International Journal of Computer Engineering and Information Technology

VOL. 9, NO. 9, September 2017, 186–191
Available online at: www.ijceit.org
E-ISSN 2412-8856 (Online)

Internet Protocol Security for Secure Communication: Fundamentals, Services and Application

Ruaa Adeeb Abdulmunem Al-faluji

University of Babylon, Babylon, Iraq

ABSTRACT

The world has become increasingly interconnected in terms of technology. The use of internet has grown dramatically. Internet plays an important role for the today's business. Every organization wants to secure their moving data because significant data loss can damage the business continuity. So the necessity of network security became obvious. The goal of this paper is to overview the network layer security mechanisms, Internet Protocols Security (IPSec), standard framework and end-to-end architecture .This paper also identifies the services , operation modes of IPSec and discusses the Virtual Private Network (VPN) as an application of IPSec.

Keywords: *IPSec,AH,ESP,Transport mode, Tunnel mode.*

1. INTRODUCTION

The uses of internet are growing with every passing day. The applications of internet in the enterprise are increasing continuously. Moreover, today's business organizations use many security responsive applications in their networks such as E-mail, E-commerce, E-transactions, online banking, etc. Different organizations are trying hard to keep their data in secure while moving in the various networks. [1]. The protection of transmitted data in the network is a crucial task especially for the critical and sensitive applications due to the problems related to the interconnecting networks without a border [2]. The Transmission Control Protocol / Internet Protocol (TCP/IP) is commonly used protocol suite to develop enterprise network. But TCP/IP protocol suite doesn't have any built-in security mechanism for protecting moving data.

Throughout the 1980s, due to massive use of internet and computers become target of hackers and attackers. The solution of these attacks was very simple, encourage users to choose a strong password, avoid to share accounts details with other. These steps can eliminate security holes in programs such as send mail and login as holes were discovered [3].

IPSec is the most widely used network layer security mechanisms in the enterprise network. It ensures secure communications across a LAN, WANs, and across the Internet. The implementation of IPSec is mandatory in IPv6 and optional in IPv4 .The authentication and encryption security services were added by the IAB as important security features in IPv6 and to handle the problems and weakness of IPv4 [4].

IPSec also provides many others high quality security services for IPv4 and IPv6 as we will discuss later. Because IPSec services are submitted at the IP layer, this in turn will offered additional protection for network and upper layer protocols [5].

In IPSec , security enrichments can be obtained using two Security protocols (Authentication Header (AH) and the Encapsulating Security Payload (ESP)) as well as using key management protocols [6].

Many security concepts are used to create IPSec such as signatures, ciphers, Keys. But one of the main characteristics of IPSec mechanisms is that they are algorithm-independent which means that different algorithms can be used without any effect on the other parts of the implementation [7].

The earlier version of IPSec was based on early implementation experiences while the latest revised version has a well-defined security model. A set of default algorithms is specified for interoperability purpose in the global Internet [8].

In this paper we are not going to discuss the logical and mathematical concept behind the used technologies in spite of their importance. But this research will focus on understanding concepts and providing the advance knowledge that is required in making decisions on the choice IPSec.

2. IPSec SERVICES

As we mentioned previously, IPSec includes two protocols that are used to provide many services of the IPSec. These protocols are:

- **An Authentication Protocol:** This protocol is designed for transfer of authenticated data between two entities.
- **A CombinedEncryption / Authentication Protocol (ESP):** This protocol specifically designed to provide encryption and optionally authentication for the transmitted data between two objects.

We gives a brief description on the IPSec services as below:

2.1 Access Control

IPSec provides access control by using the concepts of security association database (SAD) and **Security Policy Database (SPD)**.Where an association is a one-way (unidirectional) relationship between sender & receiver. It provides security on traffic between them and appears in both the authentication and confidentiality mechanisms for IP. While SPD refers to the means that relate IP traffic to specific SAs (or no SA in the case of not requiring using of IPSec) . An access control services for a packet can be obtained by checking if there is no security association already established for the arrived packet , the packet is discarded. IPSec handles each packet separately .The procedures of access control in IPSec for both outbound and inbound packets can be illustrated respectively in the following two figures.

