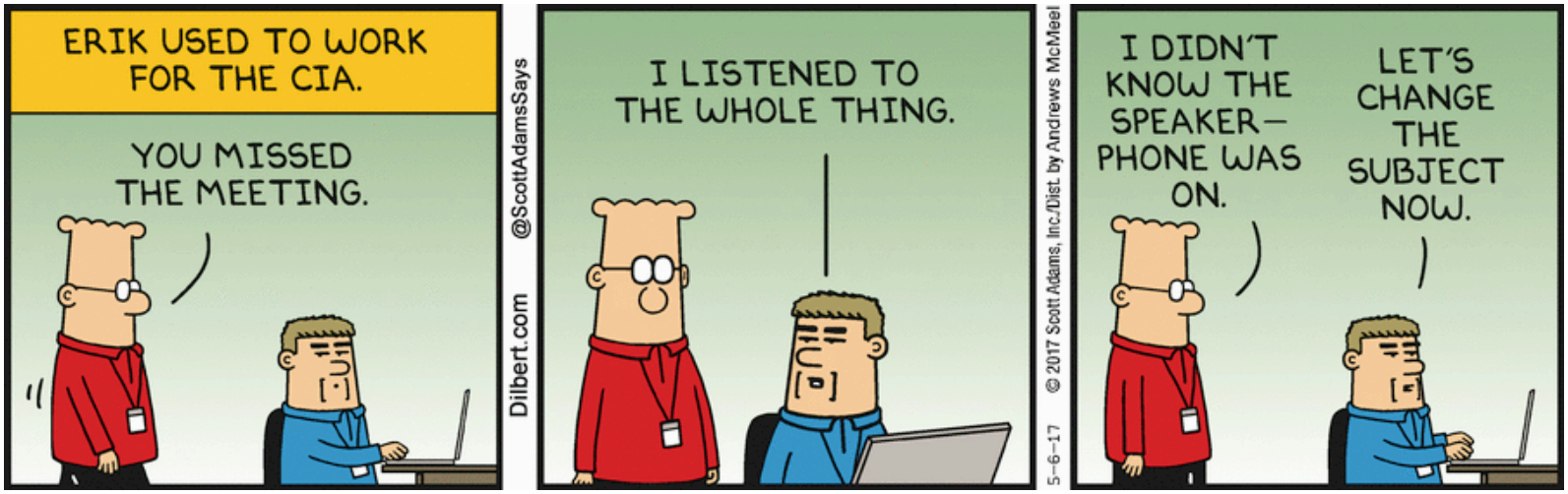
Ασφάλεια στο επίπεδο δικτύου

Νικόλαος Ε. Κολοκοτρώνης
Επίκουρος Καθηγητής

Τμήμα Πληροφορικής και Τηλεπικοινωνιών
Πανεπιστήμιο Πελοποννήσου
Email: nkolok@uop.gr
Web: http://www.uop.gr/~nkolok/

ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΩΝ

Περιεχόμενα



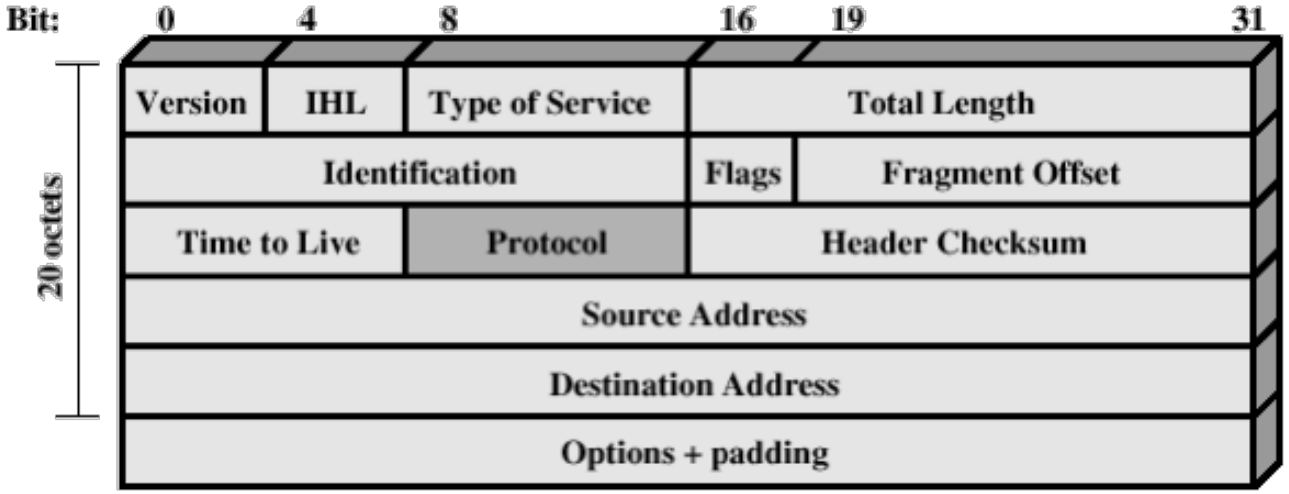
Περιεχόμενα

- Πρωτόκολλο IPsec
  - IP security overview
  - IP security policy
  - Authentication header
  - Encapsulating security payload
  - Security associations
  - Internet key exchange
  - Attacks / applications

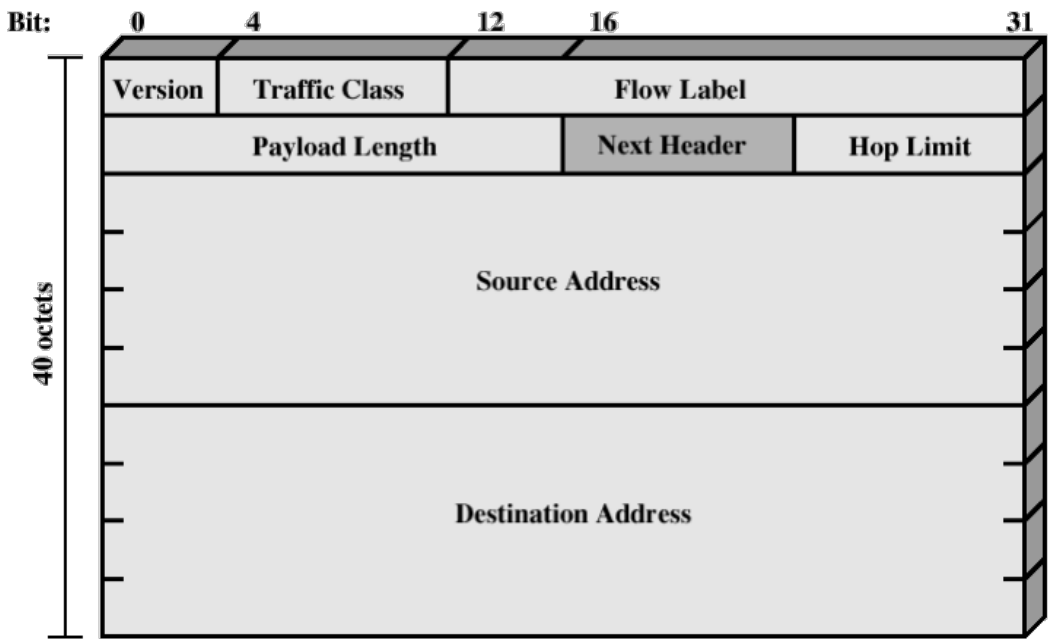
Internet protocol

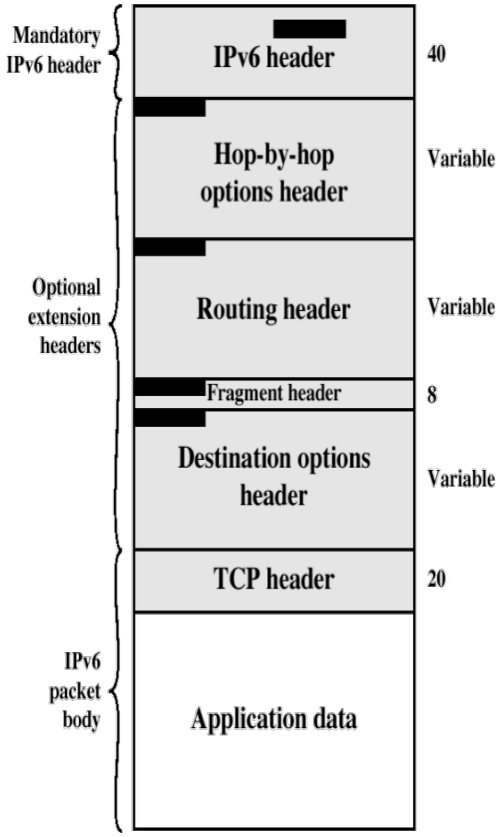
- Main facts
  - IP provides interconnection across different networks
  - IP is implemented in every end-user and in routers
- IP is an unreliable protocol
  - IP datagrams may be lost
  - IP datagrams may arrive out of order
  - TCP takes care of those problems
- Current versions: IPv4 & IPv6

Internet protocol



Internet protocol





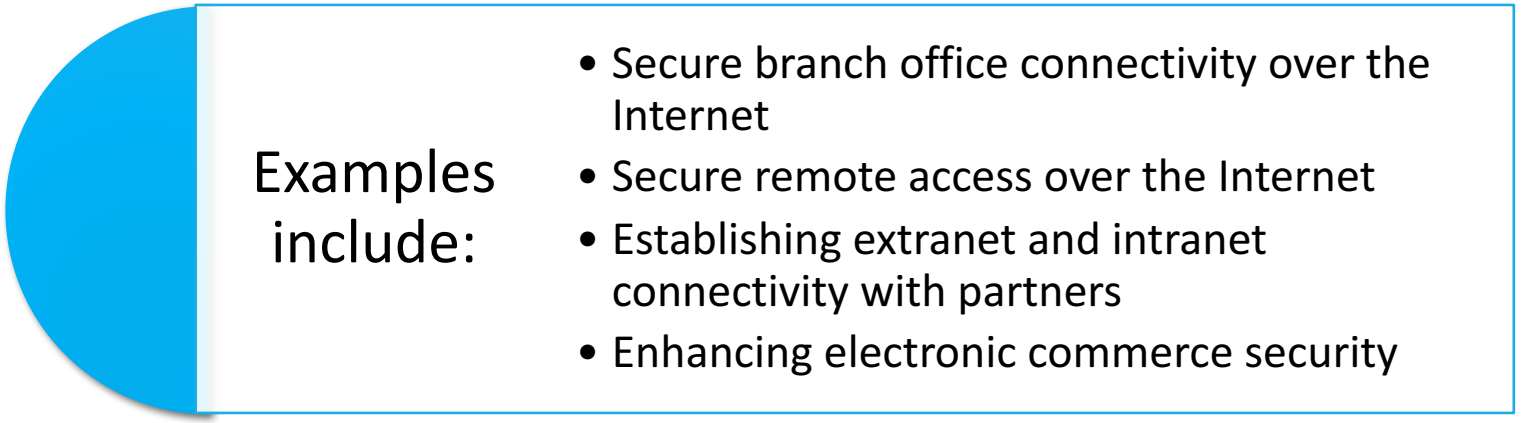
Επισκόπηση IPsec

IP security overview

- RFC 1636 “Security in the Internet Architecture”
  - Issued in 1994 by the Internet Architecture Board (IAB)
  - Identifies key areas for security mechanisms
    - Need to secure the network infrastructure from unauthorized monitoring and control of network traffic
    - Need to secure end-user-to-end-user traffic using authentication and encryption mechanisms
  - IAB included authentication and encryption as necessary security features in the next generation IP (IPv6)
    - The IPsec specification now exists as a set of Internet standards

