# Defense mechanisms for internal doS attack in a cloud

Ni-Na Shu[1], Huai-Xi Wang[1]*, Chen Wang[1] and Fang Fang[2]
[1]*Hefei Electronic Engineering Institute,460 Huangshan Rd., Hefei, Anhui, 230031, P.R.China*
[2]*School of Mechatronics Engineering, University of Electronic Science and Technology of China,2006 Xiyuan Rd., Chengdu, Sichuan, 611731, P.R. China*
*E-mail: snncyc@tom.com, paper2submit@163.com, daodewang@163.com, fangfang@163.com*
**Corresponding author*

In CSA report entitled "The Notorious Nine: Cloud Computing Top Threats in 2013", DoS attack is ranked fifth. In the practical cloud computing environment, DoS attack is always the most effective and destructive threat, bringing a great impact on the cloud. We focus on VMware vSphere which is one of the most typical and prevalent cloud computing platforms. In this paper, we describe VMware vSphere's architecture, establishing entire cloud computing environment, manipulating internal DoS experiment, and putting forward the corresponding defense mechanisms.

*Keywords*: Cloud Computing; VMware VSphere; Denial of Service; Defense Mechanism.

## 1. Introduction

Cloud computing [1, 2] is a kind of information services based on network, which focuses on sharing multiple resources, such as computing, storage and networking. Cloud computing refers to both the applications delivered as services over the Internet and the hardware and software resources in the datacenters that provide those services. Cloud computing service providers utilize virtualization technologies and self-service abilities to offer computing resources via network infrastructure. In cloud computing environments, virtual machines of several tenants are hosted on the same physical server. In terms of cloud computing, consumers only need to pay for what they use and needn't afford local infrastructures.

At an unprecedented pace, cloud computing has transformed business models and governments, and created new security challenges [3-5]. In the report entitled "The Notorious Nine: Cloud Computing Top Threats in 2013 [5]" released by CSA, experts identified the following nine critical threats to cloud security ranked in order of severity: data breaches, data loss, account hijacking,

insecure APIs, denial of service, malicious insiders, abuse of cloud services, insufficient due diligence, and shared technology issues. One of these critical threats is denial of service (DoS) attack which would result in billions of dollar losses and maybe corporate collapse. It has become the key factor of self-sustainability of cloud computing development.

Simply speaking, DoS attacks can be used to prevent users of a cloud service from being able to access their data or their applications. DoS attack can consume inordinate amounts of system resources in cloud computing such as processor power, memory, disk space or network bandwidth, thus can cause intolerable service decreases and system shutdown.

This paper is organized as follows: we introduce VMware vSphere and describe several possible internal DoS attack in a cloud based on VMware vSphere in Chapter 2, and propose the defense measures that can help users to avoid DoS attack in Chapter 3, and conclude the whole paper in Chapter 4.

## 2. VMware vSphere and Internal DOS Attacks

### 2.1. *VMware vSphere system*

We introduce VMware vSphere, a platform for virtualization and cloud computing infrastructure. The virtual technology is the foundation of cloud computing. Cloud computing depends on a scalable and elastic model for delivering IT services, and the model itself depends on virtualization to be running.

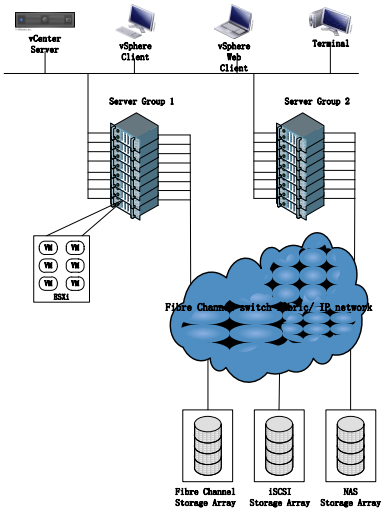


Fig. 1 VMware vSphere Datacenter Physical Topology

A typical VMware vSphere [6] data center consists of the following physical building blocks: x86/x64 virtualization servers (ESXi servers), storage networks and arrays, IP networks, a management server (vCenter Server), and desktop clients (vSphere Client, vSphere Web Client), as shown in Fig. 1.

In VMware vSphere system, ESXi servers, vCenter Server, storage networks and arrays are crucial nodes which are the key nodes for DoS attacks. Cloud computing provider need design specific scheme to protect these crucial nodes.

