EFFECTIVENESS OF SECURITY TOOLS TO ANOMALIES ON TUNNELED TRAFFIC

NAZRULAZHAR BIN BAHAMAN
ANTON SATRIA PRABUWONO
MOHD ZAKI BIN MAS'UD
DR. MOHD FAIZAL BIN ABDOLLAH

(Information Technology Journal)

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Information Technology Journal 11 (2): 191-199, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.191.199
© 2012 Asian Network for Scientific Information

Effectiveness of Security Tools to Anomalies on Tunneled Traffic

[1]Nazrulazhar Bahaman, [1]Anton Satria Prabuwono, [2]Mohd Zaki Mas'ud and [2]Mohd Faizal Abdollah
[1]Faculty of Information Science and Technology, University Kebangsaan Malaysia,
43600 UKM Bangi, Selangor D.E., Malaysia
[2]Faculty of Information and Communication Technology, University Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia

Abstract: Tunneling Mechanism has been proven as an option to link the communication between IPv6 networks and IPv4 environments without incurring the high costs of upgrading equipment. However, this mechanism has reduced the network performance and downgrade the level of security if compared to the native IPv6 network. The Transition Mechanism has also become a covert channel for spreading threats without being acknowledged by the network security tools. Even though the issue has been raised in the set of IETF rules, still they do not provide any recommendation to overcome the problem. Based on this reason, this study explored the effectiveness of conventional network security tools to detect any anomalies occurring on a tunneling mechanism especially against packet flooding attack in IPv6 tunneling. In order to achieve this objective, a testbed that has been deployed with conventional firewall and IDS is used to simulate the IPv6 to IPv4 tunneling mechanism, several network attacks are then launched and the network traffic is then captured to be analyzed. The result shows that the firewall with the default settings had blocked all the tunneling packets, while the firewall and IDS with the default rule of set had performed well in IPv4 but not in the IPv6 tunnel.

Key words: Firewall, intrusion detection, network analyzer, flooding attack, tunneling

INTRODUCTION

In recent years, there has been a significant decrease in the number of unused Internet Protocol version 4 (IPv4) addresses, with Internet users having started focusing on Internet Protocol version 6 (IPv6) (Waddington and Chang, 2002; Hassan and Sailan, 2011). In order to meet the needs of the addresses and overcome the weaknesses, Ipv6 has become an alternative to replace IPv4 as the main Internet Protocol (IP) (Deering and Hinden, 1998; Lee and Chen, 2008). Thus, researchers have begun focusing on IPv6 studies and its security.

Currently, the issue of threats to IPv6 security has become the main research topic (Xinyu *et al*., 2007*)*. Even though IPv6 security studies are being conducted actively, IPv4 security studies are still crucial especially during the transition process. According to Zagar and Grgic (2006), network security should be enhanced due to the implementation of IPv6 transition mechanisms has been offering a new vulnerabilities for network threats. IPv6 is also known as IPng (Internet Protocol Next Generation) designed as a successor to IPv4 by IETF (Internet Engineering Task Force) (Deering and Hinden 1998). The implementation is still at the preliminary level and needs time to be fully implemented as an official IP.

Threats in the IPv6 network is dominated by the Distributed Denial of Service (DDoS) attack that mainly based on four types, which are the Transmission Control Protocol (TCP) flood, the User Datagram Protocol (UDP) flood, the Internet Control Message Protocol (ICMP) flood and Smurfs (Xinyu *et al*., 2007). One of method to give an early notice that an attack is launched is by using the Intrusion Detection System (IDS) (Yoo *et al*., 2011; Bahaman *et al*., 2011). Most IDSes have the ability to successfully detect several kinds of DDoS in the IPv4 and IPv6 environments (Zhang, 2009). Yet, some researcher believes a carefully crafted attack that manipulate the packet encapsulated into the IPv4 packet via protocol type 41 is difficult to be detected by some of IDSes default rules. As protocol type 41 is an important element in the transition mechanism, the threat brought by the protocol type 41 can put the network infrastructure and resources at risk (Taib and Budiarto, 2007). Due to this reason, this paper seeks to address the said problem by looking at each of the possible transition mechanisms and studies its specific weaknesses in anticipating the

Corresponding Author: Nazrulazhar Bahaman, Faculty of Information Science and Technology, University Kebangsaan Malaysia, 43600 UKM Bangi, Selangor D.E., Malaysia potential threats. In order to achieve this goal, an experiment is conducted to test the reliability of network security tools against DDoS threat through this mechanism. ICMP and ICMPv6 flood attacks with valid IP addresses are used as a kind of threat in the experiment as it can be easily detected by IDSes.

Tunneling mechanism: The Tunneling Mechanism (Conta and Deering, 1998; Carpenter and Moore, 2001) is a kind of transition mechanism that encapsulates the IPv6 packet in IPv4 packet. Protocol field type 41 in the IPv4 header or also known as Protocol-41 (Colitti *et al*., 2004) is used by the IPv6 transition mechanism to operate in the IPv4 network. Apart from Protocol-41, packets can also be encapsulated within UDP for the same purpose. The Tunneling Mechanism allows an IPv6 to operate and essentially maintain the IPv4 network. There are several reasons why this mechanism is needed in the present network. One of them is to bring the data to the transmission across networks that are incompatible, or to provide a safe route through the network in which the safety level is unknown.

