

# CIO Tips for Beating Security Latency

## Executive Summary

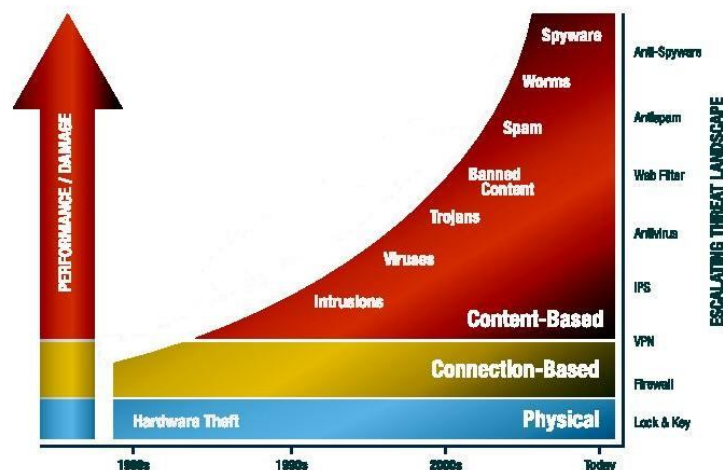
Latency in the transaction processing chain is an important issue for traders affecting financial turnover on a significant scale. Typically contributing over 20% of network delay, security firewalls are now the biggest cause of electronic trading latency. Are you doing enough to mitigate that, and keep your traders profitable against the competition?

Like it or not, every trade must take its turn going through a security firewall. This guide explains why and how you should improve the performance of firewalling within high volume/high frequency trading environments, and aim for reducing firewall latency to sub 3 microseconds.

## Why Security is Essential

### Networks can't just run 'naked'

You know that threats are increasing in volume, severity and complexity. You see this every day as the number of malware incidences continues to grow. The headlines you read are filled with examples of attackers successfully breaching network security systems. The motive and intent for these attacks has moved from notoriety to financial gain.



You have also seen the evolution of cybercrime from relatively simple network-based threats to sophisticated content-level attacks. Seemingly innocuous data traffic now transmits spam, malware, viruses and other types of IT threats. With coordinated and blended attacks now a common practice, security infrastructures need increased intelligence and processing power to counter them.

### Internet-borne threats and financial trading

In February 2010, The Wall Street Journal reported that hackers in Europe and China broke into computers at nearly 2,500 businesses over the previous 18 months in coordinated global attacks exposing vast amounts of personal and corporate secrets to theft. In more than 100 cases, the hackers gained access to corporate servers that stored large quantities of business data, such as company files, databases and online credit card transactions. The spyware used in this attack allowed hackers to control computers remotely.

These coordinated attacks are still happening. If hackers get into a trading environment then they could place unauthorised trades, making significant losses for traders and clients.

In December 2009, The Wall Street Journal reported that the FBI was investigating the theft of tens of millions of dollars when a hacker got into a financial services company's system in New York.

The impact of insecurity goes far beyond the immediate losses to the regulator imposing fines, and an undermining of faith in the business itself. The UK Financial Services Authority (FSA), for instance, is one that has issued multi-million pound fines on businesses for failing to take reasonable care to ensure they had effective systems and controls to manage the risks relating to the security of customer information.

These scenarios highlight the many challenges that trading firms face when trying to prevent data loss or theft. You are expected to reduce the potential of unauthorised access to your data and processing systems when the number of threats is increasing exponentially, and at the same time, ensure high performance and low latency of your trading environment.

## Checkpoints Cause Bottlenecks

### Accepted wisdom #1: work slowly for best accuracy

A critical factor for threat prevention technologies is the accuracy of the analysis. The need to check every single data going through the network takes time - examining all inbound and outbound packets of communications information such as transactions, file transfers, messaging and web communications - and enforcing policies such as forwarding or blocking based on regulatory compliance or corporate policy requirements.

This deep packet inspection and content analysis also takes considerable time and processing power to accurately validate against threat databases and policies. Falsely blocking legitimate messages and business critical applications, and a lack of accuracy in identifying threats can result in negative consequences for the trading community. The need for accuracy and complete content inspection impacts upon firewall latency.

