Fortinet IPS

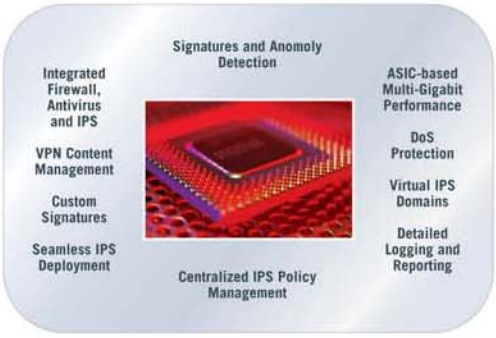
ASIC-BASED IPS Protection

IPS ACCELERATED

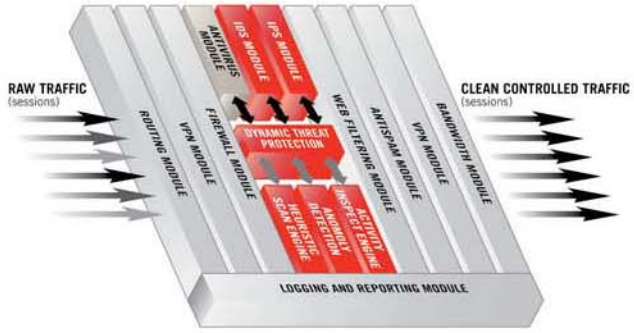
Blended and Multi-Threat Security Protection

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



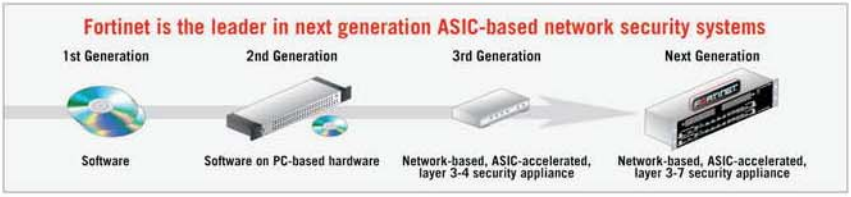
FortiOS Multi-Threat Security Protection System

Solution

Fortinet offers a scalable and easy to deploy line of FortiGate IPS security systems that can be installed seamlessly at the network edge or as an IPS solution deployed at the network core to protect critical business applications from external as well as internal originating attacks. In addition, with Fortinet's SOHO and SME FortiGate models, security administrators are now able to cost-effectively deploy the same level of IPS protection at branch offices that in the past was only available for the corporate headquarters. By tightly integrating industry leading security technologies IPS, Antivirus, Antispam and Stateful Firewall, Fortinet delivers the best-in-class security available for enterprises and service providers to combat the complex blended threats that use multiple methods to infect hosts and self-propagate.

ICSA labs CERTIFIED Intrusion Detection

NSS approved IPS



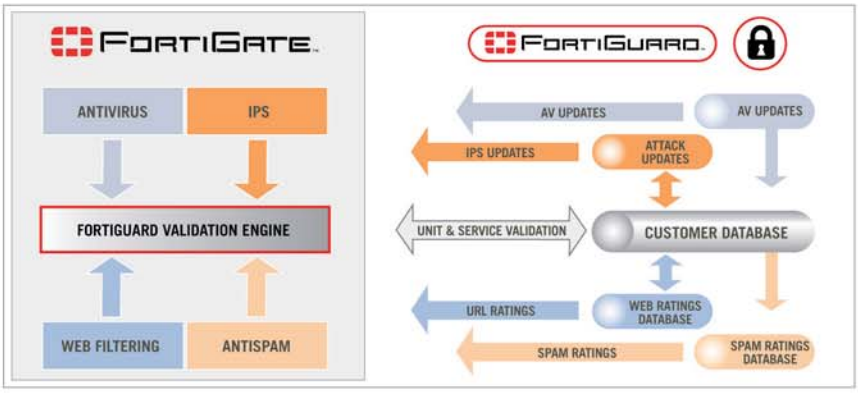
FORTINET MULTI-THREAT SECURITY SOLUTIONS

SCALABLE to Multi-Gigabit Performance

Key Features	Benefits
ASIC-based hardware design	Industry leading price per performance
Automatic updates of IPS signatures	Delivers zero-day protection against the latest attacks
User-defined custom IPS signatures	User friendly, flexible IPS engine
Inspection of VPN (IPSec and SSL) content	Prevents malicious traffic from spreading through VPNs
Bi-directional IPS content filtering	Prevents internal and external attacks
Signature and protocol anomaly engines	Multiple layers of protection against an extensive list of threats
Detailed logging and reporting	Granular logging and reports for internal auditing and traffic analysis
Support for 50+ protocols and applications	Extensive protocol and application protection
Centralized management of thousands of FortiGate systems	Ensures consistent and up to date security policies
Transparent and network tap deployments	Offers seamless deployment with no network redesign
Scalable performance and models from SOHO to multi-gigabit IPS protection	FortiGate models available for any size network

