

FortiGate® -1000-3800 Series

High Performance Security
Systems for Enterprises

Datasheet

Next Generation Hardware-Accelerated Security Solutions

High Performance Enterprise Network Security

FortiGate enterprise security solutions deliver next-generation firewall technology and multi-threat protection integrated into cost-effective security platforms that effectively block blended network threats. Point-product security solutions do not provide protection against a new breed of blended threats that utilize a multitude of attack vectors. Furthermore, assembling an array of point products is costly and requires significant expertise to engineer, maintain and manage. FortiGate solutions cost-effectively deliver complete multi-threat protection against: unauthorized access, intrusion attempts, viruses, worms, trojans, spyware, phishing attempts, spam and other types of content-based and network-based threats.

Industry-Leading Unified Threat Management (UTM)

Fortinet incorporates ICSA Labs-certified UTM functions into a single ASIC-based appliance that is simple to install and manage. Stateful firewall, IPSec and SSL-VPN, intrusion prevention, antivirus, antispam, and Web filtering features combine to form a complete enterprise-focused network security platform that offers compelling total cost of ownership.

Key Problems	Solutions
<ul style="list-style-type: none"> Holes left open in corporate firewalls for applications are commonly used to attack network resources and users 	FortiGate appliances prevent successful attacks through commonly allowed applications including: email, web-based applications, instant messaging and VoIP
<ul style="list-style-type: none"> Remote access threatens the secured perimeter, allowing threats a direct conduit into the private network 	FortiGate appliances enforce the secure perimeter model by inspecting traffic for network-level and content-left threats after termination of the encrypted tunnel and before being allowed onto the private network
<ul style="list-style-type: none"> Standalone intrusion prevention products do little to protect networks from the abundance of file-based threats commonly found in email attachments and instant messaging downloads 	FortiGate appliances intelligently integrate firewall, intrusion prevention, antivirus, Web filtering, antispam and application controls together for the best threat protection possible
<ul style="list-style-type: none"> Managing multiple security products and extracting value from the purchases is increasingly difficult in the face of shrinking budgets and dwindling technical resources 	FortiGate appliances combine essential security technologies into one cost-effective unified solution, which eases strains on resources while also reducing complexity, space and power consumption requirements



FortiGate-1000A



FortiGate-1000AFA2



FortiGate-3016B



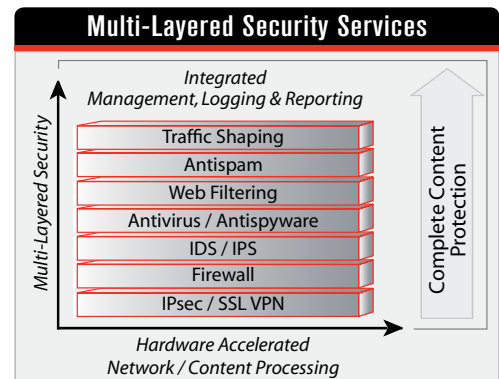
FortiGate-3600A



FortiGate-3810A

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, antispayware, 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.

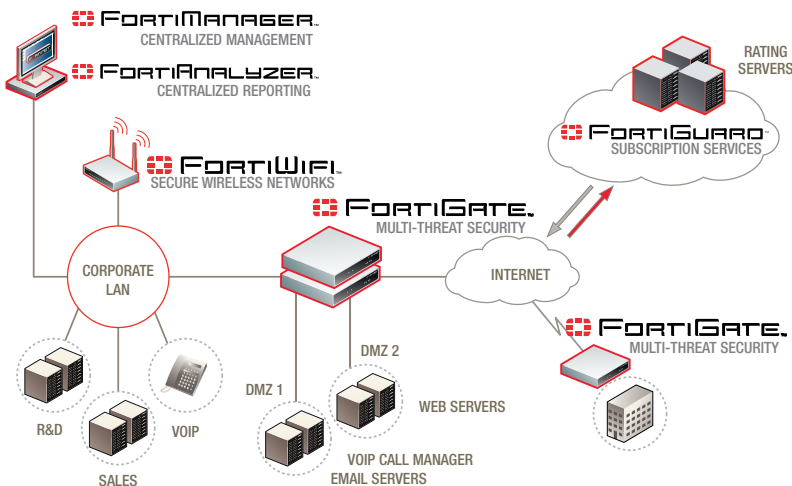
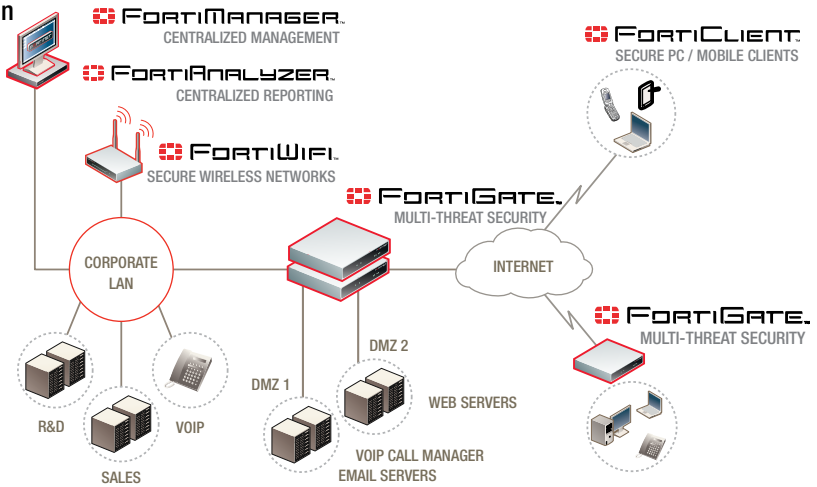


