Hybrid Security Evaluation

Mohamed Elfiky[a], Mohamed Azab [b], Magda Madbouly[a], Walaa Sheta and [b], Adel El-Zoghabi[a]

Abstract— Cloud computing uses the internet in public cloud or intranet in private cloud, remote servers for manipulating data and applications hosted by cloud service providers CSP. The backbone of cloud computing is virtualization. Cloud computing security is the main concern for CSP and end users. The implication of cloud computing is security; virtual machines (VMs) surface flatness, share the same resources for different users. The virtualization security challenges are inherited either from traditional attacks like (flooding, DDOS) or virtualization specific attacks like (Virtual botnets). This paper introduces a security evaluation of Hybrid security scheme that designed and developed in the virtual environment. This evaluation for virtual network traffic study, launching brute force attacks, Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attacks on critical VM at the same time. The study of virtual network done twice, the first one is before launching the attacks and the second after launching the attacks. Evaluating scalability of Hybrid Security by lunching previous attacks on many VMs in the virtual network. The distinctive in this paper than others, which is performing attacks and studying virtual network traffic during attacks.

.

Index Terms— Cloud computing, virtualization, Hybrid Security, Security management, cloud computing security, virtual network stress, and virtualization security evaluation.

1. INTRODUCTION

Cloud computing extract from a need. The enormous growth of the Web over the last era has raised the new class of web requirements such as millions of search queries a day supporting thousands of concurrent e-commerce transactions or. The natural response of technology companies has been to build increasingly large data centers to handle the ever-growing load; these data centers consolidate a great number of servers (hundreds, if not thousands) with associated infrastructure for storage, networking, cooling, etc. Over the years, technology companies, especially Internet companies such as Google, Amazon, eBay, or Yahoo!, have acquired a massive amount of expertise in operating these large data centers. This "know-how" extends beyond physical infrastructure to include experience with process management. Cloud computing represents a commercialization of this combined solution [1].

This cloud model is composed of five essential characteristics, three service models (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)) and four deployment models (Private cloud, Community cloud, Public cloud and Hybrid cloud) [2].

NIST define cloud computing essential characteristics as the following [3]:

On-demand self-service, a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access, the capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants [PDAs]).

Resource pooling, the provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Measured Service, the cloud systems automatically control and optimize resource utilization by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts) [4].

Service Models, Nowadays everything as a service denoted by *aaS for example security as service and Desktop as a Service but the following services are standardized from NIST. Software as a Service (SaaS), the capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Platform as a Service (PaaS), the capability provided to the

Mohamed Elfiky is currently pursuing Ph.D. degree program in information technology in Alexandria University, Egypt, PH-+201120000801 E-mail: mo.elfiky@gmail.com

a. Alexandria University, Institute of Graduate Studies and Researches (IGSR), Information Technology Department, Elshatby, Alexandria, Egypt

b. City of Scientific Research and Technological Applications, Institute of Informatics, Borg Elarab, Alexandria, Egypt.

consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

Infrastructure as a Service (IaaS), the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications [4]. NIST defined deployment models into four deployment models for cloud computing.

Private cloud, the cloud infrastructure is operated solely for an organization that may be managed by the organization or a third party and may be exist on premise or off premise.

Community cloud, the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). Can be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud, the cloud infrastructure is made available to the public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud, the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). This paper can classify this work as Security as a Service, so the security delivered as service for VMs that would be protected.

We evaluate a security robustness of Hybrid security scheme that designed and developed in virtual environment. This evaluation for virtual network traffic study, lunching brute force attacks, Denial of Service (DoS) attack and Distributed Denial of Service (DDoS) attacks on critical VM at the same time. The virtual network traffic studied two times, the first one is before launching the attacks and the second after lunching the attacks. Evaluating scalability of Hybrid Security by lunching previous attacks on many VMs in virtual network. The distinctive in this paper than others, which is performing attacks and studding virtual network traffic during attacks.

The rest of paper composed of section, which is studying the related work. Section three is the proposed work, which contains lunching attack and virtual network studding

2. Related Work

Jarraya et al developed multi-stage defense-aware security modules placement in the Cloud [5], which is depends on security deployment node. This node sort the security modules into category to select the workflow pattern. The category is divided into segments and these segments are allocated to deferent group of network nodes in the network. Every segment is assigned to security module to a network node and this assignment is calculated. The network is configured according to this assignment.

This multiple security module did not developed or evaluated.

One type of defense against hypervisor attacks in the cloud computing using Hypervisor-based Intrusion detection system. This is located between the hypervisor and guest of kernel and created by Hypervisor-based IDS. The kernel is protected using this security layer. The system metrics in the cloud is observed by Hypervisor-based IDS to detect any threats. In addition, Hypervisor-based IDS monitors the communication between hypervisor, VMs and virtual network. These security techniques developed inside the hypervisor and did not evaluated [6].

Merging VM and hypervisor intrusion detection system is proposed for detecting and preventing hypervisor attacks in cloud environment. VMHIDS adopts treats features inspecting tasks, which occur frequently and prevent suspicious event [7].

Shreyal Gajare and Shilpa Sonawani design Virtual Machin Host based Intrusion Detection System (VMHIDS) to monitors computer system and prevent suspicious internal traffic on VM. VMHIDS considered as agent to analyze internal or external traffic that try to spoof system's security policy

3. Proposed System

This section explore the related work

Security performance test is related to previous work in other paper. Hybrid portable security for cloud computing, designed to mitigate attacks on virtual network traffic. This Hybrid security scheme composed of virtual firewall (vFW) and virtual network intrusion detection system (vNIDPS) embedded on the hypervisor as Virtual Machines and integrated together. This Hybrid security scheme achieves multiple goals in security concerns like portability; moved across different types of hypervisors, scalability that can applied on any VM in the virtual network. The architecture of virtual network represented in Figure 1, which is developed and implemented to achieve security on the virtual environment and mitigates different types of attack.

Many researcher developed The next section will examine this hybrid security and perform security performance test. The previous section explores the hybrid security representation that created in the virtual environment.

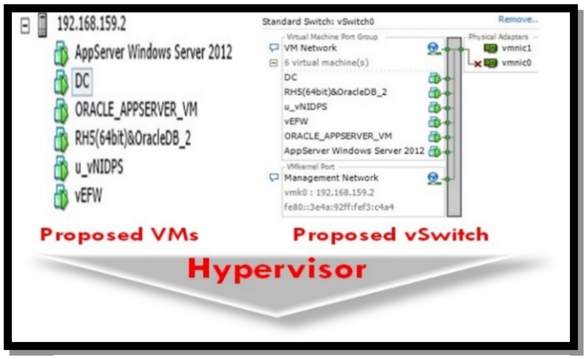


Fig. 1 Virtual Network Representation

Figure 2 illustrates the hybrid security mechanism: the first layer is virtual firewall to enforce the security police in virtual traffic and outside traffic comes from cloud user's requests. Virtual firewall examines IP address for virtual machines, blocks modifying routing table and preventing MAC Spoofing for VMs.

