Internet **P**rotocol **Sec**urity (Basic)

Safwan Muntasir (Sufi)
Networking Enthusiast

Contents

Back to Contents

Introduction

IPsec, or Internet Protocol Security, is a comprehensive suite of protocols developed to secure Internet Protocol (IP) communications. It provides a framework for secure communication over the Internet at the network layer. The development of IPsec began in the early 1990s, as the need for secure communication over the Internet grew. At the time, there were a number of different security protocols in use, but none of them were standardized or widely supported.

IPsec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), IPsec ensures confidentiality, integrity, and authenticity of data communications across a public network. In 1992, the Internet Engineering Task Force (IETF) formed the IP Security Working Group to develop a standardized set of security protocols for IP. The working group published the first IPsec standards in 1995. IPsec has been revised and updated a number of times since its initial release. The current version of IPsec is defined in a number of RFCs, including RFC 2401 and RFC 2412.

IPsec Business Applications:

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishment of extranet and intranet connectivity with partners
- Secure Inter-Network communications

Back to Contents

Features

IPSec, developed by IETF, allows two or more hosts to communicate in a secure manner by authenticating and encrypting each IP packet of a communication.

- Scales from small to very large networks
- Available in Cisco IOS software version 11.3(T) and later
- Included in PIX Firewall version 5.0, ASA firewalls

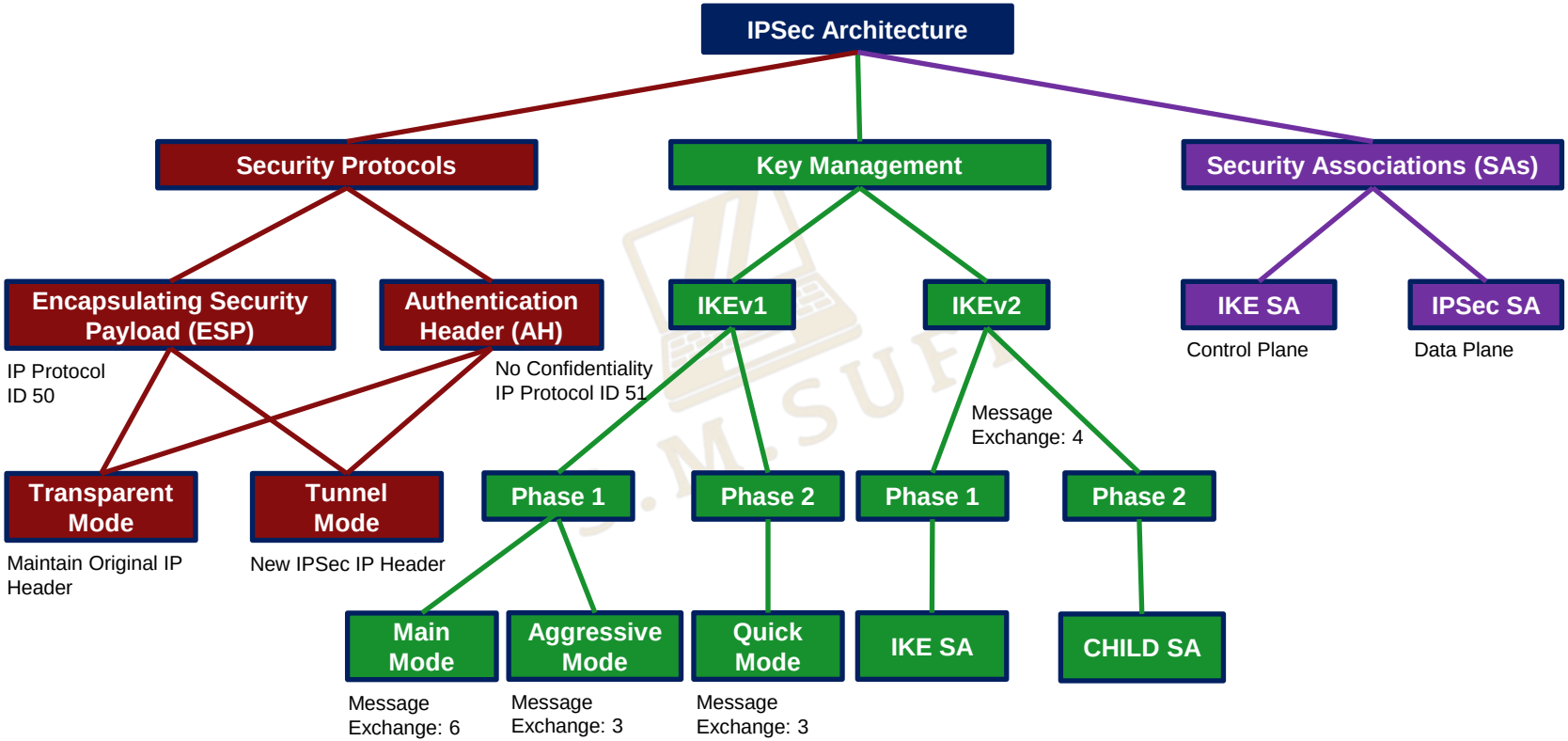
IPSec is a layer 3 technology, that mainly provides four major features-:

1. **Confidentiality:** IPsec encrypts the payload of IP packets, which prevents unauthorized users from reading the data. Means that the contents are not visible to any third parties. No snooping or wiretapping (using encryption).
2. **Integrity:** IPsec adds an authentication header to IP packets, which ensures that the data has not been tampered with (hashing algorithms).
3. **Authentication:** IPsec can be used to verify the identity of the sender of an IP packet. Provides confirmation about DataStream origin.
4. **Replay protection:** IPsec includes a replay protection mechanism that prevents old packets from being replayed. Ensuring packet received only once security service where the receiver can reject old or duplicate packets in order to defeat replay attack.

