Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

Security Network with Virtual Private Network & (IPSec) Applications

Dhari Kh Abedula Ahmed A. Sabeeh

***Abstract*—Internet communication is largely based on TCP/IP protocols. The main design of TCP/IP is for trusted peers to communicate. IP Packets have no inherent security, and therefore it is relatively easy to forge the addresses of IP packets, modify the contents of IP packets, replay old packets, and inspect the contents of IP packets in transit. In this paper, we discuss how Internet Protocol Security (IPSec) is used for secured and encrypted communication between Internet hosts. IPSec is described as an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite[1]. According to Kent *et al.*, it can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). To discuss the use of IPSec in an TCP/IP based network, we chose Virtual Private Network (VPN) as the application in describing how IPSec provides the platform for secure and encrypted channel for communication.**

***Index Terms*—TCP/IP Security, IPSec, VPN, IKE, IKE2, AH, SA, ESP**

I. Introduction

Designed by IETF, *IPSec* is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session, provides secure connections between private networks across wide area network (WAN) or Internet using IPSec tunnels, the virtual connections is also named as VPN (Virtual Private Network). IPSec protects IP datagrams by defining a method of specifying the traffic to protect, how that traffic is to be protected, and to whom the traffic is sent[2].

IPSec can protect packets between hosts, between network security gateways (e.g., routers or firewalls), or between hosts and security gateways. Since an IPSec-protected datagram is, itself, just another IP packet, it is possible to nest security services and provide, for example, end-to-end authentication between hosts and send that IPSec protected data through a tunnel which is, itself, protected by security gateways using IPSec. IPSec also defines IP packet formats and related infrastructure to provide strong authentication, integrity, and (optionally) confidentiality for network traffic. IPSec runs over the current version of IP, IPv4, and also the next generation of IP, IPv6[3]. Now it is the security standard of Internet.

A *VPN* is a means of creating secure communications over a public network infrastructure. VPNs use encryption and authentication to ensure information is kept private and confidential. This means data and resources can be shared among several locations without the worry of data integrity being compromised. Alone, the ability to make use of a public network to transmit data is also an advantage of VPN technology. Without using the Internet as a transport mechanism, you would have to purchase point-to-point TLS or some other form of leased line to connect multiple locations, or use frame relay service. Leased lines are traditionally expensive to operate, especially if the two points being connected are across a large geographic region. Using VPNs instead reduces the operating cost for your company.

VPNs provide dramatic flexibility in network design and a reduced total cost of ownership in the WAN. A VPN can be best described as an encrypted tunnel between two computers over an insecure network such as the Internet. VPNs provide secure encrypted channel to secure communication, and cost savings in the ranges of 30 to 80 percent depending on the leased line and the destination. There are various ways to implement VPN services, including at the enterprise edge router, the firewall, or a dedicated VPN appliance. Additionally, MPLS can be provided by the ISP for site-to-site VPN traffic. Another possibility is the virtual private dialup network (VPDN). Primarily used for remote-access connection to an enterprise campus network, this type of VPN combines the traditional dialup network through the PSTN with either Layer 2 Forwarding (L2F) or L2TP. All of these various technologies are available in today's marketplace, but the most popular VPN technology, by far, is the *IPSec VPN*.

II. Description of type attack that can be eliminated using IPSec

A. Denial of service (DOS) attacks

These occur when an entity uses network transmissions to prevent legitimate users from using network resources. For example, an attacker may flood a host with TCP SYN requests and thereby crash a system, or the attack may consist of repeated transmission of long mail messages with the intention of filling up a user's or site's bandwidth with nuisance traffic.

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

B. Spoofing attacks

These occur when an entity transmits packets that misrepresent the packets' origins. For example, one type of spoofing attack occurs when the attacker sends a mail message with the From: header indicating the source of the message as, say, the president of the United States. More insidious and almost as easy to engineer are those attacks that occur when packets are sent out with an incorrect source address in the headers.

