Journal of Fundamental and Applied Sciences

Research Article

ISSN 1112-9867

Special Issue

Available online at http://www.jfas.info

CONCEPTUAL FRAMEWORK AND THREAT MODEL FOR A SECURE IPV6 DEPLOYMENT

A. Mat Taib[1,*], W. N. A. Wan Ali[2] and A. Rosli[3]

[1]Universiti Teknologi MARA Perlis, 02600 Arau, Perlis, Malaysia

[2]School of Human Development and Techno-Communication (iKOM), Universiti Malaysia Perlis (UniMAP), Malaysia

[3]InterNetworks Research Laboratory, School of Computing, Universiti Utara Malaysia, 06100Sintok, Kedah, Malaysia

Published online: 30 May 2018

ABSTRACT

Among the IPv6 security concerns nowadays are securing the IPv6 deployment and preventing the present IPv4 network from being attacked via IPv6 traffic and vice versa. Since deploying IPv6 may involve the coexistence of both Internet Protocols, unavoidably, this coexistence scenario exposes the enterprise network to the threats and vulnerabilities of IPv4 as well as IPv6. Handling these security issues is vital to ensure a secure IPv6 deployment. Thus this paper addresses the problems by presenting a conceptual framework and IPv6 threat model to determine risk that can help network administrators to proceed with IPv6 deployment with some awareness of potential security attacks. The conceptual framework was tested via case study observation in the pilot project and some basic security measures were tested via experimentation which proved that threats are possible and can be countered by using the recommended security mechanisms.

Keywords: IPv6 deployment; secure transition; threat model; conceptual framework.

Author Correspondence, e-mail: abby4108@mail.com

doi: http://dx.doi.org/10.4314/jfas.v10i2s.67

1. INTRODUCTION

Enterprise networks interconnect significant numbers of devices that must be addressed for either a service or simple management purpose. With the depletion of IPv4 addresses, new hosts or new branches need to deploy IPv6 to enable connectivity to the headquarters or potential new customers[1]. In fact, Next Generation Networks (NGN) which are packet-based networks has started transition to IPv6. Nonetheless, some countries such as India and Malaysia experience slow rate of IPv6 deployment. Among the factors that contribute to this slow rate are uncertain risk to the network operators, unclear benefits of IPv6 to the network operators, lack of IPv6 applications, lack of technical knowledge and lack of public awareness [2]. Hence, educating the public or the management of enterprises networks regarding the importance of IPv6 deployment and its challenges is necessary. A mechanism or strategic framework for this purpose is required.

Before deploying IPv6, some considerations like cost on interoperability, personnel training, hardware procurement, and security are major concerns[3]. Other issues affecting adoption of IPv6 include vendor support, government policy, psychological factors, inevitability, no commercial incentive, and lack of immediate benefit[4]. Security is a main issue that concerns network service providers, business enterprises, and users. Thus, network security is crucial whereby constant tasks of evaluating a new threat, maintaining the present organizational security, and incorporating new technology are needed. An enterprise network usually has a number of subnets with specific roles and functions that may be exposed to a number of vulnerabilities. When an enterprise considers deploying IPv6, the management must understand the need for realizing related IPv6 security considerations.

Observation of several leadership companies by [5] finds that security administrators have serious difficulties in convincing their management about security risks and threats against them. Many network/security administrators lack the ability to explain/demonstrate the impact of security risks. There is a real need for a way of explaining the seriousness of the damage external or internal threats can cause. Therefore, an organizational framework is needed to ensure that, at policy level, end users are instructed and monitored, thus enhancing guidance and discipline when necessary. Thus, this paper presents a conceptual framework for securing the IPv6 deployment.

1.1.Conceptual Framework: An Overview

In general, a framework is a real or conceptual structure intended to serve as a support or guide for the building of something that expands the structure into something useful. In other perception, a framework is some kindof roadmap or yardstick that helps organizations determine where they are, and in reference to their peers [6]. The framework needs to tie with business objectivesto ensure that it is in line with enterprise's information security and privacy policy [7]. Thus, a security framework that consists oforganizational factors, security objectives and security mechanismsis crucial. To achieve and sustain a security state, an organization needs a security framework that successfully implements security mechanisms and services[8]. A conceptual framework is sometimes referred as theoretical framework. According to [9], "*A theoretical framework is an organized set of ideas and concepts and it is used for organizing a thought process about a particular object or situation. Within a theoretical framework different topics for consideration are identified, along with an indication of their interrelation*".

In this study, the conceptual framework is an abstraction of the required components to secure the transition. The components of the conceptual framework include the security properties, which acted as a goal to have a secure IPv6 deployment, and the other three components that become pillars to support the goal: IPv6 transition security considerations (6TSC), enterprise security concerns (ESC) and basic security mechanisms (BSM). A bird's eye view of the importance and relationship among these components is depicted in Fig.1.

