IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

Infrastructure Virtualization Security Architecture Specification for Private Cloud

S.S.Manikandasaran[1*], K. Balaji[2], S. Raja[3]

[1*]Department of Computer Applications, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India.
[2]Department of Computer Science, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India.
[3]Department of Computer Science, Christhu Raj College, Tiruchirappalli, Tamil Nadu, India.
Corresponding Author: balajjee.mecse@gmail.com, Tel : +91 9444341921

Available online at: www.ijcseonline.org

Abstract—This Infrastructure Virtualization has been in place at industry for several years, and most recently new business drivers and rapid advances technology are taking virtualization a step further. While major drivers in the past have been around cost savings via server consolidation, Public cloud and software defined datacenter and business agility has become one of the key components in overall infrastructure. This paper provides a security architecture specification for infrastructure virtualization for private cloud which includes Threat analysis, vulnerabilities, Security architecture requirements and Security architecture specifications.

Keywords— *Security architecture; Infrastructure virtualization; Threat; Vulnerabilities;*

I. INTRODUCTION

In Cloud computing, Infrastructure virtualization is the process of implementing various infrastructure resources at logical level. Computing resources like Compute, Network, Storage and End-User/Desktop devices may be virtualized by leveraging technologies that enable the logical implementation of those infrastructures [1]. As an example, a virtual machine/server includes virtualized memory, virtual CPU, virtual storage and virtual network connectivity. Since that's virtual representation/implementation of those resources the virtualization technology is responsible for mapping the virtualized infrastructure over to the physical infrastructure. While is understood that, eventually, specific network security controls also virtualized under the hypervisor (firewalls, etc.). Network firewalls have already been virtualized within specialized and dedicated appliances [2].

A. Conceptual view of virtualized Infrastructure.

A cloud provides virtual machine it allows software run on a computer like a system, operating system, and individual applications. The hypervisor runs on a virtual machine for serving as a platform and computes the resources. The VM provides own virtual environment for software, hardware, virtual CPU, memory, hard disk and network interface card. The hypervisor installed on the physical hardware and it acts as virtualized software in all cloud data centers and acts as a platform for the virtual machine. The virtual machine supports the entire computations with standalone physical hardware [3]. Figure 1 represents conceptual view of virtualized infrastructure in cloud environment.

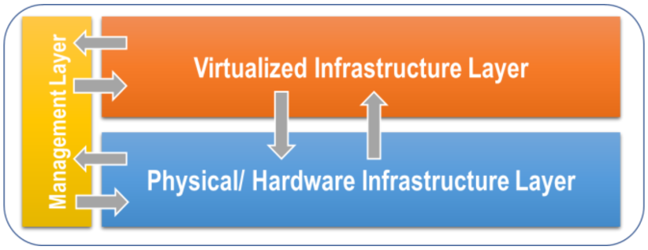
Management Layer
Virtualized Infrastructure Layer
Physical/ Hardware Infrastructure Layer

Fig. 1. Conceptual view of virtualized infrastructure

- ➢ ***Physical/Hardware Infrastructure***: This layer provides the compute, network, storage and end-user devices assets at the hardware level.

- ➢ ***Virtualized infrastructure***: This layer provides virtualization environments, such as the virtualized compute, virtualized networks, virtualized storage and virtualized desktops. This abstraction level is accomplished software components that connect to the hardware resources, and ensure that virtualized resources are exposed to the applications. From a compute perspective that realized via a hypervisor, which presents a kernel that provides device drivers (storage, network), resource scheduling, API for interfacing with management tools etc.

- ➢ ***Management***: This layer provides the management capabilities for orchestrating provisioning of infrastructure resource (hardware and/or virtualized), as well as management of overall infrastructure environment.

B. Virtualized Infrastructure Model

Figure 2 represents the virtualized infrastructure model of cloud computing environment.