### 2.2. *Internal DoS attacks*

In virtual machine architecture the guest machines and the underlying host share the physical resources such as CPU, memory, disk, and network resources. So it is possible for a guest machine or single computer outside the cloud to impose a DoS attack to ESXi server to affect the guest machines residing in the ESXi server. DoS attack in virtual environment can be described as an attack when a guest machine takes all the possible resources of the system. Hence, the system denies the service to other guests that are making requests for resources; this is because there is no resource available for other guests.

In order to evaluate the effect of internal DoS attack, we make the DoS attack experiment. In the experiment, attack computers, ESXi servers and guest machines are in the same local area network. We choose two guest machines as attack machines and an ESXi server as target machine. Here, we list the detailed physical parameters of attack computer and ESXi server, as follows:

- ESXi server is run on a Lenovo T350 server (CPU: Intel Xeon 2.8 GHz Quad core four thread, Cache: 2GB) and its internal IP address is 192.168.100.31.
- The attack computer is run on Lenovo IdeaCentre B500 (CPU: Intel Core 2.66GHz Quad core, Cache: 4GB) and the operating system is Windows 7. The internal IP addresses of two attack computers are 192.168.100.22 and 192.168.100.27. In the experiment, each compute run two threads.

In the experiments, CPU usage and network traffic is the criterion. We describe results of CPU usage and network traffic under DoS attack. We list four kinds of DoS attack: SYN-DoS, PSH&ACK-DoS, ICMP-DoS and Land-DoS.

#### 2.2.1. *SYN-DoS performance analysis*

In SYN-DoS experiment, CPU usage of ESXi server arises from 0.25% (average) to 18% (average) and network traffic arises from 1Mbps (average) to 68Mbps

(average) rapidly. The detailed experimental results are shown in Fig. 2 and Fig. 3.

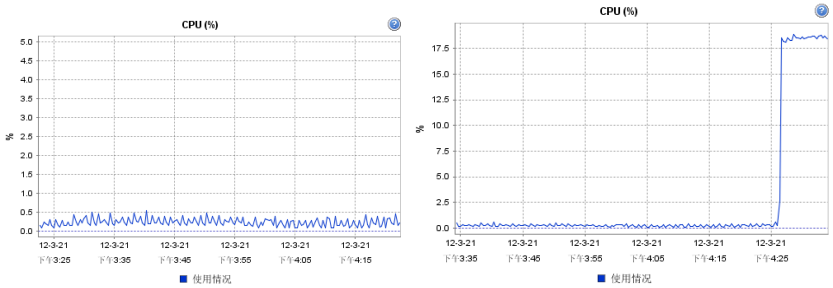


Fig. 2 Variation of CPU usage under SYN-DoS Attack.

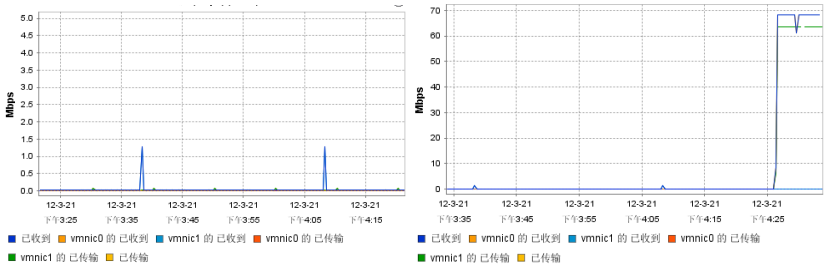


Fig. 3 Variation of network traffic under SYN-DoS Attack.

### 2.2.2. *PSH & ACK-DoS performance analysis*

In PSH&ACK-DoS experiment, CPU usage of ESXi server arises from 0.25% to 10% (average) and network traffic arises from 1Mbps (average) to 64Mbps (average) rapidly. The detailed experimental results are shown in Fig. 4 and Fig. 5.

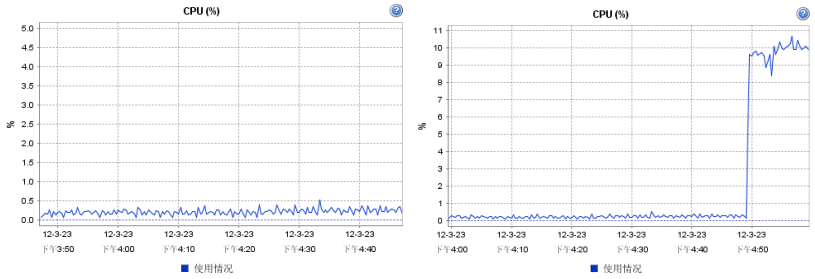


Fig. 4 Variation of CPU usage under PSH&ACK-DoS Attack.

