Security evaluation of network traffic mirroring in public cloud

Authors
Vipul Sharma, MSc (Royal Holloway, 2020)
Dimitris Tsaptsinos, ISG, Royal Holloway

Abstract

Analysis of network traffic plays a key role in overall security of an enterprise. The network traffic is often captured, monitored and analysed to detect and prevent attacks, investigate performance issues, comply with regulatory and compliance requirements and to carry out network forensics.
This paper examines the network monitoring technique called *network traffic mirroring*. Network traffic mirroring has been around for a long time in on-premises setup but is relatively new in public clouds. We demonstrate how network traffic mirroring is being implemented in public cloud and the challenges the technique faces due to the inherent characteristics of the public cloud. We also demonstrate that the security challenges, if not addressed, can be detrimental to the security posture of an enterprise.[a]

[a] This article is based on an MSc dissertation written as part of the MSc in Information Security at the ISG, Royal Holloway, University of London. The full thesis is published on the ISG's website at `https://www.royalholloway.ac.uk/research-and-teaching/departments-and-schools/information-security/research/explore-our-research/isg-technical-reports/`.

Network Traffic Mirroring - The concept

The term "network traffic mirroring" consists of:

- **Network**: a connection between two or more computers. The most common purpose of a network is to share resources. This connection between computers can be created using wired connectivity or it can be wireless. In public cloud environment, there is a concept of VPC - Virtual Private Cloud i.e. virtual implementation of the physical network.
- **Network traffic**: the flow of data (network packets) between the source and the destination.
- **Mirroring**: the technique of copying the network traffic from the source system to another system.

Hence *network traffic mirroring* is the technique involved in copying the network data from one source onto another.

Network traffic mirroring comes under a broader concept of *network traffic monitoring*. Network traffic monitoring consists of techniques in which the network traffic is observed to provide deeper insights into network data. Network traffic monitoring has been a very effective tool, and some of the most common ways to monitor network traffic include port mirroring, flow observation, packet capture and inspection.

In an on-premise environment, network mirroring is often referred as port mirroring or SPAN (Switched Port Analyser). Some common approaches to configure port mirroring in on-premise setup are described in the following.

SPAN is a technique used on switches wherein traffic from one port on the switch is copied onto another port on the switch thereby creating a mirrored copy of the network data. A switch can be configured to either copy the traffic sent on one switch port or for the entire Virtual LAN.

A TAP (Terminal Access Point) is a device that is used to capture network traffic flowing from one device to another. Although there are software versions of TAP available, TAP is mostly associated with being a hardware device.

A TAP usually consists of 3 ports: A port, B port, and monitor port.

SPAN components:

- Switch
- Source port
- Destination port
- Ingress traffic
- Egress traffic

Figure 1 shows that the network traffic flowing between device A and device B is passing through the TAP device and is being copied to the monitoring device for analysis.

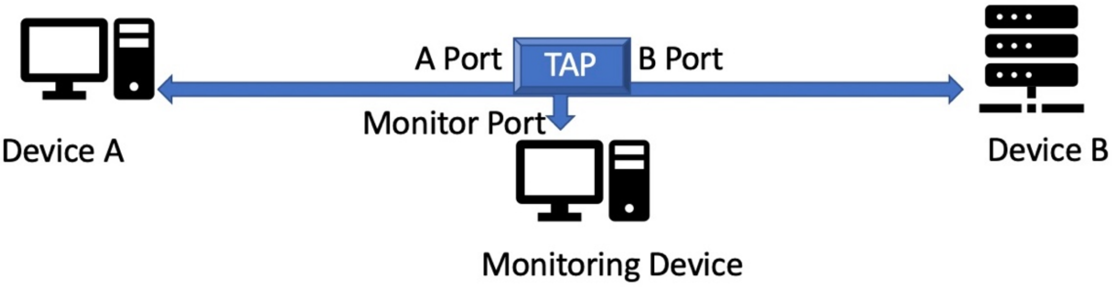

Figure 1: TAP configuration example.

