Network Security Threats and Cloud Infrastructure Services Monitoring

Murat Mukhtarov
Information Security Faculty
National Research Nuclear
University MEPhI
Moscow, Russia
milnat2004@yahoo.co.uk

Natalia Miloslavskaya
Information Security Faculty
National Research Nuclear
University MEPhI
Moscow, Russia
NGMiloslavskaya@mephi.ru

Alexander Tolstoy
Information Security Faculty
National Research Nuclear
University MEPhI
Moscow, Russia
AITolstoj@mephi.ru

***Abstract*—Today Cloud Computing and virtual infrastructure are one of the most popular ways to deploy application hosting and web-farm platforms. Cloud Infrastructure services also known as "Infrastructure as a Service" (IaaS) are the way to deliver computer infrastructure, typically virtual environment as a service. Distributed nature of IaaS and likelihood that different customers can use the same server and network deliver new security threats. Security of open source platforms of Cloud Services is discussed. Threats that impact on availability components of platform and customer separation features are shown. The distributed way of network security monitoring of availability and integrity of IaaS is described.**

Keywords-Cloud computing, Infrastructure as a Service, Virtual Infrastructure, Application Hosting, Network Security

I. INTRODUCTION

Infrastructure as a Service (IaaS) is the next-generation way to provide customers with IT resources on demand principle. Customers can buy as much "Infrastructure" as they need, i.e. "pay per use" axiom. This is a way to reduce operational expenses on IT and shift some of risks to outsourcing companies. Such type of service is very convenient for small-business and medium-size companies to get access for the novel IT technologies and collaboration services, but there are some security threats which occur in the cloud. The first main threat may happen when some customer's virtual private servers (VPS) use the same shared hardware and network devices with others customer's VPS simultaneously. In this case configuration errors may sometimes occur, hence some unauthorized access accidents may happen. Up to 31% data breaches in Australia involved third parties such as Cloud Computing (CC) IaaS providers [1].

The second one is the availability issue: business critical data and applications are stored in one place (as we say "all eggs are put in a same basket"). Large-Scale botnets are able to deliver DDoS attack to the biggest ISP and Hosting providers (Such as Bitbucket, Amazon EC2), so there are lots of the related risks: failure of the hardware, hypervisor software, guest software, network channels, etc. as a result of successful DDoS attack or system-wide failure [2].

One of the ways of Cloud networks monitoring is to use network telemetry principal with such protocols as Cisco Netflow [3] or IPFIX [4]. Design and architecture of the cloud provide opportunity to use Netflow/IPFIX probes on the hypervisor without performance reduction for the sake of the kernel-acceleration technologies (such as PF-RING in Linux Kernel). Another way to monitor connections inside IaaS cloud infrastructure is introduced in the paper. IPFIX protocol is very similar to Cisco Netflow v9, but it is not proprietary, open-standard and has some improvements [4], which can be used on open source systems such as Linux or BSD-derivate systems (FreeBSD, OpenBSD). IPFIX is flexible, lightweight way for basic network security monitoring such as connection control and volume-based traffic estimation [5].

