FORTINET

WHITE PAPER

Driving Agility and Security with data center Consolidation

Introduction

Enterprises must become more agile while controlling costs to stay competitive. The true value of IT lies in its ability to make the business better, constantly striving to provide new applications and services that deliver real benefits for the individual and the business.

Data center consolidation is part of an ongoing change process aiming at modernizing an enterprise's IT so that it becomes more rapid and agile itself, thus enabling the wider enterprise to be more agile. In this process, architectures become more flexible and new technologies are deployed to support the rapid introduction and delivery of new applications and services, in a resilient, secure and efficient manner.

With the on-going pressure to do "more with less", data center consolidation provides the following main benefits:

- CAPEX and OPEX reduction
  - Physical data center sites reduction
  - IT staff consolidation
  - Footprint reduction
  - More standardized infrastructure

- Agility
  - Virtualization for compute resources efficiency and agility
  - Advanced technologies such as software-defined networking (SDN)
  - Performance and SLA boost

- Speed
  - Short applications and service deployments cycle
  - Fast time to market

To fulfill the promise of new efficiencies and flexibility, it is imperative that security be an integral part of the design and implementation process of the data center consolidation, to enable a truly SECURE and agile data center.

The Security Aspects of Consolidation Processes

A typical data center consolidation process includes several stages, most of which must take into account security as a key consideration, as illustrated below.

Assessment	Planning	Implementation	Management
• Applications	• Applications	• Applications	• Configuration
• Compute	• Hosts/Virtualization	• Compute	• Monitoring
• Storage	• Storage Architecture	• Storage	• Reporting
• Network	• Network Architecture	• Network	• Analysis
• **Security**	• **Security Architecture**	• **Security**	• **Optimization**

Let's briefly describe the above phases and their security aspects:

1. Assessment

The assessment creates a baseline of the organization's IT assets in terms of: application deployment and usage; compute and storage resources and usage; network architecture and capabilities; security infrastructure and policies; and additional infrastructure and environmental factors (energy, foot print, etc.). This baseline is then used to identify the main gaps to address for achieving the targets of the consolidation process. Similary, from a security perspective, the assessment phase looks at the enterprise's existing security strategy, infrastructure, services, policies and overall security posture and identifies the gaps. This baseline serves as the basis for the next phase of the consolidation process – planning.

2. Planning

The planning phase translates the assessment phase output to create a detailed executable blueprint of the consolidated data center. It provides the opportunity to compare the enterprise needs and objectives - in terms of IT and TCO/ROI - to the above created baseline, in order to identify gaps in terms of resources and assets. Even when a data center consolidation adds no new applications and services, its impact on the underlying resources and infrastructure may be significant. For example, implementing virtualization in the consolidated data center to reduce overall hardware costs and increase agility will require the introduction of virtual-form security appliances in addition to the physical firewalls. This phase will also include reaching out to vendors in RFI, RFP and PoC to understand and choose among the available solutions, the security architecture and services they provide.

3. Implementation

The implementation phase actuates the detailed blueprint defined in the planning phase. This is a critical phase that brings together the different data center domains (applications, compute, storage, network and security) into a live, integrated and functioning ecosystem that serves the enterprise's business objectives and growth. For this highly complex task to complete, the enterprise must rely on the vendor expertise, know-how and guidance in terms of professional services and support.

4. Management

The management phase enables the data center lifecycle. It provides the tools and procedures to monitor, assess and evolve the data center services, SLA and overall functionality in all domains. Management provides a foundation for a planned evolution. For security in a hybrid environment, it is important that the management tools in place provide complete, end-to-end configuration, monitoring, analysis and reporting capabilities.

From a security perspective, the most significant phase is the planning phase. This is the phase during which the actual security needs, architecture and policies will be defined for implementation. To better understand the key security considerations during this major phase, we need to look at the different levels of change a consolidation process may encompass, as outlined below:

1. Physical Sites Consolidation

Enterprises and service providers are consolidating multiple data center sites to achieve cost reduction, increase operational efficiency, control and management. A consolidated data center is characterized by:

1. Increased Application Range – although not always the case, the consolidated data center may have a higher "density" and variety of applications. For example, the consolidation of internal and customer-facing applications and services may bring together, within a single data center, new types of applications, such as web applications, user portal, email, CRM and ERP.

From a security point of view, consideration must be given to the entire set of applications and their users in order to implement suitable security solutions and policies that will protect the entire application fleet and the users' access and usage rights. Therefore, the data center firewalls deployed must include a rich feature set such as AntiVirus, Intrusion Prevention, Application Control and IP Reputation.