As with the implementation options in on-premise environment, there are different ways in which network traffic mirroring can be carried out in public clouds too.

Network traffic mirroring in public cloud can be carried out at:

- **vNIC level**: In a cloud (virtual) environment each networking device including a virtual machine is assigned a virtual network interface card (vNIC). Like a hardware NIC, the vNIC also is assigned an IP Address in order to enable it to communicate in the network (i.e. send and receive network packets). In this scenario, network mirroring can be configured in such a way that the traffic sent and received by this vNIC is replicated to another interface (vNIC)

  Figure 2 shows that the network traffic received and sent by the virtual interface vNIC1 on VM1 is being mirrored across to the monitoring device. The network traffic on the other two virtual machines (VM2, VM3) is not being mirrored.

- **Virtual machine level**: In case of port mirroring being configured on a virtual machine; the network traffic sent and received by this virtual machine can be copied onto a monitoring device. It is up to the configuration whether you want to copy all traffic, incoming traffic or just the outgoing traffic. If a virtual machine has more than one virtual network interface a separate mirroring policy would need to be created to mirror the traffic on the other interface.

- **subnet level**: While implementing network mirroring in public cloud, settings can be configured to replicate the entire network traffic that is being sent and received on a particular subnet within a VPC. This would mean traffic sent and received by all computing instances within that subnet will have their network data copied onto another device.

  Figure 3 shows that the network traffic received and sent in the subnet (all virtual machines on all hosts shown i.e. VM1, VM2, VM3 on Host1, VM1, VM2 on Host 2 and VM1, VM2, VM3 on Host 3) is mirrored across to the monitoring device.

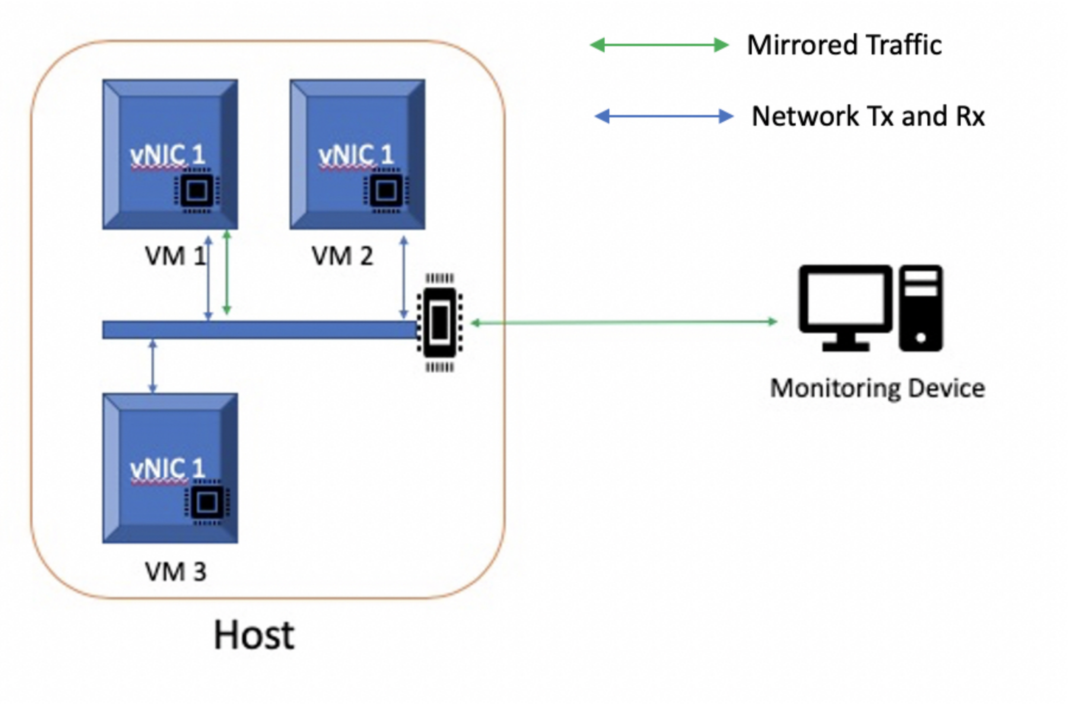

Figure 2: Network traffic mirroring on a vNIC.