II. CLOUD SERVICE INFRASTRUCTURE TYPICAL ARCHITECTURE AND THREATS

IaaS expands CC services from web hosting and application hosting to end-user services (e.g. virtual desktop workplace). Supporting such a service becomes possible for the sake of several novel technologies and new license agreements which are provided by some software vendors such as Citrix and Microsoft. On the other hand development of open source desktop systems (KDE, GNOME, XFCE, etc.), designed to run popular Linux distributions (Ubuntu, OpenSuse, Debian, Redhat), makes possible to use such systems as desktop environment on desktop virtualization applications. Open source platforms of Cloud Services like Amazon and Bitbuket consist of Hypervisor system, as usual it is Xen-based or Kernel Virtual Machine (KVM)-based hypervisors, storage component based on Linux Volume Manage (LVM) and OpenISCSI – IP Storage Network (IP SAN), external Internet channels and intercommunication network. Each component has its own security threats that should be monitored and controlled. We focus on threats which impact on availability components of platform and customer separation features. Cloud Service provides rather more services than traditional datacenters but there are also rather more surfaces of attack, such as data separation issue, shared storage and availability of platform in common. Therefore securing such a platform is more difficult task than securing perimeter-based traditional datacenter and the problem of monitoring of IaaS platforms is very complex. Data storage, storage network and interconnection network are shared between all customers of IaaS, also external network channels are common for all (Fig. 1). So attacker needs to compromise one of the components of IaaS platform, which are shared between customers to impact on the IaaS service in general. That is why it is important to use network security monitoring methods, which are to detect such impacts on transport network and shared network recourses in time.

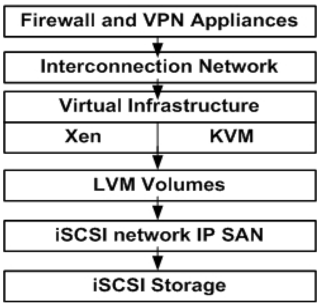


Figure 1. Architecture of open source software based IaaS platform.

A. External network channels

External network channels of nearly all datacenters including ISP’s (such as Amazon EC) are vulnerable for the DDoS attacks, because attackers use large-scale bot networks. Network channels become point of failure as well for datacenter of Cloud infrastructure in general, as for individual customer, because each customer’s network channel has finite bandwidth.

The second type of availability threat seems to be more difficult to detect and it requires distributed way of network security monitoring. Since such type of attacks is traffic volume based, the best way of lightweight monitoring of such type of attacks is using network “flow” protocols such as Cisco Netflow or IPFIX. Traffic streams from external network channels through access servers, usually going in VLAN, which is mapped to each customer, so the probe should be set on the enter point to the customers VLAN, for example on Broadband Remote Access Server (BRAS) or per Hypervisor. The second method is better for use since huge volume of flow data can impact on BRAS performance, but on the other hand using probes on each hypervisor machine can spread total load between virtual infrastructure servers.

Usually, external channels ISP’s use traffic scrubbers (Cisco Guard, solutions like Cisco-Arbor Cleaning Pipes, etc.) for protection. They have capabilities allowing them to distinguish between “good” and “bad” traffic. They mitigate DDoS attacks by forwarding only good traffic and dropping attack traffic [6]. Before going to clean bad traffic from good one, a scrubber has to identify bad traffic. Cisco and Arbor use for that purpose several techniques, but all of them are based on Netflow v5/v9 analysis opposite to direct traffic intercept. So it is possible to use best practices and principles of commercial solutions with open source IaaS platforms. There are lots of open source implementations of flow-based traffic collectors (ipcad, flowtools, ntop, nprobe, ndsad, flowd, Vermont, etc.), which could be successfully used for network security monitoring purpose in Virtual Cloud Infrastructure (VCI). Their advantage is ability to install them on open source hypervisor platforms (Linux-based Xen and KVM), opaque for customer’s software and without performance reduction.

B. Shared storage network

Shared storage network is a “point of failure” of whole IaaS infrastructure, also some iSCSI and volume mounting misconfiguration may impact on data separation between each customer and as a result some confidential data loss may occur. Usually open source Virtual Cloud is built on IP SAN (Storage Area Network) networks, because traditional FC SAN networks are rather expensive and it is not reasonable to use them in couple with open source software-based VCI. IP SAN network is based on iSCSI (Internal Small Computer Interface) protocol. iSCSI is an IP protocol that is a storage networking standard for linking data storage facilities. It is designed to carry out SCSI commands over IP networks, hence it could facilitate data transfers over local and external networks. Unlike traditional FC SAN, which requires special-purpose cabling, iSCSI can be run over long distance using existing network infrastructure. But using iSCSI is associated with several security threats: unauthorized accessing iSCSI Logical Unit Number that makes it possible to mount iSCSI running storage devices; authentication bypassing using some of attacks on CHAP protocol that is used to authenticate iSCSI peers; bypassing logical network isolation through VLAN misconfigurations or VLAN hopping attacks.

