IPv6 Transition:
Why a new security mechanisms model is necessary

Abidah Hj Mat Taib
Faculty of Information Technology and Quantitative Science
Universiti Teknolgi Mara Perlis
Malaysia
abidah@perlis.uitm.edu.my

Rahmat Budiarto
Network Research Group
School of Computer Sciences
Universiti Sains Malaysia
6046533006
rahmat@cs.usm.my

Azman Samsudin
School of Computer Sciences
Universiti Sains Malaysia
6046533635
azman@cs.usm.my

ABSTRACT
This paper describes the scenario in the transition of IPv4 to IPv6 with focusing on the security issues involved in each of the transition methods: dual stack and tunneling. Then, the paper analyze the existing security mechanisms available and identify new considerations for a new security model.

Categories and Subject Descriptors
D.3.3 **[COMPUTER-COMMUNICATION NETWORKS]**: Internetworking – *standards (IPv6), routers*

General Terms
Security

Keywords
IPv6 transition, dual stack, tunneling, security mechanisms

1. INTRODUCTION
IPv4 has been existed more than twenty years and supported various kinds of applications and services to the organizations and Internet users. Although it has played a successful role in the internetworking environment, an explosive growth and tremendous demand for new IP addresses has made it no longer capable in serving the current and future demands of the Internet users all over the world. As new Internet Protocol, IPv6, and next generation network has come along with their promising features, the deficiencies experienced in IPv4 will be taken care of by IPv6. Thus, enterprises and Internet Service Providers (ISP) shall go ahead with the transition and enjoy what IPv6 can offer. Although there is additional cost involves when migrating, stay put and not making a transition at all and just continue to patch IPv4 from time to time also involves high cost for both customers ISPs. However, IPv6 deployment will not replace the IPv4 instantly since most of network applications and services are in IPv4. Due to the scale of IPv4 network and for enterprises to maintain current levels of service, the transition will be a long process where IPv6 will be added to be operated in parallel with IPv4. This gradual migration is possible through various transition tools which can be categorized as dual stack, tunneling and translation [1,2]. The most viable way to deploy IPv6 is through dual stack and configured tunneling [3]. Nevertheless, translation is still important when communicating between IPv6 and legacy IPv4.

This paper will not cover translation security aspects as it is not in the scope of our research. Since each method of transition has its own security issues, and process of migration may consume a long period which could take years to complete, security consideration in the coexistence and migration become important and need proper attention. We have to consider both protocols (IPv4 and IPv6) security issues. Given the current security mechanisms like firewall, IDS and IPS, auditing and IPsec, are our assets and resources maintain secured in the transition period? To answer the question, we have to look at each of possible transition tools and study its specific weaknesses to anticipate the potential threats that later may change to attacks. With this awareness, we need to come up with additional considerations and modifications to the current practice for the better security of the transition period.

In this paper we discuss possible transition mechanisms from IPv4 to IPv6 with focusing on the specific security issues for each mechanism. To begin, we highlight the transition process or coexistence/migration scenario and the importance of securing the transition period. Then, we briefly discuss the most possible transition mechanisms: dual stack, tunneling and translation, as well as the related specific security issues. This followed with overview the IP security (IPsec), analyze the current security mechanisms and the new security model for the transition period. Finally, we sum up all arguments in the conclusion.

2. COEXISTENCE AND MIGRATION

2.1 Dual stack
Dual stack technique requires hosts and routers to implement both IPv4 and IPv6 protocols. This enables networks to support both IPv4 and IPv6 services and applications during the transition period in which IPv6 services emerge and IPv6 applications become available. Figure 1 shows a typical IP dual stack architecture. Nodes will use IPv4 to communicate with IPv4 nodes, and use IPv6 to communicate to IPv6 nodes. Even though IPv4 and IPv6 networks are on the same link, the dual stack router has to maintain two routing tables and the IPv4 and IPv6 nodes are not able to communicate directly to each other. Meanwhile, an IPv4/v6 node needs a DNS resolver that capable of resolving both types of DNS address records. So, the host can make decisions about when connection should be made using IPv4 or IPv6. The determination of protocol version is automatic, based on the available Domain Name System (DNS) records. Because this is based on the DNS, and normal users would use fully qualified domain name in email addresses and URLs, the transition from IPv4 to IPv6 is invisible to normal users.

