ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Design and Implementation of IPsec VPN's and its Configuration on ISP Network

Poral Vandana [1], B.Srinivasa Rao [2], C.Damini [3], K.S.Himaja [4]
[1, 2, 3, 4] Dept of electronics and Control Engineering, Sree Vidyanikethan Engineering College, India
vandana.porala@gmail.com

Abstract

This paper describes methods for implementing Virtual Private Networks (VPN) with IP Security (IPSec). A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks. The Internet Protocol Security (IPsec) standard provides a method to manage authentication and data protection between multiple crypto peers engaging in secure data transfer. The Authentication Header (AH) provides integrity and authentication for IP datagram's. ESP provides data confidentiality, integrity, and authentication. The implemented protocols are used to secure packets end to end and are normally called IP Security (IPSec). However, with intervening gateways (firewalls) or because of the faith in their own private networks, some organizations may choose to secure the packets only on the Internet and let the packets travel in clear text inside the organization.

Keywords: Authentication Header (AH), Encapsulating Security Payload (ESP), IP Security (IPSec), Transport, Virtual Private Networks (VPN).

Introduction

Virtual Private Network

Virtual Private Network (abbreviated VPN) it shows the technology to establish a private network in the public network or virtual private network (VPN) is an extension of a organization private intranet across a public network such as the Internet.

VPNs securely connect remote users and offices in a corporate network. The objective of a Virtual Private Network is to add a level of security to the exchange of data. Even when a company is using a leased line, they can deploy a VPN network to protect their data. It is a virtual network, because of the connection between any two nodes of the whole VPN is not a physical link which basically private network uses. Instead, it builds up a logic network on top of the platform which an Internet Service Provider provides, for example, Internet, Asynchronous Transmission Mode (ATM), Frame Relay (FR) and so on. And the client data is transmitted in the logical link.VPN uses the encryption and decryption process, and key management, user and device identity authentication technologies. It covers the package across the shared or public networks, the encryption and authentication validation link, extension of the private network.

IP Security

IP Security (IPsec) protocol is a security standard which is published by IETF in November of 1998. (RFC 2401) Its main motto is to provide password-based security, strong interoperability and high quality communication with security for the IPv4 and IPv6. IPsec protocol is used to establish high intensity security process to the packet at the IP layer. It aid the origin authentication, data confidentiality connectionless data integrity, and the various other security services.

IPSEC Protocols

This area will focus on the three primary components which are used for the security purpose of data .The Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE) protocols. Explaining each security protocols with their purpose and function and describing the working process to create IPsec connections. IPsec is a collection of protocols that assist in securing communications over IP networks.

Encapsulating Security Payload (ESP):

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/ decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication

Authentication Header (AH):

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched. Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known.

In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

Configuration of IPSec VPNs

Steps to configure the IPSec VPNs:

1. Configure the ISAKMP policy(IKE phase 1)
2. Configure the IPSec Transform(IKE Phase 2)
3. Crypto access control list(ACL)
4. Configure the Crypto map
5. Apply the Crypto map to the interface

Internet Key Exchange

To implement a VPN solution with encryption, periodic changing of session encryption keys is necessary. Failure to change these keys makes the VPN susceptible to brute force decryption attacks. IPsec solves the problem with the IKE protocol, which makes use of two other protocols to authenticate a crypto peer and to generate keys. IKE uses a mathematical algorithm called a Diffie-Hellman exchange to generate symmetrical session keys to be used by two crypto peers.

IKE also manages the negotiation of other security parameters such as the data to be protected, the strength of the keys, the hash methods used, and whether the packets are protected from anti-replay. ISAKMP normally uses UDP port 500 as both the source and destination port.

A Security Association (SA) is an agreement between two peers engaging in a crypto exchange. This agreement includes the type and strength of the encryption algorithm used to protect the data. The SA includes the method and strength of the data authentication and the method of creating new keys for that data protection. Crypto peers are formed as described in the following sections. Each SA possesses a lifetime value for which an SA is considered valid.

The lifetime value is measured in the both time (seconds) and volume (byte count) and is negotiated at SA creation. These two lifetime values are compared, and agreement is reached on the lower of the two. Under normal circumstances, the lifetime value expires via time before the volume limit. Thus, if an interesting packet matches the SA within the final 120 seconds of the lifetime value of an active SA, the crypto re-key process is typically invoked. The crypto re-key process establishes another active SA before the existing SA is deleted. The result is a smooth transition with minimum packet loss to the new SA.

ISAKMP Security Association

An ISAKMP SA is a single bi-directional secure negotiation channel used by both crypto peers to communicate important security parameters to each other, such as the security parameters for the IPsec SA (data tunnel).

In Cisco IOS, the ISAKMP SA policy has a default lifetime value of 86,400 seconds with no volume limit.