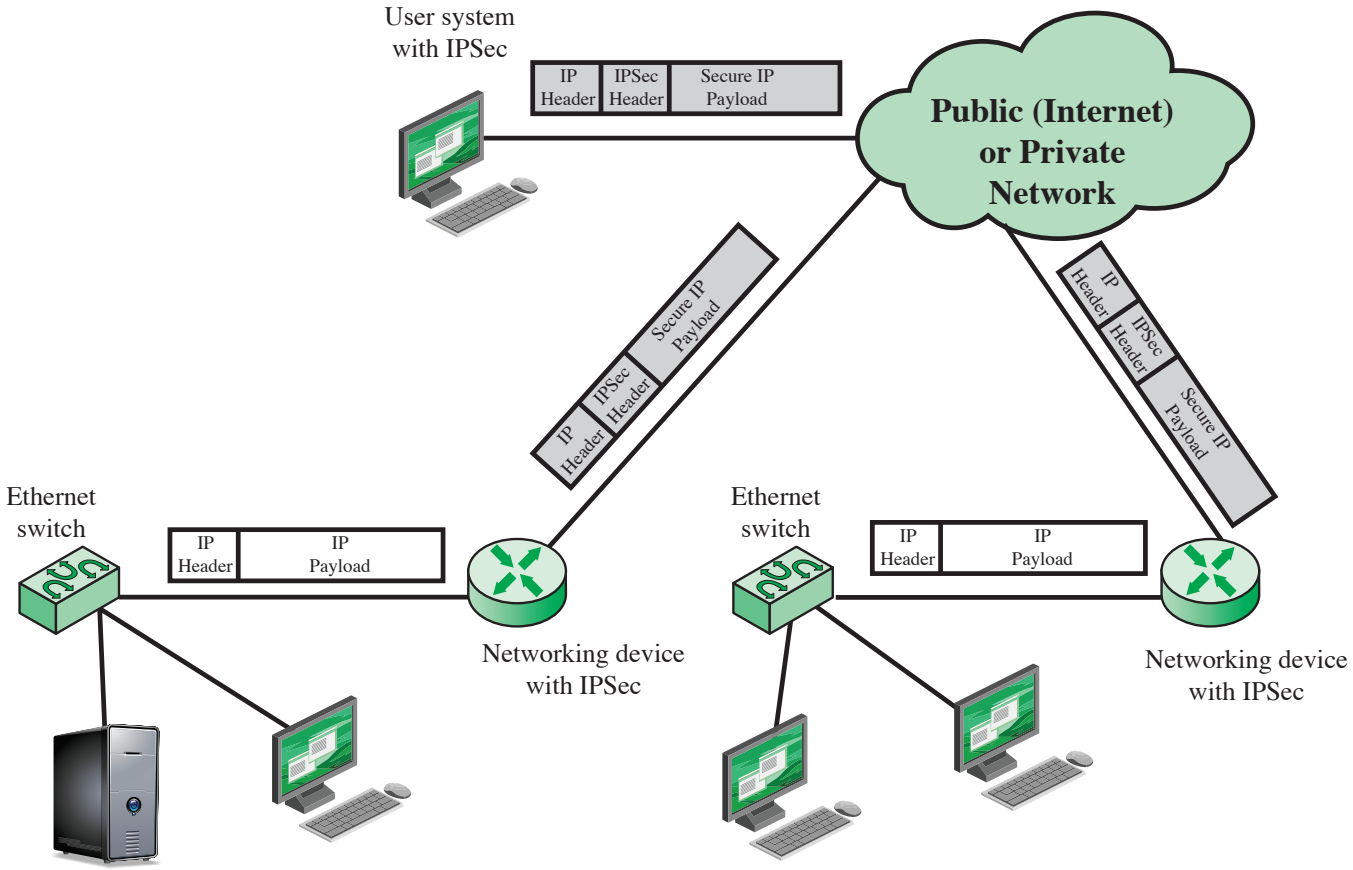
Applications of IPsec

- IPsec provides the capability to secure communications across a LAN, private and public WANs, and the Internet



- Principal feature of IPsec is that it can encrypt and/or authenticate all traffic at the IP level

An IP security scenario



Benefits of IPsec

- Provides strong security that can be applied to all traffic crossing the perimeter
  - Traffic within a company or workgroup does not incur the overhead of security-related processing
- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications
  - There is no need to change software on a user or server system when IPsec is implemented in the firewall or router

Benefits of IPsec

- IPsec can be transparent to end users
  - There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization
- IPsec can provide security for individual users if needed
  - This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications

IPsec integration

- Integration of IPsec with the native IP implementation
  - Requires access to the IP source code
  - Applicable to both hosts and security gateways
- Bump-in-the-stack (BITS) implementation
  - Between native IP implementation and network drivers
  - Appropriate for use with legacy systems
  - Usually employed in hosts
- Bump-in-the-wire (BITW) implementation
  - Has a H/W crypto processor
  - Usually the BITW device is IP addressable
  - Applicable to hosts and/or security gateways

Routing applications

- IPsec can play a vital role in the routing architecture required for internetworking

IPsec can assure that

- A router advertisement comes from an authorized router
- A router seeking to establish a neighbor relationship with a router in another domain is an authorized router
- A redirect message comes from the router to which the initial IP packet was sent
- A routing update is not forged

IPsec documents

ARCHITECTURE

- The current specification is RFC 4301 (Security Architecture for the Internet Protocol)
- Covers all the concepts, security requirements, definitions, and methods defining IPsec technology

IN GENERAL

- There are a variety of other IPsec-related RFCs, incl. those dealing with
  - security policy
  - management information base (MIB)

IPsec documents

AUTH. HEADER

- The current specification is RFC 4302 (IP Authentication Header)
- An extension header to provide message authentication

ENC. SECURITY PAYLOAD

- The current specification is RFC 4303 (IP Encapsulating Security Payload)
- Consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication

IPsec documents

INTERNET KEY EXCHANGE

- The main specification is RFC 5996 (Internet Key Exchange - IKEv2) protocol, but there are a number of related RFCs
- A collection of documents describing the key management schemes for use with IPsec

CRYPTO ALGORITHMS

- This encompasses a large set of documents that describe cryptographic algorithms for
  - encryption
  - message authentication
  - pseudorandom functions
  - cryptographic key exchange

IPsec services

- IPsec provides security services at the IP layer by enabling a system to
  - Select required security protocols
  - Determine the algorithm(s) to use for the service(s)
  - Put in place any cryptographic keys required to provide the requested services
- RFC 4301 services listed
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

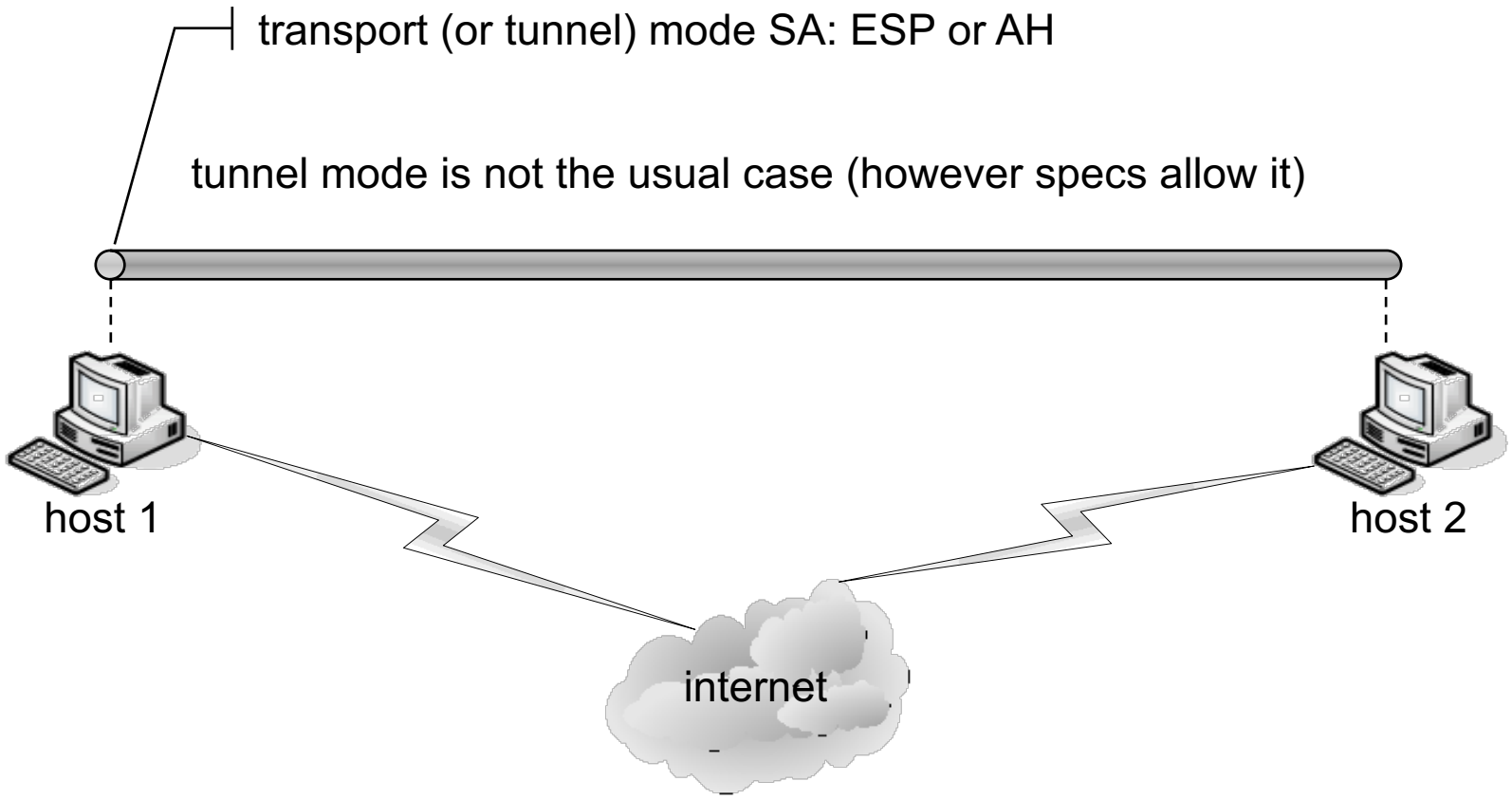
Transport and tunnel modes

	Transport Mode SA	Tunnel Mode SA
AH	Authenticates IP payload and selected portions of IP header and IPv6 extension headers.	Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers.
ESP	Encrypts IP payload and any IPv6 extension headers following the ESP header.	Encrypts entire inner IP packet.
ESP with Authentication	Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header.	Encrypts entire inner IP packet. Authenticates inner IP packet.