Taking that into account it can be concluded that customers cannot be sure that their sensitive data inside IaaS Cloud is safe. To improve data storage security, IaaS provider should monitor this threat by using some mechanisms, based on internal Linux/Unix system logging, such as syslog and mount table control scripts, and controlling VLAN separation Flow-based network measurements.

C. Shared internal network devices

Shared network devices also become one more point that needs to be controlled. Their main security risks are VLAN policy misconfiguration issues and VLAN hopping issues. As a result the separation between customers may be breached. Thus some customers may be able to have unauthorized access to essential data, stored on network resources on Virtual Service Infrastructure, Data Bases, Internal Web Portals and so on.

Another type of those threats is manipulation with Layer 2 functions of the switches, like an ARP poisoning, CAM table overflow etc. The result of such manipulations maybe unauthorized traffic interception and some sensitive data may be stolen. To avoid those risks some Layer 2 securing techniques such as “port-security”, DHCP Option 82, port authorization with 802.1x, virtual LAN with 802.1q are usually used. But sometimes configuration errors occur. For example there are several typical misconfigurations: native VLAN usage that equals 1; using 802.1q ports for customer link with native VLAN configured; allowing connections to one customer to VLAN's of others; 802.1x VLAN mapping errors – as a result of authorization process customer able to access prohibited VLANs.

The greater the size of the Virtual Infrastructure is, the more the likelihood of misconfigurations will be. Thus, the main tasks on network security monitoring of Virtual Infrastructure are to detect and to notify about separation failures. To control integrity of separation policy it is also convenient to use one of the flow-based monitoring protocols such as Netflow or IPFIX, but they should support "VLAN-ID" field in the flow template.

III. MONITORING NETWORK SECURITY AND POLICY INTEGRITY IN VIRTUAL SERVICE INFRASTRUCTURE

IaaS services's complex and tenant nature oblige service providers to use complex way of monitoring network security of their clients. In addition to traditional IDS, which have perfect present experience of known signatures' detection, the service provider must be able to detect availability threats such as DDoS attacks and anomaly network traffic flows, which may occur as a result of misconfiguration. In this view, it is very important to keep separation between customers' VPS and virtual networks.

There are several technologies, used in virtual infrastructure networks: separation of customers in own VLAN (802.1q VLAN) and isolating customers' services inside virtual appliance, controlled by hypervisor. Some of network vendors also support transport network technologies such as MPLS/VPLS network, MAC-in-MAC technology providing another separation methods for private networks. But such services are adapted to be opaque to an end customer. There are two main security threats - cloud availability (robustness against DDoS attacks) and shared network devices and hardware controlling. So we propose to monitor and detect such threats at an early stage, using IPFIX or Netflow v9 protocols, which are very similar.

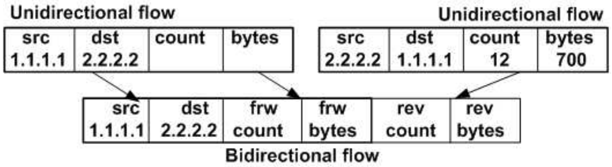
A. Flow-based measurement

Netflow v9 or IPFIX provides useful information for security analysis such as IPv4/IPv6 headers, source IP, destination IP, source port, destination port, TCP flags, TOS, QOS, volume of traffic per flow, direction of the flow, interface, AS number and some additional ISP specific information: VLAN number, MAC address, MPLS labels. There are lots of techniques and software of flow analysis, based on analyzing Cisco Netflow v5/v9 data, namely ntop, nfsens, nprobe, flowd and some commercial products, e.g. Cisco MARS. However, it is not reasonable to use commercial implementations of Netflow collectors and security tools on open source cloud platforms.