Tunneling Mechanism allows the host and router in an IPv6 network to communicate with the host and router on the other IPv6 networks through the existing IPv4 network. IPv6 packet deliveries using encapsulated Protocol-41 can be illustrated in Fig. 1. Firstly, Node_A on Network_A sends an IPv6 packet to a gateway on Router_A. Then, after referring to the routing table, the IPv6 packet is forwarded to the tunnel interface. Next, the Router_A encapsulates the IPv6 packet with an IPv4 header. Consequently, the encapsulated packet is forwarded through the tunnel on Network_C and at the end of the tunnel; the receiver router de-encapsulates the packet by removing the IPv4 packet header. Finally, based on the routing table, Router_B sends a packet to the Node_B on Network_B.

All the Tunneling Mechanisms are considered proven as a set of tools to enable a smooth transition to the IPv6. Unfortunately, not all of them are amenable as users' options. According to Karpilovsky *et al*. (2009), Teredo (Huitema, 2006) and 6-4 (Carpenter and Moore, 2001) are the other options for Tunneling Mechanisms, both of the mechanism give more performance compared to other such as 6 over 4 (Carpenter and Jung, 1999), 6 in 4 (Nordmark and Gilligan, 2005), ISATAP (Templin *et al*., 2008), 6rd (Despres, 2010), TSP (Blanchet and Parent, 2010) and DTSM (AlJaafreh *et al*., 2008). The description of the Tunneling Mechanisms is summarized in Table 1.

According to Karpilovsky *et al*. (2009) these transition mechanism technologies are mainly used to avoid restrictions on the Firewall and Network Address Translation (NAT). This situation is a threat and provides a space for attacker to exploit and launched an attack. Although (Savola and Patel, 2004) have explained the security measures for the Protocol-41 packet on RFC 3964, the effectiveness of the firewall and IDS in detecting attacks on this environment is doubtful. Thus, most of firewal products come with default rule which will drop all those packets. Consequently this action has caused all the transition mechanism is unable to be implemented successfully.

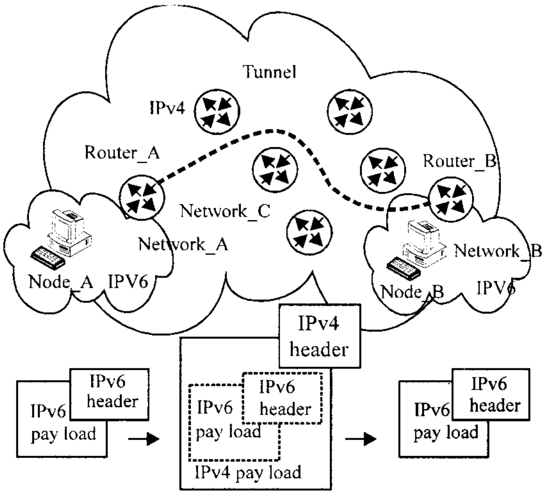


Fig. 1: Principle of IPv6 tunneling process

Table 1: Brief description of IETF tunneling mechanisms

Tunneling mechanism	Site operations	IETF references
6 over 4	Between End-node and Network-Device	RFC 2529
6 to 4	Between Network-Devices	RFC 3056
6 in 4	Between Network-Devices	RFC 4213
Teredo	Between End-node and Network-Device Between End-Nodes Between Network-Devices	RFC 4380
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	Between End-node and Network-Device	RFC 5214
6rd	Between Network-Devices	RFC 5569
Tunnel Setup Protocol (TSP)	Between End-Nodes	RFC 5572
Dual Stack Transition Mechanism (DTSM)	Between End-node and Network-Device	ID dstm-04

The network security tools: Nowadays, several network tools either freeware or commercial has been developed for the purpose to keep the network operation secure. In this study, the research used Firewall and IDS as the main security tool.

IDS is responsible to identify interference, which is defined as an illegal use, misuse or abuse of computer systems by users who are either entities with invalid credentials or external users (Vokorokos *et al.*, 2006). In addition, IDS is also used to help in preparing to defense the internal and the external attacking (Shu-Qiang *et al.*, 2009). One of the objectives in achieving early detection of invasion is to collect information from various systems and networks and analyze the sources of group information, looking for symptoms that lead to safety problems (Razak *et al.*, 2002). By analyzing the success of this information, it can help to detect the invasion activity in the network. Although IDS has the ability to detect invasive behavior, it also has some weaknesses. The following signature is an example of a rule set in IDS that generates an alert if an ICMP packet have an empty payload, TCMP type 8 and arriving from the outside.

```
Alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg:"ICNP
PING NMAP"; dsize: 0; itype: 8;)
```

Yohannes and Xu (2003) and Zagar *et al.* (2007) described firewall as a device or software intended to allow or refuse network transmissions. It is often used to protect networks from unauthorized access while allowing legal traffics to pass based upon a set of rules which can be modified according to current needs. In addition, a firewall provider usually offers free updated rule sets. Therefore, most consumers will take advantage of the default settings and do not change it manually. The firewall is typically placed between a LAN and the Internet and other insecure networks.

