



DATASHEET

FortiGate®/FortiWiFi™ -60C Series

Integrated Threat Management for Frontline Locations

Enterprise-Class Protection for Remote Offices, Retail, and Customer Premise Equipment

FortiGate/FortiWiFi-60C series consolidated security appliances deliver comprehensive enterprise-class protection for smaller locations, branch offices, customer premise equipment (CPE) and retail networks. An integrated set of essential security technologies deployed in a single device protects all of your applications and data. Simple per-device pricing, an integrated management console, and remote management capabilities significantly reduce your procurement, deployment and administration costs.

Comprehensive Protection and Optional Wireless Capability

FortiGate consolidated security appliances deliver an unmatched range of security technologies. They integrate firewall, IPSec and SSL VPN, antivirus, antispam, intrusion prevention, and web filtering into a single device at a single price. They also include data loss prevention (DLP), application control, SSL inspection, endpoint NAC and vulnerability management. In addition, Fortinet's FortiGuard® Labs is on duty around the clock and around the world, monitoring changes in the threat landscape. FortiGuard Labs deliver dynamic threat updates to protect your network against emerging threats.

FortiWiFi-60C/CM/CX appliances deliver the protection and performance you need with the convenience of wireless networking. Dual-band capabilities and support for 802.11a/b/g/n standards ensure compatibility with your existing network infrastructure. Multiple SSID support allows you to create multiple wireless access networks, enabling unencrypted guest or contractor access to the Internet while limiting access to corporate networks.

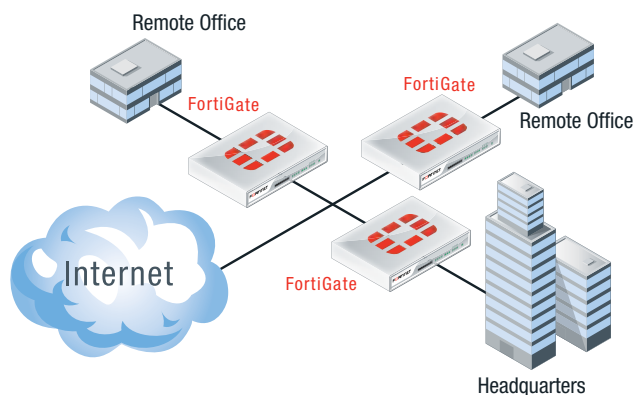
Purpose-Built Performance and Reliability

Fortinet's purpose-built hardware and software prevent your network security from becoming your network bottleneck. Custom FortiASIC processors maximize throughput while blocking unauthorized access and eliminating unwanted traffic from your network. The purpose-built FortiOS operating system minimizes delays in processing your data while efficiently enforcing your security policies.



FortiGate/FortiWiFi-60C Series Benefits

- Comprehensive protection against network, content, and application-level threats
- Segmentation of internal traffic and full security for perimeter-bound traffic
- Fortinet's purpose-built FS1 SoC processor delivers Gigabit firewall throughput
- GbE switched internal ports with dedicated WAN and DMZ ports
- Internal storage enables local log records and graphical reports
- WAN optimization and web caching improve network performance
- ExpressCard support and USB-based wireless broadband allow fast deployment of secure networks
- FortiExplorer setup utility provides easy setup and configuration



FORTIGATE IN THE DISTRIBUTED ENTERPRISE

Industry Certifications



FortiOS 4.0 Software—Raising The Bar

FortiOS 4.0: Redefining Network Security

FortiOS 4.0 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 the power of FortiASIC processors.

Fortinet's ASIC-Based Advantage

FortiASICs are a family of purpose-built, high performance processors that use an intelligent proprietary content scanning engine and multiple algorithms to accelerate security and network services.