2. Increased Data Traffic Volume – with more applications and users accessing them, traffic is greatly increased in terms of sheer volume, sessions, SSL encrypted traffic and IPsec VPNs.

The applied security solutions and infrastructure must provide the required security services with elastic performance attributes that will meet current and future needs in terms of throughput, interface speeds, new and concurrent sessions and IPsec VPNs. To ensure secure SSL transactions performance and user's Quality of Experience (QoE), consideration should be given to offloading CPU extensive SSL encryption from the application level to specific ASIC-based solutions as part of the overall application delivery infrastructure in place.

3. Increased Interface Speed and Density – with higher traffic volumes comes the need to use faster local area networks within the consolidated data center: 10/40/100Gbps Ethernet infrastructure may be required to meet the growing traffic volumes. Also, more applications, users and user groups will cause an increase in the number of physical network segments and Virtual LANs (VLANs).

From a security point of view, the data center firewalls, must be able to cater to both the interface speeds and their physical and virtual density in a scalable fashion and without becoming a potential network bottleneck.

2. Virtualization

Compute, storage and network virtualization is implemented to achieve high levels of agility and efficient resource utilization. Although the level of data center virtualization will vary, it is safe to note that compute virtualization has its lion's share within the data center: virtualization has surpassed 50% of all data center server workloads and should reach 86% in 2016, according to Gartner. Virtualization is the core foundation for cloud computing and services.

With many organizations applying "virtual first" policies in their data center – i.e. the planning assumption that any new workload will be deployed in a virtual machine - consideration must be given to securing the data center virtual environment:

1. East-West Traffic Visibility - with compute virtualization, multiple virtual machine (VM) instances share the compute resources of a physical host. This leads to a change in data traffic patterns where three quarters of data center traffic is between VMs and remains within the physical host. This traffic is known as East-West traffic, compared to North-South traffic, which enters and exits the hosts onto the physical domain.

The virtual environment creates a very challenging environment for traditional hardware security appliances, such as firewalls and Web Application Firewalls (WAF) as they have no visibility of East-West traffic and therefore, cannot protect and enforce the relevant security policies. This creates a security posture gap within the data center as East-West traffic, and as a result the data center itself is not protected against malicious and non-malicious threats such as viruses, application misbehavior, configuration mistakes, etc.

It is therefore crucial that virtual firewalls and specialized security solutions, such as WAFs, are integrated as VMs within the hosts making up the virtual compute environment. Virtual security appliances provide visibility into East-West traffic, enable segmentation to protect critical assets, eliminate security gaps within the data center and enable an overall unified security posture. These must provide the same level of functionality as hardware-based firewalls and other security appliances as similar threats lurk in both the physical and virtual domains.

2. Catch Me if You Can – agility is THE benefit provided by compute virtualization in the data center and the cloud:

- VMs and new workloads can be created within minutes instead of days and hours.
- Application & service availability is increased with session statefulness during live migrations.
- New workloads and services can be created and torn down on-demand.
- Workloads can be suspended and resumed from snapshots on different VMs.

Virtual firewalls and other security appliances need to follow this constant evolution of workloads and virtual machines to maintain the security policies defined and avoid potential security gaps created by a misalignment of workloads and security enforcement. This can be achieved through a:

- **Well-defined procedure aligning applications, workloads and virtual machines** with the appropriate security policies that must be put in place and the service enforcement point. For example, deployment of a web-facing application required the security services of a Web Application Firewall (WAF) that will be provided by a virtual WAF instance on the applications' host.

- **Tight integration with the virtual environment** to allow the automation of security policies deployment for new and changing workloads, at both deployment and enforcement levels. For example, in case of a VMware's vSphere vMotion, the virtual enforcement point will be automatically created on the target host machine and the defined policies enforced for the workloads.

- **Security automation in such an environment** can also be achieved via the integration within frameworks such as software-defined security and Cloud Management, such as OpenStack.

3. Scale-Out and Scale-Up – with the consolidated data center, both virtual and physical security appliances coexist.

Physical appliances, such as data center edge and core firewalls are required to define the data center boundaries; enforce access policies; provide segmentation; and protect against outside threats such Advanced Persistent Threats (APT), malware, viruses, DDoS attacks, malicious web sites, etc. Physical appliances have the hardware technology that allows them to deal with the ever-growing volumes of traffic entering, exiting and traversing the data center, without becoming a bottleneck or suffering from major service degradation. They basically enable security scale-up.