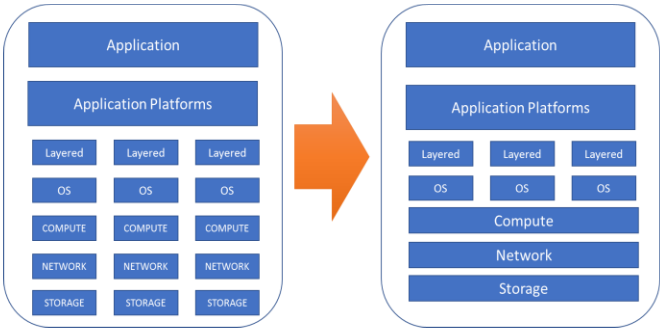

Fig. 2. Virtualized Infrastructure Model

➢ ***Compute***: Compute is fundamental component in infrastructure which does processing the workloads. In traditional, it named as server and it comprises of CPU, memory and I/O resources. It possible to virtualize these resources and shared with multiple parties. It is the core component to build virtual machine.

➢ ***Network***: Network is communication layer between compute components and it is tightly coupled with other infrastructure layer components. This also can be virtualized and mapped to the server with through vNIC (Virtual Network Interface Card) adapters.

➢ ***Storage***: Storage is collection of disks resides in storage array. Storage component perspective, storage rely on a dedicated pair of SAN (Storage area network) switch, which deliver fibre channel connectivity towards the rest of virtualized infrastructure. SAN switches support fibre channel by encapsulating it within Ethernet frames (FCOE - Fibre channel over ethernet) before deliver to the servers.

C. Management view of integrated components

Define The Management Layer for the virtualized infrastructure is comprised of an overall unified infrastructure framework. That allows for one single interface to interact with the various element (component) managers, it happens overall management across all infrastructure component. Management layer is the main component which called as orchestration layer to take care of provisioning and configuration of infrastructure services in private cloud.

Orchestration provides the following functionalities in Nutshell:

- Discovery and provisioning of components (Compute, storage and networks) as a single entity.
- Definition of infrastructure services to automate provisioning, build hypervisor clusters and manage provisioning resources and change.
- Management of virtualized infrastructure resources and resources allocation.
- Access to the devices for configurations, and changes.

In Infrastructure virtualization, Compute will transform into hypervisor which is pillar of any cloud computing service model [4]. The Hypervisor comprises two types they are:

