Cyber Security Attacks on Network with Transition Mechanisms

Shaneel Narayan, Ruchinav Gupta, Avinesh Kumar, Salman Ishrar, Ziafil Khan
Unitec Institute of Technology
Auckland, New Zealand
Email: snarayan@unitec.ac.nz

***Abstract*—Cyber security is a big part of the Internet nowadays. There are cyber-attacks happening around the world right this very moment. Attacker mainly target national or corporate organizations and use cyber-attacks to attack and penetrate their network, which include the server, routers and computers. Transition mechanisms such as NAT64, 6to4, 4to6, 4in6, 6rd, Dual Stack and ISATAP were developed by Internet Engineering Task Force (IETF) to establish communication between IPv4 and IPv6 standards. There has not been much research done in the past to show how secure these transition mechanism are. This paper shows the performance and comparison between 4to6 transition mechanism and 6to4 transition mechanism when attacked by various cyber-attacks such as the Nmap, Zenmap, Smurf6 and flood router6. This paper also compares how both the transition mechanisms perform when Virtual Private Network (VPN) such as PPTP and IPsec are configured and the different cyber-attacks are executed. The average values of UDP and TCP delay and jitter for each of the tests that was performed are shown in the graphs.**

Keywords - *Cyber-attacks, transition mechanism, 4to6, 6to4, PPTP, IPsec, VPN, performance evaluation.*

I. Introduction

Cyber-attacks are politically or socially motivated attacks which are mainly carried out over the Internet. These attacks can be performed by an individual or organizations that mainly target the national or corporate organization by hacking into their infrastructure, computer systems and their networks. The attacks can use malicious programs and codes to hack in the network or computer system of their specified targets to either steal, alter personal or institutional information from them or possibly bring down an entire network. In this research, cyber-attacks are simulated on networks with different transition mechanisms, 4to6 and 6to4 alongside with different virtual private networks to compare their network performance.

A transition mechanism is technology that is used to establish communication between IPv4 standard and IPv6 standard [1]. As we know that IPv4 address availability is close to being fully allocated, the Internet Engineering Task Force (IETF) has developed a new standard, IPv6 [1]. This new standard has got more IP addresses than the older IPv4 standard which can be used to fulfil the need for the IP addresses wanted now and/or in the near future [2]. In order for the transition to happen between the IPv4 standard and IPv6 standard, Internet Engineering Task Force (IETF) have developed different types of transition mechanisms such as NAT64, 6to4, 4to6, 4in6, Dual Stack, Teredo and ISATAP [3]. This research will solely focus on the 4to6 and 6to4 transition mechanisms and how the performance differ when they are attacked. Transition mechanisms perform when they are being attacked with different Virtual Private Networks (VPN) that have been configured on them. There are different types of VPN available such as Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPsec), Secure Socket Layer Protocol (SSTP) and Secure Socket Layer (SSL). We will only focus on PPTP and IPsec VPNs. The results graphed from the attacks with VPNs configured will be compared to the attacks performed on the on the transition mechanism without VPNs.

There are many different types of cyber-attacks available on the Internet which can be used to attack the transition mechanism such as ARP spoofing, which is a Man-In-The-Middle attack, Nmap, Zenmap, Smurf6, Urlsnarf, Intense DOS attack and username and password sniffing. Few types of attacks which we will only focus on are Nmap, Zenmap, Smurf6 and flood router6 attacks to launch attacks on the transition mechanism, both with and without the two VPNs and compare the results with each other.

II. Background

There are many types of attacks which has been attempted on IPv4/IPv6 networks. Mostly on the IPv4 network attackers have been successful in gaining credentials and gaining confidential data out of some of worlds largest companies. Cyber-attacks are known as the most effective attack which results in disruptive consequences that can compromise personal information and leads to cybercrimes. Cyber-attacks includes identity theft, Denial-of-Service attacks (DoS), password sniffing and IP spoofing.

The first proper attack that was done was in the late 1980s to the early 1990s which was called The First Computer Worm done by Robert Morris [4]. This was a self-propagating virus which spread very aggressively and quickly that it was successful in shutting down most of the Internet [4]. This virus created by Morris was a landmark incident for being the first widespread instance of a DoS attack, but since the Internet was just at its beginning stage,

978-1-4673-7309-8/15/$31.00 ©2015 IEEE

the impact was of this attack was not as devastating as it would have been in todays time[4].Compared to the attack by Robert Morris, the attacks now days have become much more intense and more devastating. Today cyber-attacks are used to hack and steal money and personal information from the general public, banks and organizations [5]. A cybercriminal gang with members from Ukraine, China and Russia have attacked up to 100 banks and financial institutions across the world in an unprecedented cyber robbery [5]. This gang of cybercriminals started operating since 2013 and are still operating till date. They have stolen roughly 1 billion dollars so far [6] and are still continuing to do so.