One of the main IPFIX/Netflow v9 protocol advantages is its bidirectional flow (or bitflow), allowing tracking full connection opposite to Netflow v5. Trivial examples of biflow applications include initial round trip time (RTT) estimation, detection of connection establishment or other transactions for the purposes of an incident detection and response, and the separation of unanswered traffic for scan detection purposes [5].

Bidirectional flow measurement is very useful for a network security application, since it provides information about full connection that makes it possible to analyze each stage of the connection establishment for TCP protocol and track client responses for UDP protocol. For example, it is very useful to monitor and track HTTP and DNS connections and detect deviations in those connections, like scans or Flood attacks. In contrast to usage of unidirectional flow it provides information initiation and end of connection that enables to monitor and control integrity of this first initial dialog establishment success.

Bidirectional flow principle also reduces traffic that generates netflow/ipfix probe in a way as shown in Fig. 2.



src	dst	count	bytes
1.1.1.1	2.2.2.2		

src	dst	count	bytes
2.2.2.2	1.1.1.1	12	700

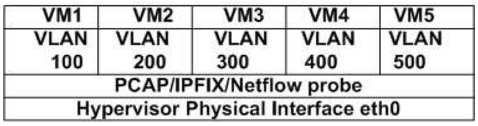
src	dst	frw count	frw bytes	rev count	rev bytes
1.1.1.1	2.2.2.2				

Figure 2. Unidirectional flow and Bidirectional flow.

Thus it is reasonable to use flow-based measurement for VCI monitoring problem.

B. Flow probes placement in Virtual Infrastructure

Flow-based measurement protocols are very convenient for classification and traffic volume analysis. Fig. 3 shows that netflow/ipfix probes can be placed in VCI network.



VM1	VM2	VM3	VM4	VM5
VLAN 100	VLAN 200	VLAN 300	VLAN 400	VLAN 500
PCAP/IPFIX/Netflow probe				
Hypervisor Physical Interface eth0				

Figure 3. PCAP/Flow probe can be set on physical interface of Hypervisor machine.

Thus by using open source software IaaS providers are able to apply powerful tools to monitor network security (nfsen, ntop, flow-tools, Vermont, etc). So it is possible to use libpcap library compatible Netflow collector with virtual network interface card such as "tap" or "tun" Linux interfaces. Here it is an example with fprobe and nfdump on each virtual interface:

```
Linux# fprobe –itap0 –fip nfdump_host:9000
Linux# fprobe –itap1 –fip nfdump_host:9001
Linux# fprobe –itap2 –fip nfdump_host:9002
```

or on main physical interface:

```
Linux# fprobe –ieth0 –fip nfdump_host:9996
```

There are a lot of network devices vendors which support Cisco Netflow v9 or IPFIX protocols. It is possible to analyze flow-data that contains VLAN-ID field on the following Cisco network switches: Catalyst 4000/4500 and 6000/6500, but additional Netflow module is a prerequisite. On the other hand lots of vendors support IPFIX/Netflow v9 flow export out of box, such as Nortel, Extreme Networks, Juniper, etc. So it is not very difficult to check separation policy integrity with Netflow v9/IPFIX enabled on such a switching device. To make Cisco Router exports VLAN-ID field within flow-data typing IOS, cli command is needed:

```
Router(config)# ip flow-capture vlan-id
```

It is possible to export VLAN-ID field within IPFIX/Netflow v9 data on Linux host to use nProbe collector:

```
Linux# nprobe –n nfdumphost:9996 –i eth0 –T “ %SRC_VLAN, %DST_VLAN, %IPV4_SRC_ADDR, %IPV4_DST_ADDR, %IN_SRC_MAC, %OUT_DST_MAC”
```

This is lightweight and chip way to monitor virtual interfaces inside Linux-based Cloud systems, which can be implemented in the current network architecture. On the other hand Netflow v9/IPFIX enables to monitor VLAN ID in traffic flows, which allows network administrator to control integrity of separation between IaaS provider’s customers. VLAN ID monitoring using flow-based protocols makes it possible to detect and inform a security officer about network separation misconfigurations in time.