C. Man-in-the-middle (MITM) attacks

These occur when an attacker (Alice) positions herself between two communicating entities (call them Bob and Carol) and intercepts all their transmissions. Alice poses as Bob when communicating with Carol, and as Carol when communicating with Bob. Alice, as a result, is able to send whatever data she wants to Bob instead of what Carol wants to send to Bob. MITM attacks are relatively easy when transmissions are not encrypted or authenticated. However, Alice can successfully attack even a protected data stream if she is able to either gain access to Carol's secret keys (or be issued a set of her own public/secret key pairs that is sufficiently similar to Carol's that Bob will be fooled).

III. IPSec VPN

IPSec is composed of a collection of underlying protocols that together provide the overall operation of parameter negotiation, connection establishment, tunnel maintenance, data transmission and connection teardown. Three protocols are used in the IPSec architecture to provide key exchange in addition to the integrity, encryption, authentication and anti-replay[4]:

- *Encapsulating Security Payload (ESP)* provides a framework for the data integrity, encryption, authentication, and anti-replay functions of an IPsec VPN.
- *Authentication Header (AH)* provides a framework for the data integrity, authentication, and anti-replay functions. (No encryption is provided when using AH.)
- *Security Associations (SA)*, IKEv1 or IKEv2 is used by IPsec for the exchange of parameters used for key negotiation, the exchange of the derived authentication/encryption keys, and overall establishment of security associations (SA) , and The Internet Security Association and Key Management Protocol(ISAKMP) provides a framework for authentication and key exchange, with actual authenticated keying material provided either by manual configuration with pre-shared keys, Internet Key Exchange (IKE and IKEv2)

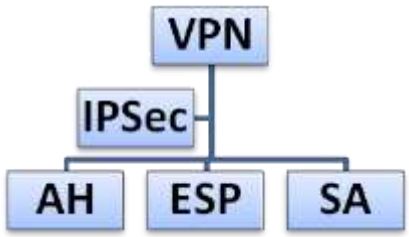

Figure 1: IPSec position in VPN communication

A. Authentication Header (AH)

AH provides authenticity guarantee for transported packets. This is done by check-summing the packages using a cryptographic algorithm. It can operate on both modes, but it is used only on transport mode as tunnel mode for AH protects the same data as transport mode for AH. AH provides data integrity, data source authentication and protection against replays but there is no option for data confidentiality. AH header contains SPI, sequence number and authentication data field The authentication data field contains a digest of the MAC used to secure the data. AH authentication, as below, covers the outer IP header of the packet. As there are IP header fields which change when the packet passes routers, these fields are set to zero before calculating the authentication data field. Other special features, like fragmentation and reassembly are also treated in AH documents. Therefore, the protection in AH covers some of the IP Header even in the transport mode. In tunnel mode of AH, the entire datagram is the protection of an IPSec Header.

The Authentication Header can be used to do the following:

- Provide strong integrity services for IP datagrams, which means the AH can be used to carry content verification data for the IP datagram
- Provide strong authentication for IP datagrams, which means that the AH can be used to link an entity with the contents of the datagram
- Provide non-repudiation for IP datagrams, assuming that a public key digital signature algorithm is used for integrity services
- Protect against replay attacks through the use of the sequence number field

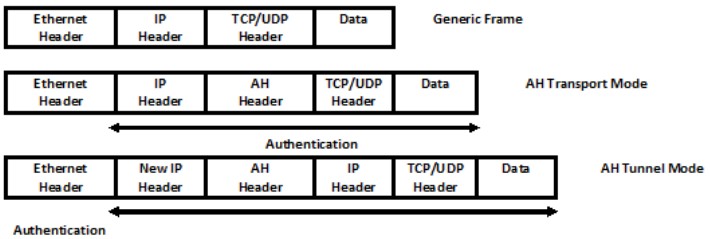

Figure 2:Authentication Header

The Authentication Header can be used in tunnel mode or in transport mode, which means that it can be used to authenticate and protect simple, direct datagram transfers

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

between two nodes, or it can be used to encapsulate an entire stream of datagrams that is sent to or from a security gateway.

In transport mode, the Authentication Header protects the payload of the original IP datagram as well as the parts of the IP Header that do not change from hop to hop (e.g., the Hop Limit field or Routing Headers). Figure 3 shows what happens to a transport-mode IP datagram as the Authentication Header is calculated and added to it (the Destination Options Header may also appear before the Authentication Header). The destination IP address and extension headers are protected only insofar as they do not change from hop to hop.

