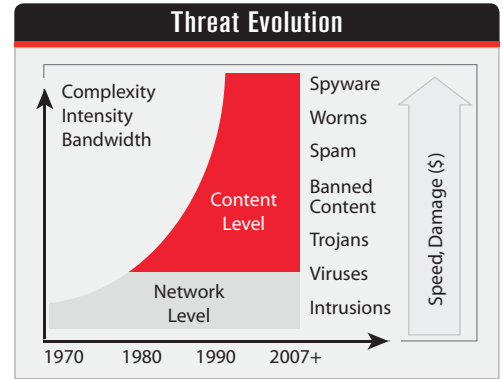


FortiOS™ Network Security Operating System

**Purpose-Built
For Security**

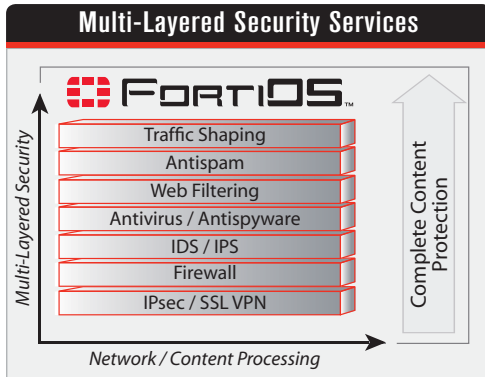
Challenges with the New Internet

Internet traffic has evolved from Web and Email to rich media and presence oriented real-time applications traffic. New applications have enabled business benefits, but have also created new opportunities for cyber attacks that can result in a loss of productivity, confidential information and/or revenues. Network security solutions must have the flexibility and power to dynamically protect against these rapidly evolving threats. New Web, IM, VoIP and other applications require the ability to define and enforce granular usage policies to manage compliance with corporate security policies and regulatory requirements. And as threats move higher up the OSI stack, network safeguards must move from basic packet inspection to complete content protection. Scalable computing power and network throughput are required to meet these increased demands. This is driving the need for purpose-built Unified Threat Management (UTM) security solutions utilizing optimized operating systems capable of providing complete content-level protection without compromising network availability.



Introducing the FortiOS™ Security Operating System

FortiOS is a security-hardened, purpose-built operating system that is the software foundation of FortiGate™ multi-threat network security platforms. Leveraging the hardware acceleration provided by the FortiASIC™ content and network processors FortiOS enables real-time content inspection, as well as signature and heuristic packet scanning for advanced threat protection. Ongoing updates from the FortiGuard™ Network ensure that security subscription services and the FortiOS operating system are always up to date and providing a complete Unified Threat Management solution.



Businesses can now benefit from an integrated solution that offers a comprehensive suite of security services – content inspection firewall, VPN, IPS, antivirus, Web filtering, antispam and IM/P2P as well as integrated bandwidth shaping. FortiOS employs an integrated policy engine that enforces granular security policies including web filtering and full content scanning for instant messaging, support for P2P rate limiting and SSL-VPN.

FortiOS is tightly integrated with the Fortinet FortiManager™ and FortiAnalyzer™ systems to provide centralized management, reporting and analysis of network traffic and threats. The security of FortiGate appliances themselves is critical, FortiOS is pre-hardened and does not include any third party applications. FortiOS has been built from the ground up to deliver security services at the highest levels of performance and is certified for Common Criteria EAL 4+.

Competitive Assessment

"Fortinet's FortiGate security solution rivals the best multi-service devices in the advanced firewall/VPN market with anti-virus, firewall, VPN, SSL VPN, content filtering, QoS, IM security, bandwidth shaping, anti-spyware, and anti-spam capabilities, plus a full services offering to ensure up-to-date definitions for signature-based features."

Current Analysis
www.currentanalysis.com
FortiGate Product Assessment
2007

FortiOS Key Features

- Integrated switching and routing engine with support for a variety of interfaces, protocols and throughputs
- Dynamic threat AV and IPS detection engines automatically updated from the FortiGuard Network
- Signature databases are also updated automatically to ensure protection against the latest threats
- Local browser-based management interface and integration with FortiManager and FortiAnalyzer
- Dynamic updates of security software and threat signatures through FortiGuard subscription services

Benefits

- ✓ Enables deployment in different network topologies and ensures interoperability with legacy equipment
- ✓ Offers continuous protection from network and application level threats without any downtime required
- ✓ Automated protection from intrusion attempts, worms, viruses, malware and blended threats
- ✓ Lowers total cost of ownership with centralized management and administration console
- ✓ Ensures optimal performance of FortiGate appliances and highest levels of threat protection

FortiGate Integrated Turn-Key Hardware, Software and Security Subscription Solutions

FortiGate platforms are based on an integrated hardware and software architecture specifically designed for high-performance application-level content processing in perimeter, core and data center networks to provide real-time security functions at multi-gigabit per second data rates. The FortiASIC™ Content Processor (CP) is a key component in all FortiGate security platforms providing a hardware scanning engine, hardware encryption, and real-time content analysis processing capabilities. The FortiASIC Network Processor (NP) series of processors provides acceleration for firewall, encryption/decryption, signature and heuristic packet scanning, and bandwidth shaping. FortiOS security services can be selectively enabled to provide a unique set of services or a full suite of UTM security services all within a single platform. The FortiGuard™ network dynamically updates system software and security services such as antivirus, antispam, Web filtering, antispam, Web filtering, antispam, and intrusion prevention to ensure the maximum level of protection is being provided.

FortiOS Security Services

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 /SCCP 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

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

INTRUSION PREVENTION SYSTEM (IPS)

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

INSTANT MESSENGER / PEER-TO-PEER ACCESS CONTROL

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



FortiOS Networking Services

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
Route Between Zones
Route Between Virtual LANs (VDOMS)
Multi-Link Aggregation (802.3ad)

TRAFFIC SHAPING

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

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



FortiOS Management Services

MANAGEMENT/ADMINISTRATION OPTIONS

Console Interface (RS-232)
WebUI (HTTP/HTTPS)
Telnet / Secure Command Shell (SSH)
Command Line Interface
Role-Based Administration
Multi-language Support
Multiple Administrators and User Levels
Upgrades and Changes Via TFTP 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

FIREWALL 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

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