FortiGate-224B

Network Access Security Solutions

Datasheet

Integrated Network Access Edge Security

Threats from the Outside – Threats on the Inside

Broadband and wireless technologies are enabling flexible virtual offices with network access anytime, anywhere, and from any device. Increased productivity, enhanced customer service and reduced costs are all welcome benefits. Not so welcome are the increasing number of security threats originating from devices inside the network. Laptops, PDAs and other mobile devices are frequently used outside the corporate network, over un-trusted connections, and exposed to viruses, worms and other security threats. Back in the corporate network, these devices are typically treated as trusted assets and given unrestricted network access. At this point the security threats acquired outside, having completely bypassed perimeter defenses, now proceed to wreak havoc. Similarly guests, such as partners or suppliers, typically access your network while onsite from within the secured perimeter, using unmanaged devices that represent a completely unknown threat to other network assets.

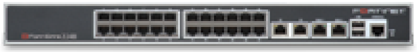
As a result of the rise in internal threats, administrators are finding that securing the network from the inside is equally as important as securing the network from the outside. In today's mobile work environment, achieving and maintaining regulatory compliance means that network access must be controlled from all points of access in order to ensure adequate security of your organization's assets. To accomplish this goal, you could use multiple point product security solutions, including endpoint software agents, policy servers and other security gateways. The problem with this approach is that these solutions are not only costly to own and manage, but also degrade performance and reduce network availability.

All-in-One Network Access Security Solutions

The FortiGate™-224B system provides the industry's most effective network access security solution by tightly integrating a high-performance Layer 2 switch with a Fortinet multi-layered security gateway. The FortiGate-224B simplifies the challenge of network access-layer security while providing the highest level of performance and protection. Performance is maximized by tightly integrating the purpose built FortiASIC™ network processor with the Layer 2 switch. Utilizing the FortiOS™ suite of security solutions, threats from endpoint devices are automatically identified and blocked before they enter the network. Devices that are not compliant with security policies or exhibit any type of threat will be placed in quarantine. The FortiGate-224B provides self-remediation features that allow users to resolve security violations and regain network access without involving the IT or security staff.

Key Solution Features and Benefits

Enhances Network Security	The FortiGate-224B enforces security policy at the network access layer to provide protection against intrusion attempts, viruses, worms, denial of service attacks, spyware and blended threats.
Reduces Complexity & Cost	The FortiGate-224B provides access control functions with the added security benefits of complete content inspection, all in a single device that eliminates requirements for other access control elements, such as costly external policy servers or difficult to manage client software.
Lowers Operational Overhead & Expense	Self-remediation reduces the need for skilled resources to identify and perform corrective actions.
Delivers the Highest Levels of Performance & Reliability	The FortiGate-224B provides maximum performance by tightly integrating a wire-speed Layer 2 switch with Fortinet's real-time FortiASIC network processor.

