JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# ROLE OF IPSEC IN NETWORK SECURITY

**Rajveer Kaur**

Assistant professor

School of Engineering

AIMETC, Jalandhar, Punjab

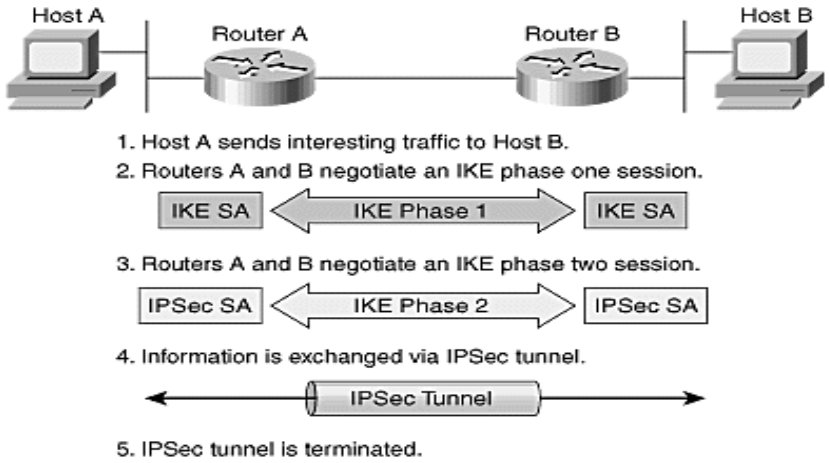
**Abstract**

IPsec (IP security) is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in a data stream. There are two modes of IPsec operation: transport mode and tunnel mode. In transport mode only the payload (message) of the IP packet is encrypted. It is fully-routable since the IP header is sent as plain text; however, it can not cross NAT interfaces, as this will invalidate its hash value. In tunnel mode, the entire IP packet is encrypted. It must then be encapsulated into a new IP packet for routing to work Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on Internet Engineering Task Force (IETF) standards.

## 1. Introduction

**Internet Protocol Security** (**IPsec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (*host-to-host*), between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host)* IPsec protects any application traffic across an IP network. Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft implementation of IPsec is based on Internet Engineering Task Force (IETF) standards

### 1.1 WORKING OF IPSEC




**Working of IPSec is Shown in Fig 1.01**

#### 1.1.1 Authentication Header (AH): Protocol – 51

Authentication Header (AH) provides authentication and integrity to the datagram passed between two systems. It achieves this by applying a keyed one-way hash function to the datagram to create a message digest.

If any part of the datagram is changed during transit, it will be detected by the receiver when it performs the same one-way hash function on the datagram and compares the value of the message digest that the sender has supplied. The one-way hash also involves the use of a secret shared between the two systems, which means that authenticity can be guaranteed.

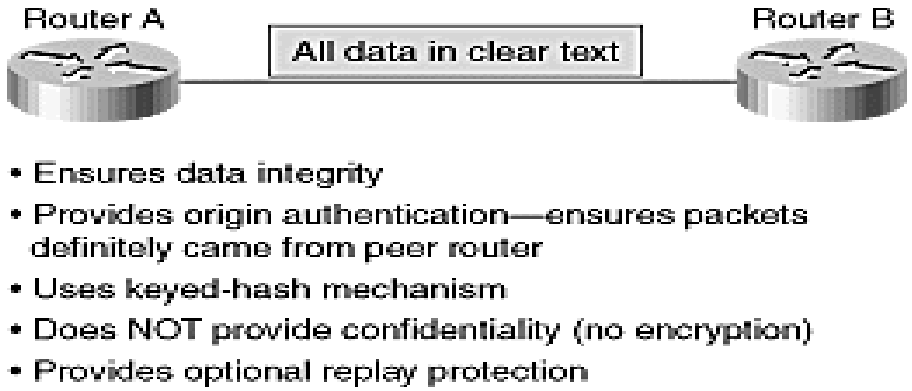



**Fig 1.02 Authentication Header (AH) Protocol-51**

**1.1.1.1 Encapsulating Security Payload (ESP): Protocol – 50**

Encapsulating Security Payload (ESP) provides data confidentiality, data integrity, authentication and anti-replay services. It does not use a transport protocol like TCP or UDP; it rides directly on top of IP using protocol number 50.

