FURTINET

SOLUTION GUIDE

Securing Financial Services

Fortinet’s High Performance Technologies and Threat Intelligence Services

Introduction

Financial services institutions are often at the forefront of innovative security initiatives that strive to ensure the integrity and confidentiality systems and data while delivering a competitive advantage. Today's high performance, low latency networks require the most advanced network security solutions to stay abreast of the evolving threat environment.

This paper will describe how Fortinet can provide both protection and competitive advantage with the highest performance, lowest latency next generation firewall in the industry, coupled with on-premise anti-DDoS protection and a dedicated threat research team.

Proven High Speed Security

Fortinet is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying your IT security infrastructure.

Fortinet's purpose-built hardware and software provide industry-leading performance for the most demanding networking environments. We developed our integrated architecture specifically to provide extremely high throughput and exceptionally low latency. Our unique approach minimizes packet processing while accurately scanning the data for threats.

- Custom FortiASIC™ processors deliver the power you need to detect malicious content at multi Gigabit speeds. FortiASIC processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck. The FortiASIC family of purpose-built, high-performance network and content processors work with the latest general-purpose processor to accelerate compute-intensive security services and to provide the performance required to deliver enterprise-class security services at multi-Gigabit speeds.

  Delivering complete content protection in today's high performance multimedia networks requires massive amounts of processing power. FortiASIC processors, using Fortinet's patented Content Pattern Recognition Language (CPRL), have been designed to deliver the highest levels of performance whether providing a single security service like firewall or a combination of security services.

- Fortinet's FortiOS™ security hardened operating system directs the operations of processors and also provides system management functions such as the local web-based interface. FortiOS and the protection services it provides are dynamically updated, via the Fortinet's FortiGuard™ global network, ensuring systems are always protected with the latest security technology.

Other security technologies cannot protect against today's wide range of content- and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap. Competitors that cobble together various OEM software elements delivered on traditional server architectures and networking appliances struggle to deliver the processing power required in order to avoid impacting overall network performance. FortiASIC and FortiOS are purpose-built to deliver the ultra-high performance, flexible scalability and comprehensive security financial service organizations require.

Protecting Virtual Environments

FortiGate virtual appliances allow you to place your security controls adjacent to your critical date, thus mitigating 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. You can deploy a mix of hardware and virtual appliances all enforcing a common set of policies, operating together and managed from a common centralized management platform. Fortinet virtualized appliances deliver the same enterprise-grade features as their physical appliance counterparts in the following product families:

FortiGate

Fortinet’s flagship network security solution. FortiGate devices deliver the broadest range of network security and network services on the market, integrated into a single device. The per-device licensing allows you to deploy as many or as few technologies as you need, including:

- Next Generation Firewall
  - Intrusion Prevention System (IPS)
  - Application Control
  - VPN (SSL & IPsec)
- Web Content Filtering
- Dual-Stack IPv6 Support
- Integrated Wireless Controller
- Antimalware & Antispam
- Layer 2/3 Routing
- WAN Optimization & Web Caching

FortiManager™

“Single pane of glass” management console provides configuration and management of any number of Fortinet devices, from several to thousands, including FortiGate, and FortiAnalyzer physical and virtual appliances, as well as FortiClient™ endpoint security agents. You can further simplify control and management of large deployments by grouping devices and agents into virtual administrative domains (ADOMs).

FortiAnalyzer™

Centralized logging, analyzing, and reporting appliances securely aggregates log data from Fortinet devices and other syslog-compatible devices. A comprehensive suite of easily customized reports enables you to analyze, report, and archive security event, network traffic, Web content, and messaging data to measure your organization’s policy compliance.

FortiMail™

Proven, powerful messaging security platform for any size organization, from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, the FortiMail solution utilizes Fortinet’s years of experience in protecting networks against spam, malware, and other message-borne threats.

FortiWeb™

FortiWeb web application firewalls protect, balance, and accelerate your web applications, databases, and any information exchanged between them. Whether you are protecting applications delivered over a large enterprise, service provider, or cloud-based provider network, FortiWeb appliances will reduce deployment time and simplify security management.