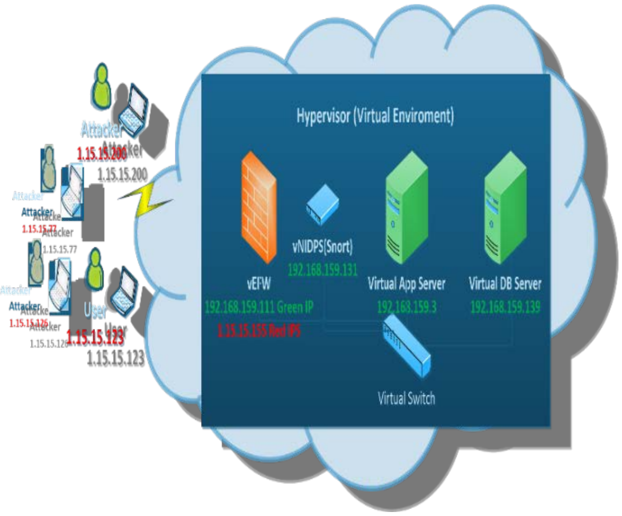


Fig. 2 The Schematic Representation of Hybrid Security Performance Test

Integrate Firewall rules with vNIDPS rules to achieve system security integrity. The second layer is vNIDPS this layer implemented between virtual firewall and target VMs to be protected. vNIDPS has two jobs first job is detecting and monitoring virtual traffic packets path between VMs themselves and incoming virtual traffic and sends alerts for ping or ICMP or ARP requesting. The second job is dropping suspicious packets based on rate filter rules that comes to virtual application server. Adding Green IPs in virtual firewall to whitelist in vNIDPS to prevent conflicts between in vNIDPS and vEFW. Using the vNIDPS mitigates DDOS attacks. Security performance test to ensure that this hybrid security is performing well.

3.1. Security Evaluation Test

Planning to measure the security performance is very important to validate that the scheme is working perfectly and protect the virtual environment. The security test plane made to ensure that this hybrid security performing well and achieves the purpose of its creation. After adjusting filtering and prevention rules in the hybrid security, we design several attacker machines in virtual environment (VM) and some of them are physical machines.

The security test plane depends on different methods and materials. Using kali rootkit built on VMware workstation as attacker VM to perform brute force attack on valuable virtual application server, Meta-exploit to find the vulnerabilities in application server` VM, nmap to perform brute force authentication Wireshark for sniffing virtual traffic and Low Orbit Ion Cannon (LOIC) to simulate DOS and DDOS attacks.

3.2. Generating Attacks

Before generating attacks on the virtual system, knowing virtual system vulnerabilities is must to start the attacks. Metaexploit used to detect the virtual system vulnerabilities specially the virtual application server using “search type: exploit” on victim VM. Port scan is made for victim VM to know the open ports and not used.

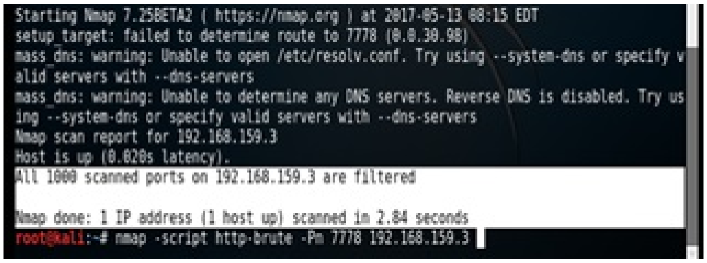
Creating First Attacker Machine (VM Linux based). All attacker outside LAN IPs classified as (Red IPs) classified in the hybrid security. Using a root kit to perform http-brute force attack on the victim VM (application server).

Other attacks type on virtual network that we generates using DOS, DDOS and ICMP flooding generating tools. Several tools can generate DOS and DDOS attacks. According to InfoSec Institute classified DOS and best attacking tools [8], LOIC tools has been chosen because it is classified as the best tools, open source network stress testing tool , anonymous used it as DOS and DDOS attacking tools.

The advantage of using LOIC that is runs on both Microsoft Windows and Linux OS and also is flooding tool used to generate a huge volume of network traffic to utilize virtual network or virtual machine application resources. This attack target the valuable VM by flooding it with promiscuous TCP, UDP, or HTTP packets. These attacks generated on victim server for 48-hour test and using several zombies. All attacks generated at the same time from different machines virtual and physical.

3.2.1 Generating Brute Force Attacks on Victim VM

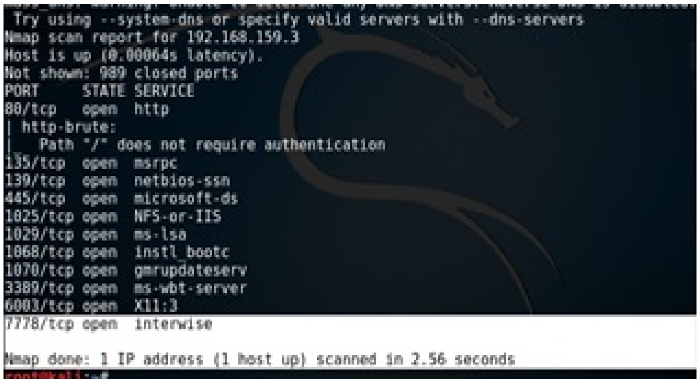
The nmap tool used to generate brute force attack on victim VM using web site URL. Figure 3 illustrates the brute force attacks on victim application server and scanning the server using its IP and scan all ports and its status if it is up and running or down.



```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-05-13 08:15 EDT
setup_target: failed to determine route to 7778 (0.0.30.98)
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify v
alid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try us
ing --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.159.3
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.159.3 are filtered

Nmap done: 1 IP address (1 host up) scanned in 2.84 seconds
root@kali:~# nmap -script http-brute -Pn 7778 192.168.159.3
```

Fig. 3 Brute Force Attack on VM Application Server

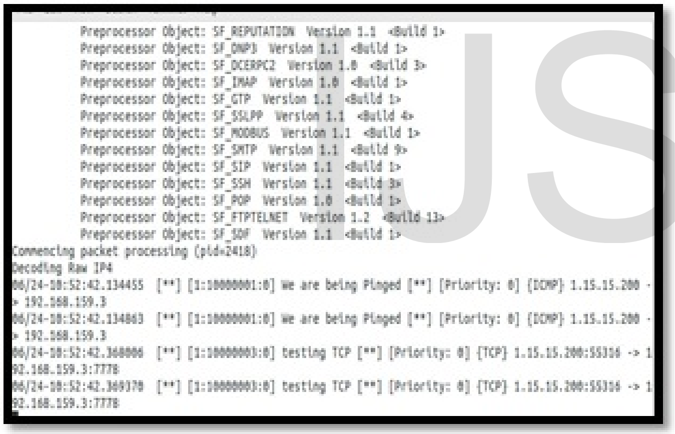
Checking the open ports to generate a brute force attack on authentication as showed in Figure 4 that does not required authentication to access to the server. The gain from this is showing that the target port "7778" is open to access to application server to block access to virtual DB through this port.



```
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.159.3
Host is up (0.00064s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
80/tcp    open  http
| http-brute:
|   Path "/" does not require authentication
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1029/tcp  open  ms-lsa
1068/tcp  open  instl_bootc
1070/tcp  open  gmrupdateserv
3389/tcp  open  ms-wbt-server
6003/tcp  open  X11:3
7778/tcp  open  interwise

Nmap done: 1 IP address (1 host up) scanned in 2.56 seconds
```

Fig. 4 Executing Brute Force Attack on VM

Some benefits are shooed as other open ports and time consumed in scanning. The results of this attack are monitors, detected by vNIDPS, and depicted in Figure 5 that contains message written in personal script roles file "we are being pinged".



```
        Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
        Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
        Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
        Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
        Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
        Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
        Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
        Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
        Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
        Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
        Preprocessor Object: SF_POP  Version 1.0  <Build 1>
        Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
        Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
Commencing packet processing (pid=2418)
Decoding Raw IP4
06/24-10:52:42.134455  [**] [1:10000001:0] We are being Pinged [**] [Priority: 0] {ICMP} 1.15.15.200 -
> 192.168.159.3
06/24-10:52:42.134863  [**] [1:10000001:0] We are being Pinged [**] [Priority: 0] {ICMP} 1.15.15.200 -
> 192.168.159.3
06/24-10:52:42.360006  [**] [1:10000003:0] testing TCP [**] [Priority: 0] {TCP} 1.15.15.200:55316 -> 1
92.168.159.3:7778
06/24-10:52:42.369370  [**] [1:10000003:0] testing TCP [**] [Priority: 0] {TCP} 1.15.15.200:55316 -> 1
92.168.159.3:7778
```

Fig. 5. vNIDPS Detect Attacks on VM

Also, show the targeted IP, time and date of attack, message ID, type of attack like (ICMP) and attacker IP.