Network traffic mirroring in public clouds

What is public cloud?

Public cloud is a cloud platform where cloud service providers provide computing services like Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS) over the public internet. These services are normally billed on a pay as you use basis but increasingly cloud service providers are offering discounts when service usage is committed in advance.

What's happening in the public cloud?

To understand and analyse the network traffic, public cloud providers have now started offering network traffic mirroring on the cloud as well. The concept is essentially the same as in case of the on-premises technique wherein data traffic is replicated for the source to the destination. However the implementation in public cloud environment is different as the network defined for the consumers (enterprises using the public cloud services) is using software. In a public cloud environment setup the tenants (consumers) have the choice to enable network traffic mirroring on their compute instances as well as the ability to mirror entire subnet's network traffic onto another device which could be a packet analyser or an intrusion detection system.

The objective of the project was to carry out a security evaluation of network traffic mirroring technique in a public cloud environment since this is a relatively new technology and is being offered by only a few cloud service providers.

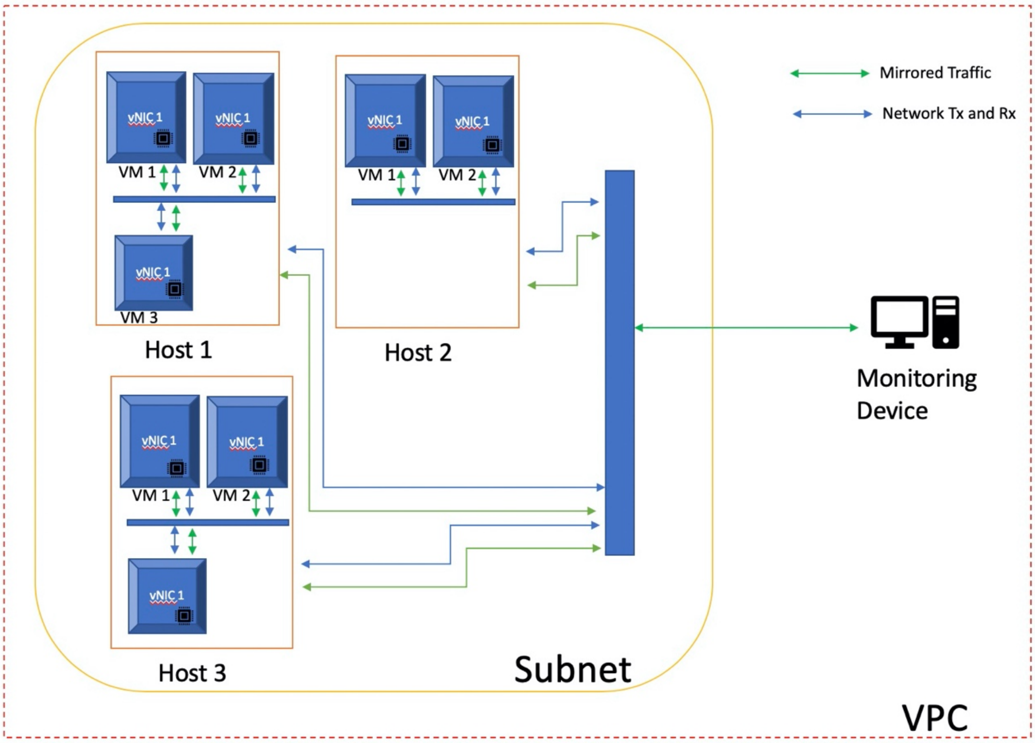

Figure 3: Network traffic mirroring in a subnet.

Experimentation

To evaluate security and to determine the reliability of this technology an experiment was carried out on two public cloud environments. The core of the technology is the same, that is, network traffic is mirrored from the source machine to another machine referred to as mirroring target or mirroring destination. However, the way the technique is implemented is different. (The full dissertation described the merits and demerits of each.)

