TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 12, No. 12, December 2014, pp. 8335 ~ 8343
DOI: 10.11591/telkomnika.v12i12.6815

Performance Comparison of Host Identity Protocol and TCP/IP with Firewall against Denial of Services

Alfan Presekal*[1], Riri Fitri Sari[2]
Department of Electrical Engineering, Universitas Indonesia, Kampus Baru UI Depok 16424, Indonesia
*Corresponding author, e-mail: alfanpresekal@gmail.com[1], riri@ui.ac.id[2]

Abstract

Host Identity Protocol (HIP) is a new kind of Internet protocol which has been developed to resolve the existing problems of Internet protocol TCP/IP. As a new protocol HIP provides many advantages compared to TCP/IP such as in the aspect of security and mobility. Unfortunately, the deployability rate of HIP was still low. One of the reason is because particular solution for currently Internet problems already popular and deployed worldwide. In this work we compare the performance of HIP and TCP/IP using several scenarios. Simulations result show that TCP response time in normal condition (zero attack condition) 98,627 ms, while HIP has the response time of 99,711 ms. We also compare the performance of the HIP, TCP/IP, and SSL against the low to medium Denial of Services attack (DoS). In the condition of low to medium DoS attack, the order from best performance are TCP/IP, HIP, and then the worst one is SSL. In the condition of high DoS attack three of them TCP/IP, SSL, and HIP cannot work. Only HIP that implements HIP Firewall with authorization scenarios that are still available for service.

Keywords: *host identity protocol, denial of service, internet protocol, security, firewall*

1. Introduction

Internet technology development has gone through a lot of success stories since the first implementation of the Internet. The Internet has had enormous impact on people live around the world. One of the indicator is the growing number of the user. Unfortunately there are still problems that is embedded into the existing Internet architecture [1]. The first design of the Internet was created without considering the future challenge of the Internet. The original Internet was developed under research network in USA. In the first implementation, the Internet was only for research purposes. In the next stage, the growth of the Internet was uncontrolled to spread around the world. After Internet became popular many problems arise such as lack of security, the limited address availability, and also mobility. For example several large-scale security threats i.e. IP spoofing, distributed denial of service (DDoS) attack, phishing, vulnerability scanning, intrusion and wide-spread worm infection have been long stayed unresolved, one of the reason is because of the lack of the accountability mechanisms in the current Internet protocol [2, 3].

To solve current problems of the Internet many ideas were proposed, some of the research try to redesign the basic protocol of the Internet [4]. As an example there are several ideas proposed to create future Internet Protocol i.e. IP Sec [5], Accountable Internet Protocol (AIP) [6], and Mobile IP [7]. Those ideas were proposed because the Internet protocol TCP/IP has many weaknesses and hard to face the future Internet challenge. Moreover TCP/IP protocols, which once acted as the basic protocol of the current Internet have been unable to provide secure platform for communications [8]. Many ideas talk about future Internet protocol to replace existing major Internet protocol TCP/IP. One of the solutions that is already proposed by the IETF is Host Identity Protocol (HIP) [9, 10].

HIP enhances the original Internet architecture by adding a new namespaces for splitting the host and the location identifier. The host identity of HIP no longer use IP address, HIP uses cryptographic key as host identity. This kind of the host identity will enhance accountability of the protocol. Moreover HIP also proposed another solution for the other problems, such as for mobility issues HIP can handle mobility through its protocol. Unfortunately the deployment of HIP is still low. One of the reason that made deployability rate of HIP low is because several solutions for current Internet problems have been deployed [11]. For example

Received September 14, 2014; Revised October 27, 2014; Accepted November 16, 2014

due to the lack of security in TCP/IP protocol, there is SSL protocol that tried to enhance the security aspect of the Internet. Currently SSL is already well known and deployed worldwide. The next example is Mobile IP that tries to improve mobility aspect of the Internet. Both of them are good solution for the existing Internet problems. Unfortunately the solutions were not integrated. That is the reason why HIP tried introduce integrated solution for various Internet challenges in a single protocol.

