

FortiGate®/FortiWiFi™ -80 Series

Enterprise-Class Protection for Branch Offices

Proven Security for Remote Offices, Retail, and Customer Premise Equipment

FortiGate/FortiWiFi-80 Series consolidated security appliances deliver comprehensive enterprise-class protection for remote locations, branch offices, customer premise equipment (CPE) and retail networks. FortiGate/FortiWiFi-80 Series platforms feature an integrated set of essential security technologies in a single device to protect all of your applications and data. Simple per-device pricing, an integrated management console, and remote management capabilities significantly reduce costs associated with deployment and management.

Comprehensive Protection

Fortinet's market-leading security technology and research results in appliances providing unmatched protection against today's sophisticated multi-vector threats. FortiGate/FortiWiFi consolidated security platforms integrate firewall, IPSec and SSL VPN, antivirus, antispam, intrusion prevention, web filtering and vulnerability management into a single device at a single price. They also provide data loss prevention (DLP), application control, and endpoint NAC.

The FortiGate/FortiWiFi-80 Series specifically addresses many policy enforcement requirements included in government and industry regulations, such as the PCI Data Security Standard. They also ease migration to new industry standards such as IPv6, supporting dynamic routing for both IPv4 and IPv6 networks. Fortinet's Global Threat Research Team and ICSA Labs-certified inspection engines ensure the best possible protection in your network.



Primary Features & Benefits

Enterprise-grade protection for smaller networks

- Enables deployment of Fortinet's unmatched protection and performance in smaller environments

Redundant connectivity methods

- Dual 10/100/1000 Ethernet, analog modem (FG/FWF-80CM models) and optional 3G wireless offer redundant WAN connections to ensure availability of data

Centralized Management

- FortiManager and FortiAnalyzer centralized management and reporting appliances simplify the deployment, monitoring, and maintenance of the security infrastructure

80 Series Deployment Options

Range of Deployment Options for Distributed Enterprises

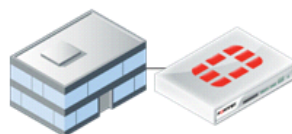
FortiGate 80 series deployment options include wired or wireless; dial backup modem or 3G wireless card support



Centralized Remote Management

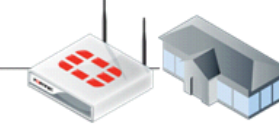
Distributed enterprises can manage thousands of FortiGate devices with FortiManager and FortiAnalyzer

Retail location with optional 3G Express Card for redundant connectivity



FortiGate 80C

Small Office with wireless for ease of deployment and WAN Optimization for lower costs



FortiWiFi 80CM



Internet

Redundant Connectivity

The FortiGate/FortiWiFi-80 Series platforms offer dual WAN Gigabit Ethernet (10/100/1000) links, for load balancing or redundant ISP connections delivering high availability and scalability to small or home office application. Six Fast Ethernet (10/100) internal security zone or switch ports and one dedicated DMZ port eliminate need for additional networking devices, reducing investment and management burden. An ExpressCard slot allows for optional 3G wireless WAN connectivity such as EV-DO, W-CDMA, HSPA and GPRS, which provides mobile network connectivity for remote deployments or backup data connectivity in the event of a network failure. The FortiGate/FortiWiFi-80CM platforms gives you the additional convenience and reliability of an analog modem.



FortiGate-80C



FortiGate-80CM

Internal Storage

The internal storage standard on the FortiGate/FortiWiFi-80 Series enables local caching of data for policy compliance or WAN optimization. WAN optimization lowers your networking costs and improves your application and network performance by reducing the amount of data transmitted over your WAN.



FortiWiFi-80CM

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 and compliance management, application control, 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 return and replace hardware support or 24x7 Comprehensive Support with advanced hardware replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and a 90-day limited software warranty.

| FortiGuard Subscription Services | | | | | | |
|----------------------------------|-----------|----------------------|---------------|-----------|---------------------|--------------------------|
| | Antivirus | Intrusion Prevention | Web Filtering | Antispam | Application Control | Vulnerability Management |
| FortiGate-80C | Supported | Supported | Supported | Supported | Supported | Supported |
| FortiGate-80CM | Supported | Supported | Supported | Supported | Supported | Supported |
| FortiWiFi-80CM | Supported | Supported | Supported | Supported | Supported | Supported |