When the Authentication Header is used in tunnel mode, however, it is used differently. The original destination IP address, along with the entire original IP datagram, is encapsulated into an entirely new IP datagram that is sent to the security gateway. Thus, the entire original IP datagram is fully protected, as are the portions of the encapsulating IP Headers that don't change.

As originally defined, the Authentication Header consisted of 64 bits of header, with the rest devoted to authentication data (see the following). Thus, the payload length field merely indicated the length (in 32-bit words) of the authentication data. With the addition of the Sequence Number field (see the following), this value now equals the length of the authentication data plus the length of the Sequence Number field. AH header fields include the following:

- Payload length: This 8-bit field indicates the entire length of the Authentication Header in units of 32-bit words, minus 2.
- Reserved: The next 16 bits are reserved for future use; at present, they must be set to all zeros.
- Security Parameter Index (SPI): This 32-bit value is an arbitrary number. Together with the destination IP address and security protocol (in this case, AH to indicate the Authentication Header), the SPI uniquely identifies the security association to be used for the Authentication Header. An SPI value of zero is for local use only and should never be transmitted; values from 1 through 255 are reserved by the Internet Assigned Numbers Authority (IANA) for future use.
- Sequence Number: This 32-bit value is a mandatory counter; it is also included by the sender, although it may not always be used by the recipient. Starting from zero, this counter is incremented with every datagram sent and is used to prevent replay attacks. When the recipient is using it for anti-replay purposes, it will discard any datagrams that duplicate a sequence number that has already been received. This means that when the counter is ready to cycle through (when 232 datagrams have been received), a new security association must be negotiated--otherwise, the receiving system will discard all datagrams once the counter is reset.
- Authentication Data: This field contains the Integrity Check Value (ICV), which is the heart of the Authentication Header. The contents must be a multiple of 32 bits in length and may contain padding to attain that length. Calculation of this value is discussed in the next section.

B. Encapsulating Security Payload (ESP)

Encapsulating Security Payload (ESP) is a key protocol in the IPsec (Internet Security) architecture, which is designed to provide a mix of security services in IPv4 and IPv6. The IP Encapsulating Security Payload (ESP) seeks to provide confidentiality and integrity by encrypting data to be protected and placing the encrypted data in the data portion of the IP ESP. Depending on the user's security requirements, this mechanism may be used to encrypt either a transport-layer segment (e.g., TCP, UDP, ICMP, IGMP) or an entire IP datagram. Encapsulating the protected data is necessary to provide confidentiality for the entire original datagram.

The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). The Internet Assigned Numbers Authority has assigned Protocol Number 50 to ESP. The header immediately preceding an ESP header will always contain the value 50 in its Next Header (IPv6) or Protocol (IPv4) field. ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes both the protected ESP header fields and the protected user data, which is either an entire IP datagram or an upper-layer protocol frame (e.g., TCP or UDP).

The ESP Header can be used in conjunction with an Authentication Header. In fact, unless the ESP Header uses some mechanism for authentication, it is recommended that the Authentication Header be used with the ESP Header.

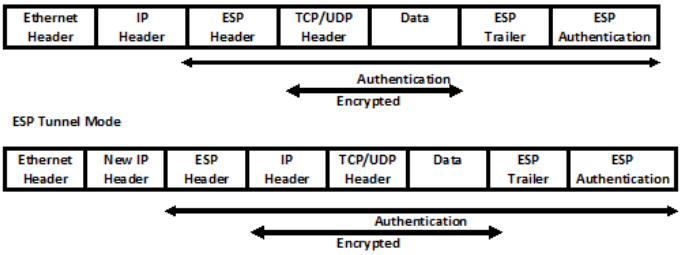

Figure 3: ESP Header

The ESP Header must follow any headers that need to be processed by nodes intermediate to the destination node. All data that follows the ESP Header will be encrypted, with the encrypted payload beginning directly after the last ESP Header field.

In transport mode, the IP Header and any Hop-by-Hop, Routing, or Fragmentation Extension Headers precede the Authentication Header (if present), followed by the ESP

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

Header. Any Destination Options Headers can either precede or follow the ESP Header, or even both any Headers that follow the ESP Header are encrypted.

