ISSN:0975-9646

Optimization of Security Policies on Virtual Machines using Flow Differentiator & Zone Manager

J.Madhulatha[1], E.S.Phalguna Krishna [2], E.Sandhya[3]

[1]. PG Student, M. Tech (CNIS), Sree Vidyanikethan Engineering College.
[2]. Assistant Professor, Dept of CSE, Sree Vidyanikethan Engineering College.
[3].Assistant Professor, Dept of IT, Sree Vidyanikethan Engineering College.

Abstract:Security is considered as most crucial aspect in cloud computing. It has attracted lots of research in the recent years. On the other hand, attackers are exploring and exploiting the vulnerabilities in cloud. The heart of the Cloud computing lies in Virtualization technology. Attackers are taking the advantage of vulnerabilities in Virtual Machines and they can able to compromise virtual machines thereby launching DDOS attacks. Services such as Saas, IaaS which are meant to support end users may get affected and attackers may launch attacks either directly or by using zombies. Generally, Data Centres own security policies for dealing with security issues. Suppose in case of DDoS attacks, only the policies which deals with it , can only been applied. However, in datacentres, all the security policies are commonly been applied on the applications irrespective of their category or security threats that it face. The existing approach consumes lots of time and wastage of resources. In this paper, we have developed an approach to segregate the applications as per the type or threats (by adapting detection mechanisms) being faced . Based on the zone in which it is lying , only the relevant security policies will only be applied. This approach is optimized where we can efficiently reduce the latency associated with applying security policies.

1.INTRODUCTION

Virtualization is considered as back bone for cloud computing with which users can access multiple instances of apps, resources etc. Virtualization technology will allow one computer to do the job of multiple computers. This environment let one computer host multiple operating systems at the same time. It transforms hardware into software. It is emulation of a fully functional virtual computer that can run its own applications and operating system and also Creates virtual elements of the CPU, RAM, and hard disk. Hardware-independence of operating system and applications. Hence, using virtualization it is possible to run operating systems and multiply applications on the same SERVER at the same time, thereby it raises the utilization and flexibility of hardware.

Some of the virtualization technologies include VMWare, Hyper V, Virtual Iron etc.,

1.1Virtual Machines

These are the things that can manage OS and application as a Single unit by encapsulating them into Virtual Machines. A Virtual machine (VM) is an efficient, isolated duplicate of a real machine.

Virtual machines can be provisioned to any system

Duplicate: The behaviour of the VM should be identical to the real machine. There is no differentiation with respect to the execution of the program at the low level.

Isolate: Multiple Virtual Instances corresponding to different VMs execute without interfering with each other.

Efficient: VM should operate at the speed of the underlying hardware.

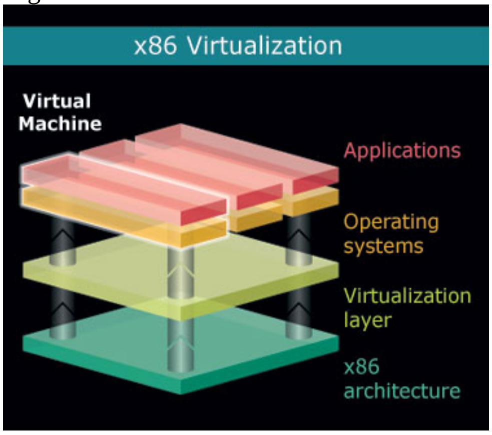


Fig 1: VIRTUALIZATION

All the resources of the physical computer are shared to create the virtual machines.By virtualization, it creates an emulation that user is actually using owned resources. But at the implementation level, these resources are shared between multiple number of users at any given point in time. Further, Disks are partitioned into virtual disks and a normal user time sharing terminal serves as Virtual machine operators console.