FortiScan™

Enables your organization to close IT compliance gaps and implement continuous monitoring for real-time results. FortiScan provides you with an enterprise-scale solution that integrates endpoint vulnerability management, industry and federal compliance, patch management, remediation, auditing and reporting into a single, unified platform.

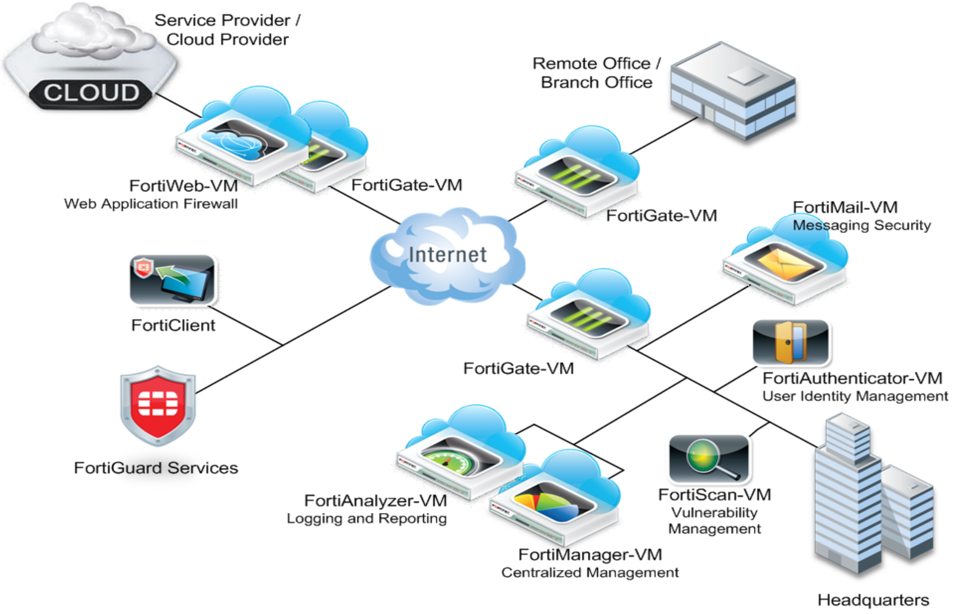

Figure 1 - The Fortinet Virtual Product Portfolio

The Criticality of Low Latency

Network latency, the delay in the movement of data through a network introduced by devices and applications, is an extremely important metric to use when evaluating network security solutions in Financial Services. Even though it should be the goal of any network security solution to have as little effect on network performance as possible, latency has not been a focus for most network security vendors.

For many financial transactions, in particular high-frequency trading, very slight changes in latency can have significant effects on the cost of that transaction. Fortunately, because of its deterministic nature, latency provides a financial services organization with a means to determine the competitive advantage it can achieve by eliminating legacy high-latency security systems.

Fortinet delivers that competitive advantage better than any other security vendor on the market. Because of Fortinet's investment in creating custom ASIC processors that provide switch-like latency for any size data packet, Financial Services customers can experience ultra-low latency while deploying multiple security technologies, such as firewall, intrusion prevention, and application control.

- In a recent NSS Labs group test of leading Intrusion Prevention products, the FortiGate-3140B delivered the lowest latency of any product tested while earning one of the highest protection scores, achieving the prestigious "Recommended" rating from NSS Labs.
- In 2010, one of the four largest financial services organizations in the Eurozone documented a FortiGate device delivering 4X to 10X lower latency than solutions from top competitors a POC using real-world network traffic. Fortinet won the business because of the specific, measurable benefit its technology could provide by reducing latency.

FortiDDoS

The FortiDDoS family of purpose-built network appliances provides effective, innovative on-premise protection against DDoS attacks. FortiDDoS helps you protect your internet-facing infrastructure from threats and service disruptions by surgically removing network and application-layer DDoS attacks. You can defend your critical on-premise and cloud infrastructure from attack while relying on FortiDDoS' sophisticated filtering technologies to allow legitimate traffic to continue to flow and your operations unaffected. These scalable, high-performance appliances deliver proven DDoS defense, and are completely interoperable with your existing security technologies and network infrastructure.

