# Analysis of Virtual Networks for Secure IP VPN Environments with IPSec

Md. Dilshad Ghani
Research Scholar, Department of Mathematics, Magadh University Bodh-Gaya, Bihar India
Dr. Md. Jawed Ikbal Khan
Assistant Professor, P.G. Department of Mathematics Mirza Ghalib College Gaya Magadh University Bodh□Gaya, Bihar India

Abstract— In today's security environment, it's difficult to make an informed decision about a Virtual Private Network (VPN). A virtual private network (VPN) allows users to connect to distant sites or other users across a public network (often the Internet) at any time and from any location. The goal of a virtual private network (VPN) is to enhance the security of data transfers between organisations and distant locations. A virtual private network (VPN) establishes a secure channel via which data may be sent. Secure Sockets Layer and Internet Protocol Security (IPSec) are the two most popular VPN protocols in use today. Both have advantages and disadvantages. This report presents a thorough examination of both technologies. The architectures and protocols of both technologies are discussed in detail, as well as the pros and cons of using them in the real world.

Keywords- Network Layer Security, VPN Architecture, Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Protocol Security (IPSec), Alternatives to IPsec, Virtual Private Network (VPN).

## 1 INTRODUCTION

By connecting a private network to the Internet through a public network, such as the Internet, a virtual private network (VPN) is created. Shared or public networks are treated as if they were part of a private network, with all of the same features, security measures, and administrative controls. The choice of a VPN depends on the apps being utilised [13]. Using a virtual private network (VPN) is a way to increase the security of data transfers. Tunneling techniques and security measures ensure the privacy of VPN data. In effect, the transmitter encrypts the data and sends it over a tunnel to the recipient, who decrypts it. For enhanced protection, it is possible to encrypt the network addresses of both the sender and receiver.

Remote user access and site-to-site communication are often used for two purposes. Distant-access VPNs may be used by individuals to connect to a remote network securely. Whereas a site-to-site VPN enables a secure link to be established between many offices that are located at different fixed locations. IPSec (Internet Protocol Security) and Alternatives to IPsec.

## 2 The Need for Network Layer Security

TCP/IP is extensively used to connect networks throughout the globe. Four distinct but interdependent layers make up the TCP/IP protocol stack. Whenever a user wishes to transmit data across networks, the data is sent from the highest layer to the lowest layer, with each layer providing extra information. The physical network is used by the lowest layer to transport the gathered data to its final destination. For the most part, the layer below encapsulates the data created by the layer above it. Figure 2-1 depicts the four TCP/IP tiers, from top to bottom.

| |
|---|
| Application Layer. In addition to the Domain Name System (DNS), HyperText Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP), this layer is responsible for sending and receiving data for specific applications (SMTP). |
| Transport Layer. This layer offers connection-oriented and connectionless services to move data from one network to another. It is possible to guarantee the reliability of communications by using the transport layer. The most common transport layer protocols are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). |
| Network Layer. This layer is responsible for the distribution of data packets across various networks. Network layer protocols such as TCP/IP are built on top of Internet Protocol (IP). Also, the Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP) are often used protocols at the network layer. |
| Data Link Layer. Communications between physical network components are handled by this layer. Ethernet is the most widely used data connection protocol. |

Figure 2-1. TCP/IP Layers

The most widely used network layer security control for securing communications is Internet Protocol Security (IPsec). IPsec is a set of open standards that make it possible to communicate securely across IP networks.

## 3 VPN Architecture

### 3.1 Gateway-to-Gateway Architecture

In order to offer secure network communications between two networks, IPsec-based VPNs are often used. This is normally accomplished by installing a VPN gateway on each network and creating a VPN connection between the two gateways, as described above. The traffic between the two networks that needs to be protected flows via the VPN connection that has been created between the two VPN

gateways. The VPN gateway may be a standalone device that simply performs VPN activities, or it may be a component of another network device, such as a firewall or router, that performs VPN services. A secured connection between two networks is shown in Figure 2-2, which displays an example of an IPsec network design that makes use of the gateway-to-gateway paradigm to achieve this.