***IPSec VPN** encrypts **Layer-3 to Layer-7** information.

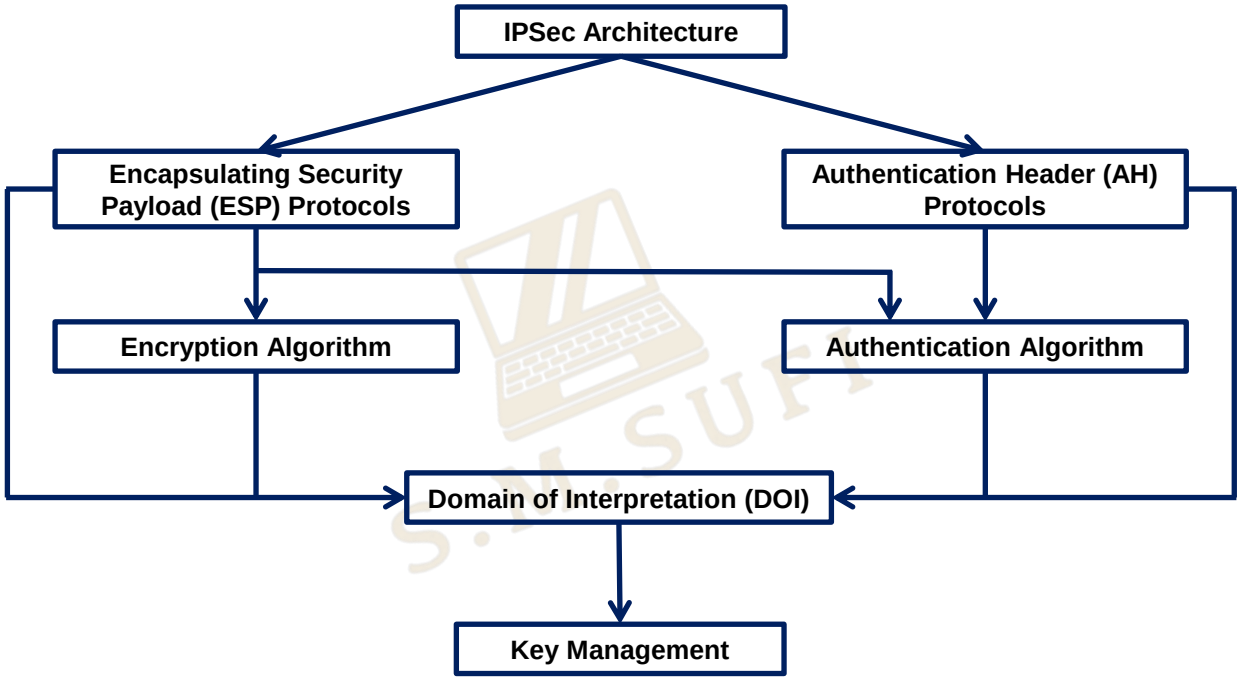
Back to Contents

Featured Architecture



Back to Contents

Flow Architecture



Back to Contents

Security Association (SA)

Security Association (SA) is a crucial component of IPsec (Internet Protocol Security), a suite of protocols that ensures secure communication over the Internet by encrypting and authenticating IP packets. SAs define the parameters and policies governing how IPsec secures communications between two entities. In simple word, SA is a kind of relationship between communicating entities to secure their communication.

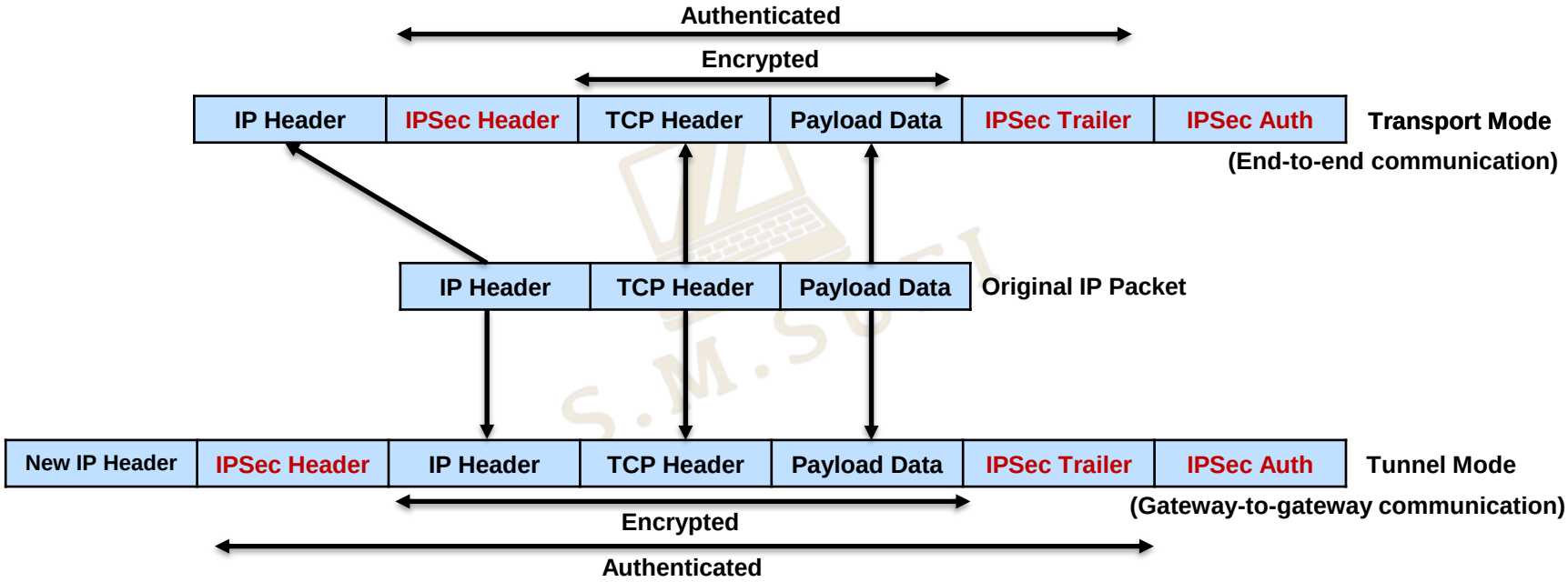
SA Components:

- **Security Parameter Index (SPI)**: A unique identifier for the SA, ensuring proper association between IPsec-protected packets and the corresponding SAs.
- **Security Protocol Identifier**: Identifies Security Protocols used such as AH or ESP.
- **Sequence Number**: A counter used to protect against replay attacks, preventing the reuse of old packets. Range 0 to (2^32 – 1).
- **Integrity Check Value (ICV)**: A cryptographic hash value used to verify the integrity of IPsec-protected packets, ensuring that data has not been tampered with.
- **Encryption Algorithm**: The specific encryption algorithm employed, such as AES, DES, or 3DES, to protect the confidentiality of the packet's payload.
- **Authentication Algorithm**: The chosen authentication algorithm, such as HMAC-SHA-1 or HMAC-MD5, used to verify the identity of the sender and the integrity of the packet.
- **Lifetime**: The duration for which the SA remains valid, after which a new SA needs to be negotiated.

Back to Contents

IPSec Modes

- **IPSec Mode**: There are two modes in IPSec – Transport Mode and Tunnel Mode.



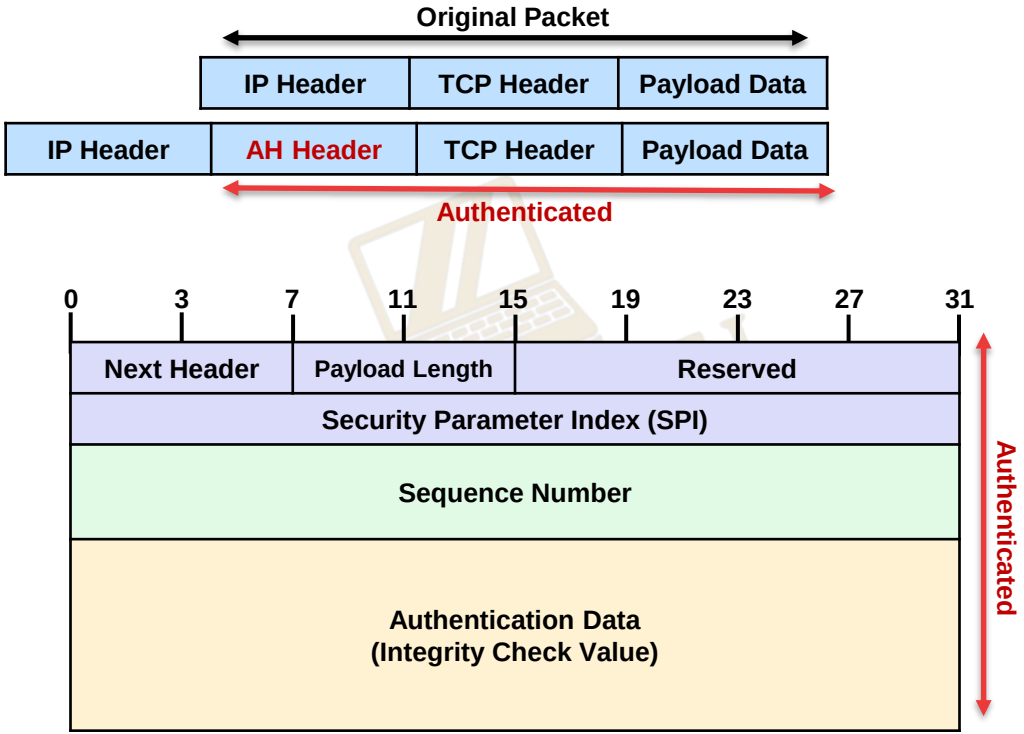
Back to Contents

Authentication Header (AH)