Flood router6 attack is a type of denial of service attacks or an intense network flooding technique, which can be used to crash routers as well as the entire network. This usually happens because your system and the network provides no security from cyber-attacks. Network Mapper (Nmap), is another cyber-attack which is a free scanning tool for exploring the network for security purposes or hacking [10]. It rapidly scans large networks and finds open ports, closed ports, mac addresses and may also include operating system details of the host machine [10]. When a scan is requested Nmap provides information on IP protocols rather than listening to ports [10]. The third cyber-attack which we are focusing on is Zenmap. This is just a GUI version of the Nmap, it is a free and a open source application which is supported by multi-platforms such as Linux, Windows, Mac OS X, BSD [7]. The aim of Zenmap is to make the use of Nmap easier for the beginners as well as advanced users [7]. Our fourth cyber-attack is called Smurf6. Which is a type of distributed denial of service (DDoS) attack which is an attack that can crash computer systems or a network by flooding it with spoofed ping messages [8]. Flooding the victims network or the system, will create high computer traffic, resulting the network or the systems to become unresponsive or crash depending on the type of DDoS [8]. Smurf6 program achieves tasks by finding and exploiting the vulnerabilities of the Internet Protocol (IP) [9] and the Internet Control Message Protocols (ICMP). Distributed Internet Traffic Generator (D-ITG) was used to measure performance metrics such as jitter and delay. D-ITG supports both IPv4/IPv6 UDP and TCP traffic types. This tools is capable of generating traffic at network, application and transport layer [21]. We chose D-ITG for this performance testing as it supports windows operating systems, works through windows command shell and also multiple flows of traffic can be generated by sending multiple flows to achieve adequate results. In our earlier research [18,19,20], the same tool has been used.

IPsec is a virtual private network (VPN) protocol that helps to ensure private and secure communication of data over the Internet Protocol (IP) by using cryptographic security service [11]. It is used for data authentication, confidentiality and integrity when data is being transferred between communication points across the network [12]. IPsec protocol provides data security at the IP packet level.

Point to point protocol is a communication protocol which allows computers to have a direct connection with each other. This connection is authenticated and encrypted to provide a secure transmission [13]. This is a full duplex protocol and can be used on many types of physical devices. The packet is encapsulated using High Speed Data Link Control (HDLC) [13]. PPTP protocol uses hashed and clear text passwords or Challenge Handshake Authentication Protocol (CHAP) [14], for data authentication.

III. Related Research

Research done in the past related to security and transition between IPv4 and IPv6 [3], which shows the potential security issues and vulnerabilities during the transition period between the two protocols. It also mentions some mechanism and solutions in order to prevent the problems that have been identified [3]. Other researches in the past have showed analysis on the behavioural of an IPv4 malware when it is attacked on an IPv6 network. The Nimda worm was used to do this research to further understand how IPv4 malware behaved on IPv6 network. The results showed that IPv6 network environment was still able to get infected by the IPv4 malware, even without any modifications on the existing malware [15]. IPv6 security threats and possible solutions [16], was a research that analysed how different types of attacks and security threats affect IPv6 networks. Security tests were also done on different transition mechanisms such as dual-stack, 6to4 and teredo. Based on the results gathered from the tests, possible solutions were given for the security threats [16]. Security on IPv6 research discussed the security measures that are available for IPv4 network explaining few common security mechanisms which include some type of attacks and IPsec [17]. It also discusses few prototypes of network attacks in the IPv6 network.

IV. Experimental Setup

An IPv4 network will have two computers. One will be the victims computer and the other will be the attackers computer (Intel Core i7 4770 CPU 3.40 GHz, 8 GB Ram). Both computers will have one network interface card each, which are connected to a TP Link Gigabit Switch (1000Mbps) which has 8 ports via a Cat5e cable (1000Mbps). ISP for the network was supplied when a Cat5e cable is connected from the wall port to the gigabit switch which gave Internet access to both the computers in the network. With all the hardware being consistent, Windows 7 operating system was installed on the victim's computer and the attacker's computer will have Kali Linux as an operating system installed on it.