IPsec Security Associations (Data Tunnel)

An IPsec SA is a uni-directional communication channel between one crypto peer to another. The actual customer data traverses only an IPsec SA, and never over the ISAKMP SA. Each side of the IPsec tunnel has a pair of IPsec SAs per connection; one to the remote, one from the remote. This IPsec SA pair information is stored locally in the SA database.

In Cisco IOS, the IPsec SA policy has a default lifetime value of 3600 seconds with a 4,608,000 Kbytes volume limit.

IKE Phase One

IKE Phase One is the initial negotiation of a bi-directional ISAKMP SA between two crypto peers, often referred to as main mode. IKE Phase One begins with an authentication in which each crypto peer verifies their identity with each other. When authenticated, the crypto peers agree upon the encryption algorithm, hash method, and other parameters described in the following sections to build the ISAKMP SA. The conversation between the two crypto peers can be subject to eavesdropping with minimal risk of the keys being recovered. The ISAKMP SA is used by the IKE process to negotiate the security parameters for the IPsec SAs. The ISAKMP SA information is stored locally in the SA database of each crypto peer.

Authentication Methods

IKE Phase One has three possible authentication methods: Pre-Shared Keys (PSK), Public Key Infrastructure (PKI) using X.509 Digital Certificates, and RSA encrypted nonces. For the purpose of this architecture, only PSK and PKI with X.509 Digital Certificates are described, but the design is feasible with any of these authentication methods.

IKE Phase Two

In IKE Phase Two, the IPsec SAs are negotiated by the IKE process using the ISAKMP bi-directional SA, often referred to as quick mode. The IPsec SAs are Uni-directional in nature, causing a separate key exchange for data flowing in each direction. One of the advantages of this strategy is to double the amount of work required by an eavesdropper to successfully recover both sides of a conversation. During the quick mode negotiation process, the crypto peers agree upon the transform sets, hash methods, and other parameters.

Encryption Algorithms

As in main mode, quick mode uses an encryption algorithm to establish the IPsec SAs. The encryption algorithm negotiated by the quick mode process can be the same or different from that in the main mode process. Cisco IOS supports DES, 3DES, AES 128, AES 192,and AES 256 encryption algorithms, with DES designated as the default.

Hashed Message Authentication Codes

As in main mode, quick mode uses an HMAC to establish the IPsec SAs. The HMAC negotiated by the quick mode process can be the same or different from that in the main mode process. Both MD5 and SHA-1 are supported within Cisco IOS, with SHA-1 designated as the default.

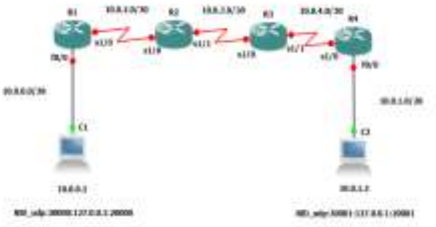
Perfect Forward Secrecy

If perfect forward secrecy (PFS) is specified in the IPsec policy, a new Diffie-Hellman exchange is performed with each quick mode negotiation, providing keying material that has greater entropy (key material life) and thereby greater resistance to cryptographic attacks. Each Diffie-Hellman exchange requires large exponentiations, thereby increasing CPU use and exacting a performance cost. PFS (Diffie-Hellman) Groups 1, 2, and 3 are supported within Cisco IOS. PFS is disabled by default. Group 1 has a key length of 768 bits, Group 2 has a key length of 1024 bits, and Group 5 has a key length of 1536 bits.

Pre-Shared Keys

PSKs are an administrative pre-defined key string in each crypto peer used to identify each other. Using the PSK, the two crypto peers are able to negotiate and establish an ISAKMP SA. A PSK usually contains a host IP address or subnet and mask that is considered valid for that particular PSK. A wildcard PSK is special kind of PSK whose network and mask can be any IP address.

