Virtual Private Networks with IPsec

Chapter 6

Network & Security

Gildas Avoine

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

SUMMARY OF CHAPTER 6

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

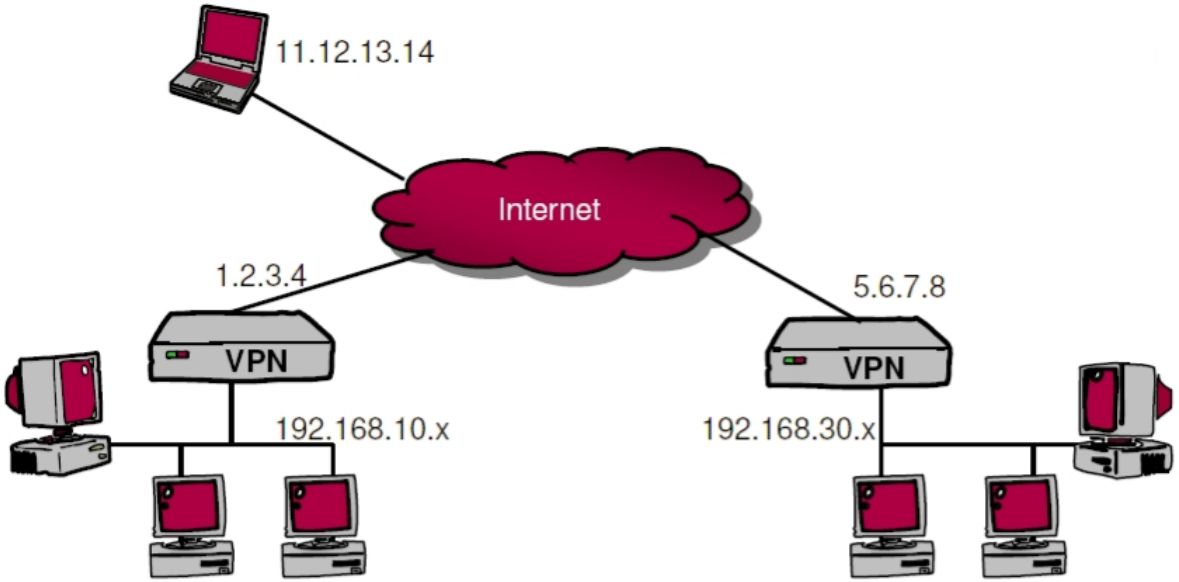
VPN PRIMER AND IPSEC PRIMER

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

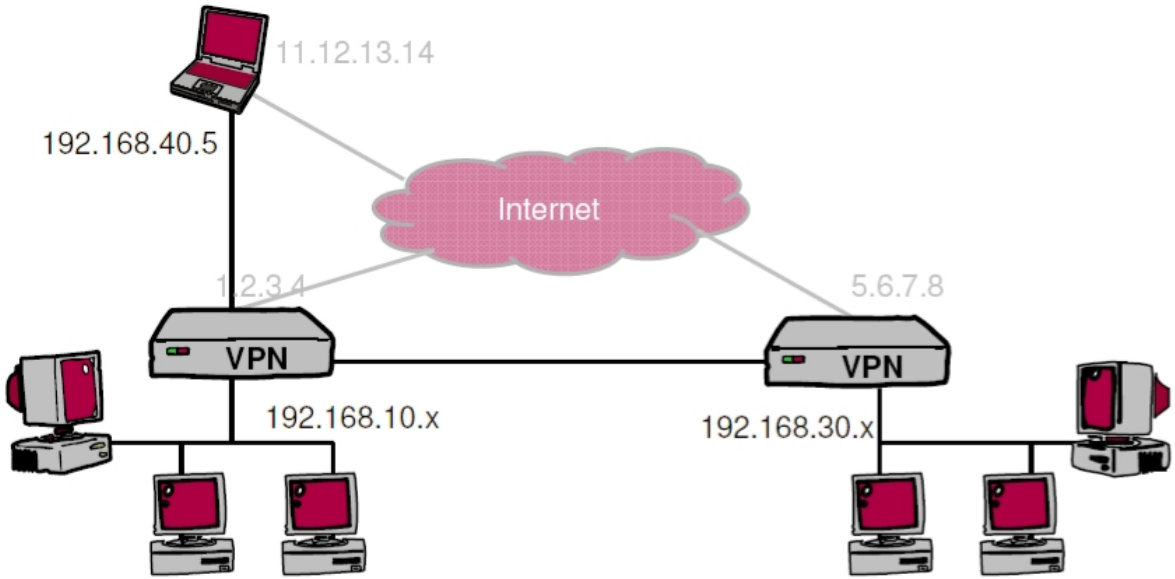
VPN Objectives

- VPNs extend a private network across a public network.
- VPN software on routers or workstations (eg. laptop).
