The 5th Student Conference on Research and Development –SCOReD 2007
11-12 December 2007, Malaysia

Security Mechanisms for the IPv4 to IPv6 Transition

Abidah Hj Mat Taib, *UiTM Perlis* and Rahmat Budiarto, *USM*

***Abstract*– Transition from IPv4 to IPv6 has been made possible through various transition mechanisms, categorized as dual-stack, tunneling and translation. However, period of transition may take years to complete which both protocols will coexist due to Internet services deployed are widely in IPv4. So, a successful IPv6 transition is depended on the compatibility with the large installed base of IPv4 hosts and routers, as well as maintaining security of the network from potential threats and vulnerabilities of both Internet Protocols. This paper classifies potential security issues in the transition period and identifies prevention mechanisms to the problems identified. As dual-stacked host or network is the most simple IPv6 deployment any enterprise can settle for now, this paper focuses on possible implementation of distributed firewall in a dual-stacked environment which involves packet filtering at the edge router as well as the host-based firewall.**

***Index Terms*—IPv6 Transition, Dual stack, Tunneling, Security Mechanisms, Distributed Firewalls.**

I. Introduction

THIS paper provides an insight on security considerations during the transition from IPv4 to IPv6. Transition to IPv6 will not occur in short time due to wide spread usage of IPv4 networks since it has been introduced more than 25 years ago. For the mean time we will settle for interoperability between IPv4 and IPv6 where both protocols will coexist and support the present Internet requirements. Since the two protocols are used in parallel, appropriate security measures must be installed to secure the network while transition from IPv4 to IPv6 is in progress. Basically, transition mechanisms [1] are categorized as dual-stack, tunneling and translation. Though, the most basic transition mechanisms [2] are dual-stacked and manually configured tunneling of IPv6 over IPv4. These two mechanisms are wise options for initial IPv6 deployment due to their simple management and less security considerations [2],[3],[5]. Nevertheless, translation is still important when communicating between IPv6 and legacy IPv4. This paper will not cover security aspects of translation mechanism as they are not in our scope of research.

A. H. M. Taib is with the Department of Computer Science, Universiti Teknologi MARA, Perlis, 02600 Arau, Perlis, Malaysia (e-mail: abidah@perlis.uitm.edu.my).

R. Budiarto is with the National Advanced IPv6 Centre (NAv6), School of Computer Sciences, Universiti Sains Malaysia, 11800 Penang, Malaysia (e-mail: rahmat@cs.usm.my).

1-4244-1470-9/07/$25.00 ©2007 IEEE.

Since present Internet services deployed are widely in IPv4, a successful IPv6 transition is depended on the compatibility with the large installed base of IPv4 hosts and routers, as well as maintaining security of the network from potential threats and vulnerabilities of both Internet Protocols. A dual stack device must employ adequate host security mechanisms as its applications can be subject to attack on both IPv4 and IPv6. So as tunneling, in which packets that enter the network through a tunnel cannot circumvent filters and introduce potential threats to the network.

The present security mechanisms are not well built to support IPv6. Many firewalls have separate rule-sets for IPv6 and IPv4 which need to be coordinated and consistent to be properly managed to avoid an inadvertent security exposure as well as intentional attack. Meanwhile, Intrusion Detection System (IDS) has lack of IPv6 signature database to perform effectively. This paper classifies potential security issues in the transition period and identifies prevention mechanisms to the problems identified. Basically, the severity of these issues related to the complexity of the transition mechanisms chosen and failure to apply appropriate mitigation techniques.

Among mitigation techniques that can be considered for IPv6 are firewalls, IPsec, auditing and intrusion detection which are also available in IPv4. However, due to some criteria [3], such as longer address size, different header format between IPv6 and IPv4 and the use of extension headers in IPv6 we have yet to see the implementation of security mechanisms specially designed for IPv6. Although IPsec is mandated in every implementation of IPv6, due to bootstrapping problem, it is not always a valid security option. On the other hand, firewalls [10] have been available for use, and works on making better of firewalls have been carried out. As dual-stacked host or network is the most simple IPv6 deployment any enterprise can settle for now, this paper focuses on possible implementation of distributed firewalls [11] in a dual-stacked environment which involves packet filtering at the edge router as well as the host-based firewall.