- Authentication Header (AH) is a member of the IPsec protocol suite.
- Guarantees the data origin by authenticating IP packets. AH can use a variety of authentication algorithms, including HMAC-SHA-1 and HMAC-MD5. The authentication algorithm is chosen during the IKE negotiation process.
- Ensures integrity by using a hash function and a secret shared key in the AH algorithm.
- Optionally a sequence number can protect the IPsec packet's contents against replay attacks, using the sliding window technique and discarding old packets.
- In IPv4, AH prevents option-insertion attacks. In IPv6, AH protects both against header insertion attacks and option insertion attacks.
- AH operates directly on top of IP, using IP Protocol number 51.
- AH can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

Back to Contents

Authentication Header (AH)



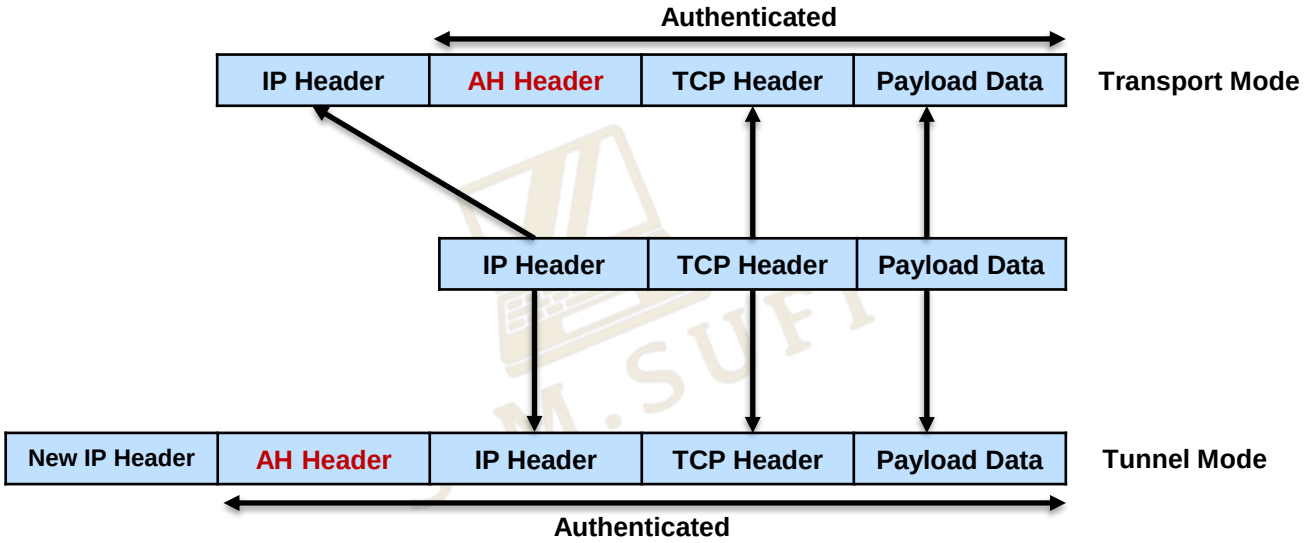
Back to Contents

Authentication Header (AH)

- **Next Header**: Contains the protocol number or type of the next header after the AH. Used to link headers together.
- **Payload Length**: Despite its name, this field measures the length of the authentication header itself, not the payload. It is measured in 32 bit units, with 2 subtracted for consistency with how header lengths are normally calculated in IPv6.
- **Reserved**: Not used; set to zeroes.
- **Security Parameter Index (SPI)**: A 32-bit value that is combined with the destination address and security protocol type to identify the security association to be used for this datagram. It is one of the Identification Parameter of the Security Association.
- **Sequence Number**: **:** A counter field initialized to zero when a security association is formed between two devices, and then incremented for each datagram sent using that SA. This is used to provide protection against replay attacks.
- **Authentication Data**: This field contains the *Integrity Check Value (ICV)* ,to check undeserved modification, resulting from the application of the optional ESP authentication algorithm. This field is variable in length.

AH protocol focuses on integrity and authentication, no encryption algorithm is applied for confidentiality.

Authentication Header (AH)

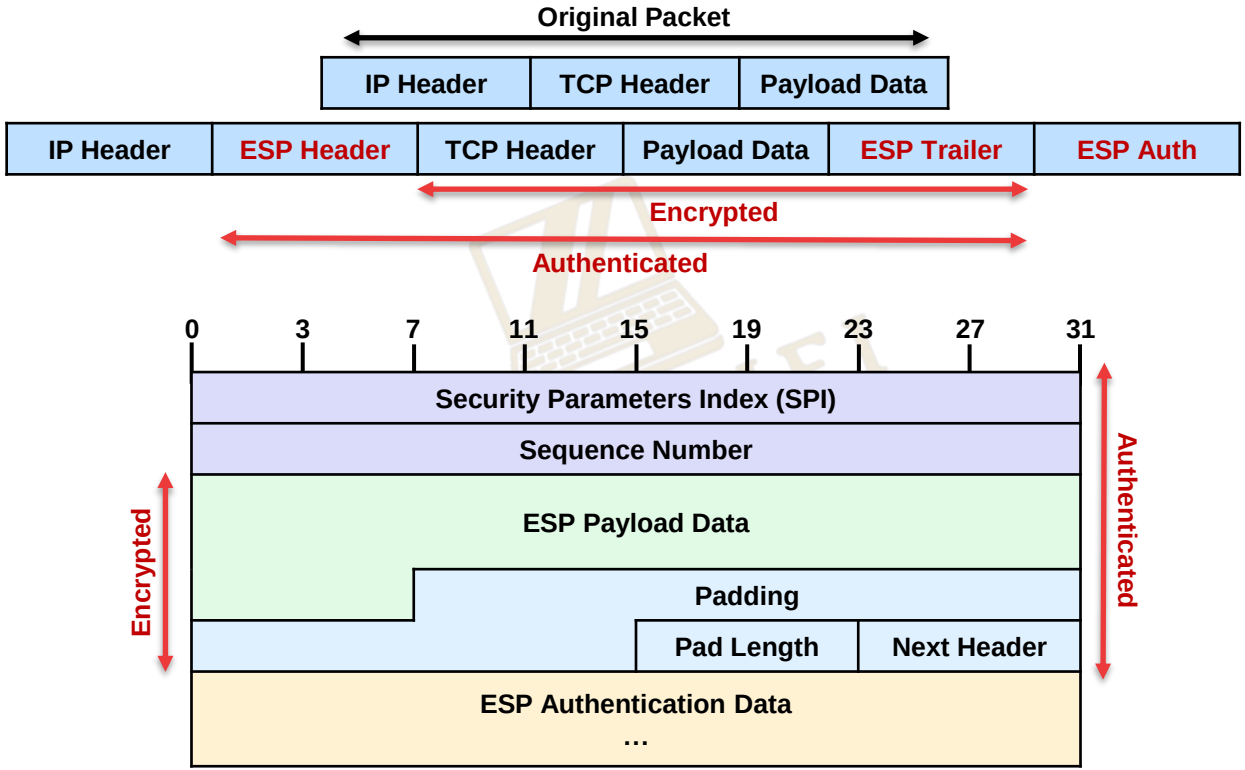


Back to Contents

Encapsulating Security Payload (ESP)