- Packet encapsulation for their journey across the Internet.
- Scenarios.
  - Interconnection of distant sites through the Internet.
  - Connection of an itinerant laptop to a private network.

Connection without VPN



Connection with VPN



Existing Protocols

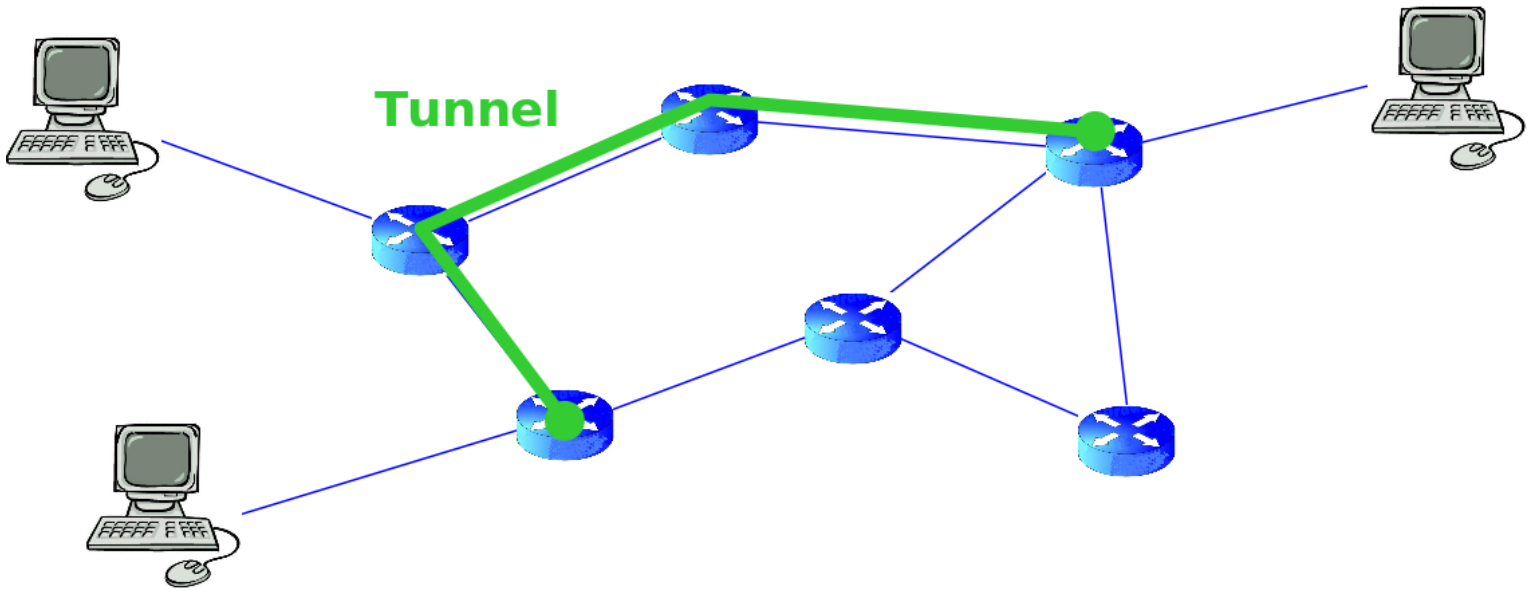
- Microsoft: PPTP (Point to Point Tunneling Protocol).
- IETF: L2TP (Layer 2 Tunneling Protocol).
  - Result of merging Cisco's L2F (Layer 2 forwarding) protocol and Microsoft's PPTP protocol.
- IETF: IPsec (IP Security), around 1993.

