Fundamentals of Information & Network Security ECE 471/571

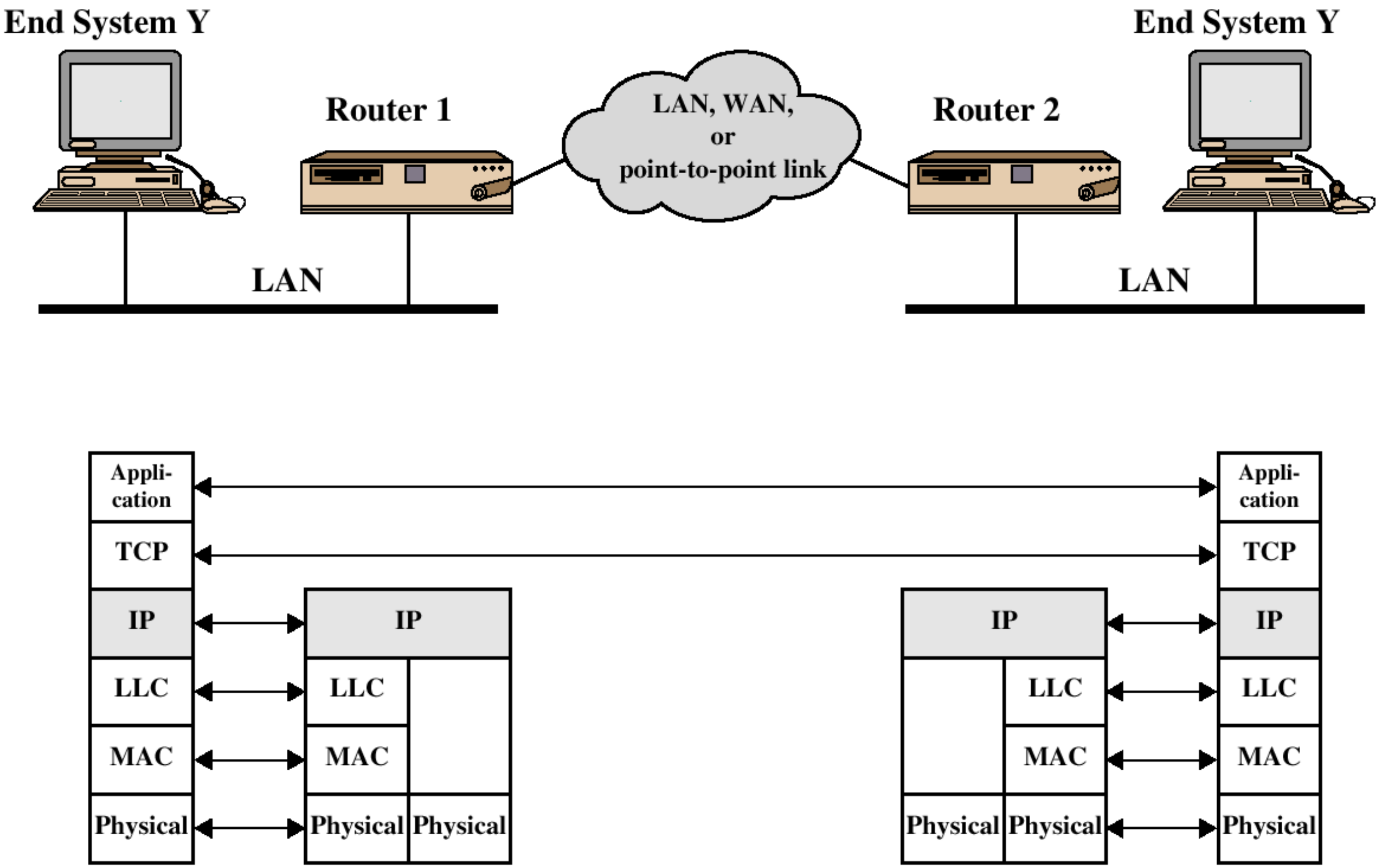
Lecture #34,35: IP security Issues and IPSec

Instructor: Ming Li

Dept of Electrical and Computer Engineering

University of Arizona

TCP/IP Review



End System Y

Router 1

LAN, WAN, or point-to-point link

Router 2

End System Y

LAN

LAN

Appli-cation

TCP

IP

LLC

MAC

Physical

IP

LLC

MAC

Physical

Physical

IP

LLC

MAC

Physical

Physical

Appli-cation

TCP

IP

LLC

MAC

Physical

Security Problems of the Internet Protocol

- When an entity receives an IP packet, it has no assurance of:
  - Data origin authentication / data integrity:
    - The packet has actually been send by the entity which is referenced by the source address of the packet
    - The packet contains the original content the sender placed into it, so that it has not been modified during transport
    - The receiving entity is in fact the entity to which the sender wanted to send the packet
  - Confidentiality:
    - The original data was not inspected by a third party while the packet was sent from the sender to the receiver

