Unified Threat Management

Bernard J. Christenson Colón
Master of Engineering in Computer Engineering
Advisor: Jeffrey Duffany, Ph.D.
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract **—** *Unified Threat Management (UTM) is an information security term that refers to a security appliance as a combination of hardware, software and networking technologies in which the primary function is to integrate increased security, visibility, and control over network security while also reducing complexity. UTM refers to a single security appliance, and within a UTM appliance, the typical features fall into the following three main subsets: firewall/intrusion prevention system (IPS)/virtual private network (VPN), secure Web gateway and messaging security. Preventing threats can be challenging to manage and expensive when using separate appliances for each specific security task, as each aspect has to be maintained and updated individually to remain current with the latest forms of malware and cyber threats. This paper approaches the OPNsense software platform, discusses the importance of network security, UTM appliance market growth, network environment, OPNsense key features, and discuss how the IDS/IPS, Block SSL certificates and Traffic Shaping implementations complement security capabilities.*

Key Terms *— IDS Block SSL Certificates, Network security, Traffic Shaper, Unified Threat Management (UTM).*

INTRODUCTION

According to Gartner, the term Unified Threat Management (UTM) is a converged platform of point security products, particularly suited to small and midsize businesses (SMBs). Typical feature sets fall into three main subsets, all within the UTM: firewall/intrusion prevention system (IPS)/virtual private network, secure Web gateway security (URL filtering, Web anti-virus) and messaging security (anti-spam, mail anti-virus) [1]. Employing network security in smaller networks can be challenging to manage and expensive when integrating separate appliances for each specific security task in the infrastructure, as each aspect has to be maintained and updated individually to remain current with the latest forms of malware and cyber threats. Network security is a serious problem that plays a significant role in drastically changing the business mindset to look for solutions that aim to simplify operations into an integrated security system to provide cost-effective outcomes. Firewalls are the first line of defense, but the more complex the network infrastructure becomes; the traditional firewall strategy usually cannot meet the demands of security.

According to research by Gartner, “99% of the vulnerabilities exploited by the end of 2020 will continue to be ones known by security and IT professionals at the time of the incident” [2]. The current vulnerabilities complicate the work of the network administrators, therefore, to protect against sophisticated threats the appliance of Unified Threat Management integrates tools into a unified security architecture. By creating a single point of defense and providing a single console, UTM solutions act as the first line of defense to networks and offer a plethora of tools to mitigate the threats from the Wide Area Network and the Local Area Network. In this paper, the UTM deployed is OPNsense, and Deciso defines it as “an open source, easy-to-use and easy-to-build FreeBSD based firewall and routing platform. OPNsense includes most of the features available in expensive commercial firewalls, and more in many cases” [3]. This paper will demonstrate, discuss the IDS/IPS Block SSL certificates feature and the Traffic Shaper feature of the platform and the benefits and justify this network security approach.

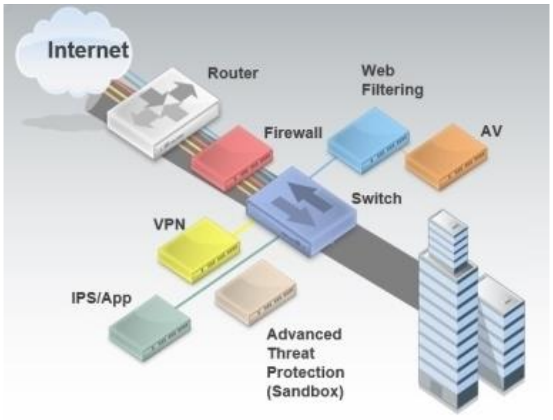


Figure 1
Traditional Solutions [4]

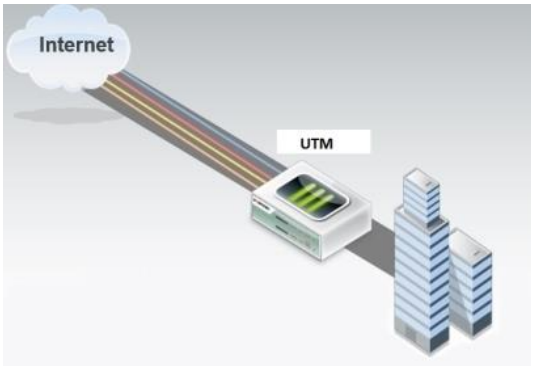
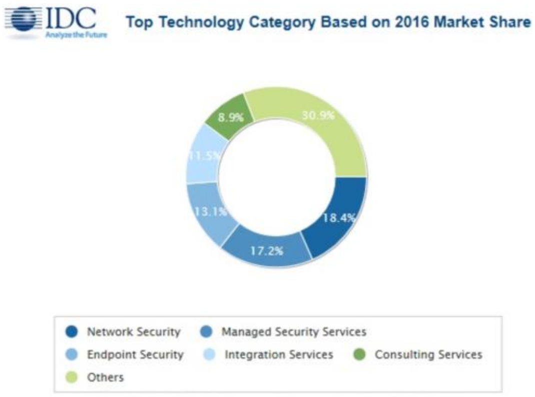


Figure 2
Consolidated/UTM Solution [4]

UTM Appliance Market Growth

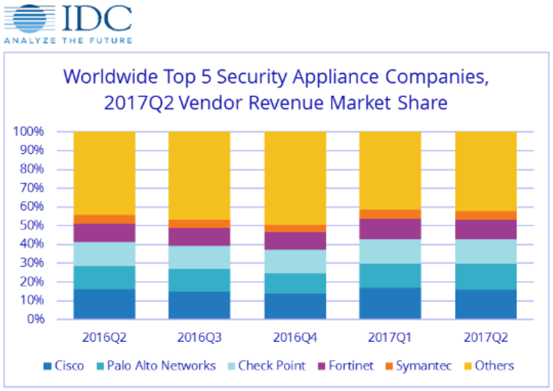
According to the International Data Corporation (IDC), it forecasted worldwide revenues for security-related hardware, software, and services reached $81.7 billion in 2017, an increase of 8.2% over 2016 [5]. IDC mentions that the expected global spending on security solutions will accelerate a little bit over the next years, achieving a compound annual growth rate (CAGR) of 8.7% through 2020 when revenues will be nearly $105 billion [5]. UTM hardware will see the fastest spending growth over the 2015-2020 forecast period of 11.9% CAGR [5]. According to Angela Vacca, senior research manager, Customer Insights and Analysis (CIA), which indicates that the “General Data Protection Regulation (GDPR) will drive up compliance-related projects significantly in 2017 and 2018 until organizations have found a cost-efficient and scalable way of dealing with data" [5].