Forming the conceptual framework was done using graphic model[10]. Designing a conceptual framework starts by determining the goal of the research that is to secure the IPv6 deployment, and identifying security properties that guaranteethe goal. As Fig. 1 shows, the up pointing arrow represents the goal of the framework, that is, to secure the IPv6 deployment in an enterprise networkby maintaining the following five interdependent security properties: confidentiality, integrity, availability, accountability and assurance[11].

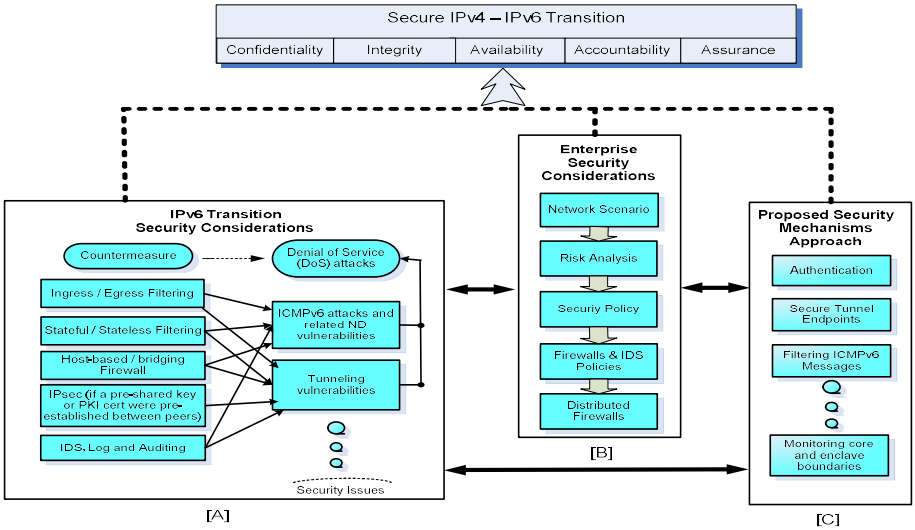

Fig.1. Conceptual framework

Confidentiality requires that private and confidential information not to be disclosed to unauthorized individuals either in storage, during processing or while in transit. Integrity ensures that information has not been modified in an unauthorized manner while in storage, during processing or while in transit. Availability assures information and services are not denied to legitimate users. On the other hand, accountability requires that actions of an entity may be traced uniquely to that entity. This is important in supporting policy requirements like non-repudiation, fault isolation, intrusion detection and prevention, after-action recovery and legal action. While, assurance is the basis for confidence that all security measures both technical and operational function as intended, to protect the system and information it processes.

Coexistence of both IPv4 and IPv6 is a scenario that most enterprises have to face for a long while. It requires the enterprises to prepare for security issues related to transition mechanisms they employed[12].Understanding the security issues in enterprise network during IPv6 transition is vital before identifying appropriate security approach to counter the problem is possible. Thus, the conceptual framework emphasizes the following three components (refer to Fig.1): IPv6 transition security considerations (6TSC) enterprise security considerations (ESC) and proposed security mechanisms approach which is called as basic security mechanisms (BSM).

6TSC identifies the security issues and challenges in IPv6 transition. An analysis on threats, vulnerabilities and risks has produced a general threat model for IPv6 transition[12]. Although

there are many potential threats, this paper only focuses on finding alternative solutions to the tunneling threats and ICMPv6 related attacks because tunneling and ICMPv6 are indispensable during the transition.

Tunneling cannot be avoided if the network infrastructure is still in IPv4. Tunneling techniques face complexity in configuring devices as well as logging and monitoring the traffic.Without built-in security, no authentication and integrity check, they are exposed to IP spoofing, injecting packet at the tunnel endpoint and bypassing firewall or ingress filtering checks. In other words, they are highly susceptible to packet forgery and DoS attacks. Fig. 2 shows a packet injection scenario at the TEP [13] where a hacker can inject traffic in the tunnel by pretending to be a legitimate user by spoofing the external IPv4 and internal IPv6 addresses.

Meanwhile, ICMPv6 messages give important information about the health of the network and are used by neighbor discovery protocol (NDP) to determine link layer addresses for neighbors attached to the same link, find routers, keep track of which neighbors are reachable and detect changed link layer address. Consequently, it is a must to prevent some ICMPv6 messages from being filtered in order to have the IPv6 networks operate properly. ICMPv6 specifications allow an error notification response to be sent to multicast addresses. This fact can be misused by an attacker. By sending a suitable packet (spoofed source) to multicast addresses, an attacker can cause multiple responses targeted at the victim.