This paper is organized as follows: We begin with a description of potential security issues in the transition period and their respective countermeasures. This is followed with review of some prevention mechanisms to counter the highlighted issues. Then we discuss the design of the distributed firewalls and the possibility of problems related to it. Finally, we sum up with the conclusion and future work.

II. Security Issues and Preventing Mechanisms

Prior to migration or co-existence with IPv6, an understanding of its security implication is necessary to avoid worries or un-acceptance among users or decision makers. We need to prepare the network users against the possible threats or attacks that may affect the network and its resources. Prior to that, we need a better understanding in order to come up with a comprehensive and enforceable security policy for the network. Security issues in the IPv6 transition/co-existence [4] can be viewed in terms of issues due to the IPv6 protocol itself, issues due to transition mechanisms and issues due to the IPv6 deployment.

A. Issues due to IPv6 Protocol

Followed to significant differences between features in IPv4 and IPv6, some of those specification changes may result in potential security issues. Overall, security issues due to the specific IPv6 protocol and their respective countermeasures can be simplified into a diagram as depicted in Fig 1. The left side boxes represent list of security mechanisms to counter the problems in the right boxes which they are pointed to. As mentioned in [6], DoS is the leading threat or key attack to the Internet. Compare to IPv4, DoS in IPv6 quite similar in which it is resulted from various security vulnerabilities and threats of the IPv6 protocol. The dim line to the right of the diagram indicates all threats and vulnerabilities that would have high potential in generating DoS attacks.

In IPv6, reconnaissance attacks may still possible. With a longer address space and larger subnet size, scanning IPv6 network by intruders would be tougher compared to IPv4. Though, some types of multicast addresses used in IPv6 network might expose some of its resources to the intruders (for instance, all routers with a site-specific address FF05::2). Information of these resources may assist intruders in launching directed attacks such as flooding which resulted in DoS. To counter this scenario, all firewalls and site boundary routers should be configured to drop packets with site scope destination address.

Another potential of DoS is misuse of routing headers to avoid access controls that is based on destination address. It is possible because any publicly accessible host can redirect the attack packets. To prevent this, ingress/egress filtering must determine whether the source address is right for the destination and ensuring that routing headers do not contain the same way point address more than once.

As ICMPv6 plays an important role in IPv6, a major concern should be paid to its related issues. For instance, ICMPv6 and multicast address in which ICMPv6 allows error notification responses to be sent when certain unprocessable packets are sent to multicast addresses. A potential attacker can craft a suitable packet sent to a multicast destination, it may draw multiple responses directed at the victim (the spoofed source of the multicast packet).

Bogus errored packets in ICMPv6 Error Messages are also part of main issues. Bogus ICMPv6 Error Messages (type 0 to 127) containing a spoofed errored packet which can impact higher layer protocols when the alleged errored packet is referred to the higher layer at the destination of the ICMPv6 packet. This can be countered by inspecting the alleged errored packet embedded in the ICMPv6 error message via firewall. Firewalls and destination hosts should be suspicious of ICMPv6 error messages with unnecessarily truncated errored packets. Details on how to address the ICMPv6 issues can be referred in [7].

Neighbor Discovery (ND) has so many issues that can be addressed in its own ND protocol. It has a close relationship with router discovery (RD) and many vulnerabilities regarding ND and RD are addressed in Neighbor Discovery Protocol (NDP). Both securing router and neighbor discovery can be done through Secure Neighbor Discovery (SeND) [8]. Another related issue is link local address and SeND in which potentiality of abuse at the tunnel end-points. For tunnel end-points, filtering has to be provided by a host-based or bridging firewall.