Source: IDC Worldwide Semiannual Security Spending Guide, 2015

Figure 3
Top Technology Category Based on 2016 Market Share [5]

According to another study from the International Data Corporation (IDC), for the second quarter of 2017 worldwide indicated that vendor revenues in the second quarter increased 9.2% year over year to $3.0 billion and shipments grew 7.0% year over year [6]. According to IDC, the trend for growth in the worldwide market driven by the Unified Threat Management (UTM) reaching $1.6 billion in 2Q17 and a year-over-year increase of 16.8%, the highest growth among all sub-markets [6]. IDC states, “The UTM market now represents more than 50% of worldwide revenues in the security appliance market” [6]. Robert Ayoub, research director, Security Products at IDC stated, "Firewall and UTM continue to be the strongest areas of growth, as those products continue to add security features leveraging and addressing cloud protection." [6].



Source: IDC 2017

Figure 4
Worldwide Top 5 Security Appliance Companies 2017Q2 Vendor Revenue Market Share [6]

NETWORK ENVIRONMENT

The UTM OPNsense in this environment is software provided as a virtual appliance installed and configured in VirtualBox in Laptop1 Windows 10. A safe virtual environment testing was set up using the VirtualBox Host-Only adapter. Furthermore, in this topology, a VirtualBox Windows 10 Virtual Machine for Intranet testing and Bridge to LAN Interface with Internet access can be utilized as required. The Laptop2 hardware is for monitoring and testing the IDS/IPS (Intrusion Detection/Prevention Systems). [Figure 5].

Hardware and Software Components Utilized

- ISP Modem (Bridge mode) and Router
- Two laptops with two Network
- Interface Cards (NIC) adapters
- CISCO switch
- Oracle VM VirtualBox Manager v5.2.12
- Microsoft Windows 10 x64 v1709 b16299.431
- UTM OPNsense virtual appliance v18.1

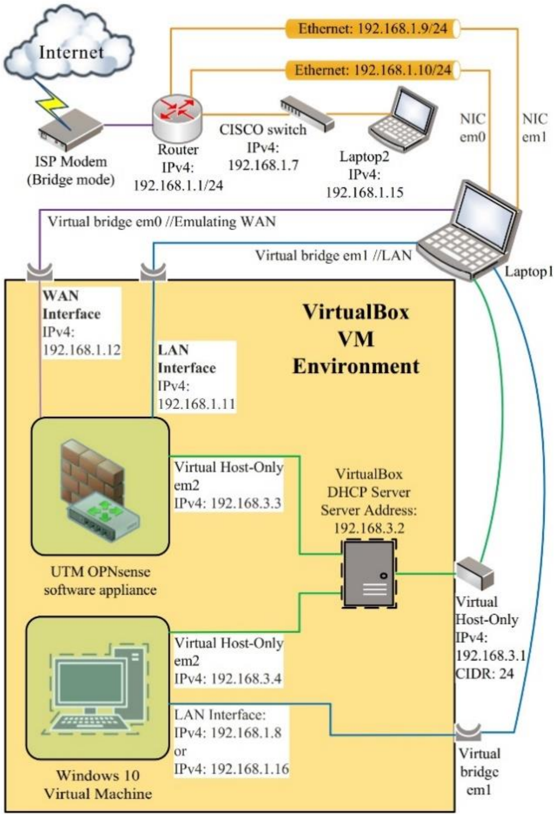
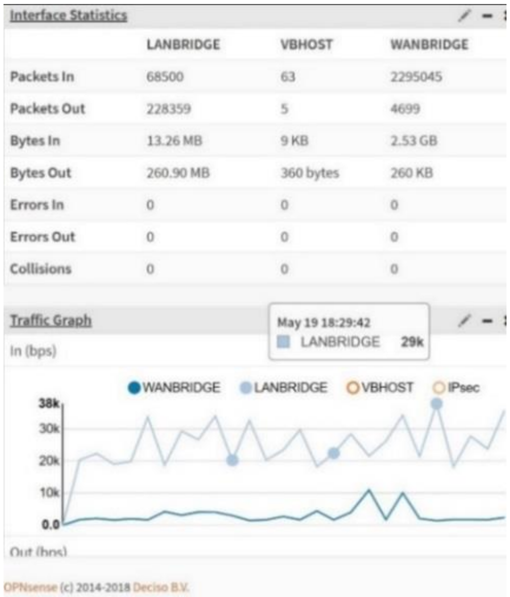


Figure 5
Network Diagram of the Testing Environment

OPNSENSE KEY FEATURES

OPNsense is an open source firewall under an OSI (Open Source Initiative) License and provides security solutions in software and hardware appliances from home to business networks. Furthermore, it provides a modern easy to use interface for business, schools, and remote offices scenarios. Besides, it offers key features such as Caching Proxy, Web Filtering, High availability, 2-Factor Authentication, router functionality, VPN (Virtual Private Network), Captive Portal and Netflow reporting [3].

- **Inline Stateful Inspection Firewall:** is a system to keep track of the state of network connections such as TCP (Transmission Control Protocol) streams and UDP (User Datagram Protocol) communication traveling across it, configurations are possible to distinguish legitimate packets for different types of connections. Only packets matching a known active connection will be allowed by the firewall, the rest will be rejected [3]. Inline Stateful Inspection Firewall. Under the Firewall 'Log Files>Overview' one can view and analyze the graphical representation of the Network traffic [Figure 7].

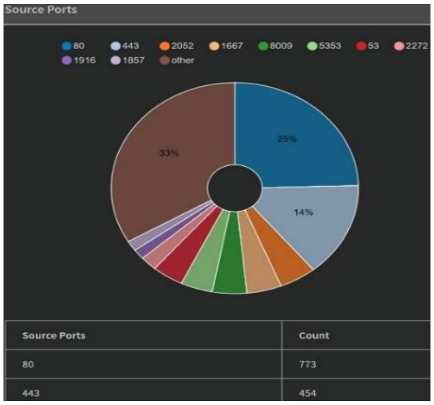

Interface Statistics

	LANBRIDGE	VBHOST	WANBRIDGE
Packets In	68500	63	2295045
Packets Out	228359	5	4699
Bytes In	13.26 MB	9 KB	2.53 GB
Bytes Out	260.90 MB	360 bytes	260 KB
Errors In	0	0	0
Errors Out	0	0	0
Collisions	0	0	0

Traffic Graph

OPNsense (c) 2014-2018 Deciso B.V.