IPsec Basics

- THE standard VPN protocol.
  - Standard developed by the IETF.
  - Open and extendable format.
  - Public algorithms for confidentiality, authentication, integrity.
- Two operation modes: tunnel, transport.
- Two secure protocols: ESP, AH.
- A key exchange protocol: IKE (out of the lecture's scope).

Routing

- Operation modes:
  - Transport: only protects the packet's payloads.
  - Tunnel: the entire packet is encapsulated in a new packet.



SECURITY POLICY DATABASE AND SECURITY ASSOCIATIONS

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

Security Policy Database

- A Security Policy Database describes what should be protected.
- Each router contains such an SPD defining which packet needs to be secured, according to destination address, source address, protocol, etc.
- Examples.
  - Secure all traffic.
  - Secure packets sent to bank offices but not to internet.
  - Secure UDP.
  - Secure TCP but not SSL.

Security Associations (1/2)

- A Security Association describes how the traffic should be protected.
- For each protected communication, the SA memorizes the algorithms, the keys, the validity periods of the keys, the sequence numbers and the partner's identity.
- One SA for each unidirectional flow: a TCP connection requires a SA for each direction.
- One SA per destination, per protocol (AH or ESP), per port.

Security Associations (2/2)

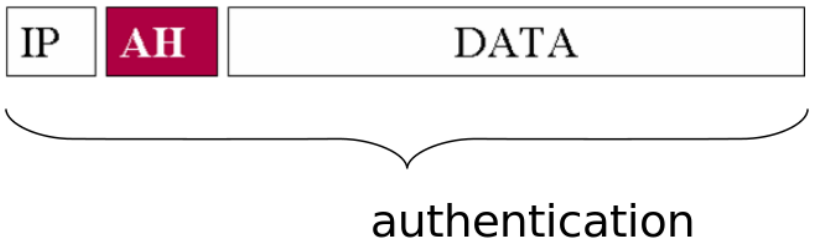
- Source decides which packets must be processed with which SA.
- SAs are identified by a Security Parameter Index (SPI).
  - The source indicates the SPI on all packets that it sends.
  - The destination uses the SPI to find the SA that describes how to deal with a received packet.
- Computers establish Security Associations (SA) using the protocol IKE.

AH AND ESP

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

Authentication Header (AH)

- The addition of an authentication header allows the recipient to verify the packet's authenticity and integrity.



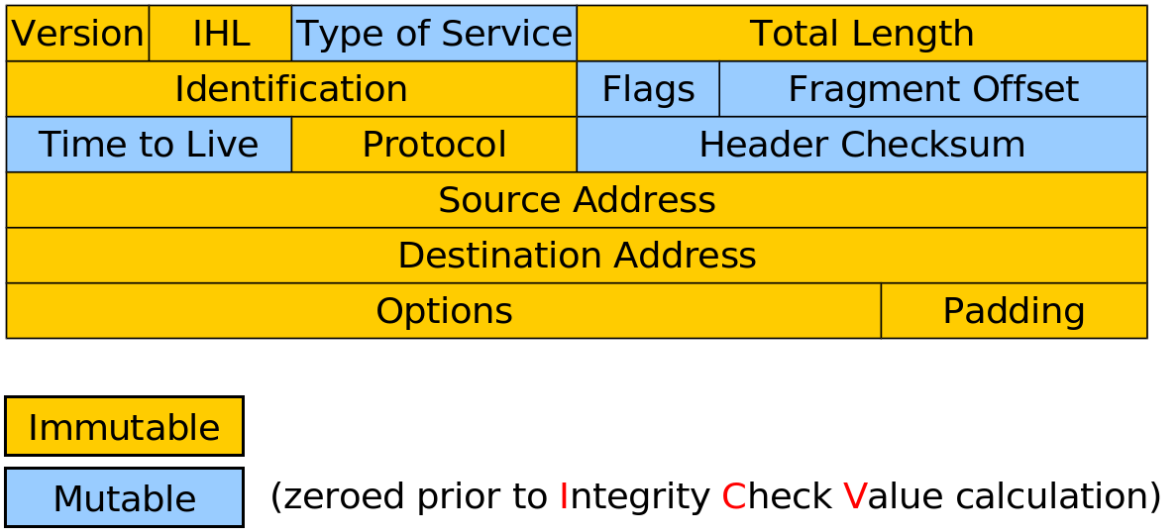
Authentication Header (AH)

Authentication Header format																															
Offsets	$Octet_{16}$	0								1								2								3					
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	*Next Header*								*Payload Len*								*Reserved*															
4	32	*Security Parameters Index (SPI)*																															
8	64	*Sequence Number*																															
C	96	*Integrity Check Value (ICV)*																															
...	...	...																															