ESP uses symmetric key algorithms like DES, 3DES, or AES, and hash methods like MD5 and SHA-1 to provide security services.

Anti-replay services ensure that datagram cannot be captured by a third party and re-transmitted. By checking sequence numbers, a receiver can determine whether a packet has already been receive and discard any repetitions.

ESP provides confidentiality by performing encryption at the IP packet layer. It supports a variety of symmetric encryption algorithms. The default algorithm for IPSec is 56-bit DES. This cipher must be implemented to guarantee interoperability among IPSec products. Cisco products also support use of 3DES for strong encryption. Confidentiality can be selected independent of all other services.

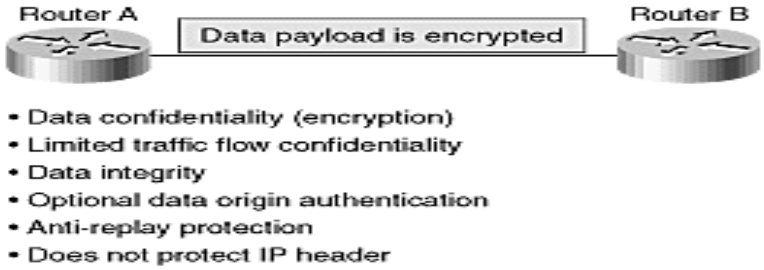



**Fig 1.1.1.1 Encapsulating Secuirty payload (ESP) Protocol-50**

**2. Secuirty using IKE**

Internet Key Exchange is a secure key management protocol used by IPsec to have information exchanged in a secure and dynamic manner with little or no intervention. IKE proposal exchange is the phase one of the IPSec tunnel establishment process. The following attributes are exchanged between IPSec peers as a part of the IKE process

- Encryption algorithm
- Hash algorithm
- Authentication method
- Diffie-Hellman group

Once these attributes are negotiated between the IPSec peers, it is used to secure future attribute exchanges that are used to protect data. IKE exchanges are authenticated using one of the following

Methods:

- Pre-shared keys
- Digital signatures
- Public key encryption

IKE is preferred over manual keys in IPSec implementations because of the ease of management and scalability.

## 2.1 IPSEC MODES

### 2.1.1 AH Tunnel Versus Transport Mode

Figure 1-7 shows the differences that the IPSec mode makes to AH. In transport mode, AH services protect the external IP header along with the data payload. AH services protect all the fields in the header that do not change in transport. The AH goes after the IP header and before the ESP header, if present, and other higher-layer protocols.