Firewall

Fortinet firewall technology delivers industry-leading performance for network and application firewalling including Web 2.0 application policies based on the application identity, up to and beyond 10 Gbps throughput. Our technology identifies traffic patterns and links them to the use of specific applications, such as instant messaging and peer-to-peer applications, permitting application access control. By coupling application intelligence with firewall technology, the FortiGate platform is able to deliver real-time security with integrated application content level inspection, thereby simplifying security deployments.

| Firewall | |
|----------------------|--|
| Feature Highlights | NAT, PAT and Transparent (Bridge) Policy-Based NAT SIP/H.323/SCCP NAT Traversal VLAN Tagging (802.1Q) IPv6 Support |
| Performance | |
| Firewall (1518 Byte) | 1.9 Gbps |
| Firewall (512 Byte) | 700 Mbps |
| Firewall (64 Byte) | 120 Mbps |

Antivirus / Antispyware

Antivirus content inspection technology provides protection against virus, spyware, worms, phishing and other forms of malware being transmitted over the network infrastructure. By intercepting application content in transit, and reassembling the data into user expected content, the FortiGate Antivirus features ensures that malicious threats hidden within legitimate application content is identified and removed from the data stream destined for internal (or external) recipients. The addition of Fortinet's FortiGuard subscription services ensured each FortiGate has access to updated malware signatures, resulting in high level of accuracy and detection capabilities including emerging and newly discovered viruses. ICSA Labs has certified our antivirus functionality.

| Antivirus | |
|-------------------------|--|
| Features Supported | Proxy Antivirus Flow-based Antivirus File Quarantine IPv6 Support |
| Performance | |
| Antivirus (Proxy-based) | 50 Mbps |
| Antivirus (Flow-based) | 190 Mbps |

Intrusion Prevention

IPS technology provides protection against current and emerging network level threats. In addition to signature-based detection, we perform anomaly-based detection whereby our system alerts users to traffic that fits a profile matching attack behavior. This behavior is then analyzed by our threat research team to identify threats as they emerge and generate new signatures that will be incorporated into our FortiGuard services.

| Intrusion Prevention System | |
|-----------------------------|---|
| Features Supported | Automatic Attack Database Update Protocol Anomaly Support IPS and DoS Prevention Sensor Custom Signature Support IPv6 Support |
| Performance | |
| IPS Throughput | 350 Mbps |

VPN

Fortinet VPN technology provides secure communications between multiple networks and hosts, through both secure socket layer, or SSL, and IPsec VPN technologies, leveraging our custom FortiASIC to provide hardware acceleration for high-performance communications and data privacy. Benefits include the ability to enforce complete content inspection and multi-threat security as part of VPN communications, including antivirus, IPS and Web filtering. Additional features include traffic optimization providing prioritization for traffic across VPNs.

| VPN | |
|--------------------------|--|
| Feature Highlights | IPSec and SSL VPN DES, 3DES, AES and SHA-1/MD5 Authentication PPTP, L2TP, VPN Client Pass Through SSL Single Sign-On Bookmarks Two-Factor Authentication |
| Performance | |
| IPSec VPN | 140 Mbps |
| SSL VPN | 70 Mbps |
| Recommend # of SSL Users | 60 |

WAN Optimization

Wide Area Network (WAN) optimization accelerates applications over geographically dispersed networks, while ensuring multithreat inspection of all network traffic. WAN optimization eliminates unnecessary and malicious traffic, optimizes legitimate traffic, and reduces the amount of bandwidth required to transmit data between applications and servers. Improved application performance and delivery of network services reduces bandwidth and infrastructure requirements, along with associated expenditures.

WAN Optimization

| | |
|--------------------|--|
| Features Highlight | Gateway-to-Gateway Optimization Bi-directional Gateway-to-client Optimization Web Caching Secure Tunnel Transparent Mode |
|--------------------|--|

End-Point NAC

Endpoint NAC enforces the use of the FortiClient Endpoint Security application (either Standard or Premium editions) on your network. It verifies the installation of the most recent version of the FortiClient application, up-to-date antivirus signatures, and enabled firewall before allowing the traffic from that endpoint to pass through the FortiGate platform. You also have the option to quarantine endpoints running applications that violate policies and require remediation.

Endpoint Network Access Control (NAC)

| | |
|--------------------|---|
| Features Highlight | Monitor & Control Hosts Running FortiClient Vulnerability Scanning of Network Nodes Quarantine Portal Application Detection and Control Built-in Application Database |
|--------------------|---|

Web Filtering

Web filtering technology is a pro-active defense feature that identifies known locations of malware and blocks access to these malicious sources. In addition, the technology enables administrators to enforce policies based on website content categories ensuring users are not accessing content that is inappropriate for their work environment. The technology restricts access to denied categories based on the policy by comparing each Web address request to a Fortinet hosted database.