Figure 6
OPNsense Lobby: Dashboard Interface Statistics and Traffic Graph



Source Ports	Count
80	773
443	454

Figure 7
OPNsense Firewall: Log Files: Overview of Top Source Ports

OPNSENSE IMPLEMENTATIONS

The features implemented and discussed in this paper include the IDS/IPS, ClamAV (Anti-Virus), Nmap and Wireshark scans, SSL Blacklisting and Traffic shaping. These features set the UTM apart from the traditional solutions and working together amplify the security and versatility of the local network.

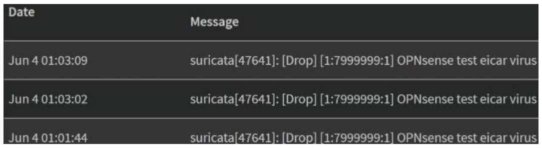
Intrusion Detection and Prevention Systems

The OPNsense Suricata IDS/IPS (Intrusion Detection/Intrusion Detection System) can apply rulesets and alerts are searchable within the user interface. The IPS is "capable of blacklisting based on SSL (Secure Socket Layer) thumbprints" [3]. Despite the depreciation of the SSL protocol and the adoption of TLS (Transport Layer Security), most people still refer to certificates as 'SSL.' It is actually TLS, which is an updated, more secure, version of SSL to provide a cryptographic protocol to provide security over internet communications [7]. The Suricata network security-monitoring engine implements a complete signature language to match known threats, policy violations, and malicious behavior. It will also detect many anomalies in the network protocol traffic it inspects to provide high performance, automatic protection. [8] [9].

ClamAV (Anti-Virus)

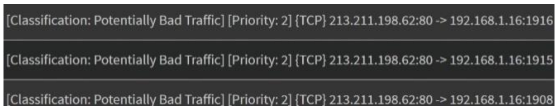
The ClamAV (Anti-Virus) is "an open source antivirus engine for detecting trojans, viruses, malware & other malicious threats" [10]. The initial testing procedure is to is to install the ClamAV plugin in OPNsense (os-clamav) accessing the 'Plugins' menu under the 'System' section. Under the 'Services' section the ClamAV menu will request the user to download the most current signatures. Afterward, additional configuration options can also be enabled as required by the network administrator. [3].

The best approach to test the ClamAV in OPNsense without infecting the network environment with malware was to download anti-malware test files from EICAR. The term initially stood for the European Institute for Computer Antivirus Research, and it provides a virus sample for research purposes. It is important to note that the following test was implemented in the Windows 10 Virtual Machine environment with Windows Defender disabled for testing purposes. EICAR has provided this test file for distribution as the "EICAR Standard Anti-Virus Test File." As stated by EICAR, "it is safe to distribute, because it is not a true virus, and does not include any fragments of viral code" [11]. Suricata IDS/IPS successfully 'drops' the connection attempt when trying to access the file.



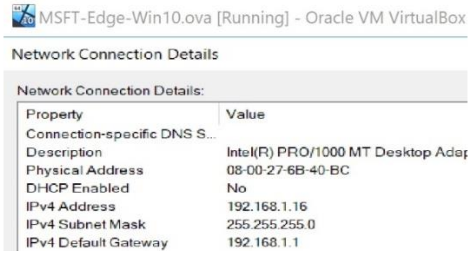
Date	Message
Jun 4 01:03:09	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus
Jun 4 01:03:02	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus
Jun 4 01:01:44	suricata[47641]: [Drop] [1:7999999:1] OPNsense test eicar virus

Figure 8
IDS/IPS EICAR Test Virus Detection Alert Part 1



```
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 213.211.198.62:80 -> 192.168.1.16:1916
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 213.211.198.62:80 -> 192.168.1.16:1915
[Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 213.211.198.62:80 -> 192.168.1.16:1908
```

Figure 9
IDS/IPS EICAR Test Virus Detection Alert Part 2


MSFT-Edge-Win10.ova [Running] - Oracle VM VirtualBox
Network Connection Details

Network Connection Details:

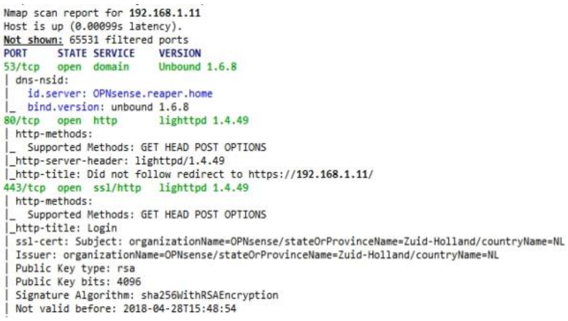
Property	Value
Connection-specific DNS S...	
Description	Intel(R) PRO/1000 MT Desktop Adap
Physical Address	08-00-27-6B-40-BC
DHCP Enabled	No
IPv4 Address	192.168.1.16
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	192.168.1.1

Figure 10
Suricata IDS/IPS EICAR Test Virtual Machine Environment

Nmap initial scan to test the IDS/IPS

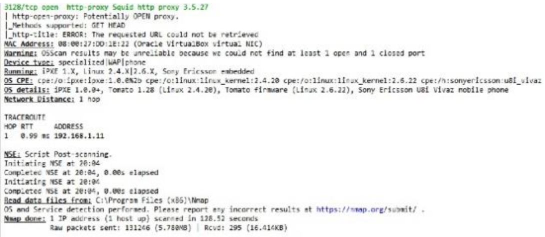
The purpose of the following analysis is to demonstrate how the UTM reacts to a Nmap (Network Mapper) scan. Nmap has many features, which are explicitly designed to circumvent Firewall defenses, and it's as “a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime” [12].

The test ‘Laptop2’ in this scan connects to the CISCO switch Ethernet LAN port to demonstrate how effective it is to acquire network information about the environment. A simple test could demonstrate how it can benefit the user in starting to obtain data that could provide the starting point for future vulnerability analysis of your network by determining which ports are vulnerable because they could be open and not required to be open. The objective of this particular scan is to demonstrate by scanning the LAN Gateway IPv4 192.168.1.11/24 for all TCP ports with the option of ‘Intense Scan’ how the UTM Suricata IDS/IPS reacted by dropping the ‘SYN’ and ‘ACK’ packets. DNS (Domain Name Service) port 53, HTTP port 80, port 443 SSL/TLS is also ‘open.’ Finally, the ‘Squid’ proxy port 3128 used for Caching Proxy is also ‘open.’ The other ports appear to be filtered by the Firewall. Additional details include the software appliance version, kernel, and the server domain. An administrator, later on, can create firewall rules, block ports and create policies as required in the network environment.



```
Nmap scan report for 192.168.1.11
Host is up (0.00099s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE    VERSION
53/tcp   open  domain     Unbound 1.6.8
| dns-nsid:
|   id.server: OPNsense.reaper.home
|_  bind.version: unbound 1.6.8
80/tcp   open  http       lighttpd 1.4.49
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: lighttpd/1.4.49
|_http-title: Did not follow redirect to https://192.168.1.11/
443/tcp  open  ssl/http   lighttpd 1.4.49
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Login
| ssl-cert: Subject: organizationName=OPNsense/stateOrProvinceName=Zuid-Holland/countryName=NL
| Issuer: organizationName=OPNsense/stateOrProvinceName=Zuid-Holland/countryName=NL
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2018-04-28T15:48:54
```