FortiOS Security Services

FIREWALL

- ICSA Labs Certified (Enterprise Firewall)
- NAT, PAT, Transparent (Bridge)
- Routing Mode (RIP, OSPF, BGP, Multicast)
- Policy-Based NAT
- Virtual Domains (NAT/Transparent mode)
- VLAN Tagging (802.1Q)
- Group-Based Authentication & Scheduling
- SIP/H.323 /SCCP NAT Traversal
- WINS Support
- Explicit Proxy Support (Citrix/TS etc.)
- VoIP Security (SIP Firewall/RTP Pinholing)
- Granular Per-Policy Protection Profiles
- Identity/Application-Based Policy
- Vulnerability Management
- IPv6 Support (NAT/Transparent mode)

VIRTUAL PRIVATE NETWORK (VPN)

- ICSA Labs Certified (IPSec)
- PPTP, IPSec, and SSL Dedicated Tunnels
- SSL-VPN Concentrator (incl. iPhone client support)
- DES, 3DES, and AES Encryption Support
- SHA-1/MD5 Authentication
- PPTP, L2TP, VPN Client Pass Through
- Hub and Spoke VPN Support
- IKE Certificate Authentication (v1 & v2)
- IPSec NAT Traversal
- Automatic IPSec Configuration
- Dead Peer Detection
- RSA SecurID Support
- SSL Single Sign-On Bookmarks
- SSL Two-Factor Authentication
- LDAP Group Authentication (SSL)

NETWORKING/ROUTING

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

USER AUTHENTICATION OPTIONS

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

DATA CENTER OPTIMIZATION

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

ANTIVIRUS / ANTISPYWARE

- ICSA Labs Certified (Gateway Antivirus)
- Includes Antispyware and Worm Prevention:
- HTTP/HTTPS SMTP/SMTSP
- POP3/POP3S IMAP/IMAPS
- FTP IM Protocols
- Flow-Based Antivirus Scanning Mode
- Automatic "Push" Content Updates
- File Quarantine Support
- Databases: Standard, Extended, Extreme, Flow
- IPv6 Support

WEB FILTERING

- 76 Unique Categories
- FortiGuard Web Filtering Service Categorizes over 2 Billion Web pages
- HTTP/HTTPS Filtering
- Web Filtering Time-Based Quota
- URL/Keyword/Phrase Block
- URL Exempt List
- Content Profiles
- Blocks Java Applet, Cookies, Active X
- MIME Content Header Filtering
- IPv6 Support

APPLICATION CONTROL

- Identify and Control Over 1400 Applications
- Control Popular IM/P2P Apps Regardless of Port/Protocol:
- AOL-IM Yahoo MSN KaZaa
- ICQ Gnutella BitTorrent MySpace
- WinNY Skype eDonkey Facebook

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

VIRTUAL DOMAINS (VDMs)

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

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

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

INTRUSION PREVENTION SYSTEM (IPS)

- ICSA Labs Certified (NIPS)
- Protection From Over 3000 Threats
- Protocol Anomaly Support
- Custom Signature Support
- Automatic Attack Database Update
- IPv6 Support

DATA LOSS PREVENTION (DLP)

- Identification and Control Over Sensitive Data in Motion
- Built-in Pattern Database
- RegEx-based Matching Engine for Customized Patterns
- Configurable Actions (block/log)
- Supports IM, HTTP/HTTPS, and More
- Many Popular File Types Supported
- International Character Sets Supported

ANTISPAM

- Support for SMTP/SMTSP, POP3/POP3S, IMAP/IMAPS
- 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

ENDPOINT COMPLIANCE AND CONTROL

- Monitor & Control Hosts Running FortiClient Endpoint Security

MANAGEMENT/ADMINISTRATION

- Console Interface (RS-232)
- WebUI (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH)
- Command Line Interface
- Role-Based Administration
- Multi-language Support: English, Japanese, Korean, Spanish, Chinese (Simplified & Traditional), French
- Multiple Administrators and User Levels
- Upgrades and Changes via TFTP and WebUI
- System Software Rollback
- Configurable Password Policy
- Optional FortiManager Central Management

LOGGING/MONITORING/VULNERABILITY

- Local Event Logging
- Log to Remote Syslog/WELF Server
- Graphical Real-Time and Historical Monitoring
- SNMP Support
- Email Notification of Viruses And Attacks
- VPN Tunnel Monitor
- Optional FortiAnalyzer Logging / Reporting
- Optional FortiGuard Analysis and Management Service

Firewall

Fortinet firewall technology delivers complete content and network protection by combining stateful inspection with a comprehensive suite of powerful security features. Application control, antivirus, IPS, Web filtering and VPN, along with advanced features such as an extreme threat database, vulnerability management and flow-based inspection work in concert to identify and mitigate the latest complex security threats. The security-hardened FortiOS operating system works together with purpose-built FortiASIC processors to accelerate inspection throughput and identification of malware.