Figure 2-2. Gateway-to-Gateway Architecture

Example

When it comes to user and host administration, the gateway-to-gateway architecture is the most straightforward to deploy. Users using gateway-to-gateway VPNs are often unaware of their existence since they do not need to undertake additional authentication in order to access the VPN. Also, in order to use the VPN, neither the users' computers nor the target hosts (like servers) should need to have VPN client software installed, nor should their systems need to be changed in any way.

### 3.2 Host-to-Gateway Architecture

It's becoming more and more popular to employ the host-to-gateway architecture for secure remote access. A VPN gateway is installed on the company's network, and each remote access user connects to the VPN gateway using their local computer (host). The VPN gateway, like the gateway-to-gateway concept, may be a separate device or a component of another network device. A secured connection for the remote user is shown in Figure 2-3 using an IPsec host-to-gateway architecture.

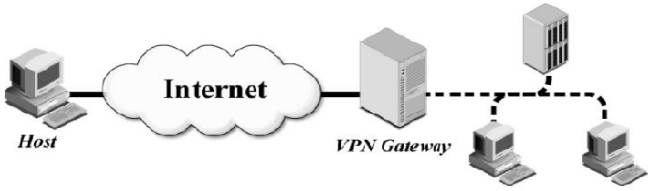



Figure 2-3. Host-to-Gateway Architecture Example

On-demand IPsec connections are formed for each VPN user in this configuration. The organization's IPsec gateway has been configured to accept IPsec clients from remote hosts. VPN gateways communicate with hosts when a remote user requests access to computing resources. The user is normally requested to authenticate by the VPN gateway before the VPN connection can be created. A dedicated authentication server may be consulted by the VPN gateway or it can handle the authentication itself. The IPsec connection is created after the client and gateway exchange data. All network communication between the user's host and the VPN gateway is encrypted, allowing the user to make use of the organization's computer capabilities. The VPN gateway can also be used to move traffic between the user and systems that are not controlled by the company. This lets IPsec security be used on this traffic as well.

### 3.3 Host-to-Host Architecture

The host-to-host model is the least popular VPN architecture and is primarily used for specialised purposes, such as remote server control by system administrators. System administrators' hosts are configured to behave as VPN clients by the organisation that provides VPN services via the server. The VPN client is used by the system administrators when connecting to a distant server. There are many ways to set up IPsec in a network, but the most common way is the host-to-host method.

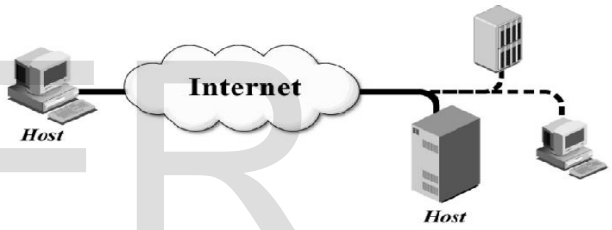



Figure 2-4. Host-to-Host Architecture

Example

On-demand IPsec connections are formed for each VPN user in this configuration. The IPsec server has been set to accept IPsec client requests from users' computers. The IPsec server communicates with the user's host when the user requests resources from the IPsec server. Before a connection can be established, the IPsec server requests authentication from the user. An IPsec connection is created when the client and server exchange information and the authentication process is successful. Users can now connect to the server, and IPsec will protect their network communications.

### 3.4 Model Comparison

Table 2-1 compares the three different types of VPN architecture.

