevention System + Antivirus

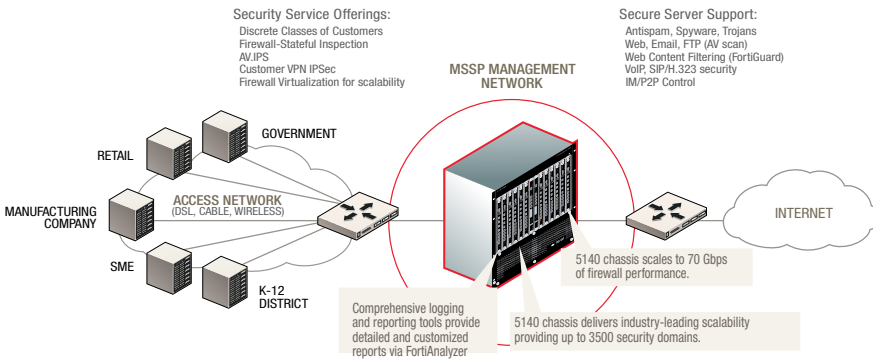
Firewalls alone aren't enough to block today's blended threats. When single packets are examined by point products with no concern for multi-vector attacks, blended threats often pass undetected. Combining content inspection firewall technology with gateway antivirus and intrusion prevention allows packet 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

Intrusion Prevention System + Antivirus + Firewall + VPN

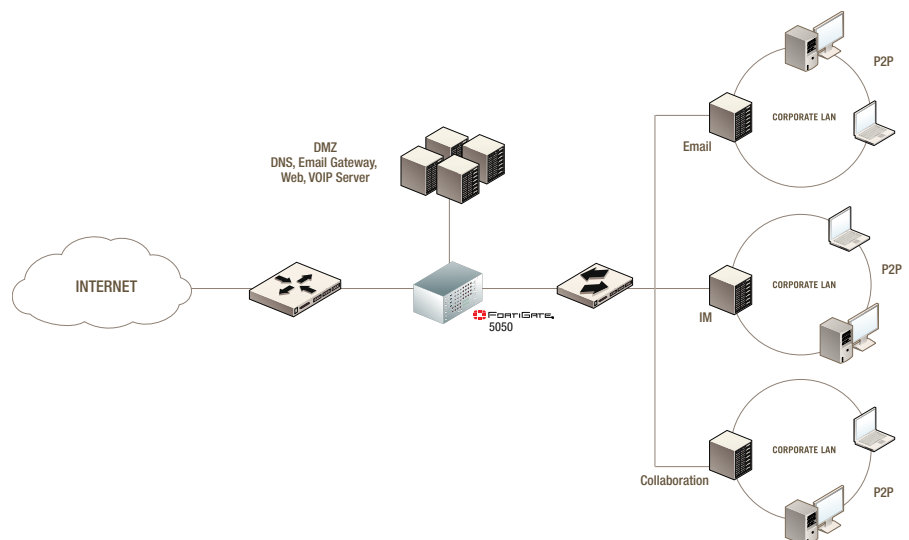
The FortiGate-5000 Series delivers comprehensive security for Managed Security Service Providers (MSSPs). The full suite of ASIC-accelerated security modules allows for customizable features for specific customers, while virtualization features like Virtual Domains (VDMs) provides up to 3,500 separate security domains. Implementing the FortiGuard Distribution Network enables MSSPs to deliver FortiGuard update services to their customers as a managed service. 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

Web Content Filtering + Antispam + IM/P2P Controls + Antivirus

Email is an essential corporate communication tool. Viruses have adapted and are now primarily transmitted via this vector. 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 content filtering, customers can ensure that email and other messaging remains secure and won't result in lost revenue or lost data.



FortiGate-5000 Series Chassis



Feature	FortiGate-5020	FortiGate-5050	FortiGate-5140
Available Slots.....	2.....	5.....	14.....
Power Source.....	AC.....	DC/AC*.....	DC/AC*.....
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 Performance.....	1.2 Gbps 3DES.....	3 Gbps 3DES.....	8.4 Gbps 3DES.....
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)
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		
Regulatory	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		

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

FortiASIC-Accelerated Security Modules

Fortinet offers fully integrated, multi-threat security solutions to protect against blended threats. You can deploy a chassis either for complete protection across all blades or dedicate one or more blades for specific functions

- Firewall (FW):** Complete content inspection and application assurance to protect your mission-critical corporate resources.
- Virtual Private Network (VPN):** With integrated FW, AV, IPS, and URL filtering that can inspect traffic inside VPN tunnels for secure communications to your data and applications from mobile workers, partners, and customers.
- Intrusion Prevention (IPS):** Signature, anomaly, and activity inspection for over 6,000 known intrusions detects and blocks network attacks aimed at exploiting application vulnerabilities, keeping applications available and preventing misuse.
- Antivirus/Antispyware (AV):** Signature-based, heuristic, and activity inspections from the only ASIC-accelerated AV engine removes malicious content from SMTP, POP3, IMAP, IM, P2P, HTTP, and FTP sessions so that communications to and from your network are clean and controlled.
- Antispam (AS):** Heuristic, and gray listing engines block up to several million unsolicited, unwanted, or inappropriate messages from clogging network resources and reducing productivity.
- Web Content Filtering (WCF):** Stops access to over 25 million offensive and undesirable internet sites with 76 categories (with multiple administrative override capabilities) that could harm your network resources.

