

Fortinet VPN



VPN ACCELERATED

Blended and Multi-Threat Security Protection

Fortinet's family of security products provide a fully integrated and complete solution to detect and eliminate a wide spectrum of attacks and malicious activity including blended threats, intrusion attempts, viruses, trojans, worms, spyware, grayware, adware and denials-of-service. Using network-based ASIC-accelerated hardware platforms, combined with an integrated series of sophisticated Dynamic Threat Protection engines, Fortinet is able to deliver the highest level of multi-threat security and industry-leading performance at a lower total cost of ownership. These security engines, delivered by Fortinet's award winning FortiOS™ can be used separately or together to provide IT administrators with a comprehensive security solution.



Fortinet's ASIC-Based Multi-Threat Security Solutions Deliver Real-Time Performance



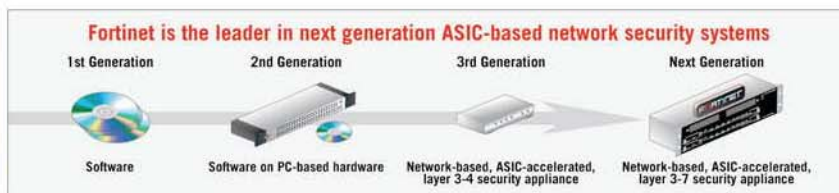
Capabilities Supported by All Advanced FortiGate Security Systems



FortiOS Multi-Threat Security Protection System

Solution

Fortinet's advanced VPN solutions meet the price/performance requirements of any-sized enterprise. Fortinet's VPN offers secure and cost-effective alternatives to expensive, low-bandwidth Frame Relay circuits to connect multiple offices across the public Internet. FortiManager™ centralized VPN management appliance provides the ability to manage thousands of FortiGate systems from a single console. Tightly integrated with Fortinet's application security protection, Firewall, Antivirus, and IPS, Fortinet provides the most secure VPN solution available in the market today.



Key Features

- ASIC accelerated VPN
- IKE: Pre-shared Key, Certs, Manual Keys
- Extensive user authentication, RADIUS, LDAP, Local Database, SecureID, X-Auth support for IPsec Clients
- IPSec, SSL, L2TP and PPTP
- VPN content inspection - Antivirus, IPS, URL Filtering
- Hub-and-spoke configuration
- FIPS 140-2 certified
- Traffic shaping prioritizes traffic across VPNs
- NAT Traversal
- Redundant VPN gateways
- Secure VPN client with integrated antivirus and FW

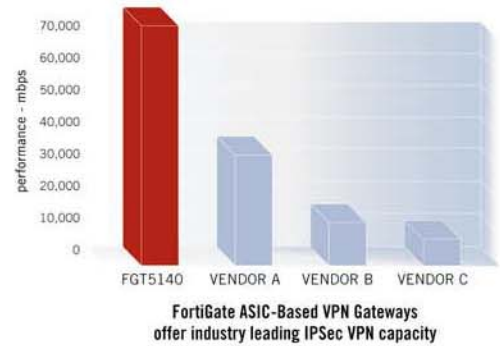


Benefits

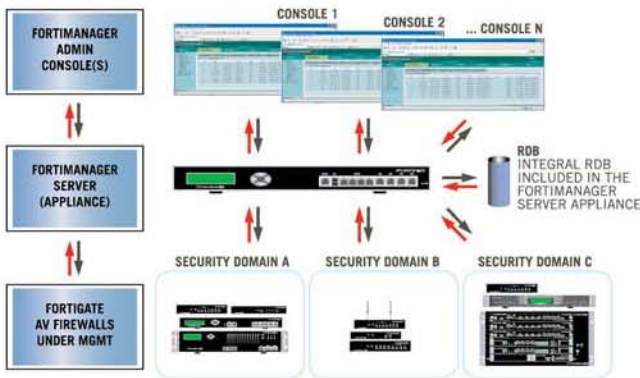
- Industry leading VPN performance scales to gigabit throughputs
- Support for IPsec industry standards
- Flexible user authentication options
- Industry support for multiple VPN standards
- Outbreak containment, prevents malicious content from propagating through a VPN
- Ideal for securing VoIP applications
- Certified for government deployments
- Ideal for VoIP and time critical applications
- Removes the costly need for static IP addresses
- Always available secure VPN tunnels
- Secures roaming users against viruses, tojans and other malware

Centralized VPN Management and Reporting

Fortinet's FortiManager™ system is a turn key, appliance-based central management and monitoring system that enables enterprises and service providers to easily manage thousands of FortiGate™ appliances. Centralized management significantly minimizes the administrative efforts in deploying branch to branch VPN's for large enterprises and managed VPN service providers with it's single console management interface. In addition, the FortiManager system can manage the full range of application security services provided by each FortiGate appliance to establish and maintain consistent and up-to-date security policies across multiple, regionally deployed FortiGate systems.