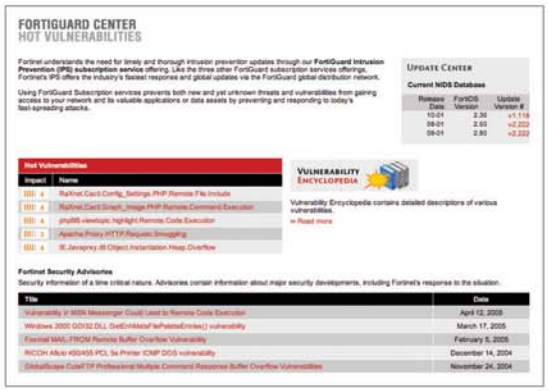
FortiGuard™ Distribution Network

Fortinet's FortiGuard Intrusion Prevention (IPS) service delivers the industry's fastest response to today's fast-spreading attacks. Via the FortiGuard global distribution network, Fortinet's (IPS) service provides automated "push" updates to all FortiGate™ platforms to deliver real-time updates to the IPS signature database and protocol anomaly engines to protect enterprises against the latest exploit attempts and detect suspicious network activity.

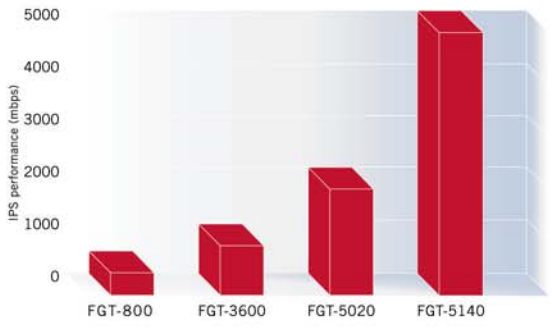


FortiGuard Delivers Industry-Leading Security Services for Real-Time Protection Against the Latest Threats

- **Automated Updates** – Keeps IPS defenses up-to-date providing real-time protection against the latest attacks
- **Industry Leading Threat Response Time** – Fortinet beats the competition in offering signature updates to block the latest attacks
- **Proactive Threat Library** – Fortinet security engineers employed around the globe provide real-time updates to the signature and anomaly databases
- **24x7 Worldwide Coverage** – Over 50 FortiGuard distribution servers are deployed in high speed data centers to provide global IPS updates
- **Online vulnerability encyclopedia** – Provides detailed descriptions on attacks and vulnerabilities



FortiGuard Center
www.fortinet.com/FortiGuardCenter



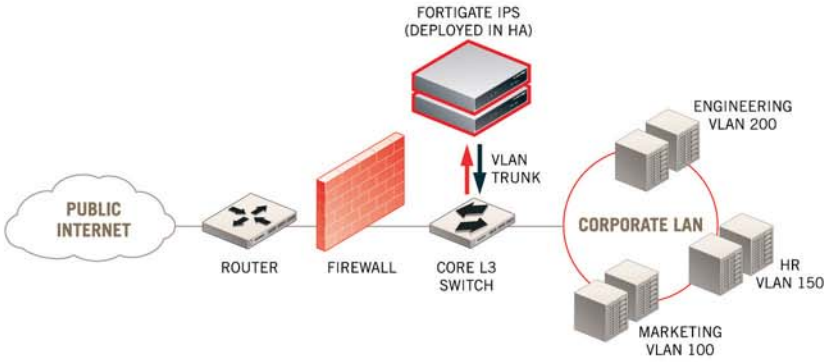
FortiGate IPS Performance by Model (using HTTP, 32k files)

Global IPS Research Team

FortiGuard's IPS service leverages Fortinet's team of worldwide security specialists to produce detection and prevention responses within two hours after recognition of a new attack exploit. Fortinet security specialists work with many of the world's threat monitoring organizations such as CERT and SANS to leverage new vulnerability discoveries, and work to produce signatures, anomaly detection engines and prevention measures to update customers' FortiGate IPS systems before the vulnerability becomes an exploit. FortiGuard's scalable distribution network can push IPS updates to all FortiGate IPS systems within minutes.