- ESP is a member of the IPSec protocol suit.
- Provides origin authenticity through authentication algorithms such as:
- Provides data integrity through hash functions such as: HMAC-SHA1, HMAC-MD5, etc.
- Provides confidentiality through encryption protection for IP packets using algorithms like: DES, 3DES, AES, etc.
- ESP supports encryption only and authentication only configurations, but using encryption without authentication is strongly discouraged because it is insecure.
- ESP operates directly on top of IP, using IP Protocol number 50.
- ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.
- ESP is discussed in RFC 2406.

Encapsulating Security Payload (ESP)



Encapsulating Security Payload (ESP)

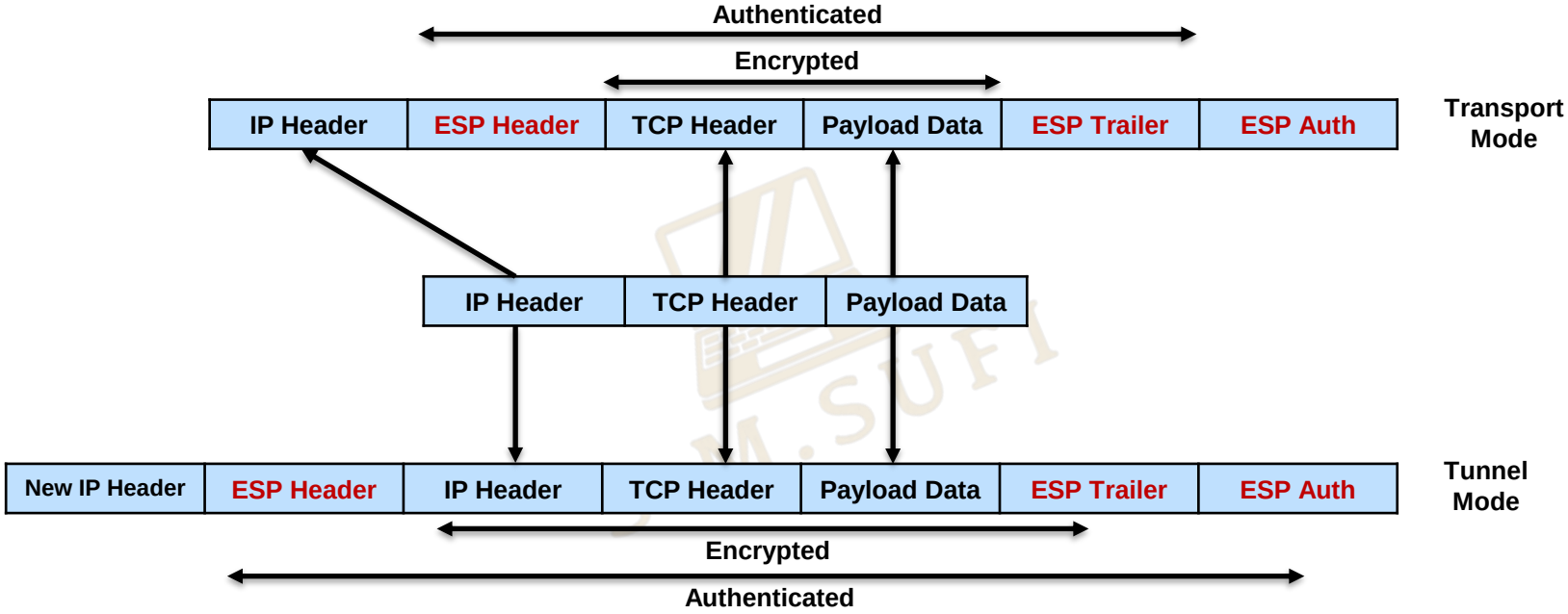
- **Security Parameter Index (SPI)**: A 32-bit value that is combined with the destination address and security protocol type to identify the security association to be used for this datagram. It is one of the Identification Parameter of the Security Association.
- **Sequence Number:** A counter field initialized to zero when a security association is formed between two devices, and then incremented for each datagram sent using that SA. This is used to provide protection against replay attacks.
- **Payload Data:** Payload data means the actual data or the actual message. The Payload data is in an encrypted format to achieve confidentiality. This field is variable.
- **Padding:** Extra bits of space are added to the original message in order to ensure confidentiality. Range is 0 to 255 bytes.
- **Pad Length:** Padding length is the size of the added bits of space in the original message.
- **Next Header:** Contains the protocol number of the next header in the datagram. Used to chain together headers. Basically identify the types of Data.
- **ESP Authentication Data:** This field contains the *Integrity Check Value (ICV)* ,to check undeserved modification, resulting from the application of the optional ESP authentication algorithm. This field is optional in ESP protocol packet format.

*****Why Padding is used in ESP?**

ESP provides encryption to Data. In the encryption algorithms, Data is send in terms of Blocks (fixed length). Thus, padding is used to adjust variable length Data to fixed length Blocks.

Back to Contents

Encapsulating Security Payload (ESP)



Back to Contents

Comparing ESP and AH

Feature	ESP	AH
Confidentiality	Yes	No
Authentication	Optional	Yes
Integrity	Yes	Yes
Anti-Replay Protection	Yes	Yes
Complexity	More Complex	Less Complex
Performance Impact	Higher	Lower
Modes	Transport and Tunnel	Transport and Tunnel
Packet Size	Adds overhead to IP Packet	Adds less overhead to IP Packet
Applications	VPNs, Secure Remote Access, Secure Inter-network Communications, etc.	DNS Security, Applications where authentication and integrity is important

Back to Contents

Algorithms

Encryption

- DES
- 3DES
- AES-128
- AES-192
- AES-256

Authentication

- Pre-Shared-Key
- Certificate

Integrity

- HMAC-MD5
- HMAC-SHA1-96
- HMAC-SHA2-128
- HMAC-SHA2-256
- HMAC-SHA2-384
- HMAC-SHA2-512
- PSK
- RSA
- EC-DSA
- Ed-DSA

Key-Exchange

- Diffie-Hellman Group 1
- Diffie-Hellman Group 2
- Diffie-Hellman Group 5
- Diffie-Hellman Group 14
- Diffie-Hellman Group 19
- Diffie-Hellman Group 20
- Diffie-Hellman Group 21
- Diffie-Hellman Group 24