The FortiASIC Advantage

The FortiASIC is the foundation of Fortinet's unique technology. FortiASICs use an intelligent, proprietary content scanning engine that accelerates the compute-intensive actions. They also contain acceleration algorithms for encryption so that FortiGate security devices can perform antivirus scanning on VPN tunnels ensuring clean and controlled communications. Coupling our custom ASIC with proprietary network processor acceleration, Fortinet's chassis systems deliver extreme performance and security at a compelling total cost of ownership.

FortiOS: Developed for Security

Fortinet's FortiOS is with security and performance as top priorities. FortiOS features full routing (BGP, OSPF, RIP), complete logging and auditing for forensic analysis, granular Virtual Security Domain (VDM) support, and a complete command line interface (CLI). No 3rd party software applications are included that might lead to a vulnerability. It is Common Criteria Certified EAL 4+.

Fortinet's AdvancedTCA Architecture

The Advanced Telecom Computing Architecture (AdvancedTCA) offers distinct performance and management advantages over proprietary designs. The FortiGate-5000 Series chassis systems are carrier-grade, offering extremely high reliability and scalability. Moreover, the AdvancedTCA chassis are Network Equipment Building System (NEBS) compliant. Fortinet is the first and only security vendor utilizing AdvancedTCA systems for security applications.



FortiGate-5001SX

Features the complete suite of FortiGate multi-layered security technologies



FortiGate-5001FA2

Features hardware acceleration for FortiGate multi-layered security technologies



FortiGate-5005FA2

Features hardware acceleration and the highest level of performance among FortiGate blade solutions



FortiSwitch-5003

Features high availability switching across the high-speed chassis backplane



FortiController-5208

Features customized high-bandwidth traffic direction for customized applications

FortiGate-5000 Series Blades

Table with 6 columns: Feature, FortiGate-5001SX, FortiGate-5001FA2, FortiGate-5005FA2, FortiSwitch-5003, FortiController-5208. Rows include SFP Ports, Base-T Ports, Network Processor Accelerated Ports, Concurrent Sessions, FW Throughput, Maximum VPN Tunnels, Unlimited User Licenses, and Maximum Policies.

Technical Specifications FortiGate-5000 Series

FortiGate-5000 Series provides the following features:

ANTIVIRUS, SPYWARE, WORM & TROJAN PROTECTION

Scans HTTP SMTP, POP3, IMAP, FTP, IM and encrypted VPN tunnels
Quarantine infected messages
Block by file size and file type
IM File transfer scanning

DYNAMIC INTRUSION PREVENTION

Protocol anomaly detection
Comprehensive attack signatures
Customizable detection signatures

FIREWALL MODES

NAT, PAT, Transparent, Route modes
Policy based NAT
Security Zones
User /Group-based authentication
H.323/SIP NAT Traversal

CONTENT FILTERING

URL/keyword/phrase block
URL exempt list
Blocks Java Applet, Cookies and ActiveX Content
FortiGuard™ Web Content
Filtering support
Automatic real-time updates

ANTI-SPAM

RBL/ORDBS support
FortiGuard Antispam Support
MIME header check
Keyword/phrase filtering
IP address blacklist/exempt list

VPN

PPTP, L2TP, IPSec
Encryption (DES, 3DES, AES)
SSL
SHA-1/MDS authentication
PPTP, L2TP, VPN client pass through
Hub & Spoke VPN architecture
IKE certificate authentication (X.509)
IPSec NAT Traversal
Aggressive mode
 Replay protection
Dead peer detection
VPN tunnel monitor

NETWORKING

Multiple WAN link support
DHCP client/server/relay
Route between zones
Policy-based routing
VLAN tagging (802.1Q)

LOGGING / MONITORING

Log to remote Syslog/WELF server
SNMP
Graphical real-time & historical monitoring
Email notification of viruses & attacks
FortiAnalyzer™ support
Web Dashboard for real-time device monitoring

HIGH AVAILABILITY (HA)

Clustering
Active/Active and Active/Passive HA
Stateful failover (FW and VPN)
Device failure detection and notification
Redundant power supplies (hot swappable)

SYSTEM MANAGEMENT

Console interface (RS-232)
WebUI (HTTPS), Command line interface
Multi-language support
Secure command shell (SSH)
FortiManager™ System

ADMINISTRATION

Role-based administration
Multiple administrators and user levels
Upgrades and changes via TFTP & WebUI
System software rollback

USER AUTHENTICATION

Internal database
External LDAP/RADIUS database support.
RSA Secure ID
Xauth over RADIUS support for IPSec VPN
IP/MAC address binding
Windows Active Directory

TRAFFIC MANAGEMENT

DiffServ Support
Policy-based traffic shaping
Guaranteed/Maximum/Priority bandwidth

ROUTING PROTOCOLS

RIP v1, v2
BGP4
OSPF
PIM sparse and dense mode
Static

INSTANT MESSENGER – ACCESS CONTROL

AOL-IM Yahoo
MSN ICQ

Fortiguard Subscription Services

Includes:

- Automatic updates from over 50 redundant high speed database servers around the globe.
Complete Wildlist virus protection for over 4500 active viruses from FortiGuard's active database of over 60,000 viruses.
Real-time IPS updates for protection against over 6000 threats.
76 rated web categories for more accurate web content filtering.
Web filtering for more than 25 million rated domains and 2 billion rated Web pages.

FortiCare Support Services

Includes:

- 24x7x365 FortiCare Web Service
Web-based and Phone-based Technical Support*
1-Year Limited Hardware Warranty
90-Day Limited Software Warranty

*8x5 and 24x7 Phone-based Technical Support Options Available



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