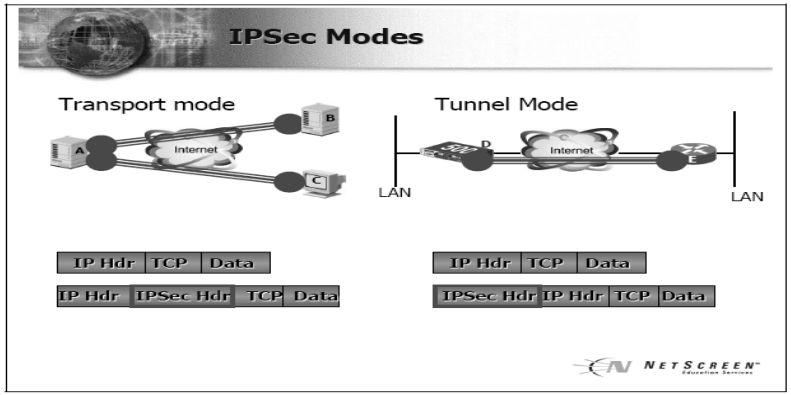



**Fig 2.1.1 IPSec Modes**

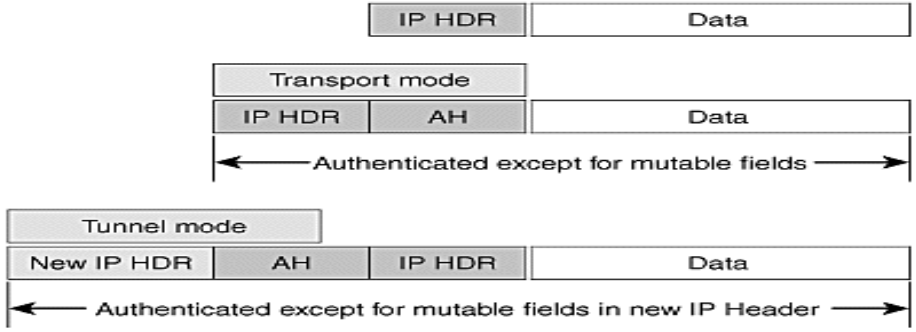



**Figure 2.1.2 AH Tunnel Versus Transport Model**

In tunnel mode, the entire original header is authenticated, a new IP header is built, and the new IP header is protected in the same way as the IP header in transport mode.

AH is incompatible with Network Address Translation (NAT) because NAT changes the source IP address, which will break the AH header and cause the packets to be rejected by the IPSec peer.

### 2.1.1.1 ESP Tunnel Versus Transport Mode

Figure 1-8 shows the differences that the IPSec mode makes to ESP. In transport mode, the IP payload is encrypted and the original headers are left intact. The ESP header is inserted after the IP header and before the upper-layer protocol header. The upper-layer protocols are encrypted and authenticated along with the ESP header. ESP does not authenticate the IP header itself. Please note that higher-layer information is not available because it is part of the encrypted payload.

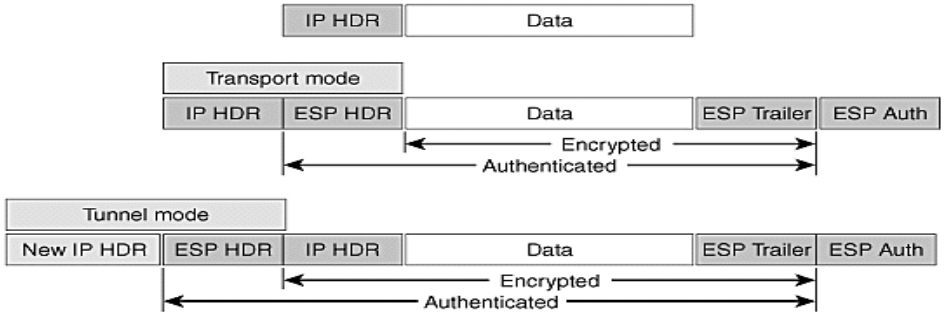



**Figure 2.1.1.1 ESP Tunnel Versus Transport Model**

When ESP is used in tunnel mode, the original IP header is well protected because the entire original IP datagram is encrypted. With an ESP authentication mechanism, the original IP datagram and the ESP header are included; however, the new IP header is not included in the authentication.

When both authentication and encryption are selected, encryption is performed first, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node. Before decrypting the packet, the receiver can detect the problem and potentially reduce the impact of denial-of-service attacks.

ESP can also provide packet authentication with an optional field for authentication. Cisco IOS software and the PIX Firewall refer to this service as ESP HMAC. Authentication is calculated after the encryption is done. The current IPSec standard specifies SHA-1 and MD5 as the mandatory HMAC algorithms.

The main difference between the authentication provided by ESP and that provided by AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). Figure 1-9 illustrates the fields protected by ESP HMAC.

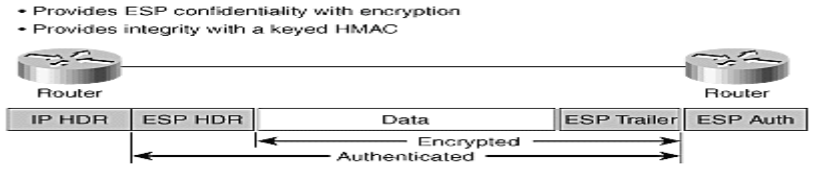



**Figure 2.1.1.2 ESP Encryption with a Keyed HMAC**

**3. Encryption Algorithms**

**3.1 Digital Encryption Standard (DES):**DES uses a 56-bit key, ensuring high-performance encryption. DES is used to encrypt and decrypt packet data. DES turns clear text into ciphertext with an encryption algorithm. The decryption algorithm on the remote end restores clear text from ciphertext. Shared secret keys enable the encryption and decryption.