ARP spoofing is a type of Man-In-The-Middle (MITM) attack that was executed first on the network. This GUI based attack allows the attacker to capture the images from the victims computer, while the victim is browsing the Internet. The attacker can also keep a log of all the images that were captured from the attack. Nmap was the second

attack that was performed on the network to obtain the MAC address of the victims computer. Zenmap was the next attack that was is a similar attack to Nmap but will gather more information from the victims computer. Information that was collected by this attack from the victim computer was MAC address, host name, computer OS and all open ports available. Password and username sniffing was the fourth attack that was performed on the network. This attack is able to get the victims credential such as the username and the password, when the victim logs in to an unsecure website on their computer. Smurf6 attack is a type of a network stress attack that was done on the network. This attack will increase the CPU usage and slow down the victims computer. Urlsnarf is a command line based attack where the attacker is able to grab the url from the victims computer when the victim is browsing any website. The attacker can also use this attack to open the same website on their computer. Flood Router6 is a network stress testing attack that was performed on the network. The attacker can use this attack to flood the CPU usage on the victims computer. This is a similar attack to Smurf6 but with more intense effects as it freezes the computer, therefore the victim has to force restart it.

Figure 1 shows 4to6 network. This network has two cisco routers (2800) which are connected by Cat5e cable on the Fast Ethernet 0/0 interfaces on both the routers. This is the 4to6 tunnel which translates IPv6 address to an IPv4 address as Fast Ethernet 0/1 is configured with IPv4 address on router 1. Fast Ethernet 0/1 is on router 1 is connected to a Host 1 Computer (Intel Core i7-4770 CPU 3.40 GHz, 8 GB Ram), with windows 7 operating system. Fast Ethernet 0/1 on router 2 is connected to a TP link Gigabit switch (1000Mbps) which connects to Host 2 Computer (same hardware specification as Host 1). Host 2 is the server in the network and has windows server 2012 operating system installed. The attacking computer which has Kali Linux installed is also connected to the same switch with the server from where the attacker will be executing attacks to the Host 2 computer on the other side of the transition mechanism.

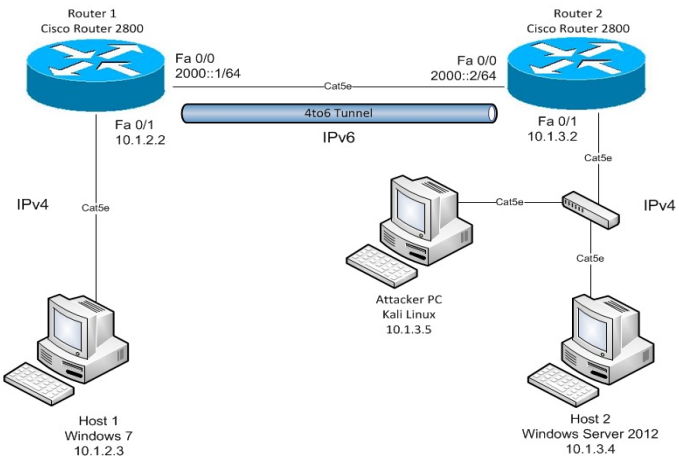

Fig. 1: 4to6 Network Diagram

Fig. 2 shows 6to4 network. This network also has the same cisco routers as similar figure 1. In this network IPv4 is configured on Fast Ethernet 0/0 as the tunnel, which translates to IPv6 address configured on Fast Ethernet 0/1. Fast Ethernet 0/0 is connected to the TP link gigabit switch which connects Fast Ethernet 0/0 on router 2 to establish end to end connectivity. On router 1 Fast Ethernet 0/1 connects to Host 1 Computer. Host 1 has windows 7 operating system installed. The attacking computer has Kali Linux installed which is connected to the TP link gigabit switch. This is where the attacker will launch all the possible attacks.