Virtual appliances complement the physical security infrastructure by providing west-east traffic visibility and security policies enforcement within the virtualized/cloud environment. They provide a full set of security services, micro segmentation between workloads, enables regulatory compliance and security agility. They enable security scale-out.

4. Single pane of management - to avoid gaps in data center security posture, a single pane of management, providing unified provisioning, management and reporting across the physical and virtual security domains is crucial.

3. Cloud Services

Even within the consolidated data center, new hosts, storage, virtualization platforms, hardware and virtual security infrastructure and other components must be deployed to support growth and new applications and services. These all involve additional CAPEX, OPEX and time.

To achieve even higher agility and cost reduction, enterprises look outside their private data center/cloud for solutions. With the availability and maturity of cloud service providers, enterprises are consuming a multitude of cloud services, such as:

- Infrastructure-as-a-Service (IaaS) – allows the consumption as a service of virtual machines and other resources, such as virtual firewalls. This may provide agility and elastic growth with lower associated costs as there is no CAPEX and the service can be consumed and terminated on demand according to the enterprise's needs. Amazon Web Services (AWS) is an example of an IaaS provider.

- Platform-as-a-Service (PaaS) – allows the consumption as a service of a complete computing platform, including OS, DB, web server, etc. This model provides cost reduction as developers can develop and run their applications without the associated CAPEX and OPEX of buying and managing the underlying hardware. Microsoft Azur is an example of a PaaS provider.

- Software-as-a-Service (SaaS) – allows the consumption as a service of applications and their databases, such as SalesForce, without the CAPEX and OPEX associated with the infrastructure required to run and maintain the applications.

The consumption of cloud services extends the enterprise's data center and private cloud and creates a hybrid environment - the hybrid cloud - where some of the enterprise data center assets are located and consumed outside the physical data center boundaries. Yet, from a security consideration, the hybrid cloud must maintain the same security posture and enforce the same enterprise security policies as in the private cloud:

- With the PaaS and SaaS models, security is handled and guaranteed by the service provider and the enterprise should make sure they meet its security requirements.

- With the IaaS model, the enterprise can lease the required security virtual appliance and services and have complete provisioning, management and reporting access. In this case, utilizing the same security virtual appliances as used in the enterprise's private cloud presents significant benefits as they share the same management, provisioning and reporting already known by the enterprise.

Building a data center Protective Ecosystem

The data center combine with private and hybrid clouds serve as the beating heart of enterprise IT. Not only does it provide the compute, data storage and applications required for the enterprise's most basic internal operations, it also enables its interaction and transaction with the overall external ecosystem – be it partners, suppliers or customers. As such, the data center is the prime target for cyber-attacks and must be equipped with appropriate security to provide continued effective defenses against an ever-changing threat landscape.

Effective data center security cannot consist in a single product or technology. Both the evolution and complexity of the data center itself and the threat landscape will not permit it. Instead, data center security should be thought of and implemented as an adaptive ecosystem, combined of specific solutions that, integrated together, provide the widest possible protective umbrella. Such ecosystem should be based on the following major premises:

- **Adaptive** – to the changing threat landscape via automatic threat intelligence update services that maintain the security ecosystem up to date with new and evolving threats

- **From Network to Application** – from network level attacks, such as volumetric DDoS attacks, to specific application level attacks, such as Cross Site Scripting (XSS) attacks or phishing emails, the ecosystem must provide a complete end-to-end security at all levels

- **Agile and Automated** – in order to not limit the agility and automation offered by virtualization in the private cloud, the security ecosystem should integrate within the data center virtualized (hypervisor) and SDN environments

- **Data center-Grade** – a data center security ecosystem must be able to stay effective in a high-volume, high-performance and low-latency environment without becoming a bottleneck or a point of service degradation.

Fortinet's Security Ecosystem for the Consolidated data center

Via a complete end-to-end security ecosystem for the data center, Fortinet enables and facilitates the enterprise's journey through the data center consolidation process. The delivery of both physical and virtual planes security appliances it offers on one side, and the unmatched performance and security capabilities it provides on the other side, allow the growth and evolution of the consolidating data center with no service degradation or bottlenecks, no compromise on security, and with an unmatched ROI:

- Fortinet's Security Fabric integrates adaptive technologies for the endpoint, access layer, network, applications, data center, content, and cloud into a single collaborative security solution that can be orchestrated through a single management interface.

- Fortinet securely and elastically *scales* protection to private, public and hybrid cloud infrastructure and workloads, and *segments* both within the cloud and between endpoints, enterprise networks, and the cloud.