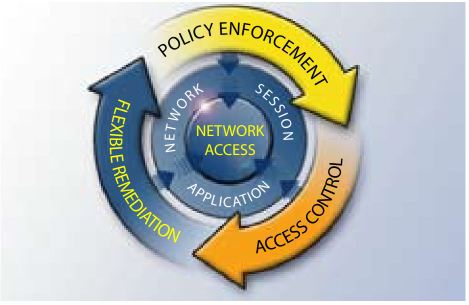

FortiGate-224B

The Network Access Protection Cycle

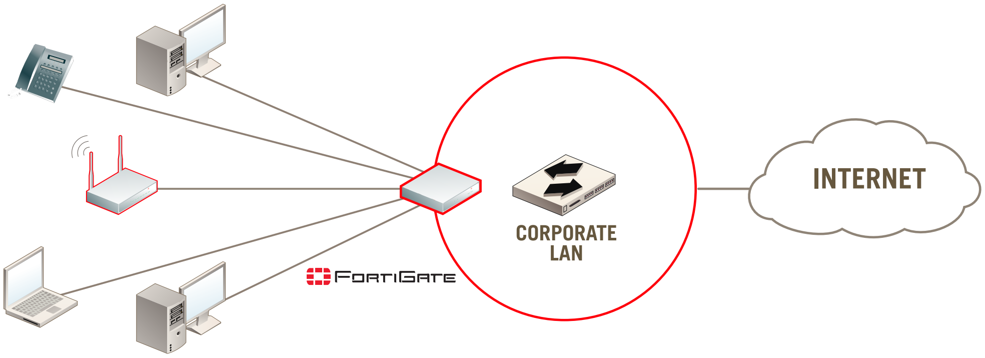
Effective network access protection requires the ability to:

1. Implement access controls that evaluate the security state of a user or device
2. Continually monitor the security state of users that are already connected
3. Quarantine users or devices based on network access and system policies
4. Allow flexible policy management and self-remediation control

Optimal solutions provide high performance and reliability yet are cost effective to manage and maintain.

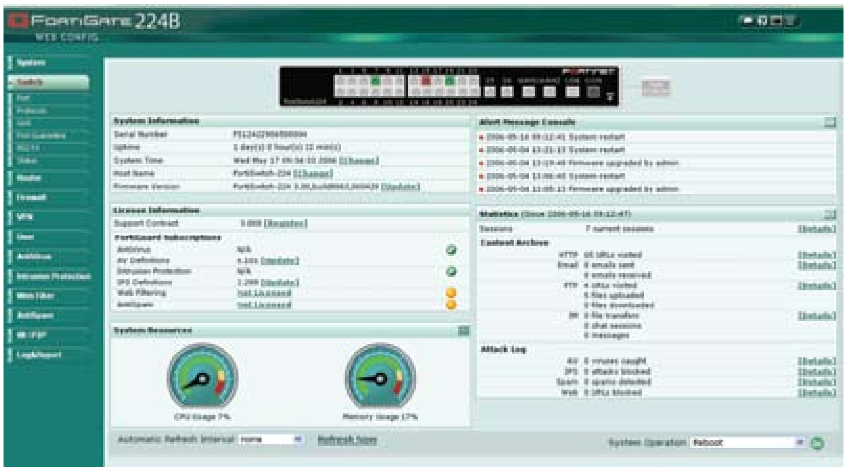


FortiGate-224B Integrated Appliance
for Network Access Security



Clientless Network Access Control

The FortiGate-224B enables clientless access security control that enforces network policies without requiring special end-user software agents. The FortiGate-224B functions as a high-performance Layer 2 switching with integrated FortiOS security solutions such as firewall, intrusion prevention and antivirus protection. The FortiGate-224B supports PCs, PDAs, VoIP phones, and wireless LAN devices. Operating in strict or dynamic modes, it transparently monitors and enforces security policies.



System Information

Serial Number [illegible]
Uptime 1 day(s) 0 hour(s) 22 min(s)
System Time Wed May 17 09:34:33 2006 [Change]
Host Name FortiSwitch-224 [Change]
Firmware Version FortiSwitch-224 3.00,build0063,060429 [Update]

License Information

Support Contract 3.000 [Register]
FortiGuard Subscriptions
AntiVirus N/A
AV Definitions 6.101 [Update]
Intrusion Protection N/A
IPS Definitions 2.288 [Update]
Web Filtering Not Licensed
AntiSpam Not Licensed

System Resources

CPU Usage 7%
Memory Usage 17%

Automatic Refresh Interval none Refresh Now

Alert Message Console

- 2006-05-16 09:12:41 System restart
- 2006-05-04 13:21:13 System restart
- 2006-05-04 13:19:48 Firmware upgraded by admin
- 2006-05-04 13:06:48 System restart
- 2006-05-04 13:05:13 Firmware upgraded by admin

Statistics (Since 2006-05-16 09:12:47)