In the following sections, we give a review on the Internet security issues, Denial of Services (DoS) attack. After that we discuss various related research topic background such as HIP and SSL as security protocol and also thr Intrusion Detection System (IDS). Then the next section will explain about the proposed scenarios. Finally, we analyze and conclude the obtained results from several scenarios.

1.1. Host Identity Protocols

Host Identity Protocol (HIP) is a protocol that has been proposed by Internet Engineering Task Force (IETF) since 1999. The first implementations of HIP with stable version starts in the year 2007. The original ideas for HIP architecture grew from the desire to provide a means for providing better support for security and mobility within the IP architecture. The main principal of HIP is the enhancement of the original Internet architecture by adding a name spaces between IP layers and transport protocol. This new name space consists of the cryptographic identifier and locator split.

With improvement on the architectural aspect, HIP can deliver solution for several Internet issues such as mobility, multi-homing, and also end-to-end security. The implementation of cryptographic identifiers will enhance the accountability of HIP. With those implementation HIP can enhance the privacy, good location anonymity, and assuring strong identities [12].

HIP Architecture implements identifier and locator split that different with existing TCP/IP protocol. In the existing Internet, each host has an IP address that have two functions; it acts both as locator to describe current topological location in the network, and as a host identifier to describe the identity of the host. On the other side the HIP separates the locator and identifier roles of the IP address by introducing a new name space, the Host Identity (HI) name space. Host identity is a public cryptographic key from a public-private key pair. The public key can be access by any parties, but the private key only accessible by its owner.

HIP can provide more accountable connection compared to TCP/IP protocol. As shown in Figure 1 the TCP/IP before connection established, there is mechanism packet base-exchange called three-way hand shake. The HIP mechanism of the base-exchange before connection established is slightly different. During the connection initialization between the two HIP hosts there is a four-way handshake. During the exchange, the hosts identify each other uses public key cryptography. In this base-exchange the hosts negotiate with the cryptography protocols to use to protect the signaling and the data massages. Basically in HIP one more step is needed for the base-exchange because of the verification process between two hosts. By this kind of mechanism HIP will provide a better accountable connection for the Internet users.

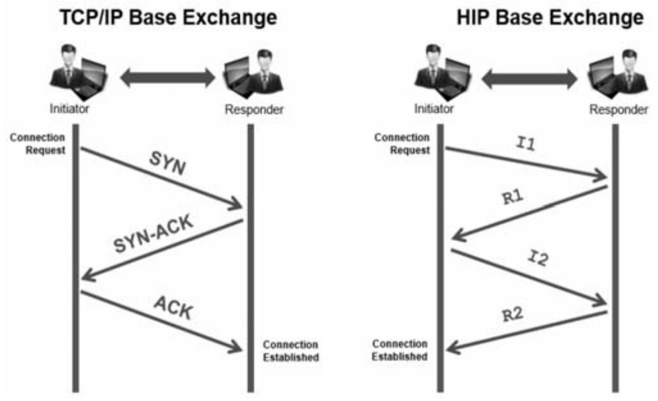

Figure 1. Comparison of HIP and TCP/IP Base Exchange

HIP Base Exchange consists of four messages, two messages from initiator host (I1 and I2) and two messages from responder host (R1 and R2). The I1 message is a trigger messages can be consist of initiator and responder HIT. It is possible to use NULL message in I1. The next message R1 responder already know initiator HIT so in R1 responder will encrypt the messages by using HIT from initiator. After that, initiator will prove its true identity by solving R1 message from responder using its private key. Then initiator will send message I2 to responder encrypted using responder HIT. As a final Base Exchange responder will send R2 to initiator indicate if the connection will start soon.

HIP using the 128-bit public key as Host Identity Tag (HIT). HIT looks like an IPv6 address with the special 28-bit prefix 2001:0010::/28, called Orchid. The next part is 100 bits taken from a cryptographic hash of the public key. From the protocol side, HIP consists of a control protocol, a number of extensions to the control protocol, and any number of data protocols. By default, the HIP control protocol is carried directly in IPv4 and IPv6 packets, without any intervening TCP or UDP header.