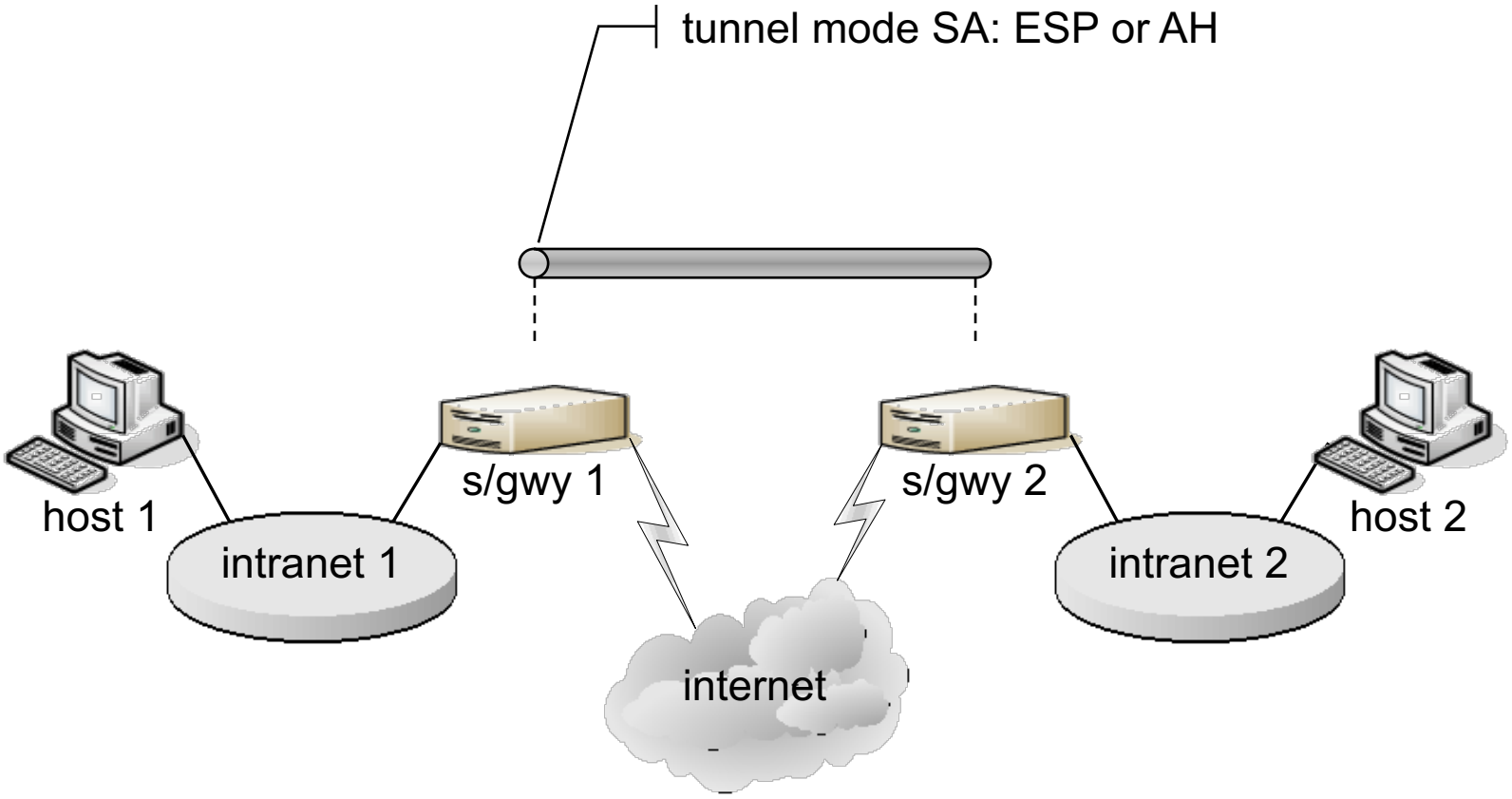
Comparison of services

	AH	ESP (encryption only)	ESP (encryption & authentication)
Connectionless integrity	√		√
Data origin authentication	√		√
Protection against replays	√	√	√
Confidentiality (encryption)		√	√
Traffic flow confidentiallity		√	√

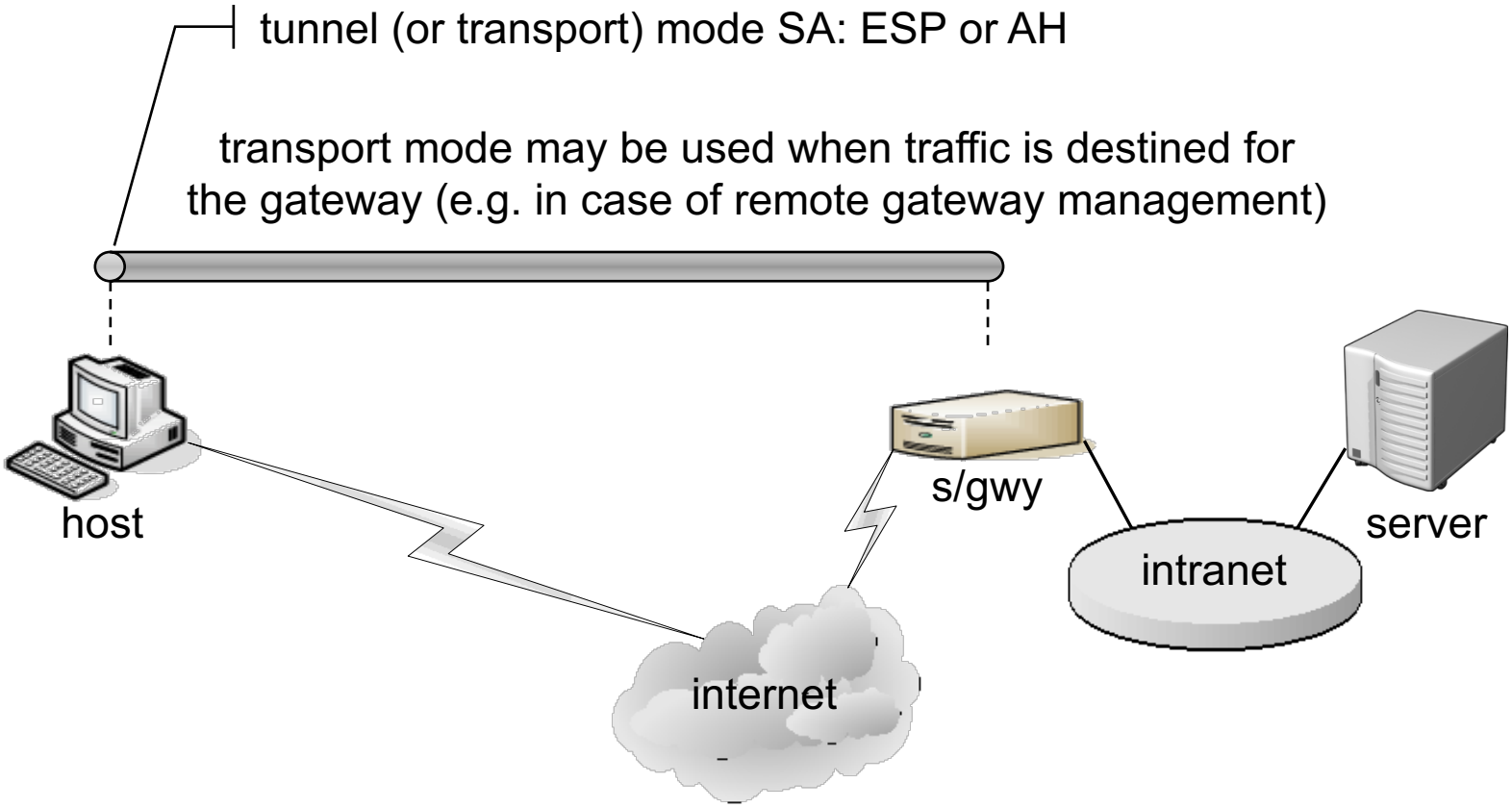
IPsec modes: host-to-host



IPsec modes: router-to-router



IPsec modes: host-to-router

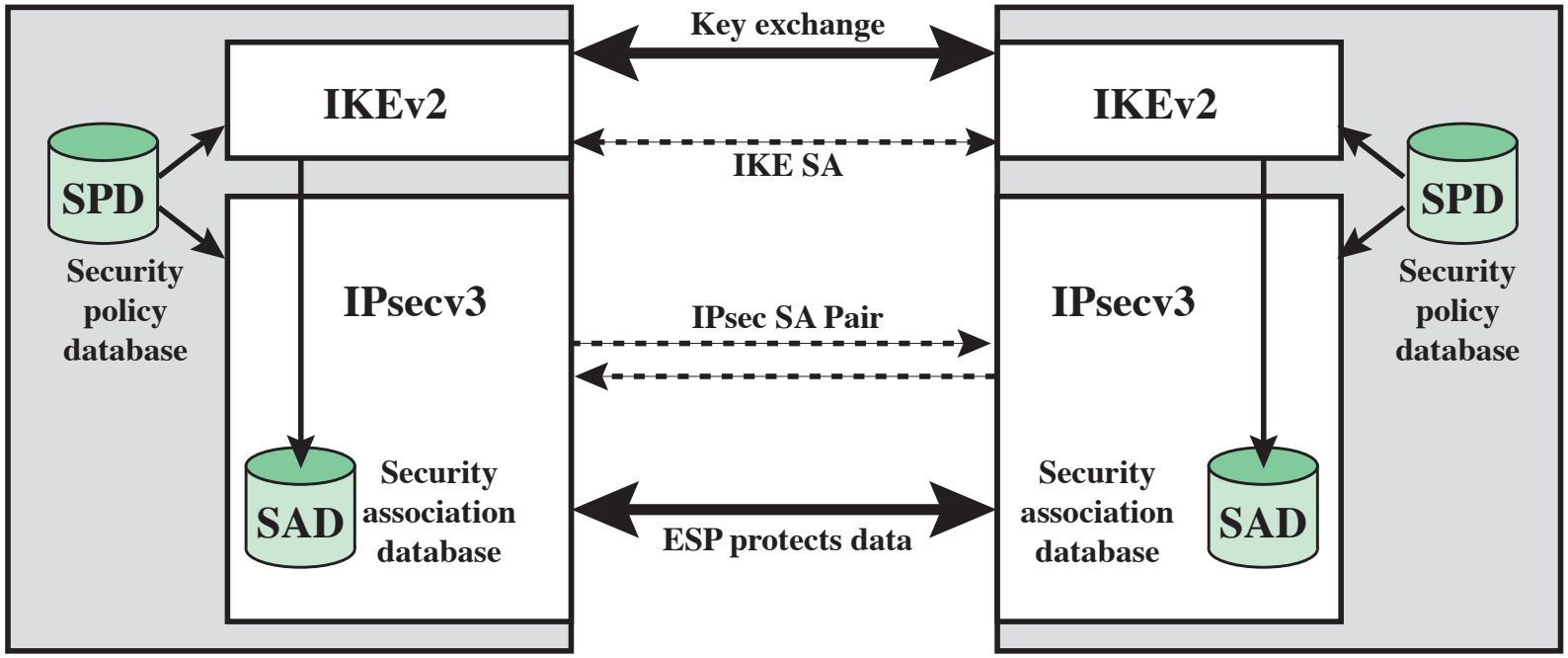


Comparison of modes

	AH	ESP (encryption only)	ESP (encryption & authentication)
Transport mode SA	Authenticates: ▪ IP payload ▪ *selected portions* of IPv6 header ▪ *selected portions* of IPv6 extension headers	Encrypts: ▪ IP payload ▪ *any* IPv6 extension header	Encrypts: ▪ IP payload ▪ *any* IPv6 extension header Authenticates: ▪ IP payload ▪ ***no*** IP header
Tunnel mode SA	Authenticates: ▪ inner IP packet ▪ *selected portions* of outer IP header (see above)	Encrypts: ▪ inner IP packet	Encrypts: ▪ inner IP packet Authenticates: ▪ inner IP packet