Figure 11
Nmap Scan Report Part 1

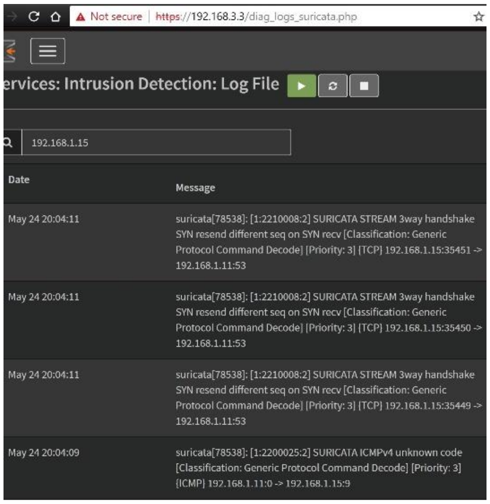


```
3128/tcp open  http-proxy Squid http proxy 3.5.27
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported: GET HEAD
|_http-title: ERROR: The requested URL could not be retrieved
MAC Address: 08:00:27:DD:1E:22 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|WAP|phone
Running: iPXE 1.X, Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:ipxe:ipxe:1.0.0%2b cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: iPXE 1.0.0+, Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.99 ms 192.168.1.11

NSE: Script Post-scanning.
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.52 seconds
           Raw packets sent: 131246 (5.780MB) | Rcvd: 295 (16.414KB)
```

Figure 12
Nmap Scan Report Part 2



Not secure | https://192.168.3.3/diag_logs_suricata.php

ervices: Intrusion Detection: Log File

192.168.1.15

Date	Message
May 24 20:04:11	suricata[78538]: [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1.15:35451 -> 192.168.1.11:53
May 24 20:04:11	suricata[78538]: [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1.15:35450 -> 192.168.1.11:53
May 24 20:04:11	suricata[78538]: [1:2210008:2] SURICATA STREAM 3way handshake SYN resend different seq on SYN recv [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.1.15:35449 -> 192.168.1.11:53
May 24 20:04:09	suricata[78538]: [1:2200025:2] SURICATA ICMPv4 unknown code [Classification: Generic Protocol Command Decode] [Priority: 3] {ICMP} 192.168.1.11:0 -> 192.168.1.15:9

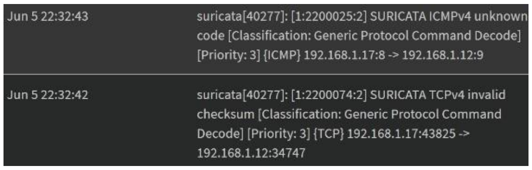
Figure 13
IDS/IPS-SYN Stream Request 3-Way Handshake Detection

Wireshark capture scans to test the IDS/IPS

Wireshark is an open-source network packet analyzer. “A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. It lets you observe what’s happening at a microscopic level” [13]. Utilizing Nmap in the ‘VM’ and running Wireshark in ‘Laptop2’ (using port mirroring with the CISCO switch). Executing the command ‘nmap -sS -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,12’ [Figure 17], can start to demonstrate the power and versatility for testing an IDS/IPS system with this methodology. The ‘-sS’ is a TCP SYN (3-way handshake) scan. For the ‘SYN’ scan if the server didn’t send an ‘RST’ packet to terminate the connection, then the server didn’t reply back, and Nmap will indicate that the target IP port as filtered [Figure 11]. This is a sign that there might be that a firewall is on the server side blocking the reply packets. The -sV’ probes open ports to determine service/version info. The ‘-T4’ goes up to

‘5’ and is the ‘aggressive’ timing template. A normal scan is ‘T3’ but it’s a much slower scan. The ‘-O’ will try and detect the Operating System of the target. The ‘-v’ will print verbose (detailed) output. The ‘-Pn’ will treat the host targets as online and skip the ‘ping’ host discovery and to skip when the host is filtering ICMP packets. The ‘--badsum’ will send packets with a bogus TCP/UDP/SCTP checksum [Figure 14] [Figure 15]. The ‘-mtu 8’ option is used to fragment probes into 8-byte packets [Figure 16]. This option causes the scan to use small fragmented IP packets by splitting up the TCP header over several packets to make it harder for packet filters and intrusion detection systems. The ‘top-ports 1000’ is to scan the most common ports. “The top 1,000 (out of 65,536 possible) finds roughly 93% of the open TCP ports and more than 95% of the open UDP ports” [12]. The target IP’s are the LAN/WAN IP’s of the Host and OPNsense [Figure 5].

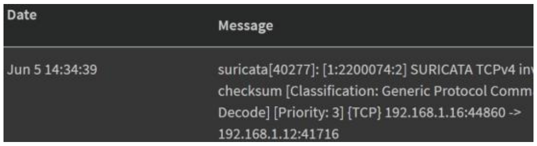
The Wireshark ‘tcp.analysis.flags’, and ‘tcp.flags.syn == 1’, ‘follow tcp stream’ are very effective. The ‘ip.addr ==x.x.x.x && ip.addr == x.x.x.x’ filter can set a conversation between the two IP’s to watch the communication between two specific hosts since the '&&' will return both conditions in the statement [Figure 18-20]. The pattern that starts to emerge is that have effective results one must use Nmap less aggressively and approach IDS/IPS more stealthily. The fragmented IP header command is an example since it received less flags in Wireshark compared to Connect, ACK, TCP Null, FIN and Xmas scans [12] [Figure 19].



```
Jun 5 22:32:43    suricata[40277]: [1:2200025:2] SURICATA ICMPv4 unknown
                  code [Classification: Generic Protocol Command Decode]
                  [Priority: 3] {ICMP} 192.168.1.17:8 -> 192.168.1.12:9

Jun 5 22:32:42    suricata[40277]: [1:2200074:2] SURICATA TCPv4 invalid
                  checksum [Classification: Generic Protocol Command
                  Decode] [Priority: 3] {TCP} 192.168.1.17:43825 ->
                  192.168.1.12:34747
```