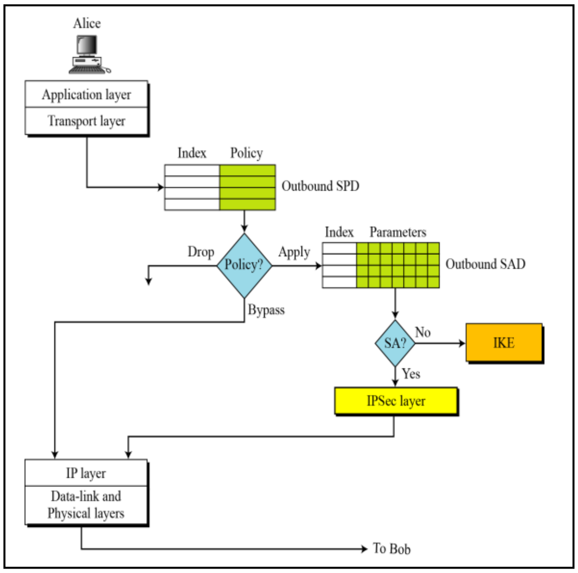


Fig. 1. Outbound Packet Processing

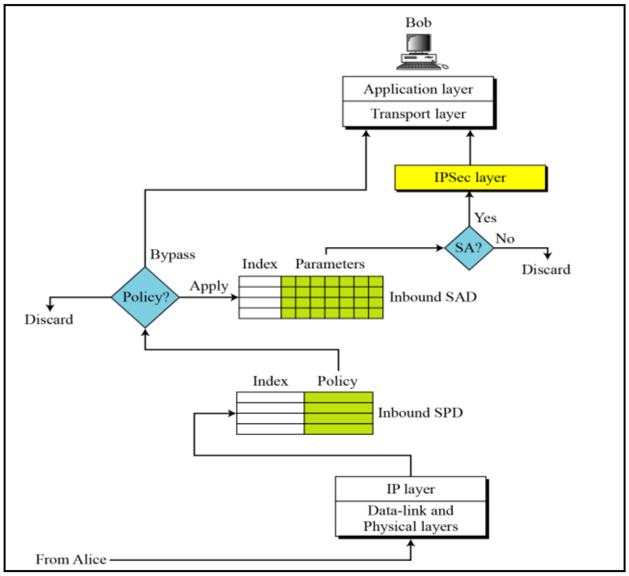


Fig. 2. Inbound Packet Processing

2.2 Message Integrity (Authentication)

It means that there is no changes occur to the content of a datagram during transmission, for any of reasons.

2.3 Data Source Authentication

It assures that the datagram was created by the claimed sender.

2.4 Confidentiality (Encryption)

It means hiding the content of a message using encryption. This service can be provided by ESP only because AH could not provide it.

2.5 Replay Attack Protection

In this type of the attacks , an attacker gets a copy of an authenticated packet and transmits it later to the intended destination.
Anti-reply service can be provided by IPSec protocols using sequence numbers and a sliding receiver window. We will clarify the procedures of this service in details.

☐ **At Sender Endpoint:**

- Each IPSec header contains a unique sequence number generated by the sender when the security association is established .
- The number starts from 0 and increases until the value reaches to 2^32 – 1.
- When the sequence number reaches to the maximum ,it is reset to 0 and the old security sssociation is deleted and a new one is established.

□ **At Receiver Endpoint**

- The receiver uses a fixed size window (the size is determined by the receiver with a default value(W=64)). The right edge of the window represents the highest sequence number, N, so far received for a valid packet. A variable uses to indicate if each packet in the current window was received or not.

- **If Received Packet's Sequence Number:**

✓ falls within the window and it has not been previously received, packet is **accepted** and marked as received.

✓ falls within the window and was previously received, the packet is **dropped** and the replay error counter is incremented.

✓ is greater than the highest sequence in the window, the packet is **accepted**, marked as received, the sliding window is moved "to the right".

✓ is less than the lowest sequence in the window, the packet is **dropped** and the replay error counter is incremented. these steps can be more illustrated in figure 3.