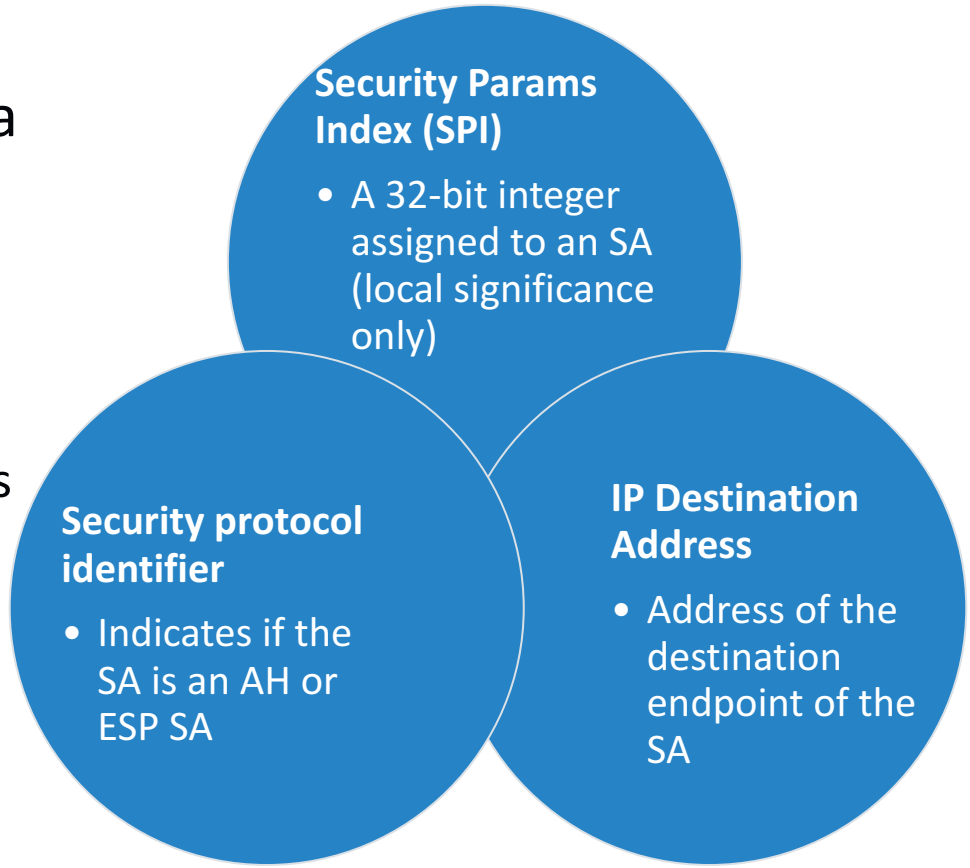
Πολιτικές IPsec

IPsec architecture



Security association: SA

- A one-way logical connection between a sender and a receiver
- The SA is uniquely identified by
  - the Destination Address in the IPv4/IPv6 header
  - and the SPI in the enclosed extension header (AH or ESP)



Security association

- SAs are not fixed (generated/customized per traffic flows)
  - Manual (no lifetime)
  - Dynamic (lifetime)
- Additionally SAs determine:
  - IPsec processing/encoding for senders (outbound)
  - IPsec processing/decoding for receivers (inbound)
- A major function of IKE is the establishment and maintenance of SAs

Security association: SPI

- The SPI is 32 bits long
- It is included in all AH and ESP headers
- It is assigned to the SA and has local significance
  - It enables the sending system to select the SA under which an outgoing packet will be processed/encoded
  - It enables the receiving system to select the SA under which an incoming packet will be processed/decoded
- The SPI is the index in the SA database where the associated SA is stored

Security association db: SAD

- Defines the parameters associated with each SA
- Normally defined by the following parameters in an SAD entry:
  - Security parameter index
  - Sequence number counter
  - Sequence counter overflow
  - Anti-replay window
  - AH information
  - ESP information
  - Lifetime of this security association
  - IPsec protocol mode
  - Path MTU

Security policy database (SPD)

- The means by which IP traffic is related to specific SAs

  Contains entries, each of which defines a subset of IP traffic and points to an SA for that traffic

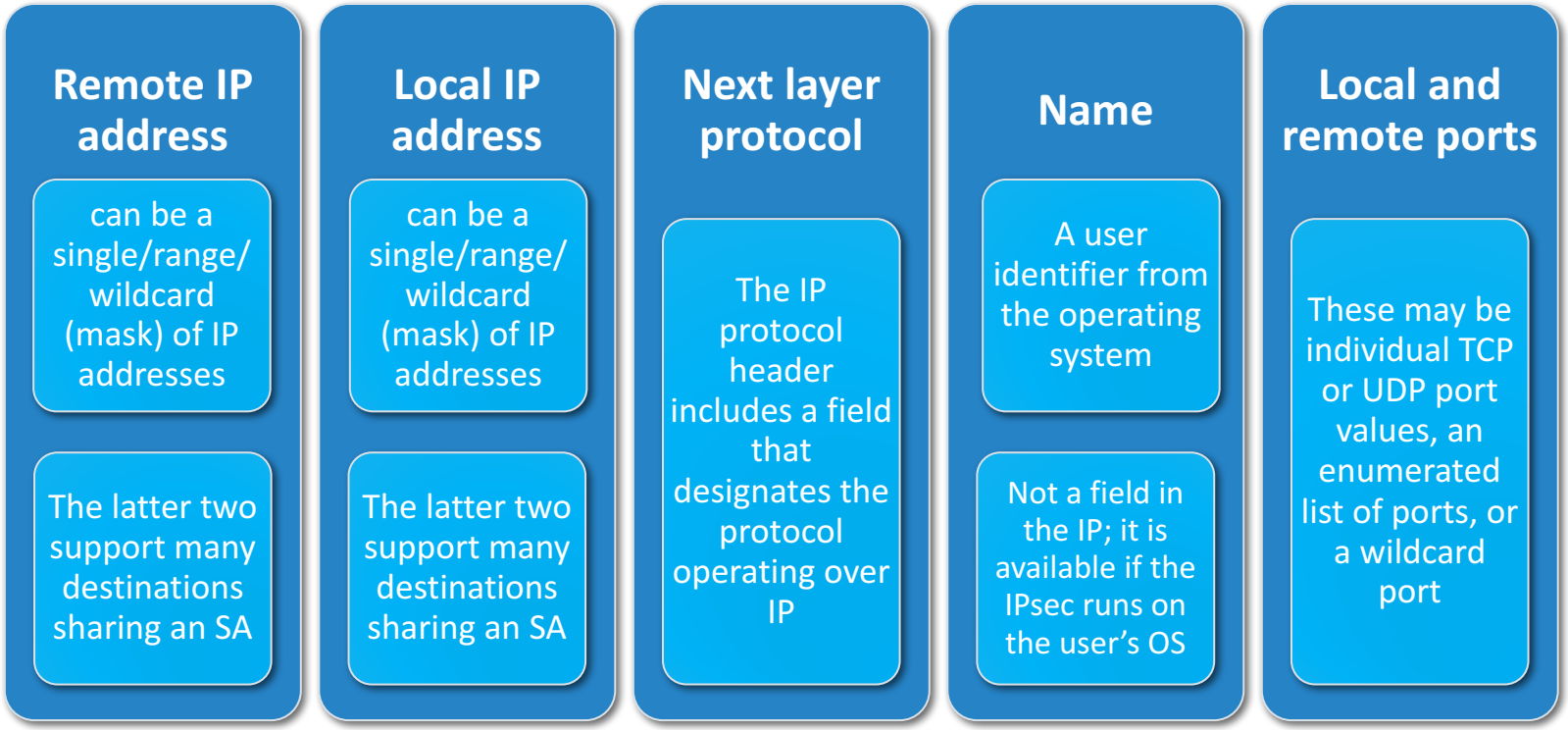
- In more complex environments, there may be multiple entries that potentially relate to a single SA or multiple SAs associated with a single SPD entry

  Each SPD entry is defined by a set of IP and upper-layer protocol field values called *selectors*

  These are used to filter outgoing traffic in order to map it into a particular SA

SPD entries

- The following selectors determine an SPD entry



SPD responsibility

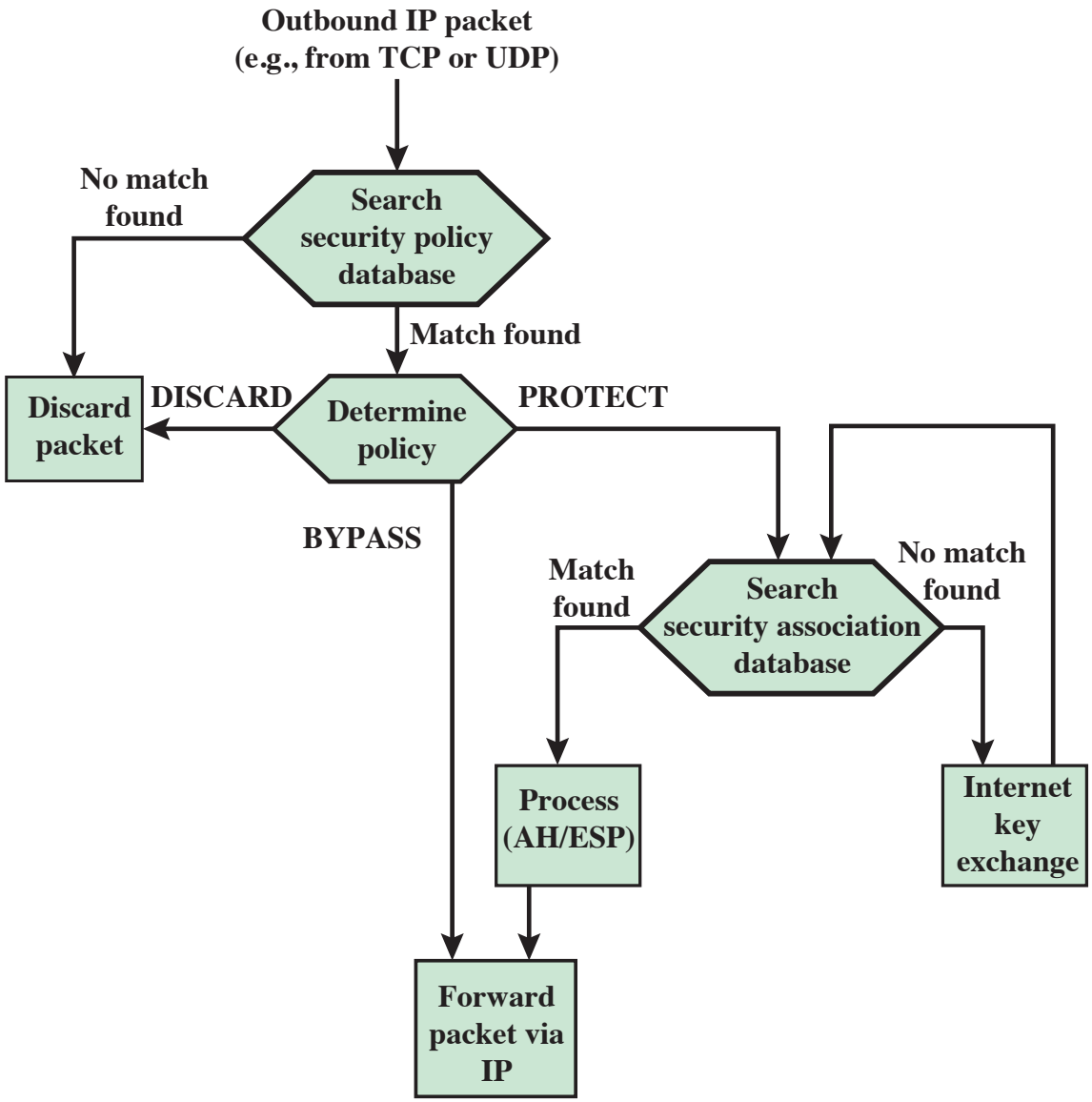
- For any outbound or inbound datagram, three processing choices are possible:
  - *Discard:* refers to traffic that is not allowed to exit the host, traverse the security gateway, or be delivered to an application at all
  - *Bypass IPsec:* refers to traffic that is allowed to pass without additional IPsec protection
  - *Apply IPsec:* refers to traffic that is afforded IPsec protection, and for such traffic the SPD must specify
    - The security services to be provided
    - The protocols and algorithms to be employed
    - …