The architectural enhancement implemented by HIP has profound consequences. A number of the previously hard networking problems become suddenly much easier. Mobility, multi homing, and baseline end-to-end security integrate neatly into the new architecture. The use of cryptographic identifiers allows enhanced accountability, thereby providing a base for easier buildup of trust. With privacy enhancements, HIP allows good location anonymity, assuring strong identity only towards relevant trusted parties. Finally, the HIP protocols have been carefully designed to take middle boxes into account, providing for overlay networks and enterprise deployment concerns.

From the protocol point of view, HIP consists of a control protocol, a number of extensions to the control protocol, and any number of data protocols. The control protocol consists of the base-exchange, any number of status update packets (that are typically used to convey extension protocols), and a three message termination handshake that allows the peer hosts to cleanly terminate a protocol run.

From an architectural point of view, the HIP architecture has been designed to restore the classical inter-networking invariants, allowing hosts to use communication environment with IPv4, IPv6, NATs, and other middle boxes. HIP provides built-in, architected support for mobility, multi-homing (including multi-access), and baseline security. It enhances the IP architecture by introducing a Host Identity (HI) name space roughly between the IP layer and the transport protocols.

Beside the basic advantage of integrated mobility, multi-homing, and security support, HIP provides for a number of potential architectural extensions. The inherent delegation capability can be used to implement sub network level mobility and multi-homing, as well as delegable application names. The architecture allows control traffic to be easily separated from data traffic, providing for enhanced protection against unwanted traffic [12].

1.2. Secure Socket Layer

Secure socket layer (SSL) is the most popular protocol used in the Internet for facilitating secure communications [13]. Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client typically a web server (website) and a browser; or a mail server and a mail client. SSL allows sensitive information such as credit card numbers and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is in a plain text and vulnerable to eavesdropping. If an attacker is able to intercept all the data being sent between a browser and a web server they can see and use that information. More specifically, SSL is a security protocol. Protocols describe how algorithms should be used; in this case, the SSL protocol determines variables of the encryption for both the link and the data being transmitted.

When SSL work on a communication between client and server, client uses web browser to connect to a website server that is secured with SSL. Then browser will ask to the web server to identify itself. Server will send to the browser a copy of its SSL certificate. On the next step browser will check whether it trusts the SSL certificate. If so the browser will send a message to the server. The server then sends back a digitally signed acknowledgement to start an SSL encrypted session. After that the secure communication through encrypted data will begin between browser (client) and server.

HTTPS stands for Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL. This is the secure version of the Hyper Text Transfer Protocol (HTTP). When the website information that received or sent is important we use this protocol. For example we use this protocol when we make a payment or sent sensitive personal information. The information in this protocol will be encrypted using 128 bit encryption and cannot be read by any party when transmitted from our computer to our servers. There are two primary differences between HTTPS and HTTP. HTTPS connects on port 443, while HTTP is on port 80. HTTPS encrypts the data sent and received with SSL, while HTTP sends it all as plain text.

Popular services such as social media and mail services are increasingly migrating to SSL to improve security and address privacy concerns. As more transactions and services are protected by SSL, DDoS attacks on SSL secured services are on the rise and are justifiably getting more attention. Some of these attacks are actually standard flood and TCP connection based attacks that have been used for years to disrupt both secured and clear text services. There are also attacks targeting SSL itself [14].

There are numerous known and potential attacks which exploit the SSL handshake to exhaust server resources. The Pushdo botnet accomplishes this quite easily by sending garbage data to a target SSL server. The SSL protocol is computationally expensive and it generates extra workload on the server to process garbage data as a legitimate handshake. Firewalls don’t help in this case because the clients have completed the TCP handshake and are sending traffic to an allowed service [15].Based on those fact SSL as secure protocol that provide cryptography still cannot resolve DoS attack. Solution that presented by Arbor Network [14] to solve DoS on SSL still need to use multiple levels technique that will use more resources.