To provide excess coverage VLAN information travelling network it is important to use flow probes on a Hypervisor host as well as on network equipment. Each Hypervisor host has its own Flow probe that exports data to a collector, where VLAN information should be analyzed and compliance control should be performed.

It makes it possible to have information about whole VLANs in one place. It is no sense weather trunk interface or access VLAN interface using on Hypervisor host.

C. *Flow analysis methods and tools*

There are lots of statistical methods of volume-based raw traffic analysis, based on classification, abnormal behavior, baseline methods, detection of anomalies and deviations [7]. Most of them can be used to analyze Netflow/IPFIX data. Basically Netflow analyzing process is reduced to find one of several data sets: Top N and Baseline; Top N Session; Top N data; Pattern matching: port matching, IP address matching. TopN principle allows finding a source of activity that cause anomaly, worm attack, flood attack and it is based on volume deviations estimation. One of the lightweight flexible ways to implement IPFIX/Netflow v9 flow-data analyzer with its own analysis algorithm is to use Perl Flow.pm library [8].

It is better to use accomplished solution that could be built by means of combing several open source software. Open source tools such as nTop and nfsen provide functionalities to set threshold values of some traffic types. They provide information about volume (e.g. http, dns, Mircosoft-RPC traffic, etc). Increase of one traffic type in time can be easily monitored without drastic impact on performance of network equipment, virtual appliance or hypervisors software. Open source nfdump utility can be used for TopN analysis. There are several internal implementations of TopN with “-s statistics” option:

```
Linux@root# nfdump -M /netflow/directory -R file1:fileX –s srcip/dstport/pps/packets/bytes ‘dst port 80’ –O bytes
```

Obviously those output entries, which exceed regular values, may signify some network traffic inconsistency or network attack. Arguments of nfdump tool shown above enable it to detect DDoS attack against Web server. Centralized data management of flow-probes and IDS, like SNORT project, can be implemented using open source session-based network data correlation engine Prism++ [8].

In order to detect VLAN separation flow-data should be analyzed. It is possible to keep table of mapping customer’s subnets and VLAN-ID’s. Each incoming Flow should be aggregated by VLAN-ID field. Then it is possible to detect separation breach by means of comparing each aggregated flow with VLAN-ID – Subnet mapping table. If unauthorized network subnet in the given VLAN-ID is detected, comparator notifies about separation issue.

The described scheme of IPFIX/Netflow v9 data analysis provides opportunities for lightweight and efficient detection of network security issues, related to multicustomer VCI Servicesdiscussed above.

D. *Impact on hypervisors perfomance*

Flow collection is rather lightweight technique of network security monitoring. It achieves good performance results for several reasons: no need to intercept whole traffic traveling across the network and no need to analyze whole network packet – only headers information.

Flow analysis provides a network administrator or a network security officer with traffic volume-based quantitative evaluation.

Also Netflow sensor, implemented in Cisco routers and firewalls, also does not cause major impact on performance. For example, Cisco Systems provides following performance evaluation for 65000 flows Netflow v9 and 8903 packets per second :

Cisco 7200 Platform with NPE G1 CPU utilization	9 %
Cisco 7200 Platform with NPE G2 CPU utilization	8 %
Cisco 3845 Router	9 %
Cisco 2811 Router	53 %

Figure 4. Cisco Routers CPU utilization for 65000 Netflow v9 flows [10]

Here is an approach of evaluation performance impact on Hypervisor running 3 virtual machines with following initial data - 1 Virtual CPU, 256 RAM, 5Gb Virtual Device HDD, 100 mbp/s Virtual NIC, System Debian Lenny, also Apache is running.