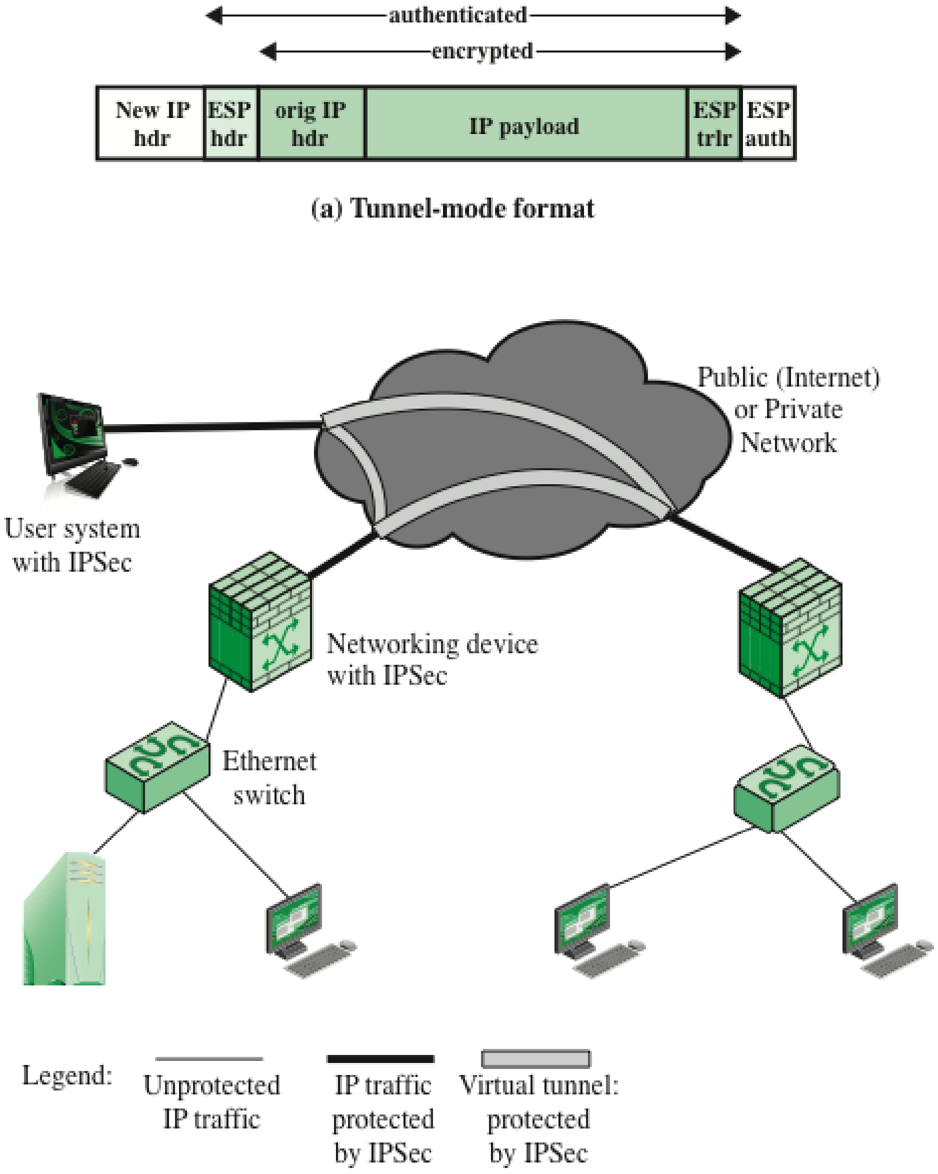
IP Security Issues

- Eavesdropping
- Modification of packets in transit
- Identity spoofing (forged source IP addresses)
- Denial of service

- Many solutions are application-specific
  - TLS for Web, S/MIME for email, SSH for remote login
- IPsec aims to provide a framework of open standards for secure communications over IP
  - Protect <u>every</u> protocol running on top of IPv4 and IPv6

IPsec

- IETF standard for real-time communication security
- Implemented at IP layer, all traffic can be secured, no matter what application.
- Transparent to applications, no changes on upper-layer software.
- Transparent to end users, no need to train users on security mechanisms, issuing keying material on a per-user basis, or revoking keying material when users leave.



(a) Tunnel-mode format

(b) Example configuration

Figure 20.1 An IPSec VPN Scenario

IPsec: Network Layer Security

IPsec = AH + ESP + IKE

Protection for IP traffic
AH provides integrity and origin authentication
ESP also confidentiality

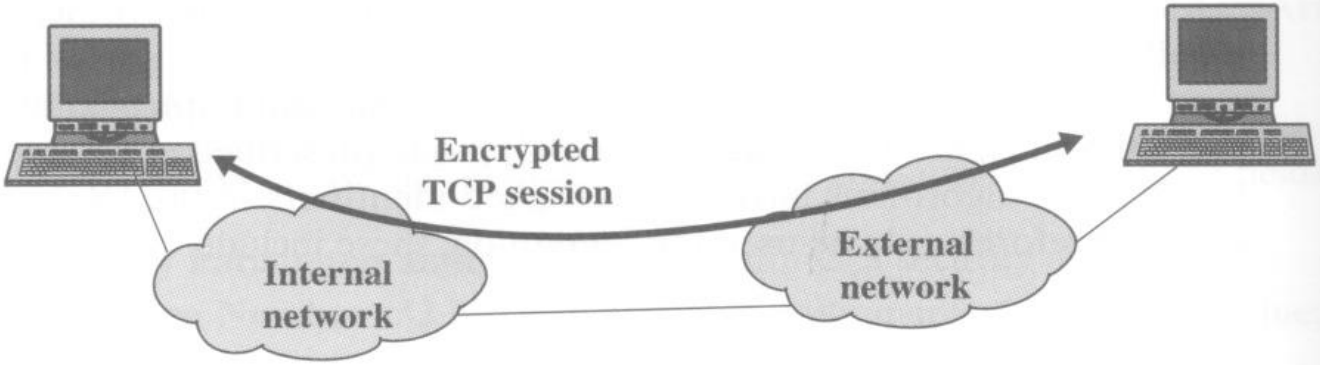
Sets up keys and algorithms for AH and ESP

- AH and ESP rely on an existing security association
  - Idea: parties must share a set of secret keys and agree on each other’s IP addresses and crypto algorithms
- Internet Key Exchange (IKE)
  - Goal: establish security association for AH and ESP
  - If IKE is broken, AH and ESP provide no protection!

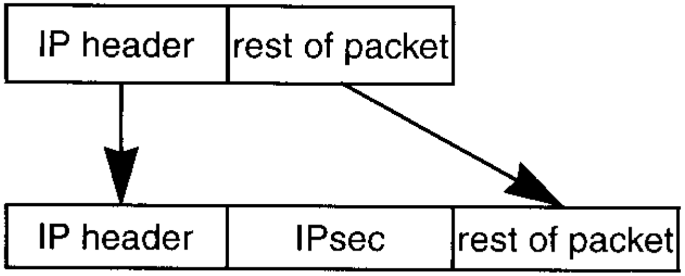
Two Modes

- Transport mode
  - Add the IPsec info between the IP header and the IP payload.
- Tunnel mode
  - Keep the original IP packet intact and add a new IP header and IPsec info outside.