- Next Header. 8 bits. Specifies the next encapsulated protocol (ICMP, TCP, UDP,...).
- Length. 8 bits. Size of the Authentication Data payload.
- Security Parameters Index. 32 bits. Contains a pseudo random value used to identify the security association for this datagram.
- Sequence number. 32 bits. Avoid replay-attacks.
- Authentication Data. Variable length. This field must contain a keyed-hash value that is a multiple of 32-bit words.

Authentication Header (AH)

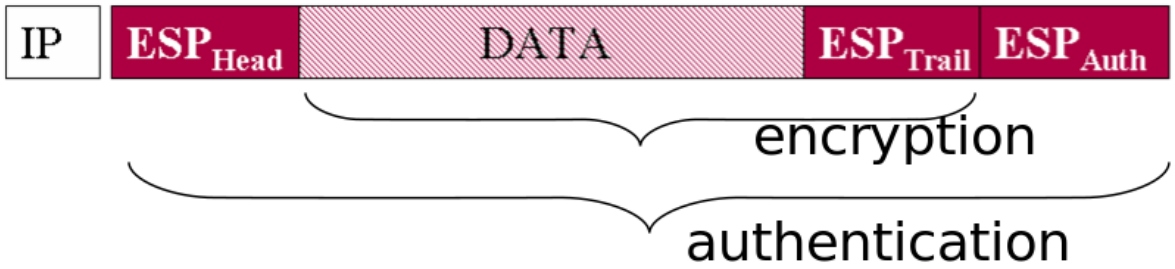
- Authentication is calculated on the following information.
  - The data that follow the AH.
  - The AH header itself: the authentication field is set to zero to compute the authentication data.
  - The important fields of the IP header: source, destination, protocol, length, version, etc.



Authentication Header (AH)

- The algorithm used to generate the authentication data is negotiated when the SA is created.
- Two algorithms must be available.
  - HMAC-SHA-96.
  - HMAC-MD5-96.
- HMAC(K,m) = H((K xor opad) II H((K xor ipad) II m))
- HMAC-SHA1-96 denotes HMAC computed with H=SHA1 and output truncated to 96 bits.

Encapsulated Security Payload (ESP)



- The ESP header allows packet encryption and authentication.
- Encryption is done only on the encapsulated data and the trailer, not on the header's fields.
- Optional authentication is done on the ESP header and all that follow, but not on the IP header.

Encapsulated Security Payload (ESP)

Encapsulating Security Payload format																															
Offsets	**Octet$_{16}$**	**0**								**1**								**2**								**3**					
Octet$_{16}$	**Bit$_{10}$**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
0	**0**	*Security Parameters Index (SPI)*																													
4	**32**	*Sequence Number*																													
8	**64**	*Payload data*																													
...	**...**																														
...	**...**									*Padding (0-255 octets)*																					
...	**...**																														
...	**...**																	*Pad Length*								*Next Header*					
...	**...**	*Integrity Check Value (ICV)*																													
...	**...**	...																													

Encapsulated Security Payload (ESP)

