



FortiOS™ Carrier 4.0 Software

Specialized Security for Service Providers

FortiOS Carrier 4.0—Consolidated Security Solutions for Service Providers

The communications industry is moving rapidly towards an IPv6 model, prompting service providers to transform their aging networks into modern service delivery infrastructures. These next-generation architectures must be able to deliver rich, high-speed digital services with improved efficiency while reducing operating costs. They must also be highly secure in order to maximize uptime and prevent fraud.

Fortinet designed and built the FortiCarrier line of consolidated security appliances from the ground-up, with strong consideration for the needs of service providers and their customers. Powered by the security-hardened FortiOS Carrier 4.0 operating system, FortiCarrier appliances provide a broad range of functionality to protect critical services and applications across high-speed networks. By designing their networks properly, Mobile operators, voice operators, managed security service providers (MSSPs), and large enterprises will benefit from a smooth and secure transition to next generation network architectures while unlocking additional revenue streams with expanding service portfolios.

FortiOS Carrier 4.0 Security Features

- IPv6-ready Firewall
- Dynamic Security Profiles and Groups
- Managed Security
- Voice Security
- MMS Security
- GPRS Tunneling Protocol (GTP)
- VPN - IPSec and SSL
- SSL-encrypted Traffic Inspection
- Antivirus / Antispyware and Antispam
- Intrusion Prevention System (IPS)
- Data Loss Prevention (DLP)
- Flow-based Inspection Options
- Web Filtering and Application Control
- Endpoint Network Access Control (NAC)
- Vulnerability Management
- WAN Optimization
- Wireless Controller
- Monitoring, Logging and Reporting
- Virtual Domains
- High Availability
- Layer 2/3 Routing Services
- FortiGuard Security Updates

One-Stop Security Services Portfolio

FortiCarrier platforms protect service provider networks and infrastructure from viruses, information theft, network overload, service hijacking and other malicious attacks. They also enable MSSPs to deliver multiple high-value security applications to their customers. Providers can create an entire service portfolio with a single stop, avoiding the lengthy product development cycles required to integrate products from multiple vendors.

IPv6 Security Platform

FortiCarrier consolidated security appliances are built from the ground up with IPv6 compatibility in mind. FortiOS Carrier 4.0 software works in concert with specialized FortiASIC™ processors to accelerate IPv6 and IPv4 traffic throughput, content inspection and other security functions. This frees other system resources, improving overall system performance and throughput.

Simplified Management

Unifying policy at the device level allows FortiCarrier appliances to deliver multi-threat protection with truly centralized management from a single platform. Powerful management features including Dynamic Security Profiles and Virtual Domains (VDMs) simplify administration, reduce security device count, and slash overhead expenses.

“A further disrupting factor is the rate of change within enterprise networking — inexorably increasing throughput, more Web-based applications, more complex connections within applications, more complex data centers and more data being presented to customers means that firewalls have had to keep up with features and performance to meet these changing needs”.

Greg Young and John Pescatore
Gartner Magic Quadrant for Enterprise Network Firewalls - March 2010.



FortiOS Carrier 4.0—Complete Content and Network Protection for Service Providers

Service providers including MSSPs, voice operators and mobile operators will benefit from the hundreds of security-related features included with FortiOS Carrier 4.0. As networks migrate to IPv6 and service providers expand their portfolios to unlock new business opportunities, FortiCarrier consolidated security appliances are ready to deploy and scale as needed. FortiOS Carrier 4.0 includes all of the security features available in FortiOS 4.0 (see FortiOS 4.0 brochure) plus additional features benefitting service providers, some of which are highlighted below:



IPv6-Ready Platform

FortiOS Carrier 4.0 software works in concert with specialized FortiASIC processors to accelerate IPv6 firewall throughput and other security functions. In addition, IPv6 is supported for the SSL VPN web portal, SNMP, DHCP, OSPF and NSSA. IPv6 traffic can be redirected for user authentication using a local database, RADIUS, TACACS+, or LDAP protocols.



One-Stop Managed Security Portfolio

FortiCarrier appliances enable MSSPs to deliver multiple high-value security applications to customers and end-users. When combined with the additional centralized management, provisioning, reporting and logging services offered by FortiManager™ and FortiAnalyzer™ appliances, they provide a secure, scalable platform on which to build an entire portfolio of managed security services.



Dynamic Security Profiles

As their customer bases grow, managed security service providers (MSSPs) find themselves managing hundreds of security policies and thousands of end-users. With Dynamic Security Profiles, MSSP administrators can apply security policies to end-users automatically, greatly reducing the need for manual provisioning and lowering operating expenses.



Mobile Provider Security

FortiCarrier appliances protect mobile network infrastructures with an integrated GPRS Tunneling Protocol (GTP) Firewall which is designed to 3GPP specifications, ensuring compatibility with a broad range of deployment scenarios. Fully integrated intrusion prevention blocks an array of GTP attacks while MMS antivirus inspects traffic on MM1/3/4/7 interfaces. MMS Flood detection blocks MMS spam and mobile content filtering blocks phishing attacks.