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

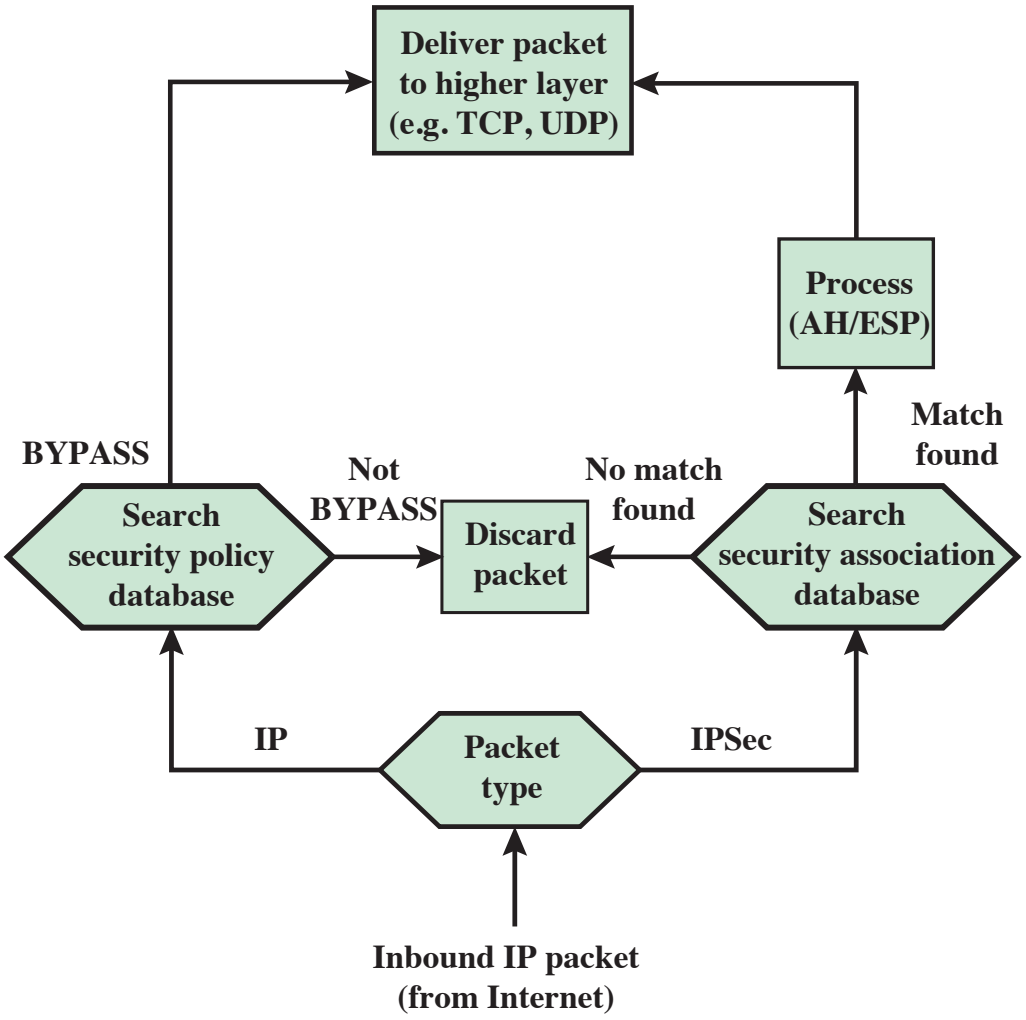
Outbound packets

Processing model



Inbound packets

Processing model

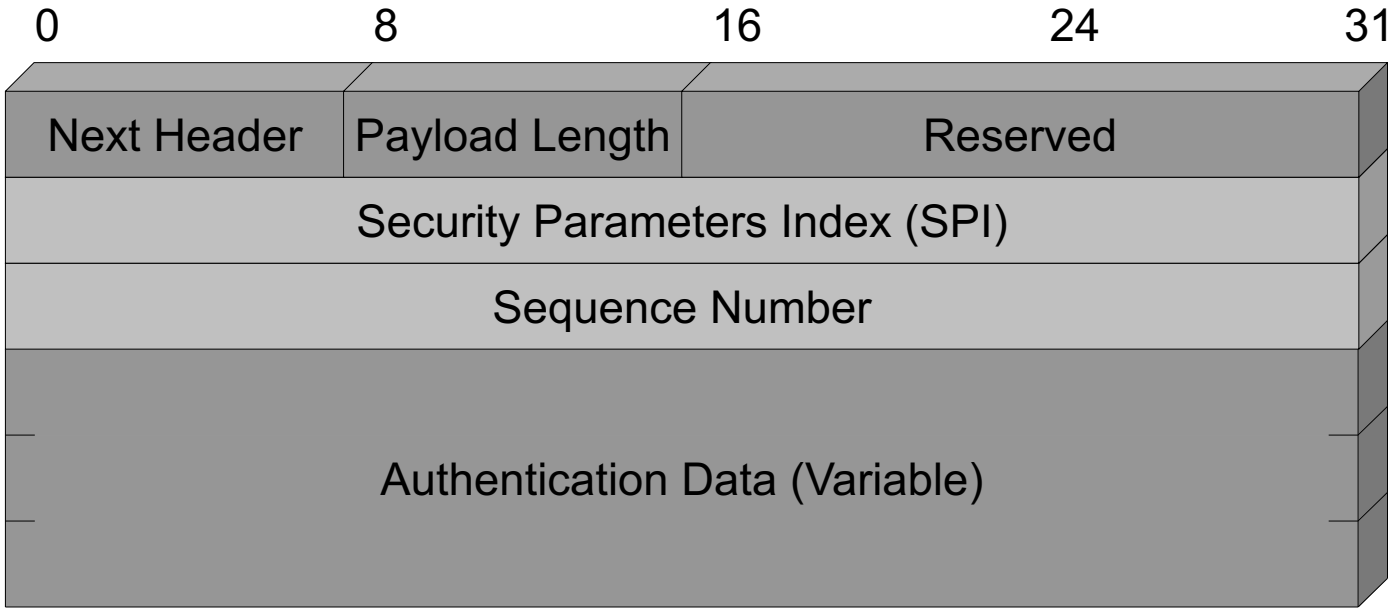


Υπηρεσία AH

Authentication header

- Provides support for authentication of IP packets
  - Use of Integrity Check Value (ICV) calculated by means of Message Authentication Codes (MAC)
- Ensures that content changes of a packet in transit can be detected (data integrity)
  - Enables an end-system to authenticate the user or application and filter traffic accordingly
  - Prevents the address spoofing attacks
- Guards against the replay attack
  - Use of anti-replay service via sequence number

Authentication header: format



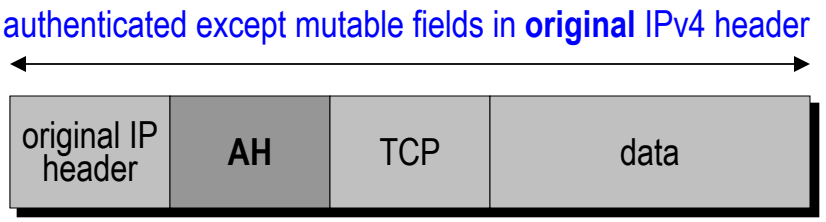
Authentication header: ICV

- The AH ICV is computed over:
  - IP header fields that are either
    - immutable in transit, or
    - mutable but predictable in value upon arrival at the endpoint for the AH SA
  - The AH header (authentication data are set to zero for this computation)
  - The upper level protocol data, which is assumed to be immutable in transit
- Code may be truncated to first 96 bits

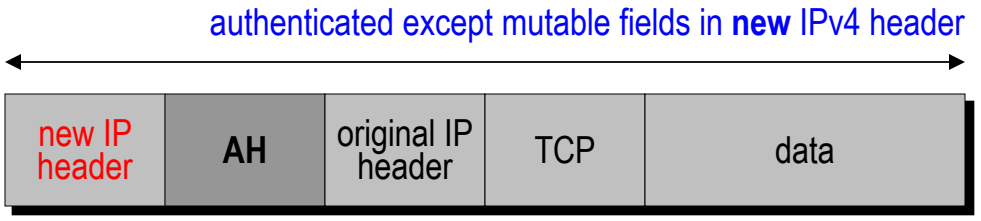
Authentication header in IPv4

Prior applying AH:

Transport mode AH:



Tunnel mode AH:

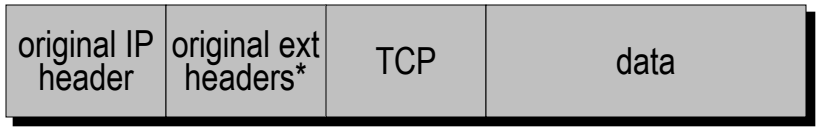


Authentication header in IPv4

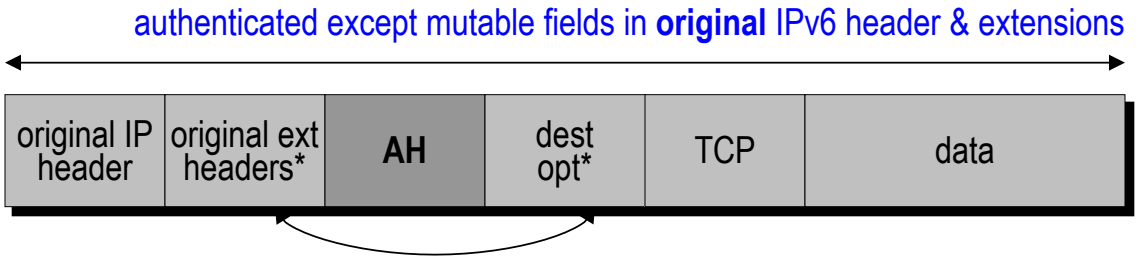
- Immutable
  - Version, Internet Header Length, Total Length, Identification
  - Protocol (this should be the value for AH)
  - Source Address, Destination Address
- Mutable but predictable
  - Destination Address (with loose or strict source routing)
- Mutable (zeroed prior to ICV calculation)
  - Type of Service, Flags, Fragment Offset, TTL, Header Checksum

Authentication header in IPv6

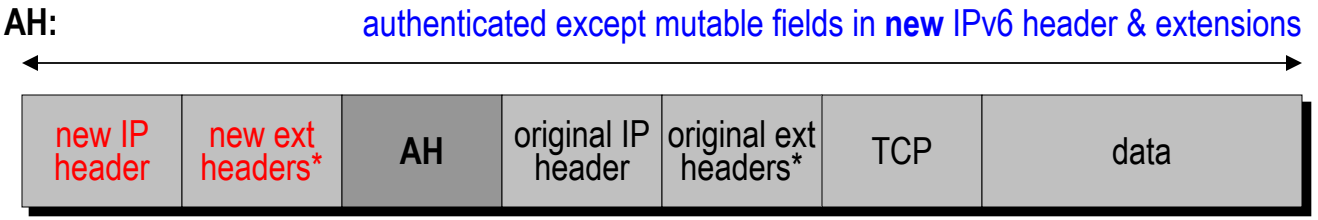
Prior applying AH:



Transport mode AH:



Tunnel mode AH:

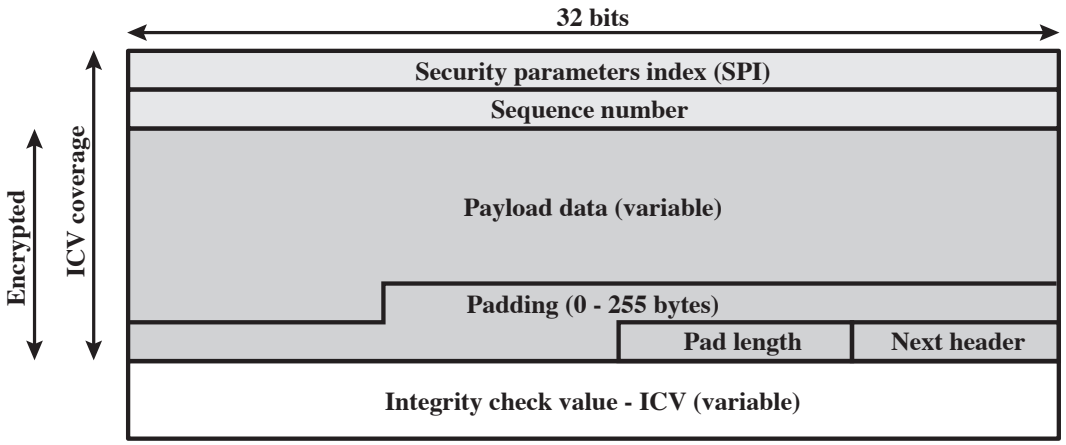


Authentication header in IPv6

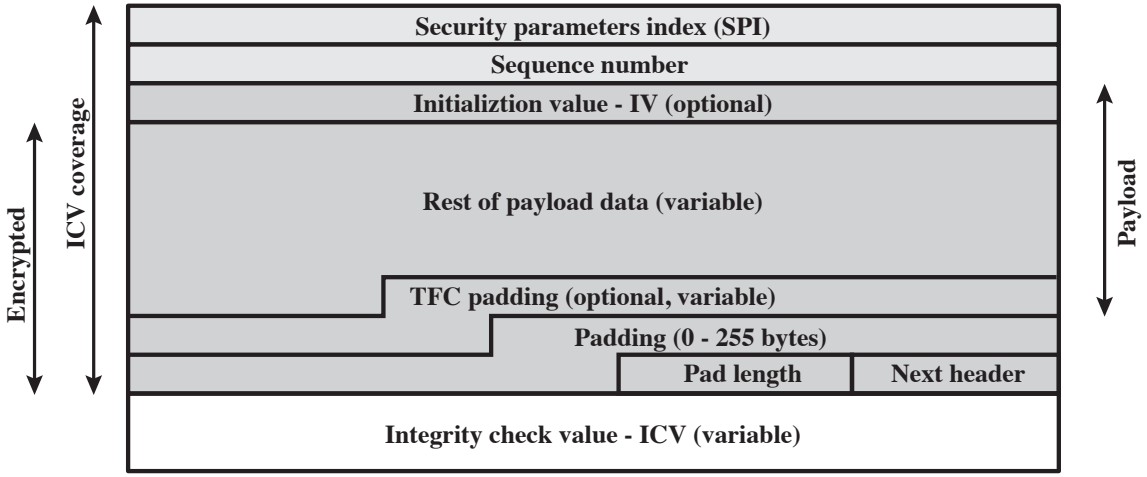
- Immutable
  - Version, Payload Length
  - Next Header (this should be the value for AH)
  - Source Address, Destination Address
- Mutable but predictable
  - Destination Address (with Routing Extension Header)
- Mutable (zeroed prior to ICV calculation)
  - Class, Flow Label, Hop Limit

Υπηρεσία ESP

ESP packet format



(a) Top-level format of an ESP Packet



(b) Substructure of payload data

Encapsulating security payload

- Used to encrypt the Payload Data, Padding, Pad Length, and Next Header fields
  - If the algorithm requires cryptographic sync data, these data may be carried explicitly at the beginning of the Payload Data field
- An optional ICV field is present only if the integrity service is selected
  - ICV is computed after the encryption is performed
  - This order of processing facilitates reducing DoS attacks' impact
  - Because the ICV is not protected by encryption, a keyed integrity algorithm must be employed to compute the ICV

Encapsulating security payload

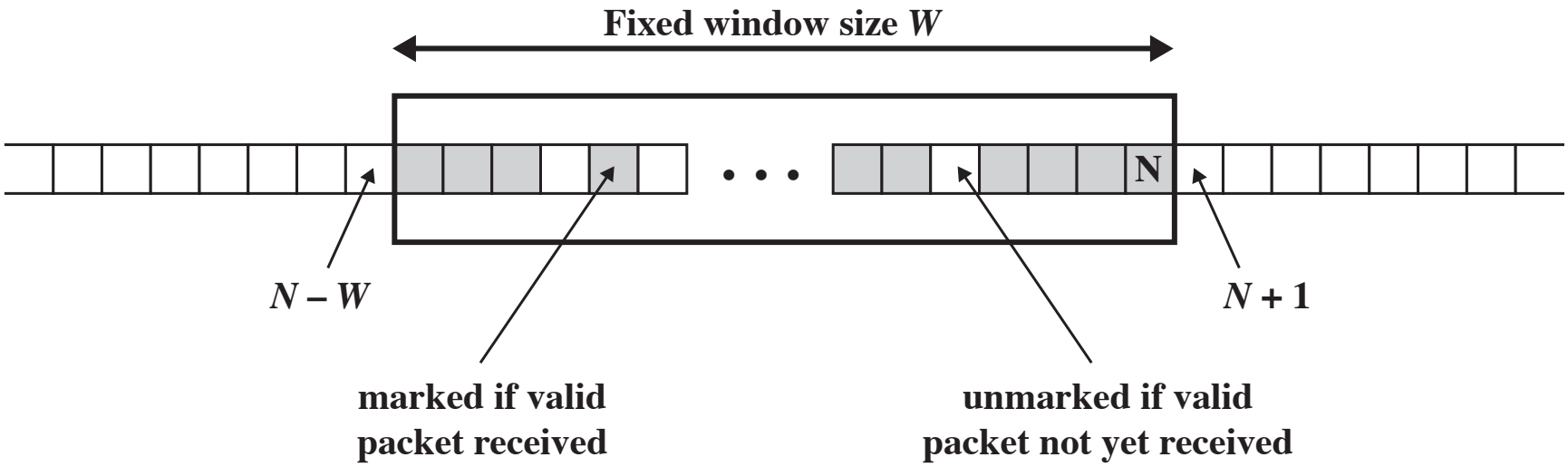
- The Padding field serves several purposes
  - If an encryption algorithm requires the plaintext to be a multiple of some number of bytes, the Padding field is used to expand the plaintext to the required length
  - Used to assure alignment of Pad Length and Next Header fields
  - Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload

IPsec anti-replay mechanism

- When a new SA is established, the sender initializes a sequence number counter to 0
- Each time a packet is sent on this SA, the sender increments the counter (copied to *Sequence Number*)
- If anti-replay is enabled (the default) the sender must not allow the sequence number to cycle past $2^{32} – 1$ back to 0
  - There would be valid packets with the same sequence number
- If the limit of $2^{32} – 1$ is reached, the sender should terminate this SA, and negotiate a new SA with a new key

IPsec anti-replay mechanism

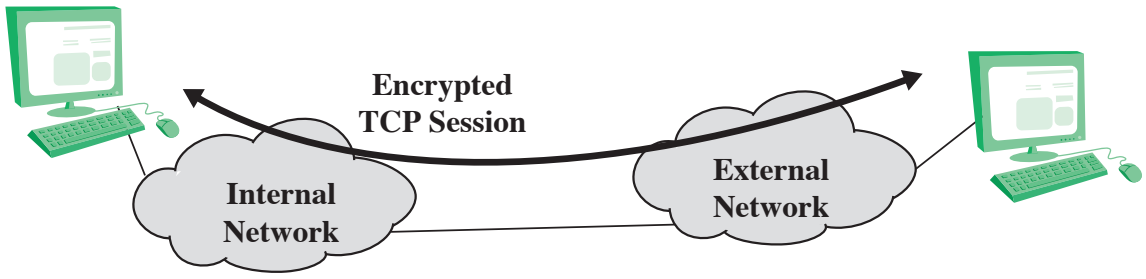
- Window size *W* can be 32 or 46



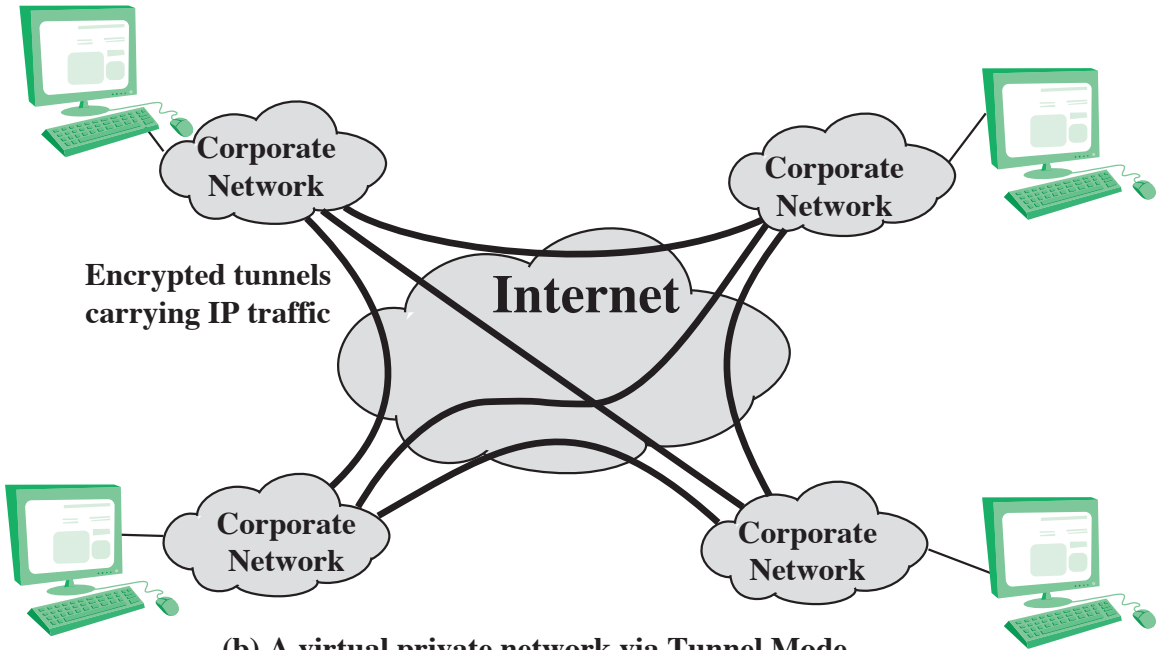
IPsec anti-replay mechanism

- a received packet falls in the window
  - If authenticated and unmarked, mark it
  - If marked, then it is a replay!
- If a received packet is > *N* (and <= 2^{32} - 1)
  - If authenticated, advance the window so that this packet is at the rightmost edge and mark it
- If a received packet is <= *N* - *W*
  - Then packet is discarded

Transport vs. tunnel mode encryption



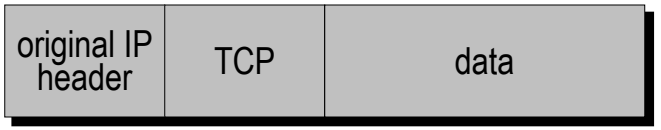
(a) Transport-level security



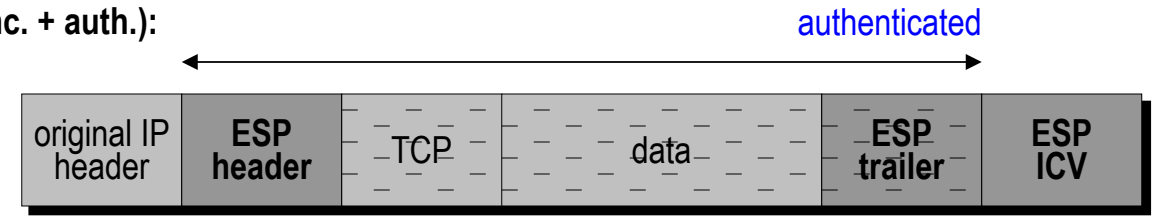
(b) A virtual private network via Tunnel Mode