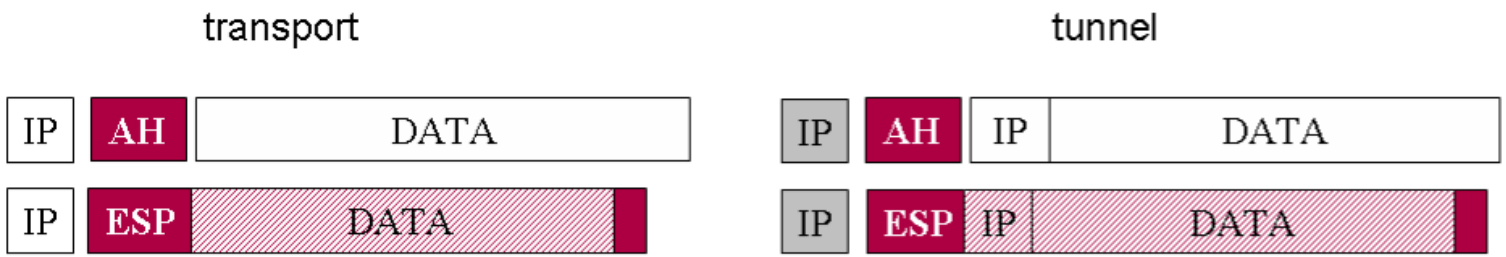
- The mandatory algorithms are:
  - Encryption: DES-CBC, NULL (RFC 2410).
  - Authentication: HMAC-SHA-96 (RFC2404), HMAC-MD5-96 (RFC2403), NULL.
- NULL encryption and NULL authentication in the same SA is not allowed.

TRANSPORT AND TUNNEL MODES

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

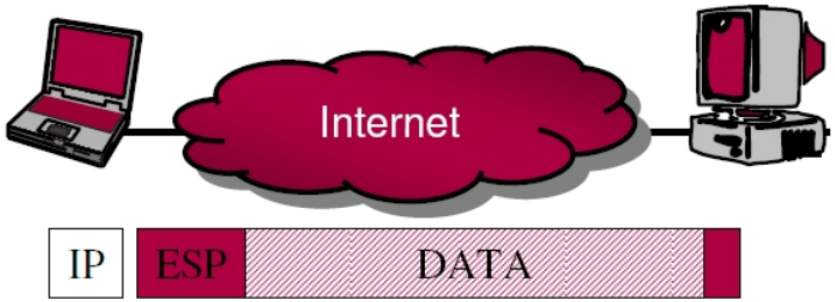
Transport/Tunnel vs AH/ESP

- Transport mode:
  - Data in the IP packet is encrypted and/or authenticated.
- Tunnel mode:
  - The entire packet is encapsulated in a new packet.



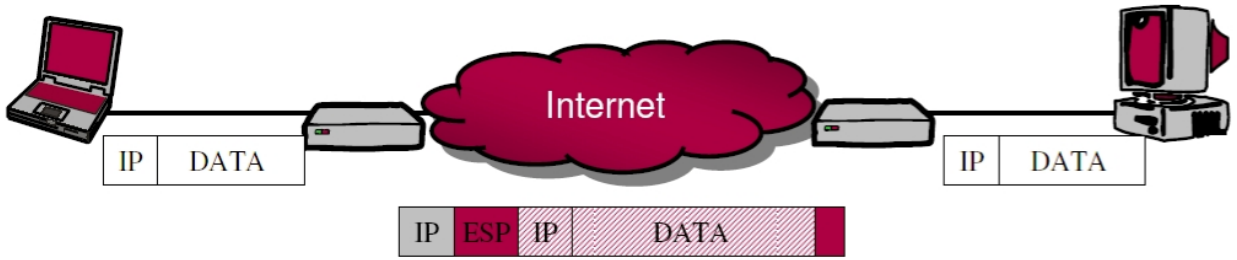
Transport Mode

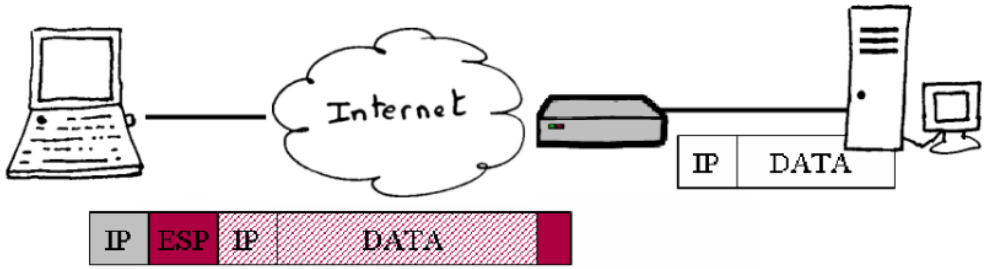
- In transport mode, security is done end-to-end.