Due to the limit of pages, we only display the experimental data and would not provide the experimental results in the charts. In ICMP-DoS experiment, CPU usage of ESXi server arises from 0.25% to 1.4% (average) and network

traffic arises from 1Mbps (average) to 93Mbps (average) rapidly. In Land-DoS experiment, CPU usage of ESXi server arise from 0.25% (average) to 1.4% (average) and network traffic arise from 0.1Mbps (average) to 1.8Mbps (average) rapidly.

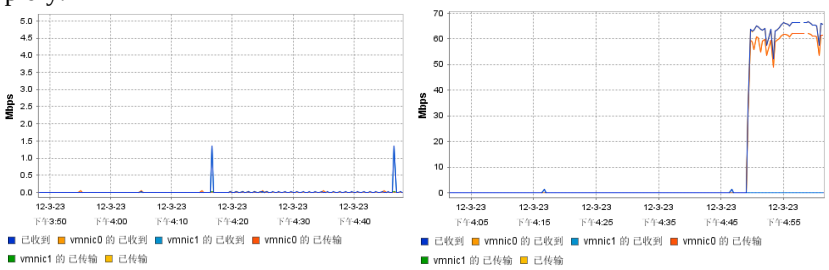


Fig. 5 Variation of network traffic under PSH&ACK-DoS Attack.

### 2.2.3. *Contrastive Analysis*

For the sake of clearance, we list the attack effect of the above four kinds of DoS packets in Tab. 1. In this table, we can see the differences of attack effect among different kinds of DoS packets. SYN-DoS makes greatest impact on CPU usage with almost 18% increment, and ICMP-DoS and Land-DoS make few impacts on CPU usage with only 1.15% increment. ICMP-DoS makes greatest impact on network traffic with 92Mbps increment, and Land-DoS makes few impacts on network traffic with only 1.7Mbps increment. Meanwhile, SYN-DoS and PSH&ACK-DoS make important import on network traffic with 60-70 Mbps increment. Generally speaking, SYN-DoS and ICMP-DoS are perfectly fit to attack CPU usage and network traffic respectively.

Tab. 1 Attack Effect of Different DoS Packets

| Type of DoS | CPU Usage Increment (%) | Traffic Increment (Mbps) |
|---|---|---|
| SYN | 17.75 | 67 |
| PSH&ACK | 9.75 | 63 |
| ICMP | 1.15 | 92 |
| Land | 1.15 | 1.7 |

All in all, internal DoS attack can make great impact on CPU usage and network traffic in a cloud computing center. Internal DoS attack can also affect other resources, such as cache memory and storage. Therefore, internal DoS attack is a critical threat in a cloud. In the same time, we can observe that different kinds of DoS attacks can make very different impacts on physical resources. This can help us to establish adequate defense schemes.

## 3. Defense Mechanisms for Internal DoS Attack

VMware vSphere provide many security manners for users [7]. In order to avoid internal DoS attack, cloud users need to strengthen three main security mechanisms: strict firewall, resource reservation and secure virtual networking.

### 3.1. *Strict firewall*

The security of VMware vSphere can be strengthened by firewall. In a cloud, isolating various types of traffic is very important for system administrator. A DMZ virtual machine should have no access to your storage system. But it is important to consider any host as a potential threat to your vSphere infrastructure. Numerous studies point to insiders as the greater risk to network security than external hackers, and even a virus or instance of malware inadvertently introduced into your environment will pose a risk to any systems it can access.

Firewalls are used to control access to hosts and other network devices by closing all network ports and paths except those specifically configured for the network to function properly. ESXi does not include a firewall because it runs a limited set of well-known services and does not allow the addition of further services. With this design, the need to run a built-in firewall, as is the case with VMware ESX, is significantly reduced in ESXi.

The deployment of firewalls to protect vSphere system will depend on your security needs. Fig. 6 shows a number of potential locations for firewalls in a typical vSphere deployment. In this example, all client traffic to the vCenter Server is routed through a firewall. This includes any management applications that will interact with vCenter Server. If you plan to provide remote console access to the virtual machines, you will further have to open your firewall to allow direct access from the client computers to the ESXi hosts for TCP port 902.