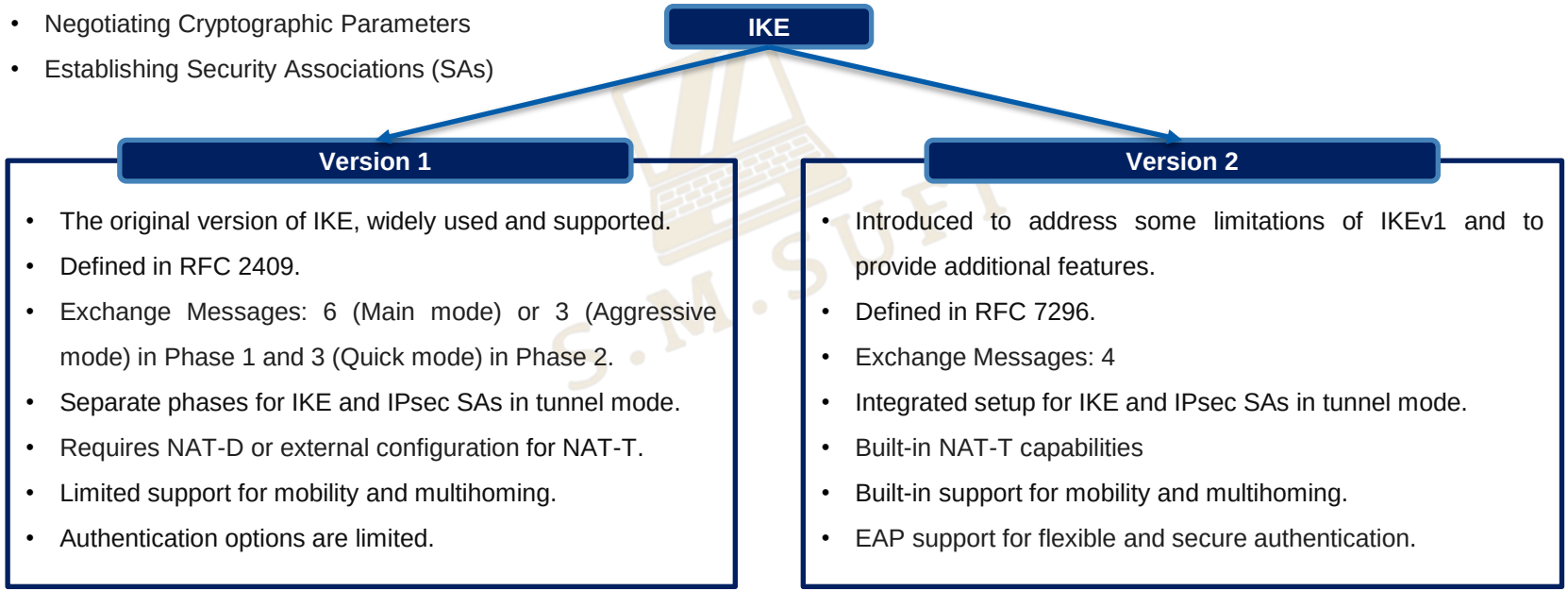
DH-Group 1,2,5 are not used because they do not provide as adequate security level against modern threat. Generally DH-Group 14 and 19 is used. DH-Group 20,21 and 24 is called Next Generation Encryption.

***Check **RFC 8221, RFC 3526, RFC 4753, RFC 4754, RFC 6617, RFC 8420** for detailed information. Explanation of these algorithms is given in another material.

Internet Key Exchange (IKE)

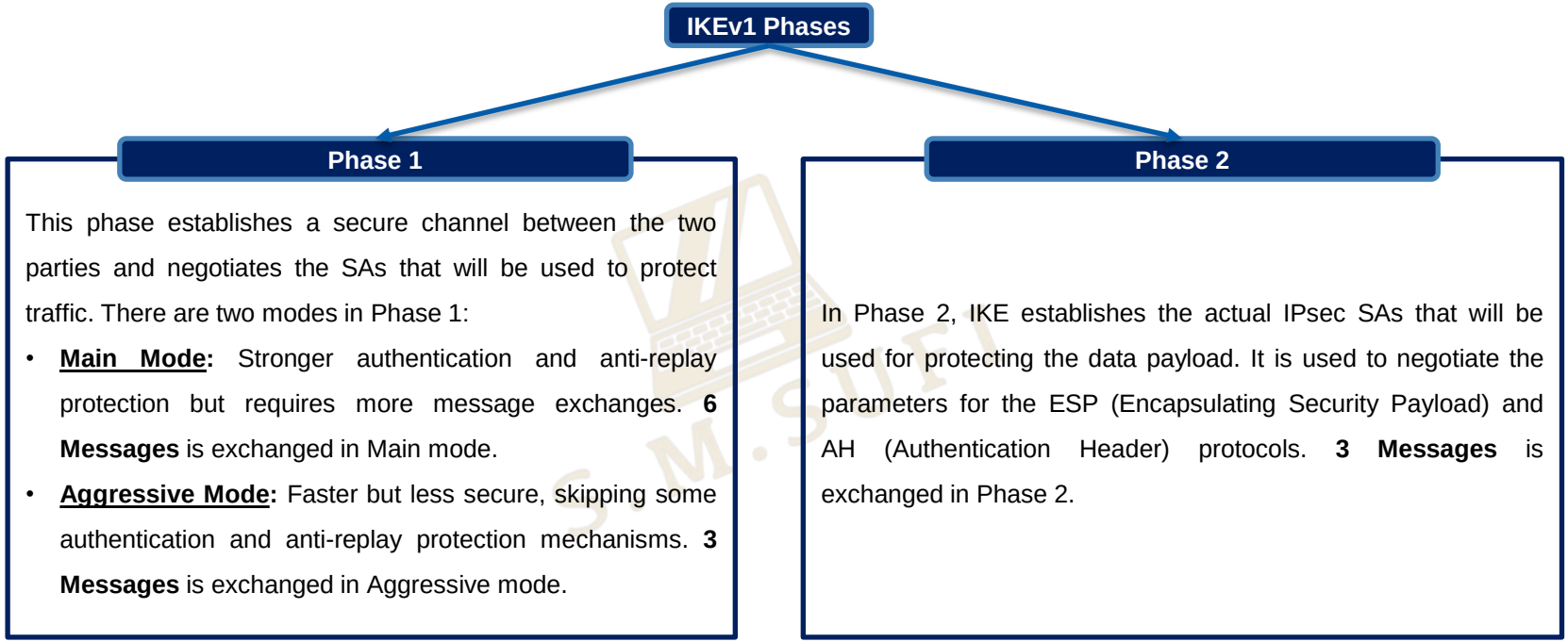
Internet Key Exchange (IKE) is a protocol suite used to securely establish shared secret keys between two parties over an insecure network, such as the Internet. It is a crucial component of IPsec (Internet Protocol Security) providing the foundation for secure communication by –

- Authenticating Peers
- Negotiating Cryptographic Parameters
- Establishing Security Associations (SAs)



