IPSec Protocol in VPN

Y. P. Raiwani

Department of Computer Science and Engineering, HNB Garhwal University, Srinagar Garhwal, Uttarakhand India-246174

Abstract

The development of networks, the conduit for users to interact with application and thereby the data, follows that securing the network is first line of defense in IT security. Virtual Private Network (VPN) has emerged an important solution to security threats surrounding the use of public networks for private communications. VPN plays a great role in Wireless LAN by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels between pair of hosts. Once tunnel is created data transfer can take place. IPSec VPN and SSL VPN are two solutions of VPN which are widely used in WLAN. SSL VPN is used to give remote users with access to Web Applications, client/server applications and internal network connections. VPN provides security by using encryption with the help of IPSec, which includes Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP) for the integrity and confidentiality of the data. VPN technology uses IPSec in the tunnel mode to provide authentication, integrity and privacy.This paper presents comprehensive role of IPSec in VPN.

Key words: VPN, IPSec, ESP, AH, IKE

Introduction

Virtual Private Network (VPN) service is scalable and inexpensive solution that provides secure connectivity between corporate and branch offices. In addition, remote access capability of VPNs can be used to provide secure access to corporate resources for mobile employees and tale-commuters. Some of the measure services thatVPN can Provides are:

- extended connections across multiple geographic locations without using a leased line.
- flexibility for remote offices and employees to use the business intranet over an existing Internet connection as if they're directly connected to the network
- Saves time and expense for employees who commute from virtual workplaces
- VPN is preferred over leased line since leases are expensive, and as the distance between offices increases, the cost of leased line increase.

Internet Protocol security (IPSec) is a protocol, not a service, that provides encryption, integrity, and authentication services for IP-based network traffic. Because IPSec provides server-to-server protection, we can use IPSec to counter internal threats to the network, including eavesdropping, tampering, man in the middle attacks, IP spoofing, and other password-based attacks. IPSec is completely transparent to applications because encryption, integrity, and authentication services are implemented at the transport level. Applications continue to communicate normally with one another using TCP and UDP ports [1].

IPSec Services

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) [14]. IPSec provides the following optional network security services. Data Confidentiality—The IPSec sender can encrypt packets before transmitting them across a network. Data Integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission. Data Origin Authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service. Anti-Replay—The IPSec receiver can detect and reject replayed packets.
IPSec provides these security services at the IP layer; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts,

between a pair of security gateways, or between a security gateway and a host.

Technology used for IPSec

IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec offers a standard way to establish authentication and encryption services between endpoints. This includes both standard algorithms and transforms, but also standard key negotiation and management mechanisms (via ISAKMP/Oakley) to promote interoperability between devices by allowing for the negotiation of services between these devices. IPSec includes Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP) [2].

Internet Key Exchange

IKE protocol is a key management protocol standard which is used in conjunction with the IPSec standard. It enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard. It enables automatic negotiation of IPSec security associations, secure communications without costly manual preconfiguration, and facilitates secure exchange of encryption keys [13]. IKE level 1, Establish secure authenticated IKE SA and IKE level 2, Exchange information necessary to creates IPSec SAs. Three messages establish IPSec, SA parameters (ESP, AH, SHA, MD5), SA lifetime and session key[19]. ISAKMP—the Internet Security Association and Key Management Protocol is a protocol framework which defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association. Oakley—A key exchange protocol which defines how to derive authenticated keying material. Skeme—A key exchange protocol which defines how to derive authenticated keying material, with rapid key refreshment. The component technologies implemented for use by IKE include: [18].

DES—The Data Encryption Standard (DES) is used to encrypt packet data. IKE implements the 56-bit DES-CBC with Explicit IV standard. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Diffie-Hellman—A public-key cryptography protocol which allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE to establish session keys. 768-bit and 1024-bit Diffie-Hellman groups are supported. MD5 (HMAC variant)—MD5 (Message Digest 5) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing.