The result appears in many respects, to simply be a regular IP datagram transmitted from source to destination, with an encrypted payload. This use of ESP in transport mode is appropriate in some cases, but it allows attackers to study traffic between the two nodes, noting which nodes are communicating, how much data they exchange, when they exchange it, and so forth. All this information may potentially provide the attacker with some information that helps defeat the communicating parties.

An alternative is to use a security gateway, much as just described for the Authentication Header. A security gateway can operate directly with a node or can link to another security gateway. A single node can use ESP in tunnel mode by encrypting all outbound packets and encapsulating them in a separate stream of IP datagrams that are sent to the security gateway. That gateway then can decrypt the traffic and resend the original datagrams to their destinations.

ESP also has weaknesses within itself, not just when compared to AH. RFC 2406 requires the use of Initialization Vectors in certain situations if the algorithm used to encrypt the payload requires cryptographic synchronization data, example an Initialization Vector (IV) must indicate the length, any structure for such data, and the location of the data as part of an RFC specifying how the algorithm is used with ESP[1][5]. This means that the IV is included in the ciphertext of every packet to allow the receiver to decrypt individual packets regardless of packet loss or reordering of packets.

Nuopponen and Vaarala[6]show that if “initialization vectors are chosen in a predictable manner in ESP, an adaptive chosen plaintext vulnerability opens up.” An attacker can break low entropy plaintext blocks using brute force[7], as well as verifying strongly suspected plaintext[8]. While these attacks are difficult, they are possible in restricted situations. There also exists a conflict between ESP and TCP performance enhancement proxy (PEP) deployed in IP wireless networks. “It is impossible for an intermediate gateway outside sender or receiver’s security enclaves to analyze an IPsec header to extract TCP flow identification and sequence number. The PEP agent cannot obtain the information needed to generate acknowledgments or retransmit data segments.”[8] Zhang argues that IPsec’s tunnel mode and layering principles are unsuitable for new networking services and applications such as Traffic Engineering, Traffic Analysis Application –Layer Proxies/Agents and Active Networks.

In situations such as this, secure socket layer (SSL) or transport layer security (TLS) can provide the necessary data security. SSL/TLS operate at the Transport layer of the OSI model, and only encrypt the TCP data not the TCP header. This allows intermediate devices to view and use the TCP state information. In this aspect, SSL/TLS are a rival for IPsec, but only where TCP is concerned. SSL/TLS does not work on UDP, ICMP or other Transport layer IP protocols.

ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association establishment and on the placement of the implementation. Confidentiality may be selected independent of all other services. However, use of confidentiality without integrity/authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service. Data origin authentication and connectionless integrity are joint services and are offered as an option in conjunction with (optional) confidentiality. The anti-replay service may be selected only if data origin authentication is selected, and its election is solely at the discretion of the receiver.

In some instance of virtual private network (VPN) implementation, emphasis is placed on the virtual aspect. Strayer[9] argues that MPLS-based VPNs, using traffic engineering and resource management (QoS), provides a dedicated private network. This private network is only illusionary because MPLS does not take into account confidentiality, which ESP provides for IPsec based VPNs. Without the use of encryption, attackers can sniff a network and obtain potentially damaging information. Also, MPLS does not work well outside of an Autonomous Systems (AS), as Strayer points out. This makes MPLS practically useless between partner corporations where IPsec, with tunnel mode, can provide the required security. Most of ESP’s strengths against other secure data transit technologies lie within IPsec’s strength as a superior method to provide secure data transfer over unsecured networks.

C. Security Associations

The Security Association (SA) is a fundamental element of IPsec. RFC 2401 defines the SA as "a simplex 'connection' that affords security services to the traffic carried by it." This rather murky definition is clarified by a description; an SA consists of three things:

- A Security Parameter Index (SPI)
- An IP destination address
- A security protocol (AH or ESP) identifier

As a simplex connection, the SA associates a single destination with the SPI; thus, for typical IP traffic there will be two SAs: one in each direction that secure traffic flows (one each for source and destination host). SAs provide security services by using either AH or ESP but not both (if a traffic stream uses both AH and ESP, it has two---or more---SAs). The Security Parameter Index (SPI) is an identifier indicating the type of IP header the security association is being used for (AH or ESP)[10].The SPI is a 32-bit value identifying the SA and differentiating it from other Sas linked

Proc. of the Intl. Conf. on Advances in Computer Science and Electronics Engineering -- CSEE 2014

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

to the same destination address. For secure communication between two systems, there would be two different security associations, one for each destination address. Each security association includes more information related to the type of security negotiated for that connection, so systems must keep track of their SAs and what type of encryption or authentication algorithms, key lengths, and key lifetimes have been negotiated with the SA destination hosts.