**3.1.1 Triple Digital Encryption Standard (3DES)**

Triple DES (3DES) is also a supported encryption protocol for use in IPSec on Cisco products. The 3DES algorithm is a variant of the 56-bit DES. 3DES operates similarly to DES in that data is broken into 64-bit blocks. 3DES then processes each block three times, each time with an independent 56-bit key. 3DES effectively doubles encryption strength over 56-bit DES.

*** Advanced Encryption Standard – 128 bit key (AES-128)**

*** Advanced Encryption Standard – 256 bit key (AES-256)**

*** CAST Encryption**

**3.1.1.1 Hashing Algorithms**

**MD5**

Message Digest 5 (MD5) is a hash algorithm used to authenticate packet data. Cisco routers and the PIX Firewall use the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. A hash is a one-way encryption
algorithm that takes an input message of arbitrary length and produces a fixed length output message. IKE, AH, and ESP use MD5 for authentication.

**Secure Hash Algorithm Version1 (SHA1)**

-Secure Hash Algorithm-1 (SHA-1) is a hash algorithm used to authenticate packet data. Cisco routers and the PIX Firewall use the SHA-1 HMAC variant, which provides an additional level of hashing. IKE, AH, and ESP use SHA-1 for authentication.

**4. Methods of Encryption/integrity for IKE**

| **Parameter** | **IKE Phase I (IKE SA)** | **IKE Phase II (IPSecSA)** |
|---|---|---|
| Encryption | AES -256(default)<br>3 DES<br>DES<br>CAST | 3DES<br>AES-128(default)<br>DES<br>NULL |
| Integrity | MD5<br>MD5<br>SHA1 (default) | MD5(default)<br>MD5(default)<br>SHA1 |

**DH Groups**

| **Parameter** | | |
|---|---|---|
| Diffie Hellman Groups | Group2 (1024 bits) (default)<br>Group1 (768 bits)<br>Group5 (1536 bits)<br>Group14 (2048 bits) | Group2 (1024 bits) (default)<br>Group1 (768 bits)<br>Group5 (1536 bits)<br>Group14 (2048 bits) |