SHA(HMAC variant)—SHA (Secure Hash Algorithm) is a hash algorithm used to authenticate packet data. HMAC is a variant which provides an additional level of hashing. RSA signatures and RSA encrypted nonces—RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Adleman. RSA signatures provides non-repudiation while RSA encrypted nonces provide repudiation.

IKE provides following benefits. [4]

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec security association.
- Allows encryption keys to change during IPSec sessions.
- Allows IPSec to provide anti-replay services.
- Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

Levels of key management

IKE performs mutual authentication between two parties and establishes an IKE security association (SA) that includes shared secret information that can be used to efficiently establish SAs for ESP [RFC2406] and/or AH [RFC2402] and a set of cryptographic algorithms to be used by the SAs to protect the traffic that they carry. An initiator proposes one or more suites by listing supported algorithms that can be combined into suites in a mix and match fashion. [3]

Level 1

Level 1 establishes a master secret from which subsequent cryptographic keys are derived in order to protect user data traffic. This is true even if no security protection yet exists between the two endpoints. VPN uses either RSA signature mode or pre shared keys to authenticate Level 1 negotiations, as well as to establish the keys that protect the IKE messages that flow during the subsequent Level 2 negotiations. A pre shared key is a nontrivial string up to 128 characters long. Both ends of a connection must agree on the pre shared key. The advantage of using pre shared keys is their simplicity, the disadvantage is that a shared secret must be distributed out-of-band, for example

over the telephone or through registered mail, before IKE negotiations. Treat your pre shared key like a password.
RSA Signature authentication provides more security than pre shared keys because this mode uses digital certificates to provide authentication. You must configure your digital certificates by using Digital Certificate Manager. In addition, some VPN solutions require RSA Signature for interoperability. For example, Windows® 2000 VPN uses RSA Signature as its default authentication method. Finally, RSA Signature provides more scalability than pre shared keys. The certificates that you use must come from certificate authorities that both key servers trust. [5]

LevelI

Level II, also called as the "Quick Mode," is used to establish the IPSec SA and to generate new keying material. A full Diffie-Hellman key exchange may be done to provide perfect forward secrecy (PFS), otherwise the keys are derived from the level I keying material. [20] Level 2, however, negotiates the security associations and keys that protect the actual application data exchanges. Up to this point, no application data has actually been sent. Level 1 protects the level 2 IKE messages.
Once level 2 negotiations are complete, your VPN establishes a secure, dynamic connection over the network and between the endpoints that we defined for our connection. All data that flows across the VPN is delivered with the degree of security and efficiency that was agreed on by the key servers during the level 1 and level 2 negotiation processes. In general, level 1 negotiations are negotiated once a day, while level 2 negotiations are refreshed every 60 minutes or as often as every five minutes. Higher refresh rates increase your data security, but decrease system performance. Use short key lifetimes to protect your most sensitive data. [5]

Authentication Header

IP Authentication Header (AH), a key protocol in the IPSec (Internet Security) architecture, is used to provide connectionless integrity and data origin authentication for IP datagrams, and to provide protection against replays. This protection service against replay is an optional service to be selected by the receiver when a Security Association is established. AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change in transit and the value of these fields, when the packet arrives at the receiver, may not be predictable by the sender. The values of such fields cannot be protected by AH. Thus the protection provided to the IP header by AH is only partial in some cases.
IPSec AH may be applied alone, in combination with the IP Encapsulating Security Payload (ESP), or in a nested fashion through the use of tunnel mode. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP may be used to provide the same security services, and it also provides a confidentiality (encryption) service.
The primary difference between the authentications provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP. [6]. To support AH may be a one way hash function(Keyed MD5 - RFC 1828, SHA - RFC 1852, HMAC MD5 - RFC 2085, HMAC SHA) or a symmetric encryption algorithm (DES).

Encapsulating Security Payload

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 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.
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 [10].