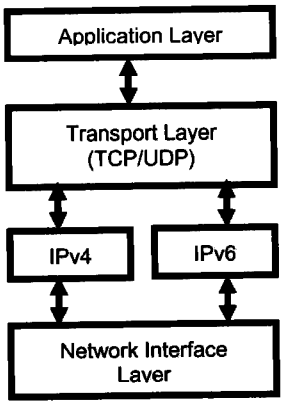

Figure 1: Typical IP dual stack architecture

2.2 Tunneling

Tunneling is needed when communicating between two end-to-end IPv6 hosts while the intermediate network is still in IPv4. To permit sending of packets, IPv6 packet is encapsulated in an IPv4 packet at the tunnel entry point (a dual stack router) so that it can travel through the IPv4 cloud before reaching the other exit point where it will be decapsulated and forwarded to the intended recipient. As a result, we have IPv6 packet in an IPv4 packet a.k.a. IPv6-in-IPv4 (Figure 2).

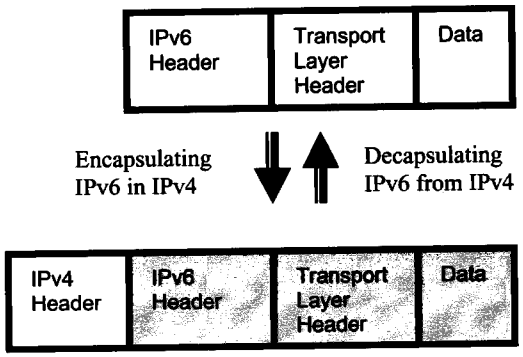

Figure 2. Encapsulating IPv6 in IPv4

Tunneling can be automatic or manually configured. Manually configured tunneling a.k.a IPv6-over-IPv4 tunneling is point-to-point tunnels where IPv4 tunnel's endpoint address is determined by configuration information on the encapsulation node. For control of the tunnel paths and to reduce the potential for tunnel relay denial of service (DoS) attacks, manually configured tunnels can be advantageous over automatically configured tunnels. There are a number of considerations need to take into account when deciding which type of tunneling to be chosen. We can opt for configured tunnel if our ISP provides IPv6 connectivity through a tunnel to some dual-stacked host or router within our network. As an alternative, to easily deploy IPv6 is by tunneling through tunnel broker. This service is a configured tunnel which is provided by an independent supplier such as Hexago Gateway 6 [4]. For a start, an enterprise can subscribe to this tunnel broker and continue doing so until there is a need to deploy a comprehensive IPv6. As for automatic tunneling, it has now been deprecated. However, some that are still preferred are 6to4 and ISATAP where IPv6 node can use different types of addresses such as 6to4 or ISATAP addresses to dynamically tunnel IPv6 packets over an IPv4 routing infrastructure. Another method is Teredo which involves tunneling packets over UDP to make IPv6 available to IPv4 host through one or more layers of network address translator (NAT). It is the last option used when no other method will work.

2.2.1 6to4

6to4 uses automatic IPv6-over-IPv4 tunneling to interconnect IPv6 networks and uses 6to4 routers and relays which accept and decapsulate IPv4 protocol 41 ("IPv6-in-IPv4") from any node in the IPv4 internet. Three general threat of 6to4 are denial of service (DoS) attacks where a malicious node prevents communication between the node under attack and other nodes, reflecting DoS attacks, and service theft where a malicious node/site/operator may make unauthorized use of service [5]. These threats arise due to 6to4 must behave as follows:

- All 6to4 routers must accept and decapsulate IPv4 packets from every other 6to4 router and from 6to4 relays.
- All 6to4 relay routers must accept traffics from any native IPv6 node.