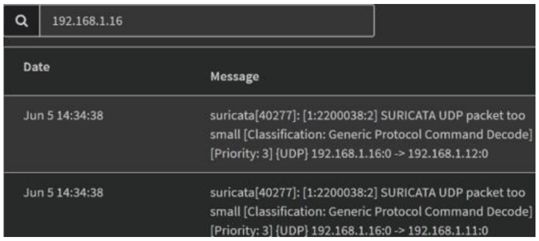
Figure 14
IDS/IPS ICMPv4 Unknown Code at WAN IP’s Interface Alert



```
Date              Message

Jun 5 14:34:39    suricata[40277]: [1:2200074:2] SURICATA TCPv4 in
                  checksum [Classification: Generic Protocol Comm
                  Decode] [Priority: 3] {TCP} 192.168.1.16:44860 ->
                  192.168.1.12:41716
```

Figure 15
IDS/IPS TCP Invalid Checksum Alert



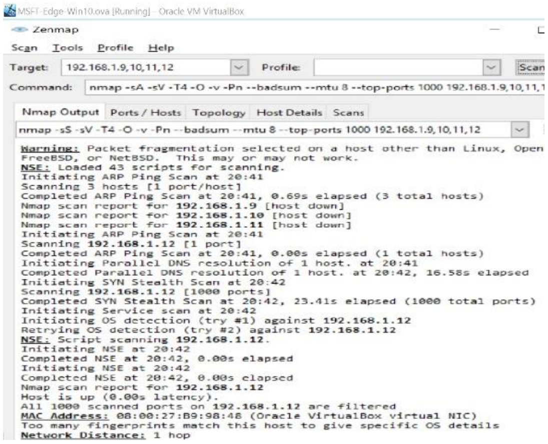
```
192.168.1.16

Date              Message

Jun 5 14:34:38    suricata[40277]: [1:2200038:2] SURICATA UDP packet too
                  small [Classification: Generic Protocol Command Decode]
                  [Priority: 3] {UDP} 192.168.1.16:0 -> 192.168.1.12:0

Jun 5 14:34:38    suricata[40277]: [1:2200038:2] SURICATA UDP packet too
                  small [Classification: Generic Protocol Command Decode]
                  [Priority: 3] {UDP} 192.168.1.16:0 -> 192.168.1.11:0
```

Figure 16
IDS/IPS-Alert for UDP Fragmented IP Packets Alert

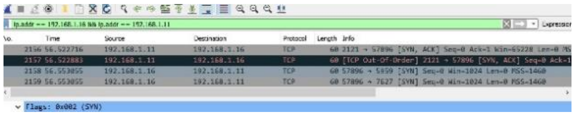


Target: 192.168.1.9,10,11,12
Profile:
Command: nmap -sA -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,1

```
nmap -sS -sV -T4 -O -v -Pn --badsum --mtu 8 --top-ports 1000 192.168.1.9,10,11,12

Warning: Packet fragmentation selected on a host other than Linux, Open
FreeBSD, or NetBSD.  This may or may not work.
NSE: Loaded 43 scripts for scanning.
Initiating ARP Ping Scan at 20:41
Scanning 3 hosts [1 port/host]
Completed ARP Ping Scan at 20:41, 0.69s elapsed (3 total hosts)
Nmap scan report for 192.168.1.9 [host down]
Nmap scan report for 192.168.1.10 [host down]
Nmap scan report for 192.168.1.11 [host down]
Initiating ARP Ping Scan at 20:41
Scanning 192.168.1.12 [1 port]
Completed ARP Ping Scan at 20:41, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:41
Completed Parallel DNS resolution of 1 host. at 20:42, 16.58s elapsed
Initiating SYN Stealth Scan at 20:42
Scanning 192.168.1.12 [1000 ports]
Completed SYN Stealth Scan at 20:42, 23.41s elapsed (1000 total ports)
Initiating Service scan at 20:42
Initiating OS detection (try #1) against 192.168.1.12
Retrying OS detection (try #2) against 192.168.1.12
NSE: Script scanning 192.168.1.12.
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
Initiating NSE at 20:42
Completed NSE at 20:42, 0.00s elapsed
Nmap scan report for 192.168.1.12
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.1.12 are filtered
MAC Address: 08:00:27:B9:98:48 (Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

Figure 17
Nmap TCP Scan Output for LAN and WAN Interface IP’s

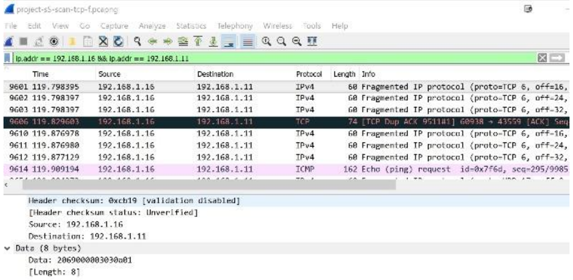


```
ip.addr == 192.168.1.16 && ip.addr == 192.168.1.11

No.   Time        Source         Destination    Protocol  Length Info
 2156 56.522716   192.168.1.11   192.168.1.16   TCP         60 2121 → 57896 [SYN, ACK] Seq=0 Ack=1 Win=65228 Len=0 MS
 2157 56.522883   192.168.1.11   192.168.1.16   TCP         60 [TCP Out-Of-Order] 2121 → 57896 [SYN, ACK] Seq=0 Ack=1
 2158 56.553055   192.168.1.16   192.168.1.11   TCP         60 57896 → 5959 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 2159 56.553055   192.168.1.16   192.168.1.11   TCP         60 57896 → 7627 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

  Flags: 0x002 (SYN)
```

Figure 18
Wireshark Output for SYN Requests TCP/Checksum Out of Order Alert



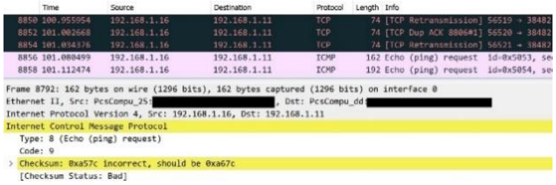
project-sS-scan-tcp-f.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 192.168.1.16 && ip.addr == 192.168.1.11

     Time         Source         Destination    Protocol  Length Info
9601 119.798395   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=16,
9602 119.798397   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=24,
9603 119.798397   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=32,
9606 119.829603   192.168.1.16   192.168.1.11   TCP         74 [TCP Dup ACK 9511#1] 60938 → 43559 [ACK] Seq
9610 119.876978   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=16,
9611 119.876980   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=24,
9612 119.877129   192.168.1.16   192.168.1.11   IPv4        60 Fragmented IP protocol (proto=TCP 6, off=32,
9614 119.909194   192.168.1.16   192.168.1.11   ICMP       162 Echo (ping) request  id=0x7f6d, seq=295/9985

    Header checksum: 0xcb19 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.16
    Destination: 192.168.1.11
  Data (8 bytes)
    Data: 2069000003030a01
    [Length: 8]
```