FORTIMANAGER

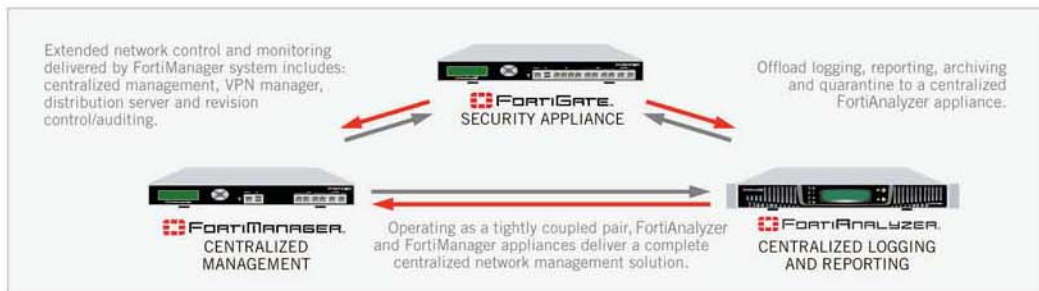


- Automated comprehensive FortiGate management capabilities to centralize VPN and security policy configurations
- Real-time monitoring of all FortiGate network protection functions
- Powerful role-based administration, ideal for Managed VPN Services
- User configurable administrator alerts
- Secure HTTPS-based user interface
- Turn key, out of the box ready FortiManager appliance eases deployment

FortiAnalyzer™

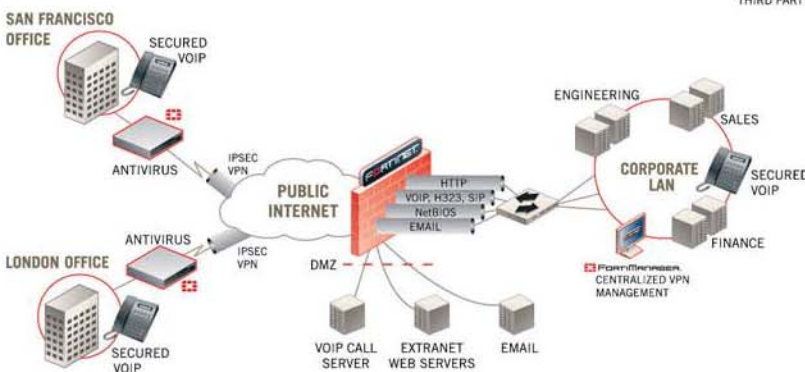
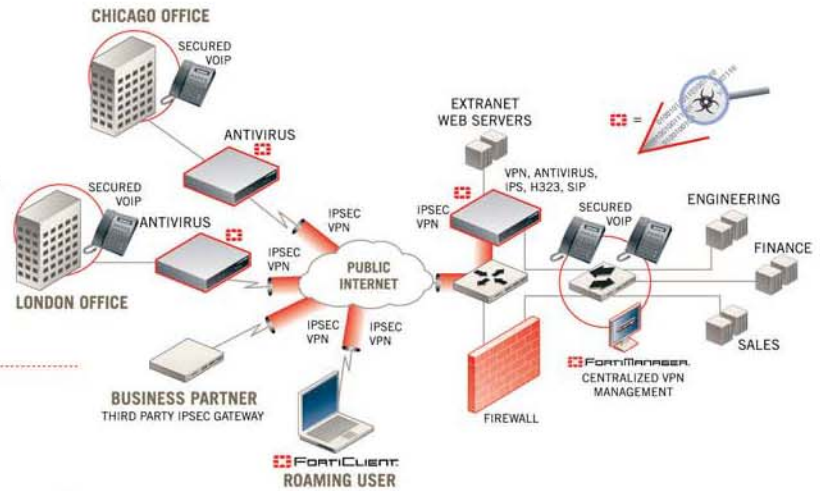
Fortinet's system provides a central logging facility that aggregates and analyzes logs from all centrally-managed FortiGate security systems. The FortiAnalyzer systems provide network administrators a real-time view of network usage and security information. They accept and process a full range of reporting information provided by the FortiGate appliances including VPN status, detected viruses, attacks and real-time traffic logs.