Table 2-1. Comparison of VPN Architecture Models

| Feature | Gateway-to- | Host-to-gateway | | Host-to-host |
|---|---|---|---|---|

| | gateway | | | |
|---|---|---|---|---|
| It provides security between the local gateway and the client. | No | N/A (client is VPN endpoint) | | N/A (client is VPN endpoint) |
| Protects VPN endpoints. | Yes | Yes | | Yes |
| Between a remote gateway and a remote server, it protects both (behind the gateway). | No | No | | N/A (server is VPN endpoint) |
| To the end user, it's clear | Yes | No | | No |
| Users-friendly systems | Yes | No | | No |
| Transparent to servers | Yes | Yes | | No |

## 4 Authentication Header (AH)

The integrity of packet headers and contents is protected, and the user is authenticated using AH, one of the IPsec security protocols. Replay and access protection are two additional features that are available as an option. No packets can be encrypted using AH. A combination of AH and ESP was widely used to offer both secrecy and integrity protection for communications in the early days of IPsec, as the ESP protocol could only provide encryption, not authentication. IPsec's second version adds authentication features to ESP, making AH less important. Some IPsec software even no longer supports AH. In spite of this, since AH can verify parts of packets that ESP cannot, AH is still of use. This guide also contains a description of AH, since many current IPsec implementations use AH.

### 4.1 AH Modes

In AH, there are two modes of transportation: transit and tunnel. An IP header for each packet is generated in tunnel mode; this is not the case while using AH in transport mode. The real source or destination IP address for packets in IPsec systems that employ a gateway must be adjusted to be the gateway's IP address. Transport mode is often used in host-to-host topologies since it cannot update or establish a new IP header. Figures 4-1 and 4-2 indicate that AH safeguards the integrity of the whole packet, independent of the mode in which it is used. There is no integrity protection for IP header fields that might change unexpectedly in transit, as discussed in Section 3.1.2.

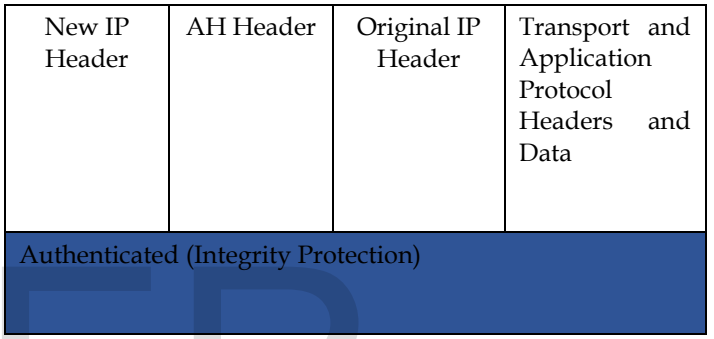



Figure 4-1. AH Tunnel Mode Packet

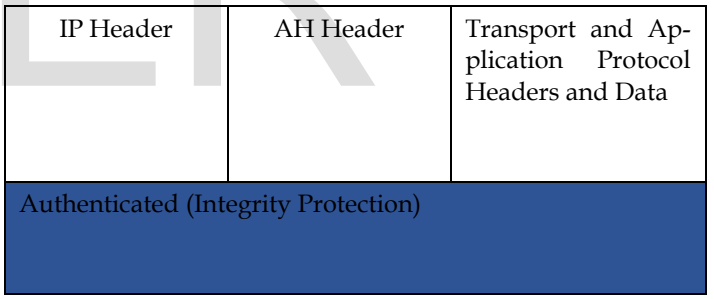



Figure 4-2. AH Transport Mode Packet

### 4.2 How AH Works

Reviewing and analysing genuine AH packets is the best way to learn how AH works. The bytes that make up a real AH packet are shown in Figure 3-4. Packet bytes in hex and ASCII translations of each hex byte may be found on the left side of the table. (A dot is used to signify bytes that cannot be converted into an ASCII character for printing.) Each part of the AH packet is seen in Figure 4-3: the Ethernet header, the IP header, the AH header, and the data. Figures 4-1 and 4-2 indicate that this packet is a transport mode packet since it only has one IP header in its body. An ICMP echo request, or ping, is included in the payload in this example. Hexadecimal numbers in the original ping represented alphabetic sequences (e.g., 61, 62, 63). The

ICMP payload is unaffected by the use of AH. This is because AH protects only the integrity of data, not the data itself.