3.2.2. Generating DOS - DDOS Attacks on Victim Application Server VM

Measuring hybrid security of mitigating DOS and DDOS attacks against the virtual environments using Low Orbit Ion Cannon (LOIC). This test have been made twice-using LOIC, one time for DOS and second time for DDOS each time generating the attack without using the hybrid security and with using the hybrid security .

The DOS built on Linux VM and starting attack as shows in Figure 6 without using the proposed hybrid security for 48 hours. It contains the victum URL that need to be flood, IP founded, port number and methods (http, TCP, UDP). After starting flood the (Figure X) explore the number of requested download and sucsseful dowload in milions times for both.

Starting the virtual hybrid security VMs and repeat this attacks again for another 48 hours.

Fig. 8 Preventing Attacks from Different Zombies

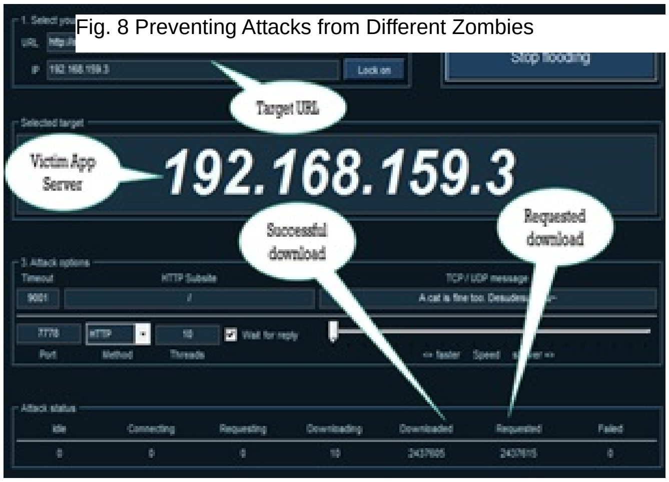


Fig. 6 Generating DDOS Attacks on Vital

Figure 7 illustrates the amazing results in requested download and successful download. Creating DDOS attacks as the same way as the previous one, but installing LOIC on several machines to benefits from complete resources (CPU, memory), those machines are windows OS targeting the victim virtual application server VM at the same. They are working as several zombies.

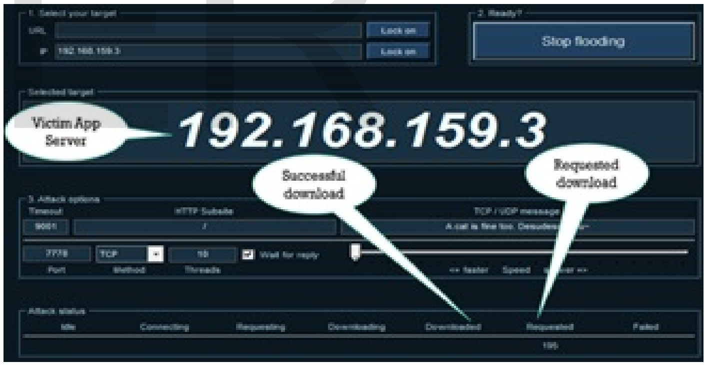
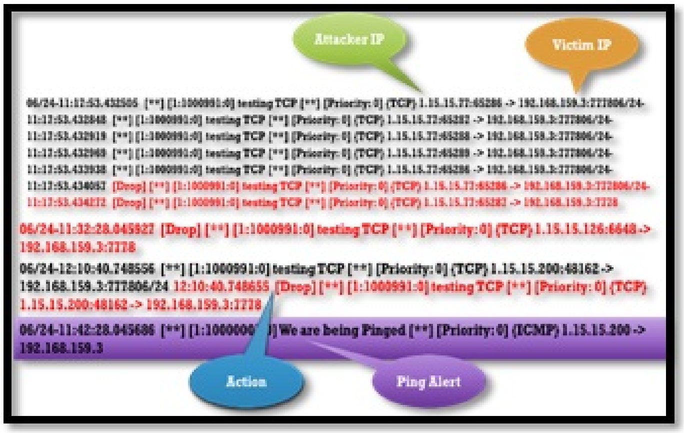


Fig. 7 Generating DDOS Attacks while using

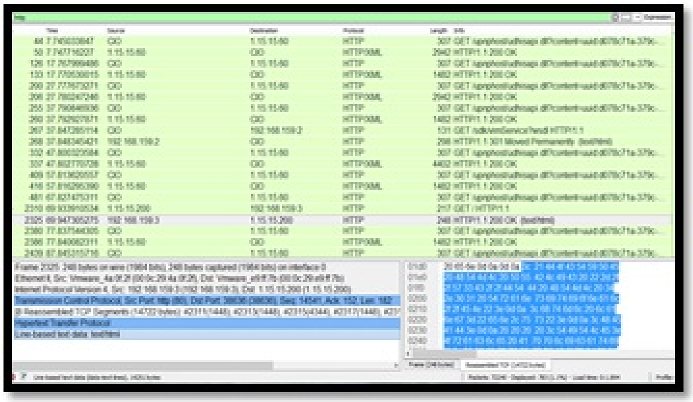
Looking at vNIDPS monitor to see how it is works under attack and how dropping malicious packets. Figure 8 shows different attacks comes from different Zombies at the same time the action from using the perversion system in virtual network, also illustrates the attackers IPs on the same victim VM and the successful result found in dropping the packet and alert messages.



```
06/24-11:12:53.432505 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.77:65286 -> 192.168.159.3:777806/24-
11:12:53.432848 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.72:65282 -> 192.168.159.3:777806/24-
11:12:53.432919 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.72:65288 -> 192.168.159.3:777806/24-
11:12:53.432969 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.72:65289 -> 192.168.159.3:777806/24-
11:12:53.432938 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.72:65286 -> 192.168.159.3:777806/24-
11:12:53.434052 [Drop] [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.77:65286 -> 192.168.159.3:777806/24-
11:12:53.434272 [Drop] [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.77:65287 -> 192.168.159.3:7778

06/24-11:32:28.045927 [Drop] [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.126:6648 ->
192.168.159.3:7778

06/24-12:10:40.748556 [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP) 1.15.15.200:48162 ->
192.168.159.3:777806/24 12:10:40.748655 [Drop] [**] [1:1000991:0] testing TCP [**] [Priority: 0] (TCP)
1.15.15.200:48162 -> 192.168.159.3:7778

06/24-11:42:28.045686 [**] [1:1000000[illegible]] We are being Pinged [**] [Priority: 0] (ICMP) 1.15.15.200 ->
192.168.159.3
```