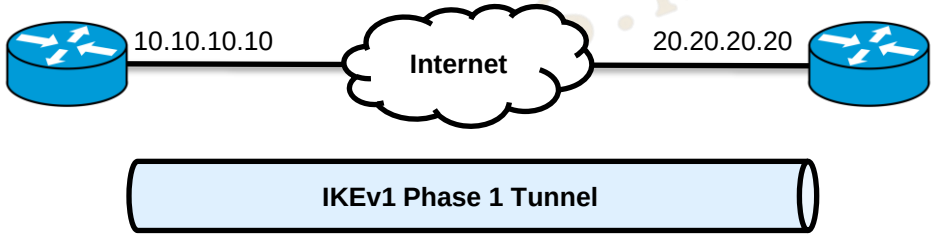
Back to Contents

IKEv1



IKEv1 Phase 1

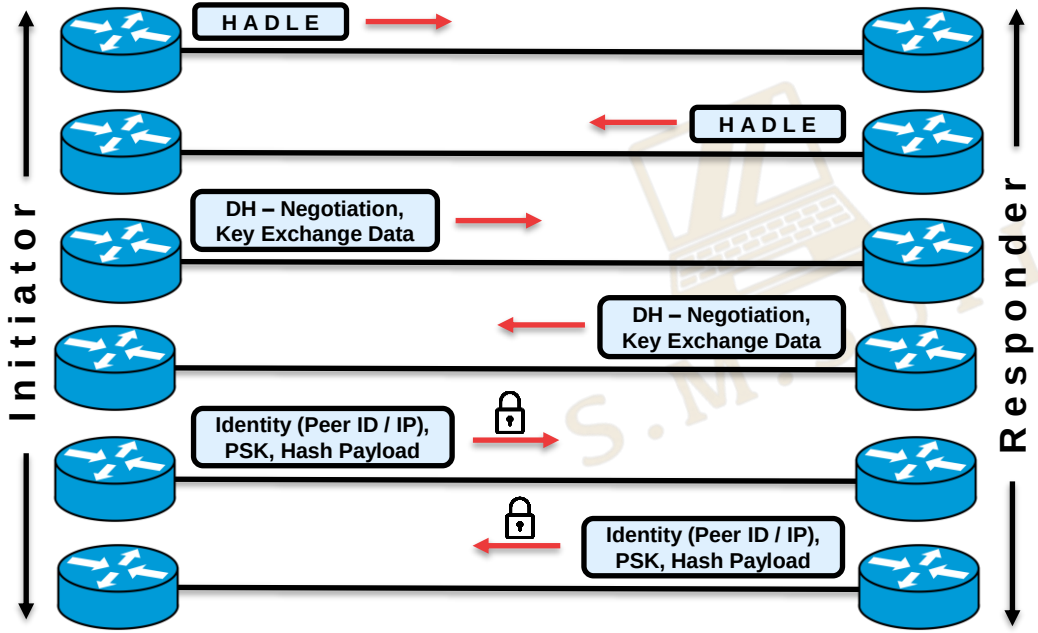
- In IKEv1 Phase 1, two peers will negotiate about the encryption, authentication, hashing and other protocols that they want to use and some other parameters that are required.
- An **ISAKMP (Internet Security Association and Key Management Protocol)** session is established. This is also called the **ISAKMP Tunnel** or **IKE Phase 1** tunnel.
- The collection of parameters that the two devices will use is called a **SA (Security Association)**.
- The IKE phase 1 tunnel is only used for **management traffic**. We use this tunnel as a *secure method to establish the second tunnel* called the **IKE Phase 2 Tunnel** or **IPsec Tunnel** and for management traffic like keepalives.
- The main purpose of IKE phase 1 is to establish a secure tunnel that we can use for IKE phase 2.
- IPSec is a **UDP** protocol and uses **Port 500** for IKE and **port 4500** for IPSec NAT-Traversal Mode.
- **HADLE** information is exchanged in the IPSec Phase Exchange Messages.



H	**Hash (Ex: SHA-256)**
A	**Authentication (Ex: PSK, Certificate)**
D	**Diffie-Hellman (Ex: Dh-Group 14)**
L	**Life Time (Ex: 8hr)**
E	**Encryption (Ex: AES-192)**

IKEv1 Phase 1 Main Mode

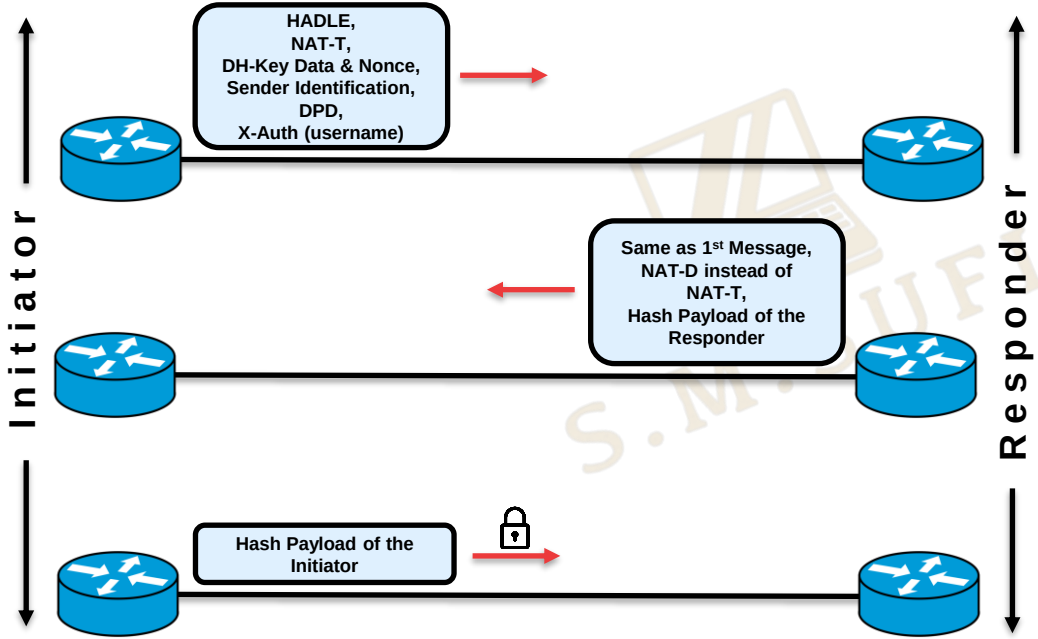
Total 6 Messages are exchange between peers in IKEv1 Phase 1 Main Mode. All the messages are illustrated below:



- Password doesn't go in the 1st & 2nd Message, just the algorithms are sent. The responder can sent more than one algorithms, but it should have at least one matching with the sender. Also Detects if both ends support NAT-T.
- Diffie-Hellman negotiation is happened in 3rd & 4th messages. Also if both devices support NAT-T, then NAT-D (Discovery) is performed.
- Identity like Peer ID or IP, Pre-Shared-Key, Hash Payload are exchanged in 5th & 6th messages. These two messages are in encrypted format.

IKEv1 Phase 1 Aggressive Mode

Total 6 Messages are exchange between peers in IKEv1 Phase 1 Main Mode. All the messages are illustrated below:



- 1st Message in Aggressive Mode is equivalent to first 4 messages in Main Mode.
- Nonce, NAT-T and NAT-D will be discussed later in this material. NAT-T is defined in RFC 3947.
- 3rd Message in Aggressive Mode is encrypted and we cannot read Hash Payload Data.