Flooding attack: This is a DoS attack (Meenakshi and Srivatsa, 2007; Huang and Meng, 2011) that is designed to bring a network or service down by multiplying out large amounts of traffic towards the target. In a typical distributed version, this attack is created using DoS software as an instrument of attack. Meanwhile a Distributed Denial of Service attack or DDoS is a collection of DoS infected nodes that has been remotely controlled by an attacker to be used for launching a DoS attack towards a target (Sam *et al.*, 2006; Bhaskaran *et al.*, 2007). According to Lee *et al.* (2011). DDoS, attacks may involve breaking into hundreds or thousands of machines all over the Internet. This can be illustrated in Fig. 2.

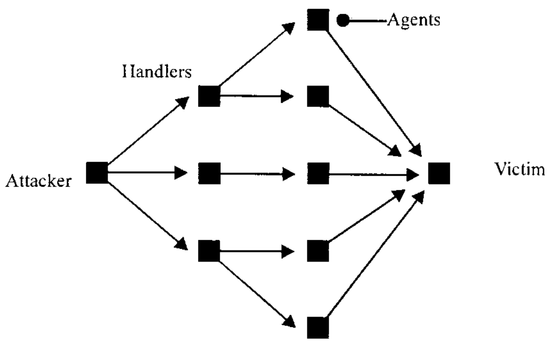


Fig. 2: Distributed Denial of Service Attack

The ICMP flood attack is one of main types of DDoS attack. It is also known as ping flood attacks and makes use of the packet echo response mechanism. The attack is produced when the attacker sends a high volume of echo request ping packet to the victim node repeatedly until the victim node does not have time to serve other services. Even though ICMP has been upgraded to ICMPv6, the problem still remains as some of their primary functions are still the same. Thus flooding attack based on echo request mechanism can still be manipulated by the attacker in order to put down services on a server.

This study look at the effectiveness of conventional network security tools to detect any anomalies occurring on a tunneling mechanism. In order to achieve this objective, a testbed that has been deployed with conventional firewall and IDS is used to simulate the IPv6 to IPv4 tunneling mechanism, several network attacks are then launched and the network traffic is then captured to be analyzed.

PROBLEM AND SECURITY ISSUES

The transition mechanism is developed for the purpose of implementing the new protocol together with the existing one on the real environment without prejudicing it. Today, the use of the transition mechanism has been widely used around the world. For example, Hurricane Electric (HE) acting as a Tunnel Broker (Waddington and Chang, 2002), offers an internet gateway using IPv6 tunneling. Although security about the transition mechanism measures has been stated at (Savola and Patel, 2004), most administrators have less knowledge in this field and expect the default configuration on network security tools such as Firewall or IDS to monitor and control it. Problems will arise when the tools cannot detect the unwanted activity on the transition mechanism. As illustrated in Fig. 3, this matter can be explained in the following scenarios.

First scenario: An IPv4 network uses a firewall to detect and act on any intrusion or unwanted activities. Subsequently, a native IPv6 network is developed and uses a tunneling method as a gateway. After the tunnel is enabled, Router_A encapsulates the IPv6 packet to the IPv4 packet. This encapsulated packet is named as IPv4 Protocol-41. Most administrators assume that the packet is foreign, thus blocking it using the firewall. Furthermore, there is a firewall that has default access list that blocks this protocol. Its purpose is to prevent the misused or unwanted packets from entering the network. As a result of the action, there is no activity on the network, even though the tunneling mechanism has been enabled. In that case, all IPv6 packets cannot be routed to the gateway at the tunnel broker.

Second scenario: A firewall allows IPv4 Protocol-41 packets to make the incoming and outgoing networks. The IPv6 network is fully operational. All types of IPv6 packets will be encapsulated to be Protocol-41, including the unwanted one. This scenario will open space for any attack from the outsider. The attack can be made to the IPv6 or IPv4 network if there is a node on the network using a dual-IP (Nordmark and Gilligan, 2005) configuration. Attacks against the network through the IPv4 network using the tunneling mechanism will occur if this Protocol-41 is unrestricted without inspection.

In the next section, an experiment is performed to evaluate the effectiveness of network security tools against threats through this transition mechanism.

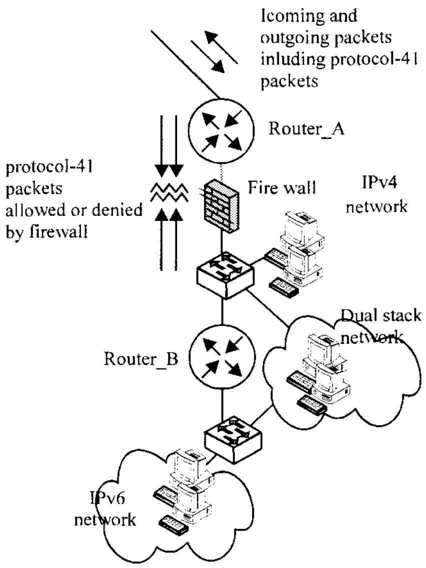

Icoming and outgoing packets inluding protocol-41 packets
Router_A
protocol-41 packets allowed or denied by firewall
Fire wall
IPv4 network
Dual stack network
Router_B
IPv6 network

Fig. 3: Scenario where protocol-41 packets are allowed or denied by firewall

EXPERIMENTAL METHOD

The experimental procedure is divided into several parts as described briefly in Fig. 4. Furthermore, each part is specified clearly in the following sections.