Enc. security payload in IPv4

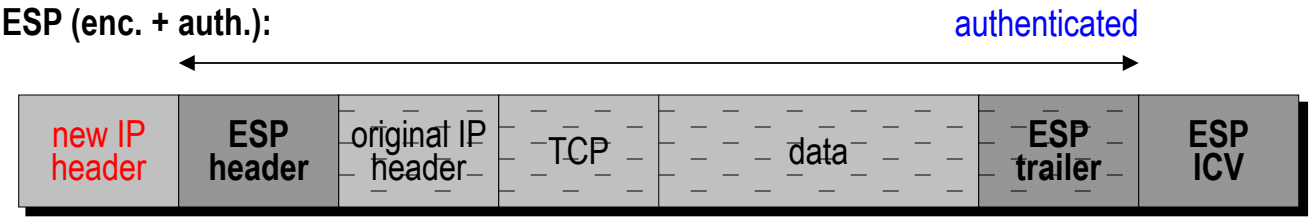
Prior applying ESP:



Transport mode ESP (enc. + auth.):

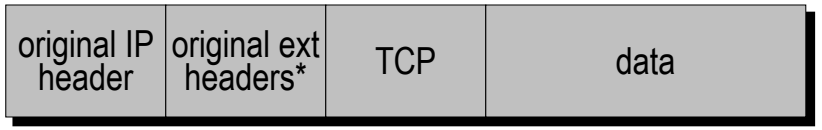


Tunnel mode ESP (enc. + auth.):

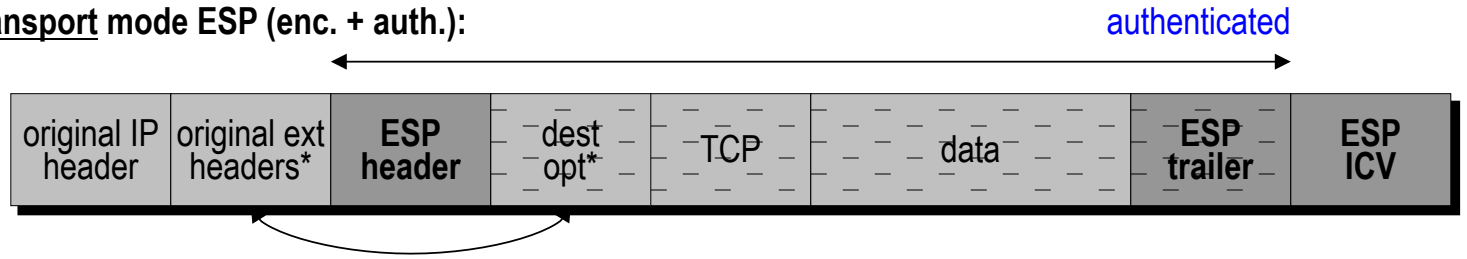


Enc. security payload in IPv6

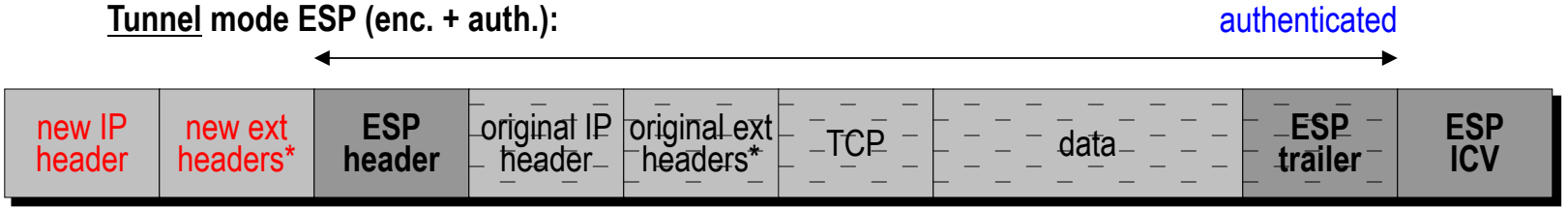
Prior applying ESP:



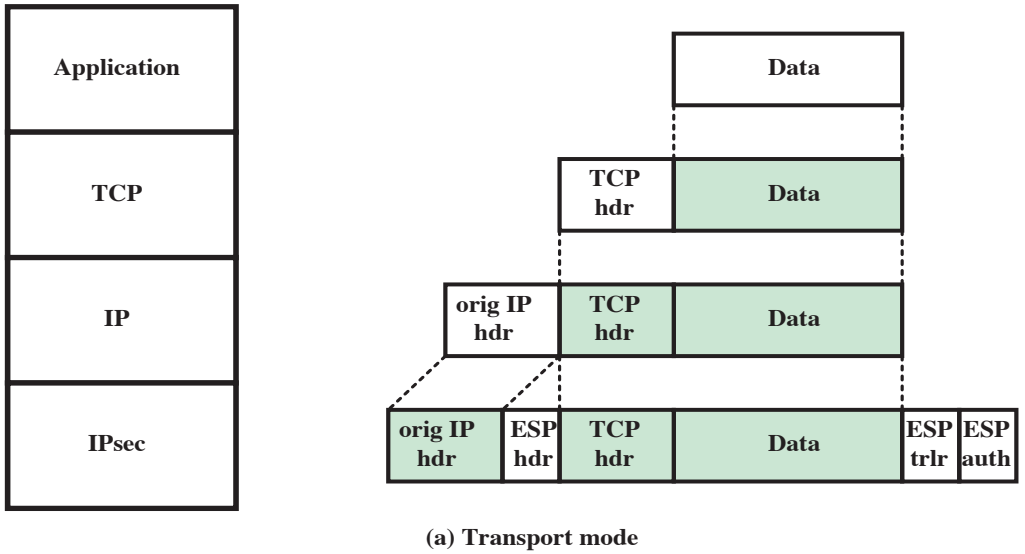
Transport mode ESP (enc. + auth.):



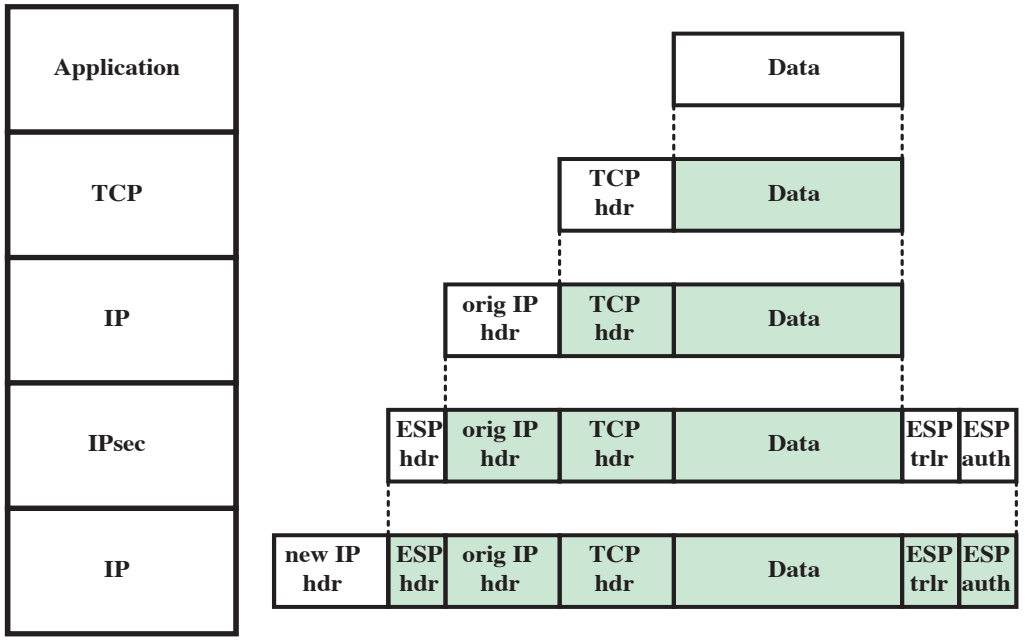
Tunnel mode ESP (enc. + auth.):



Protocol operation for ESP



(a) Transport mode



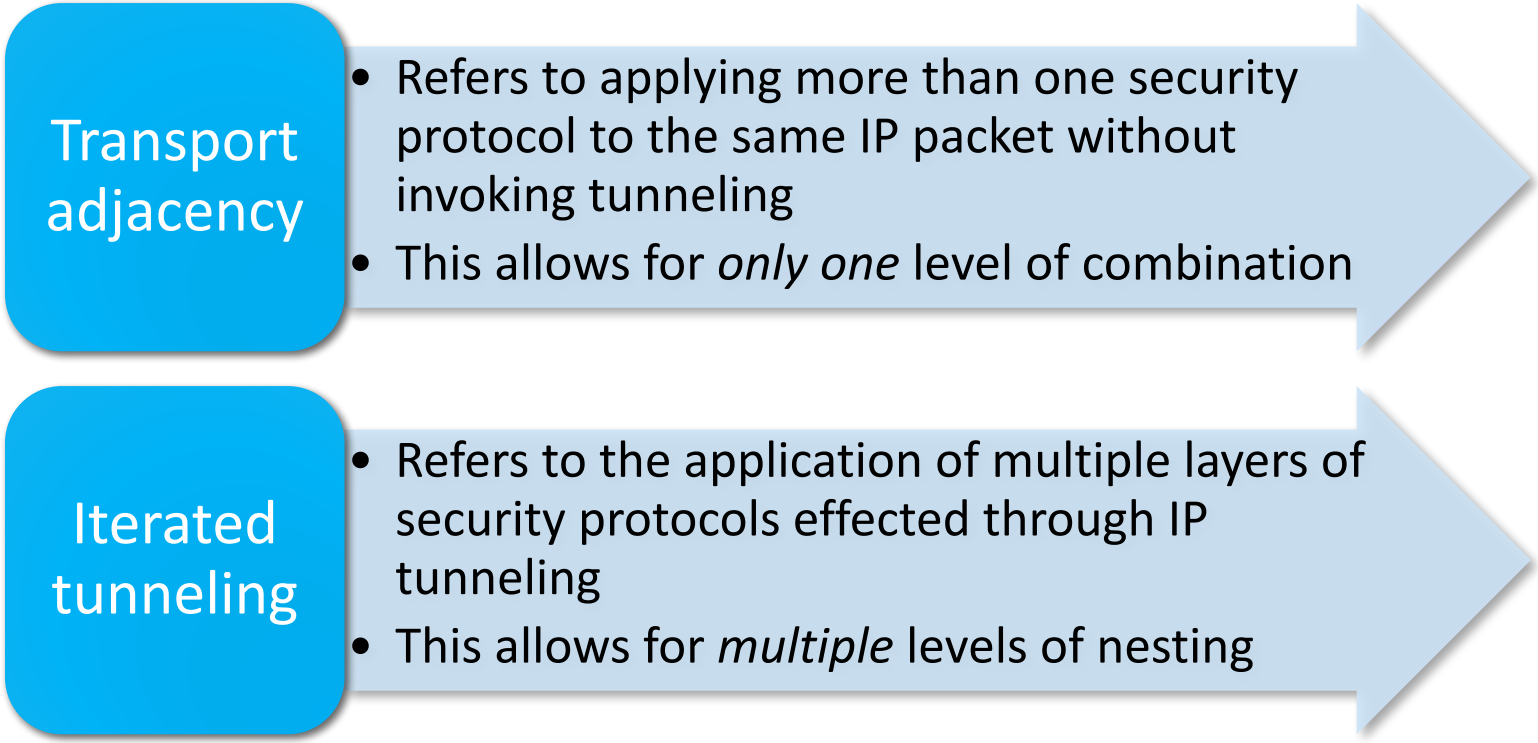
(b) Tunnel mode

Combining security associations

- An individual SA can implement either the AH or ESP protocol but not both
- *Security association bundle*
  - Refers to a sequence of SAs through which traffic must be processed to provide a desired set of IPsec services
  - The SAs in a bundle may terminate at different endpoints or at the same endpoint