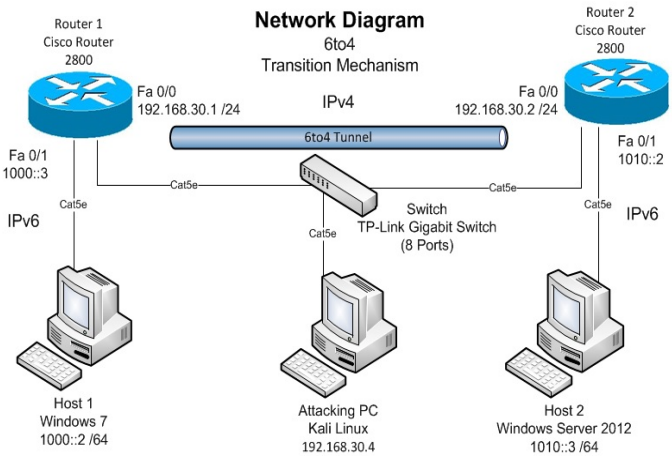

Fig. 2: 6to4 Network Diagram

V. Results and Discussion

All the results shown in this section were measured using D-ITG software with the constant value of packets being sent from sender to receiver at 200,000 and the timeframe of the packets being sent at 20 seconds. All the test were performed on each packet size four times.

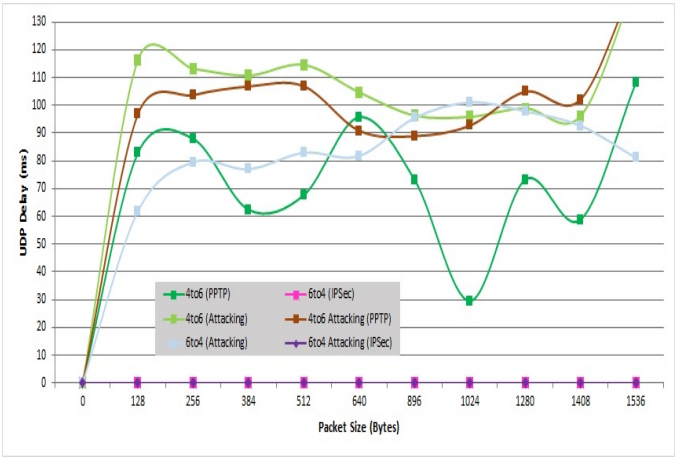

Fig. 3: UDP Delay

Fig. 3 shows the UDP delay of the two transition mechanisms, 4to6 with Point-to-Point Tunnelling Protocol and 6to4 has IPsec virtual private network (VPN) configured

on them. D-ITG was used to measure and record the data for all the packet size that were selected as shown in the graph. The UDP delay for 4to6 transition mechanism with PPTP VPN has increased rapidly till the first packet size which is 128 bytes with the average value around 82ms. The values are not constant as there were few drops in delay around 384 and 1408 packet size with one big drop at the 1024 packet size. In comparison to the other transition mechanisms, 6to4 with IPsec VPN configured on it cant be measured therefore the values for each packet size are all 0s.

Attacks were executed on the both the transition mechanism without any VPN being configured on them. Attacks such as flood router6, smurf6, nmap and zenmap were performed on both the transition and the data was recorded as shown in graph 1. As per the graph, the UDP delay for the 4to6 transition mechanism started with a rapid increase from 0 till the first packet and was fairly constant onwards till 1408 packet size. The average highest and the lowest values being around 114ms and 95ms, but increased dramatically for the 1536 packet with the average value being around 143ms. In comparison to the 6to4 transition mechanism with the attacks being performed on it, the average values of this transition mechanism are very low. The 128 byte packet size has the average value 61ms compared to the 128 bytes packet in 4to6 transition mechanism has the average value 116ms. The average values gathered from the 6to4 transition mechanism are fairly constant, with the lowest average value being at 61ms and the highest being at 101ms at the 1024 byte packet.

Attacks were performed on both, 4to6 and 6to4 transition mechanisms but this time they had VPN configured on them. As shown in the graph, the data collected by attacking the 4to6 transition mechanism with PPTP VPN configured is fairly constant till the 1408 byte packet size but the value increase dramatically for the 1536 byte packet size with the average value of 145ms. Compared to the 4to6 transition mechanism with attacks and PPTP VPN, the 6to4 transition mechanism with IPsec VPN cant be measured therefore all the values for that test are 0s.