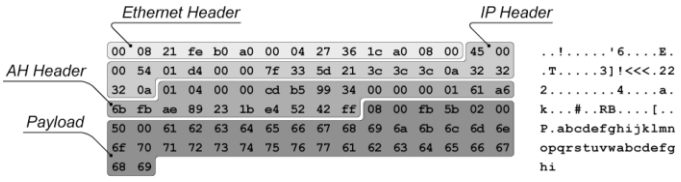



Figure 4-3. Sample AH Transport Mode Packet

## 5 Encapsulating Security Payload (ESP)

Security protocols ESP form the second core IPsec layer. When IPsec was launched, ESP was limited to encrypting just the data carried by a packet's payload. As explained in Section 3.1, the AH protocol offers integrity protection if necessary. ESP was given additional latitude in IPsec 2.0. Although it cannot authenticate the outermost IP header, it may offer integrity protection. In addition, the Null ESP Encryption Algorithm makes it possible to turn off ESP's encryption completely. As a result, ESP may be used in all but the earliest versions of IPsec to offer encryption, encryption with integrity protection, or merely integrity protection. At the end of this section, we talk about the third version of ESP, which is currently being made. We mostly talk about its features and qualities.

### 5.1 How ESP Works

A better grasp of how ESP works may be gained by studying and reviewing genuine ESP packets. ESP packet bytes and their ASCII representations are shown in Figure 5-1. ESP-protected payloads have encrypted the alphabetic sequence that was visible in the AH-protected payload. The Ethernet header, IP header, ESP header, encrypted data (payload and ESP trailer), and (optionally) authentication information are the only parts of an ESP packet that are divided into these five pieces. There is no way to tell whether this packet was created in transport or tunnel mode from the encrypted contents. Since the IP header is not encrypted (in this case, ESP), the IP protocol field in the header does reveal the payload's protocol.

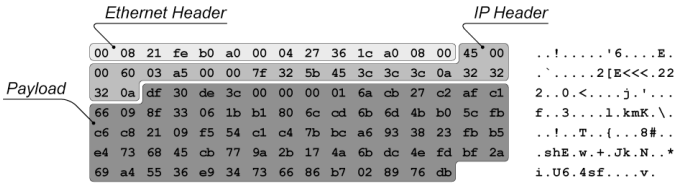



Figure 5-1. ESP Packet Capture

The ESP header fields are unencrypted, even though it's hard to see from Figure 5-1. From the first four ESP packets sent between hosts A and B in Figure 5-2, we can see the ESP header fields. As in AH, the SPI and sequence number fields are identical in ESP. Static SPI values are used by each host in order to create two one-way connections, each with its own SPI, in the ESP connection. For the second transmission, both hosts increased the sequence number from 1 to 2 from the first packet.

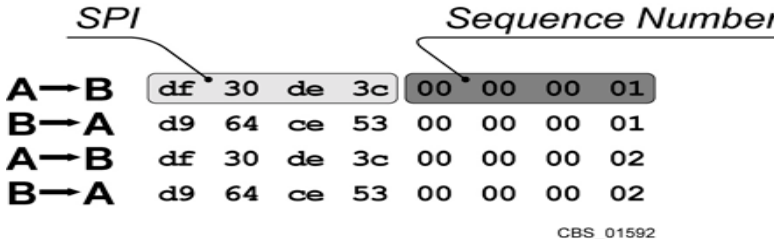



Figure 5-2. ESP Header Fields from Sample Packets

## 6 Internet Protocol Security (IPSec)

IPsec is a set of protocols that aid in the encryption of IP-based communication. IPsec protocols may be used in a number of different configurations to safeguard communications. ESP, AH, and IKE are the three basic components of an IPsec connection, and this part explains what each one does and how it all comes together to form an IPsec connection. ESP, AH, and IKE will be discussed in detail. In this section, we will also talk about IP Payload Compression Protocol (IPComp) as a benefit of implementing IPsec.