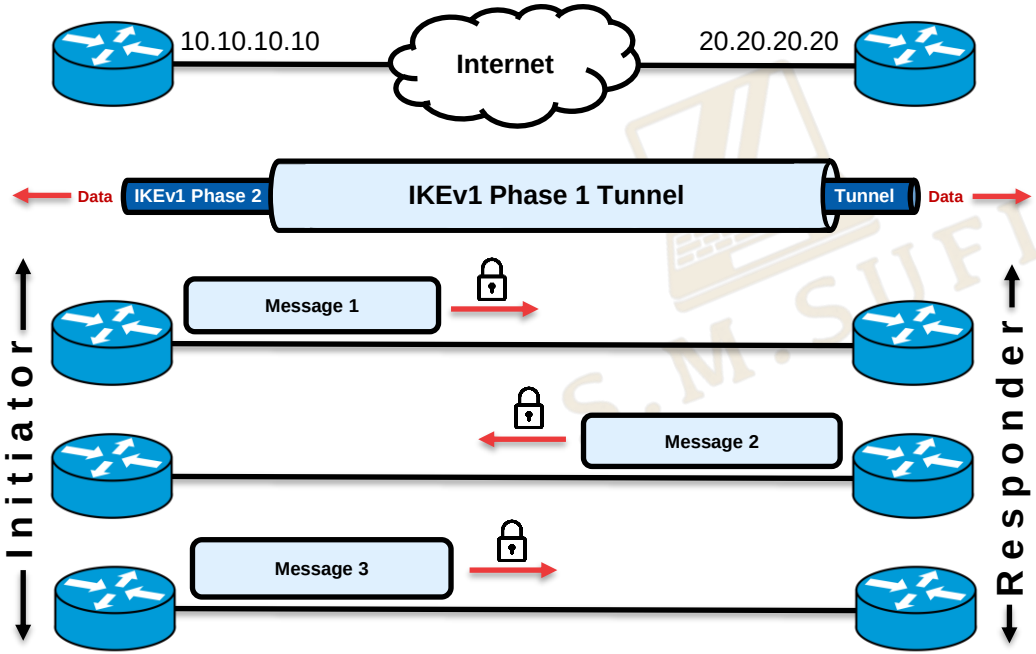
Back to Contents

Considerations Between Modes

Feature	Main Mode	Aggressive Mode
Message Exchange	6	3
Identification Exchange	Encrypted, in 5th and 6th messages	Un-encrypted, in 1st and 2nd messages
Security	More Secure	Less Secure
Man-in-middle Protection	Protected	Identity goes unencrypted
Replay Protection	Strong	Weak
Authentication	Strong	Weak
Speed	Slower	Faster
Complexity	More complex	Simpler
Dynamic Host	Not used	Used
Digital Signature	Used	Not used
Applications	VPNs, Secure Remote Access, Sensitive Data Transmission, Critical applications where security is the main concern, etc.	Mobile environment with frequent network change, Applications require low latency, Non-critical where speed is the main concern, etc.

IKEv1 Phase 2 Quick Mode

- The IKE phase 2 tunnel (IPsec tunnel) will be actually used to protect user data.
- There is only one mode to build the IKE phase 2 tunnel which is called **quick mode**.



Total 3 Messages are exchange between peers in IKEv1 Phase 2 Quick Mode.

The peers will negotiate about a number of items in phase 2:

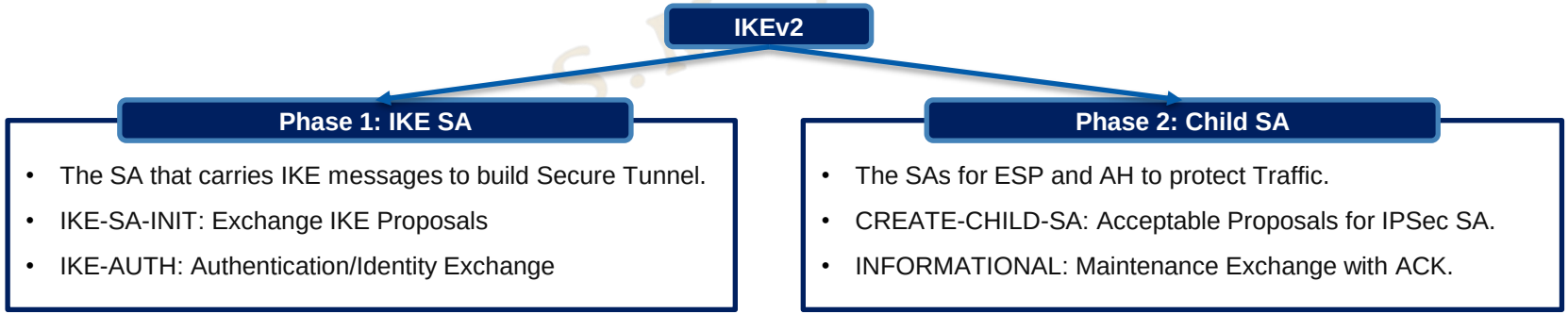
- **IPsec Protocol**: AH or ESP.
- **Encapsulation Mode**: Transport/Tunnel mode.
- **Encryption**: Encryption algorithms
- **Authentication**: Authentication algorithms
- **Lifetime**: Lifetime of the tunnel
- **(Optional) DH exchange**: Used for PFS (Perfect Forward Secrecy)

This negotiation happens within the protection of our IKE phase 1 tunnel encrypted, so we can't see anything.

Back to Contents

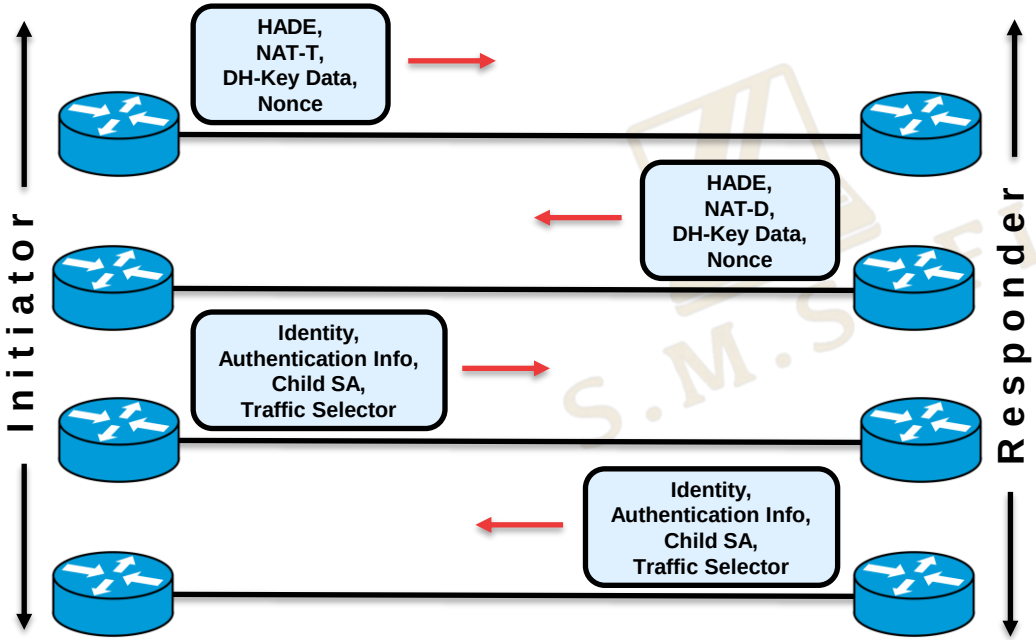
IKEv2

- Initially defined in **RFC 4306**, **RFC 5996**, **RFC 7296** and **RFC 7427**.
- Developed by Microsoft and Cisco.
- IKEv2 enhances the function of negotiating the dynamic key exchange and authentication of the negotiating systems for VPN.
- Exchange less messages than IKEv1. Thus simplifies SA negotiation and enhances negotiation efficiency.
- Runs over UDP ports 500 and 4500 (IPSec NAT Traversal).
- More resistant to DOS (Denial-of-Service) attacks with improved peer validation.
- Asymmetric authentication is supported. Such as- Certificate at one side PSK at other, Different PSK at the peers, etc.
- Built-in health keepalive check automatically re-establishes a tunnel if it goes down. It replaces the DPD in IKEv1.
- Not backwards compatible with different versions. Cannot run different IKE versions in two peers.