Figure 19
Wireshark Output for Nmap Fragmented IP Header (MTU 8)



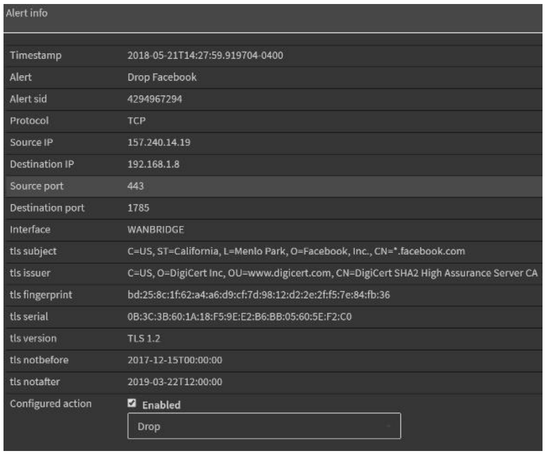
```
     Time         Source         Destination    Protocol  Length Info
8850 100.955954   192.168.1.16   192.168.1.11   TCP         74 [TCP Retransmission] 56519 → 38482
8852 101.002668   192.168.1.16   192.168.1.11   TCP         74 [TCP Dup ACK 8806#1] 56520 → 38482
8854 101.034376   192.168.1.16   192.168.1.11   TCP         74 [TCP Retransmission] 56521 → 38482
8856 101.080499   192.168.1.16   192.168.1.11   ICMP       162 Echo (ping) request  id=0x5053, se
8858 101.112474   192.168.1.16   192.168.1.11   ICMP       192 Echo (ping) request  id=0x5054, se

Frame 8792: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) on interface 0
Ethernet II, Src: PcsCompu_25:[redacted], Dst: PcsCompu_dd[redacted]
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 192.168.1.11
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 9
> Checksum: 0xa57c incorrect, should be 0xa67c
  [Checksum Status: Bad]
```

Figure 20
Wireshark Output TCP and ICMP Checksum Incorrect Alert

IDS Block SSL Certificates

In this implementation briefly explains how to setup OPNsense to drop/block SSL Certificates for SHA-1 (Secure Hashing Algorithm 1) based on their thumbprint/fingerprint property. Afterward, a network administrator could retrieve a SHA-1 thumbprint from the 'Facebook' website. The signature configured with the appropriate settings will result in the IPS logging and 'dropping' the SHA-1 monitored thumbprint and providing alerts with a timestamp and LAN IP and other properties. The first step would be to go to the 'Services>Intrusion Detection' menu, 'Enable' the 'IDS' option. Afterward, one must proceed to the 'Interfaces>Settings' menu to disable 'hardware checksum,' 'TCP segmentation' and 'large receive offload.' After that enable the 'IPS' mode, 'Promiscuous Mode' and press the 'Download' tab to obtain the latest rulesets and set to 'Enable.' Afterward, go to the 'User defined' tab and add a new rule. The thumbprint will be the SSL thumbprint property SHA-1. It is important to note that Certificate Authorities should only issue SHA-2 certificates for website records since Microsoft, Google, and Mozilla ended trust for all SHA-1 SSL Certificates [8]. Using thumbprints is easy to locate a particular certificate for a system. The value of this implementation is that instead of specifying a certificate by subject name, validity property one can supply the thumbprint property to a Web Server, which is more convenient. [8] [9].



Alert info

Timestamp	2018-05-21T14:27:59.919704-0400
Alert	Drop Facebook
Alert sid	4294967294
Protocol	TCP
Source IP	157.240.14.19
Destination IP	192.168.1.8
Source port	443
Destination port	1785
Interface	WANBRIDGE
tls subject	C=US, ST=California, L=Menlo Park, O=Facebook, Inc., CN=*.facebook.com
tls issuer	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 High Assurance Server CA
tls fingerprint	bd:25:8c:1f:62:a4:a6:d9:cf:7d:98:12:d2:2e:2f:f5:7e:84:fb:36
tls serial	0B:3C:3B:60:1A:18:F5:9E:E2:B6:BB:05:60:5E:F2:C0
tls version	TLS 1.2
tls notbefore	2017-12-15T00:00:00
tls notafter	2019-03-22T12:00:00
Configured action	☑ Enabled Drop

Figure 21
OPNsense IDS Block SSL Certificates Suricata Alert

Traffic Shaper

According to OPNsense, Traffic Shaping is "the control of computer network traffic in order to optimize or guarantee performance, lower latency, and can be used to increase usable bandwidth by delaying packets that meet certain criteria" [3]. Traffic Shaping is any action on a set of packets, which imposes an additional delay on those packets such that they adapt to a predetermined traffic profile [3]. According to OPNsense, the organization of the Traffic Shaping interface is around 'pipes,' 'queues and 'rules.' The 'pipes' define the allowed bandwidth, the 'queues' set a weight within the pipe and the 'rules' apply the shaping to a certain package flow. It is essential to know that the 'rules' applied in the 'Traffic Shaper' are handled independently from the firewall 'rules' and that this feature can be combined in the software platform OPNsense [3].

- **Traffic Shaper Terms:** The OPNsense implementation uses 'IPFW' (IP Firewall) and 'Dummynet' by first classifying packets and dividing them into 'flows' [3]. The basis for the bandwidth-defined limits are for or an interface(s), the 'IP (Internet Protocol) source and IP destination,' 'traffic direction inbound or outbound' and the port numbers for applications. The capability of sharing available bandwidth evenly over various end-users is possible if configured allowing for optimum performance [3]. The prioritization of traffic means that applications with a higher weight can consume more bandwidth than other applications when the total available bandwidth is limited. The utilization of adding 'queues' is to determine how different 'flows' share the available bandwidth and defining the appropriate 'weights' in the 'rules' section can be utilized to begin to define the traffic shaping rules of the traffic shaper. The 'weights' are not 'priorities,' which means that there is a guarantee that a 'flow' with a lower 'weight' will get its fraction of the bandwidth even if there is a packet 'flow' with a higher 'weight' permanently backlogged [3].