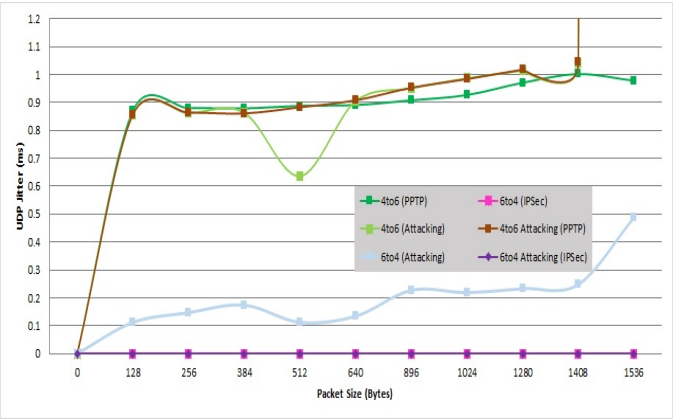

Fig. 4: UDP Jitter

Fig 4 shows the UDP Jitter for the both the transition mechanisms, 4to6 and 6to4 with VPN configured on them. 4to6 transition mechanism with PPTP configured has a rapid increase till the first packet at 128 byte packet size with the average value at 0.871ms from where it stays quite constant till the end at 1536 byte packet size with the average value 0.978ms. Compared to the 4to6 transition mechanism, the 6to4 transition mechanism with IPsec is recorded with 0 values for all the packet sizes as it cant be measured.

Attacks such as the Flood Router 6, Smurf6, Nmap and Zenmap were also executed again and the values were recorded as such. When 4to6 transition mechanism was attacked, the average values were very similar to the values recorded for the 4to6 transition mechanism with PPTP VPN configured. The only two big difference was at the 512 and the 1536 byte packet size, where the value dropped by about 0.23ms with the average value of 0.63ms. The second difference was that at 1536 byte packet size the average value shot up a lot with the value being at 63.88ms and comparing to the all the other packet sizes being at a maximum average value of 1 being the highest, the 1536 byte packet size is extremely high. Compared to the attacks being performed on 4to6 transition mechanism, the 6to4 transition mechanism had a very low value for all the packet sizes. The highest average value was 0.48ms for the 1536 byte packet size and the lowest being at 0.11ms for the 128 byte packet size. All the values for the packets in between 128 and 1536 byte packet size were consistent.

The attacks were once again performed on the both 4to6 and 6to4 transition mechanism while they had VPN (PPTP and IPsec) configured. The average values for 4to6 transition mechanism had a rapid increase till 128 byte packet size with the average value of 0.85ms and another at 1536 byte packet size with the average value of 59.86ms. All the values for the packets between the two were consistent. In comparison to 4to6 transition mechanism with attacks and VPN, the 6to4 transition mechanism with IPsec cant be measured therefore all the values for the packets are kept at 0.

Fig 5 shows the TCP delay of the 4to6 transition mechanism with PPTP and 6to4 transition mechanism with IPsec VPN configured. As shown in the graph the 4to6 transition mechanism has a gradual increase till the 128 byte packet size with the average value of 60.64ms and then remained constant till the 1536 byte packet size with the highest average value being 83.76ms and the lowest average value being 60.64ms. Comparing to 6to4 transition mechanism with IPsec VPN configured, 4to6 transition mechanism has a very low delay. 6to4 transition mechanism has a rapid increase till 128 byte packet with the average value of 139.02ms and has gone down by 13ms till the 640 byte packet size before increasing rapidly to 267.56ms till 1024 byte packet size and has been fairly constant till the last packet size of 1536 byte with the average value of 279.57ms.