Transport Mode



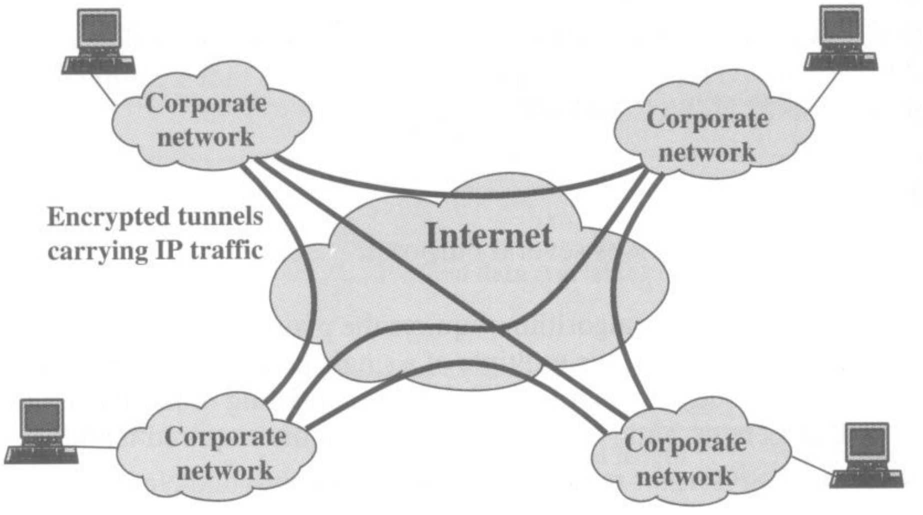
Transport Mode



- End-to-end
- Protect primarily upper-layer protocols (IP payload)
- Add IPsec between IP header and IP payload
- AH authenticates IP payload and selected portions of IP header
- ESP encrypts IP payload, authenticates IP payload, but not IP header

Tunnel Mode

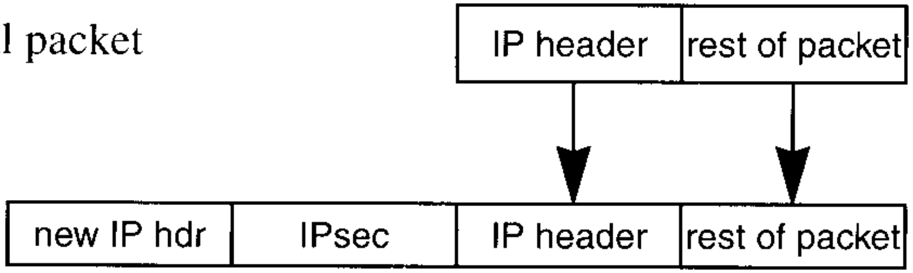
- Common use: one end is security gateway
- Protect entire IP packet
- Add New IP header
- AH authenticates entire inner IP packet plus selected portions of outer IP header
- ESP encrypts entire inner IP packet, authenticates entire inner IP packet