- **Traffic Shaper Implementation:** One can create various implementations for Traffic Shaping such as reserving dedicated bandwidth for real-time network traffic such as Voice over IP (Internet Protocol), share Internet traffic evenly using ‘queues’ to prioritize applications and multi-interface traffic shaping [Figure 22]. The purposes for traffic shaping can be, for example, to provide time-sensitive real-time financial data traffic throughput a priority over other types of not critical to a business. Another example might be to limit the bandwidth of applications that consume a lot of network traffic when many users are using the same application in the workplace, and the QoS (Quality of Service) is not adequately monitored and balanced, which could affect production [14]. The Windows 10 VM (Virtual Machine) in this network implementation has the assigned IPv4 192.168.1.8 or 192.168.1.16/24. It consists in dividing the Internet download network traffic between the connected Windows 10 VM in ‘Laptop1’ to receive an approximate amount of 10Mbps for the end-user from a maximum bandwidth of 300Mbps. The ‘pipe’ could configuration for a specific resource such as accessing a port through or a Web browser is possible [15].

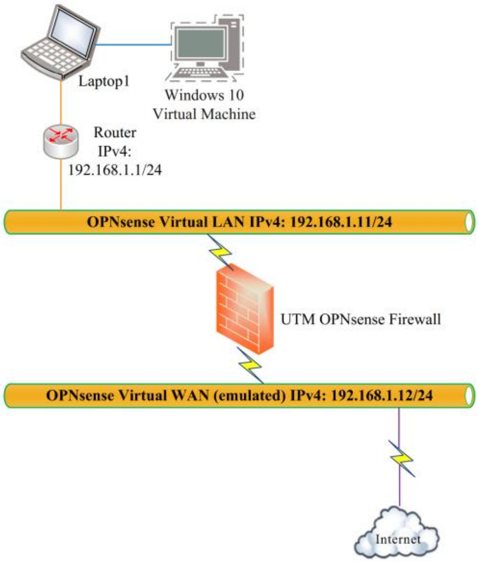
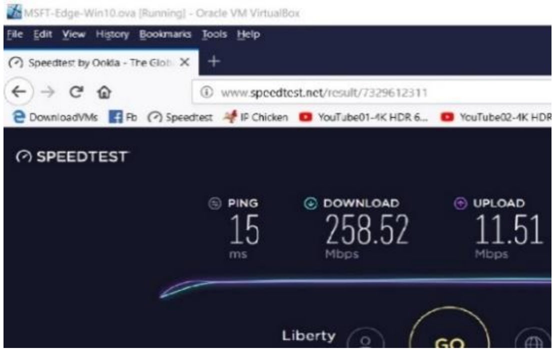

Laptop1
Windows 10
Virtual Machine
Router
IPv4:
192.168.1.1/24
OPNsense Virtual LAN IPv4: 192.168.1.11/24
UTM OPNsense Firewall
OPNsense Virtual WAN (emulated) IPv4: 192.168.1.12/24
Internet

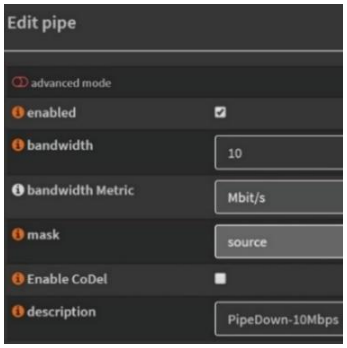
Figure 22
Traffic Shaping Virtual Machine in Laptop1

Once logged in to OPNsense platform the first step would be to proceed to the ‘Firewall>Traffic Shaper>Settings.’ On the ‘Pipes’ tab, one clicks on the ‘+’ button on the corner lower right, and a screen called the ‘Edit Pipe’ appears [Figure 24]. The important aspect is that in the ‘mask’ option drop down menu to select ‘source.’ This option is indicating the ‘pipe’ to select the source to limit bandwidth per client, which is a requirement for this type of traffic shaping implementation. Afterward, it is important to take note of the IPv4 address for the host intended for traffic shaping. If the intended target were the entire LAN (local area network), one would input the appropriate subnet in CIDR (Classless Inter-Domain Routing) notation. In the Traffic Shaper settings click on the on the ‘Rules’ tab and then click the ‘+’ button in the lower corner to the right [3]. The empty ‘Edit rule’ screen will appear in order to create a rule for traffic throughput downloading from the Internet [Figure 26]. In this implementation, OPNsense configures the sequence automatically. Select the ‘LAN Bridge’ interface, according to ‘pipe’ requirements and ports if applicable [Figure 26]. This implementation is only for the Windows 10 Virtual Machine and not for the host ‘Laptop1’ or any other host in the LAN. The entered IPv4/CIDR notation has to go in the ‘Destination’ section with an IPv4 ‘192.168.1.8/24’ obtained in ‘cmd.exe’ [Figure 25]. Afterward, proceed to select the target ‘pipe’ created earlier and press the ‘Apply’ button to enable the implementation.


MSFT-Edge-Win10.ova [Running] - Oracle VM VirtualBox
File Edit View History Bookmarks Tools Help
Speedtest by Ookla - The Glob
www.speedtest.net/result/7329612311
DownloadVMs Fb Speedtest IP Chicken YouTube01-4K HDR 6... YouTube02-4K HDR
SPEEDTEST
Liberty
GO