Sessions 7 current sessions [Details]
Content Archive
HTTP 10 URLs visited [Details]
Email 0 emails sent [Details]
0 emails received
FTP 4 URLs visited [Details]
5 files uploaded
0 files downloaded
IM 0 file transfers [Details]
0 chat sessions
0 messages
Attack Log
AV 0 viruses caught [Details]
IPS 0 attacks blocked [Details]
Spam 0 spams detected [Details]
Web 0 URLs blocked [Details]

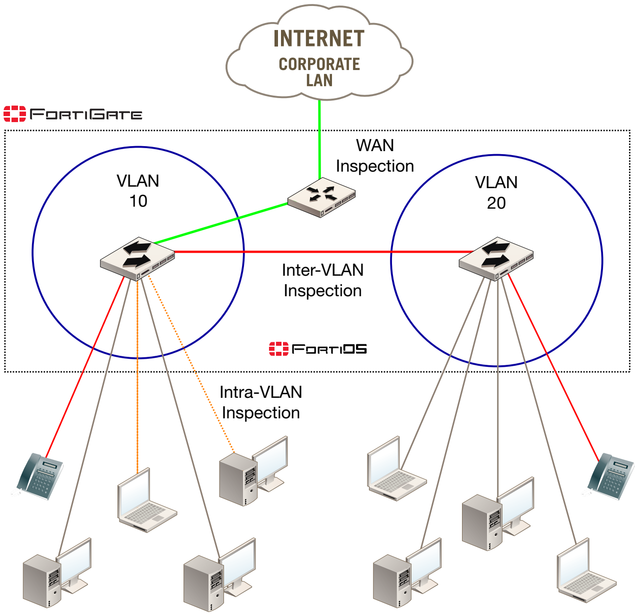
System Operation Reboot

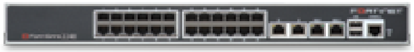
Easy to Own — Easy to Operate

Deploying and operating your network is easy using the FortiGate secure web-based user interface. Device and policy management, flexible configuration of security modules and the ability to rapidly implement new FortiGuard™ Center updates ensures you are in complete control of network access. Administrator defined self-remediation empowers users with the ability to self service infected systems without requiring skilled resources to identify and perform corrective actions.

Trust — Verify — Monitor

The FortiGate-224B employs the full-suite of FortiOS security solutions to enforce compliance with network access policies. Configurable to operate in a “strict” mode, where all ports are initially in an un-trusted quarantine state, or in “dynamic” mode in which all ports are initially in a trusted network state. Strict mode redirects access attempts to a web portal where administrator defined security checks are performed. Alternatively utilizing dynamic mode ports are allowed network access, based on administrator defined policies, until a threat or policy violation is detected. Should FortiGate antivirus or intrusion protection monitoring detect a violation the port is reassigned and all traffic is restricted to a quarantine VLAN. Once a device passes remediation requirements it is removed from quarantine.





Feature	FortiGate-224B
Security Hardened Platform	Yes
10/100 Switch Ports	24
10/100/1000 Switch Ports	2
10/100 WAN Ports	2
USB Ports	2
RS-232 Console Connection Port	Yes
Layer 2 Switch Performance	4.4 Gbps
Concurrent Sessions	400,000
New Sessions/Second	4,000
Firewall Throughput	150 Mbps
VPN 168-bit Triple-DES Throughput	70 Mbps
Anti Virus Throughput	30 Mbps
Dedicated IPsec VPN tunnels	200
Policies	2,000
Dimensions (H, W, L)	1.75 x 16.8 x 10 in (4.5 x 42.7 x 25.4 cm)
Weight	7.3 lb. (3.3 kg)
Rack Mountable	Yes
Input Voltage	100-240 VAC
Input Current	1.6A
Operating Temperature	32 to 104 deg F (0 to 40 deg C)
Storage Temperature	-13 to 158 deg F (-25 to 70 deg C)
Humidity	5 to 95% non-condensing
Regulatory	FCC Class A Part 15
	CE