Threat requirement: The main objective of this experiment is to review the effectiveness of the firewall and IDS against threats through the tunneling mechanism. According to Xinyu *et al.* (2007) almost all types of DoS/DDos attacks on the IPv6 environment can be controlled using IPSec especially when the attacker spoofs the IP addresses. Unfortunately, there are also weaknesses due to lack of protection against some attacking conditions such as a packet flooding attack uses a valid IP address. For this experiment, an ICMPv6 flood attack with the real address was used as a sample of attack because it is the most basic and popular among those other attacks (Udhayan and Anitha, 2009). In addition, this attack is easily constituted and highly destructive among various DoS/DDoS attacks (Kumar, 2007; Udhayan and Anitha, 2009). This attack, also known as ping flood attack and can be applied by using the "Ping" command for the most Operating System (OS).

Hardware and software requirement: All processes were supported by a multi platform OS with several selected software and hardware. This selection was recorded from the analysis and observation. Table 2 describes the hardware and software used in the experiment.

Environment setup: This section describes the methods of installation and configuration of the environment. An experiment was conducted accordance with a basic IPv6 network using the IPv6 tunneling mechanism as a path to other IPv6 networks and for reducing instability that may affect the results, all experiments were conducted under a controlled environment.

Basically, the testbed, as shown in Fig. 5, is developed with several different dual stack networks, namely the DS_Network_A, the DS_Network_B and the DS_Network_C. Here, Router_A and Router_C act as:

Table 2: Hardware and software

Hardware/Software	Type
Network Security tools	Snort 2.8.3 (snort rules 2.4), Kiwi Syslog Server 9.0.3, WinPcap 4.1.1, Oinkmaster 2.0, Microsoft Baseline Security Analyzer 2.1.1, WireShark 1.2.6., COMODO Firewall 3.1
C code	Initiator of attack.
Router	Cisco 2811 with IOS 12.2(2) T
Host	Ms Windows 7 and Linux Fedora 9
Switch	Cisco Catalyst 2960-24TT 24-Port Ethernet Switch

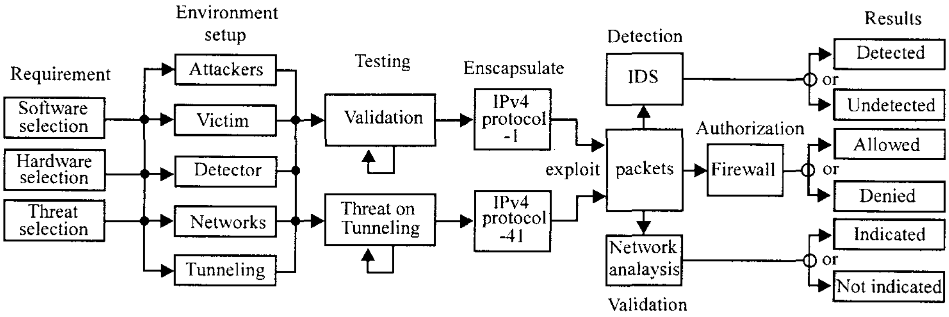


Fig. 4: The experiment work flow that contains of several parts

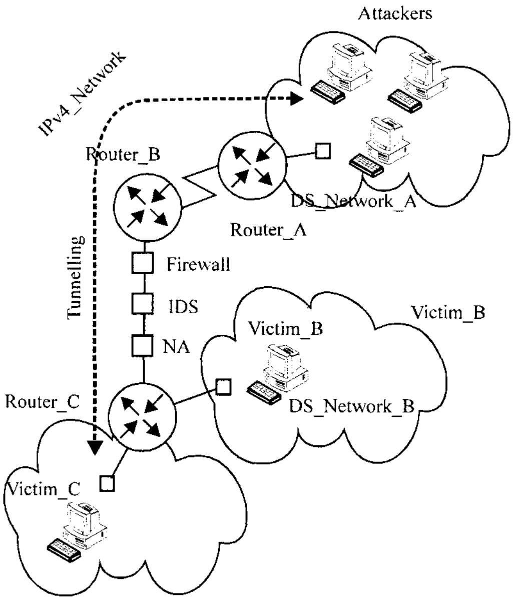


Fig. 5: Tesbed developed according to the desired environment

communication devices for the tunnel between the DS_Network_A and the rest of the networks. Next, the Firewall and the IDS are placed at the tunnel between Router_B and Router_C. After that, traffic on this tunnel is monitored by the Network_Analyzer. Nodes on the DS_Network_A are used as attackers and each of them run multiple commands in parallel at the same time. One node in each of the DS_Network_B and DS_Network_C were identified as the victim nodes.