(b) A virtual private network via tunnel mode

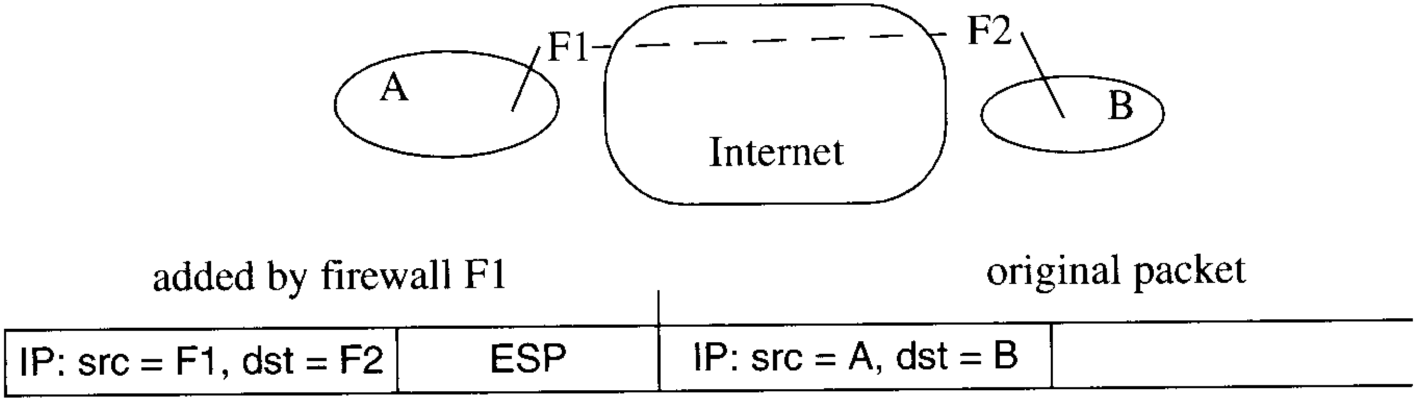
Tunnel Mode

original packet


IP header | rest of packet

new IP hdr | IPsec | IP header | rest of packet

Tunnel Mode



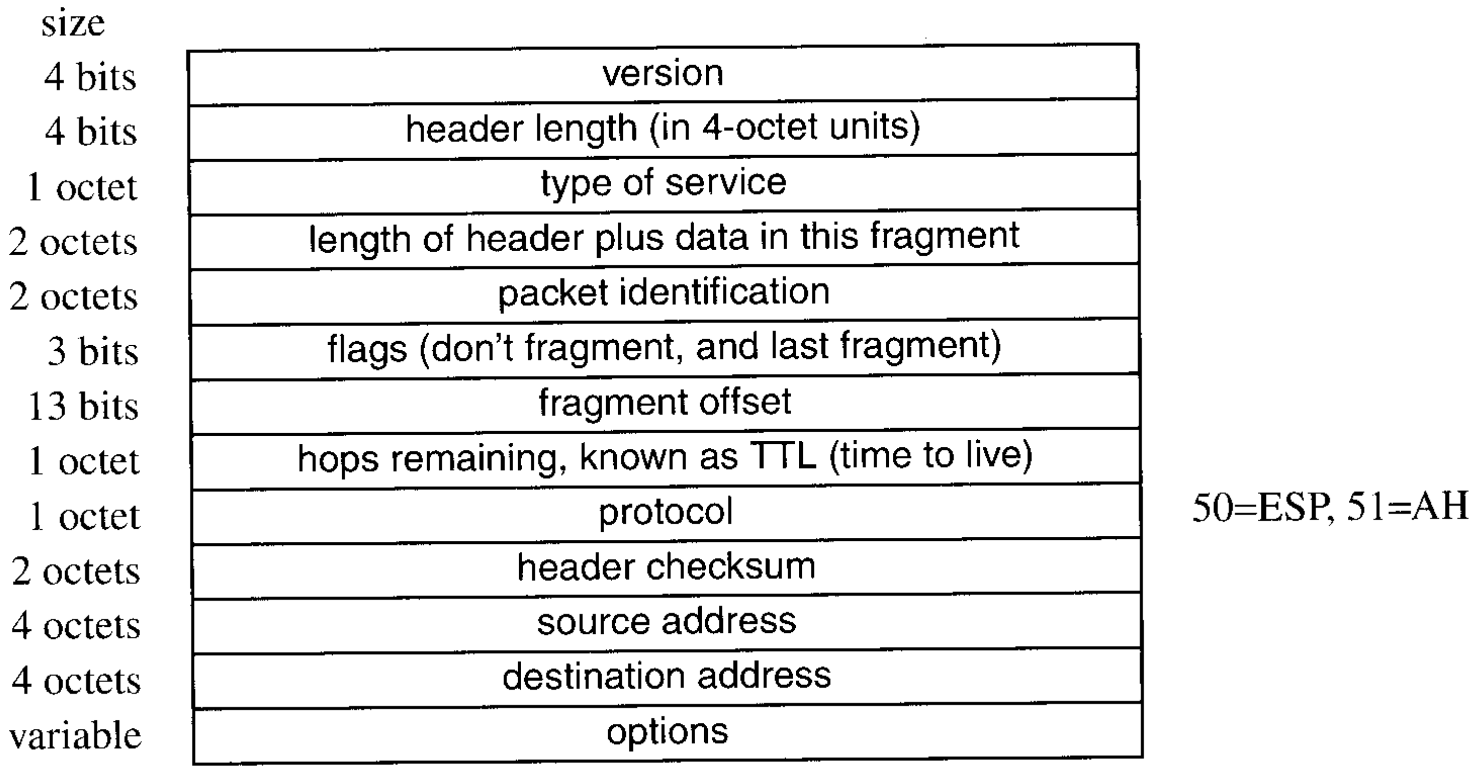
added by firewall F1		original packet	
IP: src = F1, dst = F2	ESP	IP: src = A, dst = B	

Figure 17-2. IPsec, tunnel mode, between firewalls

Figure 17-3. Multiply encrypted IP packet

IPv4 Header

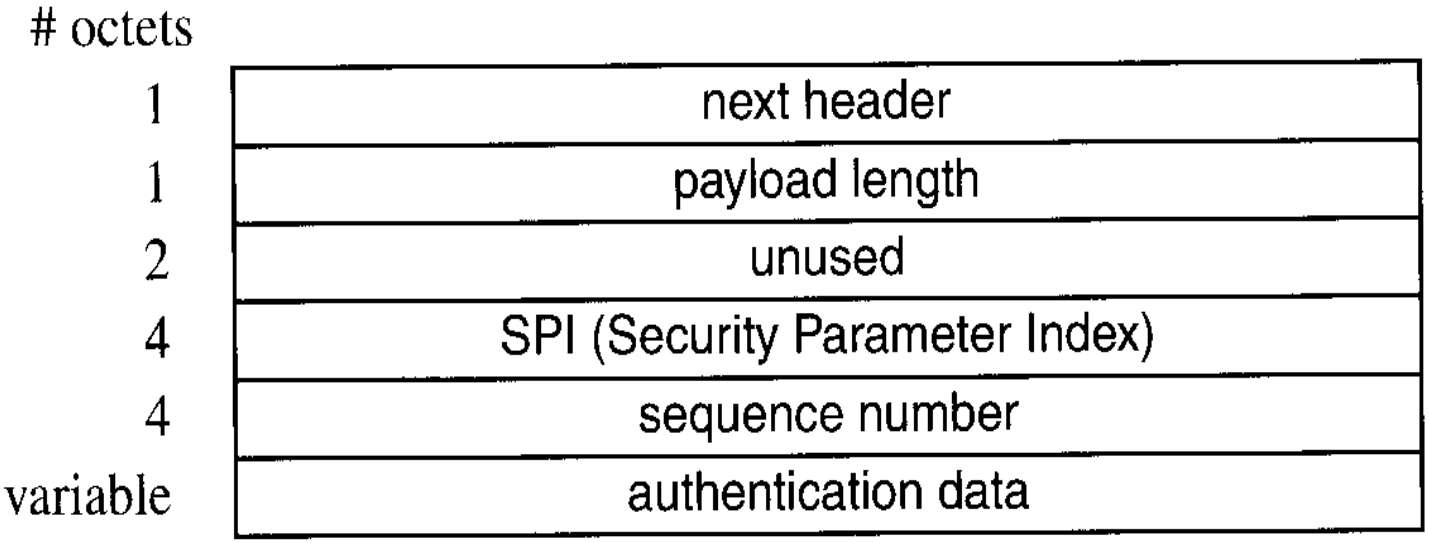
- Protocol/Next header:
  - IP (4), TCP (6), UDP (17), AH (51), ESP (50)



size		
4 bits	version	
4 bits	header length (in 4-octet units)	
1 octet	type of service	
2 octets	length of header plus data in this fragment	
2 octets	packet identification	
3 bits	flags (don’t fragment, and last fragment)	
13 bits	fragment offset	
1 octet	hops remaining, known as TTL (time to live)	
1 octet	protocol	50=ESP, 51=AH
2 octets	header checksum	
4 octets	source address	
4 octets	destination address	
variable	options	

AH (Authentication Header)

- Integrity protection
  - Data integrity: modification of packet content
  - Authentication of IP packets: address spoofing, replay attack