Voice Security

The Session Initiation Protocol (SIP) Signaling Firewall included with FortiCarrier appliances protects voice infrastructure interfacing with untrusted access, peering and trunking networks. Compatible with IP Multimedia Subsystem (IMS) and pre-IMS deployments, the FortiCarrier platform helps to ensure Quality of Service (QoS) by preventing flooding and network availability attacks. The SIP firewall integrates seamlessly with the FortiOS Carrier 4.0 intrusion prevention system, protecting voice infrastructure from Denial of Service (DoS) attacks and other network-based threats.

Managed Security Features

DYNAMIC SECURITY PROFILES

Assignment of Service Policy by User (up to 600,000 users)
Service Policy Can Define the Settings for Any of the Advanced Security Services Provided by FortiOS Carrier
Enables Parental Control and Opt-Out Services

VIRTUAL DOMAIN (VDOM)

Support for Hundreds of Enterprise Customers per Physical Blade/Appliance, Scaling to Thousands of Enterprise Customers per Chassis

CONSOLIDATED SECURITY

Firewall (ICSA Labs Certified)
IPSec VPN (ICSA Labs Certified)
SSL-VPN
Intrusion Prevention System (ICSA Labs Certified)
Gateway Antivirus (ICSA Labs Certified)
Web Filtering (Over 2 Billion URLs Categorized)
Antispam Filtering
Application Control (Thousands of Applications Categorized)
Data Loss Prevention (DLP)
L2 / L3 Routing with Rate Limiting
SSL-Based Traffic Inspection

CENTRALIZED LOGGING AND ALERTING

Provided by FortiAnalyzer Appliances
All Log and Alert Functions Configurable per Customer
Consolidates Security and System Event Logs
Event Correlation, Graphical Reports, Network Data Statistics

CENTRALIZED MANAGEMENT

Provided by FortiManager Appliances
Deployment Configuration / Provisioning
Real-Time Monitoring
Device & Security Policy Maintenance
Localized Security Content Update Server & Rating Database for Managed Devices

Voice Security Features

SIP SIGNALLING FIREWALL

Stateful and SIP Protocol-Aware Firewall
Hardware Accelerated RTP Processing for Reduced Packet Loss, Packet Latency, and Jitter.
SIP Transparent (Inspect Only) & NAT (Rewrite SIP Header) Operating Modes
Supports SIP Servers in Proxy or Redirect Operating Mode
Configurable RTP Pinholing Support
Supports Complex Source & Destination SIP NAT Environments (SIP & RTP Protocols)
NAT IP Preservation Retains Originating IP Address for Administrative Purposes (e.g. Billing)
SIP Tracking over Session Lifespan

SIP SIGNALLING FIREWALL (CONTINUED)

SIP Session Failover for Active-Passive High Availability
SIP Session Load Balancing (via Virtual IP Load Balancing)
Geographical Redundancy Support
SIP Rate Limiting to Prevent SIP Server Flooding / Overload
IP Topology Hiding of SIP & RTP Server (via NAT and NAPT)
Configurable SIP Command Control Blocks Unauthorized SIP Methods
Configurable SIP Blocking for Messages that Exceed Defined Maximum Header Length
SIP Registrar Exclusively Option to Avoid Spoofing of Clients
SIP Communication Logging to FortiAnalyzer Appliances
SIP Statistics (Active Sessions, Total Calls, Calls Failed/ Dropped, Call Succeeded)

ADDITIONAL VOICE SECURITY TECHNOLOGIES

Intrusion Prevention System with VoIP Protocol Anomaly & VoIP Protocol Aware Signature-Based Inspection Capabilities
Denial of Service (DoS) Sensor Protects Trusted Zones from Flooding Attacks
Integrated IPSec for Secured Tunnels Between Trusted Zones
Virtual Domain (VDOM) Support for Additional Isolation of Infrastructure within the Same Physical Environment

Mobile Security Features

DYNAMIC SECURITY PROFILES

Assignment of Service Policy by MSISDN (Mobile Station)
Service Policy Can Define the Settings for Any of the Advanced Security Services Provided by FortiOS Carrier
Enables Parental Control and Opt-Out Services

MMS GENERAL

Support for Multiple MMS Policy Profiles for Consolidated or MVNO Deployments
Customizable Notification Messages (Per MVNO)
MSISDN Header Parsing (Including Cookie Extraction & Hex-Based Conversions for MM1/MM7 Message Types)
MMS File Intercept to FortiAnalyzer Appliances for Forensic Analysis
MMS Content Archive (Full MMS Message Archiving to FortiAnalyzer Appliances with HTTP/SMTP Transport Headers)
Per MSISDN & Per Mobile Station Type Reporting of Malicious Activity via FortiAnalyzer Appliances