You may also consider a firewall between your vCenter Server host and your ESXi hosts. There are a limited number of ports that you have to open for this, but you should keep in mind that additional modules such as Update Manager and Data Recovery will require additional ports to be open. The sample configuration also has firewall protection between the ESXi hosts and storage devices. Between hosts, the traffic can be considered trusted, but if you have stringent security for High Availability, vMotion, Fault Tolerance, and other interhost communication. Given that vCenter Server and vSphere client do not require access to the network used for interhost communication, you may consider physically isolating the network that is used for that traffic. The same

consideration can be given to the network used to connect your ESXi hosts to your storage devices.

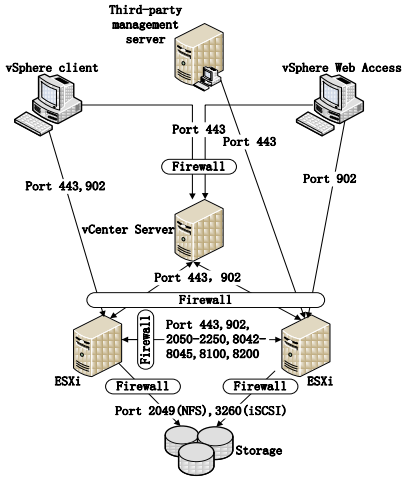


Fig. 6 Typical Firewall Deployment in vSphere

### 3.2. *Resource reservation to virtual machines*

The best approach to prevent a guest consuming all the resources is to limit the resources allocated to the guests. Current virtualization technologies just offer this mechanism. Therefore the underlying virtualization technology should be properly configured, which can prevent one guest consuming all the available resources, thereby preventing the denial of service attack.

To protect virtual machines further, you should consider the use of limits, shares, and resource reservations. ESXi server can impose a form of resource reservation to ensure that the resources of the host are divided equally among the virtual machines running on the host. If a virtual machine on the host were to be compromised by DoS attack, the other virtual machines would be partially isolated from the resource drain caused by the DoS attack. You could further limit the impact of a problem virtual machine by setting specific reservation and limits. With a reservation, you ensure that a virtual machine has a guaranteed quantity of a specific resource and you could also use a limit to ensure that a virtual machine would not consume excessive hardware resources. For low-resource virtual machines that are accessible to the Internet, you may consider lowering the CPU shares or setting a CPU limit for the virtual machines. In the case of a compromise, the virtual machine would have limited CPU resources to attack other hosts and consume fewer CPU resources on the host.

### 3.3. *Securing virtual networking*

#### 3.3.1. *Security virtual networking with VLANs*

The virtual networking layer includes virtual network adapters and virtual switches. ESXi relies on the virtual networking layer to support communications between virtual machines and their users. In addition, hosts use the virtual networking layer to communicate with iSCSI SANs, NAS storage, and so forth. The methods you use to secure a virtual machine network depend on which guest operating system is installed, whether the virtual machines operate in a trusted environment, and a variety of other factors. Virtual switches provide a substantial degree of protection when used with other common security practices, such as installing firewalls.

ESXi also supports IEEE 802.1q VLANs, which you can use to further protect the virtual machine network or storage configuration. VLANs let you segment a physical network so that two machines on the same physical network cannot send packets to or receive packets from each other unless they are on the same VLAN.

#### 3.3.2. *Configuring vSwitch security properties*

The properties for vSwitches and port groups include a number of security policies designed to safeguard your network. From the perspective of the guest operating system, the virtual NIC functions just as a physical NIC would, so a malicious program executing within the virtual machine is capable of forging MAC addresses or flooding the network to create a DoS attack.

There are three security options that you can set to prevent malicious activity, and you can set limits on network traffic to prevent excessive network load. To make changes to the security policy or traffic shaping policy of a vSwitch, you can follow these steps:

1. In the vSphere client, select the Configuration tab for a host and then select the Networking link in the Hardware pane.
2. For the vSwitch you wish to configure, select Properties.
3. Select the vSwitch port and click Edit.
4. Select the Security tab to display the security policy options shown in Fig. 7.
5. Select the Traffic Shaping tab, shown in Fig. 8. From this tab, you can configure the traffic settings for the vSwitch.
6. Make any desired changes and click OK, and then Close to complete the changes.