FORTIANALYZER



Enterprise Remote Office and Partner Extranet VPN

Deployed in parallel with an existing firewall, a FortiGate VPN gateway terminates VPNs from branch offices and extranet partners that require limited access to DMZ servers. With the FortiGate systems integrated security features, the administrator can configure granular security policies to control access to resources on the corporate LAN and DMZ.

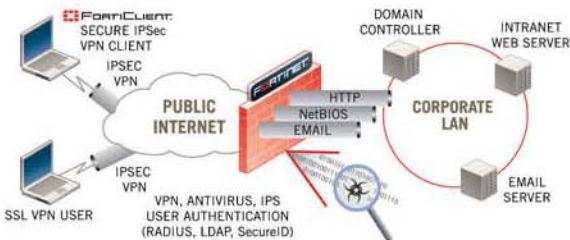
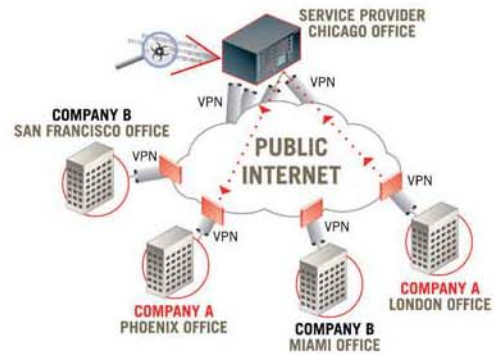


Enterprise Hub-and-Spoke VPN

Hub-and-spoke VPN configurations allow multiple remote sites to connect together without having dedicated tunnels to each site. An ideal application for this design is to transport VoIP traffic across the VPN's to reduce long-distance toll charges. Fortinet's traffic shaping features ensure VoIP traffic receives priority even through a VPN tunnel.

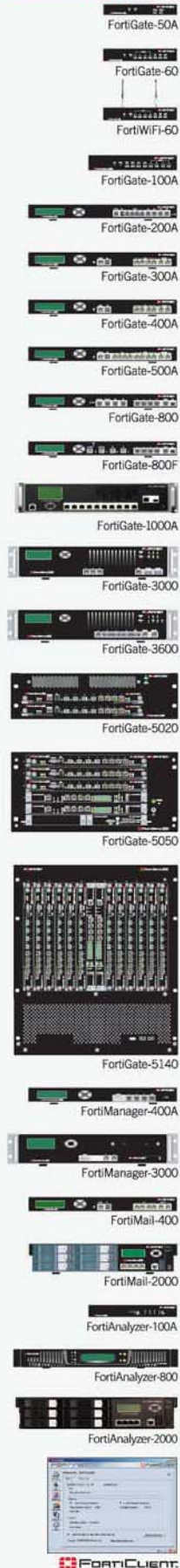
MSSP: Virus-Free Managed VPN Service

Taking advantage of Fortinet's integrated antivirus protection, managed service providers can deliver the industry's most secure VPN service by enabling Fortinet's advanced antivirus engine to block incoming and outgoing VPN traffic that contains viruses, worms, trojans, spyware and other malicious content to prevent virus outbreaks from spreading from office to office. As an added benefit, Fortinet's flexible VPN architecture allows for interoperability with most IPsec VPN gateways. Regardless of the VPN CPE the customer has in place, the FortiGate system deployed at the core will ensure virus-free VPN traffic.



Enterprise Remote Access (IPSec and SSL)

Ideal for roaming users such as remote salespeople needing secure access to resources on the corporate LAN such as email and intranet resources. Fortinet offers both a secure IPsec client (FortiClient™) and clientless SSL VPN for hotspot access in areas where IPsec may be blocked by a firewall. Strong authentication is enforced by the FortiGate VPN gateway to ensure only authorized users can establish VPN sessions.



CUSTOMER SATISFACTION

"By standardizing our managed service offering on the Fortinet platform, we can now offer enhanced security options, more rapid implementation and a lower fee structure for our clients. We are also able to offer even more high-margin services and functionality - unlike previously when we were using software from multiple vendors."

- Michael Bruck, President
BAI Security



FORTINET INCORPORATED
 1090 Kifer Road, Sunnyvale, CA 94086 USA
 Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com/sales

Copyright 2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are registered 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. SOL1020206 Rev2