# octets	
1	next header
1	payload length
2	unused
4	SPI (Security Parameter Index)
4	sequence number
variable	authentication data

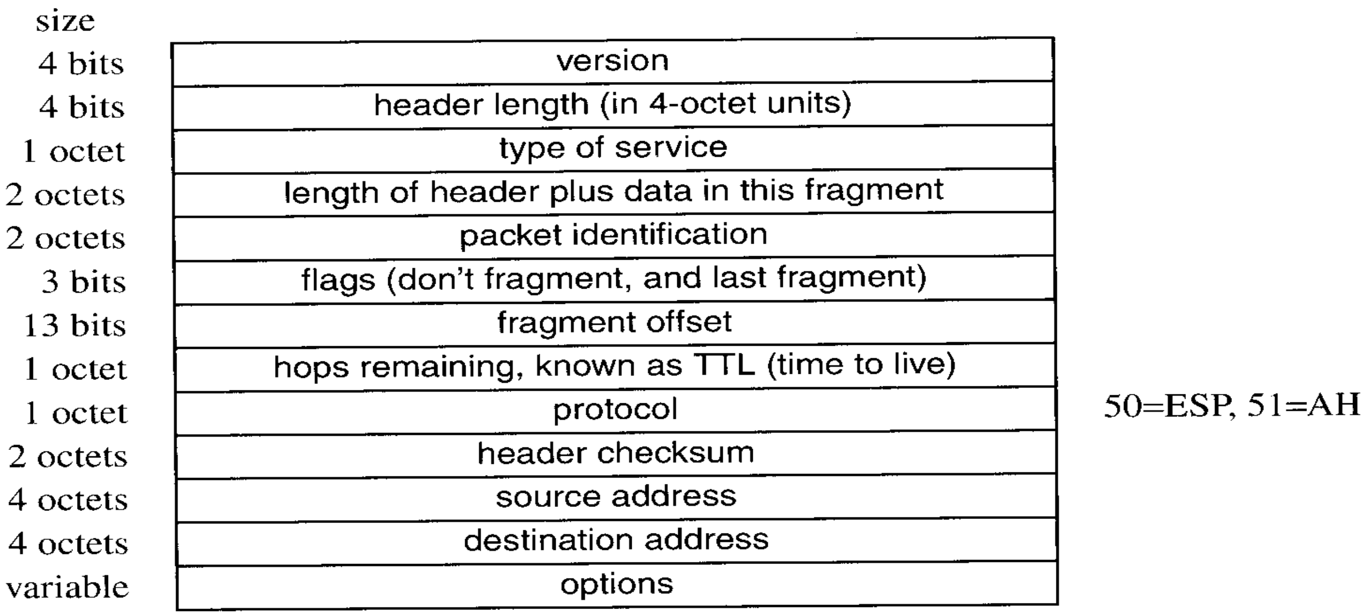
Authentication Data Field

- Integrity check value (ICV)
- HMAC-MD5-96

  HMAC-SHA-1-96
- The MAC is calculated over
  - Immutable or predictable IP header fields
  - AH header other than the Authentication data field
  - Entire upper-layer protocol data

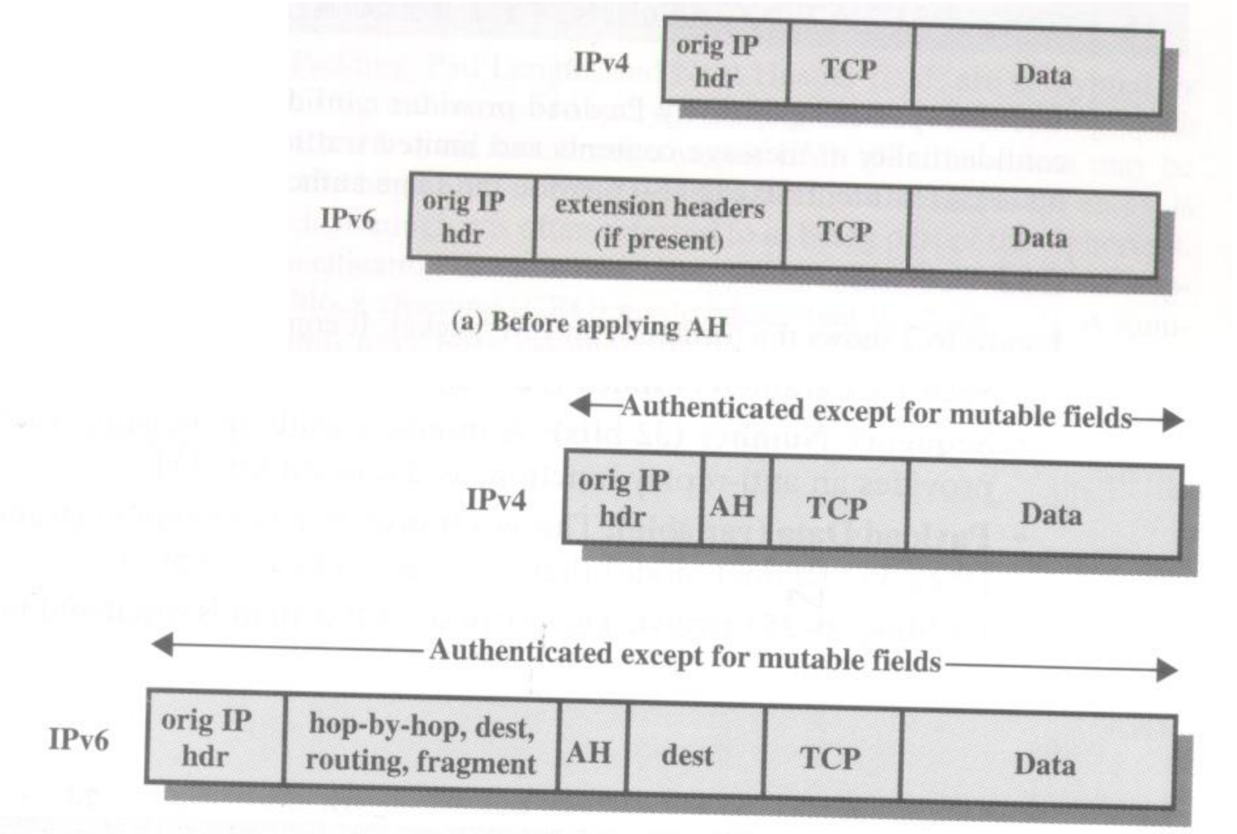
IP Header: Mutable, Immutable

- Mutable: TTL, Type of Service, Flags, Fragment Offset, Header Checksum
- Immutable: Source Address
- Mutable but Predictable: Destination Address