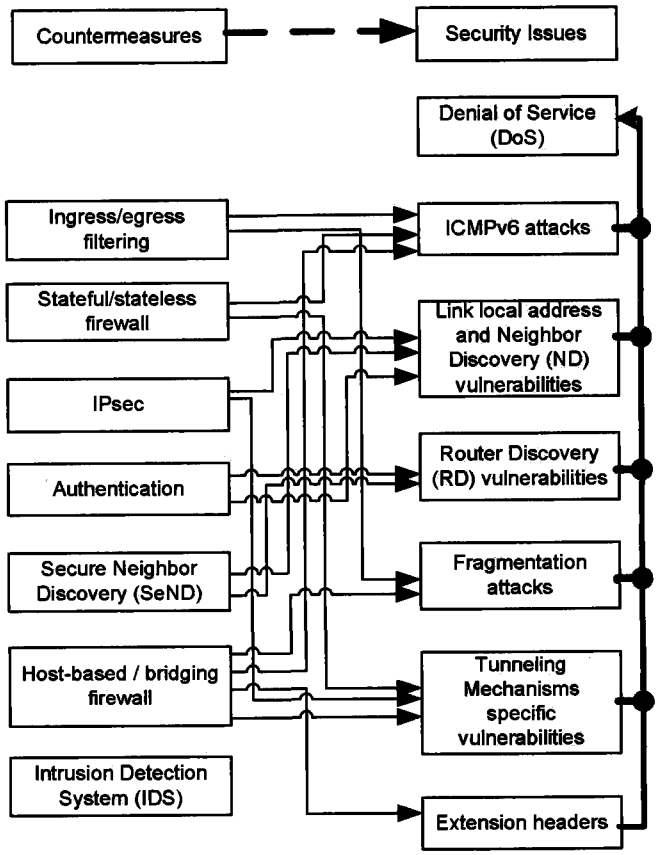

Fig. 1. Security issues and the respective countermeasures.

Fragmentation related attack is also part of IPv6 specific issue in which packets with overlapping fragments are considered to be a major security risk. Packets reassembly in IPv6 hosts – may result in DoS attack based on sending large number of small fragments without a terminating last fragment. In order to ensure that deep packet inspection can be carried out correctly on fragmented packets, many firewalls and other nodes that use deep packet inspection will collect the fragments and reassemble the packet before examining the

packet. To mitigate this scenario, firewalls must forbid overlapping packet fragments.

Security issues regarding Extension Headers are related to processing Extension Headers in middleboxes, processing Extension Headers chains, unknown headers or destination options, excessive hop-by-hop options, misues of Pad1 and PadN options and overuse router alert options. These issues are mostly due to ambiguity or incomplete specification in the base IPv6 specification. Security mechanisms needed here will be depending on the specific issues that require attention and most of them are related to configuring a respective firewall.

B. Issues due to Transition Mechanisms

The more complex the mechanism, the greater the danger introduced. The threats could be encountered in the mechanisms themselves, in the interaction between mechanisms or by introducing unsecured path through multiple mechanisms. So, in depth understanding of the security implications of the transition mechanism may help network security administrators to apply suitable security mechanisms in their network. We are concern only with dual stack and tunneling.

As for dual stack, a device must employ adequate host security mechanisms as its applications can be subject to attack on both IPv4 and IPv6. Therefore, any host controls such as firewalls, VPN clients and IDSs must be able to inspect traffic from both IP versions and block specific traffic when a block is necessary. What the network administrator should consider here is to extend the firewall with IPv6 support and corresponding rule sets for IPv6 or implement separate IPv6-only firewall which can secure the hosts and network as the same way its IPv4 counterpart does. In addition, appropriate IPv6 access control lists (ACLs) must also crafted and placed accordingly which are capable to implement the same restrictions as IPv4's ACLs .