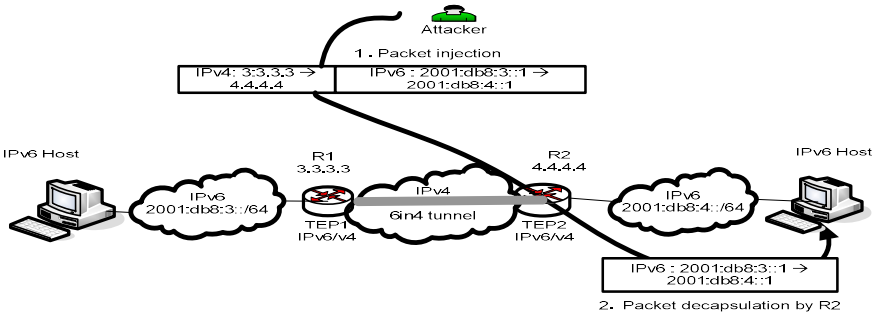

Fig. Erreur ! Il n'y a pas de texte répondant à ce style dans ce document.**.** Packet Injection in TEP

In parallel to understanding the security issues in transition, security administrators must also identify and analyze the security concerns of enterprise networks when deploying IPv6. Both 6TSC and ESC must be aware and understood by people who are responsible for IPv6

transition. Consequently, the last factor that was emphasized is the basic security mechanism (BSM) to handle the security concerns already identified in both 6TSC and ESC. Hence, to ensure a secure transition to IPv6, an enterprise network must consider all the three components. The two-point arrows connecting 6TSC and ESC as well as 6TSC and BSM show that 6TSC is associated with ESC as well as with BSM. Similarly, ESC is associated with 6TSC as well as with BSM.

1.2. Enterprise Security Concerns (ESC)

As for transitioning to IPv6, the relationship among risk analysis, the organization's culture and security policy is important in determining the success of the security during transition.Hence,the following five **s**ubcomponentsof ESC highlight the important steps during IPv6 deployment.

1.2.1. Network Transition Scenario

Network transition scenario is the condition or stage of the network during IPv6 deployment which tells whether the network is a native IPv4, a dual stack or a native IPv6 and how the network is connected to the Internet. A dual stack host in a native IPv4 network needs a v6-in-v4 tunnel to send IPv6 packets. Similarly, a native IPv6 network needs to send IPv4 packets via a v4-in-v6 tunnel, while dual stack network infrastructure uses IPv4 connectivity for IPv4 packet and IPv6 connectivity for IPv6 packet. At any stage of network scenario, it must identify assets important to the enterprise and security properties that need to be implemented.After identifying how these enterprise network scenarios operate, a risk analysis of the potential threats and vulnerabilities should be carried out.

1.2.2. Risk Analysis

Risk analysis is a systematic process to examine the threats facing the IT assets and the vulnerabilities of these assets and to show the likelihood that these threats will be realized[14]. Besides, risk analysis is considered appropriate for securing computer/IT assets which mostly physical in nature and of which the threats and vulnerabilities can be estimated by means of qualitative or/and quantitative measures. The basic stage of risk analysis begins with risk identification, risk estimation and risk evaluation[15] and is followed with risk management.Nevertheless, this study adopts risk assessment overview [16]as a guideline to identify the assets and security measures the policy must address.

In the risk analysis process, the network or security administrator has to identify assets that must be protected, people who can attack the assets, tools (and their sources) that can be used to attack the assets, immediate costs if the asset is attacked, and time needed to recover from the attack. Then, the appropriate security mechanisms to protect the particular assets and services must be determined. The risk to an asset is zero if no threats or vulnerabilities exist for the asset. In facing the threats and vulnerabilities of IPv6 deployment,the enterprise can calculate the expected risk for each asset as follows [17]:

$$Risk1(A) = \sum_{n=1}^{\infty} (ThreatValue(A) * Vul'nerabilityValue(A)) \quad (1)$$

$$Risk\ (A) = Risk\ 1(A) * AssetValue\ \ (A) \quad (2)$$

Threat assessment consists of identification of threat sources, the threat target and the threat likelihood. Identifying and assessing threats can be done through threat modeling[18,22]. Besides, threat categorization can be based on the goals or the purposes of the attack such as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privileges.

Vulnerability is a weakness that could be exploited by a threat, causing the violation of an asset's security property[19]. An enterprise vulnerability assessment helps the administrator to identify the weakness of the enterprise's assets and the systems that enable access to them and evaluates the severity if vulnerability were to be exploited. It then needs to identify vulnerabilities that can be exploited by existed threats previously identified. In other words, it is needed to determine whether the vulnerability has an associated threat. If any vulnerability is found to have no associated threat, it can be removed from consideration list. Determining whether the vulnerability has an associated threat or not can be done by figuring out whether the security properties (confidentiality, integrity, availability, accountability and assurance) could be compromised as a result of the weakness. This requires a building of threat-vulnerability table.

Later, a vulnerability severity scale is built by first defining a rank, then a meaning and description to each rank. The rating represents the degree to which the asset is susceptible to

the vulnerability, and the potential impact should the vulnerability be exploited. The range and description are at the discretion of the enterprise.

Rating the severity of vulnerability can be done according to the following[16]:

- Number of threats that can be realized as a result of a given vulnerability being exploited, number of systems affected.
- The prevalence of the system affected.
- Whether or not the weakness exists in default configurations or installation.
- Whether any precondition need to be existed before the vulnerability can be exploited.
- Whether the affected asset is responsible for monitoring or protecting other assets.
- Whether the attacker needs to lure victim to a hostile server in order to exploit the vulnerability.