FortiGate multi-threat security solutions are designed for enterprise networks.

Secure Network Perimeters / Internal Segmentation

Firewall and VPN services are deployed at the perimeter of the internal network to securely connect remote offices and mobile users to an organization's private resources while at the same time preventing any other unauthorized access. Intrusion prevention, antivirus and Web filtering services ensure that network-based threats and content-based threats are stopped inbound as well as outbound.

Inside the network, segmentation can be achieved using firewall, intrusion prevention and antivirus technologies. Internal segmentation effectively isolates outbreaks before they are allowed to spread throughout an organization's network.



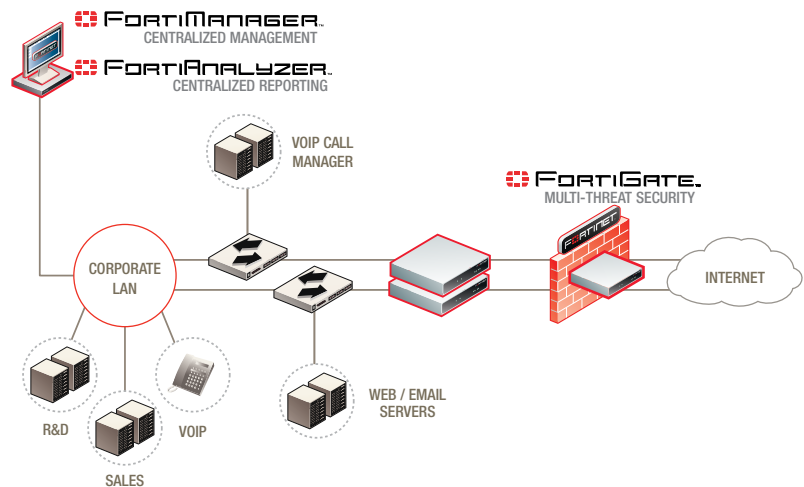
Virtual Security Domains / Distributed Enterprises

FortiGate platforms support multiple security zones and virtual security domains to customize a network's security policy anywhere requirements demand. Virtual Domains (VDOMs) can also be used to provision services for external customers.

All FortiGate solutions start from the same flexible high performance architecture. Core networking features found in every model such as High Availability (HA) and support for dynamic routing protocols enable the FortiGate to be deployed into highly distributed and fully meshed network environments.

Datacenter and Critical Applications Security

Effectively protecting an organization's mission critical applications from a new generation of application-based threats that are now targeting Web 2.0, VoIP and even IPTV applications requires a comprehensive security strategy that contains multiple layers of network-based defenses. Unfortunately, many of these new applications are time-critical, forcing administrators to choose between performance and security. The FortiGate family of multi-gigabit performance solutions deliver real-time protection against multi-layered security threats which target application servers. In addition to protecting against these new threat types, advanced antispam filtering relieves the ever evolving problem of unsolicited bulk mail while also filtering mail for spyware and security policy violating content.