3.3 Sniffing Virtual Network Traffic Packets during Attacks

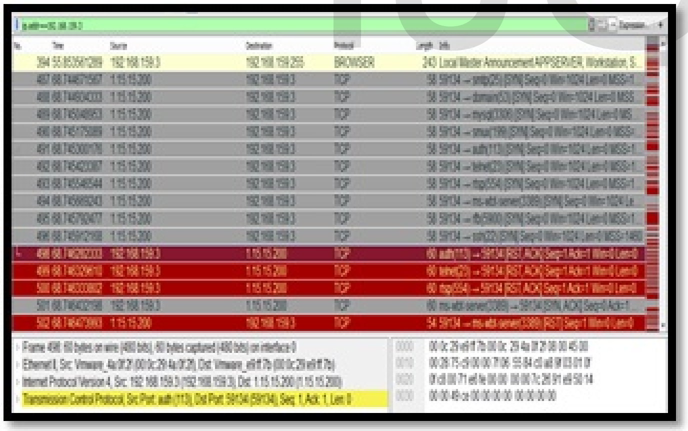
Watching virtual network packets using Wireshark tool and look up these packets during regular use of virtual network and during the attacks. Figure 9 indicates the regular use of the application Server VM and using of http protocol from regular users.



```
No.   Time            Source          Destination     Protocol  Length Info
44    7.745033847     OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
50    7.747716207     1.15.15.60      OD              HTTP/XML  2942 HTTP/1.1 200 OK
126   17.767999486    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
133   17.770536015    1.15.15.60      OD              HTTP/XML  1482 HTTP/1.1 200 OK
200   27.777673271    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
206   27.780247246    1.15.15.60      OD              HTTP/XML  2942 HTTP/1.1 200 OK
255   37.790846936    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
260   37.792927871    1.15.15.60      OD              HTTP/XML  1482 HTTP/1.1 200 OK
267   37.847285114    OD              192.168.159.2   HTTP      131 GET /idk/ServiceTrend HTTP/1.1
268   37.848345421    192.168.159.2   OD              HTTP      298 HTTP/1.1 301 Moved Permanently (text/html)
332   47.800323584    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
337   47.802770728    1.15.15.60      OD              HTTP/XML  4402 HTTP/1.1 200 OK
409   57.813620557    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
416   57.816295390    1.15.15.60      OD              HTTP/XML  1482 HTTP/1.1 200 OK
481   67.827475311    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
2310  69.933910534    1.15.15.200     192.168.159.3   HTTP      217 GET / HTTP/1.1
2325  69.947305275    192.168.159.3   1.15.15.200     HTTP      248 HTTP/1.1 200 OK (text/html)
2380  77.837546305    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
2386  77.840082311    1.15.15.60      OD              HTTP/XML  1482 HTTP/1.1 200 OK
2439  87.845315716    OD              1.15.15.60      HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...

Frame 2325: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0
Ethernet II, Src: Vmware_4a:0f:2f (00:0c:29:4a:0f:2f), Dst: Vmware_e9:f7:fb (00:0c:29:e9:f7:fb)
Internet Protocol Version 4, Src: 192.168.159.3 (192.168.159.3), Dst: 1.15.15.200 (1.15.15.200)
Transmission Control Protocol, Src Port: http (80), Dst Port: 38636 (38636), Seq: 14541, Ack: 152, Len: 182
[8 Reassembled TCP Segments (14722 bytes): #2311(1448), #2313(1448), #2315(4344), #2317(1448), #2...
Hypertext Transfer Protocol
Line-based text data: text/html
```

Fig 9. Sniffing HTTP Packets in normal web activity

Sniffing virtual network traffic for victim application server VM during attacks that indicates how heavy attacker packets coming to victim server as showed in Figure 10. Analyzing, the gray area indicates that the attacker starting exploitation of victim VM to find the vulnerabilities on VM. The Red area indicates that the hybrid security blocks this attack.



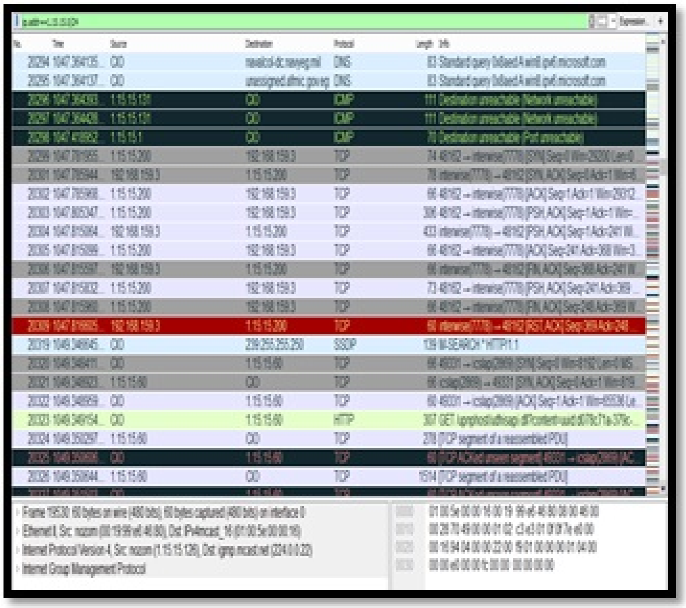
```
ip.addr==192.168.159.3
No.  Time          Source         Destination      Protocol  Length Info
394  55.853561289  192.168.159.3  192.168.159.255  BROWSER   243 Local Master Announcement APPSERVER, Workstation, S...
487  68.744671567  1.15.15.200    192.168.159.3    TCP       58 59134 → smtp(25) [SYN] Seq=0 Win=1024 Len=0 MSS=1...
488  68.744604333  1.15.15.200    192.168.159.3    TCP       58 59134 → domain(53) [SYN] Seq=0 Win=1024 Len=0 MSS
489  68.745048953  1.15.15.200    192.168.159.3    TCP       58 59134 → mysql(3306) [SYN] Seq=0 Win=1024 Len=0 MS...
490  68.745175089  1.15.15.200    192.168.159.3    TCP       58 59134 → smux(199) [SYN] Seq=0 Win=1024 Len=0 MSS=...
491  68.745300176  1.15.15.200    192.168.159.3    TCP       58 59134 → auth(113) [SYN] Seq=0 Win=1024 Len=0 MSS=1...
492  68.745420387  1.15.15.200    192.168.159.3    TCP       58 59134 → telnet(23) [SYN] Seq=0 Win=1024 Len=0 MSS=1...
493  68.745546544  1.15.15.200    192.168.159.3    TCP       58 59134 → rtsp(554) [SYN] Seq=0 Win=1024 Len=0 MSS=1...
494  68.745669243  1.15.15.200    192.168.159.3    TCP       58 59134 → ms-wbt-server(3389) [SYN] Seq=0 Win=1024 Le...
495  68.745792477  1.15.15.200    192.168.159.3    TCP       58 59134 → tfs(5900) [SYN] Seq=0 Win=1024 Len=0 MSS=1...
496  68.745912168  1.15.15.200    192.168.159.3    TCP       58 59134 → ssh(22) [SYN] Seq=0 Win=1024 Len=0 MSS=1460
498  68.746262033  192.168.159.3  1.15.15.200      TCP       60 auth(113) → 59134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
499  68.746329610  192.168.159.3  1.15.15.200      TCP       60 telnet(23) → 59134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
500  68.746330802  192.168.159.3  1.15.15.200      TCP       60 rtsp(554) → 59134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
501  68.746402198  192.168.159.3  1.15.15.200      TCP       60 ms-wbt-server(3389) → 59134 [SYN, ACK] Seq=0 Ack=1...
502  68.746473993  1.15.15.200    192.168.159.3    TCP       54 59134 → ms-wbt-server(3389) [RST] Seq=1 Win=0 Len=0

Frame 498: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Vmware_4a:0f:2f (00:0c:29:4a:0f:2f), Dst: Vmware_e9:f7:fb (00:0c:29:e9:f7:fb)
Internet Protocol Version 4, Src: 192.168.159.3 (192.168.159.3), Dst: 1.15.15.200 (1.15.15.200)
Transmission Control Protocol, Src Port: auth (113), Dst Port: 59134 (59134), Seq: 1, Ack: 1, Len: 0

0000  00 0c 29 e9 f7 fb 00 0c 29 4a 0f 2f 08 00 45 00
0010  00 28 75 c9 00 00 80 06 55 84 c0 a8 9f 03 01 0f
0020  0f c8 00 71 e6 fe 00 00 00 00 7c 26 91 e8 50 14
0030  00 00 49 ca 00 00 00 00 00 00 00 00
```

Fig 10. Sniffing Attacker Packets

ICMP, ARP and http packets that comes from zombies on victim server and dropped by the hybrid security.