Security measures that are already in position helpthe enterprise to counter the resistance to the vulnerability and the severity of damage it causes.

All assets need protection, but the one should be entertained first depends on the rank of priority, which is based on the severity of the impact. Subsequently, respective security policy must be designed. The administrator must include policy respective to IPv6 to the existing policy setup for IPv4.

1.2.3.Security Policy

The security policy is the result of the risk assessment analysis and is linked to the business and operational practices of a particular corporation. Although a uniformed comprehensive policy for most environments is impossible, the ultimate goal is to maintain the availability, confidentiality, integrity of devices and data.

During a transition, anti-spoofing via ingress and egress filtering is important. Filtering the packet can be based on the address prefix. Since only a small fraction of the total IPv6 address space has been allocated, security policy can be designed to only permit packet sourced from the prefixes of the IPv6 allocated space while all other IPv6 addresses would be blocked. Moreover, due to IPv6's address hierarchy, the list of the IPv6 addresses that are legitimate and should be granted is small and maintainable.Network security policy determines the extent to which a network will be exposed to the outside world and the degree to which a policy allows an attack to spread within the network.

Thus, the security administrator can come up with a comprehensive security policy which enables the system to scale up as needed in parallel to IPv6 transition. A site security manager or administrator has to design a comprehensive policy for the site network to deal with many end-to-end communications and threats related to site-local scope addresses due to IPv6 transition. Nevertheless, in some organization a network administrator is responsible to both job specifications.

1.2.4. Firewall and IDS Policy

Detailed itemized policies for certain nodes and subnets or departments must be clearly defined to ensure that appropriate user or machine is given the privilege to access service according to its role and function. This includes identifying and assigning hosts and people to correct privileges. This network security policy together with the best security practices for IPv6 deployment would be considered in designing the firewalls and IDS policy. All these policies will be integrated and centralized in a repository of a hybrid distributed firewalls concept to ensure end-to-end security.To function effectively, IPv6-capable firewalls need to maintain state tables for both IPv4 and IPv6 and application-aware firewalls must keep track both IPv4 and IPv6 transactions simultaneously. Consequently, these issues give an impact on configuration complexity for the network engineer as well as the throughput performance of the firewall and the end-to-end sessions.

It is equally important to have an intrusion detection system installed. Network-based IDS (NIDS) should be used in monitoring the network real-time on a specified network segment, such as in the DMZ. It is needed to be deployed inside the intranet firewall to monitor a firewall and to ensure that there are no tunnels being established through the firewall to violate the network system. Meanwhile, Host-based IDS (HIDS) should be implemented on the host that operates critical data. The NIDS and HIDS will provide protection by having intrusion-detection agents that monitor unusual administrative activities or configuration changes and reporting intrusions to a managing agent installed on a central computer. This implementation makes management of security in the network becomes easier.

1.2.5. Distributed Firewall

A firewall is considered as a part of distributed firewalls when it has communication with several neighboring firewalls and shares a part of their policy. Distributed firewalls are a set

of firewalls that are managed together with the objective to consolidate their security policy. When these firewalls are managed centrally, only one configuration is required and the overall policy is coherent if well implemented but they may suffer several problemsdue to various number of firewalls and localized policies. On the other hand, when those firewalls are independent and are administered separately, they are called decentralized distributed firewalls[20].

When IPv6 is deployed, end-to-end communication and IPsec tunnel would be common since IPsec is mandatory in IPv6 installation. Thus, its usage may result in many packets being encrypted. Solelyrelying on perimeter firewall to secure the network from external attacks is no longer sufficient because the perimeter firewall could not filter the packet's content. It is the responsibility of the host to ensure the integrity and authenticity of the packet it receives.

Moreover, the entrance to the network can be via many ways. Encrypted traffic may definitely escape from being filtered at the edge router or border firewall. Hence, there is a possibility that the intruder's packets could bypass the firewall and safely enter the network. Besides, insiders too can easily generate the attack anytime without being checked. Hence, a hybrid-distributed firewall which consists of perimeter firewall and host-based firewall is essential. Fig. 3 shows the recommendation implementation of distributed firewalls. Each host should have its own policy and enforce it without relying on the perimeter firewall to ensure security of the whole network.