- From network-level attacks, such as volumetric DDoS attacks, to specific application-level attacks, such as Cross Site Scripting (XSS) attacks or phishing emails, Fortinet's security ecosystem provides a complete **end-to-end security at all levels**:

  1. FortiGate for segmentation, FW, AntiVirus, IPS, Application Control, Web filtering, NGFW, etc.
  2. FortiDDoS for network and application level DDoS mitigation
  3. FortiWeb for Web Application Firewall (WAF)
  4. FortiMail for secured mail gateway
  5. FortiADC for application delivery assurance and SSL offloading
  6. FortiSandbox for breach detection and Advanced Threat Protection (ATP)

- Via a wide range of data center virtual appliances and Virtual Domains (VDOMs), Fortinet's solutions integrate within the Data Center virtualized (hypervisor) and SDN environments, offering a wide range of security services with the **agility & automation required**, as demonstrated in the below table:

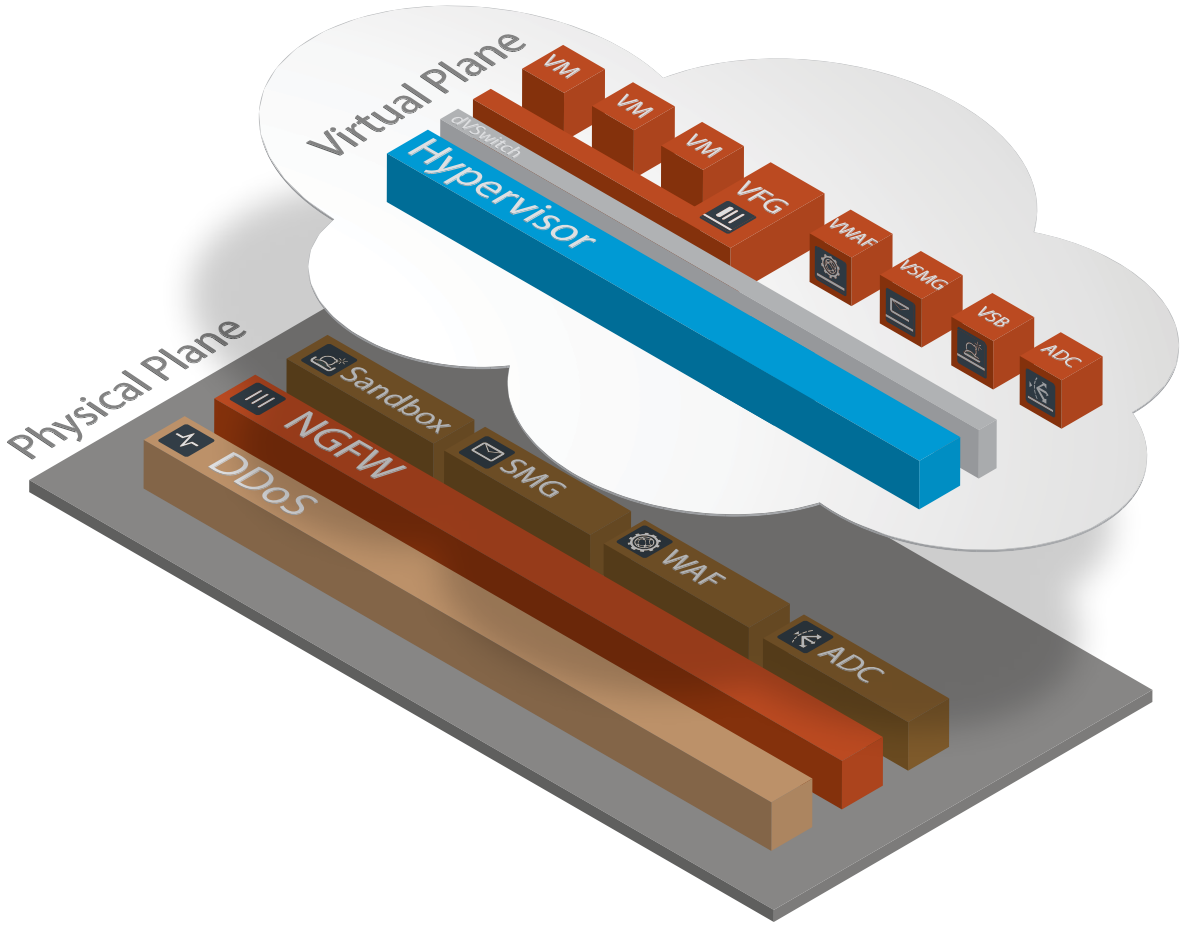
Virtual Appliance	VMware				Citrix		Open Source		Amazon	Microsoft	
	vSphere v4.0/4.1	vSphere v5.0	vSphere v5.1	vSphere v5.5	Xen Server v5.6 SP2	Xen Server v6.0	Xen	KVM	AWS	Hyper-V 2008 R2	Hyper-V 2012
FortiGate-VM	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
FortiManager-VM	✔	✔	✔	✔					✔	✔	✔
FortiAnalyzer-VM	✔	✔	✔	✔					✔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