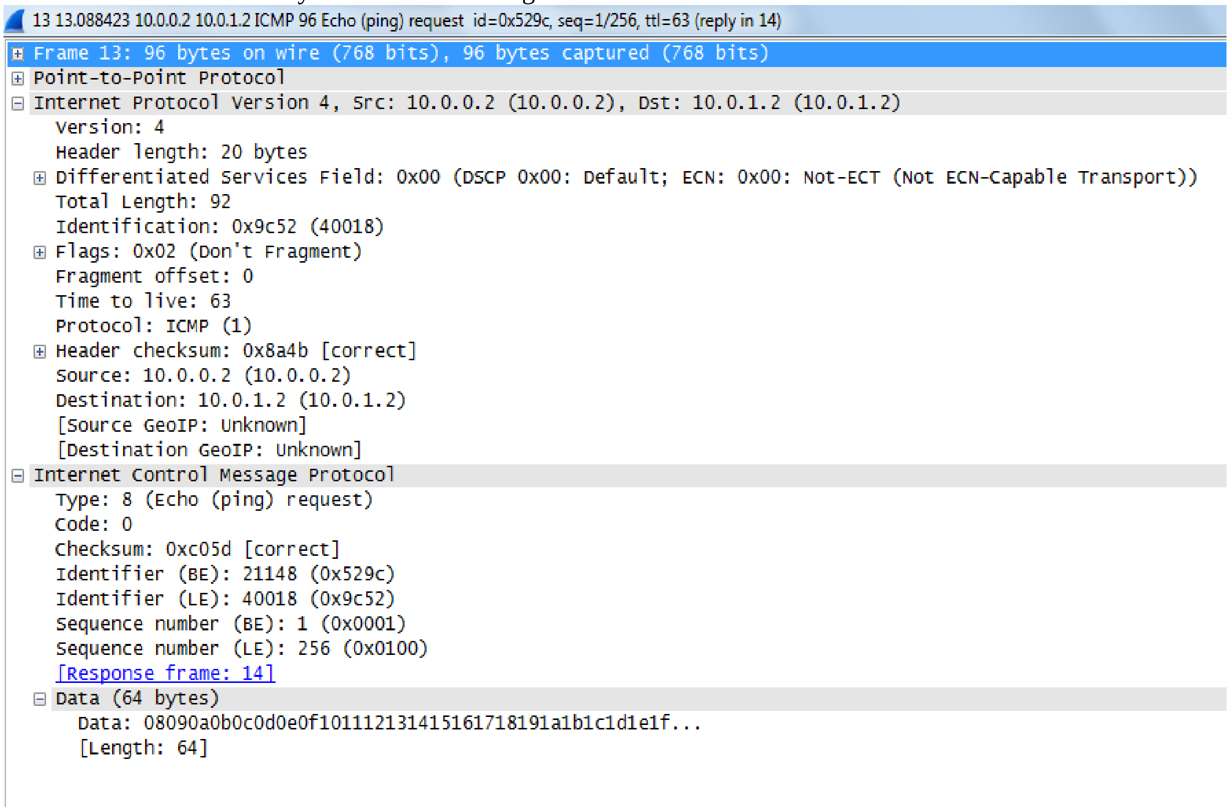
Main Topology



Conclusion and Results

VPN is an absolute new network technology. IPsec allow VPN network a standard security for the corporate network. IPSec is the most trusted and secure VPN solution available in the current market. The dispute of VPN is agreeably solved by IPSec enable VPN by compromise certain level of overhead, performance parameter in order to enable security with IPSec.