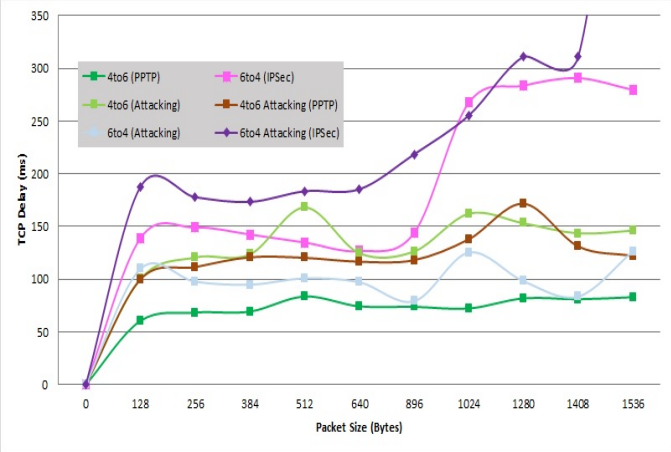

Fig. 5: TCP Delay

Attacks were executed on both the transition mechanisms without any VPN configured on them to record the data for TCP delay as shown in graph 3. As per the graph, average values recorded for the attacks performed on 4to6 transition mechanism were fairly consistent. There were only two packet sizes where the average values had increased, 512 and 1024 byte packet size. The average value of 512 byte packet size had increase by 45ms from 123.67ms to 168.19ms before coming back down to 124.77ms at 640 byte packet size. There was another slight jump in delay at 1024 byte packet size of 36ms from 126.48ms at the 896 byte packet size to 162.28ms, from where it remains steady with only a drop of an average value of 20ms till the last packet. Highest and the lowest average values for the 4to6 transition mechanism with attacks are 100.34ms at the 128 byte packet size and 168.19ms at the 512 byte packet size. In comparison to 4to6, the attacks performed on 6to4 transition mechanism had a slightly less delay.

For the third test of TCP delay, both PPTP and IPsec were configured on both the transition mechanisms and the attacks were executed once again. As shown in the graph from the data recorded from 4to6 transition mechanism with VPN configured and attacks performed, was fairly consistent apart from the 1280 byte packet. There was a slight increase in delay for that packet size by 33ms from 138.08ms for 1024 byte packet size to 171.72ms before coming back down to 131.17ms. Compared to the 6to4 transition mechanism with IPsec configured while executing attacks on it had a much higher delay. It increased rapidly till the 128 byte packet with the average value of 187.90ms compared to the 128byte packet size value for 4to6 transition mechanism of 99.94ms. 6to4 transition mechanism remained quite steady till the 640 byte packet size from where it gradually increased till the 1408 byte packet size which had an average value of 311.46ms. The increase between 640 byte packet sizes till 1408 byte packet was by 126ms. One major difference was that the 1536 byte packet size had a dramatic increase in the value from 311.46ms at 1408 byte packet size by 381ms to 692ms. The highest and the lowest values for this test for 6to4 transition mechanism with VPN and attacks were 173.44ms at 384 byte packet size and 692ms at the 1536 byte packet size.

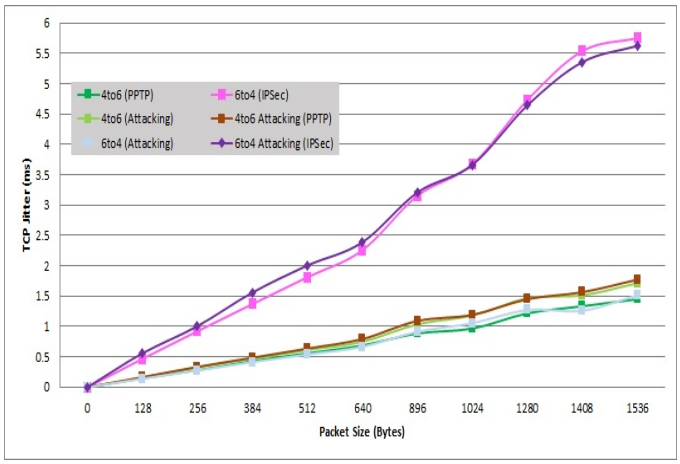

Fig. 6: TCP Jitter

Fig 6 shows TCP jitter values for both 4to6 and 6to4 transition mechanisms with VPN configured. As shown in the graph the 4to6 transition mechanism with PPTP VPN configured on it had an increase from 0.147ms at 128 byte packet size to 1.452ms at 1536 packet size. The increase was at a steady rate with the average value 0.1ms ever packet size. Compared to 4to6, the 6to4 transition mechanism with IPsec configured also had a steady increase but the total average value per packet size was more. The 128 byte packet size for 6to4 transition mechanism had an average value of 0.467ms compared to the 128 byte packet for 4to6 transition mechanism at 0.147ms. The average value for the 1536 byte packet size for 6to4 transition mechanism was 5.755ms, which is much higher than the value for 4to6 transition mechanism which had an average value of 1.452ms. The average values for each packets started increasing from 0.5ms from the 128 byte packet size and got to 1.1ms by the 1408 byte packet size and only increased by 0.2ms for 1536 byte packet size.

Second test for TCP Jitter was by executing attacks on both transition mechanism. As shown in the graph, the average TCP jitter values that were recorded was very much similar to the values with just PPTP VPN configured on it. Values for each packet increased at a steady rate of 0.1ms per packet. The noticeable difference in the graph was that the values for 6to4 transition mechanism with just attacks were very low and similar to the 4to6 transition mechanism with attacks. Whereas the average values for the 6to4 transition mechanism with IPsec VPN configured were very high.