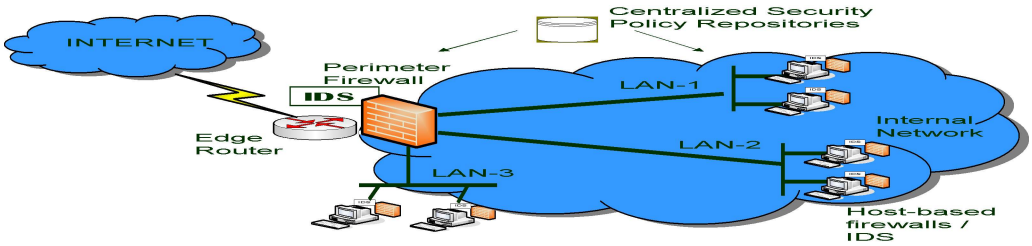

Fig.3. Segmentation and Hybrid-Distributed Firewall

2. METHODOLOGY

2.1.Evaluation of the Conceptual Framework

Evaluation of the conceptual framework was performed using experimentation as well as case study on the pilot transition project of several government agencies. The applicability of the ESC could be observed during the case study. Experimentation was used to verify and

validate the 6TSC (component A) and BSM (component C). The respective testing was integrated in the experimentto verify the suggested basic security mechanisms.

In this work, the case study answers the "how" and "why" questions that relate to how the transition can be done and why they are being done in that particular way and what are the consequences of the approach in terms of security and how is that possible and what can be done to reduce the negative impact. This case study aimed to observe the transition process and its security issues and countermeasures in a way to answer how the transition occurs in the real world in terms of what tasks are involved in order to allow both IPv4 and IPv6 to exist in a network and how to maintain security as much as possible. Besides, observation was also done to seek if the idea presented in the conceptual framework really happened or could be carried out during the transition process and verify whether the suggested basic security mechanism worked as planned.

In the pilot project, the IPv6 deployment was implemented using tunnel and dual stack. Hence, for test purposes, a similar topology was created as an experimental testbed to emulate the reality of an agency has IPv6 connectivity with some other departments via tunnels. Fig. 4 shows the manually configured tunnel used in the experimental testbed.The nodes in the network were set to be in dual stacked with both IPv4 and IPv6 address installed.

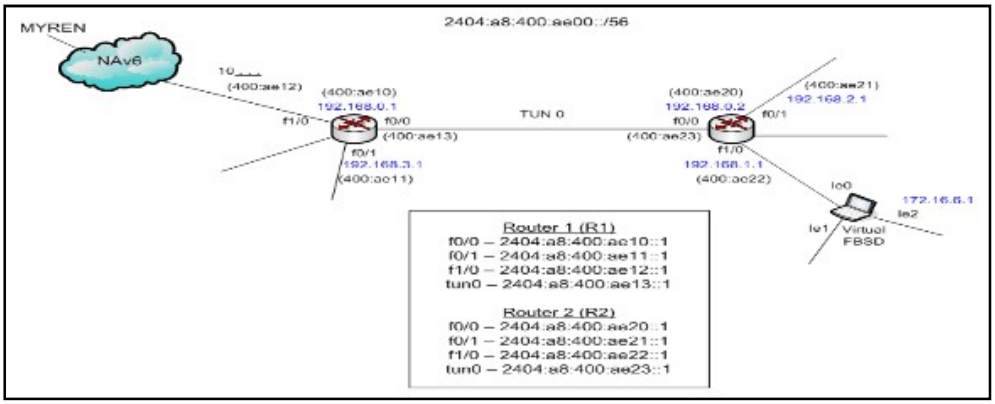

Fig.4. Manually configured tunnel

2.2.Potential Threats and Vulnerabilities

Unsurprisingly, Agency_B's existing firewall did not support IPv6 filtering. Generally, people think that when they do not enable the IPv6 in their network, they do not have to apply any IPv6 filtering at the gateway. They are not aware that most operating systems are IPv6-enabled by default, consequently, an adversary can possibly manage to implant an IPv6

fake router program which advertises an IPv6 prefix. Hence, if a host inside the network solicits an IPv6 prefix, an auto-configuration with EUI-64 address is possible. Then, it causes IPv6 packet to exist in the network. If an attacker can control the packet, he can pass anyharmfuldata or malicious code as a payload of IPv6 packet that freely travels coming in or going out from the network because a firewall was not configured to filter an IPv6 packet.

Threats may result from ICMPv6 messages that open the door for many attacks, including flooding and DoS attack. These are possible because any malicious node that generates ICMPv6 packets can easily fool other nodes on a network segment to follow the packet's instructions. If the attacker generates a flood of ICMPv6 messages, a victim node or network segment suffers decreasein performance. Since no ICMPv6 filtering is configured, the network is exposed to this kind of attack. Hence, appropriate actions should be taken to configure basic filtering mechanisms for ingress and egress filtering using access control list (ACL) at the router interface.

2.3. Lesson learned from the Observation

The basic security means of computer networks are firewalls devices and access control lists (ACL) in network routers and switches. Thus, network security policy term in this section refers to firewall rules and ACLs. From the observation, we found thatthe Agency_A's existing security policydoes not consider IPv6 traffic because it is new to them and all this while they are operating in IPv4. Hence, the policy need to be modified to include IPv6 considerations, or else, the network may be exposed to attacks generated by the bad guy who exploits the default IPv6 address to attack the network.