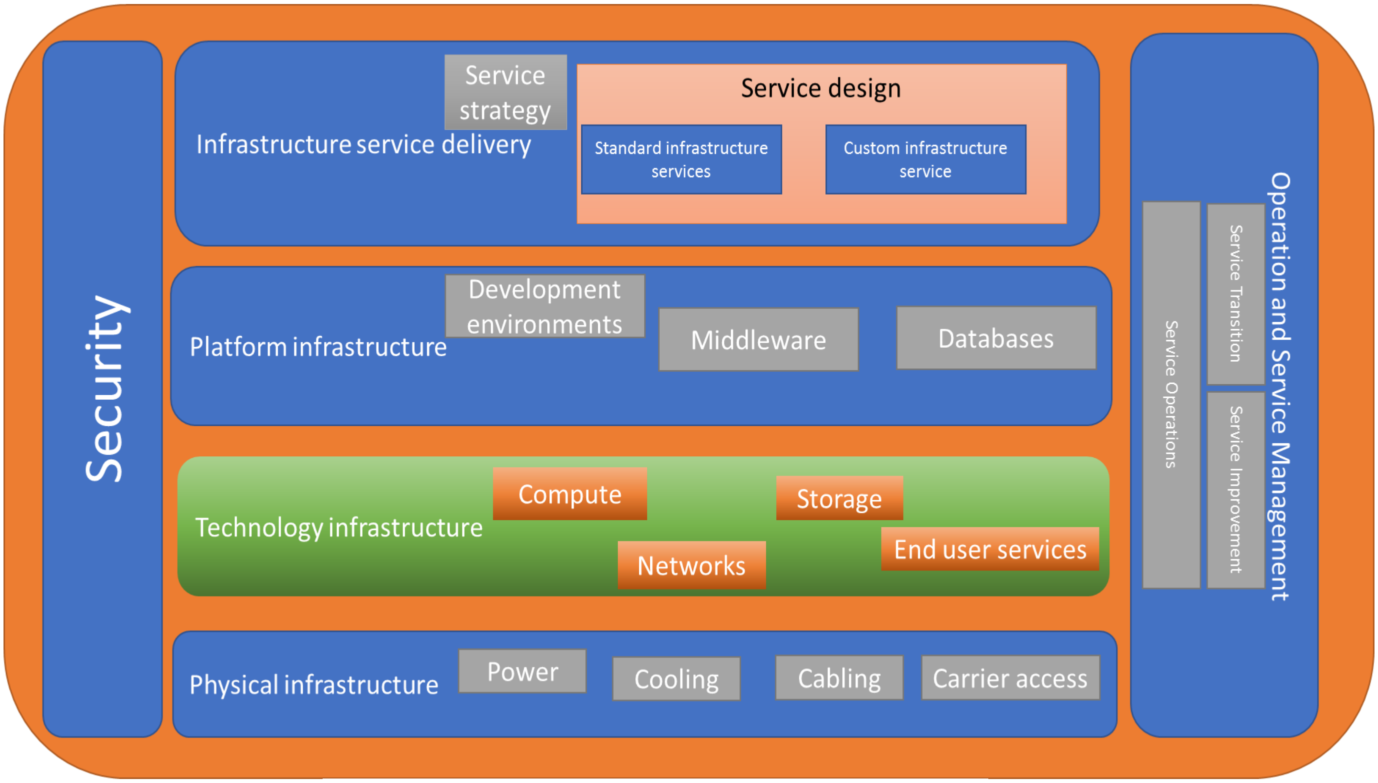

Fig. 3. Security Specification for Infrastructure Virtualization

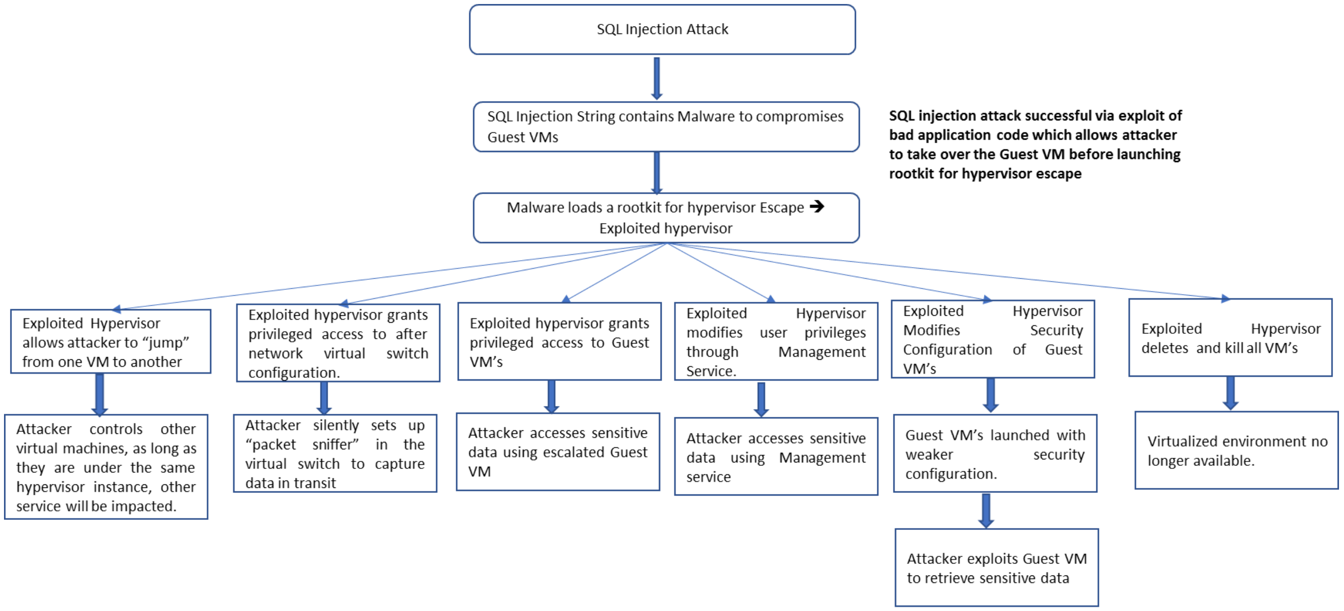
SQL Injection Attack
SQL Injection String contains Malware to compromises Guest VMs
SQL injection attack successful via exploit of bad application code which allows attacker to take over the Guest VM before launching rootkit for hypervisor escape
Malware loads a rootkit for hypervisor Escape ➔ Exploited hypervisor
Exploited Hypervisor allows attacker to "jump" from one VM to another
Attacker controls other virtual machines, as long as they are under the same hypervisor instance, other service will be impacted.
Exploited hypervisor grants privileged access to after network virtual switch configuration.
Attacker silently sets up "packet sniffer" in the virtual switch to capture data in transit
Exploited hypervisor grants privileged access to Guest VM's
Attacker accesses sensitive data using escalated Guest VM
Exploited Hypervisor modifies user privileges through Management Service.
Attacker accesses sensitive data using Management service
Exploited Hypervisor Modifies Security Configuration of Guest VM's
Guest VM's launched with weaker security configuration.
Attacker exploits Guest VM to retrieve sensitive data
Exploited Hypervisor deletes and kill all VM's
Virtualized environment no longer available.