Third test for TCP jitter was by having both transition mechanism, 4to6 configured with PPTP and 6to4 configured

with IPsec VPN and execute the attacks once again. Surprisingly the average values that were recorded for 4to6 transition mechanism with PPTP were very similar to the all the above tests such as 4to6 transition mechanism with just PPTP and 4to6 transition mechanism with just attacks as well as 6to4 with just attacks, but different to the 6to4 transition mechanism with IPsec. Similarly the average values recorded for the 6to4 transition mechanism with IPsec VPN configured and attacks performed were very much the same for the test that was done for 6to4 transition mechanism with just IPsec VPN configured.

VI. Conclusion

This research shows the comparison between two transition mechanisms (4to6 and 6to4) on how they perform, when they are attacked by four different cyber-attacks (Nmap, Zenmap, Smurf6, Flood router6) by measuring two different performance metrics such delay and jitter. D-ITG was used to measure both traffic types (UDP and TCP) on both the networks. The following are some specific conclusions that can be drawn by analysing the results shown in the graphs above.

1.UDP delay shown for 4to6 transition mechanism with PPTP VPN configured on it is not steady. The values for this test range from 30ms to 110ms. Compared to 6to4 transition mechanism with IPsec VPN for which the UDP delay cant be measured at all. The UDP delay for 4to6 transition mechanism with attacks was much higher than the delay for 6to4 transition mechanism with the highest value for 4to6 being at 143ms compared to the highest value for 6to4 being at just 101ms. The delay for 4to6 transition mechanism with attacks and PPTP VPN was measurable and also having a highest value of 145ms, close to the value for just 4to6 transition mechanism with out and attacks, but comparing it to 6to4 transition mechanism with IPsec VPN, that cant be measured at all.

2.The UDP jitter for 4to6 transition mechanism with PPTP was measurable and the values were fairly steady throughout, whereas the jitter values for 6to4 transition mechanism with IPsec was not able to be measured. The jitter values for attack on 4to6 and 6to4 transition mechanism had a big difference because the jitter for 4to6 was much higher than 6to4. The highest average values for 4to6 was around 63ms and for 6to4 was measured around 0.48ms. Similar to UDP delay, the average UDP jitter values for 4to6 transition mechanism with attacks and PPTP VPN was able to be measured, whereas for 6to4 with attacks and IPsec VPN was still not measurable.

3.The TCP delay for 4to6 transition with PPTP had a lowest delay compared to all the other tests for TCP delay. The average values remained steady throughout. 6to4 transition with IPsec VPN was measureable and comparing to 4to6 with PPTP the 6to4 with IPsec was a little bit higher and remained steady will the 896byte packet before rising to an average value between 267ms and 290ms for the remainder of the packet sizes. TCP delay for attacks performed on 4to6 and 6to4 transition mechanism had similar flow and pattern to each other with only one difference being that the average values for 4to6 transition being a little higher than 6to4. Compared to attacks on transition without VPN, the TCP delay for 4ot6 transition mechanism with attacks and VPN had lower values than 6to4 transition mechanism with attacks and VPN. The highest average values for 4to6 being 171ms and for 6to4 being at 692ms.

4.The TCP jitter for all the six tests had two noticeable differences. One was that IPsec VPN was measurable compared to UDP jitter, where it couldnt be measured. The second major difference is that, two tests (6to4 with IPsec and 6to4 with attacks and IPsec have similar values for each packet size and the flow of the graphs for both test are very similar with a maximum difference for the average values being around 0.1ms. Similarly, all the other 4 tests have quite similar values and the flow of the graphs for the tests are also very much the same with the maximum average value change of 0.1ms.

Based on the four conclusion drawn above, the research shows that performance of both the transition mechanism are generally consistent and have similar results in UDP and TCP jitter metrics apart from IPsec. IPsec cant be measured in UDP jitter, whereas for TCP jitter it can be measured. However the performance whereas for TCP jitter it can be measured. However the performance for UDP delay and TCP delay is different with only one similarity to jitter which is the IPsec is not measurable in UDP whereas it is measurable in TCP. One major difference for both UDP and TCP delay is that, 4to6 transition mechanism in general for all the test is higher in UDP compared to the 6to4 transition mechanism being higher in TCP.