The gray area indicates that the attacker starting exploitation of victim VM to find the vulnerabilities on VM. The Red area indicates that the hybrid security blocks this attack.

Figure 11 explores the sniffing of the virtual network traffic



```
ip.addr==1.15.15.0/24
No.    Time          Source         Destination          Protocol  Length Info
20294  1047.364135…  OD             nawlabdc.naveg.ml    DNS       83 Standard query 0x0aed A wpad.microsoft.com
20295  1047.364137…  OD             unassigned.dhcp.naveg DNS      83 Standard query 0x0aed A wpad.microsoft.com
20296  1047.364393…  1.15.15.131    OD                   ICMP      111 Destination unreachable (Network unreachable)
20297  1047.364428…  1.15.15.131    OD                   ICMP      111 Destination unreachable (Network unreachable)
20298  1047.410852…  1.15.15.1      OD                   ICMP      70 Destination unreachable (Port unreachable)
20299  1047.781955…  1.15.15.200    192.168.159.3        TCP       74 48162 → interwise(7778) [SYN] Seq=0 Win=29200 Len=0
20301  1047.785944…  192.168.159.3  1.15.15.200          TCP       78 interwise(7778) → 48162 [SYN, ACK] Seq=0 Ack=1 Win=8...
20302  1047.785968…  1.15.15.200    192.168.159.3        TCP       66 48162 → interwise(7778) [ACK] Seq=1 Ack=1 Win=29312
20303  1047.805347…  1.15.15.200    192.168.159.3        TCP       306 48162 → interwise(7778) [PSH, ACK] Seq=1 Ack=1 Win=...
20304  1047.815084…  192.168.159.3  1.15.15.200          TCP       433 interwise(7778) → 48162 [PSH, ACK] Seq=1 Ack=241 Wi...
20305  1047.815099…  1.15.15.200    192.168.159.3        TCP       66 48162 → interwise(7778) [ACK] Seq=241 Ack=368 Win=3...
20306  1047.815597…  192.168.159.3  1.15.15.200          TCP       66 interwise(7778) → 48162 [FIN, ACK] Seq=368 Ack=241 Wi...
20307  1047.815832…  1.15.15.200    192.168.159.3        TCP       73 48162 → interwise(7778) [PSH, ACK] Seq=241 Ack=369
20308  1047.815960…  1.15.15.200    192.168.159.3        TCP       66 48162 → interwise(7778) [FIN, ACK] Seq=248 Ack=369 Wi...
20309  1047.816605…  192.168.159.3  1.15.15.200          TCP       60 interwise(7778) → 48162 [RST, ACK] Seq=369 Ack=248
20319  1049.348645…  OD             239.255.255.250      SSDP      139 M-SEARCH * HTTP/1.1
20320  1049.348411…  OD             1.15.15.60           TCP       66 49331 → icslap(2869) [SYN] Seq=0 Win=8192 Len=0 MS...
20321  1049.348923…  1.15.15.60     OD                   TCP       66 icslap(2869) → 49331 [SYN, ACK] Seq=0 Ack=1 Win=819...
20322  1049.348959…  OD             1.15.15.60           TCP       60 49331 → icslap(2869) [ACK] Seq=1 Ack=1 Win=65536 Le...
20323  1049.349154…  OD             1.15.15.60           HTTP      307 GET /apnphost/ud/soap dl?content=uuid:d078c71a-379c...
20324  1049.350297…  1.15.15.60     OD                   TCP       278 [TCP segment of a reassembled PDU]
20325  1049.350606…  OD             1.15.15.60           TCP       60 [TCP ACKed unseen segment] 49331 → icslap(2869) [AC...
20326  1049.350644…  1.15.15.60     OD                   TCP       1514 [TCP segment of a reassembled PDU]

Frame 19530: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: nozom (00:19:99:e6:46:80), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: nozom (1.15.15.126), Dst: igmp.mcast.net (224.0.0.22)
Internet Group Management Protocol

0000  01 00 5e 00 00 16 00 19 99 e6 46 80 08 00 46 00
0010  00 28 74 49 00 00 01 02 c3 e0 01 0f 0f 7e e0 00
0020  00 16 94 04 00 00 22 00 f9 01 00 00 00 01 04 00
0030  00 00 e0 00 00 fc 00 00 00 00 00 00
```

Fig 11. Sniffing Attacker Packets on Virtual Network

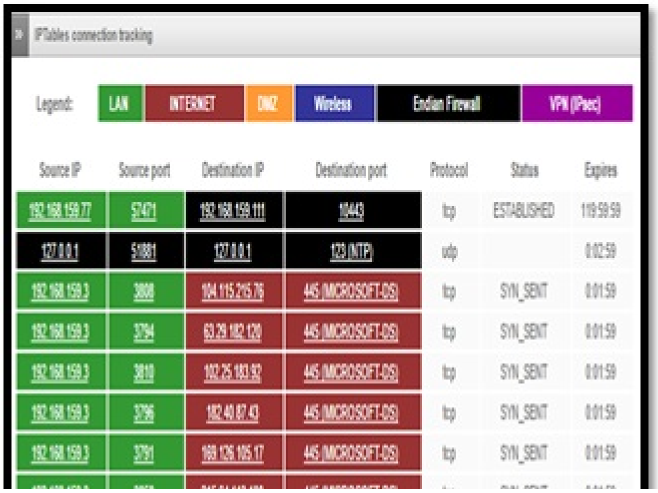
and indicates Zombies packets that tray to effects on the virtual service. Attacker use protocols stop like (http, ICMP, TCP, DNS and SSDP Simple Service Discovery Protocol). ICMP stopped by virtual firewall as shown in the black area in (Figure X), TCP flooding stopped by vNIDPS as shown in red area, the cyan area shows the SSDP protocol the attacker try to discover the virtual network, the gray area attacker is trying to access the application server through port "7778".

3.4. Virtual Network Traffic Study

The virtual for network study to evaluate the performance of the hybrid security during the attacks and showing the virtual traffic load.

3.4.1 Virtual firewall traffic studying

Studying those attacks effects on virtual network traffic without using the hybrid security and with using the hybrid security. The virtual firewall IP-table connection tracking in normal usage of virtual network, which includes source IPs, source ports, destination IPs, destination ports and protocol, is used as illustrated in Figure 12, which indicates the minimum usage for virtual firewall (black area in the dashboard) on virtual traffic.