As for tunneling, mechanism that we can simply settle for at the beginning of IPv6 deployment is a Tunnel Broker. However, it becomes an issue if site administrator totally unaware of users on their site who use tunnel brokers. Without any guidelines or site requisite for "proper" IPv6 deployment may introduce security holes which the administrator does not know about and therefore does not guard against.

For configured tunneling, concerns lie at a host behind IPv4 firewall when it needs to open firewall for protocol 41 (IPv6) and in some cases also for protocol 58 (ICMPv6) at least for the host at the remote end of the tunnel, which will be the source of the incoming IPv4 traffic that contains the IPv4 packets. Since there is no particular type of authentication mechanism for tunnels was defined, packet verification is done by checking on the IPv4 packet's source address. As a result, exploitation such as IP spoofing, injecting packet at the tunnel endpoint, and bypassing firewall or avoiding ingress filtering checks [4] become major threats in tunneling mechanism. RFC4891 [9] may help us in defining methods to secure IPv6-in-IPv4 tunnels.

Certain tunneling mechanisms establish communication with native IPv6 nodes or between the automatic tunneling mechanisms via the use of relay. They are 6to4 (encapsulate the IPv6 packet directly in an IPv4 packet) and Toredo (encapsulate the IPv6 packet directly in an IPv4 UDP packet). These relays could be deployed in various location such as all native IPv6 nodes, native IPv6 sites, in IPv6-enabled ISPs or just somewhere in the Internet. These relays provide a potential vehicle for address spoofing, DoS and other threats.

Automatic tunneling mechanisms [3] such as 6to4, Toredo and ISATAP are less secure compared to configured tunneling. They are susceptible to packet forgery and DoS attacks as there is no preconfigured association between endpoints. Moreover, receiving nodes must allow decapsulation of traffic sourced from anywhere in the Internet. Thus, a decapsulation function must be extremely well secured to deal with the wide range of the potential sources. When deploying automatic tunneling, users must be warned of the possible consequences and proper guidelines should be underlined so as not to compromise the security assumptions held by the users.

To deal with transition security, the network architecture must provide separate IPv4 and IPv6 firewalls with tunneled IPv6 traffic arriving encapsulated in IPv4 packets routed through the IPv4 firewall before being decapsulated, and then through the IPv6 firewall as depicted in Fig. 2.

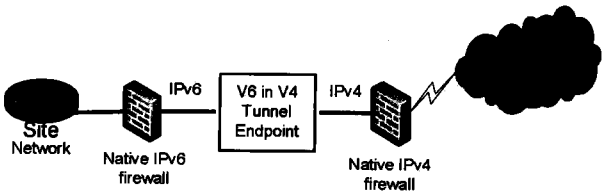

Fig 2. Separate IPv4 and IPv6 firewalls

C. Issues due to IPv6 Deployment

If possible we would like to have all electronic devices manufactured to be IPv6 capable. If that is so, with IPsec ready we do not have to worry much on the security implication when deploying IPv6. However, the lack of equipments or tools such as IPv6 IDS and firewalls may leave the hosts and routers unprotected. Hence, it would create a problem if the IPv6 capabilities are turned on by default in new equipment or new release of operating system without the network administrators realized of the potential security exposure they may end up with. So, we need to continue testing and exploring the IPsec key management issues, IPv6 firewalls and IPv6 IDS in order to find the possible solutions .

Other issues include DNS server problem, addressing scheme and securing routers, and consequences of multiple addresses in IPv6 [4] which require proper observation to deal with them.

Meanwhile, many IPv6 implementations are quite new and there are inadequate IPv6 assessment tools [3] available to audit our own network. In addition, untested codes in IPv6 implementation may also contribute to security flaws which exposed the network to security threats and attacks.

D. Prevention Mechanisms Review

Among the prevention mechanisms available are firewalls, IPsec and Intrusion Detection System (IDS).

