FORTINET

SOLUTION GUIDE

Securing Big Data

Big Data Security impact, challenges and solutions

In the digital age, information is the new currency. And in order to get information, enterprises are mining data – lots of it – for the knowledge that it can yield. Big Data is a broad term for a quantity of raw data (data sets) so large or complex that traditional data processing applications are inadequate.

Data sets grow in size in part because they are increasingly being gath devices, such as mobile and wireless devices, software logs, street cameras, microphones, radio-frequency identification (RFID) readers, the Internet of Things (IoT) and many more sources. The world's technological per-capita capacity to store information has grown significantly with the advance in technology.

On the scale of Internet commerce or social networks, the amount of data can be pretty large - think of the hundreds of millions of smartphones and end-user devices. On the scale of consumer, medical, scientific, or research data, it can be even larger, as sensors and instruments can collect vast amounts of raw data, whether from a single source (such as instrumentation of a GE aircraft engine during a flight) or from the projected 26 billion devices that will make up the Internet of Things.

The Gold Rush that we currently see for collecting and analyzing Big Data, which in turn is increasingly being fed by the Internet of Things, is creating significant challenges for data center networks and their security in four key areas:

Big Data Aggregation

Fact: Increasingly, rather than processing and reducing the raw data at the data source to a more manageable volume, raw data is being transferred and stored centrally – because it now can be – so that it can be analyzed in different ways over time. Today, enterprises are transferring terabytes of data over long distances every day. The sheer quantity of data is forcing core network and data center upgrades, such as 100GbE switching fabric, to deal with individual data transfers at 10Gbps or even higher. Ranked by NSS Labs as having the lowest total cost of ownership per protected-Mbps, the FortiGate 1500D not only gives you the high bandwidth and security your institution needs, it also makes your IT budget go further.

The Challenge: This creates challenges for traditional perimeter security products, such as firewalls, since many vendor solutions are not designed to handle such large inflows and sessions. For example, a firewall that boasts 10 GbE ports or 40 Gbps aggregate throughput may not actually have the internal processing paths to handle an individual 10Gbps flow. LAN congestion from normal enterprise campus traffic may further saturate the CPU or memory resources, causing large flows to stall or even drop.

Fortinet's Solution: FortiGate high performance data center firewalls are based on purpose-built FortiASIC technology that meets the most demanding Big Data performance environments in several aspects:

1. Throughput / latency - ranging from 80 Gbps to over 1T bps / smaller than 7 µs
2. Port density – from six to hundreds of ports per appliance
3. High speed interfaces – support for 10/40/100 Gbps

The FortiGate family of Data Center firewalls provides the range and flexibility to adapt to different sizes and requirements of Big Data and Data Center environments, as outlines in the following table:

	FortiGate-1500D	FortiGate-3700D	FortiGate-3810D
Firewall Throughput	80 Gbps	160 Gbps	320 Gbps
Firewall Latency	3 µs	2 µs	5 µs
Interfaces	8x 10GE SFP+/ GE SFP, 16x GE SFP, 18x GE RJ45	4x 40GE QSFP+, 20x 10GE SFP+/GE SFP, 8x SFP+, 2x GE RJ45	6x 100GE CFP2, 2x GE RJ45

Big Data Processing

Fact: Big data flows are not symmetrical – the raw data that goes in does not necessarily go out in the same form and volume. Instead, the data kept in storage arrays is typically analyzed by an intermediary set of servers and further reduced and delivered as a reduced set of insights before exiting the data center.

The Challenge: What all of this means is that there is a rapidly growing volume of lateral, intra-server traffic , or east-west traffic, which never leaves the data center. Many studies show that east-west traffic now accounts for up more than 70% of data center traffic and is expected to increase even further as the amount of big data analytics continues to increases.
East-west traffic needs to be segmented and inspected, not just for blocking lateral movement of advanced persistent threats and insider attacks, but to secure the data itself, some of which can be sensitive if disclosed or leaked. Network security architectures need to evolve from perimeter or security gateway oriented, to a multi-tiered, hybrid architecture that supports an increasingly virtualized and abstracted environment through the adoption of server and network virtualization and cloud computing.