The FortiGate-224B Features

Providing the following switching and security features:

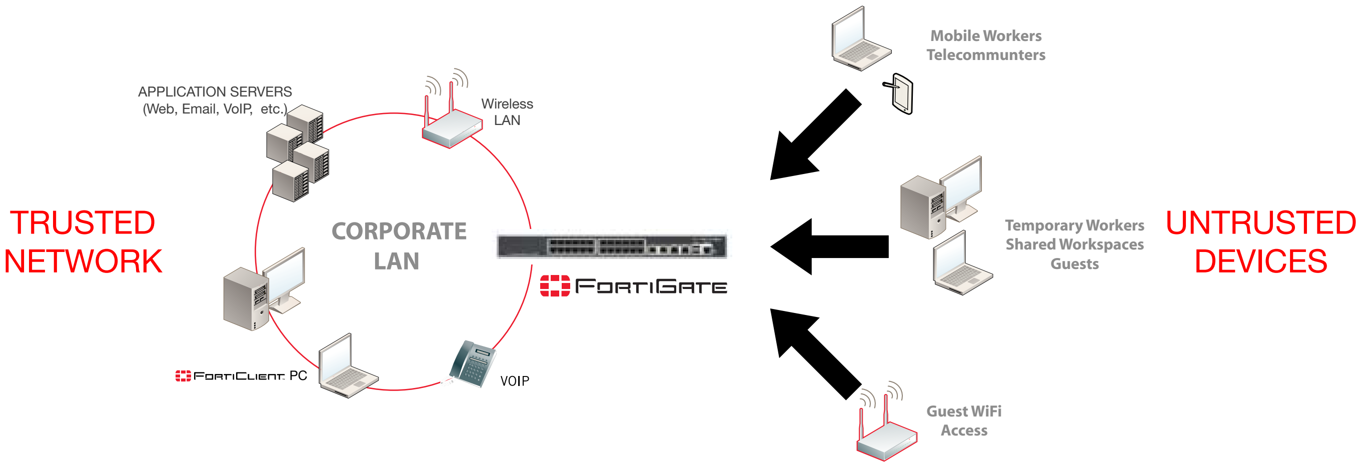
FortiOS Multi-Threat Security Suite	The functionality and performance of a FortiGate™ security system. This includes firewall, antivirus, intrusion detection / prevention, IPsec and SSL VPN, web content filtering, antispyware and antispam features.
Layer 2 Switching	Multi-port 10/100/1000 Ethernet switching with advanced routing, load sharing, QoS and Authentication.
Clientless Port-Based Quarantine	Simpler and less costly to implement than typical NAC solutions. In addition to providing access control functionality, The FortiGate-224B also provides threat blocking and device quarantine, all without requiring client software.
Configurable Port Quarantinee	Trusted or un-trusted access control based on security policies.
Self-Remediation	User self-remediation can include options such as loading software patches/updates, installation of the FortiClient PC security software or other options based on administrator definitions. Users must pass host checking requirements to be allowed back in to the network.

Dynamic Quarantine

The FortiGate-224B “dynamic” quarantine is perfect for situations in which partners, suppliers or other visitors need to access the network. Initially all ports and devices are “trusted,” but continually verified by the integrated FortiOS security functions. In the event a security threat or policy violation is detected the FortiGate-224B immediately quarantines the port to avoid further exposure.

Self-Remediation

The FortiGate-224B provides configurable self-remediation options such as directing users to: FortiClient software, internal web portals, operating system updates or access to other client software. Self-remediation reduces ongoing operating costs.


