KRISH SRIVASTAVA — AP21110010802
PRADIP KUMAR GIRI — AP21110010999
AYUSH SINGH RATHORE — AP21110010570

Page No.:
Date:
YOUVA

* IP Sec Class Assignment

Q1)

→ An end user whose system is equipped with IP sec protocols can make a local call over the internet: An end user whose system is equipped with IP sec protocols can make a local call to ISP and gain access to a company corporate network

1) Specifies the traffic and level of security required.
2) Configure Security Association (both on remote server and client).
3) Choose an authentication method for verifying identities.
4) Configure IKE for key generation and exchange.

Q2)

→ IPSec adds processing overhead for encryption & decryption, potentially impacting network performance.

1) Hardware ~~Acceleration~~ Decolaration → Utilize hardware based ~~acceleration~~ encryption features on routers or VPN appliances to offload processing from the CPU.

2) Strong Ciphers → While stronger ciphers offer better security, choosing a balance

3) Optimize key exchange → Techniques like pre-shared keys can streamline IKE negotiation, reducing overhead

AP21110010999
Pradip Kumar Giri
AP21110010302
Krish Srivastava
Ayush Singh Rathore (AP21110010570)
AP21110010570

5) Phase 1: IKE SA (Security Association) Establishment.

i. Initiation:
- Alice & bob both initiate the IKE negotiation process
- They exchange ISAKMP messages to establish a secure channel.
- They agree on parameters (encryption algorithms, authentication method, etc).

ii. Key exchange:
They perform a Diffe-Hellman key exchange to generate shared secret material.

iii. SA Establishment:
Using the shared secret, they establish the IKE SA.

Phase 2: IPSec SA Establishment

i. Proposal and selection:
Alice & Bob negotiate parameters for IPsec, like encryption algorithms.

ii. Authentication:
They authenticate each other using established IKE SA.

iii. Key Material Generation:
Based on negotiated parameters, they generate key material.

iv. SA establishment:
Using the key material, they establish the IPsec SA for secure data exchange.

Page No :
Date :

Pradip Kumar Giri (AP21110010999)
Krish Srivastava (AP21110010302)
Ayush Singh Rathore (AP21110010570)

4) Comparision of Main and Aggressive Mode in IKE Phase 1:

Main mode:

- Step count: Involves three pairs of messages exchanged between the parties (6 messages)
- Security: Offers higher security because it provides more opportunities for negotiation & key exchange.
- Speed: Slower compared to Aggresive Mode due to the higher no. of messages exchanged.

Aggressive Mode:

- Step count: Involves a single pair of messages exchanged between the parties (3 messages)
- Security: Offers lower security compared to Main mode as it reveals more info. during the negotiation process.
- Speed: Faster compared to Main mode due to the lower no. of messages exchanged.

Network Security

Ayush Singh Rathore
AP21110010570

Pradip Kumar Giri
AP21110010999

Krish Srivastav
AP21110010302

5. ESP & AH

→ Differences between AH & ESP.

Authentication Header	Encapsulating Security Payload
• AH provides data integrity data origin authentication and anti-replay protection for IP packets.	• ESP provides confidentiality data integrity, data origin authentication.
• AH Does not provide Confidentiality; the original IP Packet is not encrypted	• It achieves Confidentiality by encrypting the entire IP payload. Using symmetric encryption
• AH typically used in scenerios where data integrity & authentication are paramount, but confidentiality is not required	• used in scenerios where both integrity & confidentiality is required.

* Circumstances when AH prefer over ESP
  → when primary concern is ensuring data integrity & authentication.
  → in situation where compatibility with legacy systems that only support AH is required.

* when ESP prefer over AH
  → confidentiality is required along with integrity.
  → for ensuring VPN connection over untrusted network.