- Fortinet security appliances provide high availability and are based on purpose-built FortiASIC technology that meets the most demanding data center-grade performance 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 – 10/40/100 Gbps

- Single-pane-of-glass Management: With FortiManager and FortiAnalyzer, central management, reporting and analysis are provided for both hardware based and virtual security appliances.

The below illustration describes the Fortinet ecosystem, encompassing the data center physical and virtual planes:



Physical Plane

Although many security functions can, and sometimes must, be implemented at the virtual plane level, physical security appliances at the physical plane level must still be implemented, as described in the following examples:

1. DDoS protection (FortiDDoS) must be provided at the physical network layer to protect from network- and application-level DDoS attacks. Trying to implement DDoS protection at the virtual plane only will leave the data center vulnerable to these types of attacks coming connected networks, such as the Internet and the organization's extranet.

2. Next-generation edge and core data center firewalling (FortiGate) must also be implemented at the data center physical plane due to following main reasons:

   A. Non-virtualized asset protection – in most cases, data centers are not 100% virtualized. Therefore, the non-virtualized compute and storage assets must be protected against the largest possible set of attacks, which will be provided by a FortiGate NGFW.

   B. Physical segmentation – Operational considerations and the need to comply with different data privacy and protection regulations (such as HIPPA and PCI) requires the creation of trusted security zones segmented by a firewall. As long as these sensitive assets and the trusted security zones are also implemented in the physical plane, a physical FortiGate firewall is required to enforce their segmentation and protection.

   C. Hypervisor protection – when no physical firewall is enforcing security at the physical plane, the hypervisor itself becomes potentially vulnerable to attacks. This is due to the fact that only after traversing the hypervisor, the virtual firewalls have data visibility. This is a very dangerous security loop hole that must be avoided by implementing a physical FortiGate as a NGFW at the data center's edge.

   D. Performance – security in the consolidated data center needs to deliver a rich set of security services for an ever-growing volume of data. To do so without becoming a bottleneck, data center security appliances must provide the appropriate level of performance (such as throughput, session scalability, delay, etc.). While such performance levels can be easily provided by a physical FortiGate appliance, meeting them by just adding virtual security appliances for a greater aggregated security performance may prove to be difficult from both a cost perspective and a management complexity perspective.

Physical security appliances (DDoS protection and NGFW) at the data center's physical plane are a must for an effective and complete protection. Some of the purpose-built security appliances, such as Secure Mail Gateway (SMG – FortiMail), Web Application Firewall (WAF – FortiWeb), Application Delivery Controller (ADC – FortiADC) and sandboxing (FotiSandbox), may be implemented as virtual appliances, based on specific considerations such as performance, cost and services provided.

Virtual Plane

At the data center virtual plane, Fortinet provides a rich set of virtual appliances, which are provided as standard virtual machines (VMs) on top of a virtual switch and hypervisor, and can therefore take benefit of the agility and flexibility provided.

In a VMware environment, Fortinet's FortiGate-VMX provides a kernel level integration so that every VM in a host can be provided with a complete NGFW segmentation and protection. FortiGate-VMX is VMware NSX compatible, which allows automated and dynamic workload security enforcement in the SDN Software Defined data center (SDDC).

Fortinet security operating system, FortiOS, is common to both virtual and physical security appliances. Therefore, the same rich set of security services and capabilities are available on both planes, eliminating possible security gaps and providing a full set of security services for today's and future threats.

Summary

Fortinet's security ecosystem supports and facilitates the deployment of a complete end-to-end security solution for the consolidated data center. It encompasses physical and virtual security appliances for modern data center's physical and virtual planes, providing the performance, agility, compliancy and cost effectiveness required by these high-performance and dynamic environments.

With FortiManager and FortiAnalyzer, centralized device management and event logging and analysis, security management in the data center is enabled and facilitated.

Regardless of the evolution of your data center and the stage of your consolidation process, Fortinet provides you with the solutions, expertise and know how to ensure optimal security.

www.fortinet.com

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

EMEA SALES OFFICE
905, rue Albert Einstein
06560, Valbonne
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