Technical Specifications



HARDWARE SPECIFICATIONS	FortiGate-1000A	FortiGate-1000AFA2	FortiGate-3016B	FortiGate-3600A	FortiGate-3810A
10/100/1000 Interfaces (Copper)	10	10	2	8	8
1Gb SFP Interfaces	0	2	16 - 20*	2 - 6*	2 - 26*
SFP Transceivers Provided	NA	2 (SX)	4 (SX) / 4 (TX)	2 (SX)	2 (SX)
USB Ports	1	1	2	2	1
AMC Expansion Slots	0	0	1 single width	1 single width	2 single width 2 double width
SYSTEM PERFORMANCE					
Concurrent Sessions	1,100,000	1,100,000	1,100,000	1,100,000	2,000,000
New Sessions/Second	15,000	15,000	25,000	40,000	40,000
Firewall Throughput (Gbps)	2 Gbps	2 Gbps	16 - 20* Gbps	6 - 10* Gbps	7 - 37* Gbps
VPN Throughput (IPSec)	600 Mbps	600 Mbps	12 - 15* Gbps	0.8 - 3.8* Gbps	1 - 19* Gbps
IPS Throughput	1 Gbps	1 Gbps	2 Gbps	3 Gbps	4 Gbps
Antivirus Throughput	200 Mbps	200 Mbps	300 Mbps	400 Mbps	500 Mbps
Unlimited Concurrent Users	Yes	Yes	Yes	Yes	Yes
Site-to-site IPSec VPN Tunnels (System / VDOM)	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000
Client-to-Site IPSec VPN Tunnels	10,000	10,000	64,000	64,000	64,000
Number of Concurrent SSL Users (Recommended)	1,000	1,000	2,000	3,000	5,000
Policies	100,000	100,000	100,000	100,000	100,000
Virtual Domains (VDOMS) (standard / with optional license)	10 / NA	10 / NA	10 / 250	10 / 250	10 / 250
DIMENSIONS					
(H, W, L, weight)	3.5 in (88.9 mm) 16.75 in (425.5 mm) 20.5 in (520.7 mm) 17.5 lbs (8 kg)	3.5 in (88.9 mm) 16.75 in (425.5 mm) 20.5 in (520.7 mm) 17.5 lbs (8 kg)	3.5 in (88.9 mm) 16.9 in (429.3 mm) 18.3 in (464.8 mm) 25.6 lbs (11.6 kg)	3.5 in (88.9 mm) 16.9 in (429.3 mm) 16.9 in (429.3 mm) 26 lbs (11.8 kg)	3.5 in (88.9 mm) 16.9 in (429.3 mm) 18.5 in (469.9 mm) 36 lbs (16.4 kg)
AC POWER OPTION	Dual 100-240 VAC, 50-60 Hz, 8 Amp (Max)				
DC POWER OPTION	N/A	N/A	N/A	N/A	-48V DC (Normal) (-36 ~ -72V DC / 500W Max)
POWER CONSUMPTION (AVG)	220W	220W	168W	220W	275W
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, UL/CUL, C Tick, CE, VCCI				
CERTIFICATIONS	ICSA Labs, NSS Labs, Common Criteria, FIPS 140-2				

* Higher Values Include Properties of Optional Expansion Modules

Fortinet Advanced Mezzanine Card (AMC) Expansion Modules

The AMC standard, also known as AdvancedMC™, was developed by the PCI Industrial Computers Manufacturers Group (PICMG), which has over 100 companies building to the specification. AdvancedMC has been developed to meet the requirements for the next generation of *carrier grade* equipment.



ADM-XB2

10-Gigabit Ethernet AMC Module

- 2-Port FortiASIC hardware accelerated 10-Gigabit Ethernet module (Includes 2x SR XFP transceivers)
- 11 Gbps Firewall performance
- 6 Gbps IPSec VPN performance
- Requires double-width slot (FG-3810A)



ADM-FB8

8-Port Gigabit Ethernet AMC Module

- 8-Port FortiASIC hardware accelerated Gigabit Ethernet module (Includes 4x SX SFP transceivers)
- 8 Gbps Firewall performance
- 6 Gbps IPSec VPN Performance
- Requires double-width slot (FG-3810A)



ASM-FB4

4-Port Gigabit Ethernet AMC Module

- 4-Port FortiASIC hardware accelerated Gigabit SFP module (Includes 4x SX SFP transceivers)
- 4 Gbps Firewall performance
- 3 Gbps IPsec VPN performance
- Requires single-width slot (FG-3016B/FG-3600A/FG-3810A)



ASM-S08

80 GB Storage AMC Module

- 80 Gigabyte hard disk drive storage module
- High duty cycle hard drive design
- Requires single-width slot (FG-3016B/FG-3600A/FG-3810A)

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 reliability, it is a purpose-built operating system that leverages power of the the FortiASIC 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-1000-3800 Series



FortiGate-1000A

FortiGate-1000AFA2

FortiGate-3016B

FortiGate-3600A

FortiGate-3810A

FortiGate-1000-3800-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 (VDMs)
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 (VDMs)

Separate Firewall/Routing domains
Separate Administrative domains
Separate VLAN interfaces
10 VDMs (standard)
Up to 250 VDMs (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
- 8x5 telephone-based technical support (24x7 - optional)
- 1-Year limited hardware warranty
- Technical account management service available
- Professional services available
- 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 +33-4-8987-0501

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