So, 6to4 routers are not able to identify whether any 6to4 relays are legitimate. Besides 6to4 relays can be subject to "administrative abuse" 6to4 architecture can be used to participate in "packet laundering" which making another attack harder to trace. Thus, makes the logging and auditing functions of 6to4 traffic extremely critical. Hence, it is crucial to have 6to4 router or relay security checks be correctly implemented

2.2.2 ISATAP

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) connects IPv6 hosts/routers over an IPv4 network. It views the IPv4 network as a link layer for IPv6 and views other nodes on the network as potential IPv6 hosts/routers and therefore does not require the underlying IPv4 network infrastructure to support multicast. It defines a method for generating a link-local IPv6 address from an IPv4 address. ISATAP host is configured with a potential router list (PRL), which is a set of entries about potential routers that used to support router and prefix discovery. Since PRL provides a list of IPv4 addresses representing advertising ISATAP interfaces of routers that hosts use in filtering decisions, PRL must be kept up to date [6]. To avoid IP spoofing, the IPv4 virtual link must be delimited carefully at the network edge, so that external IPv4 hosts cannot pretend to be part of the ISATAP link. In addition, site border routers should implement IPv4 ingress filtering and IP protocol 41 filtering. Protecting ISATAP traffic can also be done by configuring IPsec for IPv4 policy settings to protect, all traffic with IP protocol set to 41.

2.2.3 Teredo

Teredo involves tunneling packets over UDP to make IPv6 available to IPv4 host through one or more layers of network address translator (NAT). It aims to provide nodes located behind a NAT with a globally routable IPv6 address. It is the last option used when no other method will work. The negative effects of Teredo services can be classify into four categories: security risks of directly connecting a node to the IPv6 Internet, spoofing of Teredo servers to enable man in the middle attack, potential attacks aimed at denying the Teredo service to a Teredo client, and denial of service attacks against non-Teredo participating

nodes that would be enable by the Teredo service [7]. As for countermeasure, Teredo nodes can use IPsec services like Internet Key Exchange (IKE), Authenticated Header (AH) and Encapsulating Security Payload (ESP). Encrypting the client's IPv6 traffic using IPsec will prevent third parties from spoofing and listening of the IPv6 packets, even if the IPv4 and UDP headers are vulnerable.

2.3 Translation

Translation is needed when the hosts can only communicate using IPv6 at the network layer. Translation techniques are varied according to the layer they may appear: network layer, transport layer or application layer. In the network layer, the header of the datagram is translated from IPv6 to IPv4 (or vice versa), which happens in the operating system of the originating host. In the transport layer, the general mechanism is the use of relay, which the data has to pass through. This relay is commonly a dual stack device that will translate and pass on datagrams between the different networks. In the application layer, an "application layer gateway" (ALG) is used, e.g. a web proxy. ALGs have to be set up for each and every application or service one wants to offer. Among IPv6 translation methods available are Stateless IP/ICMP Translation (SIIT), Network Address Translation-Protocol Translation (NAT-PT) and NAPT-PT.

3. SECURITY ISSUES

The transition from native IPv4 network to a network where IPv4 and IPv6 co-exists creates extra security considerations which need to be looked into closely. Basically the severity of these issues related to the complexity of the transition mechanisms chosen. Security issues will be introduced either in the mechanisms themselves, in the interaction between mechanisms or by introducing unsecured paths through multiple mechanisms [8].

3.1 Dual-stack Issues

Being 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 .

3.2 Tunneling Issues

Some generic dangers to tunneling include [3,8,9,10]:

- no authentication mechanism for tunnels except a check on the IPv4 packet's source address which is easily circumvented by IP spoofing .
- attacker may inject arbitrary IPv6 packets into the IPv6 network at a tunnel endpoint simply by spoofing the IPv4 address of the other endpoint.
- it may be easier to bypass firewalls and avoid ingress filtering checks
- it is possible to attack the tunnel interface: several IPv6 security mechanisms depend on checking that Hop Limit equals 255 on receipt and that link-local addresses are used.
- automatic tunneling mechanisms are susceptible to packet forgery and DoS attacks as there is no preconfigured association between endpoints.

Certain tunneling mechanisms establish communication with native IPv6 nodes or between the automatic tunneling mechanisms via the use of relay. These relays provide a potential vehicle for address spoofing, DoS and other threats.