Technology for secure VPN

IPSec has two methods of forwarding data across a network: transport mode and tunnel mode. Each differs in their application as well as in the amount of overhead added to the passenger packet.

Tunnel Mode

Tunnel Mode encapsulates and protects an entire IP packet. Because tunnel mode encapsulates or hides the IP header of the packet, a new IP header must be added in order for the packet to be successfully forwarded. The encrypting routers themselves own the IP addresses used in these new headers. Tunnel mode may be employed with either or both ESP and AH. Tunnel mode encrypts both payload and the whole header (UDP/TCP and IP).

In tunnel mode, the "inner" IP header carries the ultimate (IP) source and destination addresses, while an "outer" IP header contains the addresses of the IPSec "peers," e.g., addresses of security gateways. In tunnel mode, AH protects the entire inner IP packet, including the entire inner IP header. The position of AH in tunnel mode, relative to the outer IP header, is the same as for AH in transport mode. The following diagram illustrates AH tunnel mode positioning for typical IPv4 and IPv6 packets. [8], [15]

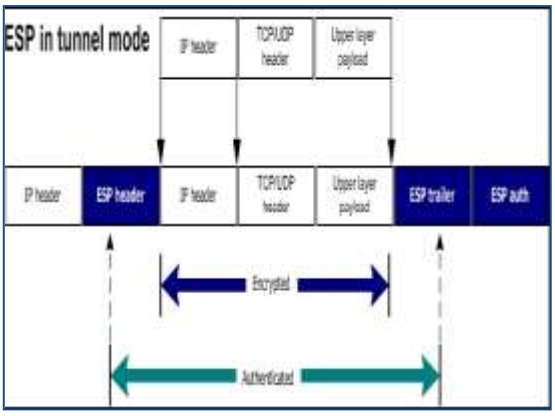
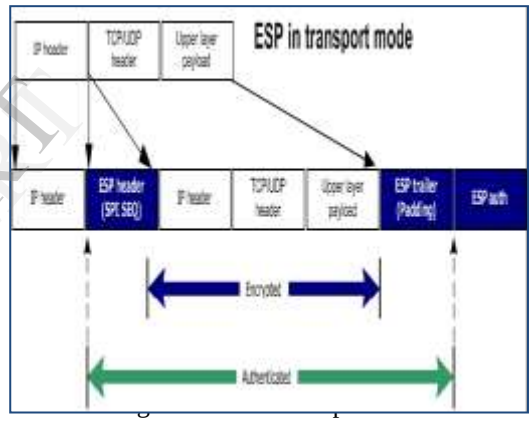


Fig. 1-ESP in Tunnel Mode

Transport Mode

In transport mode, AH is inserted after the IP header and before a next layer protocol, e.g., TCP, UDP, ICMP, etc. or before any other IPSec headers that have already been inserted. In the context of IPv4, this calls for placing AH after the IP header (and any options that it contains), but before the next layer protocol. (Note that the term "transport" mode should not be misconstrued as restricting its use to TCP and UDP.) Transport Mode encrypts only the data portion and leaves the IP header untouched.

In the IPv6 context, AH is viewed as an end-to-end payload, and thus should appear after hop-by-hop, routing, and fragmentation extension headers. The destination options extension header(s) could appear before or after or both before and after the AH header depending on the semantics desired. The following diagram illustrates AH transport mode positioning for a typical IPv6 packet.ESP and AH headers can be combined in a variety of modes [15].



IPSec VPN Challenges

IPSec implementations require IPSec gateway vendors to continually verify their implementations' compliance with standards to ensure correctness and interoperability. Performance and scalability must also be constantly upgraded and verified to satisfy the growing needs of the IPSec VPN industry. Managed service providers and network managers must deal with the impact of IPSec VPNs on the performance of applications across the network and with the interoperability of network elements and services in multi-vendor environments.

These issues need to be adequately addressed by the IPSec community to ensure rapid growth. The IETF is in the process of updating some of the protocols used with IPSec VPNs (for instance, a newer version of IKE - called IKEv2). These present new and ongoing challenges to the IPSec community [11].