### Accepted wisdom #2: more security means more latency

As the number of transactions and network bandwidth increase, so does your risk profile and the need for larger and faster security. Unfortunately, most firewalls start dropping packets under medium traffic loads and can completely freeze under heavy multicast loads.

In addition, today's complex and blended security threats need to be addressed by multiple security functions, not just IP packet inspection. This has resulted in cumbersome, complex network security architectures being built with multiple appliances providing increased firewall capacity and other devices with multiple security functionality. Multiple point products and security functions, which multiply the stop and search inspection for packets of information transversing your network, only serve to add to the network latency issue, not improve it.

## Don't Ignore the Opportunity: Best Performance Wins

Most traders and data providers have finely honed their market data feeds and their trading execution systems in order to gain a market advantage. In 2008 TABB Group estimated that if a broker's electronic trading platform is 5 milliseconds behind the competition, it could lose at least 1% of its flow. That equated to \$4 million in revenues per millisecond. Up to 10 milliseconds of latency could result in a 10% drop in revenues. Today, latency is more often measured in microseconds ( $\mu\text{s}$ ), with the current impact per  $\mu\text{s}$  commonly accepted by many traders to be \$100,000 per year.

Beefing up your network to compensate for the latency deficiencies is a common response. Network switches have been upgraded to provide gigabit speeds to ensure network traffic is not being squeezed and delayed. Highly accurate network latency monitoring capabilities have been developed and implemented to ensure fine tuning of network performance. However, implementing scaled security solutions to match these high performance networks could end up eating into the performance gains.

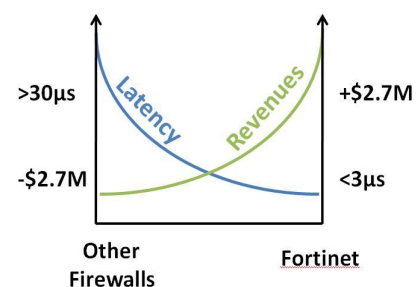
Security firewalls are the biggest cause of electronic trading latency, typically contributing over 20% of network delay. Existing security performance must not be approached as an accepted sacrifice, but heavily scrutinised to ensure you gain a significant latency advantage.

### Choosing a fast and secure solution

To tackle security latency and improve security performance, you must consider a number of areas:

- Hardware-accelerated security processing
- Solutions which minimise packet processing (i.e. repeated IP packet disassembly and reassembly)
- Deployment of fewer network and security elements
- Prioritisation of critical applications
- Continually mapping and monitoring all sources of latency
- Centralised management, analysis and reporting of the security solution for greater visibility and control
- Future proof scalability to the next order of magnitude

Currently, the majority of firewall installations in trading environments involve firewall latencies in excess of 30  $\mu\text{s}$ . Fortinet's FortiGate security appliances can provide a latency as low as 3  $\mu\text{s}$ . Using the trading community's own rule of thumb, then the Fortinet solution's tenfold reduction in existing firewall latency registers a gain valued in excess of \$2.7M per year.



### Hardware and software built for low-latency trading demands

Fortinet's purpose-built hardware and software provides industry-leading performance for the most demanding networking environments. We developed our integrated security architecture specifically to provide extremely high throughput and exceptionally low latency. Our unique approach minimises

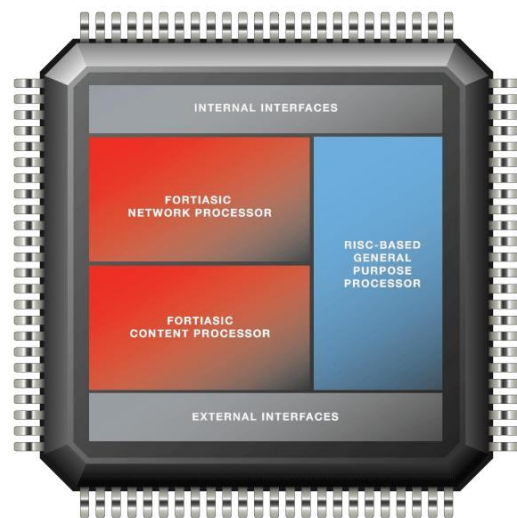
packet processing, eliminating redundant processing by ensuring that traffic is disassembled and re-assembled as few times as possible, while accurately scanning data for threats and enabling complete content protection.