WEB Filtering

| | |
|--------------------|--|
| Features Highlight | HTTP/HTTPS Filtering URL / Keyword / Phrase Block Blocks Java Applet, Cookies or Active X MIME Content Header Filtering IPv6 Support |
|--------------------|--|

SSL Inspection

SSL-Encrypted Traffic Inspection protects clients and web and application servers from malicious SSL-encrypted traffic, to which most security devices are often blind. SSL Inspection intercepts encrypted traffic and inspects it for threats, prior to routing it to its final destination. SSL Inspection applies to both client-oriented SSL traffic (such as users connecting to an SSL-encrypted hosted CRM site) and inbound traffic destined an organization's own web and application servers. You now have the ability to enforce appropriate use policies on inappropriate encrypted web content, and protect servers from

SSL Inspection

| | |
|--------------------|---|
| Features Highlight | Protocol: HTTPS, SMTPS, POP3S, IMAPS Inspection support: Antivirus, Web Filtering, Antispam, Data Loss Prevention SSL Offload |
|--------------------|---|

Data Loss Prevention

It is imperative for you to control the vast amount of confidential, regulated, and proprietary data traversing your network, and keep it within defined network boundaries. Working across multiple applications (including those encrypting their communications), DLP uses a sophisticated pattern-matching engine to identify and then prevent the communication of sensitive information outside the network perimeter. In addition to protecting your organization's critical information, DLP also provides audit trails for data and files to aid in policy compliance. You can use the wide range of configurable actions to log, block, and archive data, as well as ban or quarantine users.

Data Loss Prevention (DLP)

| | |
|--------------------|---|
| Features Highlight | Identification And Control Over Data in Motion Built-in Pattern Database RegEx Based Matching Engine Common File Format Inspection International Character Sets Supported |
|--------------------|---|

Logging & Monitoring

FortiGate units provide extensive logging capabilities for traffic, system and network protection functions. They also allow you to compile reports from the detailed log information gathered. Reports provide historical and current analysis of network activity to help identify security issues that will reduce and prevent network misuse and abuse.

Logging and Monitoring

| | |
|--------------------|--|
| Features Highlight | Internal Log storage and Report Generation Graphical Real-Time and Historical Monitoring Graphical Report Scheduling Support Optional FortiAnalyzer Logging (including per VDOM) Optional FortiGuard Analysis and Management Service |
|--------------------|--|

Virtual Domain

Virtual Domain (VDM) enables a single FortiGate system to function as multiple independent virtual FortiGate systems. Each VDM contains its own virtual interfaces, security profiles, routing table, administration and many other features. FortiGate VDMs reduce the complexity of your physical network by virtualizing different security resources over a common platform, greatly reducing the power and footprint required by multiple point solutions.

| Virtual Domains | |
|----------------------|--|
| Features Highlight | Separate Firewall / Routing Domains Separate Administrative Domains Separate VLAN Interfaces |
| VDMs (Max / Default) | 10 / 10 |

Application Control

Application control enables you to define and enforce policies for thousands of applications running on your endpoints, regardless of the port or the protocol used for communication. Application classification and control is essential to manage the explosion of new web-based applications bombarding networks today, as most application traffic looks like normal web traffic to traditional firewalls. Fortinet's application control technology identifies application traffic and then applies security policies easily defined by the administrator. The end result is more flexible and granular policy control, with deeper visibility into your network traffic.

| Application Control | |
|---------------------|--|
| Features Highlight | Identify and Control Over 1800 Applications Traffic Shaping (Per Application) Control Popular IM/P2P Apps Regardless of Port / Protocol Popular Applications include: AOL-IM Yahoo MSN KaZaa ICQ Gnutella BitTorrent MySpace WinNY Skype eDonkey Facebook and more |

High Availability

High Availability (HA) configuration enhances reliability and increases performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide the maximum flexibility for utilizing each member within the HA cluster. The HA feature is included as part of the FortiOS operation system so end-users can benefit from the reliability enhancement without the extra cost.

| High Availability (HA) | |
|------------------------|---|
| Features Highlight | Active-Active and Active-Passive Stateful Failover (FW and VPN) Link State Monitor and Failover Device Failure Detection and Notification Server Load Balancing |