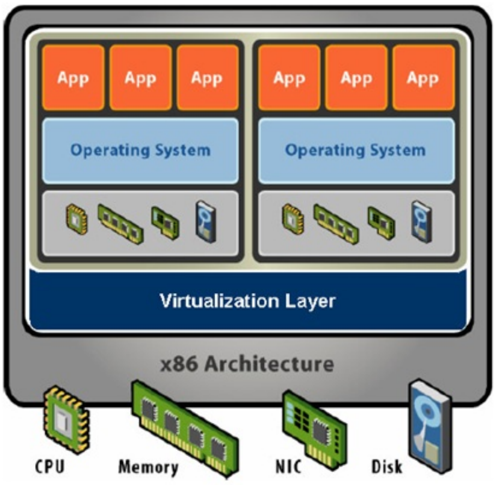


Fig 2: Virtual Machine & Its Layers

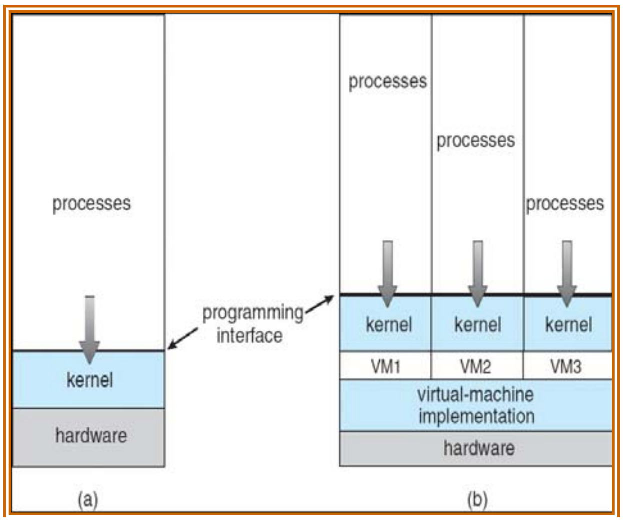


Fig 3: VIRTUAL MACHINE

1.2 Types of Virtual Machines: Type 1 / Type 2

1)Type 1 .

They are also Called Hypervisors or virtual machine monitor or VMM. Hypervisors of this type is dependent of bare metal (bare machine) and always interacts with the machine. They Sit just above the HW and virtualizes the complete hardware. It runs at the physical hardware and is the real operating system. Normal unmodified operating systems, like Linux or Windows runs atop of the hypervisor. The server which is hosting Type 1 Hypervisor requires some form of persistent storage for storing the files of concern. In ESX server, the kernel uses device drives to actually get interfaced with bare metal.

• Example: Xen , VMware ESX server

2)Type 2 hypervisor

It is considered as most common type of hypervisor and depends on the underlying OS. Such hypervisors requires to be directly installed on bare metal. It runs within an OS, and rely on OS services to manage HW. A normal unmodified host operating system like Linux or Windows runs on the physical hardware.

A type 2 hypervisor like VMware Workstation runs on the host operating system. Once after installing host operating system, we can now deploy hypervisor and it doesn't modify it. Examples include QEMU, VMware Workstation etc.

2. THREATS ON VMS:

Like any other technology, Virtual Machines are prone to different categories of threats. Some attacks against virtual machine, or VM, environments are variations of common threats such as denial of service etc. Others are still largely theoretical but likely approaching as buzz and means increase, these are the critical weaknesses.

1) VM Sprawl:

VMs are easy to deploy, and many organizations view them as hardware-like tools that don't merit formal policies. This has led to VM sprawl, which is the unplanned proliferation of VMs.

Attackers can take advantage of poorly monitored resources. More deployments also mean more failure points, so sprawl can cause problems even if no malice is involved.

2) Hyperjacking :

Hyperjacking takes control of the hypervisor to gain access to the VMs and their data. It is typically launched against type 2 hypervisors that run over a host OS although type 1 attacks are theoretically possible but practically difficult.

In reality, hyperjackings are rare due to the difficulty of directly accessing hypervisors. However, Hyperjacking is considered a real-world threat, and administrators should take the offensive and plan for it.

3)VM escape :

A guest OS escapes from its VM encapsulation to interact directly with the hypervisor. By doing so, the attacker can gain access to all VMs and, if guest privileges are high enough, the host machine can also be targeted as well. Although few, if any instances are known, experts consider VM escape to be the most serious threat to VM security.

4) Denial of Service:

Considered most common threat. These attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources. The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services.

5) Incorrect VM Isolation:

To remain secure and correctly share resources, VMs must be isolated from each other. Improper control over VM deployments can lead to isolation breaches in which VMs communicate. Attackers can exploit this virtual drawbridge to gain access to multiple guests and possibly the host. The attacker can take the loop holes in the interfaces and can attack.

6) Unsecured VM migration:

This occurs when a VM is migrated to a new host, and security policies and configuration are not updated to reflect the change. Potentially, the host and other guests could become more vulnerable. Attackers have an advantage in that administrators are likely unaware of having introduced weaknesses and will not be on alert.

7) Host and guest vulnerabilities:

Host and guest interactions can magnify system vulnerabilities at several points. Their operating systems, particularly Windows, are likely to have multiple weaknesses. Like other systems, they are subject to vulnerabilities in email, Web browsing, and network protocols. However, virtual linkages and the co-hosting of different data sets make a serious attack on a virtual environment particularly damaging.