Fig. 4. Virtualization/Hypervisor Threats and attacks Tree

(a) Bare metal hypervisor which can be installed on top of the hardware.

(b) Host Hypervisor which can be installed on top of the operating system.

II. MOTIVATION

In adaptation with any virtualization, the security factors are should be considered. Since the resources are sharing mode, it causes high probability to leakage of information. In that security factors to be more focused in Infrastructure virtualization in Private Cloud. Private cloud is the model which is hosted in one company served to different departments when hosting the internet facing application it will be exposed to the outside the world. Security will be more focused and need to build security architecture specification to build compound wall around the private cloud. In cloud computing service model security is the main consideration when any companies indent to adopt in cloud. Figure 3 depicts security specification for infrastructure virtualization.

III. SECURITY THREATS AND FUNCTIONALITIES

Table 1 focused on threats and attacks applicable to virtualize the infrastructure and hypervisor vulnerabilities [5].

TABLE I. THREAT CATEGORY

Threat Category	**Description**
Spoofing	Threat action aimed to illegally access and use another user's credentials such as username and password
Tampering	Threat actions aimed to maliciously change/modify persistent data in database, and the alteration of data in transit between two computers over an open network.
Repudiation	Threat action aimed to perform illegal operations in a system that lacks the ability to trace the prohibited operations
Information disclosure	Threat actions to read a file that one was not granted access to, or to read data in transit.
Denial of service	Threat aimed to deny access to valid users, such as by making a web server temporarily unavailable or unusable
Elevation of Privilege	Threat aimed to gain privileged access to resources for gaining unauthorized access to information or to compromise a system

Figure 4 represents tree structure that comprises the different levels of threat and attacks considered on virtualized infrastructure. The hosting of internet the organizations focused security consideration issues in private cloud [6].

The virtualization layer (Hypervisor/VMM) represents major component in the converged infrastructure/Virtualization platform. As any piece of software, it always contains vulnerabilities and it is targeted by attackers as a point of compromise. The implications from a compromise of this layer are greater than others as it may allow bigger control over resource and data [7]. Figure 5 describes different security roles in the cloud virtualization.

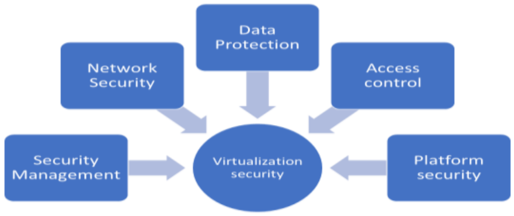

Fig. 5. Virtualization Security Roles

Table 2 describes the security functionalities and functional description when hosting the internet on the private cloud environment.