Wireless Controller

Wireless controller integrated into every FortiGate platform centralizes the management and monitoring of all FortiAP units. All wireless traffic is directed to the FortiGate multi-threat security platform and undergoes identity-aware firewall policies and UTM engine inspection. Only authorized wireless traffic is forwarded. From a single console you can control network access, update policies quickly and easily, and monitor compliance.

| Wireless Controller | |
|---------------------|--|
| Features Highlight | Managed and Monitor FortiAP product Rogue AP Detection, Control and Reporting Virtual AP with different SSID |

| Technical Specifications | FortiGate-80C | FortiGate-80CM | FortiWiFi-80CM |
|--|---|----------------|---------------------|
| Hardware Specifications | | | |
| 10/100/1000 WAN Interfaces (Copper, RJ-45) | 2 | 2 | 2 |
| 10/100 Internal Switch Interfaces (Copper, RJ-45) | 6 | 6 | 6 |
| 10/100 DMZ Interfaces (Copper, RJ-45) | 1 | 1 | 1 |
| Management Console Interface (Copper, RJ-45) | 1 | 1 | 1 |
| USB Interfaces | 2 | 2 | 2 |
| ExpressCard Slot | 1 | 1 | 1 |
| WLAN Support | - | - | 802.11 a/n or b/g/n |
| Modem Port | - | Yes | Yes |
| Internal Storage | 8 GB | | |
| System Performance | | | |
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | 1900 / 700 / 120 Mbps | | |
| Firewall Latency (64 byte UDP packets) | 45 µs | | |
| Firewall Throughput (Packets Per Second) | 180 Kpps | | |
| Concurrent Sessions (TCP) | 1 Million | | |
| New Sessions/Sec (TCP) | 12,000 | | |
| Firewall Policies | 5,000 | | |
| IPSec VPN Throughput (512 byte packets) | 140 Mbps | | |
| Gateway-to-Gateway IPSec VPN Tunnels | 200 | | |
| Client-to-Gateway IPSec VPN Tunnels | 1,000 | | |
| SSL-VPN Throughput | 70 Mbps | | |
| Concurrent SSL-VPN Users (Recommended Max) | 60 | | |
| IPS Throughput | 350 Mbps | | |
| Antivirus Throughput (Proxy Based / Flow Based) | 50 / 190 Mbps | | |
| Virtual Domains (Default / Max) | 10 / 10 | | |
| Max Number of FortiAPs | 16 | | |
| Max Number of FortiTokens | 100 | | |
| Max Number of Registered FortiClients | 10 | | |
| High Availability Configurations | Active/Active, Active/Passive, Clustering | | |
| Unlimited User Licenses | Yes | | |
| Dimensions | | | |
| Height x Width x Length | 1.75 x 10.87 x 6.13 in (4.45 x 27.61 x 15.57 cm) | | |
| Weight | 3.3 lb (1.5 kg) | | |
| Wall Mountable | Yes | | |
| Environment | | | |
| Power Required | 100-240 VAC, 50-60 Hz | | |
| Power Consumption (AVG / Max) | 25 / 30 W | 26 / 31.2 W | 28 / 33.6 W |
| Heat Dissipation | 102.3 BTU | 106.5 BTU | 115 BTU |
| Operating Temperature | 32 – 104 deg F (0 – 40 deg C) | | |
| Storage Temperature | -13 – 158 deg F (-25 – 70 deg C) | | |
| Humidity | 20 to 95% non-condensing | | |
| Compliance & Certification | | | |
| Compliance | FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, CB | | |
| Certification | ICSA Labs: Firewall, IPSec, IPS, Antivirus, SSL VPN | | |

All performance values are "up to" and vary depending on system configuration. Antivirus performance is measured using 44 Kbyte HTTP files. IPS performance is measured using 1 Mbyte HTTP files.

| Ordering Info | |
|--|---------------------|
| Unit | SKU |
| FortiGate-80C | FG-80C |
| FortiGate-80CM | FG-80CM |
| FortiWiFi-80CM | FWF-80CM |
| Optional Accessories | SKU |
| DC Adapter for the FG-80C, FG-80CM, FWF-80CM | SP-FG80-PDC |
| Wall Mount Kit (with express card lock) | SP-FG-50B-60B-MOUNT |

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, 199555 Singapore
Tel: +65-6513-3734
Fax: +65-6295-0015

Industry Certifications

FORTINET

Copyright © 2013 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.