8) Dynamic environment:

Tracking and updating what you have can be a challenge as people create, suspend and move virtual machines. If you don't update your golden image from which virtual machines are deployed, you can end up needing to find and patch many virtual machines.

Mitigating Risk:

In order to overcome the existing problem with respect to the security, one can take Several steps to minimize risk.

- **Characterization:** The first task is to accurately characterize all deployed virtualization and any active security measures beyond built-in hypervisor controls on VMs.
- **Standards:** Security controls should be compared against industry standards to determine gaps. Coverage should include anti-virus, intrusion detection, and active vulnerability scanning.

Additionally, consider these action steps:

VM traffic monitoring: Efficient monitoring of VM backbone network traffic is critical. Conventional methods will not detect VM traffic because it is controlled by internal soft switches. However, hypervisors have effective monitoring tools that should be enabled and tested. Also , by maintaining traffic logs ,one can have vigilance over the network traffic.

Administrative control : Procedures such as authentication, authorization ,Identity management etc must be done as a regular process by the concerned admins. Sometimes, Secure access can become compromised due to VM sprawl and other issues.

Customer security: Outside of the VM, make sure protection is in place for Customer interactive interfaces such as websites.

VM segregation: In addition to normal isolation, strengthen VM security through functional segregation.

For example, consider creating separate security zones for desktops and servers. The goal is to minimize intersection points to the extent feasible.

3. VIRUALIZATION VULNERABILITIES

Virtualization has eased many aspects of IT management but has also complicated the task of cyber security. The nature of virtualization introduces a new threat matrix.

Single Server :

- VMs run on a single server which poses serious security problems.
- Virtual monitor should be root secure meaning that no privilege within the virtualized guest environment permits interference with the host system been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges.
- For example, the vulnerability of Microsoft Virtual PC and Microsoft Virtual Server could allow a guest operating system user to run code on the host or another guest OS.
- Vulnerability in Virtual PC and Virtual Server could allow elevation of privilege.

A perfection of properties like isolation is yet to be completely achieved.

Ease of reconfiguration:

Ability to flexibly reconfigure restart and also movement of VM‘s to other servers. Because of this easiness, an optimal environment to propagate vulnerabilities and unknown configuration errors has been created.

Dormant machines:

In public-cloud environments, VM is available to any application even though it is offline.

- For example, a Web server that can access the physical server on which it resides.
- So a remote user on one VM can access another dormant VM if both reside on the same physical server.
- As Dormant machines can‘t perform malware scans, they are highly susceptible to malware attacks.
- Exploitation of this vulnerability is not only restricted to the VMs on a particular hypervisor but also affect other physical devices in the cloud.

For example: A Dormant machine might have been backed up or archived to another server or storage device.

Patch management:

Generally users does the patch management in cloud computing and attackers could easily misuse this opportunity to attack VMs.

Cross-VM information leakage:

It is the ability of a malicious instance to utilize side channels to learn information about co-resident instances.

4. MODULES:

1) Packet Feeder:

Packet arrives from multiple streams and they are feeded into the packet feeder module which acts as entry point for this approach. The responsibility of the packet feeder is to collect packets from various incoming streams and feed them to the module “FLOW DISCRIMINATOR”.

2) Flow Differentiator:

It differentiates as per the type of packets based on its properties (multimedia, text, voice, images etc)

3) Decision Maker:

This Module applies “Outlier Analysis” technique to discriminate and differentiate different types of flows or vulnerablilities. For example: Normal traffic, Flash Crowd traffic, DDOS traffic etc. Our approach using Outliers requires lesser amount of computations and considered to be effective in discriminating the attacks.

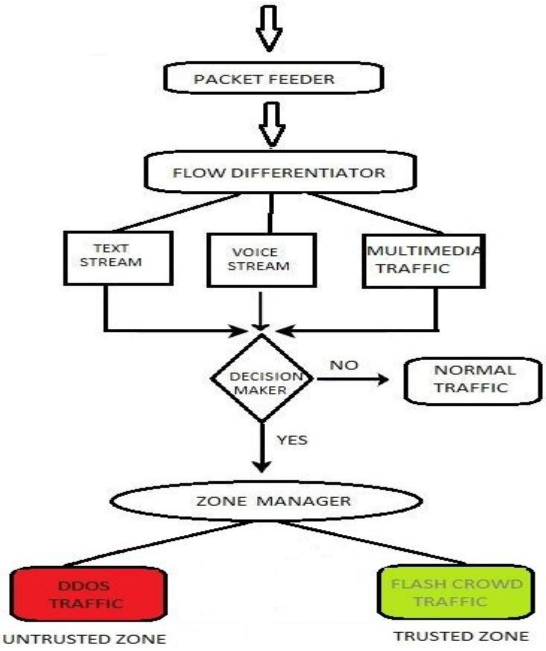
4) Zone Manager :

Based upon the nature of VMs , it is prescribed to adopt necessarily relevant policies.