2. Internet Security Issues

Recently the Internet Security became the main popular issue worldwide. Many cases related to Internet security occurs every day. The number of cyber security threats increase every year [16]. There are many kinds of Internet security threats i.e. hacktivism, vulnerabilities, malware and spam. Most of the threats remain unresolved by current Internet technologies.

One of the popular Internet security threats is the Denial of Services (DoS). DoS can be defined as an action that prevent the network element from functioning in accordance with its intended purpose. The network element may be rendered partially or entirely unusable for legitimate user. The Denial of Services may cause operations which depend on timelines to be delayed. When there are a lot of DoS attackers and their location were distributed, it could become Distributed Denial of Services (DDoS).

Latest security incident trend statistics [17-19], currently showing an increase in denial of service (DoS) attacks.This kind of attack still has high possibility to occur in the current Internet architecture due to lack of accountability. In the current Internet, user can falsify their identity and the packet using spoofing technique. There is no accurate host verification in the existing TCP/IP protocol [20]. Moreover the Internet architecture has no fundamental ability to associate an action with the responsible entity. Real-world security depends on accountability and the same applies to the Internet. Spoofing the source IP address of packets on the internet is one of the major tools used by hackers to launch DDoS attacks. In such attacks, the attackers forge the source IP of packets that are used in the attack by using an arbitrary IP address which is selected either randomly or intentionally [21].

Denial of Service attacks overwhelm a target with either too many connection requests or too much bandwidth. The intended result is to make the target inaccessible, although other infrastructure elements (routers, switches, load balancers, etc.) may suffer collateral damage along the path of an attack. A variety of attack types, including connection floods, TCP SYN floods, ICMP and UDP floods may be used in such an attack [22]. DoS is a threat that potentially violates the availability of a resource in a system [23]. Denial of service attacks come in a variety of forms and aim at a variety of services. CERT Coordination Center defines three basic types of attacks: consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, and physical destruction or alteration of network components [22].

The different types of denial of service attacks can be broadly classified into vulnerability attacks (also called semantic attacks) and flooding attacks (also called brute-force attacks). A DoS vulnerability attack exploits one or more flaws in a policy or in the mechanism that enforces the policy, or a bug in the software that implements the target system, and aims to consume excessive amount of resources of the target by sending it a few carefully crafted requests. A DoS brute-force attack, on the other hand, aims to deny service to legitimate users of a service by invoking vast amount of seemingly valid service requests and trying to exhaust a key resource of the target. Currently the Internet Security issues was not only related to technology, there are many aspect that related with this issue, such as political intention. We can found the number of cyber hacktivism which organiz targeted attack to the government website as a protest for government policy [3, 25].

3. Research Method

In this research to obtain information regarding performance of each tested protocols we use response time measurement for every tested condition and also gain information regarding service availability. To conduct the test we use computer with specification ProcessorCore i7 2.2 GHz, 8 GB RAM, and using Windows 7 64bit Operating System. On single machine we implement virtualization using VMWare workstation. Inside virtual machine this scenario uses Ubuntu 12.10. All virtual machine allocated with similar setting 2 GB RAM. There are several virtual machines in this scenario: non-HIP client, non-HIP server, HIP client, HIP server, and one machine will perform DoS attack. The virtual machine in this scenario connected with virtual network to communicate each other’s. For every test at least we use two virtual machine as client and as server. There are three test in our implementation, first test would like to measure base performance of HIP and TCP/IP without DoS, second we would like to measure performance of TCP/IP, SSL, and HIP to deal with DoS attack, and the third we observe service availability during high intensity of DoS attack.