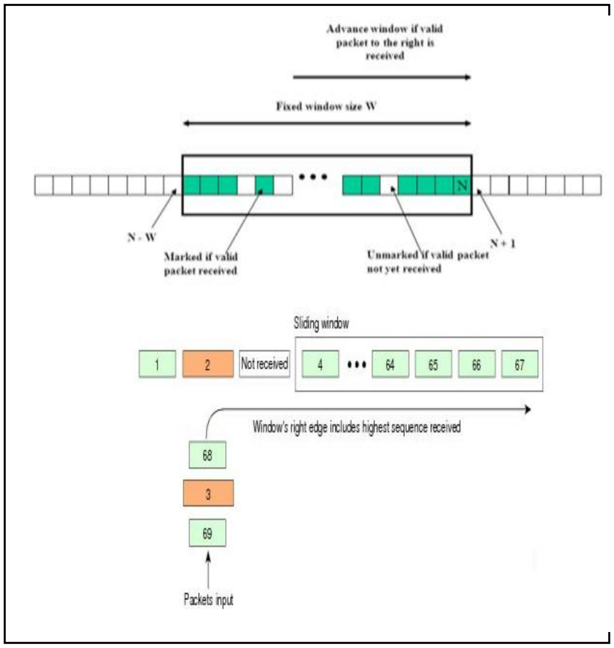

Advance window if valid packet to the right is received
Fixed window size W
N
N - W
Marked if valid packet received
Unmarked if valid packet not yet received
N + 1
Sliding window
1
2
Not received
4
64
65
66
67
Window's right edge includes highest sequence received
68
3
69
Packets input

Fig. 3. Anti- reply Mechanism

While Tabel 1 shows a summary of the main services that are provided by IPSec protocols.

Tabel 1: IPSec Services

	AH	ESP (Encryption Service Only)	ESP (Both Encryption and Authentication Services)
Access Control	y	y	y
Message Integrity	Y		Y
Data Source Authentication	Y		Y
Replay Attack Protection	Y	Y	Y
Confidentiality	N	Y	Y

Where Y=Yes and N=No.

3. IPSEC OPERATION MODES

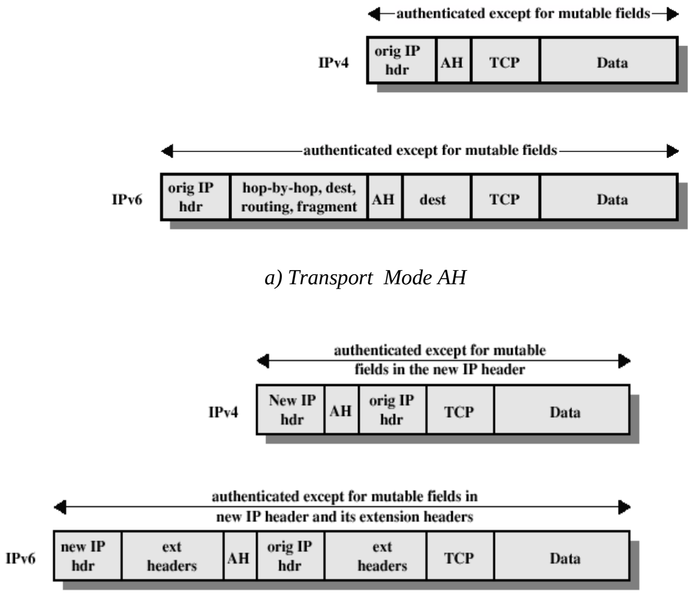
Transport mode and tunnel mode are two modes of operation used for each of IPSec protocols (AH and ESP). Depending on the security needs, the structure of the network and the logical connections between the endpoints the suitable mode can be chosen.

The main characteristics of the transport and tunnel modes can be summarized in the below table.

Table 2: Transport and Tunnel Mode Characteristics

Transport Mode	Tunnel Mode
The payload coming from the transport layer is protected while there is not any protection offered to the IP header.	The entire IP packet is protected.
The flow is from the transport layer to IPSec layer and then to the network layer.	The flow is from the network layer to the IPSec layer and then back to the network layer again.
It is practical when host-to-host (end-to-end) protection of data is required (e.g., a client and a server, or two workstations).	It is suitable between two routers, a host and a router, or between a router and a host .
Original routing information is used.	New routing information is added.

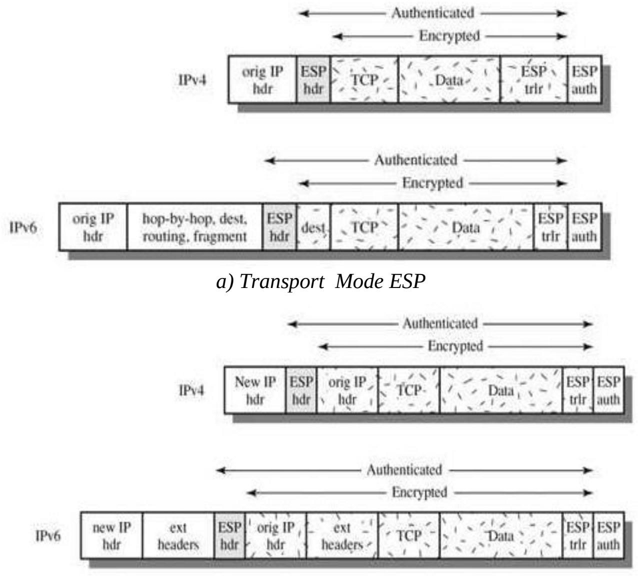
The AH and ESP protocols in both transport and tunnel mode can be shown in the following two figures.


authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data
authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
authenticated except for mutable fields in new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

a) Transport Mode AH

b) Tunnel Mode AH

Fig. 4. AH Protocol in Transport and Tunnel Modes



a) Transport Mode ESP

b) Tunnel Mode ESP

Fig. 5. ESP Protocol in Transport and Tunnel Modes

4. KEY MANAGEMENT IN IPSec

Key management is a significant feature of IPSec. It is related to handling the generation and distribution of keys for the secure communication.

There are also two mechanisms used for key management in IPSec [9] .The first one enables the manual configuration of the required keys for every system (its own keys and the keys of other systems that it will communicating with them) by system administrator .This type of management is suitable for small, relatively static environments.

While in the second type of management, the on-demand creation of keys are implemented by an automated system and this is practical for large environments.

These keys will ensure that only the authorized senders and receivers will get access to the messages. The common key management protocols used in the IPSec are:

- Oakley Key Determination Protocol: This protocol is based on the Diffie-Hellman algorithm but some features likes the cookies , nonces are added to overcome the weaknesses. Oakley does not required specific formats.
- and Internet Security Association and Key Management Protocol (ISAKMP): ISAKMP enables the Internet key management and it is independent of key exchange protocol, encryption algorithm, and authentication method.

5. VIRTUAL PRIVATE NETWORK (VPN)

In this section we will discuss the virtual private network as a common application of IPSec .VPN is a virtual network of an enterprise used to enable the data to be transferred securely over the public networks e.g. internet using VPN services. It can be built over the existing physical network. One of the main advantages of VPN is reducing the cost required to establish a private network of an enterprise which has several branch offices at various geographical separated places. It creates a secure communication tunnel between senders and receivers. All encrypted data are passed over this secure tunnel. So hackers get garbage data if they hack the data in transit. There are three types of VPN structures [10]:

1- Host-to-Host Architecture
2- Host-to-Gateway Architecture
3- Gateway-to-Gateway Architecture

Host-to-Host Architecture: The Host-to-Host Architecture is typically suitable for host to host connectivity. For example, if a system administrator wants to manage a single server remotely, the Host-to-Host Architecture is used. The VPN client is used in the administrator ends to establish a connection to the remote server. The following figure 6 shows a Host-to-Host architecture.

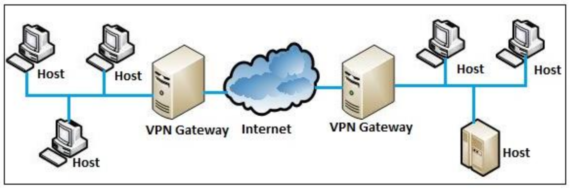


Fig. 6. Host-to-Host Architecture

Host-to-Gateway Architecture: This model is practical for providing secure remote accesses. In this model, a remote user can establish a VPN connection from local host to a VPN gateway that is deployed in the network of the enterprise. The host of the user sends a request to the VPN gateway to get access to the remote resources through VPN. The VPN gateway authenticate the user of request initiator before establish a connection. This VPN gateway may be a router or dedicated server. After exchanging information between host and gateway, the IPSec connection is established. The following figure 7 shows a Host-to-Gateway architecture.

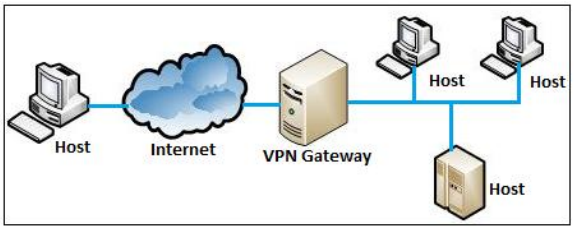


Fig. 7. Host-to-Gateway Architecture

Gateway-to-Gateway Architecture: This type is used to ensure secure communication between two different networks. In this architecture, a VPN connection is established between two gateways of the networks. For an IPSec connection establishment, a request is send from one VPN gateway to the other and exchange information with each other. All host of the network are routed to communicate over this IPSec connection. This model is suitable for connecting the branch offices of a enterprise to its head office over the internet. It minimizes the cost of building private WAN for a business. The VPN Gateway may be a router, firewall or a dedicated server. The following figure 8 shows a Gateway-to-Gateway architecture.