Internet Security Association and Key Management Protocol (ISAKMP)

ISAKMP takes care of parameter negotiation between peers (for example, DH groups, lifetimes, encryption [if required], and authentication)[10]. The process of negotiating these parameters between peers is required for the successful establishment of SAs. After an SA has been established, ISAKMP defines the procedures followed for correct maintenance and removal of the SA during connection termination.

Oakley

Oakley provides the key-exchange function between peers using the DH protocol. DH is an asynchronous protocol, meaning each peer uses its own set of keys for communications establishment and operation between peers. However, the keys are never exchanged, providing a much higher level of security than synchronous protocols (DES, 3DES, and so on) that require both peers to use the same keys for operation. After both peers have established their shared communication path, they can proceed to exchange the keys used by the various synchronous protocols for authentication and encryption purposes.

IKEv1

IKEv1 provides a framework for the parameter negotiation and key exchange between VPN peers for the correct establishment of an SA. However, the actual processes of key exchange and parameter negotiation are carried out by two protocols used by IKEv1[11]:

IKEv1 Phase 1: During this phase, both peers negotiate parameters (integrity and encryption algorithms, authentication methods) to set up a secure and authenticated tunnel. This is also called a management channel because no user data is flowing through it (and it is actually a bidirectional IKE SA)[10]. Its sole scope is to handle secure Phase 2 negotiations. It is called bidirectional because both peers use only one session key to secure both incoming and outgoing traffic. Peer authentication can be carried out by one of the following methods:

- Pre-shared keys
- Digital certificates

IKEv1 Phase 2: This second mandatory phase uses the negotiated parameters in Phase 1 for secure IPsec SA creation. However, unlike the single bidirectional SA created within Phase 1, the IPsec SAs are unidirectional, meaning a different session key is used for each direction (one for inbound, or decrypted, traffic, and one for outbound, or encrypted, traffic). This is applicable for any administrator-configured source-destination network pair. Therefore, you might end up with four unidirectional IPsec SAs if you have two source-destination network pairs defined in a VPN policy. (IPsec VPN policy configuration is discussed in later chapters.)IKEv1 uses either IKEv1 Main mode or IKEv1 Aggressive mode in Phase 1 to carry out the actions required to build a bidirectional tunnel. It then uses IKEv1 Quick mode for Phase 2 operations.IKEv1 Main mode (Phase 1) uses three pairs of messages(making six in total) between peers:

Pair 1 consists of the IKEv1 security policies configured on the device: One peer (initiator) begins by sending one or more IKEv1 policies, and the receiving peer responds (responder) with its choice from the policies.

Pair 2 includes DH public key exchange: DH creates shared secret keys using the agreed upon DH group/algorithm exchanged in pair 1 and encrypts nonces (a randomly generated number) that begin life by first being exchanged between peers. They are then encrypted by the receiving peer and sent back to the sender and decrypted using the generated keys[11].

Pair 3 is used for ISAKMP authentication: Each peer is authenticated and their identity validated by the other using pre-shared keys or digital certificates[12]. These packets and all others exchanged from now on during the negotiations are encrypted and authenticated using the policies exchanged and agreed upon in pair 2. IKEv1 Aggressive mode (Phase 1) uses just three messages rather than the six used with Main mode. The same information is exchanged between peers. However, the process is abbreviated by carrying out the following actions:

- The initiator sends DH groups signed nonces (randomly generated numbers), identity information, IKEv1 policies, and so on.
  - The responder authenticates the packet and sends back accepted IKEv1 policies, nonces, key material, and an identification hash that are required to complete the exchange.
- The initiator authenticates the responder's packet and sends the authentication hash.