Here we describe the experimentation of network traffic mirroring across public cloud environments and evaluate the test result. The experimentation conducted involved looking at the weaknesses of the techniques used on public cloud to carry our network traffic mirroring.

The experiment focussed on three most used protocols (ICMP, HTTP and DNS) and was carried out in three separate scenarios:

- Examining ICMP traffic: Network traffic generated using the `ping` command.
- Examining HTTP traffic: Network traffic generated when accessing a web page.
- Examining DNS traffic: Network traffic generated using a DNS lookup.

Lab environment setup

To carry out the experiment a lab environment was setup that was used to carry out the security evaluation of network traffic mirroring techniques across two public cloud services providers. At the time of carrying out this project, network traffic mirroring is offered by three cloud service providers namely: Google Cloud Platform, Amazon Web Services and Microsoft Azure.

For the experiment we used Google Cloud Platform (GCP) and Amazon Web Services (AWS) as both were offering network mirroring capability natively. In the case of Microsoft Azure, the offering was in preview mode and required going through an enrolment process.

Detailed setup and configuration of the lab environment can be found in the full dissertation.

Result summary

The main observations made and potential weaknesses discovered in this experiment are:

1. Inability to mirror DNS traffic.
2. Challenges with autoscaling of the mirror source node.
3. Challenges with addition of a new virtual network interface.

The network traffic mirroring experiment showed that the network traffic for ICMP and HTTP is mirrored across from the mirror source instance to the mirror destination instances. However, in both the test environments it was discovered that the DNS traffic does not get mirrored across from mirroring source to the mirroring destination.

Figure 4 gives a graphical representation of the experiment carried out for network traffic mirroring on the public cloud setup for AWS and GCP.

The green arrow represents ICMP traffic, the blue arrows represent the HTTP traffic and the red traffic represents the DNS traffic.

Data exfiltration using DNS

The seriousness of this was proven in the next experiment: we managed to carry out data exfiltration using DNS traffic. We exfiltrated data from the mirror source instances in AWS and GCP onto a DNS server (ns1.exfilrus.net, ns1.exfilrus.com and ns1.exfilrus.org) set up for this experiment. As the DNS traffic is not mirrored across, there is no record of this on the mirror destination instance in both AWS as well as GCP.

Countermeasures

As demonstrated by the data exfiltration using DNS, the lack of mirroring of DNS traffic in the cloud setup is a weakness that needs to be addressed. We propose a few countermeasures that can be introduced to address this weakness in public cloud setup

- Addressing the DNS network traffic mirroring in Google Cloud Platform:

  Specifying the DNS server name along with the DNS query.

- Addressing the DNS network traffic mirroring in Amazon Web Services:

  There are two ways in which the DNS traffic can be mirrored from the source instance to the destination:

  - Specifying the DNS server name along with the DNS query.
  - Specifically adding the DNS check with the Mirroring Filter.