Since no IPv6 security mechanism was deployed to filter IPv6 connectivity, a minimum IPv6 filtering was done at the router via ACL filtering rules. At least, it gave some basic IPv6 security during the transition. The ACL rules as shown in Fig. 5 were applied to the IPv6 router. These rules basically deny all kinds of tunnels except the configured tunnel between two agencies. As for managing the dual stack network, an IPv6 capable network monitoring suite was installed.

```
ipv6 access-list INET-WAN-V6-IN
        deny ipv6 200::/7 any
        deny ipv6 3FEE::/16 any
        deny ipv6 5F00::/8 any
        deny ipv6 FEC0::/10 any
        deny ipv6 2001:0DB8::/32 any
        permit icmp FE80::/10 any
        permit tcp any host 2404:a8:400:a802::1000 eq 22
        permit icmp any any
        permit tcp any 2404:a8:400:a800::/56 established
        deny ipv6 any any
```

Fig.5.IPv6 filtering via ACL rules at the router

3. RESULTS AND DISCUSSION

3.1.The Applicability of the Conceptual Framework in the Case Study

The applicability of the conceptual framework had been tested in the case study during the IPv6 transition pilot project of the three government agencies. After proving the connectivity was successful, the threat model of IPv6 transition was mapped to the dual stack network scenario. The conceptual framework, particularly the stages in ESC was used as a reference in analyzing the potential security issues in the project. After considering that a dual stack and tunneling IPv6-in-IPv4 were the scenarios that involved in the transition, a risk analysis had been carried out.

3.1.1. Risk Determination

In determining the vulnerabilities and threats of the transitioned network, this study had identified that the router, the switch and hosts in the VLANs, the firewalls, the servers and data or information of the network were the possible assets that could be threatened. Moreover, these resources must be protected from being misused by the adversary. Thus, to determine the expected risk for each asset, the threat value, vulnerability value and the asset value formed the inputs to the Equation (1) and Equation (2).

Asset value is assigned to measure the relative important of an asset. For this purpose, this study adopted the asset value scale, the event likelihood table and risk rating translation by [16]in assigning the threat value.

Table 1. Event likelihood

Rating	Severity	Description
6	Extreme	The threat action is continually occurring
5	Very High	The threat action occurs very often
4	High	The threat action regularly happens

Table 2. Risk translation

Rating	Range
6	656 - 786
5	525 - 655
4	394 - 524

3	Medium	The threat action occurs infrequently	3	263 393
2	Low	The threat action rarely takes place	2	132 - 262
1	Negligible	The occurrence of this threat action is extremely unlikely within a human lifetime	1	1 - 131

This study then builds a threat-vulnerability table for information and network assets (see Table 3). This is done by extending the threat table by associating vulnerability with a threat action. As mentioned in NIST800-30, the severity of vulnerability can be measured as high, medium, or low[21]. As Table 3 shows the threat-vulnerability table pairs the vulnerabilities with threats. The threat value is represented by the frequency of threat occurs and the vulnerability value is represented by the severity of the vulnerability. These values are used in the Equation(1)and Equation(2) to calculate the expected risk.

Table 3. Threat-vulnerability table for information and network assets

Threat Action	Frequency	Vulnerability	Severity
Employee / Personnel			
Unauthorized access of information assets	5	Weak information security controls enabling unauthorized access	3
Data entry errors	5	Lack of data validation during form input	2
Leaking confidential information	3	Exposure of information assets	3
Data got corrupted or lost due to malicious software	5	Ignorance that the IPv6 is enabled by default in the current operating system and potentially exploited by the attacker to inject Trojan	3
Network resources (Router, switch, client host, server, firewall)			

Router miss-forwarding	4	Susceptibility to fake neighbor solicitation	3
Switch miss-forwarding	4	Susceptibility to fake neighbor solicitation	3
Autoconfiguration threat	3	Susceptibility to fake router advertisement	3
		Susceptibility to duplicate error detection	3
		Susceptibility to fake router redirect	3
Client host exposes to malicious code as a result of encrypted packet that has not been filtered after decrypting and could come from a banned source	3	Lack of host-based filtering	4
Server being denied to the authorized access	4	Lack of mechanism to prevent DoS attack	3
Bypassing firewall	4	Lack of checking the packet source origin	3
		Lack of checking the IPv6-in-IPv4 tunnel packet or protocol 41	3

Hence, using information in Table 3, a risk evaluation for network assets is calculated as follows:

Risk (network resources) = 12 + 12 + (9+9+9) +12 + 12 + (12 +12) = 99

Risk (Router) = 4 * 99 = 396

Risk (Switch) = 4 * 99 = 396

Risk (Client host) = 4 * 99 = 396

Risk (Server) = 5 * 99 = 495

Risk (Data/Information) = 5 * 99 = 495

Risk (Employee/Personnel) = (15 + 10 +9 + 15) * 6 = 294

Risk (Firewall) = 55 * 99 = 495

Risk (Bandwidth) = 4 * 99 = 396

Risk (Speed) = 4 * 99 = 396

Asset value for the risk calculation was obtained from a vulnerability severity scale in[16]. For instance, asset value of a network system administrator or security officer is extreme, equal to 6. Hence, the calculated risk is put in column 3 of Table 4 that lists associated value for asset and risk of the enterprise network. The priority of asset according to its risk values is listed in column 4.