MMS ANTIVIRUS

Monitor Only & Active Blocking Modes (Per Interface Type)
Simultaneous Malware Scanning of MM1/MM3/MM4/MM7 Message Types
Remove Malicious Content Only Option (Allows Message Transaction to Complete)
File Type Analysis with Configurable Block or Intercept Actions (File Extension Independent)
Configurable Retrieve Message Scanning (MM1) to Avoid Redundant Inspection
Per Sender Scanning with Configurable Block/Archive/ Intercept Actions
MM1/MM7 Client & Server Comforting

MMS ANTISPAM / ANTIFRAUD

MM1/MM4 Flood Detection with Three Configurable Thresholds with Discrete Actions
MM1/MM4 Duplicate Message Detection with Configurable Thresholds and Actions
Configurable Alert Notification to Administrator of Spam or Fraud Activity
MM1/MM7 Banned Word Scoring with Configurable Block/ Pass Actions

GTP FIREWALL

Based on 3GPP 29.060 version 6.9.0
Integrated Intrusion Prevention Inspection for GTP Payloads For Gn/Gp Interfaces
GTP Packet Sanity Check, Length Filtering & Type Screening
GSN Tunnel Limiting & Rate Limiting
GTP Stateful Inspection
Hanging GTP Tunnel Cleanup
GTP Tunnel Fail-Over for High Availability
GTP IMSI Prefix (up to 1000) & APN (up to 2000) Filtering
GTP Sequence Number Validation
IP Fragmentation of GTP Messages
GGSN & SGSN Redirection
Detecting GTP-in-GTP Packets
GTP Traffic Counting & Logging
Anti-Overbilling Together with Gi Firewall
Encapsulated Traffic Filtering with Anti-Spoofing Capabilities
GTP Protocol Anomaly Detection and Exploit Prevention
Handover Control to Prevent Session Hijacking
For Gi Interface
Anti-Overbilling Together with Gn/Gp Firewall

FortiOS Networking Services

NETWORKING/ROUTING

- Multiple WAN Link Support
- PPPoE Support
- DHCP Client/Server
- Policy-Based Routing
- Dynamic Routing for IPv4 (RIP, OSPF, IS-IS, BGP, & Multicast protocols)
- Dynamic Routing for IPv6 (RIP, OSPF, & BGP)
- Multi-Zone Support
- Route Between Zones
- Route Between Virtual LANs (VLANs)
- Multi-Link Aggregation (802.3ad)
- IPv6 Support (Firewall, DNS, Transparent Mode, SIP, Dynamic Routing, Admin Access, Management)
- VRRP and Link Failure Control
- sFlow Client

TRAFFIC SHAPING

- Policy-based Traffic Shaping
- Application-based and Per-IP Traffic Shaping
- Differentiated Services (DiffServ) Support
- Guarantee/Max/Priority Bandwidth
- Shaping via Accounting, Traffic Quotas

VIRTUAL DOMAINS (VDOMs)

- Separate Firewall/ Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- 10 VDOM License Std. (more can be added)

DATA CENTER OPTIMIZATION

- Web Server Caching
- TCP Multiplexing
- HTTPS Offloading
- WCCP Support

HIGH AVAILABILITY (HA)

- Active-Active, Active-Passive
- Stateful Failover (FW and VPN)
- Device Failure Detection and Notification
- Link Status Monitor
- Link failover
- Server Load Balancing

WAN OPTIMIZATION

- Bi-Directional / Gateway to Client/Gateway
- Integrated Caching and Protocol Optimization
- Accelerates CIFS/FTP/MAPI/HTTP/HTTPS/Generic TCP
- Requires a FortiGate device with Hard Drive

FortiOS Management Services

MANAGEMENT/ADMINISTRATION OPTIONS

- Web UI (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH), and Command Line Interface (CLI)
- Role-Based Administration
- Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
- Multiple Administrators and User Levels
- System Software Rollback
- Configurable Password Policy
- Customizable Dashboard Widgets (Web UI)
- Central Management via FortiManager (optional)

LOGGING/MONITORING/VULNERABILITY MGMT

- Network Vulnerability Scanning
- Graphical Report Scheduling Support
- Graphical Real-Time and Historical Monitoring
- Local and Remote Syslog/WELF server logging
- SNMP Support
- Email Notification of Events
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging (including per-VDOM)
- Optional FortiGuard Analysis and Management Service

FIREWALL USER AUTHENTICATION OPTIONS

- Local Database
- Windows Active Directory (AD) Integration (w/ FSAAE)
- External RADIUS/LDAP/TACACS+ Integration
- Xauth over RADIUS for IPSEC VPN
- RSA SecurID Support
- LDAP Group Support
- FortiToken Support

WIRELESS CONTROLLER

- Unified WiFi and Access Point Management
- Automatic Provisioning of APs
- On-wire Detection and Blocking of Rogue APs
- Virtual APs with Different SSIDs
- Multiple Authentication Methods

Fortinet Certifications



FortiGuard® Security Subscription Services deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability management, web application firewall, and database security services.

FortiCare™ Support Services provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with hardware return for replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.

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 – SINGAPORE

Fortinet Incorporated
300 Beach Road 20-01
The Concourse, Singapore 199555
Tel +65-6513-3734
Fax +65-6295-0015



Copyright© 2011 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.