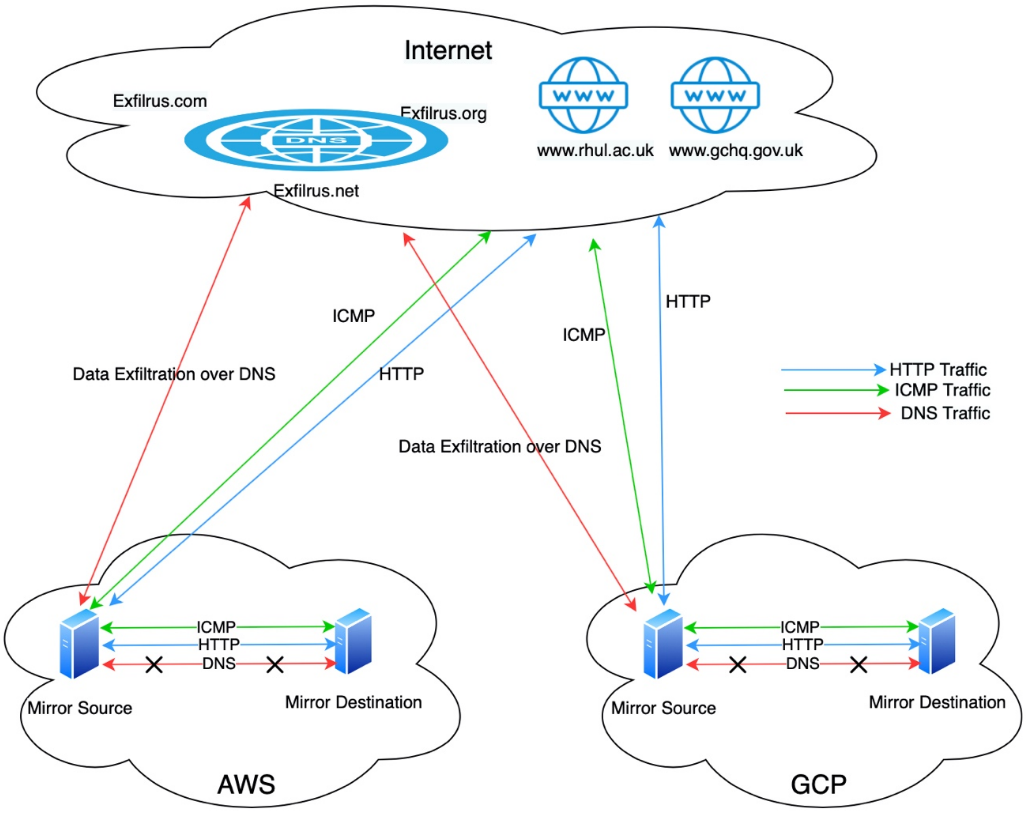

Figure 4: Network traffic mirroring experiment summary.

- Addressing the changes due to addition of a new instance due to autoscaling:

  In a scenario where a new instance is added for the application that is part of an autoscaling group, a serverless function can be setup which invoke the necessary APIs to create the mirroring setup components in order to start mirroring network traffic from this newly added virtual instance.

- Addressing the changes due to addition of a new network interface card:

  Another weakness identified was that when a new virtual network interface card(vNIC) is added to an instance the traffic mirroring for that newly added vNIC is not mirrored automatically. One way to address this is by creating a new mirroring policy (target, session and filter) when a new vNIC is added to the instance. This can be automated using serverless functionality like lambda (AWS) and Cloud functions (GCP) wherein an event will be triggered when a new vNIC is added to the source instance. This in turn invokes a serverless function to create a mirroring policy to include the newly added network interface card as a source.

Conclusion

Our experiment found that network traffic mirroring in public cloud is a relatively new technology and while it offers various advantages for analysing and monitoring network traffic, it is not yet a mature technology and has some major flaws, including the inability to mirror DNS traffic. In the experiment this flaw was exploited to carry out data exfiltration thus highlighting this serious security drawback.

We also suggested ways in which this situation can be addressed. However they come with some restrictions and needs to be evaluated based on individual requirement.

Further improvements in the design and implementation of network traffic mirroring in public cloud are required to ensure that mirroring technique mirrors all required network data reliably.

Biographies

Vipul Sharma s an IT professional with over 20 years of experience in designing and security enterprise IT. He has vast experience in working with enterprises and helping them use technology effectively to solve business challenges. He holds various certifications including the CISSP and CCSP. He completed the MSc in Information Security from Royal Holloway University of London with distinction. He is also a committee member of British Standards Institute (BSI) IST/33/1 - Information Security Management Systems

Dimitris Tsaptsinos is a visiting tutor at Royal Holloway since 2017, following his retirement as an Associate Professor at Kingston University, in the school of School of Computer Science and Mathematics. He designed, developed and directed an undergraduate degree in Cybersecurity and Computer Forensics. He was awarded the Kingston University Teaching Fellowship in 2008. The fellowship recognised achievements in teaching and support for learning. He has acted as an external examiner for Staffordshire University, for the MSc Forensic Computing course, and Sheffield Hallam University, for the BSc Computing and Network Engineering. He has acted as Phd examiner for universities in the UK, Italy and France and has more than 50 publications.

Series editor: S.- L. Ng