Fortinet's custom FortiASIC™ processors deliver the power you need to detect malicious content at multi-Gigabit speeds via hardware acceleration of the security inspection process. Other security technologies cannot protect against today's wide range of content- and network-based threats because they rely on general-purpose processors, causing a dangerous performance gap. 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.

Fortinet's security firewalls embed three types of FortiASICs:

- 1) NP provides fast processing of routine network security
- 2) CP provides acceleration of security functions to process content, and
- 3) SP provides acceleration for specific security functions like IPv6, multicast routing, IPS, application control and flow anti-virus inspection.

This co-processing hardware works with other general processors to accelerate all security functions in our proprietary FortiOS operating system and contributes to performance scalability.



All the security functions of the FortiOS operating system have been developed on the same source code in order to optimise security performance and eliminate redundant operations related to packet or flow processing. Other security products on the market are unable to do this because security functions have been based upon multiple, disparate source code.

## The Future of Security Latency

We believe the way to deal with the changing threatscape and demanding high performance needs of the trading community is to take a more strategic approach to your application, data and network security. What this means is that you develop a security infrastructure that is able to adapt to the threat evolution whilst also keeping up with changes in the business environment.

If hardware acceleration can be easily recognised as a requirement for maintaining continuity and removing security at the network bottleneck, only the complete integration of specialised hardware, fully integrated software, and original security content can offer the highest levels of efficiency, addressing the issue of security latency. With this approach, integrated network security including application visibility and control within high speed, real time critical networks, is now possible.

## Fortinet Solutions – High Performance – Total Protection

Fortinet is a common feature in many financial trading security infrastructures, driving low-latency initiatives for traders in London, New York and most other major financial centres. Moreover, the size and performance of Fortinet solutions also make them ideally suited to multicast market data environments at some of the world's largest stock exchanges. Fortinet is the only network security vendor which can offer hardware-accelerated packet multicast capability and therefore enable secure, accelerated, zero packet-loss transmission of third party market data feeds to unlimited recipients without compromising security or compliance positions.

Outside of trading, Fortinet is used as a keystone for security strategy at 9 of the top 10 Fortune banking companies. Here, the full extent of Fortinet's multi-threat capability is utilised, from high-end firewalling, IPS, antivirus, content filtering, IPsec & SSL VPN and anti-spam, to comprehensive database and web application protection, as well as unified security for branch office wired/wireless networks, individual PCs and smartphones.

Our security products and subscription services provide integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Third-party certification across all core security technologies validates our consolidated approach, while still meeting the highest standards of performance and accuracy. In today's tough competitive, economic and regulatory environment, it's the most secure investment you can make, with low-latency, control, visibility and ease of management.

Our customers include traders, stock exchanges, banks, enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100.

---

Fortinet® (NASDAQ: FTNT) is a worldwide provider of network security appliances. Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Fortinet's platform delivers low-latency security, control, visibility and ease of management to more than 75,000 customers worldwide. Those include major financial institutions, international telecommunications carriers, government organisations and the majority of the Fortune Global 100. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.



### Global Headquarters

Fortinet Incorporated  
1090 Kifer Road, Sunnyvale, CA 94086  
USA  
Tel: +1 408 235 7700  
Fax: +1 408 235 7737  
[www.fortinet.com](http://www.fortinet.com)

### EMEA Sales Office

Fortinet Incorporated  
120 rue Albert Caquot  
06560 Sophia Antipolis  
France  
Tel: +33 4 8987 0510  
Fax: +33 4 8987 0501

### APAC Sales Office

Fortinet Incorporated  
300 Beach Road #20-01  
The Concourse  
Singapore 199550  
Tel: +65 6513 3730  
Fax: +65 6223 6784