Features

- NAT, PAT and Transparent (Bridge)
- Policy-Based NAT
- SIP/H.323/SCCP NAT Traversal
- VLAN Tagging (802.1Q)
- Vulnerability Management
- IPv6 Support

Firewall Throughput

1518 Byte Packets	1 Gbps
512 Byte Packets	1 Gbps
64 Byte Packets	950 Mbps

Antivirus / Antispyware

Antivirus content inspection technology protects against viruses, spyware, worms, and other forms of malware which can infect network infrastructure and endpoint devices. By intercepting and inspecting application-based traffic and content, antivirus protection ensures that malicious threats hidden within legitimate application content are identified and removed from data streams before they can cause damage. FortiGuard subscription services ensure that FortiGate devices are updated with the latest malware signatures for high levels of detection and mitigation.

Features

- Automatic Database Updates
- Proxy-based Antivirus
- Flow-based Antivirus
- File Quarantine
- IPv6 Support

Antivirus Performance

Antivirus Throughput	20 Mbps
----------------------	---------

Intrusion Prevention

IPS technology protects against current and emerging network-level threats. In addition to signature-based threat detection, IPS performs anomaly-based detection which alerts users to any traffic that matches attack behavior profiles. The Fortinet threat research team analyzes suspicious behavior, identifies and classifies emerging threats, and generate new signatures to include with FortiGuard Service updates.

Features

- Automatic Database Updates
- Protocol Anomaly Support
- IPS and DoS Prevention Sensor
- Custom Signature Support
- IPv6 Support

IPS Throughput

IPS	100 Mbps
-----	----------

VPN

Fortinet VPN technology provides secure communications between multiple networks and hosts, using SSL and IPsec VPN technologies. Both services leverage our custom FortiASIC processors to provide acceleration in the encryption and decryption steps. The FortiGate VPN service enforces complete content inspection and multi-threat protections including antivirus, intrusion prevention and Web filtering. Traffic optimization provides prioritization for critical communications traversing VPN tunnels.

Features

- 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

VPN Performance

IPSec VPN Throughput	70 Mbps
SSL VPN Throughput	15 Mbps
Concurrent SSL VPN Users Recommended (Max)	50
Client-to-Gateway IPSec VPN Tunnels	100

WAN Optimization

Wide Area Network (WAN) optimization accelerates applications over geographically dispersed networks, while ensuring multi-threat 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.

Features

- Gateway-to-Gateway Optimization
- Bidirectional Gateway-to-client Optimization
- Web Caching
- Secure Tunnel
- Transparent Mode

Endpoint NAC

Endpoint NAC can enforce the use of FortiClient Endpoint Security for users connecting to corporate networks. Endpoint NAC verifies FortiClient Endpoint Security installation, firewall operation and up-to-date antivirus signatures before allowing network access. Non-compliant endpoints, such as endpoints running applications that violate security policies can be quarantined or sent to remediation.

Features

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

Web Filtering

Web filtering protects endpoints, networks and sensitive information against Web-based threats by preventing users from accessing known phishing sites and sources of malware. In addition, administrators can enforce policies based on Website categories to easily prevent users from accessing inappropriate content and logging networks with unwanted traffic.