Table 4. Asset and the calculated risk

Asset	Asset Value	Risk value	Priority
Firewall	5	495	High
Server	5	495	High
Database	5	495	High
Information	5	495	High
Router	4	396	High
Switch	4	396	High
Bandwidth	4	396	High
End host	4	396	High
Speed	4	396	High
Personnel	6	294	medium

A risk with a higher priority needs more concern. In other words, all assets need protection but which one should be entertained first depends on the rank of priority. Subsequently, a respective security policy must be designed. The administrator must include an IPv6-related policy into the existing policy setup for IPv4. After determining the risk, the required policy associated with the risk needs to be developed. The following section discusses the development on the required policy to deal with threats and vulnerabilities.

3.1.2.Network Security Policy Development

The author assumes that there is a potential attack in every packet or message transmitted in

an IPv6/IPv4 coexistence network. There is a possibility that several transition mechanisms could be abused by third parties or spammers. Hence, a proper access control must be devised to secure the transition. Since both IP versions coexist in the network, the same policy in IPv4 must also be applied for IPv6 packets. IPv6 rules must be configured to emphasize the same enforcement. Besides, an IPv6 address can be blocked inbound and outbound at network perimeters according to its prefix. In addition, perimeter firewall should also filter network's own address space from being advertised to the network from a customer or any peer. This should protect anyone from trying to destabilize the network's routing.

A network administrator may use special-use IPv6 addresses in RFC5156 to craft filters to prevent these packets from traversing network perimeters. It is essential to always filter packets coming to the network that are sourced from bogus addresses. Nevertheless, some additional rules to cater for tunneling endpoints and ICMPv6 messages need to be included. The intention was to permit the minimum set of ICMPv6 messages to allow IPv6 to function properly. Policy regarding ICMPv6 is detailed out in another paper which demonstrated a selective filtering to secure ICMPv6 messages for IPv6 Deployment[22].

When creating a comprehensive IPv6 security strategy, the administrator must consider the security of the IPv6-enabled host computers. Security challenge in the host is also due to the fact that nodes have multiple IPv6 addresses. Therefore, a security policy must consider all these multiple addresses when designing rules for each host. Once connectivity of hosts is working properly and both protocols can operate in the network, respective security policy for dual stack environment is installed.

3.1.3. Implementation of the Firewall and IDS Policy

Implementation of the filtering policy includes security policy regarding tunnel endpoints, ICMPv6 messages and the integration of these two into a hybrid-distributed firewall. Meanwhile, messages that should be dropped had been filtered earlier before further checking was executed. As for unallocated error messages that had not been defined by IANA, the proposed policy decided to drop the messages to avoid risks because these messages could be used as covert channels[23]. In addition, among the rules of thumbs for an administrator's action are to disable unused services, remove unused program and close unused ports in order to reduce potential attacks caused by exploitation of these unused services by attackers.

However, the policy can be revised from time to time as the needs arise.

It is good to have the implementation of separate IPv6 and IPv4 firewall in an enterprise network[13]. In this case, IPv4 travels through IPv4 router while IPv6 travels through IPv6 router. Having a separate IPv6 firewall could also reduce the potential impact of IPv6 on an existing IPv4 firewall[24]. The firewall implementation had involved packet filtering at layer-3 as well as application layer firewall at the host. Proper ingress and egress filtering were done at the router as well as the host. IPv6 packets can be crafted in many ways to try to cause a DoS attack or consume firewall resources. Hence, firewall should drop packets that do not follow the standard header rules or violate basic packet sanity. Besides, network administrator must consider valid IPv6 address ranges and filter out packets that use the unallocated address.

As for detecting potential intrusion system, Snort 2.9 was usedfor monitoring the anomalies activities in the enterprise network based on a signature-based IDS and anomaly-based IDS. In detecting the traffic, all packets and events are checked against the configured set of policies and rules. Rules were created to detect any ICMPv6-related messages that were prevented from entering the network. Tackling the intrusion was done by checking associate rules assigned for each router. Snort can capture data for real time and offline analysis.

In real time analysis, the IDS warning on syslog during an attack occurrence proved that IDS had been activated and was functional [25]. Meanwhile, offline analysis requires capturing the traffic in batch, such as for a day or a week, then replay the data to look for intrusions. With Snort and Basic Analysis and Security Engine (BASE) as web-based graphic user interface, alerts displayed can help the network administrator to monitor the network and take appropriate actions to counter the security threats and vulnerabilities.

4. CONCLUSION

This paper describes the components of the conceptual framework and presents how they are capable of guiding a secure IPv6 deployment.Initially, each enterprise network must identify its network transition scenario and then do carry out risk analysis for each step in IPv6 deployment stages. After identifying the possible risks and prioritizing the security mechanisms to be employed, it has to state the required enterprise security policy.