TABLE II. SECURITY FUNCTIONALITIES

Security Control Roles	**Functional Description**
Network Security	It ensures that proper security controls are in place for the virtualized network, by providing network zoning segmentation and policy enforcement.
Platform Security	It supports the hardening of the overall platform, by defining configuration control points driven from security requirements, which includes security posture hardening of the various virtualization management layers.
Data protection	It provides security mechanisms for isolation and encryption in alignment with overall data protection requirements
Access Control/IAM	It provides policy decision and enforcement to ensure that authentication, authorization and accounting is implemented across the virtualization infrastructure for systems administrative access, aligned with IAM framework.
Security Management	It provides security Management controls to account for detective, preventative, and reactive measures required for the virtualization infrastructure (e.g. logging/SIEM, vulnerability management/scanning intrusion detection)

IV. SECURITY SPECIFICATIONS AND CONTROLS FOR PROTOCOL LAYERS IN VIRTULIZATION

Security is most considerable factor in cloud computing environment [8]. It affects the each portion of the cloud especially, virtualized environment. Virtualization security architecture controls with a defense-in-depth architecture approach to provide platform security, network security, access control, data protection, and security management is vital role in virtualized infrastructure. Table 3 depicts how the different virtualization security controls apply to the different protocol layers.

TABLE III. SECURITY CONTROLS APPLY TO THE DIFFERENT PROTOCOL LAYERS

Security controls	**Security control Role**	**Functional Description**
Network Firewall	Network security	Network firewalls are used to segment security zones and tenants. As such, Network firewall are policy enforcement points to ensure segmentation is in place, as well as enforcing communication policies between different zones /tenants by blocking unauthorized traffic. Network firewalls also provide NAT (Network address translation) mechanisms to support masking.
Router (ACLs, NAT, IP Routing)	Network Security	Routers provide ACLs to support security requirements on further segmentation/access control (as a secondary layer of defense), as well as masking of network segments and their IP addresses spaces via NAT. In addition, routers may provide IP routing protocols (e.g BGP) for filtering out routes, which supports access control and masking between different network segments and zones/tenants
Switches (ACLs, VLANs, SANs)	Network Security	Switches support additional segmentation requirements by defining different VLANs. As a configuration control point, only configured VLAN trunks are established between them. Switches also support ACLs to support. Further requirements (as a secondary layer of defence). In addition, Fiber channel SAN Switches support segmentation and access control requirements.
WAF – Web application firewall	Network Security	WAFs support access control and masking requirements at the HTTP/HTTPS (Layer-7) level, by inspecting web application traffic and enforcing access control policies based on its configured rules and specific application security requirements. WAF also support encryption.
ESB/XML Gateway Appliances	Network security	ESB/XML based appliances, which supports the enterprise service infrastructure, provide network security zoning segmentation to support such requirements in the “Overlay Zones” use cases.
Intrusion Detection, Prevention (IDS/IPS) & Advanced Malware detection	Network Security, Security Management	IDS/IPS and advanced-malware-detection devices will support monitoring requirements, as well as access control and masking – based on pre-configured policies.
VPN gateway & Concentrator	Network Security	VPN concentrator/gateway supports segmentation requirements, as it may be a point of entry into a security zone as it sits at the end of the VPN tunnel. It also provides encryption capabilities for the VPN tunnel.
Host Based Firewall + DLP/Endpoint	Platform Security, Data Protection	Host -based firewall and DLP/Endpoint provides another level of defense to block unauthorized traffic.
Security Monitoring (e.g. Net Witness, DLP,Vulnerability Mgmt,SIEM Logging)	Security Management	Provide the ability to detect, identify, locate and report on vulnerabilities or security incidents. Occasionally they may be able to provide remediation and disrupt attacks. It integrates with centralized SIEM/logging framework.
Application Delivery controllers	Network Security	ADCs may provide segmentation and filtering functionality based on specific requirements by applying “firewalling” mechanisms. In addition, it may provide masking and decrypt/encrypt functions to support SSL termination requirements.
AAA/Bastion Host	Access control/ IAM	Centralized access control to address specific access control (AAA) requirements. It needs to integrate with overall IAM framework.
Proxy	Network Security	Proxy may provide reverse-proxy functionality when in front of other servers for inbound traffic, As its supports access control, filtering and monitoring. For inbound traffic, it may also provide segmentation to support “Overlay Zones”. Proxy for outbound traffic may provide access control and masking/monitoring capabilities to support of zoning such as web proxy for internal user’s internet access.
DDoS Detection & Mitigation	Network Security	DoS detection and mitigation provides identification and protection against denial of service attacks.
Hypervisor Hardening	Platform Security, Security Management	Hypervisor configuration controls may be used to harden the security posture (defined in the hypervisor technical security requirements). This includes integrity validation controls for the hypervisor (example trusted boot) may be implemented. In addition, configuration compliance management and patch management