Features

- HTTP/HTTPS Filtering
- URL / Keyword / Phrase Block
- Blocks Java Applet, Cookies or Active X
- MIME Content Header Filtering
- Flow-based Web Filtering
- IPv6 Support

SSL-Encrypted Traffic Inspection

SSL-encrypted traffic inspection protects endpoint clients and Web and application servers from hidden threats. SSL Inspection intercepts encrypted traffic and inspects it for threats prior to routing it to its final destination. It can be applied to client-oriented SSL traffic, such as users connecting to cloud-based CRM site, and to inbound Web and application server traffic. SSL inspection enables you to enforce appropriate use policies on encrypted Web content and to protect servers from threats which may be hidden inside encrypted traffic flows.

Features

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

Data Loss Prevention

DLP uses a sophisticated pattern-matching engine to identify and prevent the transfer of sensitive information outside of your network perimeter, even when applications encrypt their communications. In addition to protecting your organization's critical data, Fortinet DLP provides audit trails to aid in policy compliance. You can select from a wide range of configurable actions to log, block, and archive data, and quarantine or ban users.

Features

- Identification and Control Over Data in Motion
- Built-in Pattern Database
- RegEx Based Matching Engine
- Common File Format Inspection
- International Character Sets Supported
- Flow-based DLP

Logging, Reporting and Monitoring

FortiGate consolidated security appliances provide extensive logging capabilities for traffic, system, and network protection functions. They also allow you to assemble drill-down and graphical reports from detailed log information. Reports can provide historical and current analysis of network activity to aid with identification of security issues and to prevent network misuse and abuse.

Features

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

High Availability

High Availability (HA) configurations enhance reliability and increase performance by clustering multiple FortiGate appliances into a single entity. FortiGate High Availability supports Active-Active and Active-Passive options to provide maximum flexibility for utilizing each member within the HA cluster. The HA feature is included as part of the FortiOS operation system and is available with most FortiGate appliances.

Features

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

Virtual Domains

Virtual Domains (VDOMs) enable a single FortiGate system to function as multiple independent virtual FortiGate systems. Each VDOM contains its own virtual interfaces, security profiles, routing table, administration, and many other features. FortiGate VDOMs reduce the complexity of securing disparate networks by virtualizing security resources on the FortiGate platform, greatly reducing the power and footprint required as compared to multiple point products. Ideal for large enterprise and managed service providers.

Features

- Separate Firewall / Routing Domains
- Separate Administrative Domains
- Separate VLAN Interfaces
- Maximum VDOMs: 10
- Default VDOMs: 10

Wireless Controller

All FortiGate and FortiWiFi™ consolidated security platforms have an integrated wireless controller, enabling centralized management of FortiAP™ secure access points and wireless LANs. Unauthorized wireless traffic is blocked, while allowed traffic is subject to identity-aware firewall policies and multi-threat security inspection. From a single console you can control network access, update security policies, and enable automatic identification and suppression of rogue access points.

Features

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

Application Control

Application control enables you to define and enforce policies for thousands of applications running across networks regardless of port or the protocol used for communication. The explosion of new Internet-based and Web 2.0 applications bombarding networks today make application control essential, as most application traffic looks like normal Web traffic to traditional firewalls. Fortinet application control provides granular control of applications along with traffic shaping capabilities and flow-based inspection options.

Features

- Identify and Control Over 1,400 Applications
- Traffic Shaping (Per Application)
- Control Popular Apps Regardless of Port or Protocol
- Popular Applications include:
 - AOL-IM
 - Yahoo
 - MSN
 - KaZaa
 - ICQ
 - Gnutella
 - BitTorrent
 - MySpace
 - WinNY
 - Skype
 - eDonkey
 - Facebook
- and more...

Setup / Configuration Options

Fortinet provides administrators with a variety of methods and wizards for configuring FortiGate appliances during deployment. From the easy-to-use Web-based interface to the advanced capabilities of the command-line interface, FortiGate systems offer the flexibility and simplicity you need.