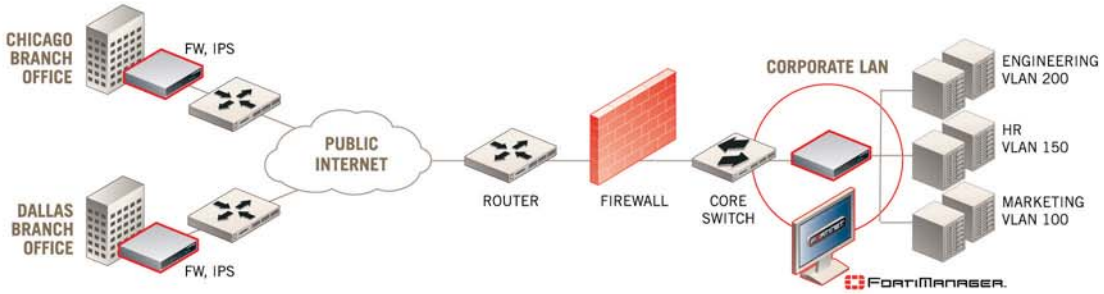
IPS Deployment

Deployed in conjunction with an existing firewall, the FortiGate™ IPS system is deployed in the traffic path inspecting incoming and outgoing packets for malicious and malformed content. The FortiGate system's highly accurate IPS engine and high availability (HA) configuration ensures maximum availability of network resources.



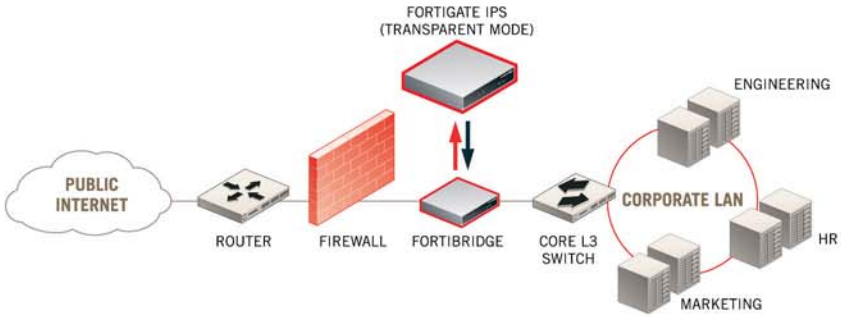
Network Core and Branch Office IPS

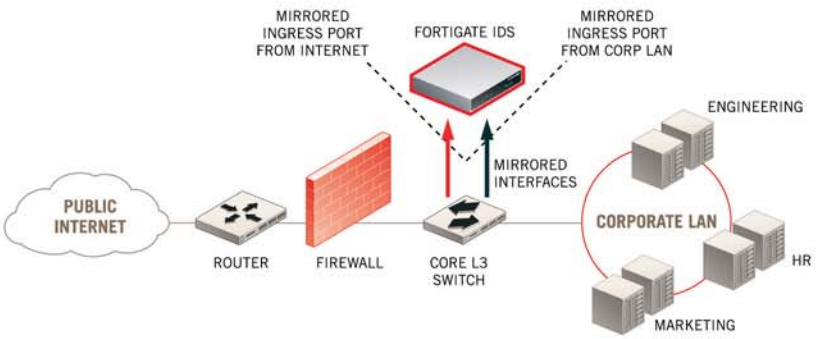
Fortinet's flexible architecture and scalable product line allows for network core deployments to protect against external and internal attacks while the FortiGate system's extensive product line allows security administrators to cost effectively deploy IPS protection to smaller branch offices. FortiManager™ centralized management delivers a single console interface to manage thousands of FortiGate systems.



Enterprise with IPS Bypass

Fortinet's FortiBridge™ option offers enterprises fail-open protection for FortiGate systems deployed inline in transparent mode. The FortiBridge device's zero-power fail open technology means that the FortiBridge unit will also fail open in the event of a complete power failure.





IDS Deployment

For traditional IDS deployments, the FortiGate system's flexible architecture supports monitoring of traffic from a network tap or mirrored interfaces from the core switch. The FortiGate system can generate detailed traffic logs and alerts for analysis and auditing.


FortiGate-50A


FortiGate-60


FortiWiFi-60


FortiGate-100A


FortiGate-200A


FortiGate-300A


FortiGate-400A


FortiGate-500A


FortiGate-800


FortiGate-800F


FortiGate-1000A


FortiGate-3000


FortiGate-3600


FortiGate-5020


FortiGate-5050


FortiGate-5140


FortiManager-400A


FortiManager-3000


FortiMail-400


FortiMail-2000


FortiAnalyzer-100A


FortiAnalyzer-800


FortiAnalyzer-2000

FORTINET
REAL TIME NETWORK PROTECTION

CUSTOMER SATISFACTION

"Securing our customers' VoIP conference calls is a top priority for Polycom and we are excited that our work with Fortinet has enabled secure, real-time UCC calls for our customers."

- Ed Elliot, Sr. Vice President & General Manager
Polycom Video Systems Division

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. SOL1050206 Rev2