ADVANTAGES:

- Optimizes the application of rule sets on different categories of applications.
- This approach significantly reduces the time taken by the data centre admin by applying only essential set of security policies.

BLOCK DIAGRAM:



5. METHODOLOGY:

Users from various locations sends the service requests in the stream of packets to the Virtual servers/ Virtual machines , which internally utilizing virtualization technology. The packets arrived are feeded into the "**Packet Feeder**" module which acts as entry point for this approach. The responsibility of the packet feeder is to collect packets from various incoming streams and feed them to the module "**Flow Discriminator**".

The flow discriminator which takes various streams of packets as input differentiates what type of packet stream it is based on its properties like file extension, contents in the packet etc and categorizes them accordingly such as multimedia, voice, text, images etc. The discrimination is done mainly to adopt the relevant decision strategies and appropriate security policies. All categorized packet streams are given as input next module named "**Decision Maker**".

Decision Maker is the most important module which applies Outlier Analysis technique to discriminate and differentiate different types of vulnerablilities in the flow. For example: Normal traffic, Flash Crowd traffic, DDOS traffic. An advantage of using Outliers in this approach just not only requires lesser amount of computations but also considered to be effective in terms of discriminating the attacks.

Finally the identified malicious traffic from normal traffic is sent to the "**Zone Manager**" which in turn discriminates the DDOS traffic from FLASH CROWD traffic . Based upon the nature of VMs it is prescribed to adopt necessarily untypical policies to safeguard users trust.

This paper consists of three cases : Normal Traffic, DDoS, Flash Crowd. Based on the case, we apply the relevant necessary security policies. This is in converse with the previous approach , where in which the admins of the data centre used to adopt common security policies for discrete set of applications. The previous approach not only consumes time but also leads to consuming more number of processor cycles.

6.ANALOGY:

Normally datacentre own discrete categories of applications. In order to provide the security, each and every data centre maintains set of security policies. It specifies what it means to be secure for a system, organization or other entity. But the scenario is like data centre admins or tools apply complete set of security policies irrespective of the concept thereby consuming lots of processor cycles and raises latency.

In this paper, we have used an approach to segregate the applications as per the type or threats (by adapting detection mechanisms) being faced and we segregate them into zones. Based on the zone in which it is lying , only the relevant security will only be applied. This approach is optimized where we can efficiently reduce the latency associated with applying security policies.

Consider a scenario in which a datacentre hosts different set of software applications on their infrastructure. Let S be the main rule set, there exists Subsets S_i , S_j, S_k. For example A,B,C,D applications belong to a particular type of application (multimedia) or facing particular threat (DDoS).Let P,Q,R & X,Y be different categories. Then suppose, A, B, C, D, are the applications that are facing DDoS attack as a threat at this instance, Then it may be relevant to apply for example Si set of rules on those machines which are affected by it, Instead of applying S. Where Si,Sj,Sk ⊆ S. We assumed applications A,B,C,D as web apps and they are prone to DDoS attacks and Si as the subset of rule set that consists of the security policies and mitigation strategies to be applied for DDoS. Similarly $S_j \in (P,Q,R,S)$ and $S_k \in (X,Y)$.

7.APPLCATIONS:

- The approach can be adopted to the data centres consisting diversified applications.
- The approach is applicable to the datacentres which considers security as a service.

8.SECURITY POLICIES:

A security policy is a comprehensive document that defines a companies' methods for prevention, detection, reaction, classification, accountability of data security practices and enforcement methods. It generally follows industry best practices as defined by ISO 17799, 27001-02, PCI, ITIL, SAS-70, HIPPA , SOX or a mix of them. It is the key document in effective security practices.

Following are some of the policies of data centers:

- Develop a checklist for standard operating procedures to follow in the event of an attack, including internal firewall teams, intrusion detection teams and network teams. Identify who should be contacted during an attack, what processes should be followed by each and what information is needed.
- ISPs and hosting providers might provide mitigation services. Be aware of the service-level agreement provisions.