size		
4 bits	version	
4 bits	header length (in 4-octet units)	
1 octet	type of service	
2 octets	length of header plus data in this fragment	
2 octets	packet identification	
3 bits	flags (don't fragment, and last fragment)	
13 bits	fragment offset	
1 octet	hops remaining, known as TTL (time to live)	
1 octet	protocol	50=ESP, 51=AH
2 octets	header checksum	
4 octets	source address	
4 octets	destination address	
variable	options	

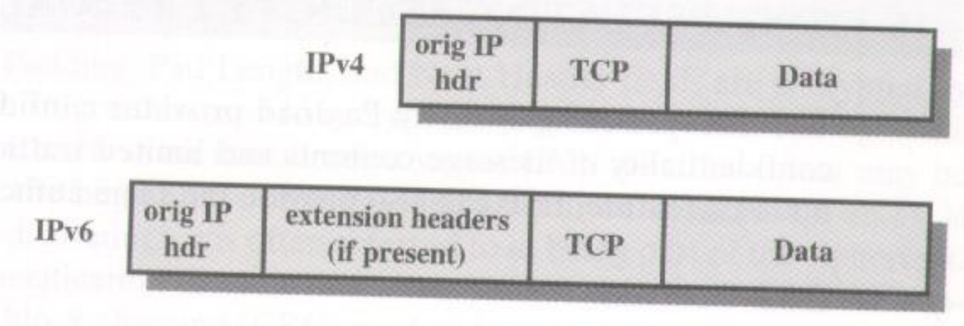
Transport Mode AH


IPv4
orig IP hdr
TCP
Data
IPv6
orig IP hdr
extension headers (if present)
TCP
Data
Authenticated except for mutable fields
IPv4
orig IP hdr
AH
TCP
Data
Authenticated except for mutable fields
IPv6
orig IP hdr
hop-by-hop, dest, routing, fragment
AH
dest
TCP
Data