To look at each tunneling techniques security issues, we summarize them into a table below.

Table 1. Tunneling mechanisms and their specific security issues

Tunneling Mechanisms	Security Issues
Configured Tunnel	At a host behind IPv4 firewall, need 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.
Tunnel Broker	A site administrator may be blissfully unaware of users on their site who use tunnel brokers, thus not creating any site demand for "proper" IPv6 deployment and possibly creating security holes which the administrator does not know about and therefore does not guard against.
6to4	• Attacks with Neighbor Discovery (ND) Messsages. • Spoofing traffic to 6to4 nodes • Reflecting traffic from 6to4 nodes • Local IPv4 broadcast attack
ISATAP	Possible spoofing attack:- • bogus IP protocol 41 packets are injected into an ISATAP link from outside. • bogus IP protocol 41 packets are injected from within an ISATAP link by a node pretending to be a router.
Teredo	• Bypassing security controls • Reducing defense in depth • Allowing unsolicited traffic • Laundering Dos attacks from IPv4 to IPv4 • Dos attacks from IPv4 to IPv6, IPv6 to IPv4

4. SECURITY MECHANISMS

Ample security mechanisms are important to protect electronic communications from malicious individuals who are determine to spoof, corrupt, alter or destroy the data or render critical services unavailable. This involves safeguarding every device that is participating in networked communication and all information that either is stored on a device or is in transit between communicating devices. Since IPsec is mandated in every IPv6 capable device, we should consider it seriously to provide the necessary authentication, integrity and confidentiality services.

4.1 IP Security (IPsec)

IPsec provides data confidentiality, data integrity and data origin authenticity between participating peers: a pair of hosts, a pair of security gateways or between a security gateway and a host. 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 the defined packet structure using extension headers. IPsec consists of two protocols: authentication header (AH) and encapsulating security payload (ESP). AH provides data authentication and optional anti-replay services while ESP provides confidentiality, data origin authentication, connectionless integrity, anti-replay service and traffic flow confidentiality for all end-to-end data transported in an IP packet. Both protocols support two modes of operation: transport mode and tunnel mode. In transport mode, two hosts provide protection primarily for upper layer protocols. The cryptographic endpoints are the source and destination of the data packet. As for AH in transport mode, the whole payload including the fields of the IPv6 header, which do not change in transit, is secured. While in tunnel mode, the inner packets of AH contains the IP address of sender and receiver. The outer IP header contains the IP address of the tunnel endpoints. Thus, the complete original packet, including the fields of the outer header that do not change in transit, is secured. As for ESP in transport mode, the IP header and the Extension Headers that follow are not encrypted; otherwise the packet could not be forwarded. If the complete packet has to be encrypted, the choice is to use tunnel mode. Figure 3 and figure 4 demonstrate IPv6 IPsec AH and ESP protection in transport mode and tunnel mode respectively. The ESP can be used with a NULL encryption option, which makes only the authentication option of the ESP is used, and the packet is not encrypted.