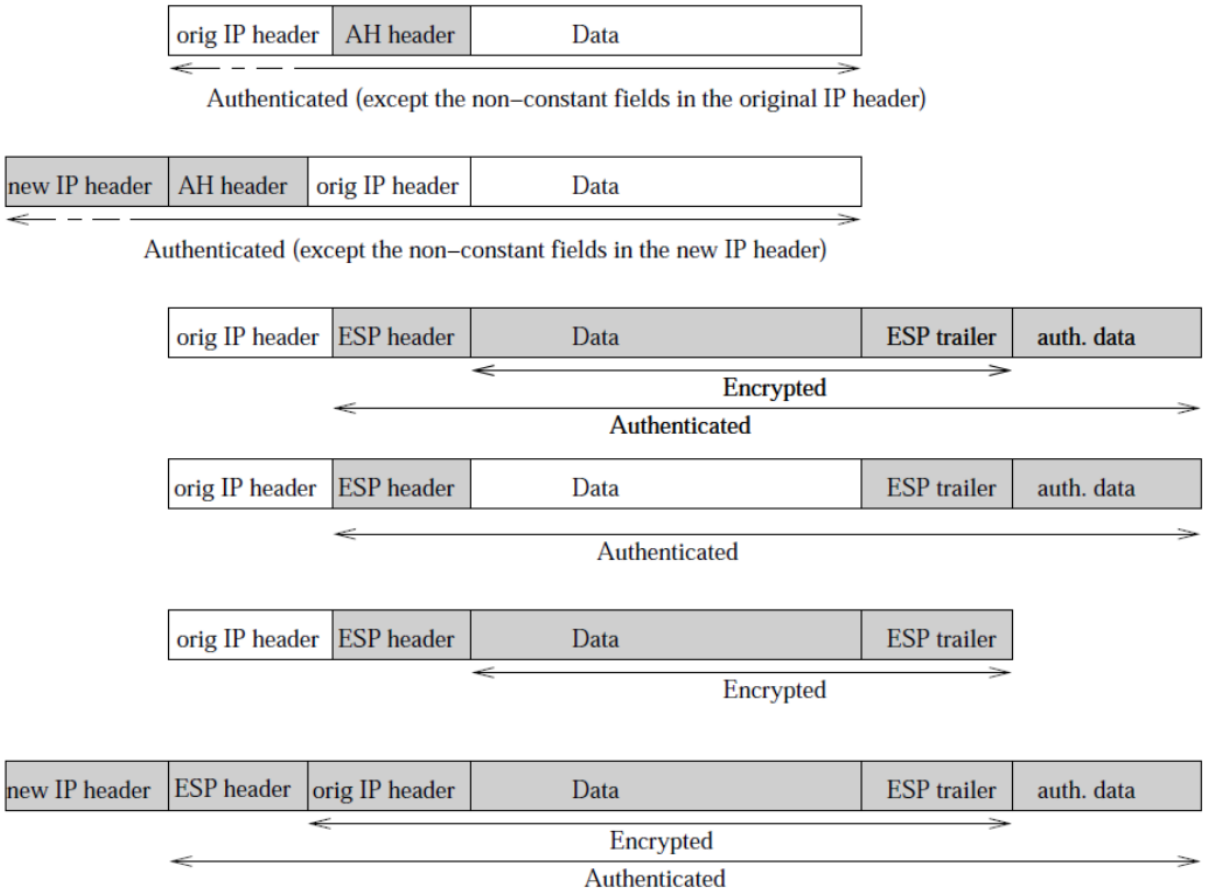
Tunnel Mode

- In tunnel mode, it can be done by intermediate routers.