**Fig 4.1 IKE Phase I**

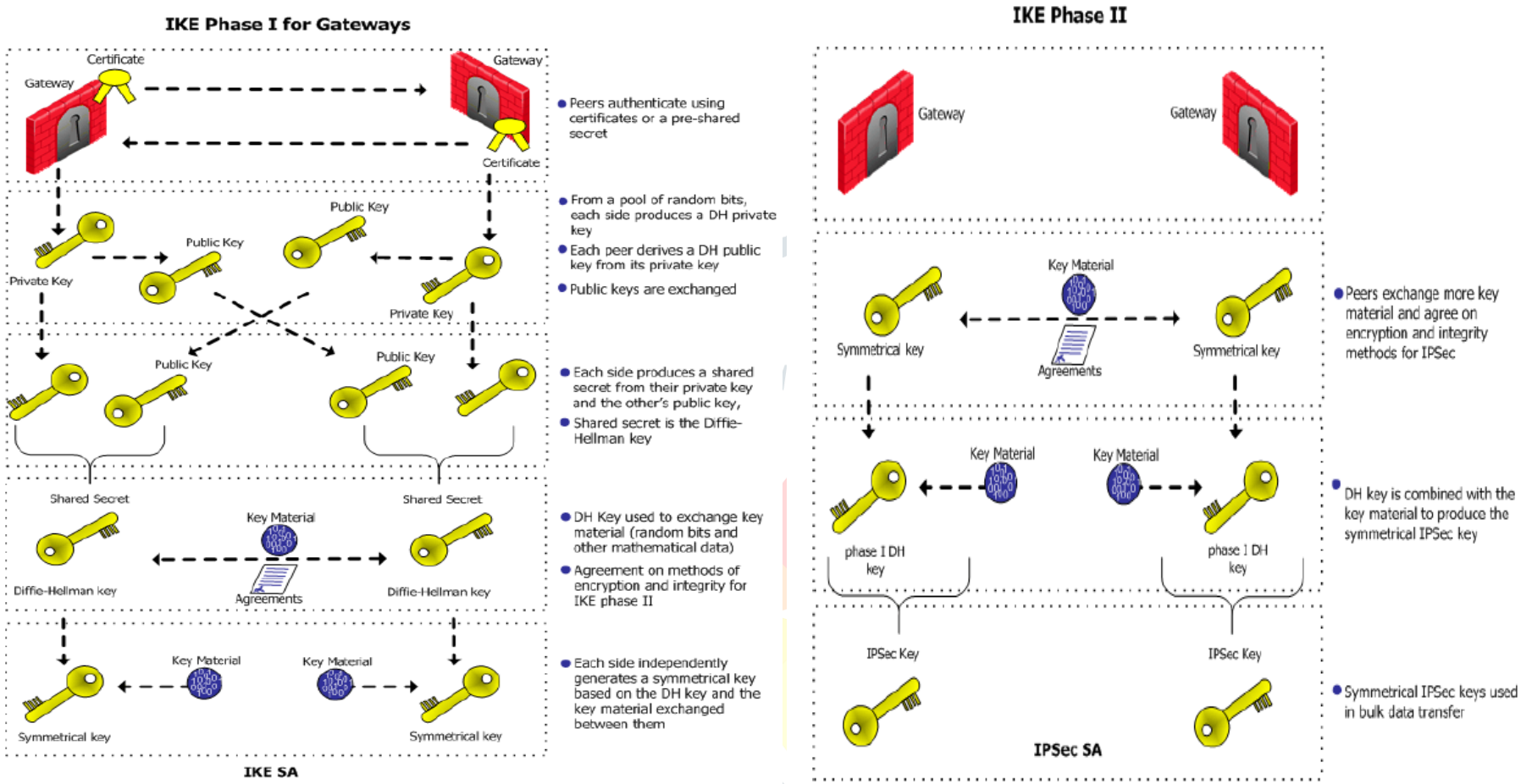



**Fig 4.2 IKE Phase II**

## 5. MODELS

### Phase I modes

VPN-1 Power supplies two modes for IKE phase I between Gateways:

- Main Mode
- Aggressive Mode

**Phase II modes**

- Quick Mode

Phase 1 establishes a secured channel between gateways for Phase 2 negotiations to occur. The Diffie-Hellman key exchange algorithm is used to establish a shared key for encryption.

Phase 2 establishes the specific VPN connections. Security Associations (SAs) are negotiated to determine the encryption and authentication algorithms to be used when sending user data. The

SA is identified by a unique SPI, which is also negotiated during Phase 2. A single Phase 1 channel can be used to establish multiple Phase 2 SAs or VPNs. When for example, the specifications for the NS5XP is a limit of 10 tunnels, it means 10 IKE Phase 1 gateways. If desired, a second Diffie-Hellman exchange can be performed during Phase 2 to negotiate a new tunnel key. Because this exchange is encrypted, this is called Perfect Forward Secrecy.

**IKE Phase 1: Main Model**

IKE Main Model is used when both tunnel peers have static IP addresses. The Phase 1 exchange determines the following attributes.

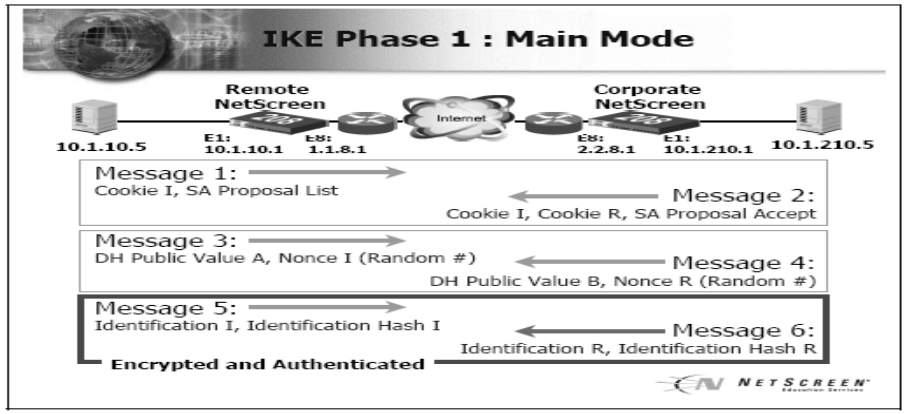



**Fig 5.1 Models**

The first two messages validate the peer configuration (by checking the cookie against the locally configured peer IP address), and negotiate the above parameters. Both tunnel peers must have at least one matching proposal configured in order for the Phase 1 exchange to be successful.