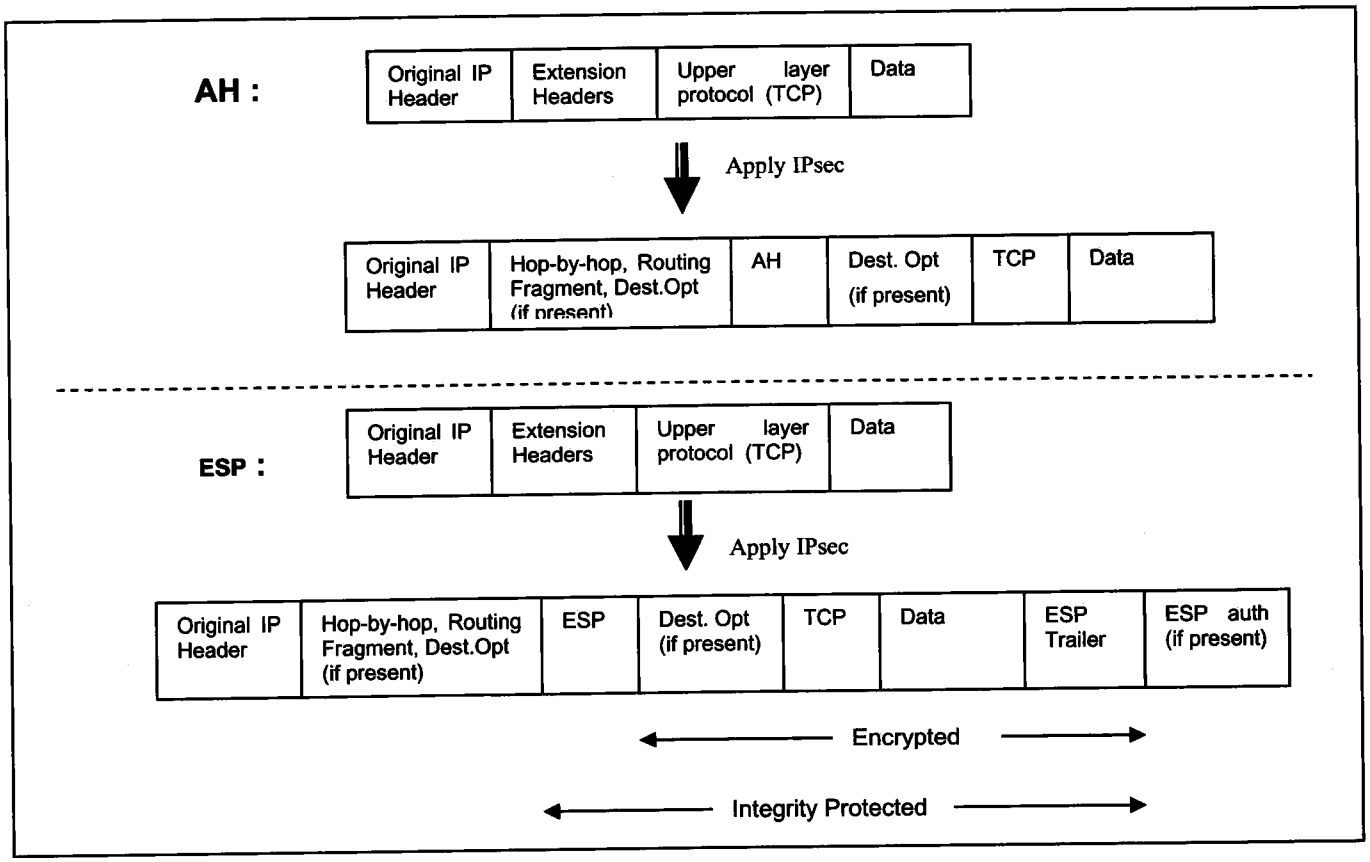

Figure 3. AH/ESP in Transport Mode

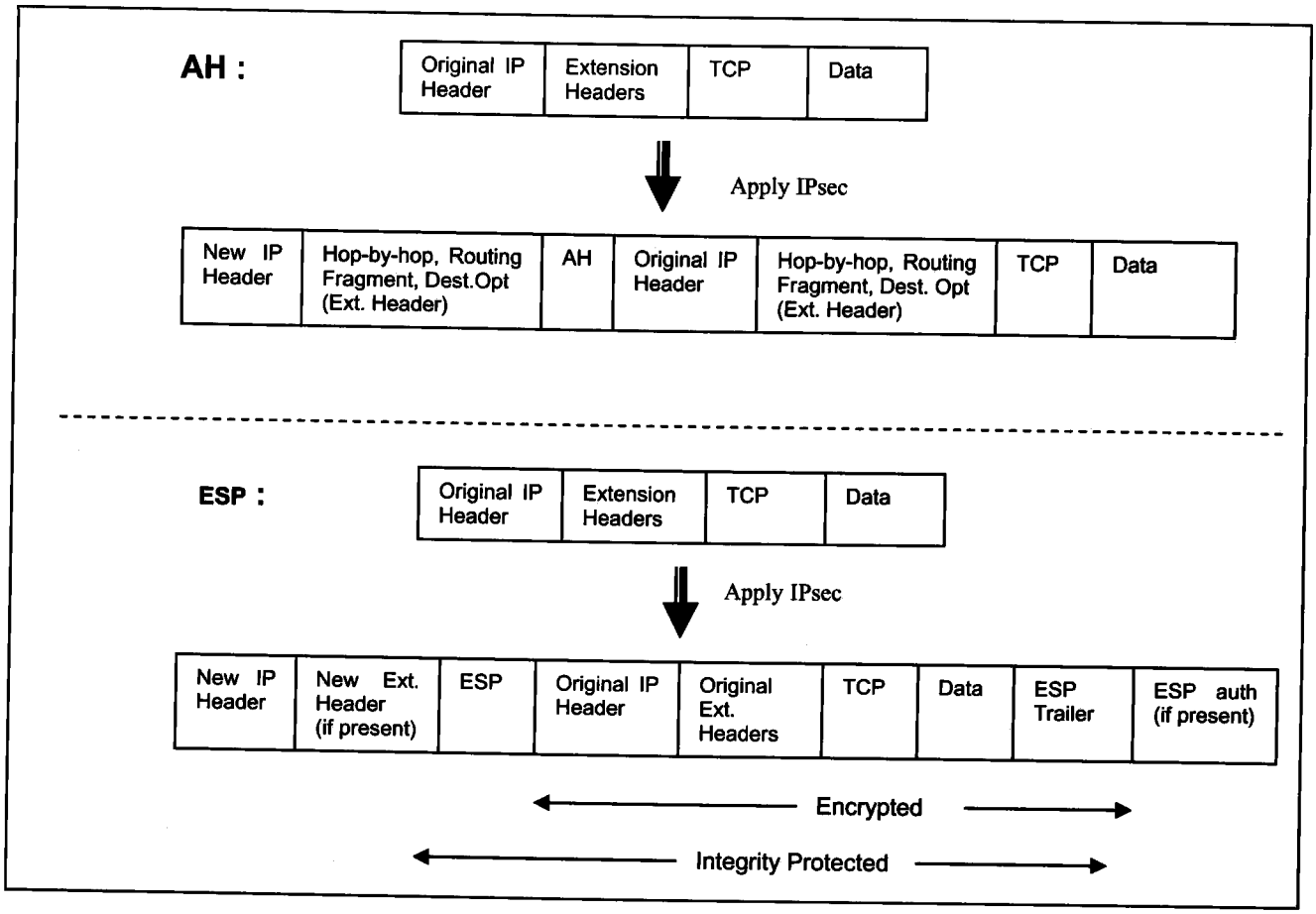

Figure 4. AH/ESP in Tunnel Mode

Although the AH and ESP protocols provide the actual cryptographic services at the network layer, we still need mechanisms that will determine which services should be applied to different traffic flows, and to negotiate the required cryptographic keys for those services. These tasks are accomplished through a combinations of Security Policy Database (SPD), the Security Association (SA) and the Internet Key Exchange (IKE) protocol. The SPD identifies the service to be applied to IPsec packets, and is consulted in the processing of all traffic (inbound and outbound), including non-IPsec traffic. For any packet, SPD will identify process to proceed, either discard, bypass IPsec, or aplly IPsec. The SA is use by IPsec to keep track of the details of a negotiated IPsec sessions between two nodes. A pair of SAs is required for communication between a pair of nodes. An SA is uniquely identified by a destination IP address, a security protocol identifier (AH or ESP), and a Security Parameter Index (SPI). It solves a problem of tracking the IKE agreements with respect to services, algorithms, and parameters for particular traffic flows. The IKE determines which service should be applied to the different traffic flows, and to negotiate the required cryptographic keys for those services. IKE has two phases: Phase 1 is used to establish a secure channel (ISAKAMP SA) through which IPsec cryptographic services and algorithm can be negotiated. Another phase, phase 2 is the actual negotiation of the IPsec cryptographic services and algorithms through the secure channel established in Phase 1.