Simultaneously, the steps taken towards transitioning to IPv6 must be put under attention of respective security measures. Despite handling the security issues in the transition, the types of threats that concern an enterprise depend on its risk assessment.Risk assessment is conducted to identify the security risks and determine appropriate controls that are necessary to mitigate the identified risks. Thus, the administrator needs to apply respective security measures according to the threats and risks faced by the scenario of the network during the transition.In conclusion,the conceptual framework can be materialized to determine the potential risks and appropriate security approaches could be taken to prevent the expected attacks.

5. ACKNOWLEDGEMENTS

The work presented in this paper was also supported in part by the Fundamental Research Grant Scheme (FRGS) grant No. 600-RMI/SSP/FRGS 5/3/Fsp (54/2010) and grant No. 203/PKOMP/671182.

6. REFERENCES

[1] Gupta N, Gupta S, Pandey M. Evolution of new version of internet protocol (IPv6): Replacement of IPv4. IITM Journal of Management and IT, 2017, 8(1):86-89

[2] Limkar S V, Jha R K, Pimpalkar S. IPv6: Issues and solution for next millennium of internet. In International Conference and Workshop on Emerging Trends in Technology, 2011, pp. 953–954

[3] Huston G. In defence of NATs: An opinion. In IEEE Conference on Computer Communications Workshops, 2017, pp. 625–628

[4] Oxley A. Issues affecting the adoption of IPv6. In International Conference on Computer and Information Sciences, 2014, pp. 1–6

[5] Kondakci S. A new assessment and improvement model of risk propagation in information security.International Journal of Information, Computing and Security, 2007, 1(3):341–366

[6] Allen J. Governing for enterprise security: Networked systems survivability program. Software Engineering Institute, 2005

[7] Vorakulpipat C, Sirapaisan S, Rattanalerdnusorn E, Savangsuk V. A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. Security and Communication Networks, 2017, 2017:1-11

[8] Ballardie T, Crowcroft J. Multicast-specific security threats and counter-measures. In Symposium on Network and Distributed System Security, 1995, pp. 2–16

[9] Karyda M, Kiountouzis E., Kokolakis S. Information systems security policies: Acontextual perspective.Computer Security, 2005, 24(3):246–260

[10] Whetten D A. Modeling theoretical propositions. Designing Research for Publication, 2009, pp. 217-250

[11] Stoneburner G.Underlying technical models for information technology security.No. Special Publication (NIST SP)-800-33, Maryland: National Institute of Standards and Technology, 2001

[12] Taib A H, Budiarto R. Security mechanisms for the IPv4 to IPv6 transition. In IEEE 5th Student Conference on Research and Development, 2007, pp. 1-6).

[13] Taib A M, Budiarto R. Securing tunnel endpoints for IPv6 transition in enterprise networks. In IEEE International Conference on Science and Social Research, 2010, pp. 1114-1119

[14] Gerber M, Von Solms R. Management of risk in the information age. Computers and Security, 2005, 24(1):16-30

[15]Tchankova L. Risk identification-Basic stage in risk management. Environmental Management and Health, 2002, 13(3):290-297

[16] Schumacher M, Fernandez-Buglioni E, Hybertson D, Buschmann F, Sommerlad P. Security patterns: Integrating security and systems engineering.New Jersey: John Wiley and Sons, 2013

[17] Ye N.Secure computer and network systems: Modeling, analysis and design. New Jersey: John Wiley and Sons, 2008

[18] Meier J D. Web application security engineering.IEEE Security and Privacy, 2006, 4(4):16–24

[19] Rosli A, Taib AM, Ali WN. Utilizing the enhanced risk assessment equation to determine the apparent risk due to user datagram protocol (UDP) flooding attack. Sains Humanika, 2017,

9(1-4):21-25

[20] Leroy D. Assessment software development for distributed firewalls. Master thesis, Belgium: Université Catholique de Louvain, 2006

[21] Stoneburner G, Goguen A Y, Feringa A. Sp 800-30: Risk management guide for information technology systems.Maryland: National Institute of Standards and Technology, 2002

[22] Taib A H, Ali W N, Shaari N S. ICMPV6 vulnerability: The importance of threat model and SF-ICMP6.International Journal of Mobile Computing and Multimedia Communication, 2013, 5(2):78–100

[23] Groat S, Dunlop M, Marchany R, Tront J. IPv6: Nowhere to run, nowhere to hide. In IEEE 44th Hawaii International Conference on System Sciences, 2011, pp. 1-10

[24] Abdulla S A. Survey of security issues in IPv4 to IPv6 tunnel transition mechanisms. International Journal of Security and Networks, 2017, 12(2):83-102

[25] Bahaman N, Anton Satria P, Mas' ud Z. Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. Journal of Applied Sciences, 2011, 11(1):118-124

How to cite this article:
Mat Taib A, Wan Ali W N A, Rosli A. Conceptual framework and threat model for a secure ipv6 deployment. J. Fundam. Appl. Sci., 2018, *10(2S), 927-947.*