Before conduct test performace of the protocols on DoS attack simulation, first we compare the base performace for TCP/IP and HIP using base response time. To obtain response time we send ICMP packet for both protocols. This test conducted on same condition of hardware specification for server and client. The first test ICMP will run over TCP/IP protocol and another test ICMP will run over HIP protocol. For HIP test both client and server are set to implement HIP protocol by using Host Identity Protocol For Linux (HIPL) [26]. Every test will send 100 ICMP packets, then we collect data based on average response time for every 100 ICMP packets. We repeat measurement of response time 20 times to get average response time of TCP/IP and HIP.

Second test would like evaluate the performace of selected protocols TCP, SSL and HIP to deal several DoS attack scenarios. In this test we add SSL as new protocol variable because recently SSL known as most popular secure protocol [27]. We compare performance of the protocols based on response time on various DoS attack condition. To generate DoS attack we use ostinato traffic generator. Using ostinato we generate variation of DoS attack: ICMP flood, TCP sync flood, and UDP flood with different port target. We use Ostinato because compared to another traffic generator, Ostinato is easy to use with common GUI and have better performace to generate TCP Sync [28].

The third scenarios we would like to test targeted protocols and implement HIP with firewall. This HIP firewall will be perform as access control firewall. HIP firewall will classify between HIP and non-HIP packet. The scenario shows in Figure 2.

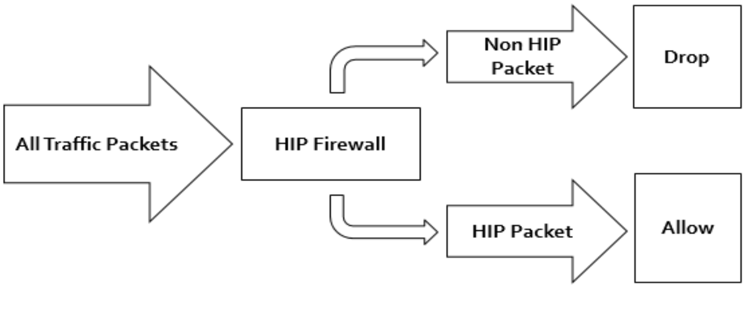

Figure 2. HIP Firewall

After the firewall classify HIP and non-HIP packet, in this scenario non-HIP packet will be dropped while HIP packet will be accept. The next step the system will perform authorization for user who ask for access. Authorization will be conduct based on listed Host Identity Tag (HIT). The users who do not have same HIT with listed HIT will be block, while the users who have HIT on the list will be authorized for further access.

To evaluate performance of proposed firewall, this proposed HIP firewall will be tested on different DoS attack intensity as well as on TCP/IP and SSL protocol. From the DoS test we would like to know the service availability for every scenarios. To know service availability we run web server service on the server side. This server will run in different scenarios and targeted as victim of DoS attack with variation of attack intensity.

4. Performance Evaluation

In this part we would like to present result of comparison performance of HIP and TCP/IP as a basic protocol. The first experiment compares base response time between HIP and TCP/IP by using 100 ping of ICMP packets. Figure 3 shows comparation 20 response time of the HIP and TCP/IP during zero attack condition, without any DoS attack. From the graphic compared to TCP/IP, HIP has longger response time. Average response time on the TCP/IP was 98,627 ms while the HIP response time was 99,711 ms. According to the first scenario TCP/IP has a better response time compared to HIP. This happens because by default the connection establishment of HIP are more complex compared to TCP/IP.

