

# FortiGate® Virtual Appliances

## Consolidated Security for Virtual Environments

FortiGate virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. Moreover, FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

### Proven Success in Virtual Environments

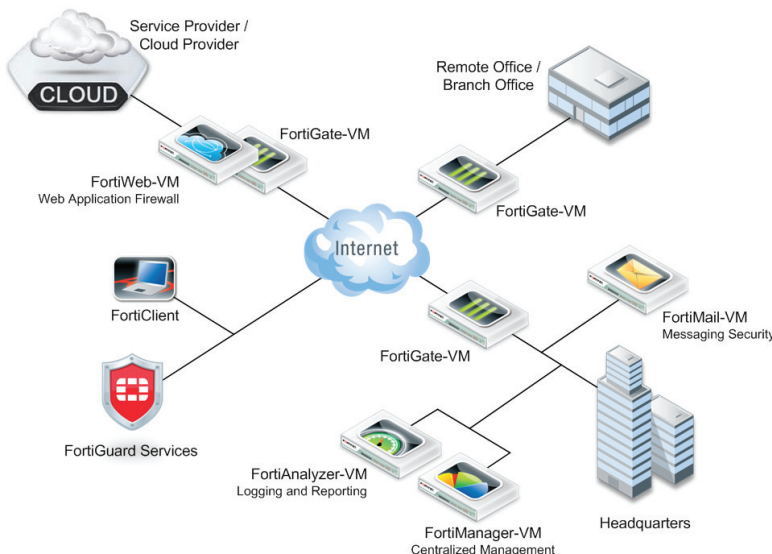
Fortinet introduced Virtual Domain (VDM) technology in 2004. Since that time, we have offered virtualized security to service providers and enterprises alike. With the addition of the virtual appliance form factor, Fortinet now offers greater choice and flexibility to customers by providing the ability to deploy our security solution within an existing virtualized infrastructure.

### Choice of Form Factor

Few organizations use 100% hardware or 100% virtual IT infrastructure today, creating a need for both hardware appliances and virtual appliances in your security strategy. Fortinet allows you to build the security solution that's right for your environment with hardware and virtual appliances to secure the core, the edge and increase visibility and control over communications within the virtualized infrastructure. FortiManager virtual appliances allow you to easily manage and update your Fortinet security assets – hardware, virtual or both – from a single pane of glass. FortiAnalyzer central reporting, FortiWeb web application firewall, and FortiMail messaging security appliances round out Fortinet's current virtual appliance solutions.

### Multi-Threat Security

Using the advanced FortiOS™ operating system, FortiGate appliances effectively neutralize a wide range of security threats facing your virtualized environment. Whether deployed at the edge as a front-line defense, or deep within the virtual infrastructure for inter-zone security, FortiGate appliances protect your infrastructure with some of the most effective security available today.

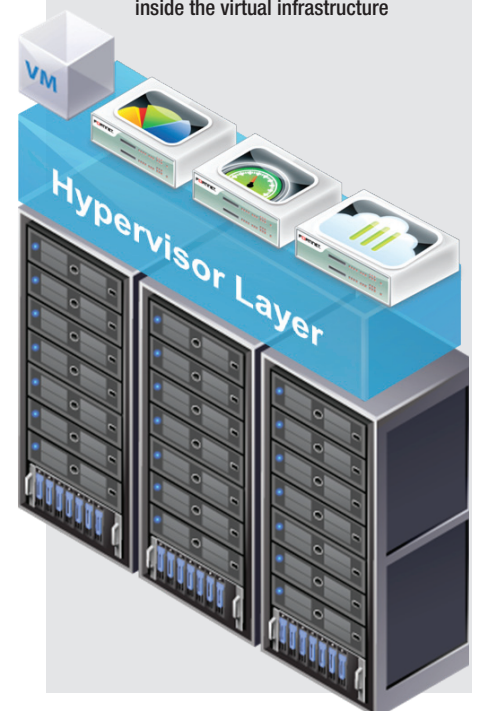


### FortiGate Virtual Appliance Benefits

FortiGate virtual appliances offer protection from a broad array of threats, with support for all of the security and networking services offered by the FortiOS operating system. In addition, the appliances offer these benefits:

- Increased visibility within virtualized infrastructure
- Rapid deployment capability
- Ability to manage virtual appliances and physical appliances from a single pane of glass management platform
- Simple licensing with no per-user fees

FortiGate Virtual Appliances deployed inside the virtual infrastructure



## The Fortinet Virtual Appliance Family

### FortiGate-VM multi-threat security

- Consolidated security in a virtual form factor
- 5 virtual appliance models available

### FortiManager-VM centralized management

- Command and control for Fortinet infrastructure
- Stackable license model to grow with your environment