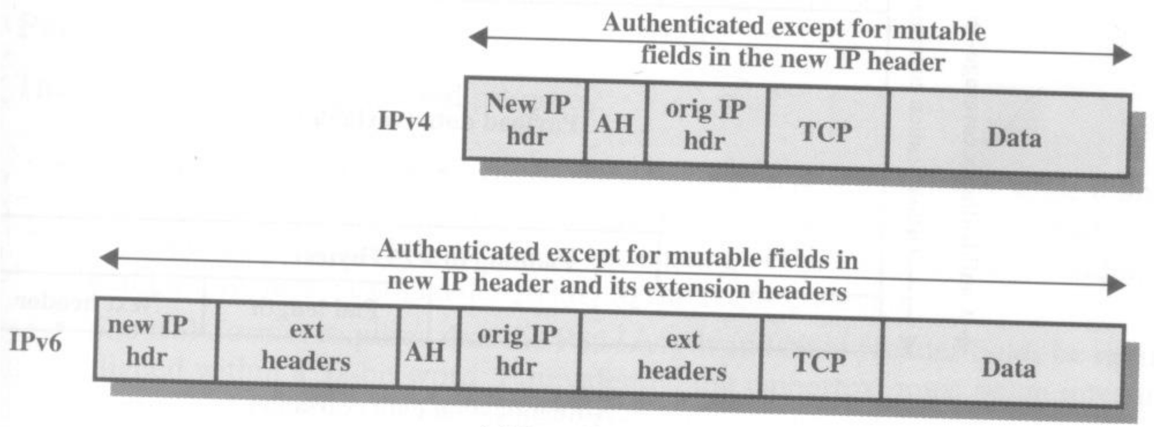
(a) Before applying AH

(b) Transport mode

Tunnel Mode AH



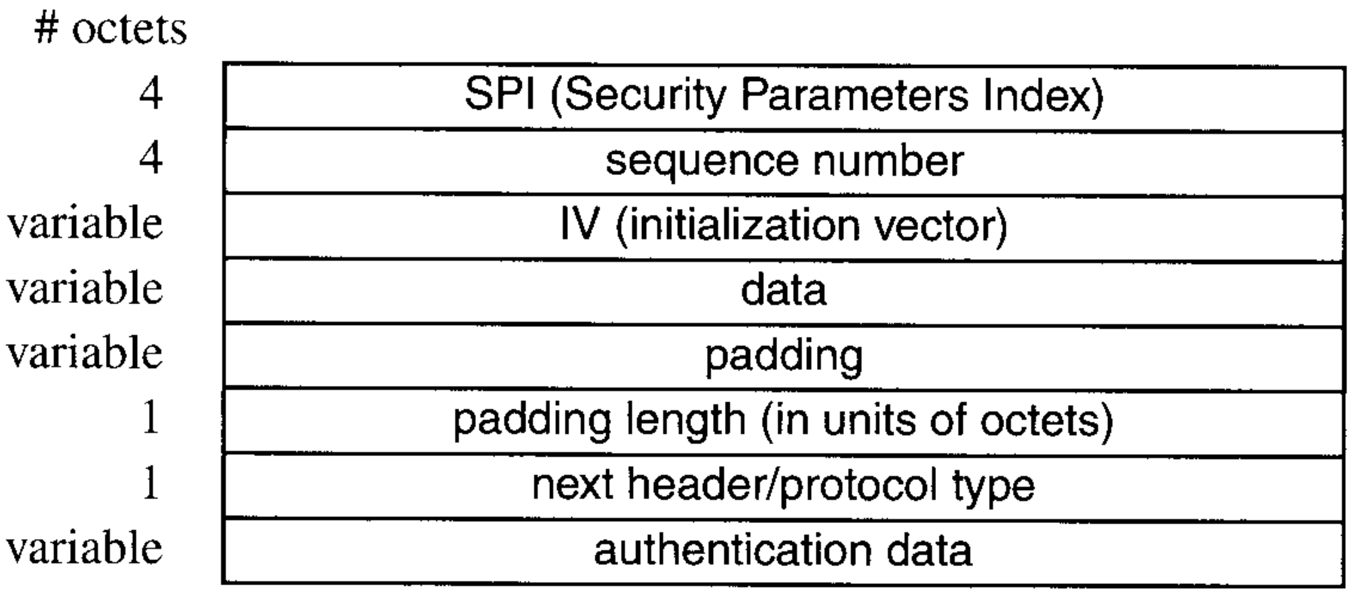
(a) Before applying AH


Authenticated except for mutable fields in the new IP header
IPv4
New IP hdr
AH
orig IP hdr
TCP
Data
Authenticated except for mutable fields in new IP header and its extension headers
IPv6
new IP hdr
ext headers
AH
orig IP hdr
ext headers
TCP
Data

(c) Tunnel mode

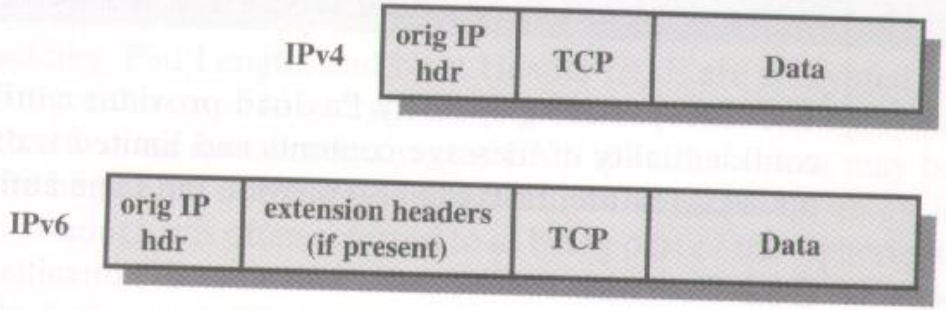
ESP (Encapsulating Security Payload)

- Encryption and/or Integrity protection

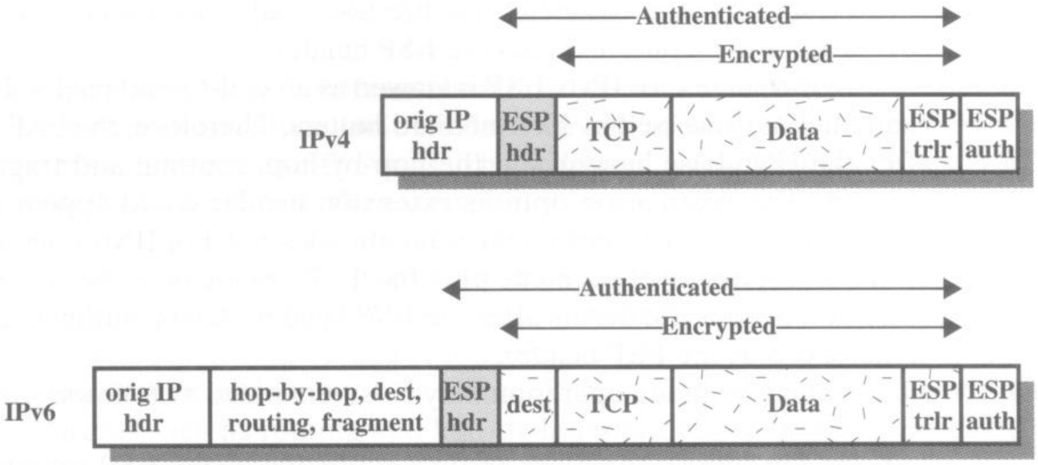


# octets	
4	SPI (Security Parameters Index)
4	sequence number
variable	IV (initialization vector)
variable	data
variable	padding
1	padding length (in units of octets)
1	next header/protocol type
variable	authentication data

Transport Mode ESP

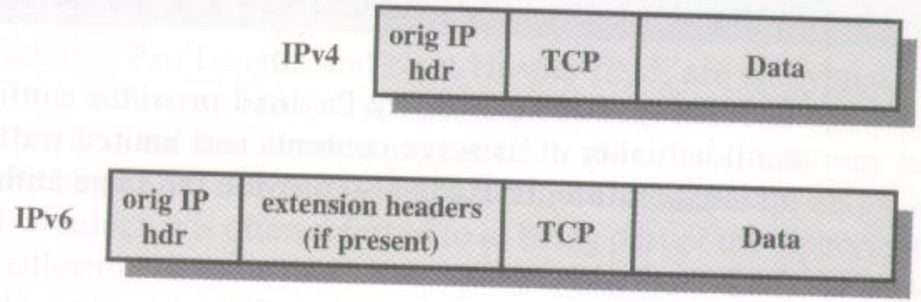


(a) Before applying AH

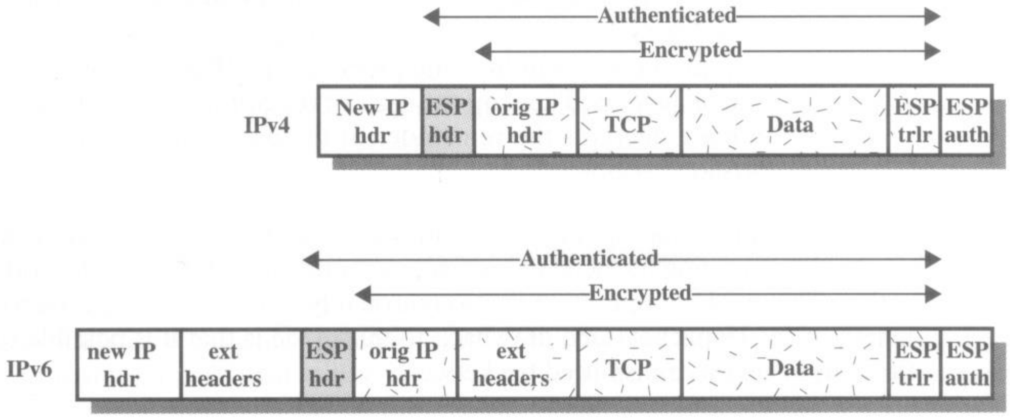


(a) Transport mode

Tunnel Mode ESP



(a) Before applying AH



(b) Tunnel mode

AH and ESP

- AH does only integrity protection.
- ESP allows
  - encryption only
  - integrity only
  - encryption+integrity
- ESP can replace AH except that
  - AH also protect the immutable fields in the IP header (source and destination IP addresses), while ESP works only on the payload.