4.2 Current Security Model

The preferred model for enterprise network security in IPv4 stresses the use of a security perimeter controlled by autonomous firewalls and incorporating NATs. Both perimeter firewalls and NATs introduce asymmetric and reduce the transparency of communications through these perimeters. At present, we just make use of similar firewalling and intrusion detection techniques meant for IPv4 but still inadequate to check IPv4 traffic. [11,13] Table 2 highlights some existing security mechanisms or threats mitigation techniques and their respective challenges to handle IPv6 traffic. While IPsec may be use to solve many issues in IPv4 or IPv6, it has some limitations. For instance, in a scenario where we do not have prior trust relationship, we need to first establish an IPv6 address in order to set up the IP security associations which creates a chicken and egg problem. Nevertheless, IPsec can be used in environment where prior relationship exists and there is a pre-defined security model in place which relies on either pre-configured keys or a PKI infrastructure.

As for IDS systems, Network-based IDS (NIDS) and Host-based IDS (HIDS) can be applied concurrently where NIDS detect attacks by capturing and analyzing network packets while HIDS could analyze the data with greater reliability and more precisely. Since IPv6 has not been widely use worldwide, we are yet to see the IPv6 signature database for IDS.

Table 2. IPv6 Mitigation Techniques and Challenges

Mitigation Techniques	Challenges
Firewalls	Lots of different extension headers and options make it hard for a firewall to filter correctly and get it right not to buffer overflow or DoS.
IPsec	IPsec is not always a valid security option because of a bootstrapping problem. (improve series: RFC4301 – RFC4309)
Logging/ Auditing	Most logging and auditing of IPv6 traffic is implemented using IPv4 transport, need IPv6 transport to successfully log and audit dual-stack network infrastructure.
Intrusion Detection	Lack of signature database. Pattern based mechanisms used for IPv4 may not be the most appropriate as end-to-end encrypted becomes more prevalent. Future systems may be more reliant on traffic flow pattern recognition.

4.3 A New Security Model

Since transition to IPv6 will be a long process, we must be ready with a better tools to secure our assets and resources while deploying IPv6 in parallel with IPv4. Moreover, as highlighted by a prominent hacker, Van Hauser, there are attacking tools that are already available to be used [12]. For a start these tools can be used for penetrating test as well as improving security on our networks (see Figure 5) by expanding the mitigation techniques in Table 2.

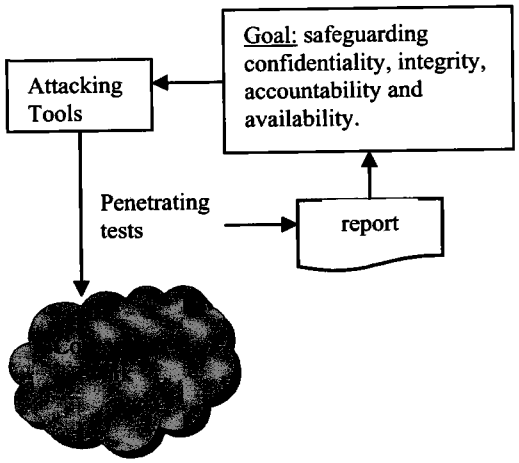

Figure 5. Penetrating test to improve security on the corporate network.

Besides the mitigation techniques, each enterprise needs to devise optimum security policies to ensure the most effective security architecture while migrating to IPv6. The main goal is to safeguarding the confidentiality, integrity, accountability and availability of the devices and the data. The bottom line, any effective security policy always needs to be technically feasible, operationally, deployable and enforceable [9].

A new model should incorporate the concept of distributed firewall. As suggested by Hagen [13], new model has to consists of managed host-based firewalls on top of the conventional perimeter firewall model with the aim to implement defense in depth. This involves a combination of centralized security policy repositories and distribution mechanisms (see Figure 6). Thus, permits network managers to place more reliance on security mechanisms at the end points and allow end points to influence the behavior of the perimeter firewalls. Perimeter firewalls responsible for securing the network from general attacks, and the end node responsible for securing itself from node-related attacks. So, firewall policies must consider all related specific security issues in the IPv6 transition as well as following an established firewall deployment model on a network. IPsec may be used to solve many issues in IPv6. For instance, tunneled IPsec may contain malicious data, which can be mitigated through IPsec firewall. There could be slightly different requirement between an enterprise security model and unmanaged network security model.