When it comes to network layer security controls, IPsec has emerged as the most widely utilised method of securing communications. IPsec is a set of open standards for maintaining the confidentiality of IP-based communications. IPsec can offer any combination of the following, depending on how it is built and set up.

- Confidentiality. IPsec may prevent unauthorised individuals from accessing data. With the use of an algorithm and a secret key known only to the people transferring data, this may be done. Only the owner of the secret key is able to decode the information.

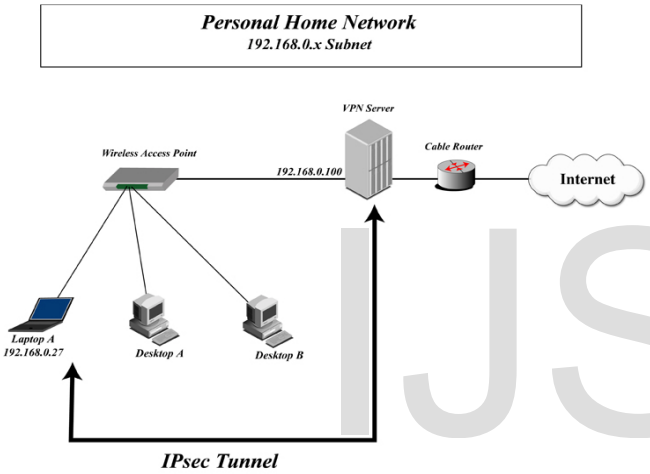
- Integrity. It is possible to tell whether data has been altered in transit using IPsec (intentionally or accidentally). An encryption checksum called a message authentication code (MAC) may be used to verify the integrity of the data. Data changes may affect the MAC, so the old and new values will be different.

- Peer Authentication. When sending data over an IPsec network, each endpoint checks to make sure the other endpoint it wants to talk to is also using IPsec.

- Replay Protection. Data is neither, repeated or provided out of sequence, nor is the same data delivered more than once. IPsec can't guarantee that information will be sent in the same order in which it was encoded.

- Traffic Analysis Protection. There is no way for a network traffic monitor to identify who is communicating and how frequently or how much data is being shared between parties. Packet-to-packet transmissions may, however, be tallied.

- Access Control. Endpoints that utilise IPsec may filter traffic to guarantee that only authorised IPsec users have access to certain network resources. IPsec endpoints can, for example, allow or deny access to Web servers and limit file sharing.




## 7 Alternatives to IPsec

Some situations may be better served by different protocols than IPsec, notwithstanding IPsec's adaptability. IPsec's various shortcomings are addressed in this section by presenting a comparison table of other VPN protocols and grouping them according to the TCP/IP model layer (as illustrated in Figure 5-1) at which they operate. Aside from IPsec, this section focuses on protocols for the data connection, transport, and application layers of the VPN. There is a short explanation for each protocol, along with a description of the conditions in which it is better than IPsec.

| |
|---|
| Application Layer. This layer (SMTP) is used by applications such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP). |
| Transport Layer. In order to transmit application layer services across networks, this layer offers either connection-oriented or connection-less services. It is possible to guarantee the reliability of communications by using the transport layer. The most common transport layer protocols are User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). |
| Network Layer. This layer is responsible for the distribution of data packets across various networks. TCP/network IP's transport layer protocol is known as Internet Protocol (IP). It's also common to see protocols like ICMP and IP Group Management Protocol (IGMP) in use on networks (IGMP). |
| Data Link Layer. The physical network layer is responsible for all communications. Ethernet is the most well-known protocol for the data connection layer. |

## 8 Analysis

Using IPsec tunnels to connect external systems to a trustworthy gateway is an excellent technique to keep sensitive data safe from prying eyes. There was no need for extra hardware or software to be purchased, and the design and implementation processes were substantially sped up. External organisations FTP server access was only restricted to certain users with special permissions, thus no new accounts were created or new policies were specified. Because the agency had previously built a solution for telecommuter access, this deployment was a breeze. It was necessary to modify the telecommuter solution to provide FTP users with limited access to the organization's network in order to meet their FTP server needs. While FTP-only telecommuting is still an option, there are several notable differences between the two:

- Available Resources. More computer resources are available to telecommuters than to FTP-only users. The government has established which protocols are required for the telecommuters to access. Additionally, telecommuters have access to a number of web servers, the corporate directory server, and the corporate antivirus server through FTP, among other options (to download software and signature updates). The IPsec gateway's telecommuters' group and packet filters are set up to only allow access to the appropriate host computers.

