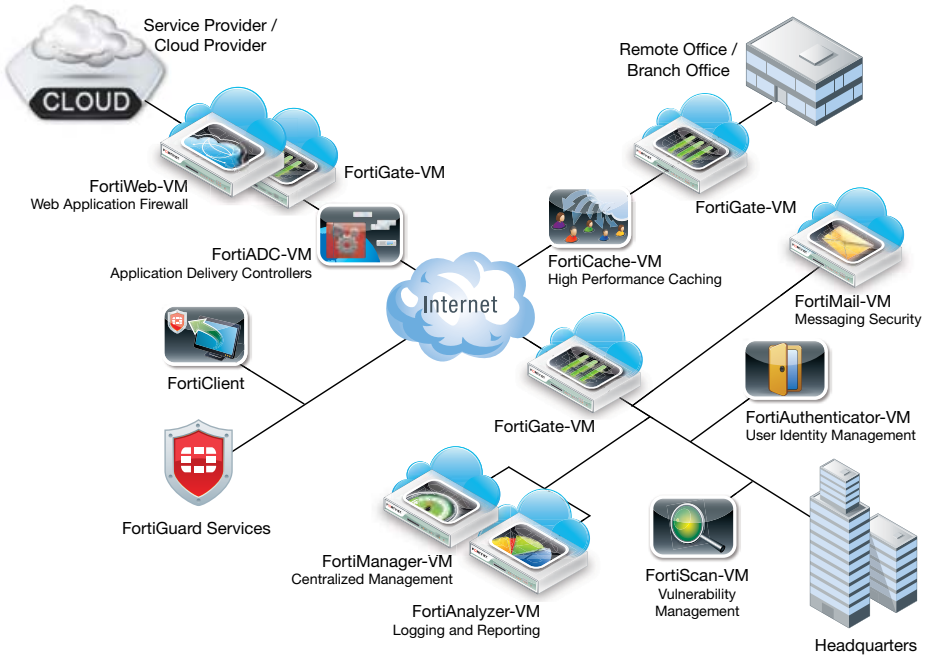
FortiGate® Virtual Appliances

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 (VDOM) 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.



FortiGate Virtual Appliances deployed inside the virtual infrastructure

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
- Support for multiple virtualization platforms

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.

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

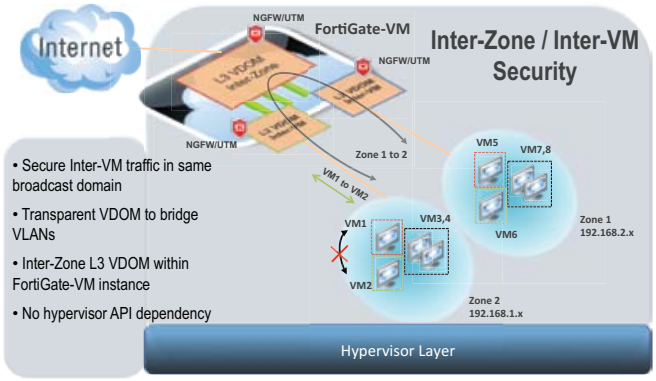
FortiWeb-VM web application firewall
- Protect, balance and accelerate web applications
- Improves security of confidential information and aides PCI compliance

FortiScan-VM vulnerability management
- Provides both active scanning and passive observation
- Identify and analyze unmanaged devices and assets on your network
- Offers remediation recommendations based on available patches and existing workflows

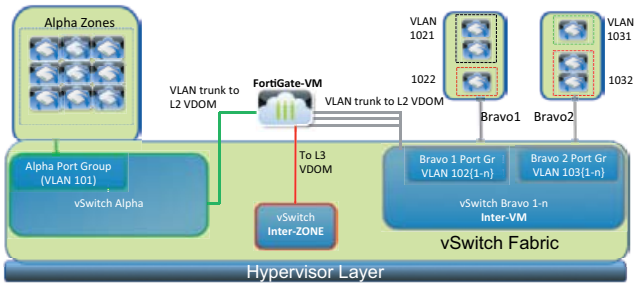
FortiAuthenticator-VM
- Standards-based secure authentication which works in conjunction with FortiTokens to deliver secure two-factor authentication
- Low cost per user and a stackable licensing model

FortiADC-VM
- Intelligent traffic management for optimized application delivery and availability
- Delivers 99.999% uptime for enterprise application services

FortiCache-VM
- Increases network performance and reduced bandwidth costs while minimizing latency
- FortiGuard Web Filtering and antimalware blocks unwanted web content



All Inter-VM traffic in Bravo Zones are subject to full UTM scan through L2 VDOM.
Inter-Zone traffic subject to full Next Gen Firewall and UTM scan by L3 VDOM.
Alpha Zone VMs can all talk to each other freely.



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.