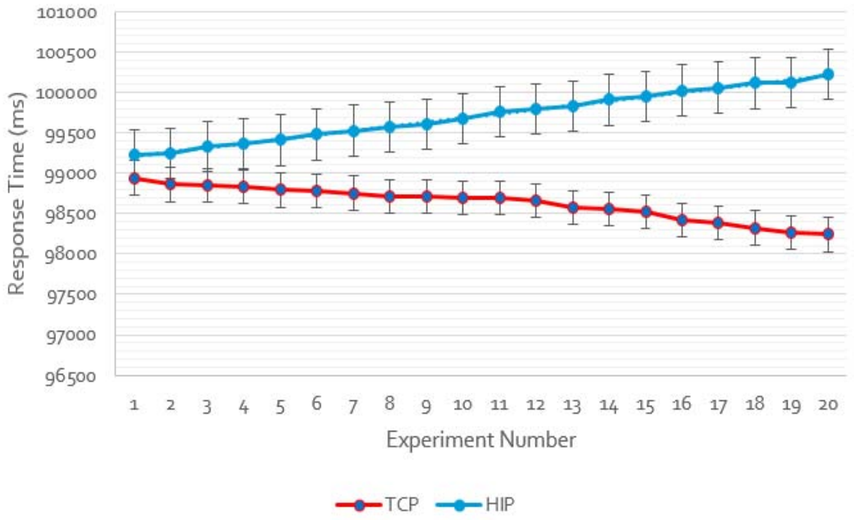

Figure 3. ICMP response time comparison HIP and TCP/IP

In the second scenario we would like to compare the HIP, TCP/IP, and SSL in a low to medium DoS attack intensity. The DoS attack vary between 0 to one million packets per second. There are three types of attack will be tested: TCP Sync flood attack, UDP targeted Port 10500 flood attack, and UDP targeted Port 110 flood attack. TCP sync flood attack and UDP Port 110 flood were chosen because both of them are common DoS attack. While UDP Port 10500 was chosen because Port 10500 used by HIP. During the variation of attack occurs this scenario will measure the connection time to the server. To measure connection time to the server we use httperf application.

From the second scenario in the condition of DoS attack all protocols are still stable under 10,000 DoS packets per second. When the number of attack is more than 10,000, the connection time in all protocols were increased. Figures 4, 5, 6 shows the comparison graphic for each of the scenario. According to the graphic the order of the performance from the best to the worst in the condition of low to medium DoS attack are TCP/IP, HIP, and the last SSL.