TESTING AND EVALUATION

Experiments were conducted to obtain the results, through two different experiments called the Validation Test and Threat on Tunneling. The first experiment was aimed to ensure that the firewall and IDS were functioning. The second test was performed to meet the study's objective.

The validation test experiment: The first step was to produce an early threat situation of ICMP flood attacks on the IPv4 environment. This was implemented using the ICMP packet encapsulation or IPv4 Protocol-1 on layer 3 OSI model. ICMP echo request packets were launched from the DS_Network_A in which 10 nodes has been set as attackers and the target or the victim's node is set in the DS_Network_B and DS_Network_C. The packets were produced by the ICMP echo command using C programming. This flood attack was used to flood large amounts of data packets to the victim's node in an attempt to overload it. The following is part of the programming script used on the attacker node to initiate the attack.

```
#define BUFFER_SIZE 1000
#define PACKET_DELAY_USEC 30
#define DEF_NUM_PACKETS 100
.
.
void set_ip_layer_fields(struct icmphdr *icmp, struct ip *ip)
{
 // IP Layer
 ip->ip_v = 4;
 ip->ip_hl = sizeof*ip >> 2;
 ip->ip_tos = 0;
 ip->ip_len = htons(sizeof(buf));
 ip->ip_id = htons(4321);
 ip->ip_off = htons(0);
 ip->ip_ttl = 255;
 ip->ip_p = 1;
 ip->ip_sum = 0; /* Let kernel fill in */

 // ICMP Layer icmp->type = ICMP_ECHO;
 icmp->code = 0;
 icmp->checksum = htons(~(ICMP_ECHO << 8));
}
```

Command line arguments:

```
# ./icmp_flood <saddr> <daddr> <# packets>
 <saddr> = spoofed source address
 <daddr> = target IP address
 <# packets> = is the number of packets to send.
```

The first argument needed in the script is the source IP address, the second argument is the destination address, and the third is the number of packets to be sent. The program above instructs the attacker node to generate packets to the victim node with IPv4 protocol-1 and ICMP type-0 (ICMP echo request). The buffer size of all packets is constant and equal to 1000 bytes. At the same time, all network security tools which task was to evaluate had been activated. Network Analyzer (NA) was used to validate all the ICMP packets. This scenario is illustrated by Fig. 6.

Threat on tunneling experiment: In this experiment, the same approach as the previous experiment is used but with both IPv4 and IPv6 are enabled. An IPv4 Protocol-41 or IPv6-in-IPv4 encapsulation process was used. ICMPv6 echo request (IPv6 next header-58 and ICMPv6 type-128) packets were launched from 10 nodes in the DS_Network_A as the attackers and the victims is in the DS_Network_B and in DS_Network_C.

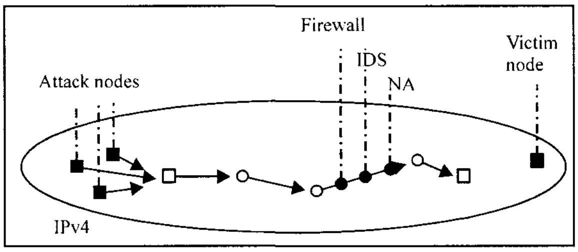


Fig. 6: The validation test environment

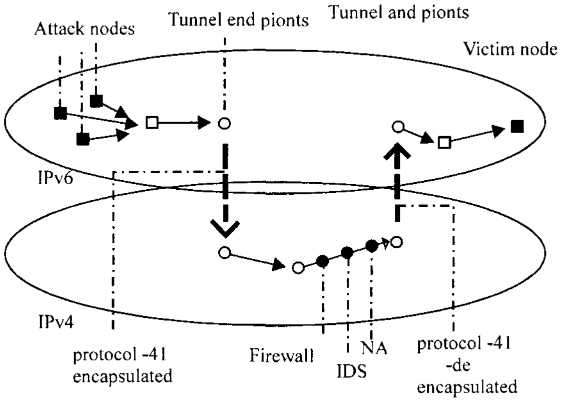


Fig. 7: The Threat on tunneling test environment

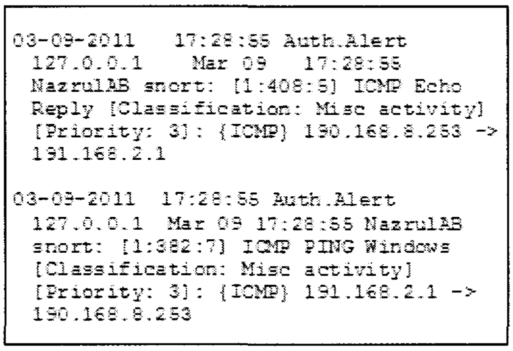
The Firewall, IDS and NA were reused for the same purpose as the previous experiment. This scenario is shown through Fig. 7.