SA: Security Association

- A cryptographically protected connection
- Unidirectional: a bidirectional conversation consists of two SAs, one in each direction
- Information associated with each end of a SA:
  - identity of the other end
  - sequence number currently being used
  - cryptographic services being used: integrity or encryption+integrity, algorithms, keys, IVs, life time, etc…
  - IPsec protocol mode: tunnel, transport,
  - …

SA identifier

- A system need to know which SA a packet belongs to. The SA of any packet is uniquely determined by
  - Security Parameter Index (SPI): a field in AH or ESP headers, assigned during IKE negotiation.
  - Destination IP address
  - Security Protocol Identifier: AH or ESP

Q: Why destination address is needed?

SA defined by: <SPI, destination address, flag for whether it's AH or ESP>

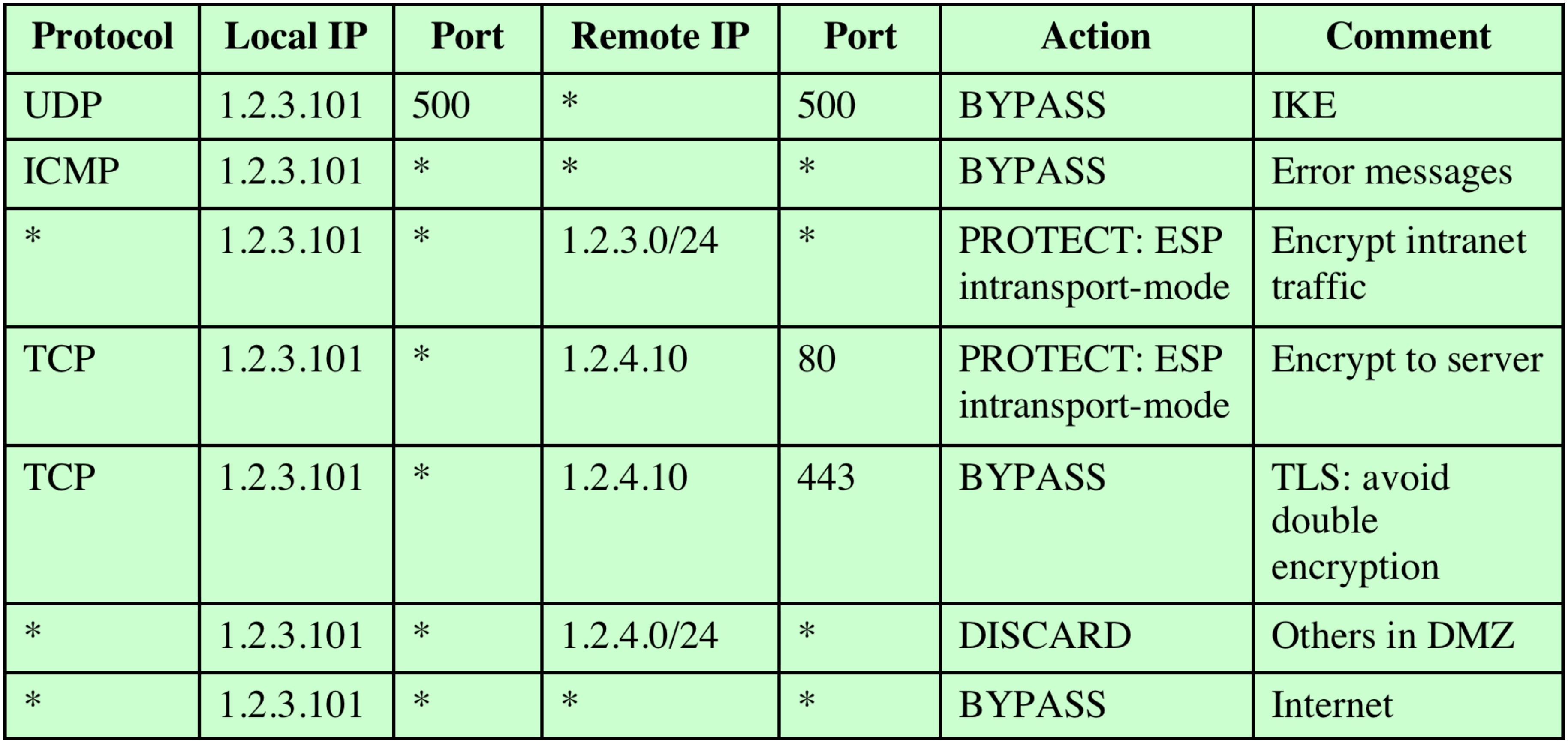
Security Association Database

- Given a packet, the sender looks up in the database for an appropriate SA, which tells it how to process the packet.
- The receiver looks up in the database for a corresponding SA, which tells it how to reverse the processing and recover the packet.

Security Policy Database

- An IPsec-enabled system has a security policy database (SPD), describing how to treat the outbound packets. Each policy matches certain traffic streams and specifies the action: drop, forward, IPsec, etc. If the action is IPsec, it also provides all needed parameters.
- When a packet matches an IPsec policy, the computer first looks up if there is an existing SA. If so, process the packet. Otherwise, invoke IKE to negotiate one first.

Host SPD Example



Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

IPsec doesn’t work well with

- NAT (Network Address Translation)
  - Source address is encrypted in ESP tunnel mode
  - Source address is in the checksum in ESP transport mode
  - Source address affects the crypto-checksum in AH
- Firewalls
  - IPsec encrypts information (TCP ports etc.) that firewall wants to inspect.