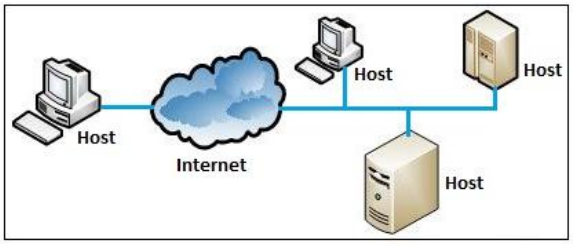


Fig. 8. Gateway-to-Gateway Architecture

6. COMMUNICATION WITH IPSec

This section presents an IPSec solution between two offices for securing communication. The figure shows that an organization has a main office and a remote office and they need to communicate with each other securely. The users at the remote office need to access the resources of the head office. There are several servers like mail server, file server, web server, database server etc are installed in the network of the head office. Communication with these resources remotely involves risk because these data sensitive for the business. The organization needs to ensure data confidentiality and integrity in its transit with a cost effective way.

In this scenario, the organization needs to establish a VPN solution between the remote office and head office. A secure VPN tunnel between the head office and remote office over the internet can protect the communications. The figure 4 shows that two routers are installed and configured at the edge of the two networks for implanting the VPN solution. These routers are configured as IPSec VPN gateways for creating tunnel between them. The networks of the head office and branch office are completely separated network and both are connected to the internet separately. But an IPSec tunnel has been created between these two routers, so the encrypted traffic will be forwarded from the source router to the destination router securely. The data will be decrypted only to the right destination. A pre-shared key will authenticate the senders and receivers. The encryption algorithm in the router will encrypt the data in transit [11].

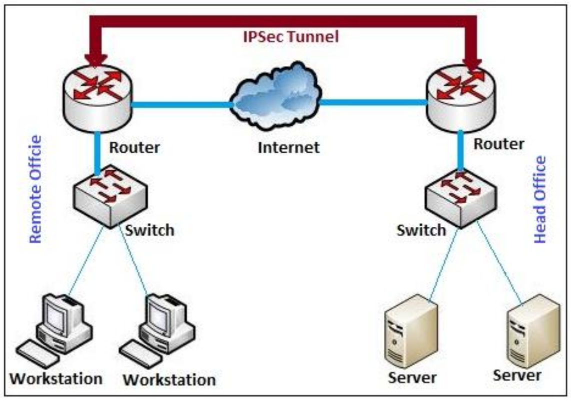


Fig. 9. An IPSec Solution between Offices

6. CONCLUSION

In this paper, We discussed IPSec as solution for a secure communication .We gave a description on the IPSec fundamentals , components, services , features and its' operation modes. The VPN Model has been discusses as an application of the IPSec and finally a secure communication between a branch office and head office through IPSec has been made.

8. Acknowledgment

I would like to thank Dr.wesam Bhaya and Dr. Rafid Sagban for their valuable assistant in completion this work.

REFERENCES

[1] D.Shinder,"Securing Data in Transit with IPSec,"TechGenix,2003.
[2] S.F.W.a.R.N.C.L.Wu,"IPSec/PHIL(Packet Header Information List):Design,Implementationand Evaluation,"Processeding of 10 national conference on Computer communication and network.
[3] M. R. a. A. M. Tuomas Aura, "Experiences with Host-to-Host IPsec," Microsoft Research, 2015.
[4] D. M. V. M. Mojtaba Sadeghi, "Secure Authentication Mechanism in Mobile Internet Protocol Version 6," Dubai, 2013.
[5] A. Harrison, "Internet Protocol security," Technology Quickstudy, 1999.
[6] IBM, "Application level security," IBM Knowledge Centre, 2017.
[7] J. Feiman, "Technologies for application-level security," Computer Weekly, 2009.
[8] T. K. David Bittlingmeier, "CompTIA Security+ Exam: Devices, Media, and Topology Security," Pearson, 2013.
[9] G. Kreizman, "An Introduction to Information Security Architecture," Gartner The Future of IT Conference, Mexico City, 2011.
[10] N. Doraswamy and D. Harkins, IPSec: the new security standard for the Internet, intranets, and virtual private networks, 2nd ed. Prentice Hall, Mar. 2003.
[11] D. Whiting, B. Schneier, and S. Bellovin, “AES key agility issues in high-speed IPSec implementations,” Counterplane Internet Security, May 2000.