FORTINET

WHITE PAPER

Data Center Trends And Network Security Impact

Data Center Trends And Network Security Impact

Table of Contents

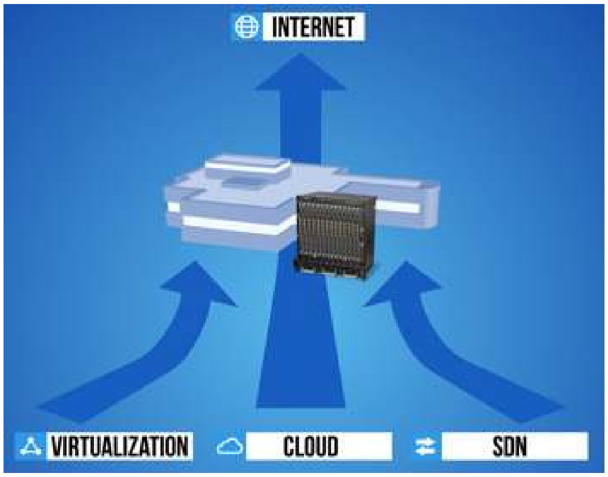
Introduction

The data center is evolving rapidly with new technologies such as virtualization and cloud- computing, and software-defined networks. These have a fundamental effect on how network security is designed and deployed.

This paper gives a high-level overview of key trends shaping the data center and their impact on network security. The paper is divided into the following topic areas:

- Perimeter firewall
- Core network segmentation
- Virtualization
- Cloud computing (infrastructure-as-a-service)
- Software-defined networking (SDN)
- Network Function Virtualization (NFV)

Considerations for enterprises and service providers to select and deploy network security is discussed, as well as Fortinet's approach to delivering solutions in this new era.



Perimeter Firewall

The Perimeter Is Dead…Long Live the Perimeter!

The perimeter is porous. The enterprise is under siege. Web and e-mail are fat pipes for malware. Advanced threats are already inside the network. Users are mobile and bypassing the enterprise network. The perimeter is an M&M - a thin hard shell with a soft chewy interior. The perimeter is dead.

With all the talk of the demise of the perimeter, one would think that the notion of perimeter security is long gone. But to the contrary - in an interconnected world where there are no longer clear boundaries, a solid perimeter firewall is more important than ever. Rather than thinking of the perimeter firewall only as castle wall that must keep all the bad guys out with no defenses inside, today the perimeter firewall is more like a baseball field - a set of boundaries that establish how and where the game will be played. Without a clear set of bases and markings, of outfield and stands, a baseball game would be chaos. The field lets the players establish where they play offense and defense, while keeping unruly fans out on the sidelines.

The firewall thus establishes that clear deny-by-default boundary and the limited paths into the data center, keeping riffraff out while controlling the chaos of what enters. It anchors where additional layers of protection are then applied, whether at ingress/egress points or deeper within the network. The perimeter firewall has not been made obsolete, it has become the baseline (quite literally derived from the paths between the bases of the baseball diamond) that shapes how other security layers are deployed.

Mobile Devices and the Internet of Things

With the proliferation of wireless productivity devices such smartphones and tablets, the number of devices connecting to and accessing applications within the data center is exploding. This is increasing the burden of perimeter security as services are being accessed from anywhere and with greater traffic volume.

Mobile device traffic also may require more emphasis on *small packet performance,* as data center applications are geared more towards smaller screens and smaller bites of information. Some network security solutions achieve their performance specs with larger packet sizes, but can degrade significantly when the traffic shift towards a larger number of users and smaller packet sizes.

IEnsuring Availability in a Service-Centric World

Web-based services accessible from the broader Internet will also increasingly become a target of competitors, activists, and others with a negative or political agenda. Widespread denial-of-service attacks are a highly visible means of disrupting business, and motivated interest groups no longer need to have technical sophistication themselves. Armies of botnets are readily available for rent out for *distributed denial-of-service* (DDoS) attacks from organized hacking groups, as long as those special interests have the means to pay.

As the data center becomes more user-centric, employees and customers will rely increasingly on services to be available on-demand. Enterprises therefore need to ensure their business-critical data center services can maintain accessibility from not just technical contingencies but also from motivated opposition as well.

Takeaways

- Baseline perimeter security
- Small packet performance
- DDoS protection

Product Options

- FortiGate
- FortiDDos

Core Network Segmentation

Moore’s Law and Increasing Speed

Network speeds continue to increase in a relentless Moore’s Law fashion due to the pace of technological innovation. Always-connected mobile devices are accelerating this trend, as are virtualization and cloud computing. While it wouldn’t immediately seem that consolidating servers more efficiently should have any net Impact on the amount of network traffic, these technologies have made it easier for IT teams to provision new servers and quickened business team ability to roll out new projects - leading to real phenomenon such as *VM sprawl* and server containment. Cloud computing further empowers new services to “go viral” seemingly without regard to IT constraints on compute or network bandwidth.

With all this increased connectivity and access from anywhere, it is even more urgent that the internal network be properly segmented to ensure that external threats or improper access does not permeate the data center. At the same time core firewall segmentation must keep up with ever increasing speeds at the network core.