The next two messages exchange Diffie-Hellman public key values and nonces necessary to compute the shared key.

The last two messages send simple identification information using the negotiated key; these messages validate that the key was calculated properly.

**Message 1 & Message 2**

Peers exchange cookies and SA proposals. Cookies are 8 byte pseudo-random numbers generated by the sending machine. (I=Initiator) and receiving machine (R=Receptor). Every cookie is unique to the machine and to each particular exchange. This guarantees uniqueness and replay protection by hashing the sender's IP address, port, protocol and timestamp

which results in a unique identifier known only to the originator. Hence, they are included in every IPsec packet and used to identify the communication. In turn, the Receptor will insert it's known

cookie in Message 2 if it accepts the SA proposal. The Initiator would see that the cookies from both parties would not match if a man-in the-middle generated numerous false messages with a false return address. When the Initiator receives the 2nd message with a cookie that is not its own, the communication is simply stopped; further messages are not sent. The NetScreen supports up to 4 SA proposals. An IPsec SA proposal will contain the following:

Phase 1 Authentication Method (main or aggressive mode)

Diffie-Hellman Group Number

Encryption Algorithm
Authentication Algorithm
Key Lifetime

**Message 3 and Message 4**

Now the Diffie-Hellman public values are exchanged to create a common session key. Nonces, which are essentially random numbers, are also exchanged at this time to be used as seeds for keys generated later.

After both sides have exchanged their Diffie-Hellman public values, a key is created on each side to encrypt the rest of the IKE Phase 1 messages. The session key is a result of the exchanged public keys being sent to each partner.

**Message 5 and Message 6**

Messages containing the preshared key, Diffie-Hellman session key, cookies, and nonces are exchanged to verify identity and validate the new session key.

**IKE Phase 1: Aggressive Model**

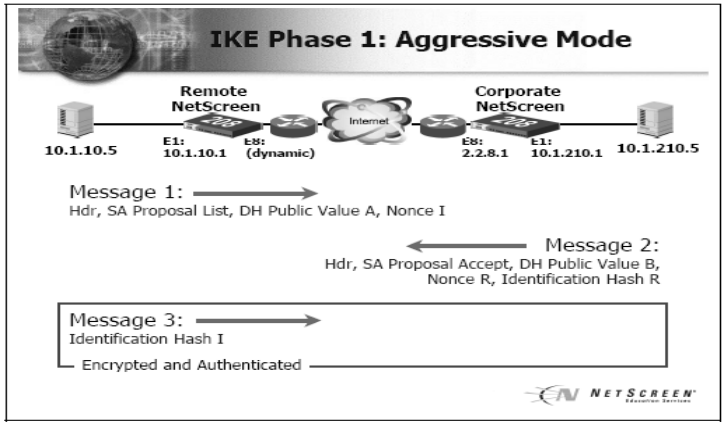



**Fig 5.2 Aggressive mode**

IKE Aggressive mode is used when one of the tunnel peers has a dynamic IP address. This could be a remote end user dialing in to the Internet, or a remote site using DHCP to acquire an IP address.

(Main mode cannot be used because the first two messages validate peer IP addresses. In the case of a dynamic host address, the address cannot be preconfigured at the peer.)

Phase 1 Aggressive mode must be initiated by the device with the dynamic IP address. The first two messages negotiate policy, exchange Diffie-Hellman public values and nonces. In addition thesecond message authenticates the responder; the ID hash is compared with the locally-configured peer ID.

The third message authenticates the initiator and provides a proof of participation in the exchange.