- Identify and prioritize critical services that should be maintained during an attack so as to keep resources turned off or blocked as needed to limit the effects of the attack.
- Ensure that critical systems have sufficient capacity to withstand an attack.
- Determine whether the denial of service attack is attempting to consume:
  a. Network bandwidth resources, or
  b. Server resources.
- Separate or compartmentalize critical services, including public and private services; intranet, extranet, and Internet services and create single-purpose servers for services such as HTTP, FTP, and DNS.
- Keep network diagrams, IT infrastructure details and asset inventories current and available to help understand the environment.
- Have a baseline of the daily volume, type, and performance of network traffic to help identify the type, target and vector of attack.
- Identify existing bottlenecks and remediation actions needed.
- Harden the configuration settings of the network, operating systems and applications by disabling unnecessary services and applications.
- Implement a bogon (bogus IP address) block list at the network boundary to drop bogus IP traffic.
- Employ service screening on edge routers: very useful to decrease the load on stateful security devices such as firewalls.

Mitigation Strategies of DDOS attacks in data centres:

Data centres cannot rely on their ISP alone to provide a complete DDoS solution that includes application layer protection.

To protect against application-layer DoS, several mitigation strategies can be considered:

I. Traffic subjected to rate limits, prioritization, and load balancing.

II. Fast-expiring session aging

III. Two-factor authentication to validate user roles, especially at admin levels.

IV. Advanced next generation firewalls (NGFWs), such as Fortinet's FortiGate products, offer DDoS and IPS services.

V. Dedicated DDoS Attack Mitigation Appliances: These are dedicated hardware-based devices that are deployed in a data centre used to detect and stop basic (layer 3 and 4) and advanced (layer 7) DDoS attacks.

VI. Deployed at the primary entry point for all web-based traffic, they can both block bulk volumetric attacks and monitor all traffic coming in and leaving the network to detect suspicious patterns of layer 7 threats.

Top three mitigation solutions:

To make services more robust against a DDoS attack, the following combination of strategies are proposed, they are:

1. **Increase the barrier to entry by using a Pricing-Based Scheme:**

Price of entry varies with the load level. This will throttle the machines used in the attack, thereby forcing the attacker to employ (or subvert) a larger number of machines.

2. **Differentiated model**:

Allocating a priority mechanism to desirable clients is key which Provides prioritized access to classes of users though a DDoS attack will raise the price so high that lower priority classes get locked out, higher priority clients can still access the service.

3. **Dynamic and Differential pricing mechanism** : This will be applied to penalize clients who are responsible for a load on the server and it typically requires flow monitoring and isolation capabilities.

Flash Crowd Mitigation Strategies:

a. Adaptive Admission Control Based on Application-Level Observations.
b. Flash Crowd Detection within the realms of an Internet Service Provider (ISP).
c. Dynamic CDN against Flash Crowds.
d. Managing Flash Crowds on the Internet
e. Handling Flash Crowds from your Garage
f. KadCache : Employing Kad to Mitigate Flash Crowds and Application Layer DDoS Attacks Against Web Servers

9. Conclusion:

The flow differentiator is responsible to identify and discriminate attack ,normal flows. Further, we apply zone managers, which will move VM's & its applications to respective zones .Only the relevant security policies will only be applied on the VM's which are running those applications that are affected with security vulnerabilities. Our approach is considered to be effective in optimizing the security policies. Further, this approach is considered to be effective and consumes less resources and time.

References:

1. Shui Yu, Weijia Jia, Song Guo, Yong Xiang, and Feilong Tang ”Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient” IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 6, June 2012.
2. Ke Li, Wanlei Zhou, Ping Li, Jing Hai and Jianwen Liu “Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics” Third International Conference on Network and System Security pno: 9-17 .2009.
3. Zhang Fu, Marina Papatriantafilou, and Philippas Tsigas “Mitigating Distributed Denial of Service Attacks in Multiparty Applications in the Presence of Clock Drifts” IEEE Transactions On Dependable And Secure Computing, Vol.9, No.3, May/June 2012.
4. Arbor Application Brief**: “**The Growing Threat of Application-Layer DDoS Attacks”.2011.
5. Employing Kad to Mitigate Flash Crowds and Application Layer DDoS Attacks Against Web Servers.
6. Ari, B. Hong, E. L. Miller, S. A. Brandt, and D. D. E. Long, “ Modeling , Analysis and Simulation of Flash Crowds on the Internet,” Storage Systems Research Centre Jack Baskin School of Engineering University of California, Santa Cruz Santa Cruz, CA, ech. Rep. UCSC-CRL-03-15, Feb. 28, 2004 http://ssrc.cse.ucsc.edu/, 95064.