Features

- FortiExplorer Setup Wizard over USB (FG-60C/FWF-60C/FWF-60CM/FWF-60CX-ADSL)
- Web-based User Interface
- Command Line Interface (CLI) Over Serial Connection
- Pre-configured Settings from USB Drive

Technical Specifications	FortiGate-60C	FortiWiFi-60C	FortiWiFi-60CM	FortiWiFi-60CX-ADSL-A
Interfaces				
10/100/1000 Internal Switch Interfaces (Copper, RJ-45)	5	5	5	4
10/100 Internal Switch Interfaces (Copper, RJ-45)	-	-	-	4
10/100/1000 WAN Interfaces (Copper, RJ-45)	2	2	2	2
10/100/1000 DMZ Interfaces (Copper, RJ-45)	1	1	1	-
Modem Port	-	-	1	-
ADSL2+ Annex A Interface	-	-	-	1
Management Console Interface (Copper, RJ-45)	1			
USB Interfaces	2 (1 Type-A, 1 Type-B)			
ExpressCard Slot	1			
Internal Storage	8 GB			
Wireless Standards Supported	-	802.11 a/b/g/n	802.11 a/b/g/n	802.11 a/b/g/n
System Performance				
Firewall Throughput (1518 byte UDP packets)	1 Gbps			
Firewall Throughput (512 byte UDP packets)	1 Gbps			
Firewall Throughput (64 byte UDP packets)	950 Mbps			
IPSec VPN Throughput	70 Mbps			
SSL VPN Throughput	15 Mbps			
IPS Throughput	100 Mbps			
Antivirus Throughput* (Proxy-based)	20 Mbps			
Antivirus Throughput* (Flow-based)	35 Mbps			
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	50 / 50			
Client-to-Gateway IPSec VPN Tunnels	100			
Max Concurrent Firewall Sessions	80,000			
Firewall Sessions/Sec	3,000			
Max Concurrent SSL-VPN Users	50			
Firewall Policies (System / VDOM)	5,000 / 500			
Virtual Domains (Max / Default)	10 / 10			
Wireless Access Points Controlled	4			
Unlimited User Licenses	Yes			
Mean Time Between Failures	More than 7 years			
Dimensions				
Height x Width x Length	1.44 x 8.50 x 5.81 in (3.66 x 21.59 x 14.76 cm)			1.74 x 13.51 x 8.27 in (4.44 x 34.33 x 21.0 cm)
Weight	1.9 lb (0.86 kg)	2.1 lb (0.95 kg)	1.89 lb (0.85 kg)	4.67lb (2.12 kg)
Wall Mountable	No	Yes	Yes	No
Environment				
Power Required	100-240 VAC, 50-60 Hz, 1.5 Amp Max			
Power Consumption (AVG)	15.7 W	19 W	11.6 W	19.7 W
Heat Dissipation	53.6 BTU	64.8 BTU	47.5 BTU	81.9 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)			
Storage Temperature	-13 – 158 deg F (-25 – 70 deg C)			
Humidity	5 to 95% non-condensing			
Compliance				
Industry Certifications	ICSA Labs: Firewall, Antivirus, SSL VPN, Intrusion Prevention			
Safety Certifications	FCC Part 15, UL/CUL, C Tick, CE, VCCI			

* Antivirus performance is measured using HTTP traffic with 32 Kbyte file attachments. IPS performance is measured base on NSS like test methodology with 44K HTTP files.

Ordering Information

SKU	Description
FG-60C	(2) 10/100/1000 WAN ports, (1) 10/100/1000 DMZ port, (5) 10/100/1000 internal switch ports, (2) USB, ExpressCard slot, 8GB internal storage
FWF-60C	Wireless (802.11a/b/g/n), (2) 10/100/1000 WAN ports, (1) 10/100/1000 DMZ port, (5) 10/100/1000 internal switch ports, (2) USB, ExpressCard slot, 8GB internal storage
FWF-60CM	Wireless (802.11a/b/g/n), (2) 10/100 WAN ports, (1) 10/100 DMZ port, (5) 10/100/1000 internal switch ports, (1) ExpressCard slot, analog modem port
FWF-60CX-ADSL-A	Wireless (802.11a/b/g/n), (2) 10/100/1000 WAN ports, (4) 10/100/1000 ports, 4-port 10/100 internal switch, (1) ADSL2+ Annex A interface, ExpressCard slot, 8GB local storage

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.