### FortiAnalyzer-VM centralized reporting

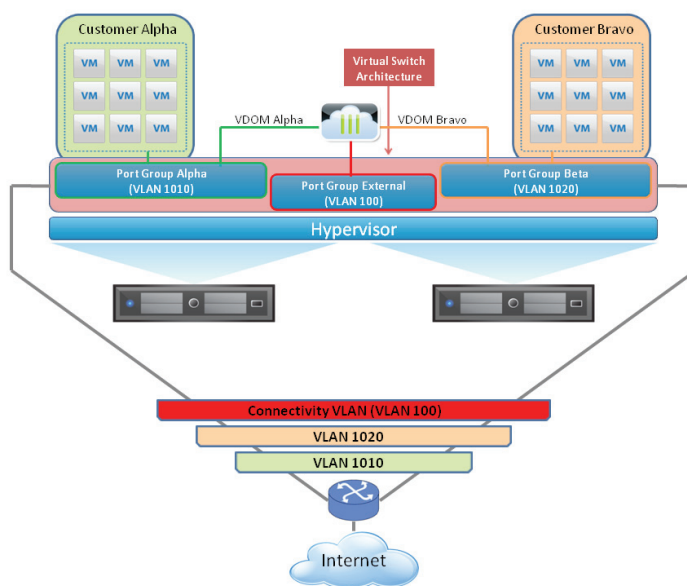
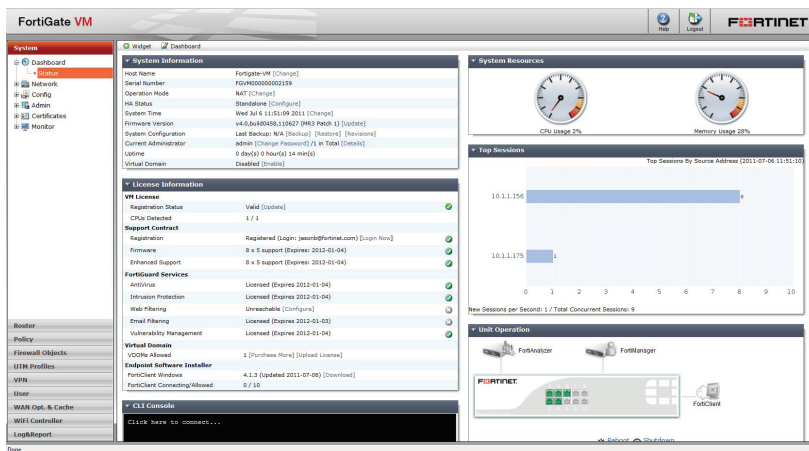
- Aggregate log data for forensic analysis
- Perform vulnerability assessments of networked hosts
- Generate graphical reports to aid in demonstrating compliance

### FortiMail-VM messaging security

- Block spam and malware from users' inboxes
- Archive mail for compliance and e-discovery purposes

### FortiWeb-VM web application firewall

- Protect, balance and accelerate web applications
- Improves security of confidential information and aids PCI compliance



## FortiGuard and FortiCare Services

**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, application control, vulnerability and compliance management, and database security services.

For more information about FortiGuard Services, please visit [www.fortiguard.com](http://www.fortiguard.com).

FortiGuard Subscription Services						
Product	Antivirus	Intrusion Prevention	Web Filtering	Antispam	Application Control	Vulnerability & Compliance
FortiGate Virtual Appliance	Supported	Supported	Supported	Supported	Supported	Supported

**FortiCare™** Support Services offerings provide global support for all Fortinet products and services. Customer satisfaction and responsiveness is Fortinet's number one priority. With FortiCare support, customers can be assured that their Fortinet security products are performing optimally and protecting their corporate assets with the best security technology at the best possible price.

Fortinet offers end-users multiple options for FortiCare contracts so that they can obtain the right level of support for their organization's needs. Attractively priced options include 24x7 support with advanced hardware replacement, 8x5 support with enhanced Web features, Premium Support with technical account management, and Premium RMA support with enhanced service levels.

Additionally, Fortinet Professional Services can be engaged for projects with critical deadlines projects that are large in scope, or initial deployments.

# FortiOS 4.0 Software—Raising The Bar

## FortiOS 4.0: Redefining Network Security

FortiOS is the foundation of FortiGate-VM multi-threat security platforms. Developed solely for security, performance, and reliability, it is a purpose-built operating system that in the case of FortiGate Virtual Appliances leverages the power of virtualization.

## Fortinet's Complete Content and Network Protection

The FortiOS purpose-built operating system continues to increase the breadth and depth of security and networking services offered. By adding new functionality and enhancing existing services, FortiOS continues to demonstrate it's the gold standard in multi-threat security.

### 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 (VDOMS)
- 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/SMTPS
- 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 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 (VDOMS)

- Separate Firewall/Routing 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/SMTPS, 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

FortiGate-VM00	500 Mbps
FortiGate-VM01	1.0 Gbps
FortiGate-VM02	1.6 Gbps
FortiGate-VM04	2.0 Gbps
FortiGate-VM08	4.0 Gbps*

## 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

FortiGate-VM00	100 Mbps
FortiGate-VM01	200 Mbps
FortiGate-VM02	350 Mbps
FortiGate-VM04	500 Mbps
FortiGate-VM08	600 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

FortiGate-VM00	200 Mbps
FortiGate-VM01	400 Mbps
FortiGate-VM02	600 Mbps
FortiGate-VM04	800 Mbps
FortiGate-VM08	1.0 Gbps