IPSec Security Association

The concept of a security association (SA) is fundamental to IPSec. An SA is a relationship between two or more entities that describes how the entities will use security services to communicate securely. IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption, integrity, authenticity, or all three. When the security service is determined, the two IPSec peers must determine exactly which algorithms to use (for example, DES or 3DES for encryption, MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. As you can see, there is quite a bit of information to manage. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. A separate pair of IPSec SAs are set up for AH and ESP transform. Each IPSec peer agrees to set up SAs consisting of policy parameters to be used during the IPSec session. The SAs are unidirectional for IPSec so that peer 1 will offer peer 2 a policy. If peer 2 accepts this policy, it will send that policy back to peer 1. This establishes two one-way SAs between the peers. Two-way communication consists of two SAs, one for each direction [9]. The IPSec Packet processing component secures the packets using information in security associations of outbound security bundle. Inbound security associations are used to decrypt and authenticate inbound packets [16].
Some of the security algorithms that are still being used in IPsec have already been cracked. This poses a huge security risk, especially if the network administrators unknowingly use those algorithms instead of newer, more complex ones that are already available.

VPN Scope

The main benefit of a VPN is the potential for significant cost savings compared to traditional leased line networking. As the popularity of the Internet grew, businesses turned to it as a means of extending their own networks. Now, companies are creating their own VPN to accommodate the needs of remote employees and distant offices. VPN can also be helpful in the infectious disease like bird-flu, it can allow people to work from their home using a VPN connection [21].

Conclusion

Being based at the network layer allows IPsec to completely invisible in its operation and is ideal for monitoring and securing all sorts of internet traffic, inbound as well as outbound. IPSec VPN ensures network security by encrypting all data transfers between predetermined endpoints. It allows network address hiding without address translation. IPSec protects all traffic against unauthorized modification and eavesdropping, and also securely authenticates the communicating parties. IPSec supports certificate authorities and Internet Key Exchange (IKE) negotiation. IPSec VPNs can protect against many of the most common attack methods, including Denial of Service (DoS), replay, and "man-in-the-middle" attacks.

References

[1] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan "Improving Web Application Security: Threats and Countermeasures", http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/HTUseIPSec.a
[2] http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scIPSec.htm
[3] Internet Draft, draft-ietf-IPSec-ikev2-17.txt http://www3.ietf.org/proceedings/05mar/IDs/draft-ietf-IPSec-ikev2-17.txt
[4] http//www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt4/scike.htm
[5] http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/rzaja/rzajasecassociations.htm
[6] IPSec AH is defined by IETF (www.ietf.org) in RFC 2402.Reference
[7] Deering, S., and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[8] Internet Draft, IP Authentication Header draft-ietf-IPSec-rfc2402bis-07.txt
[9] IPSec Security Associations (SAs) http://www.ciscopress.com/articles/article.asp? p=24833 & seqNum=7.
[10] ESP is defined by IETF (www.ietf.org) in RFC 2406
[11] IPSec Virtual Private Networks: Conformance and Performance Testing http://www.ixiacom.com/library/white_papers/display?skey=IPSec
[12] Securing L2TP using IPSec http://www.ietf.org/rfc/rfc3193.txt
[13] Deploying IPSec Virtual Networks www.cisco.com/en/US/products/ps6635/products_white_paper09186a0080117919.shtml

[14] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[15] VPN White paper http://www.intotoinc.com
[16] White paper http://www.ixiacom.com/library/white_papers/display?skey=ipsec,
[17] http://www.ietf.org/rfc/rfc2408.txt, (RFC 2408)
[18] http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113newft/113t/1133t/isakmp.htm
[19] Network Security Architectures, Sean Convery, Cisco Press
[20] http://www.techonline.com/community/ed_resource/feature_article/21194__MR6294881394NF
[21] http://computer.howstuffworks.com/vpn5.htm