TRUSTED NETWORK
APPLICATION SERVERS (Web, Email, VoIP, etc.)
Wireless LAN
CORPORATE LAN
FORTIGATE
FORTICLIENT PC
VOIP
Mobile Workers Telecommunters
Temporary Workers Shared Workspaces Guests
UNTRUSTED DEVICES
Guest WiFi Access

Policy Enforcement ◆ Access Control ◆ Flexible Remediation

TECHNICAL SPECIFICATIONS: The FortiGate-224B provides the following features:

SYSTEM MANAGEMENT
Console Interface (RS-232)
Web User Interface (HTTP / HTTPS)
Telnet
Multi-Language Support
Command Line Interface
Secure Command Shell (SSH)

NETWORKING
Multiple Wan Link Support
PPPoE
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP V1 & V2, OSPF, BGP and Multicast)
Multi-Zone Support
Route Between Zones
Route Between Virtual LANs

LAYER 2 SWITCHING
802.1x Authentication
Port-Based L2 Forwarding (Wire-Speed)
Spanning Tree Features Supports STP, RSTP, PVST+
802.3ad Link Aggregation
802.1Q VLAN Tagging
802.1p Class of Service
Per Port Queuing and QOS

QUARANTINE
Strict or Dynamic Modes
Client-Less Port-Based Quarantine
Port-Based Quarantining
Antivirus or IPS Signature Trigger
Quarantine VLAN
Administrator Defined Resource Access
Manual or Dynamic Configuration Options
Quarantine Portal
Redirect Web Request to Internal Portal
- Client Remediation
- Administrator Defined Parameters
User Self Remediation

VPN
PPTP, IPsec, and SSL
Dedicated Tunnels
Encryption (DES, 3DES, AES)
SHA-1 / MD5 Authentication
PPTP, L2TP, VPN Client Pass Though
Hub and Spoke VPN Support
IKE Certificate Authentication
IPsec NAT Traversal
Dead Peer Detection
RSA SecurID 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

HIGH AVAILABILITY (HA)
Active-Active, Active-Passive
Stateful Failover (FW And VPN)
Device Failure Detection and Notification
Link Status Monitor
Link Failover

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 NAT Traversal
WINS Support
Customized Protection Profiles

SECURITY FEATURES
Complete FortiOS Multi-Threat Security
Inspection of Traffic Between VLANs
Secure Port
Inspection of Traffic to / from a Specific Port
WAN Ports Policies
Inspection of Traffic to / from WAN Port
All Policies Can Be Mixed

WEB CONTENT FILTERING
URL/Keyword/Phrase Block
URL Exempt List
Content Profiles
Blocks Java Applet, Cookies, ActiveX
Automatic Real-Time Updates From FortiGuard Network

INTRUSION PREVENTION SYSTEM (IPS)
Prevention for Over 2000 Attacks
Customizable Dynamic Detection Signature List
Automatic Attack Database Update

TRAFFIC SHAPING
Policy-Based Traffic Shaping
Diffserv Setting (DSCP)
Guarantee / Max / Priority Bandwidth

ANTIVIRUS / ANTISPYWARE
Scans HTTP, SMTP, POP3, IMAP, FTP and IM Encrypted VPN Tunnels
Automatic “Push” Virus Database Update
Quarantine Infected Messages
Block by File Size
Block by Type
Automatic Real-Time Updates From FortiGuard Network

FortiGuard Subscription Services
Includes:
- Automatic updates from over 50 redundant high speed database servers around the globe.
- Complete Wildlist virus protection for over 4,500 active viruses from FortiGuard’s active database of over 60,000 viruses.
- Real-time signature updates for protection against over 6,000 threats.
- 76 rated web categories for more accurate web content filtering.
- Web filtering for more than 25 million rated domains and 2 billion rated Web pages.

FortiCare™ Support Services
Includes:
- 24 X 7 X 365 FortiCare Web Service
- Email Technical Support *
- 1-Year Limited Hardware Warranty
- 90-Day Limited Software Warranty

* 24 X 7 Telephone Technical Support available.

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 +33-1-5858-0025

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

©Copyright 2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiGuard, FortiCare, FortiASIC, FortiManager, FortiWiFi, FortiClient, FortiLog and FortiReporter are trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600, DAT140-0906-R2