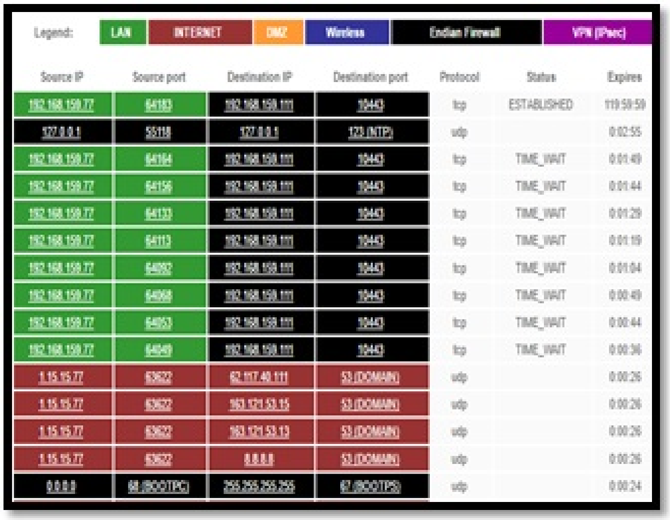
IPTables connection tracking

Legend: 🟩 LAN 🟥 INTERNET 🟧 DMZ 🟦 Wireless ⬛ Endian Firewall 🟪 VPN (IPsec)

Source IP	Source port	Destination IP	Destination port	Protocol	Status	Expires
192.168.159.77	57471	192.168.159.111	10443	tcp	ESTABLISHED	119:59:59
127.0.0.1	51881	127.0.0.1	123 (NTP)	udp		0:02:59
192.168.159.3	3808	104.115.215.76	445 (MICROSOFT-DS)	tcp	SYN_SENT	0:01:59
192.168.159.3	3794	63.29.182.120	445 (MICROSOFT-DS)	tcp	SYN_SENT	0:01:59
192.168.159.3	3810	102.25.183.92	445 (MICROSOFT-DS)	tcp	SYN_SENT	0:01:59
192.168.159.3	3796	182.40.87.43	445 (MICROSOFT-DS)	tcp	SYN_SENT	0:01:59
192.168.159.3	3791	169.126.105.17	445 (MICROSOFT-DS)	tcp	SYN_SENT	0:01:59

Fig 12. Sniffing Attacker Packets on Virtual Network

The virtual firewall dashboard indicates that the IP-table connection-tracking while attack. The black area in the snapshot is highly used in IP table connection indicates that the virtual firewall is working and blocking attacker IP, the used protocol (tcp, udp) and its status, which is "wait" as shown in Figure 13.



Legend: LAN | INTERNET | DMZ | Wireless | Endian Firewall | VPN (IPsec)

Source IP	Source port	Destination IP	Destination port	Protocol	Status	Expires
192.168.159.77	64183	192.168.159.111	10443	tcp	ESTABLISHED	119:59:59
127.0.0.1	55118	127.0.0.1	123 (NTP)	udp		0:02:55
192.168.159.77	64164	192.168.159.111	10443	tcp	TIME_WAIT	0:01:49
192.168.159.77	64156	192.168.159.111	10443	tcp	TIME_WAIT	0:01:44
192.168.159.77	64133	192.168.159.111	10443	tcp	TIME_WAIT	0:01:29
192.168.159.77	64113	192.168.159.111	10443	tcp	TIME_WAIT	0:01:19
192.168.159.77	64092	192.168.159.111	10443	tcp	TIME_WAIT	0:01:04
192.168.159.77	64068	192.168.159.111	10443	tcp	TIME_WAIT	0:00:49
192.168.159.77	64053	192.168.159.111	10443	tcp	TIME_WAIT	0:00:44
192.168.159.77	64049	192.168.159.111	10443	tcp	TIME_WAIT	0:00:36
1.15.15.77	63622	62.117.40.111	53 (DOMAIN)	udp		0:00:26
1.15.15.77	63622	163.121.53.15	53 (DOMAIN)	udp		0:00:26
1.15.15.77	63622	163.121.53.13	53 (DOMAIN)	udp		0:00:26
1.15.15.77	63622	8.8.8.8	53 (DOMAIN)	udp		0:00:26
0.0.0.0	68 (BOOTPC)	255.255.255.255	67 (BOOTPS)	udp		0:00:24

Fig 13. vFW Network Connection during Attacks

Analyzing the incoming virtual traffic and outgoing virtual traffic in KB/s on virtual firewall during normal mode as depicted in Figure 14. The incoming traffic from green IPs (virtual network) and incoming traffic red IPs from cloud clients. The outgoing traffic for green IPs and red IPs is staple in normal usage for the network.

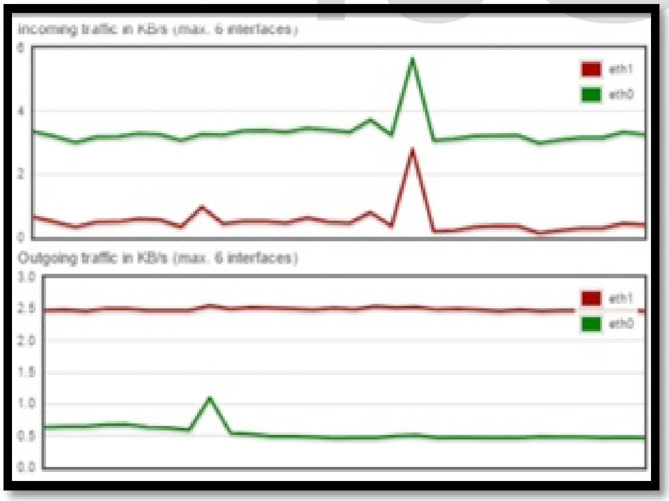


Fig 14. Virtual firewall traffic normal Mode

Looking at the incoming traffic and outgoing traffic on the virtual firewall during the attacks as depict in Figure 15. This comparison illustrates the incoming traffic from green IPs and from red IPs, is very high traffic for both on the virtual network. The outgoing traffic for green IPs is normal but in the red IPS is blocked during the attack. The outgoing traffic for red IP, which comes from attacker, is zero frequency during the attack

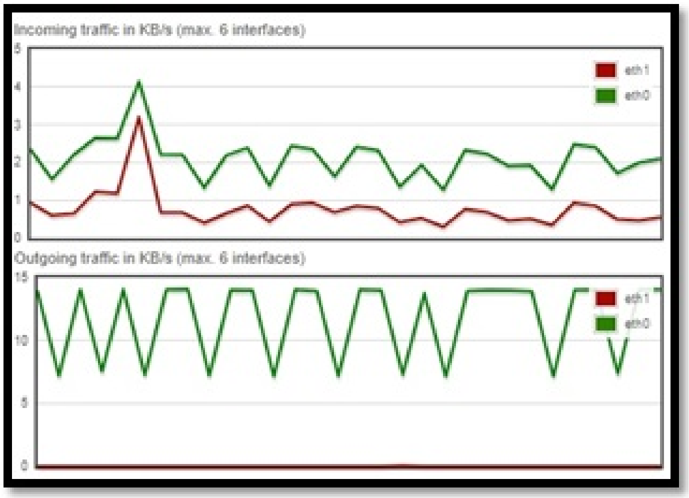


Fig 15. Virtual Firewall Traffic during Attacks

3.4.2. Network Real Time Data Usage during Attacks

Analyzing the virtual network real time data usage during the attacks using hybrid security and virtual network real time data usage without using this hybrid security. Figure 16 illustrates network real time data usage during the attacks without using the hybrid security. The gray area indicates how the traffic on victim virtual application machine usage is too high about 400 kb/s during attacks without the hybrid security. Also indicates the very low reach to virtual DB server, In addition to that shows two parallel steady lines orange and red for hybrid security sensors which means those are turned off.