RESULTS

In the testing phase, the IDS have shown its ability to detect threats created by the ICMP flood attacks towards the Victim_B. The same result was produced when the second attack conducted to the Victim_C. Meanwhile, the firewall has been allowing ICMP echo request packet entering the networks. Although, it obviously looked that the load of echo request packets were modified, yet the firewall default rules had ignored the packets. Fig. 8 show some alerts displayed by the Kiwi_syslog immediately after the attack was launched.

The observation through the NA shows that the captured packet is correctly significance with the reading. Fig. 9 shows traffic captured by NA is and the result proved that IDS had been activated and was functional.

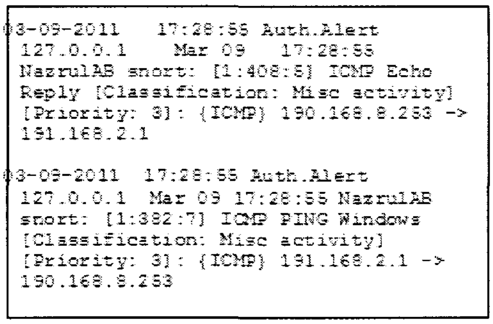
On the second experiment, it was found that the IDS have no reaction after the threats are launched to both



```
03-09-2011   17:28:55 Auth.Alert
  127.0.0.1    Mar 09   17:28:55
  NazrulAB snort: [1:408:5] ICMP Echo
  Reply [Classification: Misc activity]
  [Priority: 3]: {ICMP} 190.168.8.253 ->
  191.168.2.1

03-09-2011  17:28:55 Auth.Alert
  127.0.0.1  Mar 09 17:28:55 NazrulAB
  snort: [1:382:7] ICMP PING Windows
  [Classification: Misc activity]
  [Priority: 3]: {ICMP} 191.168.2.1 ->
  190.168.8.253
```

Fig. 8: Some of the IDS alert appeared on syslog



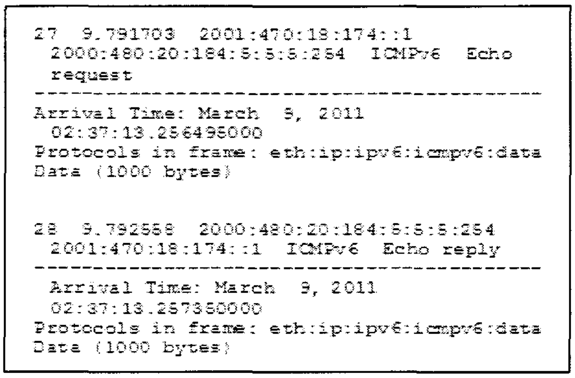
```
03-09-2011   17:28:55 Auth.Alert
 127.0.0.1    Mar 09   17:28:55
 NazrulAB snort: [1:408:5] ICMP Echo
 Reply [Classification: Misc activity]
 [Priority: 3]: {ICMP} 190.168.8.253 ->
 191.168.2.1

03-09-2011  17:28:55 Auth.Alert
 127.0.0.1  Mar 09 17:28:55 NazrulAB
 snort: [1:382:7] ICMP PING Windows
 [Classification: Misc activity]
 [Priority: 3]: {ICMP} 191.168.2.1 ->
 190.168.8.253
```

Fig. 9: The packet captured by network analyzer

Table 3: Summary of results obtained from the experiments.

Packet flooding	Encapsulate	Victim nodes	Firewall	IDS	Network analyzer
Validation test experiment					
ICMP	IPv4 Protocol-1	Victim_B	Allowed	detected	indicated
ICMP	IPv4 Protocol-1	Victim_C	Allowed	detected	indicated
Threat on tunneling experiment					
ICMPv6	IPv4 Protocol-41	Victim_B	Denied (Default Setting)	undetected	Not indicated
ICMPv6	IPv4 Protocol-41	Victim_C	Denied (Default Setting)	undetected	Not indicated
ICMPv6	IPv4 Protocol-41	Victim_B	Allowed	undetected	Indicated
ICMPv6	IPv4 Protocol-41	Victim_C	Allowed	undetected	Indicated



```
27  9.791703  2001:470:18:174::1
  2000:480:20:184:5:5:5:254  ICMPv6  Echo
  request
------------------------------------------
Arrival Time: March  9, 2011
  02:37:13.256495000
Protocols in frame: eth:ip:ipv6:icmpv6:data
Data (1000 bytes)


28  9.792558  2000:480:20:184:5:5:5:254
  2001:470:18:174::1  ICMPv6  Echo reply
------------------------------------------
  Arrival Time: March  9, 2011
  02:37:13.257350000
Protocols in frame: eth:ip:ipv6:icmpv6:data
Data (1000 bytes)
```

Fig. 10: ICMPv6 in IPv4 Protocol-41 packet through tunneling captured by Network Analyzer.

victim_B and Victim_C, even the NA did not indicate there are threat in the traffics. From the observation, this is due to the default firewall configuration that had dropped all the Protocol-41 traffic. The IDS still did not detect any malicious activity in the traffic although the firewall rule set has been changed to a new configuration and the test is repeated. Thus it shows that the IDS see IPv4 protocol-41 as a non –malicious packet even though it's containing a malicious content. Fig. 10 shows the content of example of ICMP echo request and reply captured by NA. The readings showed that the threat attack by ICMPv6 packet is exist but the IDS see it as a normal traffic. Table 3 summarized the result of the entire experiment.