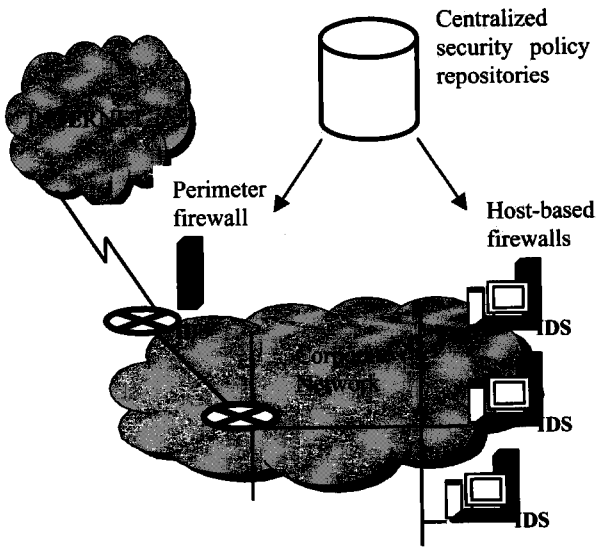

Figure 6. A combination of centralized security policy repositories and distribution mechanisms

5. CONCLUSION

Transition to IPv6 will be a long process in which both IPv4 and IPv6 will coexist and interoperating for a long while. The transition mechanisms available include dual stack, tunneling and translation. Each transition method may introduce some security effects which need to be countered for both protocols. Since both protocols co-exists in the network, current security mechanisms that support only IPv4 traffic or network properties are not sufficient. While IPsec must be implemented in standards compliant implementations, all protocols and mechanisms of IPsec need to be examined in the aim of making it useful for securing the migration period as well as the native IPv6. New considerations that apply to networks and traffic in the IP transition need to be identified and analyzed. Among of those analysis have been highlighted in the paper. A new security model and revised policy are crucial for securing the transition period as the network could be under attack or inadvertently misused by the naïve worker. Our future work

will focus on designing the new model and testing it for efficiency.

6. ACKNOWLEDGMENTS

Our thanks to the NRG members who help us with the time off for the network engineering discourse.

7. REFERENCES

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

[2] Tatipamula, M., Grossetete, P. and Esaki, H. IPv6 Integration and Coexistence Strategies for Next-Generation Networks. IEEE Communications Magazine, January 2004, 88-96.

[3] Nordmark, E. and Gilligan, R. Basic IPv6 Transition Mechanisms (RFC4213), October 2005.

[4] Hexago Gateway6. http://www.go6.net

[5] Savola, P. and Patel, C. Security Considerations for 6to4 (RFC3964), December 2004.

[6] Templin, F., Gleeson, T., Talwar, M. and Thaler, D. Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) (RFC4214), October 2005.

[7] Huitema, C. Teredo: Tunneling IPv6 over UDP through Network Address Translation (NATs) (RFC4380), February 2006.

[8] Davies, E., Krishnan, S. and Savola, P. IPv6 Transition/Co-existence Security Considerations. Draft-ietf-v60ps-security-overview-06.txt (work in progress), Oct 2006.

[9] Kaeo, M., Green, D., Bound, J. and Pouffary, Y. NAv6TF Technology Report "IPv6 Security Technology Paper" (July 2006). http://www.nav6tf.org.

[10] Colitti, L., Battista, G. D. and Patrignani, M. IPv6-in-IPv4 Tunnel Discovery:Methods and Experimental Results, IEEE eTransactions on Network and Service Management, Second Quarter 2004, 30-38.

[11] Zagar, D. and Vidakovic, S. IPv6 Security: Improvements and Implementation Aspects, Proceedings of the 8th International Conference in Telecommunications, 2005, ConTEL 2005, 15-17 June 2005,Volume 1, 29-34.

[12] The Hackers Choice. http://www.thc.org

[13] Hagen, S. IPv6 Essentials, O'Reilly Media, USA, 2006.