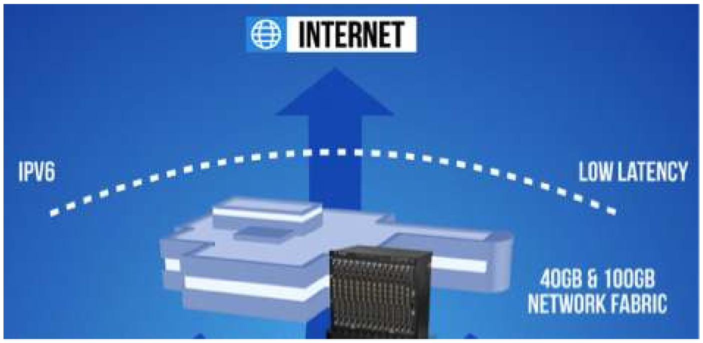
Next-Generation Interfaces - 40GbE and 100GbE

Wasn’t it only just a few years ago that everyone was talking about getting networks ready for 10 Gigabit Ethernet? But things move quickly, and today 40 is the new 10. Indeed, in 2014 already 10GbE will be commonplace with 77% of organizations will be utilizing it in their networks, with 21% adopting 40GbE as well[1], according to a recent study by Network Instruments.

As core network speeds increase, the need for high- speed 40GbE and 100GbE network interfaces and high port density becomes critical, and network security appliances with higher throughput must also efficiently interconnect with high speed network fabric. Infonetics found that with typical firewall throughput requirements in the 100-200Gbps range and Increasing, some businesses are even looking at skipping 40GbE and going straight to 100GbE security appliances, as more core network infrastructure becomes available with 100GbE ports in 2014 and 2015[2].

[1] “Sixth annual state of the network study”, Network Instruments, 2013

[2] “High End Firewall Strategies, Infonetics Research



IPv6 Support

The inevitable march to IPv6 support is already underway in enterprise planning. While the proliferation of mobile devices is not the sole or even primary contributor, certainly it is a stark visual reminder that the world is running out of IP addresses. While enterprises are preparing networks for IPv6 support, not all are scrutinizing *IPv6 forwarding performance* carefully. As traffic migrates to IPv6, there is potential risk that network equipment may not keep at an equivalent rate to IPv4 speeds, causing network bottlenecks. It is therefore important when evaluating new network security devices to ensure that they not only support IPv6 but will also not degrade throughput substantially from IPv4.

Takeaways

- Moore's law increase in network speeds
- High-speed 40/100 GbE interface ports
- IPv6 forwarding performance

Product Options

- FortiGate

Virtualization

It's a Virtual-First World

Virtualization, more specifically x86 server virtualization as popularized by VMware and others, has dramatically transformed the data center in the last decade. What started as workstation technology primarily for testing, development and labs evolved into data center infrastructure for server consolidation - high utilization with efficient capital and operating expenses - and now into a core foundation for cloud computing.

Today the number of virtual servers in the world has long surpassed the number of physical servers, with virtualization not only acceptable in production environments but mission-critical. Enterprises are not just consolidating servers and racks, but often re- architecting entire sites and facilities with *data center consolidation* and transformation in mind and "*virtual- first*" policies – i.e. the planning assumption that any new workloads will be deployed in a virtual machine, and that justification has to be provided for exceptions that need a physical machine.

Mixed Trust Zones

As soon as virtualization moved from test/development into production environments, the issues and concerns on security started early on. Some asserted that there was no change at all in security solutions and security posture when existing workloads went "P2V" (*physical-to-virtual*). Others encountered both architectural concerns and operational issues.

Some of the earliest virtual security discussions were around "*mixed trust zones*", referring to the risk of hosting virtual servers of different data sensitivity or Internet exposure on the same hypervisor instance (physical server host)[3]. Sensitive data ran the risk of being breached should a more exposed virtual server be compromised and the underlying hypervisor VM isolation (thus far exceedingly unlikely in practice) as well.

The PCI Council was heavily involved in these debates, as different servers, such as those storing credit card numbers or other payment card industry data and those without, would normally be kept physically separate by function and segmented by network firewalls, per the PCI Council's Data Security Standards (DSS). Fortunately the PCI Council virtualization Special Interest Group (SIG) working group, in providing guidance for revision 2.0 of the DSS, specifically did not put restrictions on the use of virtualization technology nor mixed trust zones in 2010[4], with the guidelines for the next 3.0 revision maintaining the neutrality of the standards with respect to new technologies, e.g. cloud computing.

However, the use of mixed trust zones can extend the *scope of compliance* audit to additional non-DSS virtual servers, which can increase regulatory and audit costs and efforts.

[2] "High End Firewall Strategies, Infonetics Research, October 2013

[3] "Attacking and Defending Virtual Environments, Burton Group, Pete Lindstrom, 2008

[4] "Securing Virtual Payment Systems", Version 1.0, PCI Security Standards Council, Virtualization Special Interest Group, January 2010