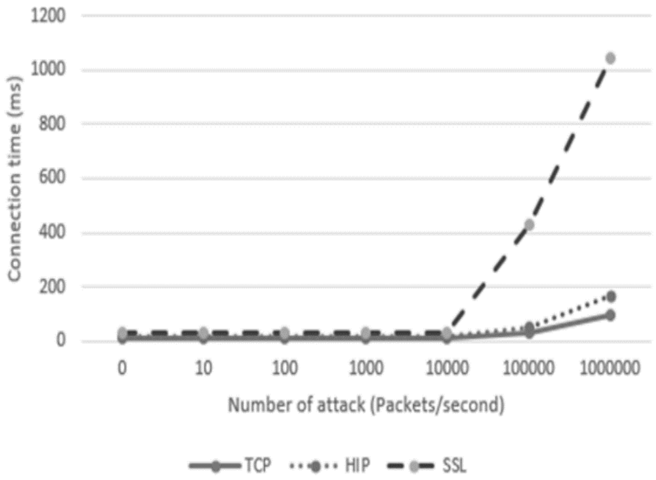

Figure 4. Connection time during TCP Sync flood attack

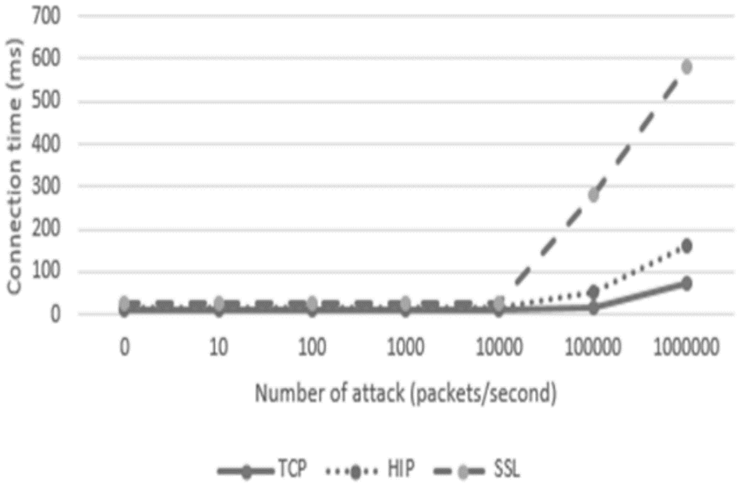

Figure 5. Connection time during UDP targeted port 10500 flood attack

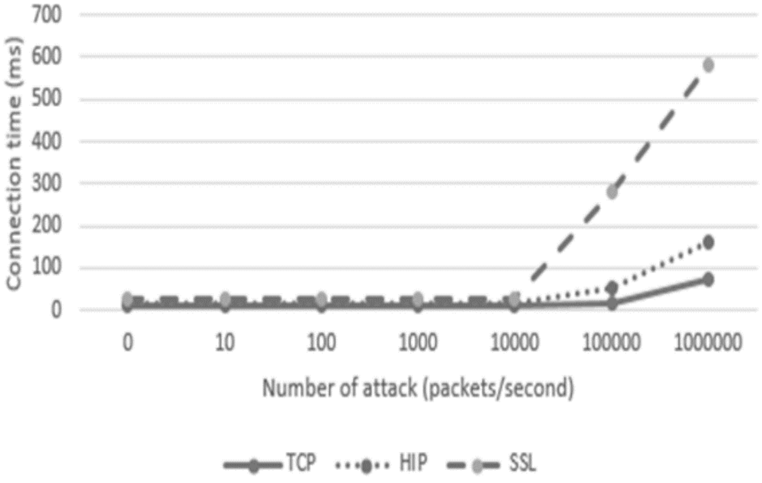

Figure 6. Connection time during UDP targeted port 110 flood attack

On the third scenario we compare performance every protocols (TCP/IP, SSL, and HIP) and HIP Firewall with authorization. All of the protocols tested regarding service availability as web server on difference DoS attack intensity (Low, Medium, and High). From the test we got following result:

Table 1. Comparison service availability

Protocol	DoS Attack Intensity		
Scenarios	Low	Medium	High
TCP/IP	V	V	X
SSL	V	V	X
HIP	V	V	X
HIP + HIP Firewall + HIT Authorization	V	V	V

V = Service available (can access web page)
X = Service not available (cannot access web page)

According to the experiment result, all of the protocol still can provide service in the condition low until medium DoS attack. But in the condition of high DoS attack, only HIP Firewall can survive. This is happen because HIP Firewall will block all non-HIP packet, then among HIP packet will be filtered again on authorization process. Authorization will allow registered HIT only to run over the HIP.

5. Conclusion

From this work we can obtain performance comparison of HIP and TCP/IP. In the normal condition without any DoS attack response time for 100 ICMP packets of HIP was 99,711 ms while TCP/IP 98,627 ms. In the low to medium DoS attack the order of the protocol from the best performance are TCP/IP, HIP, and SSL. According to this information HIP has better performance in the condition low to medium DoS attack compared with SSL. On the condition of high intensity DoS attack all of the protocol TCP/IP, SSL, and HIP cannot work. To against this kind of attack, we implement enhancement of HIP protocol using HIP firewall with HIT authorization. According to the experiment enhancement implementation of HIP was succesfully work to avoid high intensity DoS attack.

From this experiment we can say that the default HIP cannot overcome DoS when work alongside with another types of protocol. This is because of the existence of another packets beside HIP packet. HIP can work to encounter DoS when this protocol implement the additional function. According to this fact, HIP cannot give best performance in today's Internet condition. In existing Internet all trafficsare mixed with various packet types. HIP can work best if this protocol is implemented a stand alone protocol on the Internet.