FORTIGUARD SUBSCRIPTION SERVICES						
Product	**Antivirus**	**Intrusion Prevention**	**Web Filtering**	**Antispam**	**Application Control**	**Vulnerability Management**
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 5.0: Redefining Network Security

FortiOS 5, the world's most powerful security operating system, is the foundation for all Fortinet FortiGate integrated security platforms. It provides more security, intelligence and control to help protect enterprises against today's advanced threats and secure dynamic technologies like BYOD.

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.

More Security: Fighting Advanced Threats

- A client reputation feature delivers a cumulative security ranking of each device based on a range of behaviors. It provides specific, actionable information that enables you to identify compromised systems and potential zero-day attacks in real time.
- The new advanced anti-malware detection system adds an on-device behavior-based heuristic engine and cloud-based antimalware services that includes an operating system sandbox and botnet IP reputation database.
- Together with superior industry-validated antimalware signatures, FortiOS 5 delivers unbeatable multi-layered protection against today's sophisticated malware.

More Control: Securing Mobile Devices

- Identify devices and apply specific access policies and security profiles, according to the device type or device group, location and usage.

More Intelligence: Building Smart Policies

- Automatic adjustment of role-based policies for users and guests based on location, data and application profile. Enhanced reporting and analysis provides more intelligence on network behavior, users, devices, applications and threats.

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 is purpose-built for inspection 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

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

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

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

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

VPN

Fortinet VPN technology provides secure communications between multiple networks and hosts, using SSL and IPsec VPN technologies. 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

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

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 clogging 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

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

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

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

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 1,800 Applications
- Traffic Shaping (Per Application)
- Control Popular Apps Regardless of Port or Protocol
- Popular Applications include:
  - AOL-IM
  - ICQ
  - WinNY
  - Yahoo
  - Gnutella
  - Skype
  - MSN
  - BitTorrent
  - eDonkey
  - KaZaa
  - MySpace
  - 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

SPECIFICATIONS

	FORTIGATE-VM00	FORTIGATE-VM01	FORTIGATE-VM02	FORTIGATE-VM04	FORTIGATE-VM08
Technical Specifications					
Hypervisor Support	VMware ESX/ESXi 4.0/4.1/5.0/5.1, Citrix XenServer 5.6 SP2/6.0 or later, Open Source Xen 3.4.3/4.1 or later, Microsoft Hyper-V 2008 R2/2012, KVM				
vCPU Support (Min / Max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Network Interface Support (Min / Max)	2 / 10	2 / 10	2 / 10	2 / 10	2 / 10
Memory Support (Min / Max)	1 GB / 1 GB	1 GB / 2 GB	1 GB / 4 GB	1 GB / 6 GB	1 GB / 12 GB
Storage Support (Min / Max)	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB	30 GB / 2 TB
Wireless Access Points Controlled (Tunnel / Global)	32 / 32	32 / 64	256 / 512	256 / 512	1,024 / 4,096
Virtual Domains (Default / Max)	1	10 / 10	10 / 25	10 / 50	10 / 250
Firewall Policies (VDOM / System)	5,000	20,000 / 40,000	50,000 / 100,000	50,000 / 100,000	50,000 / 100,000
Unlimited User License	Yes	Yes	Yes	Yes	Yes
System Performance (VMware Platform)					
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	400 Mbps	600 Mbps	925 Mbps	1.15 Gbps	1.4 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	500,000	1.0 Million	2.5 Million	3.5 Million	8.0 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
System Performance (Xen Platform)					
Firewall Throughput (UDP packets)	500 Mbps	1.0 Gbps	1.6 Gbps	2.0 Gbps	4.0 Gbps*
IPSec VPN Throughput (AES256+SHA1)	10 Mbps	20 Mbps	30 Mbps	40 Mbps	50 Mbps
IPS Throughput	200 Mbps	400 Mbps	600 Mbps	700 Mbps	800 Mbps
Antivirus Throughput	100 Mbps	200 Mbps	300 Mbps	350 Mbps	400 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	500,000	1 Million	2.5 Million	3.5 Million	8 Million
New Sessions/Sec	10,000	20,000	25,000	65,000	95,000
Concurrent SSL-VPN Users (Recommended Max)	400	1,250	2,500	TBD	TBD
SSL-VPN Throughput	125 Mbps	150 Mbps	250 Mbps	350 Mbps	410 Mbps

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. Testing was conducted on VMware ESXi 4.1 and Citrix XenServer 5.6sp2 virtualization platforms.

ORDER INFORMATION

Description	SKU			
FortiGate-VM00	FG-VM00	FG-VM00-Xen	FG-VM00-KVM	FG-VM00-HV
FortiGate-VM01	FG-VM01	FG-VM01-Xen	FG-VM01-KVM	FG-VM01-HV
FortiGate-VM02	FG-VM02	FG-VM02-Xen	FG-VM02-KVM	FG-VM02-HV
FortiGate-VM04	FG-VM04	FG-VM04-Xen	FG-VM04-KVM	FG-VM04-HV
FortiGate-VM08	FG-VM08	FG-VM08-Xen	FG-VM08-KVM	FG-VM08-HV

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 AvailabilityVirtual 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 Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia Antipolis,
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480