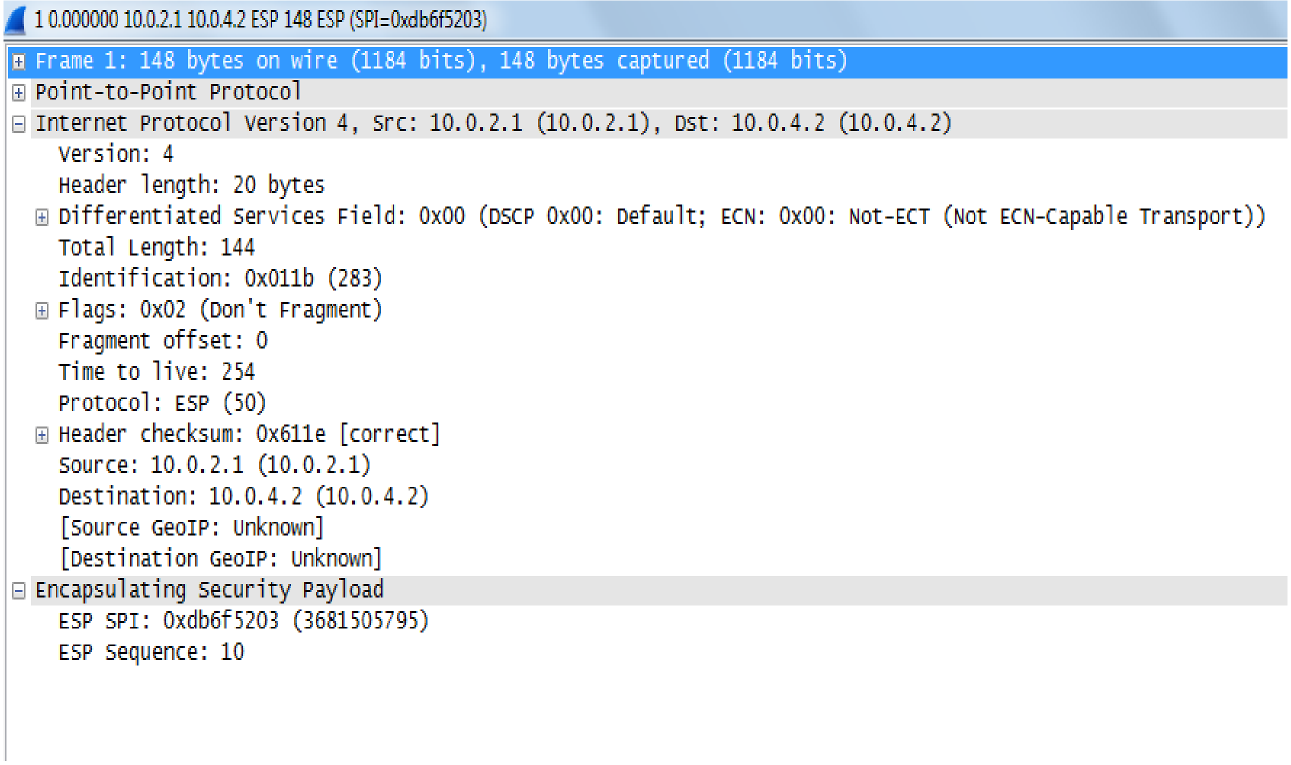
ICMP Packet Data Visibility Before IPsec Configuration



```
13 13.088423 10.0.0.2 10.0.1.2 ICMP 96 Echo (ping) request  id=0x529c, seq=1/256, ttl=63 (reply in 14)

⊞ Frame 13: 96 bytes on wire (768 bits), 96 bytes captured (768 bits)
⊞ Point-to-Point Protocol
⊟ Internet Protocol Version 4, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.1.2 (10.0.1.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 92
    Identification: 0x9c52 (40018)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (1)
  ⊞ Header checksum: 0x8a4b [correct]
    Source: 10.0.0.2 (10.0.0.2)
    Destination: 10.0.1.2 (10.0.1.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xc05d [correct]
    Identifier (BE): 21148 (0x529c)
    Identifier (LE): 40018 (0x9c52)
    Sequence number (BE): 1 (0x0001)
    Sequence number (LE): 256 (0x0100)
    [Response frame: 14]
  ⊟ Data (64 bytes)
      Data: 08090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f...
      [Length: 64]
```

ICMP Packet Data Visibility After IPsec Configuration



```
1 0.000000 10.0.2.1 10.0.4.2 ESP 148 ESP (SPI=0xdb6f5203)
⊞ Frame 1: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
⊞ Point-to-Point Protocol
⊟ Internet Protocol Version 4, Src: 10.0.2.1 (10.0.2.1), Dst: 10.0.4.2 (10.0.4.2)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 144
    Identification: 0x011b (283)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 254
    Protocol: ESP (50)
  ⊞ Header checksum: 0x611e [correct]
    Source: 10.0.2.1 (10.0.2.1)
    Destination: 10.0.4.2 (10.0.4.2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Encapsulating Security Payload
    ESP SPI: 0xdb6f5203 (3681505795)
    ESP Sequence: 10
```

References

1. Mr. Hitesh dhall, Ms. Dolly Dhall, Ms. Sonia Batra, Ms. Pooja Rani IMPLEMENTATION OF IPSEC PROTOCOL 2012 Second International Conference on Advanced Computing & Communication Technologies*978-0-7695-4640-7/12*
2. RFC 2401, Security Architecture for the Internet Protocol, provides an overview of IPsec. The RFC is available for download at *http://www.ietf.org/rfc/rfc2401.txt.*
3. AH is IP protocol number 51. The AH version 2 standard is defined in RFC 2402, IP Authentication Header, available at *http://www.ietf.org/rfc/rfc2402.txt*
4. Olalekan Adeyinka Analysis of problems associatedwith IPSec VPN Technology 2008, *978-1-4244-1643-1/08*
5. ESP is IP protocol number 50. The ESP version 2standard is defined in RFC 2406, IP EncapsulatingSecurity Payload (ESP), available at*http://www.ietf.org/rfc/rfc2406.txt.*
6. D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409 (Proposed Standard), Internet Engineering Task Force, Nov. 2008.
7. Ankur Lal, Dr.Sipi Dubey,Mr.Bharat Pesswani "Reliability of MANET through the Performance Evaluation of AODV, DSDV, DSR "International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, No. 5,May 2012,pp. 213- 216.
8. D. Harkins and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409 (Proposed Standard), Internet Engineering Task Force, Nov. 2008.
9. Muhammad Awais Azam, Zaka-Ul-Mustafa, Usman Tahir, S. M. Ahsan, Muhammad Adnan Naseem, Imran Rashid, Muhammad Adeel” Overhead Analysis of Security Implementation Using IPSec “
10. S. P. Meenakshi S. V. Raghavan “Impact of IPSec Overhead on Web Application Servers”