		must be used.
Data/ Storage isolation	Data Protection	Path isolation of storage traffic may be provided by virtual SANs and SAN zoning, as well as access controls based on LUN (Logical unit number) masking.
Transparent encryption	Data Protection	Data at rest encryption (DARE) may be provided by the storage infrastructure

NAT –	Network Address translation
ACL –	Access control List
IP –	Internet Protocol
BGP –	Border gateway Protocol
VLAN –	Virtual Local Area Network
SAN –	Storage Area Network
WAF –	Web Application Firewall
ESB –	Enterprise Service Infrastructure
XML –	eXtensible Markup Language
IDS –	Intrusion Detection system
IPS –	Intrusion Prevention System
VPN –	Virtual Private Network
DLP –	Data loss prevention
SIEM –	Security information and event management
ADC –	Application Delivery controller
AAA –	Authentication, authorization and Accounting
DDoS –	Distributed Denial of service
LUN –	Logical Unit Number
DARE –	Data at Rest Encryption

V. Conclusion and Future Work

This paper covered the detailed infrastructure components in private cloud and functionalities of it. The detailed security architecture specification for infrastructure virtualization in private cloud is explained and the security parameters need to be considered to tighten the security. It comprised category of threats available and different ways of exposable threat tree analysis is provided. The paper also discussed about different layers of security and virtualization security architecture controls. It absolutely covers the virtualization security in private cloud which hosted in on-premises. In the future work, private cloud will be hosted inside the public cloud. Currently the name is getting popular in cloud industry is that SDDC – software defined data center. The security parameters will slightly different when user's intent to host the private from on-premises to off-premises.

References

[1] A. R. Riddle and S. M. Chung, "*A Survey on the Security of Hypervisors in Cloud Computing,*" IEEE 35th International Conference on Distributed Computing Systems Workshops, Columbus, OH, pp.100-104, 2015.

[2] Arockiam, L. and Monikandan, S. and Parthasarathy G. *"Cloud Computing: A Survey. International Journal of Internet Computing"*, Volume 1, No. 2, , pp.26-33, 2011.

[3] A. Tolnai and S. H. von Solms, *"Securing the Cloud's Core Virtual Infrastructure"* , IEEE International Conference on Broadband, Wireless Computing, Communication and Applications, Fukuoka, , pp. 447-452, 2010.

[4] K. M. Babu and P. S. Kiran, *"A secure virtualized cloud environment with pseudo-hypervisor IP based technology"*, IEEE 2nd International Conference on Next Generation Computing Technologies (NGCT), Dehradun, pp. 626-630, 2016.

[5] Tony UcedaVelez, Marco M. Morana, *"Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis"*, John Wiley & sons, pp. 547, 2015.

[6] S. N. Brohi, M. A. Bamiah, M. N. Brohi and R. Kamran, *"Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures"*, IEEE International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), Dubai, pp. 151-155, 2012.

[7] W. Yang and C. Fung, *"A survey on security in network functions virtualization"*, IEEE NetSoft Conference and Workshops (NetSoft), Seoul, pp. 15-19, 2016.

[8] Arockiam, L. and Monikandan S. *"Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm"*, International Journal of Advanced Research in Computer and Communication Engineering, Volume 2, No. 8, pp. 3064-3070, 2013.