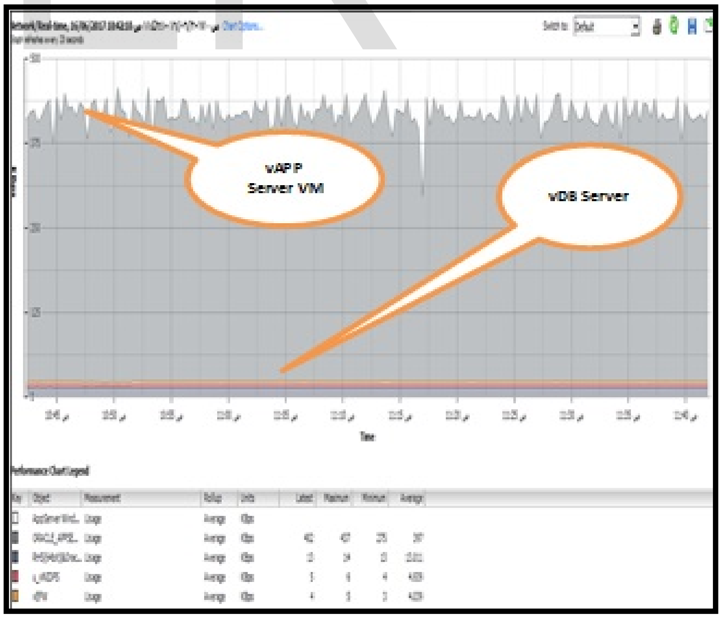


Fig 16. Network real time data usage during the attacks without Hybrid Security

Turning the hybrid security sensors power on and watching the real time virtual network data usage on VMs as shows in Figure 17. The data usage on vApp server downsized to 17.5 KB/s and indicates the virtual network real time data usage on the vNIDPS and virtual firewall is working. Also indicates how the virtual traffic controlled using a hybrid security.

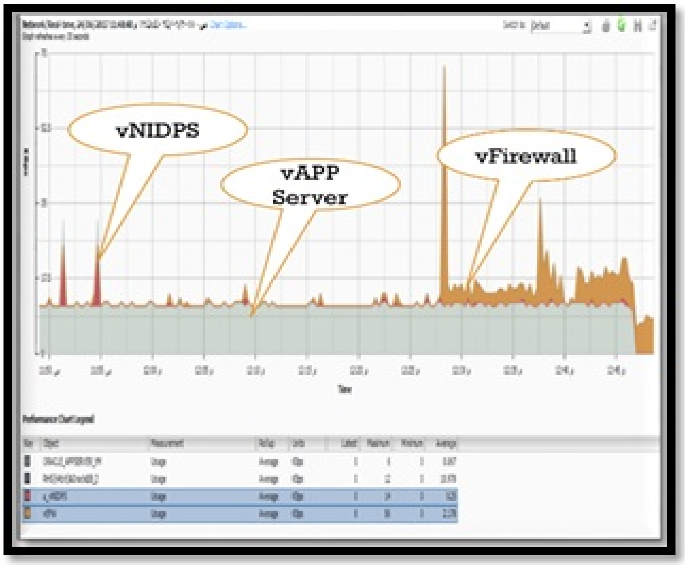


Fig. 17. Network Real Time data usage during attacks using Hybrid Security

3.4.3. Network Real Time Data Transmit Rate during Attacks

A virtual network real time data transmit rate without using the hybrid security sensors. Figure 18 shows the real time data transmit rate for one hour on vApp server VM and vDB server VM. This study repeated again for one hour on virtual network real time data transmit rate but with using the hybrid security at this time as depict in Figures above that indicate the using of virtual firewall and vNIDPS.

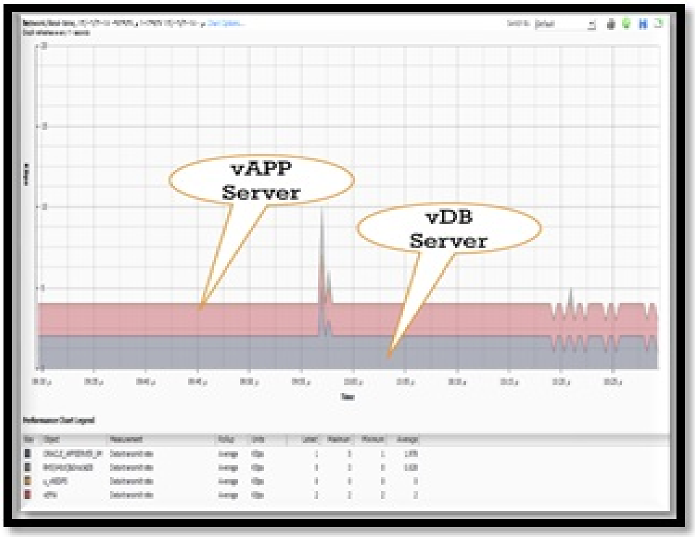


Fig. 18 Network real time data transmit rate during attacks without Hybrid Security

3.4.4. Network Real Time Data Receive Rate during Attacks

The virtual network real time data receive rate during attacks without using the hybrid security illustrated in Figure 19. The data receive rate-monitoring test for one hour and noticed the huge traffic on virtual application server in comparison with virtual DB server. The virtual network real time data receive rate during attacks using the hybrid security, noticed that the hybrid security is working in red and orange zones, with the minimum data receive rate during the attack.

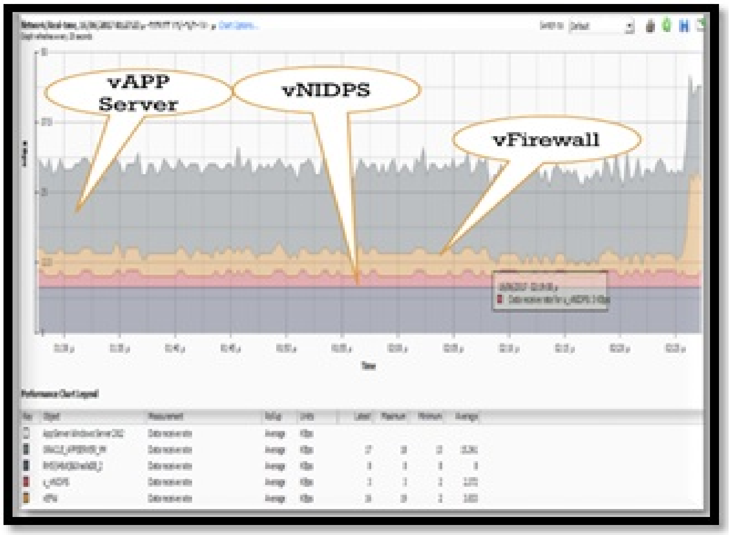


Fig 19. Network real time data receive rate during the attacks

3.4.5. Network Real Time Broadcast Received during Attacks Using Hybrid security

The virtual network real time broadcast received during attacks using hybrid security as showed in Figure 20 that indicates all VMs is working under flooding in the performance chart highlighted in the chart.