References

[1] Khanse.A, *Cyber Attacks Definition, Types, Prevention*. Retrieved from ¡http://www.thewindowsclub.com/cyber-attacks-definition-types-prevention¿.

[2] *What constitutes a cyber-attack*, Information Management: NEC.2015. Retrieved from ¡http://www.nec.com/en/global/solutions/safety/infomanagement/cyberattack.html¿.

[3] T Abidah Hj Mat, T , Perlis, U , Budiarto, R.2007. *Security Mechanisms for the IPv4 to IPv6 Transition*. The 5th Student Conference on Research and Development SCOReD 2007, pp. 1-5.

[4] S. Kamal, B Issac, 2007. Analysis of Network Communication Attacks. The 5th Student Conference on Research and Development SCOReD 2007, pp. 1-6.

[5] *Defining Moments in the history of Cyber-Security*, Infosecurity Magazine. 2015. Retrieved from ¡http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/¿.

[6] BBC News, *BBC Cyber Attacks*. 2015. Retrieved from ¡http://www.bbc.com/news/business-31482985¿.

[7] *How to use Zenmap in Kali Linux. Scan network for victims or intruders*.2015 Retrieved from ¡http://ultimatepeter.com/how-to-use-zenmap-in-kali-linux-scan-local-network-for-victims-or-intruders-find-open-ports/¿.

[8] Janssen C, *What is Smurf Attack. Definition from Techopedia*.2015 Retrieved from ¡http://www.techopedia.com/definition/17294/smurf-attack¿.
[9] *Smurf attack Threats and Mitigation by Kaspersky Lab*. 2015. Retrieved from ¡https://usa.kaspersky.com/internet-security-center/definitions/smurf-attack.VYCePmqqko¿.
[10] Fyodor. Nmap. *Penetration Testing Tools*. 2015. Retrieved from ¡http://tools.kali.org/information-gathering/nmap¿.
[11] *What is IPsec. Security policy; Security Services*.2015. Retrieved from ¡https://technet.microsoft.com/en-us/library/cc776369(v=ws.10).aspx¿.
[12] *What is IPsec. How does it work*.2005. Retrieved from ¡http://documentation.netgear.com/reference/enu/vpn/VPNBasics-3-02.html¿.
[13] Rouse M. *Point to Point Protocol Definition*.2015. Retrieved from ¡http://searchnetworking.techtarget.com/definition/PPP¿.
[14] Point to Point Tunnelling Protocol. Virtual Private Network. 1999. Retrieved from ¡ftp://kierer.at/compaq/partners/microsoft/infolib/ecg5150899.pdf¿.
[15] Zulkiflee M, Azirah S.A, Haniza N, Zakiah A, Shahrim Shahrin S, 2011. *Behavioural Analysis on IPv4 Malware on different platforms in IPv6 Network Environment*. IEEE Conference on Open System (ICOS 2011), pp. 1-6.
[16] Drago Z, Kresimir G, 2006. *IPv6 Security Threats and Possible Solutions*. World Automation Congress (WAC) 2006, pp. 1-7.
[17] Yang D. Song X, Guo Q. 2010. *Security on IPv6*. IEEE 2010, pp. 1-4.
[18] Narayan S, Tauch S, 2010. Network performance evaluation of IPv4-v6 configured tunnel and 6to4 transition mechanisms on windows server operating systems. In *Proceedings of the IEEE International Conference on Computer Design and Applications (ICCDA)*. (Vol. 5, p. 435-440). doi: 10.1109/ICCDA.2010.5540939
[19] Narayan, S, Shi, Y, 2010. TCP/UDP network performance analysis of windows operating systems with IPv4 and IPv6. In *Proceedings of the 2nd IEEE International Conference on Signal Processing Systems (ICSPS)* (Vol. 2, p. 219-222). doi: 10.1109/ICSPS.2010.5555285
[20] Narayan, S, Feng T, Xu, X, Ardham, S, 2009. Network performance evaluation of wireless IEEE802.11n encryption methods on windows vista and windows server 2008 operating systems. In *Proceedings of the IEEE/IFIP International Conference on Wireless and Optical Communications Networks (WOCN)*. (p. 1-5).
[21] D-ITG, Distributed Internet Traffic Generator, 2015, D-ITG, Distributed Internet Traffic Generator, Retrieved from ¡http://traffic.comics.unina.it/software/ITG/¿. 23 June 2015.