DISCUSSION

In this study, the aim is to confirm the effectiveness of conventional network security tools to detect any anomalies occurring on a tunneling mechanism especially against packet flooding attack in IPv6 tunneling. The result of the experiments shows the selected Firewall with default rule set is incapable to filter the ICMPv6 flood traffic that travel through the tunneling mechanism. It proves the finding of Colitti *et al.* (2004) and Taib and Budiarto (2007) that the limitation problem on the firewall in recognizing the packet IPv4 protocol-41 since the firewall are only inspecting the exterior of the packet and do not investigate the payload content. In this case, blocking this protocol on the firewall setting is not the best solution as it will terminate the tunnel link, meanwhile if the firewall setting is too loose it will expose the network infrastructure to attack that can hide under the encapsulated packet. Hence, to improve the defense mechanism for the transition process to IPv6, administrator can consider deploying another firewall solely for IPv6 traffic at the both end of tunneling mechanism but this will only increase the cost.

The similar occurrence is found on IDS. The results obtained sustain the opinion by Bai and Kobayashi (2003) and Tseng *et al.* (2004) that IDS is unable to filter the IPv4 Protocol-41 payload and the lack of set of rules pertaining to new intrusion activity makes it less effective to detect threat luring in the tunneling environment. Likewise, the threat packet might be overlooked due to the IDS overwhelmed with processing the set of rules in comparing the captured packet with the signature. For that reason, some serious actions are needed in order to achieve the highest possible level of security. As a matter of concern, it is highly recommended to improve the detection technique of this network security tools, especially in IPv6 transition mechanisms. According to Lorenzo-Fonseca *et al.* (2009), various research studies recommended anomaly detection based on Artificial Neural Network (ANN) is an appropriate technique for this effort.

Although Firewall and IDS are widely used as a conventional defense mechanism, there are still some other potential alternative safety tools can be considered. One of the options to be added to the defense mechanism is by using NA as packet viewer software. As implemented NA in this study and also supported by Zagar and Grgic (2006), anomaly packets were clearly appeared on the output status display. The only drawback of placing NA as a safeguard tool is that NA cannot detect and alert the administrator automatically, it will require the administrator to recognize the attack by the way of observing the anomalies in captured network traffic patterns.

CONCLUSION

In conclusion this research found that the current filtering and detection technique of the firewall and IDS are not fully capable of solving the network security problem during the transition period of IPv4 to IPv6 network. Further research need to be done to overcome this security problem. In the near future, this research will be focusing on developing a suitable technique to detect the threats of DoS/DDoS attacks through the IPv6 tunneling mechanism, especially on automatic tunneling.

ACKNOWLEDGMENTS

The authors would like to thanks Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka for providing facilities and financial support under Fundamental Research Grant Scheme No. FRGS/2010/FTMK/TK02/5/F0091.

REFERENCES

AlJaafreh, R., J. Mellor and I. Awan, 2008. Evaluating BDMS and DSTM transition mechanisms. Proceedings of the UKSIM European Symposium, Computer Modeling and Simulation, September 8-10, 2008, IEEE., pp: 8-10.

Bahaman, N., A.S. Prabuwono and M.Z. Masud, 2011. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. J. Applied Sci., 11: 118-124.

Bai, Y. and H. Kobayashi, 2003. Intrusion detection systems: Technology and development. Proceedings of the 17th International Conference on Advanced Information Networking and Applications, March 27-29, 2003, Nihon University and BeiHang University, pp: 710-717.

Bhaskaran, V.M., A.M. Natarajan and S.N. Sivanandam, 2007. A new promising IP traceback approach and its comparison with existing approaches. Inform. Technol. J., 6: 182-188.

Blanchet, M. and F. Parent, 2010. IPv6 tunnel broker with the Tunnel Setup Protocol (TSP): R. f. C. 5572. Internet Engineering Task Force.

Carpenter, B. and C. Jung, 1999. Transmission of IPv6 over IPv4 domains without explicit tunnels: R. f. C. 2529. Internet Engineering Task Force.

Carpenter, B. and K. Moore, 2001. Connection of IPv6 domains via IPv4 clouds: R. f. C. 3056. Internet Engineering Task Force.

Colitti, L., G. Di Battista and M. Patrignani, 2004. IPv6-in-IPv4 tunnel discovery: Methods and experimental results. Network Service Manage., IEEE Trans., 111: 30-38.

Conta, A. and S. Deering, 1998. Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. R. F. C.: 2463, Internet Engineering Task Force.

Deering, S. and R. Hinden, 1998. Internet protocol, version 6 (IPv6) specification. R. f. C. 2460. Internet Engineering Task Force.

Despres, R., 2010. IPv6 rapid deployment on IPv4 infrastructures (6rd): R. f. C. 5569. Internet Engineering Task Force.

Hassan, R. and M.K. Sailan, 2011. End-to-end baseline file transfer performance testbed. Inform. Technol. J., 10: 446-451.