Fortinet's Solution: In order to provide visibility for east-west traffic and the enforcement of security and segmentation between virtual machines (VMs), Fortinet provides a wide range of virtual appliances, from virtual firewalls, through virtual Web Application Firewall (WAF) to Application Delivery Controller (ADC), that integrate into all major virtualized environments as outlines in the below table:

Virtual Appliance	VMware					Citrix		Open Source		Amazon	Microsoft	
	vSphere v4.0/4.1	vSphere v5.0	vSphere v5.1	vSphere v5.5	vSphere v6.0	Xen Server v5.6 SP2	Xen Server v6.0	Xen	KVM	AWS	Hyper-V 2008 R2	Hyper-V 2012
FortiGate-VM	■	■	■	■	■	■	■	■	■	■	■	■
FortiManager-VM	■	■	■	■	■		■	■	■	■	■	■
FortiAnalyzer-VM	■	■	■	■	■		■	■	■	■	■	■
FortiWeb-VM	■	■	■	■	■		■	■		■		■
FortiMail-VM	■	■	■	■	■		■		■		■	■
FortiAthenticator-VM	■	■	■	■							■	■
FortiADC-VM		■	■	■								
FortiCache-VM	■	■	■	■								
FortiSandbox-VM			■	■								
FortiGate-VMX				■								

Big Data Access & Ownership

Fact: A growing number of companies are using Big Data technology to store and analyze petabytes of data to gain better insights about their customers and their business. As a result, information classification becomes critical and information ownership must be addressed to facilitate any reasonable classification. Enterprises need to identify owners for the outputs of Big Data processes, as well as the raw data. Thus data ownership will be distinct from information ownership – perhaps with IT owning the raw data and business units taking responsibility for the outputs.

The Challenge: With data is being archived for long periods the question must be asked, who is authorized to access which data, and for what purposes? Often there is not just a single data set, but rather multiple repositories of data that may be combined and analyzed together. Each set of data may contain sensitive or confidential information and may be subjected to specific regulations or internal controls. Further, there is often not just one group of analysts or researchers but many different constituents seeking to gain different insights over a long period of time. A large pharmaceutical company provided a good example where their Big Data research efforts were open to not just internal employees, but also to contractors, interns, and visiting scholars. However, a separate analytics sandbox needed to be created for each of them with individual access and auditing rights.

Fortinet's Solution: Fortinet's physical and virtual firewall appliances provides the ability to enforce segmentation to create trust zones and zero trust zones with related security policies so that access and utilization of applications, data sets and analytic data are restricted based on the organization's policies and appropriate national and vertical regulations. Granular identification and permissions can be implemented, managed and enforced with FortiAuthenticator or via the integration of FortiGate with 3rd party identity management solutions.
FortiGate and FortiMail - Fortinet's secure mail gateway appliance - also provide for Data Loss Protection (DLP) so that Big Data information will not be sent out to unauthorized sources.

Big Data and the Cloud

Fact: Only a limited number of organizations are likely to build a Big Data environment entirely in-house, so the Cloud and Big Data will be inextricably linked. However, storing data in the cloud does not alleviate the enterprise's responsibility for protecting it - from both a regulatory and a commercial perspective.

The Challenge: Storing data in the public cloud, which is outside of the organization's security infrastructure, still requires the same type of security mechanisms and policies found in the enterprise network. As cloud providers differ in the scope of the security appliances they allow enterprises to deploy within their network, it is of crucial importance that the cloud provider's security offering meets the enterprise's requirements and provide full protection and segmentation of the stored data.

Fortinet's Solution: Fortinet's wide range of physical appliances, and the industry leading performance they provide, is used by cloud providers to secure their cloud environment. The availability of FortiGate and FortiWeb as virtual appliances available on major cloud providers, such as Amazon Web Services (AWS) and Microsoft Azure, allows enterprises to implement a robust and full security implementation to protect their data stored in the cloud.

Conclusion

IT organizations may need to fundamentally re-think network security instead of taking incremental steps to meet evolving data center security needs. In many cases, data center transformation is happening not just because of Big Data but by cloud computing and SaaS initiatives as well. As part of this transformation, IT should consider an architecture that is:

- High performance – able to support the larger volumes of data with higher network throughput and high-speed ports (e.g. 40G/100G fabric) with high port density, but also be scalable and elastic to accommodate ever-growing data sets.
- Secure – augment perimeter security with increased internal segmentation to secure east-west movement of data and monitor for advanced and insider threats.
- Consolidated – integrate multiple security functions from core security functions like firewalling/VPN, anti-malware and intrusion prevention to advanced threat protection, strong authentication and access control.
- Hybrid – deploy security for data stored in the cloud to enforce an enterprise wide security posture.

Finally, customers may consider Big Data as an opportunity to improve their security posture. With more control and monitoring points being deployed throughout the network and with SIEM (security information and event management) and log management tools to aggregate security logs and event data, more security analytics and insight are possible using big data techniques and tools to better protect both big data and the data center as a whole.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

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

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

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