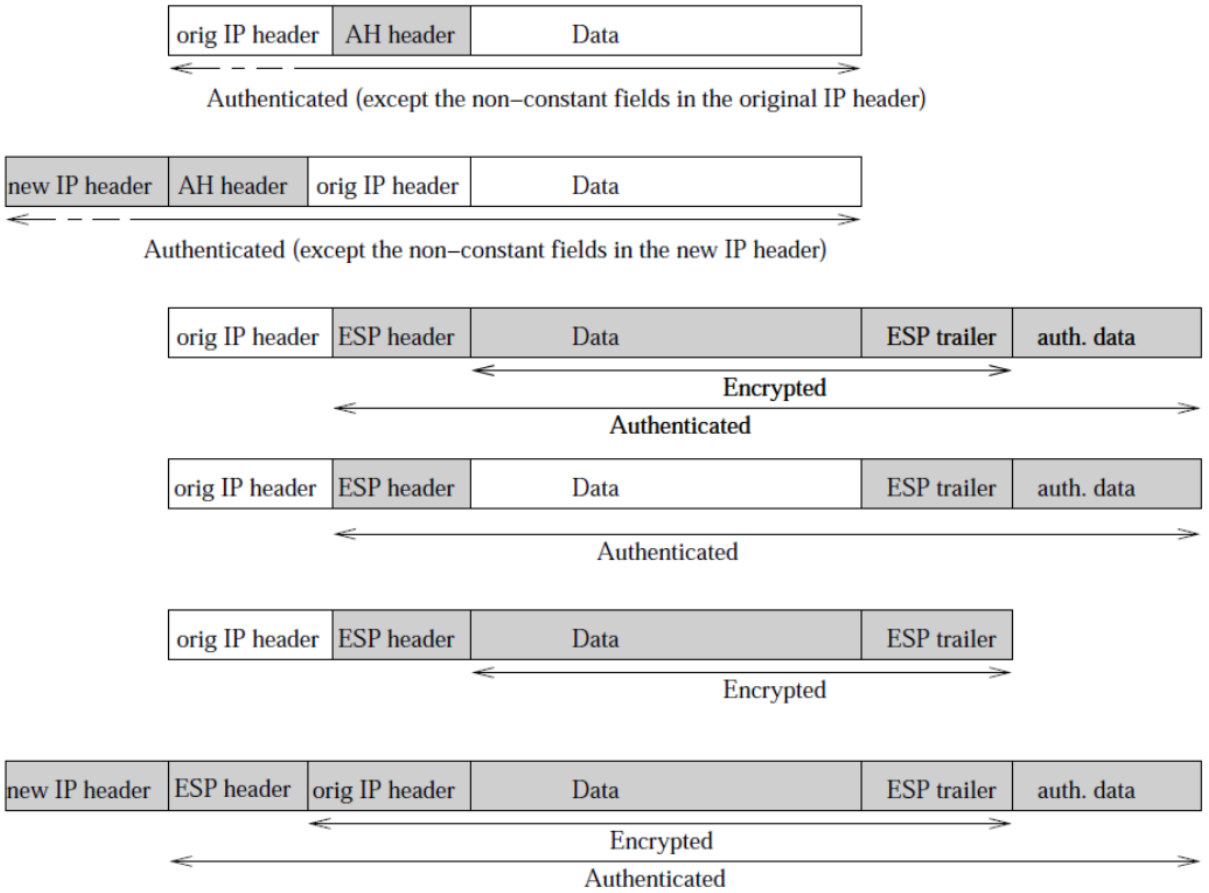
Test: What is the Applied Mode?



IPSEC USED BEHIND NAT

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

IPsec and NAT



IPsec and NAT

- The TCP and UDP checksum calculation includes a pseudo-header made of src and dst IP addresses and ports.
- When doing NAT, the checksum has to be readjusted every time the source IP address changes.
- This does not work if the payload is encrypted or authenticated.
- NAT-T (NAT traversal): encapsulate IPsec in UDP.

CONCLUSION AND REFERENCES

- VPN Primer and IPsec Primer
- Security Policy Database and Security Associations
- AH and ESP
- Transport and Tunnel Modes
- IPsec Used Behind NAT
- Conclusion and References

Conclusion

- IPsec is a standard that is safe, flexible, and open.
- Being a network-layer protocol, IPsec reduces the flexibility of the TCP/IP architecture (e.g. NAT).
- The IPsec-related RFCs are very complex, and so make the IPsec implementations usually non-interoperable.

References

- IPsec, The New Security Standard for the Internet, Intranets, and Virtual Private Networks (2nde edition), Naganand Doraswamy and Dan Harkins, 2003, Prentice Hall.
- http://unixwiz.net/techtips/iguide-ipsec.html