ISBN: 978-1-63248-000-2 doi: 10.15224/ 978-1-63248-000-2-33

During IKEv1 Quick mode (Phase 2), IKEv1 transform sets (a list of encryption and hashing protocols) used for IPsec policy negotiation and unidirectional SA creation are exchanged between peers. Regardless of the parameters/attributes selected within a transform set, the same five pieces of information are always sent:

- IPsec encryption algorithm (DES, 3DES, AES)
- IPsec authentication algorithm (MD5, SHA-1)
- IPsec protocol (AH or ESP)
- IPsec SA lifetime (seconds or kilobytes)
- IPsec mode (Tunnel, Transport)

An optional *Extended Authentication (XAUTH)* phase can also take place after successful Phase 1 SA creation. XAUTH carries out the process of end host/device authentication before a user can use the VPN connection. Be careful not to confuse this optional step with the peer authentication carried out within IKEv1 Phase 1[10]. The difference is IKEv1 Phase 1 carries out the authentication of the VPN peers used to terminate each end of the SA, whereas XAUTH is used for the authentication of users or devices that will be transmitting and receiving data across the established VPN tunnel. This phase can occur in remote-access or Easy VPN scenarios, but not in site-to-site VPNs. XAUTH authentication can be achieved by using either of the following:

- Static username and passwords
- One-time passwords (OTP)

IV. Conclusion

The encryption and message authentication services provided by IPsec[12], however, require significant computation time. Consequently, IPsec can degrade performance when compared to unsecured transmissions which is one of the obstacles before the wide application of IPSec VPN[13]. IPsec (Internet Protocol Security) provides a method of authentication and encryption for each IP packet of a communications session. IPSec leverages protocols such as AH (Authentication Header) for integrity and authentication; ESP (Encapsulating Security Payload) for confidentiality, authentication, integrity, and anti-replay; and ISAKMP (Internet Security Association and Key Management Protocol) for a framework for authentication and key exchange.

REFERENCES

[1] S. A. Kent, R. , "IP Encapsulating Security Payload (ESP)," *IETF. RFC 2406*, 1998.

[2] D. H. Naganand Doraswamy, "IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks," *Prentice Hall PTR*, March 13 2003.

[3] N.Dunbar, "IPsec Networking Standards - An Overview," *Information Security Technical Report*, vol. 6, pp. 35-48, March 2001.

[4] P.Loshin, "The IP Security Protocol (IPsec)," *IPv6 (Second Edition)*, pp. 89-121, 2004.

[5] C. N. A. Program, "Fundamentals of Network Security Companion Guide," *Cisco Press*, 2004.

[6] A. a. V. Nuopponen, Sami, "Attacking Predictable IPsec ESP Initialization Vectors," *Helsinki University of Technology*, 2002.

[7] A. a. V. Nuopponen, Sami, "An Attack against IPsec Transport Mode HTTP Access," *Helsinki Univeristy of Technology*, 2002.

[8] Y. Zhang, "A Multilayer IP Security Protocol for TCP Performance Enhancement in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, 2004.

[9] W. T. Strayer, "Privacy Issues in Virtual Private Networks," *Computer Communications*, vol. 27, pp. 517-521, April 2004.

[10] C. Press, "CCNP Security VPN " *Official Cert Guide*, vol. 2nd Edition, pp. 642-648, 2012.

[11] M. L. Anne Henmi, M. L. Abhishek Singh and Chris Cantrell, "Chapter 5 - Defining a VPN in Firewall Policies and VPN Configurations," *Burlington: Syngress*, pp. 211-265, 2006.

[12] M. Lewis, "Comparing, Designing, and Deploying VPNs," *Cisco Press*, 2006.

[13] J.-C. Lin, "Design Implementation and Performance Evaluation of IP-VPN," *Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA'03)*, 2003.

About Author (s):

Dhari KH Abedula, is an IT Security enthusiast and a researcher in Universiti Teknologi Malaysia (UTM). He has a more than ten years experience in the IT industry and a wide range of certifications.
[dhari.kahled@gmail.com]

Ahmed A. Sabeeh, is an IT security specialist in the American International Group (AIG). He has more than eight years of experience in the IT Security industry and a master of Information Security and a wide range of certifications.
[ahmed.sabeeh@live.com]