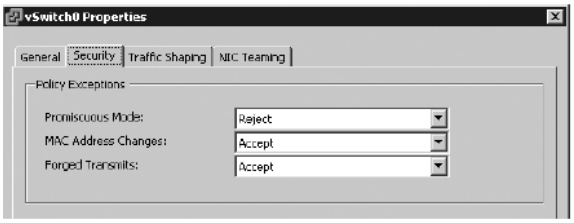


Fig. 7 Configuring security policies on a vSwitch

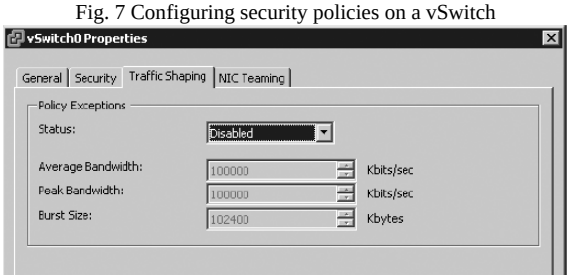


Fig. 8 Configuring traffic settings on a vSwitch

The first setting on the Security tab is Promiscuous Mode. The option is by default set to reject. This eliminates the possibility that the virtual machine could be used to capture all traffic on the vSwitch, as the vSwitch will filter network traffic to ensure that the virtual machine receives only packets destined for that specific virtual machine. In some cases, if you are running network sniffer or intrusion detection software, you may need to allow Promiscuous Mode on a vSwitch, but for most vSwitches, this setting can be left with the default setting.

The second option to configure is MAC Address Changes. This option is set to accept. When a virtual NIC is added to a virtual machine, it is automatically assigned a MAC address. The guest operating system can change the MAC address and will begin to receive traffic destined for the new MAC address. This can be required in some situations such as using Microsoft Network Load Balancing in unicast mode. Additionally, the iSCSI initiator relies on being able to get MAC address changes from some types of storage. If the setting is change to Reject, ESXi will not honor a request by the virtual machine to change the MAC address from the initial value.

The last setting on the Security tab is Forged Transmits. When the option is set to Accept, ESXi does not compare source and effective MAC addresses. To protect against MAC impersonation, you can set this option to Reject. With that setting, ESXi compares the source MAC address as generated by the guest operating system with the effective MAC address for the adapters and drops the

packet if there is not a match. This setting can impact applications that require a specific MAC address for licensing.

On the Traffic Shaping tab, you can set the traffic shaping policy for the vSwitch. This can be useful to ensure that a virtual machine is not used to saturate a vSwitch, which could create a DoS for other virtual machines or ESXi system services on that vSwitch. The traffic shaping policy is defined by the following three attributes: Average Bandwidth, Peak Bandwidth, and Burst Size. Average Bandwidth sets the bits per second to allow through the port averaged over time. Peak Bandwidth is the maximum number of bits per second allowed through the port when it is receiving or sending a burst of traffic. This setting, along with Burst Size, allows a vSwitch to transmit beyond the Average Bandwidth restriction. The Burst Size setting specifies the maximum number of bytes to allow in a burst of network traffic.

## 4. Conclusion

VMware vSphere is the most prevalent cloud computing system in industrial and business area. The security of vSphere engages many attentions from researchers and engineers. In this paper, we study the internal DoS attack in vSphere and propose corresponding defense mechanisms.

## References

1. Brian Hayes: Cloud computing. Communication of ACM 51(7): 9-11, 2008.
2. Subashini S., Kavitha V.: A survey on security issues in service delivery models of cloud computing. Journal of Network & Computer Applications, 34(1):1–11, 2011.
3. Alzain M A, Pardede E, Soh B, et al: Cloud Computing Security: From Single to Multi-clouds. IEEE 47th Hawaii International Conference on System Sciences: 5490-5499, 2012.
4. Sengupta, Shubhashis, V. Kaulgud, and V. S. Sharma. "Cloud Computing Security--Trends and Research Directions." Services: 524-531, 2011.
5. Cloud Security Alliance: The Notorious Nine: Cloud Computing Top Threats in 2013, Technical report, 2013.
6. VMware Inc. VMware vSphere Basics Guide. http://www.vmware.com/support/pubs.
7. VMware Inc. VMware vSphere Security Guide. http://www.vmware.com/support/pubs.