- Split Tunneling. Telecommuters pose a greater danger to the agency since they may interact with dozens of the agency's hosts using a variety of protocols and because each telecommuter's system is linked. Because split tunnelling isn't allowed, hacked telecommuter systems can't have as much of an influence on the agency.

- Client Host Security. Also prohibited by the agency is the use of IPsec by telecommuters in split tunnelling. Virus and antispyware software, as well as a personal firewall, must be installed and activated on the computers of telecommuters to protect them from online threats. The major goal of

these rules is to prevent client hosts from being hacked and to minimise the damage of any hacked hosts.

## 9 Future Directions

### Revised IPsec Standards

This working group of the IETF has produced a large number of RFCs and Internet-Drafts relevant to IPsec standards updates. IKEv2 is a proposed standard that would significantly alter the performance and capabilities of IKE. Even while there have been proposed standards for version 3 of ESP, AH, and IPsec's basic design and processing model, none of these modifications are as significant as the ones in IKE. IKE also mentions a proposed standard for encapsulating IP packets in UDP, which may be found here. It's a way to get around NAT problems. As companies start to add these features to their products, IPsec implementations are likely to get better.

## REFERENCES

[1] R. Kajal, D. Saini and K. Grewal, "Virutal Private Network" Interna-tional Journal of Advanced Research in Computer Science & Sofware Engineering, 2012, Vol. 2 (10), pp. 428-432. W.-K. Chen, *Linear Networks and Systems.* Belmont, Calif.: Wadsworth, pp. 123-135, 1993. (Book style)

[2] P.K. Singh and P.P. Singh, "A Novel approach for the Analysis & Issues of IPsec VPN" International Journal of Sciences and Research, 2013,Vol 2 (7), pp. 187-89.

[3] Wikipedia (www.en.w.ikipedia.org/wiki/IPsec)

[4] Root, Don and R. Rissler,"IPsec and SSL VPN Decision Criteria A Technology White Paper by Juniper Networks"(2006), May, 1-13.

[5] Pathan, A. Hassan and M. Irshad,"IP Based Virtual Private Network Implementation on Financial Institution and Banking System", (2014) pp. 30-34.

[6] J. Scarpati, IPsec vs SSL VPNs Understanding the Basics (http://searchnetworking.techtarget.com/feature/ IPsec-vs-SSL-VPNs-Understanding-th-basics), 2014

[7] K.V.Besien "Implementation of a VPN Network" Master Thesis, University of La Rochelle. (2006)

[8] White Paper "Virtual Private Networks: Improving Network Secu-rity for a diverse user community". (http://www.pdfio.net/k-7234709.html).

[9] Gupta, OP, Rani Sita, "Accelerating Molecular Sequence Analysis using Distributed Computing Environment" International Journal of Scientific & Engineering Research – IJSER, Oct 2013. ISSN 2229-5518

[10] L. Phifer, Tunnel Vission : Choosing a VPN-SSL VPN vs IPsec VPN. (http://searchsecurity.techtarget.com/feature/Tunnel-Vision- Choosing-a-VPN-SSL-VPN-vs-IP sec-VPN). 2003

[11] A. Sastry, IPsec VPN vs. SSL VPN: comparing respective VPN security risks (http://searchsecurity.tech target.com/tip/IPsec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks), 2011

[12] I. Akbar and K. Shahzad "Security in Private Branch IP-Telephony Network with QoS Demands" Master Thesis, Halmstad University. (2009)