Hypervisor configuration is one Intel DualCore E8400 Processor, with 2048mb RAM and 500Gb HDD without RAID.

For testing purpose we used file with size 1024mb, that was took from dd command:

Linux@root# dd if =/dev/zero of=/var/www/test_root/test.iso bs=1M count=1024

So we stressed Web server, trying to send GET requests to this file until Apache web-server forked enough childs (worker model) to take 80 % of CPU usage.

So we make comparison results with running and not running nProbe collector on Hypervisor system of CPU load Hypervisor System. Here are the tables for Hypervisor CPU Load without and with nProbe collector (fig. 5 and fig. 6 correspondently):

CPU Load	Hits per minute
22%	174 hits/minute
25%	243 hits/minute
34%	312 hits/minute
51%	362 hits/minute
74%	486 hits/minute

Figure 5. CPU Load of web server for hits per minute without nProbe running

CPU Load	Hits per minute
20%	171 hits/minute
26%	247 hits/minute
33%	311 hits/minute
52%	372 hits/minute
75%	492 hits/minute

Figure 6. CPU Load of web server for hits per minute with nProbe running

It seems that general impact on CPU is caused by Apache worker process. nProbe collector process in top –S output, always takes 0 % of CPU time.

To measure CPU load and Hits per minute we use Apache mod_status and net_snmp packages. For controlling we checked out CPU usage with top Unix-command and Nagios nrpe sensor.

Accuracy of results is not very high, we use rough estimates, but for evaluation performance of flow analysis that should be enough.

It is obvious that CPU usage impact will be noticeable only on huge amount of traffic – like thousands packets per second. Traffic rate is not very high in common web applications and low performance virtual platforms. Real CPU usage impact may occur only for flow analysis, performing on ISP equipment such as backbone routers.

IV. Conclusion

VCI services have several security issues and attack surfaces: customers use the same external network channels, shared network devices (separation is implemented via VLAN technologies), storage network and hardware. It is important to monitor and control availability of customers' virtual appliance and keep customers, separated in Virtual Infrastructure network. Flow-based measurement protocols such as Netflow v9/IPFIX are suggested to monitor separation of the customers, by means of controlling VLAN-ID in each flow and mapping it to the customer. Netflow v9/IPFIX flow-data analysis also provides opportunities for monitoring deviations of several types of traffic that may occur as a result of DDoS attacks or some network worms' activity inside or outside IaaS platform infrastructure. This way of monitoring network security of open source software, based VCI, is more productive and easy to implement in existing Virtual Clouds due to design and implementations of Netflow v9 and IPFIX protocols.

References

[1] Tay L. and Kotadia M. Data breaches to cost more in the cloud http://www.securecomputing.net.au (2010). (23 March 2011)

[2] McNamara P. DDoS attack against Bitbucket darkens Amazon cloud http://www.networkworld.com (2009). (23 March 2011)

[3] Claise B. RFC 3954 Cisco Systems Netflow Services Export Version 9 (2004).

[4] Claise B. RFC 5101 Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information (2008).

[5] Boschi E. and Trammell B. Bidirectional Flow Measurement, IPFIX, and Security Analysis pp. 8-10 (2006).

[6] Ramachadran V. and Nandi S. Bleeding Edge DDoS Mitigation Techniques for ISPs pp.8-9 (2004).

[7] Shanbhag S. and Tilman W. AnomBench: A Benchmark for Volume-Based Internet Anomaly Detection pp. 1-3 (2009).

[8] Kobayashi A. Net::Flow - decode and encode NetFlow/IPFIX datagrams http://search.cpan.org/~akoba/Net-Flow/ (2008). (24 March 2011)

[9] Dresslerand F. and Carle G. "HISTORY-HighSpeedNetworkMonitoring and Analysis," in 24th IEEE Conference on Computer Communications pp.2-4 (2005).

[9] Netflow Perfomance Analysis, Technical White Paper, Cisco Systems (2007).

ISBN: 978-1-61208-133-5