Huang, W. and B. Meng, 2011. Automated proof of resistance of denial of service attacks in remote internet voting protocol with extended applied Pi calculus. Inform. Technol. J., 10: 1468-1483.

Huitema, C., 2006. Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs): R. f. C. 4380. Internet Engineering Task Force.

Karpilovsky, E., A. Gerber, D. Pei, J. Rexford and A. Shaikh, 2009. Quantifying the extent of IPv6 deployment. Passive Active Network Measurement, 5448: 13-22.

Kumar, S., 2007. Smurf-based Distributed Denial of Service (DDoS) attack amplification in internet. Proceedings of the Conference on Internet Monitoring and Protection, July 1-5, 2007, IEEE., pp: 25-25.

Lee, J.H., D.S. Kim, S.M. Lee and J.S. Park, 2011. DDoS attacks detection using GA based optimized traffic matrix. Proceedings of the 5th Innovative Mobile and Internet Services in Ubiquitous Computing Conference, June 30-July 2, 2011, IEEE., pp: 216-220.

Lee, L.T. and C.W. Chen, 2008. The web services with security mechanisms base on IPv4 and IPv6. Inform. Technol. J., 7: 1188-1193.

Lorenzo-Fonseca, I., F. Macia-Perez, F.J. Mora-Gimeno, R. Lau-Fernandez, J.A. Gil-Martinez-Abarca and D. Marcos-Jorquera, 2009. Shelf-life extension of pre-baked buns by an active packaging ethanol emitter. Bio-Inspired Syst. Comput. Ambient Intelli., 5517: 1296-1303.

Meenakshi, S. and S.K. Srivatsa, 2007. A distributed framework with less false positive ratio against distributed denial of service attack. Inform. Technol. J., 6: 1139-1145.

Nordmark, E. and R. Gilligan, 2005. Basic transition mechanisms for IPv6 hosts and routers: R. f. C. 4213. Internet Engineering Task Force.

Razak, S., M. Zhou and S.D. Lang, 2002. Network intrusion simulation using OPNET. Proceedings of the OPNETWORK Conference, August 26-30, 2002, USA., pp: 1-5.

Sam, S.B., S. Sujatha, A. Kannan and P. Vivekanandan, 2006. Network topology against distributed denial of service attacks. Inform. Technol. J., 5: 489-493.

Savola, P. and C. Patel, 2004. Security considerations for 6to4: R. f. C. 3964. Internet Engineering Task Force.

Shu-Qiang, H., Z. Huan-Ming and Y. Guo-Xiang, 2009. Research of NIDS in IPV6 based on protocol analysis and pattern matching. Proceedings of the 2nd International Workshop on Knowledge Discovery and Data Mining, January 23-25, 2009, Moscow, pp: 542-545.

Taib, A.H.M. and R. Budiarto, 2007. Security mechanisms for the IPv4 to IPv6 transition. Proceedings of the 5th Student Conference on Research and Development, December, 2007, Selangor, pp: 1-5.

Templin, F., T. Gleeson and D. Thaler, 2008. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP): R. f. C. 5214. Internet Engineering Task Force.

Tseng, B., C.Y. Chen and C.S. Laih, 2004. Design and implementation of an IPv6-enabled intrusion detection system (6IDS). Proceedings of International Computer Symposium, Dec. 15-17, Taipei, Taiwan, pp: 684-689.

Udhayan, J. and R. Anitha, 2009. Demystifying and rate limiting ICMP hosted DoS/DDoS flooding attacks with attack productivity analysis. Proceedings of the IEEE International Advance Computing Conference, March 6-7, 2009, Patiala, pp: 558-564.

Vokorokos, L., A. Balaz and M. Chovanec, 2006. Intrusion detection system using self organizing map. Acta Electrotechnica Informatica, 6: 1-6.

Waddington, D.G. and F. Chang, 2002. Realizing the transition to Ipv6. IEEE Commun. Magazine, 40: 138-147.

Xinyu, Y., M. Ting and S. Yi, 2007. Typical DoS/DDoS threats under IPv6. Proceedings of the International Multi-Conference on Computing in the Global Information Technology, March 4-9, 2007, Gosier, Guadaloupe, pp: 55-55.

Yohannes, D. and Z.Q. Xu, 2003. The current security awareness and reliability in area enterprise networks. J. Applied Sci., 3: 17-22.

Yoo, S.G., S. Lee, Y. Lee, Y.K. Yang and J. Kim, 2011. Enhanced intrusion detection system for PKMv2 EAP-AKA used in WiBro. Inform. Technol. J., 10: 1882-1895.

Zagar, D. and K. Grgic, 2006. IPv6 security threats and possible solutions. Proceedings of the World Automation Congress, July 24-26, 2006, Budapes, pp: 1-7.

Zagar, D., K. Grgic and S. Rimac-Drlje, 2007. Security aspects in IPv6 networks-implementation and testing. Comput. Electr. Eng., 33: 425-437.

Zhang, Y., 2009. Study on intrusion IPv6 detection system on LINUX. Proceedings of the Asia-Pacific Conference on Computational Intelligence and Industrial Applications, November 28-29, 2009, China, pp: 5-8.