## 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

	VM00	VM01	VM02	VM04	VM08
IPSec VPN Throughput	100 Mbps	125 Mbps	150 Mbps	175 Mbps	200 Mbps
SSL VPN Throughput	150 Mbps	170 Mbps	300 Mbps	450 Mbps	550 Mbps
Concurrent SSL VPN Users	500	1,500	3,000	10,000	25,000
Recommended (Max)					

## 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 / Default VDOMs:

FortiGate-VM00	1
FortiGate-VM01	10 / 10
FortiGate-VM02	25 / 10
FortiGate-VM04	50 / 10
FortiGate-VM08	250 / 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

- Web-based User Interface
- Command Line Interface (CLI) Over Serial Connection
- Pre-configured Settings from USB Drive

	FortiGate-VM00	FortiGate-VM01	FortiGate-VM02	FortiGate-VM04	FortiGate-VM08
<b>Technical Specifications</b>					
Hypervisors Supported	VMware ESX/ESXi 3.5/4.0/4.1	VMware ESX/ESXi 3.5/4.0/4.1	VMware ESX/ESXi 3.5/4.0/4.1	VMware ESX/ESXi 3.5/4.0/4.1	VMware ESX/ESXi 3.5/4.0/4.1
Max vCPUs Supported	1	1	2	4	8
Max Network Interfaces Supported	10	10	10	10	10
Max VM Memory Support	512 MB	1 GB	3 GB	4 GB	4 GB
VM Memory Required (Minimum)	512 MB	512 MB	512 MB	512 MB	512 MB
VM Storage Required (Minimum)	30 GB	30 GB	30 GB	30 GB	30 GB
<b>System Performance</b>					
Firewall Throughput (UDP packets)	500 Mbps	1.0 Gbps	1.6 Gbps	2.0 Gbps	4.0 Gbps*
IPSec VPN Throughput (AES256+SHA1)	100 Mbps	125 Mbps	150 Mbps	175 Mbps	200 Mbps
IPS Throughput	200 Mbps	400 Mbps	600 Mbps	800 Mbps	1.0 Gbps
Antivirus Throughput	100 Mbps	200 Mbps	350 Mbps	500 Mbps	600 Mbps
Gateway-to-Gateway IPSec VPN Tunnels (System / VDOM)	1,500 / 1,500	6,000 / 3,000	10,000 / 5,000	10,000 / 5,000	10,000 / 5,000
Client-to-Gateway IPSec VPN Tunnels	1,500	3,000	20,000	30,000	64,000
Concurrent Sessions	400,000	600,000	800,000	1.1 Million	1.2 Million
New Sessions/Sec	10,000	20,000	25,000	75,000	100,000
Concurrent SSL-VPN Users (Recommended Max)	500	1,500	3,000	10,000	25,000
SSL VPN Throughput	150 Mbps	170 Mbps	300 Mbps	450 Mbps	550 Mbps
Firewall Policies (VDOM/System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Virtual Domains (Max / Default)	1	10 / 10	25 / 10	50 / 10	250 / 10
Wireless Access Points Controlled	32	256	512	512	1,024
Unlimited User Licenses	Yes	Yes	Yes	Yes	Yes
Available for Order	Yes	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using a Dell PowerEdge R715 server (AMD Opteron Processor 6128 CPU 2 GHz, 4 physical 1 GbE interfaces - 2 in / 2 out) running ESXi v4.1 update 1 with max vRAM assigned to each FortiGate virtual appliance.

Antivirus performance is measured based on HTTP traffic with 32 KB file attachments.

\* Tested on Dell M910 (Intel Xeon Processor E7-4830 CPU 2.13 GHz, 2 physical 10 GbE interfaces) and optimized traffic flow.

Ordering Info	
Product Description	SKU
FortiGate-VM00	FG-VM00
FortiGate-VM01	FG-VM01
FortiGate-VM02	FG-VM02
FortiGate-VM04	FG-VM04
FortiGate-VM08	FG-VM08
Optional Accessories	SKU
Virtual Domain (VDOM) Upgrade License 11-25	FG-VDOM-25
Virtual Domain (VDOM) Upgrade License 26-50	FG-VDOM-50
Virtual Domain (VDOM) Upgrade License 51-100	FG-VDOM-100
Virtual Domain (VDOM) Upgrade License 101-250	FG-VDOM-250
Virtual Domain (VDOM) Upgrade License 11-250	FG-VDOM

## FortiGate Virtual Appliance multi-threat security appliances also include

Multiple Deployment Modes (Transparent/Routing)  
 Advanced Layer-2/3 Routing Capabilities  
 High Availability  
 Virtual Domains (vDOMs)  
 Data Center Traffic Optimization  
 Traffic Shaping and Prioritization  
 WAN Optimization  
 Multiple Device Authentication Options

### MANAGEMENT OPTIONS

Local Web-Based Management Interface  
 Command Line Management Interface (CLI)  
 Local Event Logging  
 Centralized Management (FortiManager Appliance Required)  
 Centralized Event Logging (FortiAnalyzer Appliance Required)

#### 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](http://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 +65-6513-3730  
 Fax +65-6223-6784



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.