IKEv2 Phase 1 IKE SA

IKEv2 Phase 1 has a two step negotiation process. 2 Message exchanges happen between peers in IKEv2 Phase 1 **IKE_SA**. All the messages are illustrated below:



1ST and 2nd messages are **IKE_SA_INT**. It performs these functions -

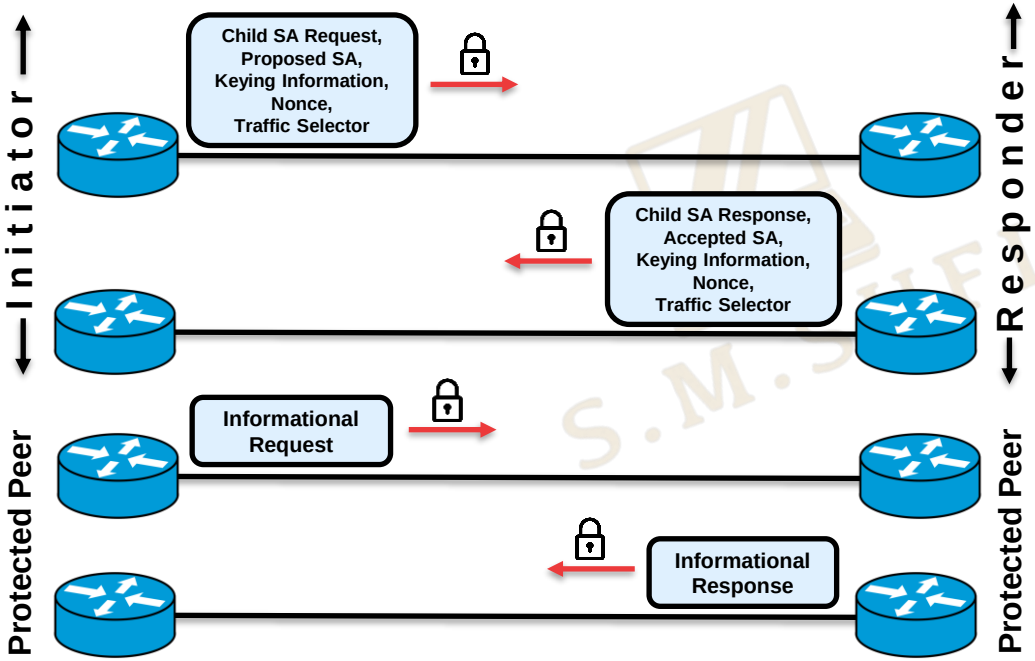
- Negotiates Security parameters for the IKE-SA
- Sends Nonces
- Sends Diffie-Hellman values

3rd and 4th messages are **IKE_AUTH**. It performs these functions –

- Authenticate remote peer by exchanging identities.
- Supports asymmetric & symmetric authentication (PSK and/or Certificate) and EAP.
- Establishes the first, and usually the only, AH and/or ESP CHILD-SA.
- Determines what traffic is allowed through the tunnel.
- Certificate exchange and configuration exchange (optional).

IKEv2 Phase 2 CHILD SA

There are also 2 Message exchanges happen in between peers in IKEv2 Phase 2 **CHILD_SA**. All the messages are illustrated below:



3rd and 4th message also include **CREATE_CHILD_SA** request, containing a list of acceptable proposals for the child SA. The attributes can be negotiated include-

- Protocol (AH or ESP)
- Encapsulation Mode (Tunnel or Transport)
- H A D E Information

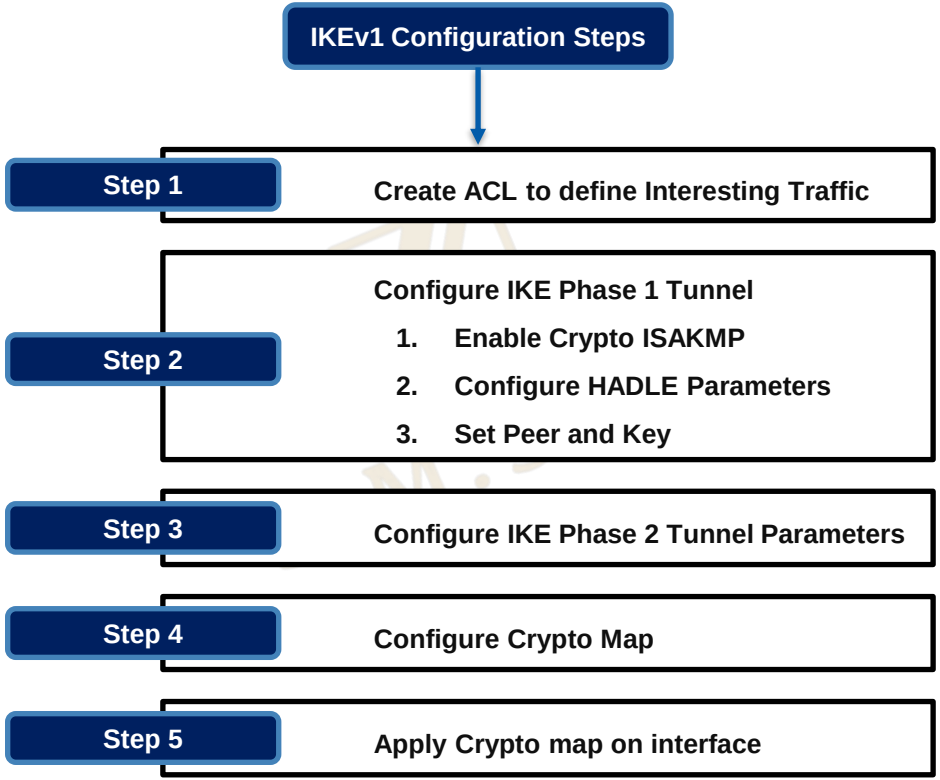
Responder picks a proposal that is acceptable and returns the choice in response.

After IPSec tunnel is formed, **INFORMATIONAL**, which is a maintenance exchange that performs a variety of functions to maintain the SAs including-

- Check SA liveliness, status and report error conditions (N)
- Delete SAs as needed (D)
- Exchange configuration information between IKE peers (CP) like REQUEST, REPLY, SET, ACK, etc.

Back to Contents

Basic Configuration



Thank You

Feel free to reach out to me for any **suggestions** or **feedback** via **LinkedIn** or **Mail**

 www.github.com/smsufi

 www.linkedin.com/in/smsufi

 safwanm.cse@gmail.com