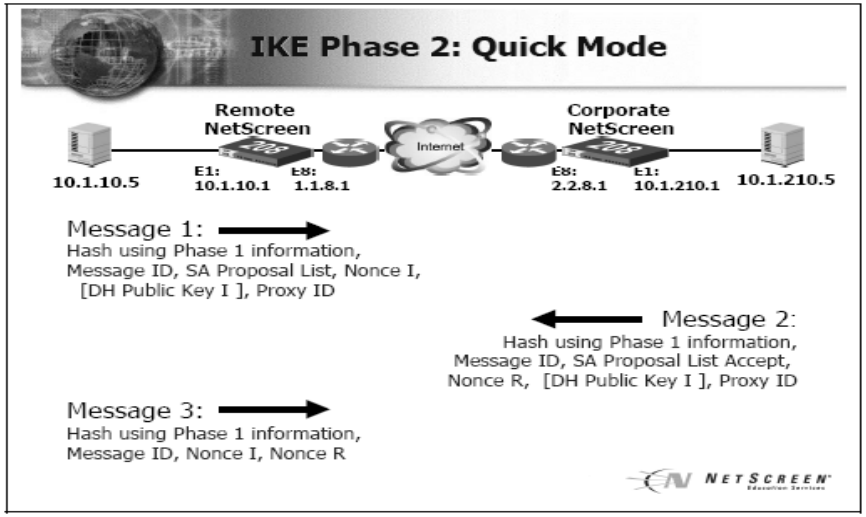



**Fig 5.3 Quick mode**

Once Phase 1 is complete, proposals are exchanged to establish a specific VPN. The following attributes are negotiated in phase 2:

- Security protocol (ESP or AH)
- Tunnel or transport mode
- Proxy-ids
- Optional DH group.

Upon successful completion of quick mode, user data will be encrypted between the configured IPSec peers. Both tunnel peers must have at least one matching proposal configured in order for the Phase 2 exchange to be successful.

The result of Phase two is to create an IPSec VPN for user data to be securely transmitted through the network.

**Message 1 and Message 2**

A Phase 2 proposal list is exchanged which contains encrypted and authenticated information that will determine the algorithms and keys for encrypting/authenticating user data.

Again, up to four proposals can be exchanged and as long as 1 proposal is acceptable then Phase 2 continues to message 3.

The Phase 2 Proposal list contains:

- ESP or AH

- Diffie-Hellman Group Number (0 for No PFS)
- Encryption Algorithm
- Authentication Algorithm
- Key Lifetime
- Proxy ID (Policy Rule)
- Diffie Hellman Public Keys (Optional if using PFS)

**Message 3**

Used to acknowledge information sent from Quick Mode message 2 so that the Phase 2 tunnel may established.

## 6. CONCLUSIONS

It can be argued that the solution so proposed will not create additional load affecting the network performance. But the final question that remains is if the users are ready to choose speed over security. Or to sacrifice some amount of speed to operate in rather a secure network environment. This debate can go on forever.

## 7. References

TRIVEDI, Kaushal" Based Network Access Control", IEEE Std 802.1X-2004, IEEE Standard for Local and metropolitan area networks, PortCSCI 693 Research Paper: 34.

Geier, J (2007 ) "802.1X Offers Authentication and Key Management." *Wi-Fi Plane.t*

Sutton, M (2008) "Hacking the Invisible Network-Insecurities in 802.11x",

Barken L, Bermel E (2004) *"Wireless Hacking: Projects for Wi-Fi Enthusiastics"*, Syngress Publishing , 1st ed. Rockland , pp. 29-348.

Conti, G ( 2006) "Why Computer Scientists Should Attend Hacker Conferences," *Comm. ACM*, vol.48, no. 3, gregconti publications 20050301_CACM_HackingConferences_Conti.pdf.

Gregg, M (2006) "*Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network"*, Syngress.

Vladimirov A. A, Gavrilenko K. V, and Mikhailovsky, A. A(2004), "*Wi-Foo: The Secrets of Wireless Hacking"*, 1st ed. Boston: Addison Wesley, pp. 42-500.

Potter, B "Wireless Security Future," *IEEE Security &Privacy*, vol. 1, no. 4, 2003, pp. 68-72.

Sheetal, J (2008) "Wireless Security," presented at OWASP Conference, Tech Mahindra, Mumbai, India, Available: http://www.owasp.org.