Firewalls are widely deployed in most organization connected to the Internet. Based on set of rules or security policy, firewalls act as a sentry to the network which determines whether particular packet or stream of packets can pass through them or not. The common firewall implementation is setting it as perimeter firewall because it is believed that intruders always come from outside while in reality, the greater effect of security breach or harmful attacks are mostly come from the insiders. So, effort to reduce the risks should include deployment of multiple firewalls that are capable of filtering IPv4 and IPv6 packets at the edge router (perimeter firewall) as well as at the hosts (personal firewalls). In choosing appropriate firewall technologies [10] for particular scenario, network security personnel can consider options depicted in Fig. 3 .

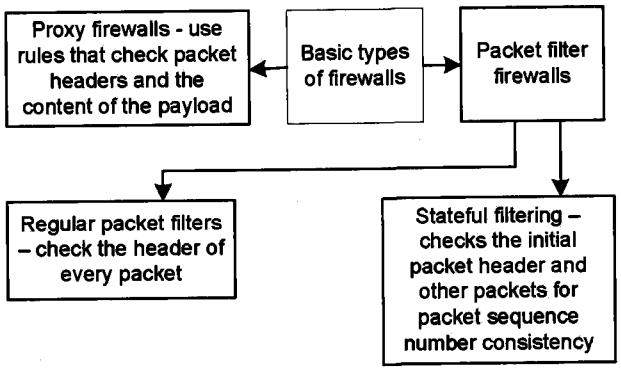

Fig. 3. Firewall Technologies

In real implementation, hybrid firewalls may be used in which the features of both types of firewalls are combined. Among IPv6 firewalls available are open source-based such as Packet Filter from OpenBSD or FreeBSD and Linux p6tables.

Basically, firewall must filter internal-use IPv6 addresses like site-local addresses and specific multicast addresses at the edge router in order to safeguard from mis-configurations and rogue devices. Then, filter ingress/egress interface to deny spoofed traffic with the host portion of the IPv6 address. Same goes with unneeded services, they must be unreachable at the edge firewall to reduce any additional exploits. Denied traffic should be logged as they may notify of a potential malicious intrusion.

IPsec provides security to end-to-end communications at the network layer. The security features include access control, connectionless integrity, data origin authentication, protection against replay attacks, confidentiality, and limited traffic flow confidentiality. IPsec uses the Internet Key Exchange (IKE) protocol to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used. Compared to IPv4 which had to retrofit IPsec headers into the original IPv4 frame, IPv6 supports IPsec within rhe defined packet structure using extension headers. However, usage of IPsec resulted in new problem for network administrators and decrease the effectiveness of perimeter firewalls because of the increase prevalence of encrypted packets on which the firewalls cannot perform deep packet inspection and filtering. Bootstrapping problem in IPsec has caused cryptographic protections become unpopular in many IPv6 deployment. Nevertheless, a successful IPsec deployment will only affect the network layer and does nothing to the most common attacks which targeting the application layer.

Logging and auditing of data traffic are important to detect or analyze successful security violations. We should log routing protocol state changes, all router events, all devices access, all commands issued to the device and all configuration changes. Traffic auditing is possible via IDS system. IDS can be in the form of hardware or software system for supervision and analysis of different events occurring in the network or on the particular host. The purpose of IDS is to find potential security problems and to detect an authorized intrusion and misuse of network resources. Problem with IDS is lack of IPv6 signature database because pattern based mechanism used for IPv4 may not be appropriate anymore. Both IPv6 Netwok-Based IDS and Host-Based IDS need to be available in order to deal with the IPv6 deployment. Work done in [12] to come up with IPv6 IDS has shown a promising result but more study on IDS is needed to face the challenges in the IPv6 deployment.

In order to have defense in depth, mechanism like distributed firewalls (Fig.4.) would be a good choice.