Some of the key features provided by FortiDDoS are:

Virtualized Segments

With FortiDDoS's virtualization feature, policy administrators can establish and oversee up to eight independent policy domains in a single appliance, which prevents attacks delivered in one network segment from impacting other network segments. The virtualization feature also helps to reduce the need for replicated network segments. And virtual instances can also be an effective mechanism in defense escalation. Rather than relying on a single set of policies, IT administrators can define multiple sets in advance, which create the ability to apply a more stringent set of policies if the previous ones happened to be inadequate.

Geolocation

FortiDDoS geolocation technologies allow you to block malicious traffic coming from unknown or suspicious foreign sources. Specifically, FortiDDoS appliances can block traffic based on geolocation through efficient hardware logic, and, when used judiciously, can also be used to reduce load and energy consumption on the backend servers by eliminating traffic from regions outside the organization's geographic footprint and market.

Improved Visibility

Visibility is a key aspect in any DDoS defense strategy. The FortiDDoS product line offers granular visibility and control, so IT administrators have a comprehensive view into the entirety of the network. That same granular visibility into network behavior helps administrators get to the root of the attack's cause and block flood traffic while allowing legitimate traffic to pass freely. It also hands administrators the ability to conduct real-time and historic attack analysis for in-depth forensics. Plus, advanced source tracking will further propel defensive efforts by pinpointing the address of a non-spoofed attack and will even contact the offender's domain administrator.

Bandwidth Control

The FortiDDoS appliances also put control of bandwidth right where it should be—in the hands of IT administrators. Bandwidth management capabilities allow IT administrators to stay on top of policies while predefining usage to customers, employees or contractors. And header and state anomaly prevention technologies ensure a "clean pipe," that allows FortiDDoS to instantly block dark address scans and prevent the outbreak of worms and other stealthy activity. In addition, line-rate granular ACLs power FortiDDoS to protect infrastructure from unwanted traffic in the data center.

FortiGuard Labs Global Threat Research

At the heart of every FortiGate is the FortiGuard global threat research team. Our team of researchers continuously monitors the evolving threat landscape, providing dedicated, continuous analysis of the latest threats. FortiGuard Labs compiles threat statistics and trends based on data voluntarily supplied by many of the more than 750,000 FortiGate network security appliances and intelligence systems in production worldwide.

The team of over 125 FortiGuard Labs researchers also rely on data gleaned from honeypots incorporated in their own intelligence network, complete with servers worldwide, as well as their own custom tools and sensors. From the myriad of unrefined data, they're able to receive and analyze events and create real time detection based off of the gathered intelligence.

FortiGuard Labs provides around the clock coverage to ensure your network stays protected. It delivers rapid product updates and detailed security knowledge, providing protection from new and emerging threats. The FortiGuard distribution network has data centers around the world located in secure, high availability locations that automatically deliver updates to Fortinet security platforms.

The FortiGuard security team continually develops new attack filters to address the latest vulnerabilities and incorporates these filters into heuristic anomaly detection algorithms and security signatures. Updates are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats and sophisticated evasion techniques. The FortiGuard global distribution network delivers these updates to customers several times a day with no user interaction required. This constant updating against both the most prevalent and unexploited threats provides unmatched protection to Fortinet customers.

Conclusion

Fortinet provides the high performance security solutions Financial Services organizations like yours needs need to stay abreast of changes in the threat landscape and ahead of the competition. We deliver protection against attacks targeting applications, systems, and users, including high-volume DDoS attacks, the latest advanced malware, and malicious application-borne content. Our global security intelligence research team provides up-to-date protection against the evolving threat landscape to ensure your systems and data are protected.

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 +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
61 Robinson Road, #09-04 Robinson Centre
Singapore 068893
Tel +65-6513-3730
Fax +65-6223-6784