References

[1] S Shenkers, et al. Foundamental Design Issues for the Future Internet. *Selected Area in Communication IEEE Journal*. 1995.
[2] J Mirkovic et al. Building accountability into the future Internet. *4th Workshop on Secure Network Protocols, NPSec*. 2008.
[3] Y Oh, T Obi. Identifying Phishing Threat in Government Web Services. *International Journal of Information and Network Security (IJINS)*. 2013; 23-42.
[4] C Marco, et al. Research ChallengesToward the Future Internet. *Elsevier Computer and Communication*. 2011.
[5] Keromytis AD, et al. Implementing IPsec. *IEEE Global Telecommunications Conference*. 1997.
[6] DG Andersen, et al. Accountable Internet Protocol (AIP). *SIGCOMM*. 2008.
[7] CE Perkins. Mobile networking through Mobile IP. *IEEE Internet Computing.* 1998; 2(1).
[8] L Yanyan et al. Prospect for the Future Internet A Study Based on TCP/IP Vulnerabilities. *International Conference on Computing, Measurement, Control and Sensor Network*. 2012.
[9] R Moskowitz et al. Host Identity Protocol. *IETF RFC 5201.http://tools.ietf.org/html/rfc5201*. 2008.
[10] R. Moskowitz et al. Prospect for the Future Internet A Study Based on TCP/IP Vulnerabilities. *International Conference on Computing, Measurement, Control and Sensor Network*. 2012.
[11] T. Leva et al. Adoption Barriers of Network Layer Protocols: The Case of Host Identity Protocol.*Computer Network Journal Elsavier*. 2013.

[12] P Nikander et al. Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks.*IEEE Communication Surveys and Tutorials. Second Quarter* 2010; 12(2): 186202.

[13] H, Otrok et al. Improving the Secure Socket Layer Protocol by modifying its Authentication function. *World Automation Congress*. 2006; 1-6.

[14] J, Lewis. DDoS Attacks on SSL: Something Old, Something New. DDoS and SecurityReports http://www.arbornetworks.com/asert/2012/04/ddos-attacks-on-ssl-something-oldsomething-new/. 2012.

[15] J Larimer. Pushdo SSL DDoS Attacks.*IBM Internet Security System*. http://www.iss.net/threats/pushdoSSLDDoS.html. 2010.

[16] Symatec. Internet Security Threat Report 2014.*Symatec Internet Security Threat Report.* 2014*;* 19.

[17] NSFOCUS Ltd. Mid-Year DDoS Threat Report 2013. *Technical Report 2013-07*. Beijing: NSFOCUSLtd; 2013.

[18] Prolexic Ltd. Prolexic Quarterly Global DDoS Attack Report. *Technical Report 2013-07*. Hollywood: Prolexic Ltd; 2013.

[19] Radware Inc. Global Application and Network Security Report. Technical Report 2013-01.Mahwah: Radware Inc.; 2013.

[20] NE Heastings et al. TCP/IP Spoofing Foundamentals.*IEEE Fifteenth Annual InternationalPhoenix Conference on Computers and Communication*. 1996.

[21] Yunji Ma. An Effective Method for Defense against IP Spoofing Attack.*6th InternationalConference Wireless Communications Networking and Mobile Computing (WiCOM)*. 2010.

[22] M. Abliz. Internet Denial of Service Attacks and Defense Mechanisms.*University of Pittsburgh Technical Report*, No. TR-11-178. 2011.

[23] H, Waguih. A Data Mining Approach for the Detection of Denial of Service Attack. *International Journal of Artificial Intelligence*. 2013: 99-106.

[24] CERT. Denial of Service Attacks. http://www.cert.org/historical/tech?tips/denial?of?service.cfm.

[25] M Wazid, et al. Hacktivism trends, digital forensic tools and challenges: A survey.*IEEEConference on Information and Communication Technologies (ICT).* 2013.

[26] A Pathak et al. Host identity protocol for Linux. *Linux Journal.* 2009: 187(5).

[27] Kant K et al. Architectural Impact of Secure Socket Layer on Internet Servers*. IEEE 30thInternational Conference on Computer Design (ICCD)*. 2012; 27-34.

[28] S Srivastava et al. Comparative Study of Various Traffic Generator Tools.*Recent Advancein Engineering and Computational Sciences (RAECS)*. 2014; 1-6.