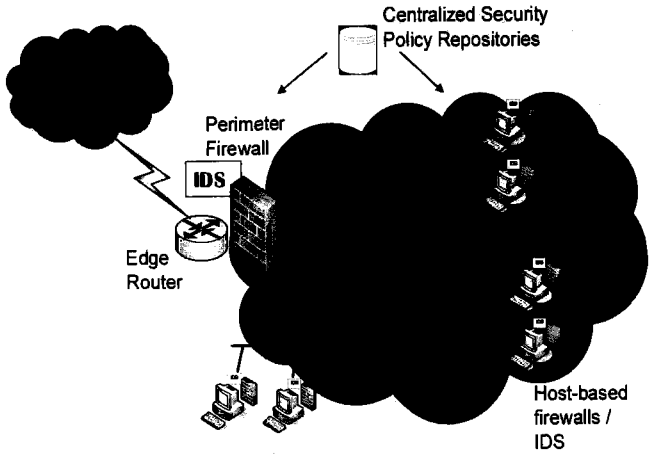

Fig. 4. Distributed firewalls

III. DISTRIBUTED FIREWALLS

Distributed firewalls may consist of managed host-based IPv6 firewalls on top of the conventional perimeter firewall. This involves a combination of centralized security policy which controls the edge router as well as individual hosts in the network.

Three ideas that forming a distributed firewalls [11] are: a policy language, any number of system management tools and IPsec. So, a compiler translates the policy language into some internal format which then be distributed by the system-management software to all host protected by firewall. Incoming packets are granted or denied by each host

depending on both the policy and the IPsec verified identity of each sender. Policy is enforced by each individual host that participates in a distributed firewall. The security administer defines the security policy in terms of host identifiers. This policy is then consulted before processing incoming or outgoing messages. The local host would have a much stronger assurance of its identity if peer host is identified by a certificate.

By having end-to-end IPsec, each incoming packet can be associated with a certificate. The rights assigned to the certificate will determine the access of the associated packet. So, any packet with different certificate name or without IPsec protection, will be dropped as illegal. Implementation of certificate version is also necessary to protect against new, insecure machines that are installed on an inside network. Certificate will not be issued until the appropriate filtering software and rulesets are installed. This means the machine is assumed an outside machine although it is physically inside the network.

Perimeter firewalls perform a first layer screening to ensure the packet is valid, arrive from a valid source and then pass the packet to the destination host. At the destination host firewall, a second layer screening take place where detail packet inspection is carry on. The inspection will be incorporating some intelligent IPsec-aware function. If the packet is encrypted and was not examined in detail at the perimeter firewall, this can be done at the end-host where the received packet is decrypted first prior to checking the upper layer protocols. Upon successful, a packet is sent to the application process. On the other hand, the fail packet will be rejected by the host firewall followed with a violation report sent to its security management system.

Perimeter firewalls responsible for securing the network from general attacks and the individual nodes or hosts firewalls responsible for securing itself from node-related attacks since IPv6 enabled nodes most likely have global addresses which mean they may be reachable from any other IPv6 nodes in the Internet. Hence, host can become a server and has a end-to-end connection with its counterpart somewhere out there, which then will require distributed checking and proper authentication or valid certificate. This will not be a problem as distributed firewalls permit end-to-end encryption.

As shown in Fig. 4, we try to integrate the NIDS and HIDS together in the implementation of Distributed firewall. for this to work, distributed firewall need to be equipped with capability detecting probes and forward them to some central location for processing and correlation. Challenges or problems that we foresee is greater susceptibility to lack of cooperation by users. Nevertheless, distributed firewalls can reduce the threat of actual attacks by insiders by simply making it easier to set up smaller group of users and limit their rights to access server based on least of privilege rules.