PING 15 ms
DOWNLOAD 258.52 Mbps
UPLOAD 11.51 Mbps

Figure 23
Windows 10 VM Speedtest without Traffic Shaping



Edit pipe

advanced mode

enabled ☑

bandwidth 10

bandwidth Metric Mbit/s

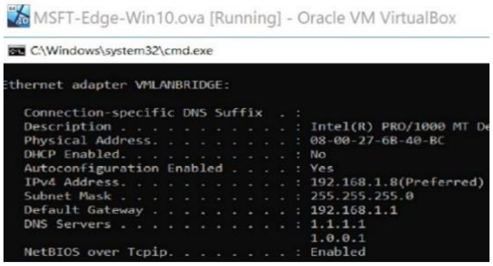
mask source

Enable CoDel □

description PipeDown-10Mbps

Figure 24

Edit Pipe Graphical User Interface



MSFT-Edge-Win10.ova [Running] - Oracle VM VirtualBox

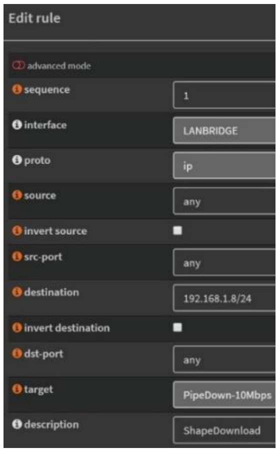
C:\Windows\system32\cmd.exe

```
Ethernet adapter VMLANBRIDGE:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT De
   Physical Address. . . . . . . . . : 08-00-27-6B-40-BC
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DNS Servers . . . . . . . . . . . : 1.1.1.1
                                       1.0.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 25

LAN VM Internet Protocol Configuration



Edit rule

advanced mode

sequence 1

interface LANBRIDGE

proto ip

source any

invert source □

src-port any

destination 192.168.1.8/24

invert destination □

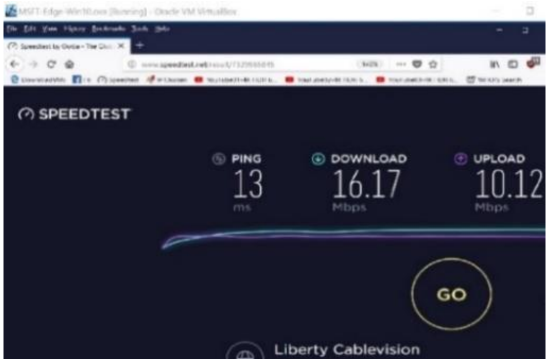
dst-port any

target PipeDown-10Mbps

description ShapeDownload

Figure 26

Edit Rule Graphical User Interface



SPEEDTEST

PING 13 ms

DOWNLOAD 16.17 Mbps

UPLOAD 10.12 Mbps

Figure 27

Windows 10 VM Speedtest with Traffic Shaping Applied

FUTURE WORK

To develop and maintain an effective IDS/IPS, one must take into account how everyone participating in the OPNsense community official forums can effectively be involved to improve the Suricata IDS/IPS and other features. An area future work could be combining features such as the Caching Proxy, testing the UTM Web Filtering protection against viruses and malware. In addition, Traffic Shaper queues, High Availability and enabling QoS (Quality of Service) in parallel with the Suricata IDS/IPS to improve network security [3]. Moreover, deploying the supported OPNsense Amazon Web Services cloud image deployment can be beneficial, and it provides additional processing capabilities from a data center for telemetry capture and Data Governance when the demand exists for small and medium business deploying infrastructure migration to a Cloud platform [3]. Furthermore, future work testing with Nmap can prove to be effective in identifying gaps in the Firewall IDS ruleset and open ports that can be set to 'closed.' Kali Linux Metasploit Framework, which is "a penetration testing platform that enables you to find, exploit, and validate vulnerabilities" [16], it's the most thorough recommended approach for IDS/IPS testing since it provides "the infrastructure, content, and tools to perform penetration tests and extensive security auditing" [16]. Utilizing a database of exploits, one can safely simulate real-world attacks on a network to train the experts to spot and stop cyber-attacks [16].

CONCLUSION

This paper presented the market demand for network security appliances, which the UTM shares. The paper focusses in providing the OPNsense software appliance features deployed in a virtual secure network environment. The benefits of combining the functional characteristics of an Inline Firewall in parallel with that of ClamAV (Anti-Virus), an IDS/IPS (Intrusion Detection and Prevention System) features and Traffic Shaping help to provide multiple layers of security that are transparent to the end-user to configure and therefore highly beneficial. OPNsense provides an effective way to identify and analyze some challenging issues that are present nowadays in network security for current small and medium-sized businesses; however, it is essential to keep in mind that hardware appliances also exist but each day become more exclusive to the Enterprise level market because of the cost. The first line of protection in any small and medium size network could be a Free Open Source Software UTM appliance because it monitors your zone effectively and does not consume too much footprint in the infrastructure. Therefore, an open source software UTM is an attractive solution particularly if it provides an integrated Inline Firewall, Anti-Virus, and IDS/IPS features.

Furthermore, it provides a lower initial up-front cost as well as less management for appliances, lower software support costs and less overhead expenses requirements that should help in the ability to mitigate the incoming/outgoing network threats. A UTM also provides simplicity in its initial setup to protect systems efficiently, and comprehensive configurations for complex hybrid environments are possible if required. Therefore, it is essential to consult with professionals to audit vulnerabilities and security holes. If authorized, it could be ideal to deploy OPNsense in a real production environment to provide compliance Vulnerability, Business Impact Analysis, and Risk Assessments to support all future business continuity requirements [4] [14] [15] [17].

REFERENCES

[1] Gartner IT Glossary. (2018). *Unified Threat Management (UTM)* Available: https://www.gartner.com/it-glossary/unified-threat-management-utm/.

[2] Moore, S. (2017, November 2). *Focus on the Biggest Security Threats, Not the Most Publicized*. [Online]. Available: https://www.gartner.com/smarterwithgartner/focus-on-the-biggest-security-threats-not-the-most-publicized/.

[3] OPNsense. (2016). *Welcome to OPNsense's documentation!* [Online]. Available: https://wiki.opnsense.org/index.html.

[4] Complytec Enterprise Compliance (n. d.). *Fortinet - Next Generation Firewall (NGF) Unified Threat Management (UTM)*. [Online]. Available: http://complytec.com/products/fortinet-unified-threat-management/.

[5] IDC. (2018). *Worldwide Spending on Security Technology Forecast to Reach $81.7 Billion in 2017* [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS42425417.

[6] IDC. (2018). *UTM and Firewall Growth Drive the Worldwide Security Appliance Market Expansion in Q2 2017* [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS43066017.

[7] Suricata Open Source IDS. (n. d.). *Suricata Features* [Online]. Available: https://suricata-ids.org/features/.

[8] V. Lynch. (2016, September 21). *Why Your SSL Certificate Still Has A SHA-1 Thumbprint* [Online]. Available: https://www.thesslstore.com/blog/ssl-certificate-still-sha-1-thumbprint/.

[9] M. Simonsen. (2013, April 16). *How Certificates Use Digital Signatures*. [Online]. Available: https://morgansimonsen.com/2013/04/16/understanding-x-509-digital-certificate-thumbprints/.

[10] ClamAV. (2004). *About ClamAV* [Online]. Available: https://www.clamav.net/.

[11] *EICAR*. (1998). *Intended Use – Anti-malware Testfile* [Online]. Available: http://www.eicar.org/86-0-Intended-use.html.

[12] Nmap. (n. d.). *Nmap Security* [Online]. Available: https://nmap.org.

[13] Wireshark. (n. d.). *About Wireshark* [Online]. Available: https://www.wireshark.org/.

[14] A. Froehlich. (2016, August 15). *The Basics of QoS*. [Online]. Available: https://www.networkcomputing.com/networking/basics-qos/402199215.

[15] S. Gibson. (2016). *Shields UP!! Port Authority Edition* [Online]. Available: https://www.grc.com/port_80.htm.

[16] Kali Tools. (2018). *Metasploit Framework* [Online]. Available: https://tools.kali.org/exploitation-tools/metasploit-framework.

[17] C. Brodbeck. (2018, February 8). *NGFW and UTM Firewall: Find out the main differences* [Online]. Available: https://ostec.blog/en/perimeter/firewall-utm-ngfw-differences.