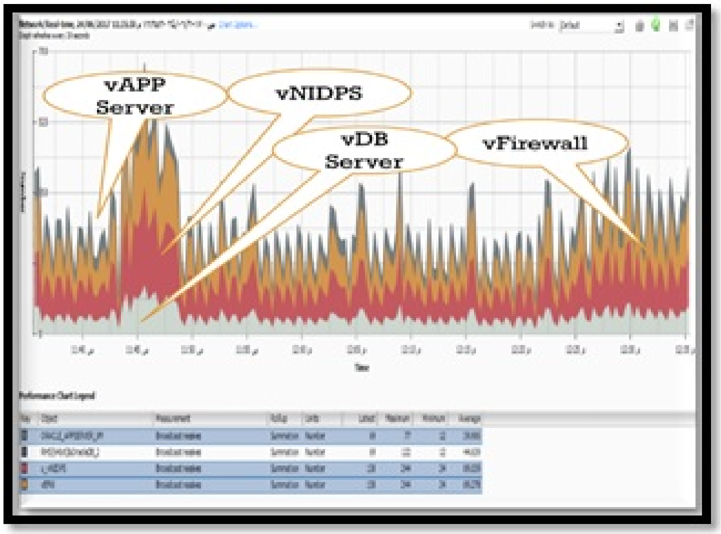
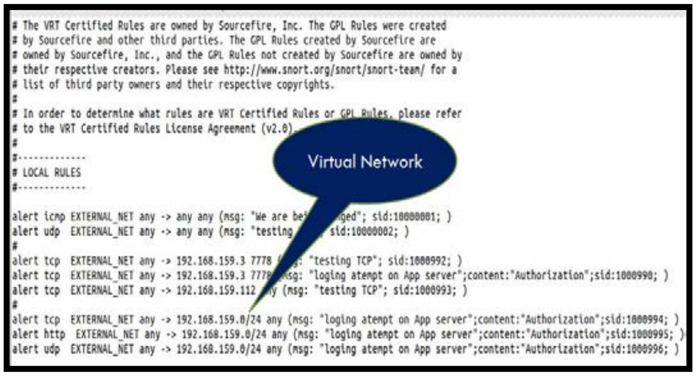


Fig 20. Network real time broadcast received during the attacks using Hybrid Security

The conclusion of this traffic study in different cases on the virtual network is the hybrid security that is works well against several attacks. The virtual environments works well under this hybrid security protection.

3.5. Scalability Evolution

Changing the scope of hybrid security to defense on all server VMs in the virtual network instead of defensing on the critical VM. The virtual has domain server VM, 2 application server and database server, in addition to hybrid security VMs. Figure 21 shows how we changed the scope of sensors to protect all VMs in the virtual network.



```
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0)
#
#-------------
# LOCAL RULES
#-------------

alert icmp EXTERNAL_NET any -> any any (msg: "We are be     ged"; sid:10000001; )
alert udp  EXTERNAL_NET any -> any any (msg: "testing       sid:10000002; )
#
alert tcp  EXTERNAL_NET any -> 192.168.159.3 7778    : "testing TCP"; sid:1000992; )
alert tcp  EXTERNAL_NET any -> 192.168.159.3 777   sg: "loging atempt on App server";content:"Authorization";sid:1000990; )
alert tcp  EXTERNAL_NET any -> 192.168.159.112   y (msg: "testing TCP"; sid:1000993; )
#
alert tcp  EXTERNAL_NET any -> 192.168.159.0/24 any (msg: "loging atempt on App server";content:"Authorization";sid:1000994; )
alert http  EXTERNAL_NET any -> 192.168.159.0/24 any (msg: "loging atempt on App server";content:"Authorization";sid:1000995; )
alert udp  EXTERNAL_NET any -> 192.168.159.0/24 any (msg: "loging atempt on App server";content:"Authorization";sid:1000996; )
```

Fig 21. Changing the network sensors scope

3.5.1 Lunching attacks on many server.

Lunching attacks on many servers VMs, for example (Oracle app. Server, database server, domain controller server and web server) using the same tools that we used before. Repeating the previous attacks (DoS-DDoS, Brute force attack comes from many attackers to many VMs at the same time. The Hybrid Security dropped all attackers packet according to sensors script.

4. CONCLUSION

This paper introduced an innovative security scheme, which makes layers of security around virtual traffic, and critical VMs that can be attacked from insider VM or from external attackers. The security evaluation of the Hybrid security shows how could avoid an attacks on hypervisor. Lunching brought force attack and DoS-DDoS on Hybrid Security system through creating attack module. Examining the hybrid security sensors results and defense in depth on the critical VM. Studying virtual network traffic during stressing on virtual network and VMs. Changing the scope to works on virtual network instead of critical VM and lunching the attack on May VMs at the same time to check the scalability. All attacker packets dropped by hybrid security. Analyzing virtual traffic packets to verify that all attacker packets is dropped by Hybrid security scheme and it is successful in mitigating risks on virtual environment. The future work is planning to increase the number of attacker to check the availability of our virtual environment.

REFERENCES

[1] J. L. Paul T. Jaeger, "Cloud Computing and Information Policy," Journal of Information Technology & Politics, pp. 269-283, 2011.

[2] T. G. Peter Mell, "Definition of Cloud Computing,," NIST Special Publication , pp. 145-800, September 2011.

[3] N. S. P. 800-145, "The NIST Definition of Cloud Computing," Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, 2011.

[4] N. C. –. 092, "NIST Cloud Computing Standards Roadmap," 5 July 2011.

[5] A. S.-S. M. F.-A. M. P. M. C. Yoser Jarraya, "Multi-Stage Defense-Aware Security Modules Placement in the Cloud," US. Patent Application Publication, pp. 1-13, 1 Feb. 2018.

[6] M. M. K. B. D. M. H. S. K. M. K. a. K. R. C. S. Iqbal, "“On Cloud Security Attacks: A Taxonomy and Intrusion Detection and Prevention as a Service”.," Journal of Network and Computer Applications,, vol. 74, p. 98 –120, 2016.

[7] P. S. Shreyal Gajare, "Safeguard Hypervisor attacks in cloud computing," International Journal of Scientific Engineering and Applied Science (IJSEAS) , vol. 3, no. 12, December 2017.

[8] I. institute, "Best DOS Attacking tools," 2017. [Online]. Available: http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/. [Accessed 13 10 2017].

[9] Vmware, "vSphere-ESXi-vcenter-server-50-networking-guide," Vmware, 2011. [Online]. Available: http://www.vmware.com/support.

[10] C. N. M. ·. K. Acha, "Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review," J Supercomput, July 2016.

[11] S. K. a. A. Gupta, "Security Issues in Cloud," International Journal of Innovations & Advancement in Computer Science IJIACS, vol. 6, no. 1, January 2017.

[12] j. Reiner Sailer, "Building a MAC-Based Security Architecture for the Xen Open-Source Hypervisor," Hawthorne,, NY 10532 USA.

[13] M. Godfrey, "AServer-SideSolutiontoCache-BasedSide Channel Attacks in the Cloud.In," in the Cloud Computing (CLOUD), 2013 IEEE Sixth International Conferenceon, 2013. IEEE, 2013.

[14] C. Sunita Sharma and Amit, "survey on cloud storage security," nternational Journal of Innovative Research in Computer and Communication Engineering, made I, vol. 1, no. 2, April 2013.

[15] T. C. Group, "Trusted Computing," 2017. [Online]. Available: https://trustedcomputinggroup.org/. [Accessed 2017].

[16] C. A. 1000V, "Cloud Firewall Getting Started Guide.," Cisco, [Online]. Available:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html..

[17] M. A. E. Nashwa Abdelbaki, "Cloud Computing Virtualization Security Management," CIIT International Journal of Artificial Intelligent Systems and Machine Learning, vol. 16, no. 4, pp. 148-154, 2014.

[18] R. J. Rubal Dahat, "An Approach for Intrusion Detection and Countermeasure Selection in Virtual Network System," International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) , vol. 4 , no. 4, April 2015.

[19] J. R.Sasikala, "Secure Conserve Data Split To Avoid Network Intrusion Detection," International Journal of Engineering and Technical Research (IJETR), vol. 3, no. 3, March 2015.