In addition, delegation of filtering tasks to the end hosts will reduce the performance bottleneck. Besides, distributed firewall is more subtle in which it has certain knowledge of the host intends. Thus, relying on the host to make the right decision is more secure. While the significant advantage is hosts that are not within the topological boundary are also protected all the time, regardless of whether or not the tunnel is set up. Meanwhile, packets that are authenticated by IPsec are granted more privileges while packets from random Internet hosts can be rejected. Hence, IPsec provides anti-spoofing protection.

IV. CONCLUSIONS

Transition/coexistence of both IPv4 and IPv6 has caused major security considerations to the network and alarmed us to be prepared with appropriate security mechanisms. We highlighted possible security issues in the transition period and subsequently discussed the mechanisms to deal with the issues. Finally we give a brief introduction to the proposed defense in depth mechanism that is the use of hybrid model which combine IPv6 distributed firewalls and Intrusion Detection System to secure the transition network. In future we will observe the effects of the distributed IPv6 firewalls with some probability to increase the network performance.

V. REFERENCES

[1] D. G. Waddington, and F. Chang, "Realizing the Transition to IPv6", *IEEE Communications Magazine*, pp. 138-148, June 2002.

[2] E. Nordmark, and R. Gilligan "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC4213, Oct 2005.

[3] S. Hagen, "Security with IPv6", in IPv6 Essentials, 2nd ed, USA: O'reilly, 2006, pp. 101 – 127.

[4] E. Davies, S. Krishnan and P. Savola, "IPv6 Transition/Co-existence Security Considerations", Internet Draft, Draft-ietf-v6ops-security-overview-06.txt (work in progress), Oct 2006.

[5] L. Colitti, G. D. Battista, and M. Patrignani, "IPv6-in-IPv4 Tunnel Discovery: Methods and Experimental Results:, *IEEE Trans. Network and Service Management*, pp 30 -38, Second Quarter 2004.

[6] Xinyu Yang, Ting Ma, and Yi Shi, "Typical DoS/DDoS threats under IPv6", in *Proc. 2007 IEEE International Multi-Conference on Computing in the Global Information Technology (ICCGI'07)*,

[7] J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC4890, May 2007.

[8] J. Arrko, J. Kempf, B. Zill, and P. Nikander, "Secure Neighbor Discovery", RFC3971, March 2005.

[9] R. Graveman, M. Parthasarathy, P. Savola, and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC4891, May 2007.

[10] J. Stuart Broderick, "Firewalls", Information Security Technical Report, vol. 10, issue 4, 2005, pp. 204-212.

[11] Steven M. Belovin, "Distributed Firewalls", login, November 1999.

[12] Benjamin Tseng, Chi Yuan Chen, and Chi Sung Laih,. Design and Implementation of an IPv6-enabled Intrusion Detection System (6IDS). Presented at Int. Computer Symposium, Dec. 15-17, 2004, Taipeh, Taiwan.

VI. BIOGRAPHIES

Abidah Hj Mat Taib received her B.Sc. in Computer Science from Universiti Teknologi Malaysia (UTM) in 1990 and her M.Sc. IT from De Montfort Univ, UK in 1998. She joined Universiti Teknologi MARA, Perlis as a lecturer in 1992. She is currently working towards the PhD degree at the Network Research Group, School of Computer Sciences, USM. Her main research is directed to IPv6 security mechanisms including firewall, IPsec and IDS. Her other research interests include Network and Information Security and Social Engineering.

Rahmat Budiarto received a B.E. in Math Science from ITB, Bandung, Indonesia in 1986. He obtained a M.E. and a PhD in Computer and Electrical Engineering from Nagoya Institute of Technology, Japan in 1995 and 1998 respectively. He is an associate professor at the School of Computer Sciences, USM in the field of Network Management and Security. He is also a researcher at the Network Research Group and his fields of interest include Artificial Intelligent Systems, IPv6, Network Monitoring and Network Security. He has published over 80 research papers and won a number of awards for his research products I-Netmon and J-Netmon. At present, he is a Deputy Director of National Advanced IPv6 Centre of Excellent, USM.