

FortiCarrier™ Voice Security

Solution Brief

VOICE SECURITY

SIP FIREWALL

INTRUSION PREVENTION

DENIAL OF SERVICE PREVENTION

Securing Converged IP Networks

Carriers and service providers alike are benefiting from the increased revenue and service reach of SIP-based voice services. As these services continue to grow in popularity, it's vital to address the unique security issues they introduce. An effective solution addresses all aspects of next-generation voice security, inclusive of network, service, and subscriber security.

FortiCarrier hardware and FortiOS™ Carrier software, the platform's security specific operating system, provide an integrated suite of security applications for carriers and service provider networks. The solution provides IP, application, and SIP-based voice security modules delivered on scalable ATCA™ carrier-class service delivery platforms.

The FortiCarrier platform's voice security features protect a network and its services from malicious threats and rogue traffic. There are three integrated components which provide threat identification and prevention, as well as traffic stabilization: a stateful application-layer SIP firewall, an intrusion prevention module, and a Denial of Service (DoS) prevention module. Using FortiASIC™ processors, a family of custom designed security hardware designed to accelerate security inspection and policy enforcement, the FortiCarrier platform is capable of scaling to meet the needs of the largest SIP environments.

FortiCarrier platforms act as a SIP security gateway which provides threat protection for access and peering services within IMS or NGN networks. Within an NGN network, the SIP security gateway is implemented at the network edges while the B2BUA (SBC, Softswitch) is located in the service edge and network core. For IMS implementations the SIP security gateway provides a signalling firewall in conjunction with the P-CSCF and the I-BCF.

FortiCarrier and SIP Security

FortiCarrier protects Tier-1 wireline and wireless carriers worldwide, with specialized security solutions for mobile, data, and managed security services. FortiCarrier voice security further extends FortiOS Carrier to enable the protection of SIP-based voice networks, applications, and services.

The SIP security features, as well as the entire suite of FortiCarrier security applications, can be virtualized as a hosted service for large enterprise networks and can additionally be used to enable VPN, MPLS scanning and data firewalling services.



FortiCarrier-5001A
(FCR-5001A-DW)



FortiCarrier-3810A
(FCR-3810A-DW)

Within NGN and IMS Network Environments, FortiCarrier Platforms Enable:

- Protection of a trusted network from an untrusted network (IP and VoIP traffic)
- SIP header and message body inspection to prevent SIP-specific attacks
- Active and passive modes (SIP NAP/T and SIP transparent modes)
- Multi-Gigabit RTP pin-holing with FortiASIC hardware acceleration for ultra-low latency
- Intrusion Prevention System (IPS) with SIP awareness
- Protection from DoS attacks that affect service availability
- Inter-networking of overlapping SIP/RTP networks
- Protection of hundreds of enterprise customers / peers using Virtual Domains (VDOMs)

FortiCarrier can be implemented in a high availability configuration supporting network, card, or chassis stateful call migration. Data and voice security can be supported within the same platform along with any combination of the multi-threat security features provided by FortiOS Carrier. Finally, FortiGuard™ subscription services provide updated security content for key technologies to protect against the latest evolving threats.

VOICE SECURITY FEATURES

SIP SIGNALING 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 SIGNALING 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 Reporting

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

OTHER 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

MULTI-THREAT SECURITY

Firewall (ICSA Labs Certified)
IPSec VPN (ICSA Labs Certified)
SSL-VPN (ICSA Labs Certified)

MULTI-THREAT SECURITY (CONTINUED)

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 Leakage Prevention (DLP)
L2 / L3 Routing with Rate Limiting
SSL-Based Traffic Inspection

Refer to FortiOS 4.0 Software Brochure for Complete Details on the Wide-Range of Multi-Threat Security Features Offered

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 PERFORMANCE

SIP Signalling Throughput Up to 10,000 messages per second
SIP Call Setup Throughput..... Up to 2,000 call attempts per second (CAPS)
SIP Signalling Sessions (Max)..... 500,000

Performance metrics given apply to FortiCarrier hardware models FCR-5001A and FCR-3810A

SIP performance is benchmarked using signalling traffic only

Messages per second and CAPS performance varies dependant on configuration



FortiGuard Security Subscription Services

- Antivirus
- Intrusion Prevention
- Web Filtering
- Antispam
- Premier Signature Service
Includes Antivirus and Intrusion Prevention Updates with additional service level agreements

FortiCare™ Support Services

- 24/7/365 Web-Based Technical Support
- Technical Account Management Service (Optional)
- 24-Hour Phone-Based Support (Optional)
- Professional Services (Optional)
- 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
Tel +1-408-235-7737
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
61 Robinson Road
#09-04 Robinson Centre
Singapore 068893
Tel: +65-6513-3730
Fax: +65-6223-6784

Copyright© 2009 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. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract 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.