Combining security associations

- May be combined into bundles in two ways



ESP with authentication option

- In this approach, the first user applies ESP to the data to be protected and then appends the authentication data

Transport mode ESP

- Authentication and encryption apply to the IP payload delivered to the host, but the IP header is not protected

Tunnel mode ESP

- Authentication applies to the entire packet delivered to the outer IP destination address and authentication is performed at that destination
- The entire inner IP packet is protected by the privacy mechanism for delivery to the inner IP destination

- For both cases authentication applies to the ciphertext rather than the plaintext

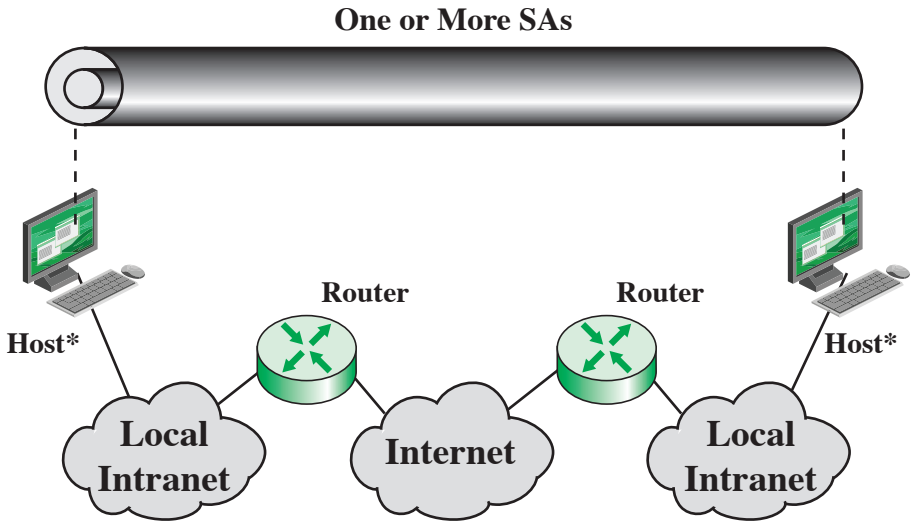
Transport adjacency

- Another way to apply authentication after encryption is to use two bundled transport SAs, with the inner being an ESP SA and the outer being an AH SA
  - In this case ESP is used without its authentication option
  - Encryption is applied to the IP payload
  - AH is then applied in transport mode
  - Advantage of this approach is that the authentication covers more fields
  - Disadvantage is the overhead of two SAs versus one SA

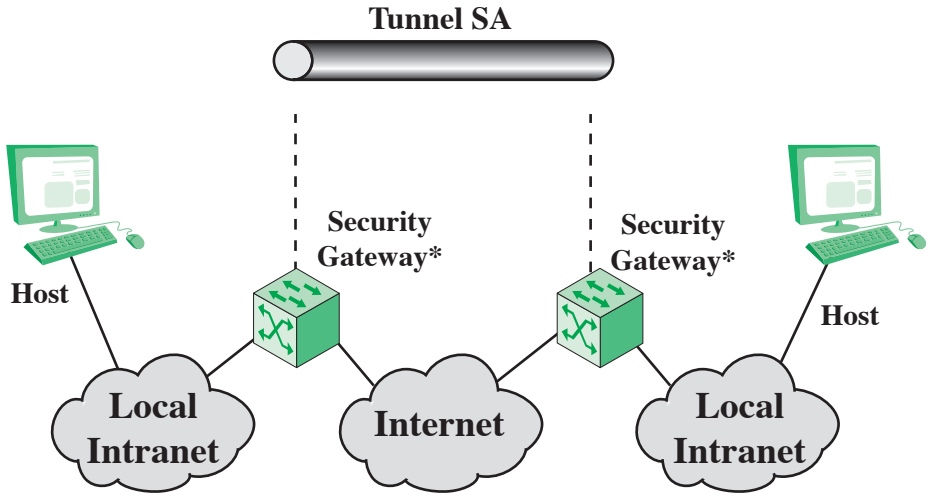
Transport-tunnel bundle

- The use of authentication prior to encryption might be preferable for several reasons:
  - It is impossible for anyone to intercept the message and alter the authentication data without detection
  - It may be desirable to store the authentication information with the message at the destination for later reference
- One approach is to use a bundle consisting of an inner AH transport SA and an outer ESP tunnel SA
  - Authentication is applied to the IP payload plus the IP header
  - The resulting IP packet is then processed in tunnel mode by ESP
    - The result is that the entire authenticated inner packet is encrypted and a new outer IP header is added

Basic combinations of SAs

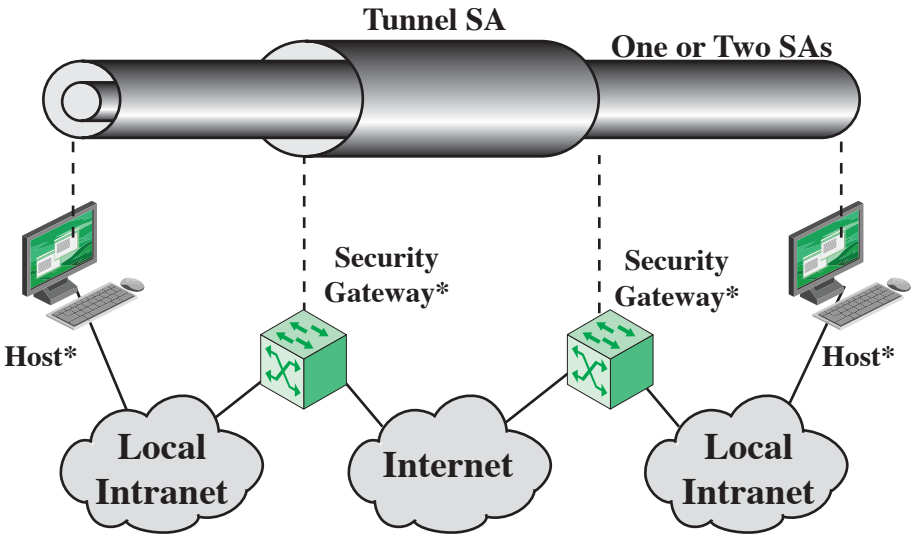


(a) Case 1

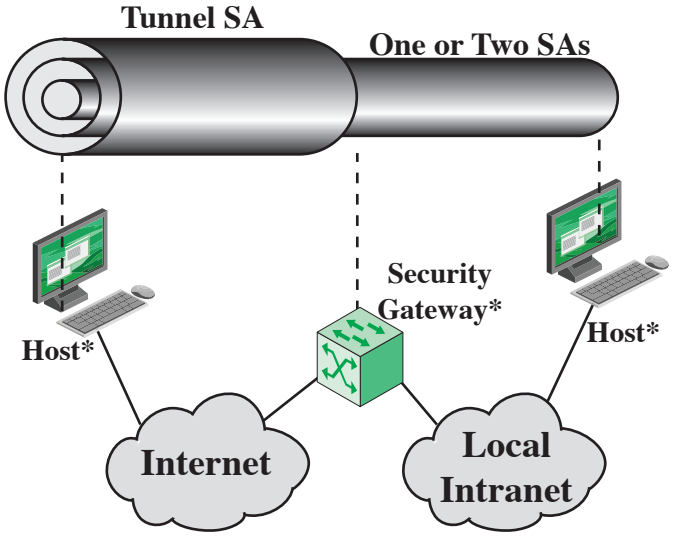


(b) Case 2

Basic combinations of SAs



(c) Case 3



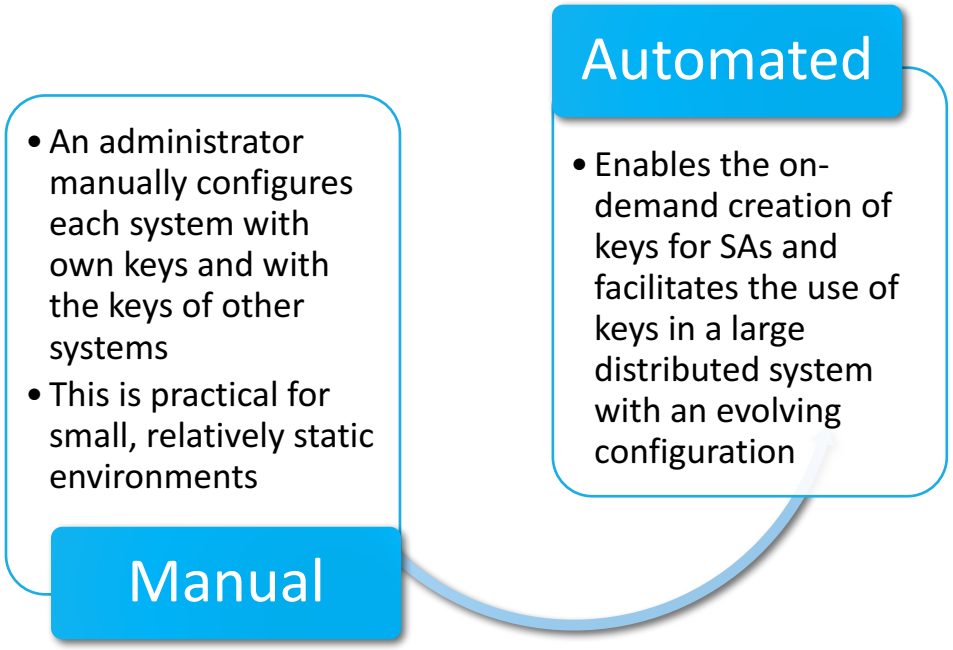
(d) Case 4

Internet key exchange

Internet key exchange

- Key management is about determining & distributing keys
  - A requirement is four keys for communication between two applications
  - Transmit and receive pairs for both integrity and confidentiality

- The IPsec supports two types of key management



Internet key exchange

- The automated key management is referred to as *Internet Key Exchange* (IKE)
  - It provides a standardized method for dynamically authenticating IPsec peers and negotiating security parameters
- Negotiated Parameters
  - Authentication Mechanism (secret or public key, certificates)
  - Encryption Algorithm (mode, key length, initialization vector)
  - Hash Algorithm
  - Key values and key lifetimes
  - SA renewal period

ISAKMP/Oakley

- The default automated key management protocol of IPsec
- Consists of:
  - Internet Security Association and Key Management Protocol (ISAKMP)
    - Provides a framework for Internet key management and provides the specific protocol support, including formats, for negotiation of security attributes
    - Consists of a set of message types that enable the use of a variety of key exchange algorithms
  - Oakley Key Determination Protocol
    - A key exchange protocol based on the Diffie-Hellman algorithm but providing added security
    - Generic in that it does not dictate specific formats

ISAKMP negotiation phases

- Negotiation phase 1
  - Two entities agree on how to protect further negotiation traffic by establishing an ISAKMP SA
  - The ISAKMP SA is then used to protect the negotiations for the Protocol SA being requested
  - The entities can negotiate (and have active) multiple ISAKMP SAs
- Negotiation phase 2
  - Used to establish SAs for other security protocols (e.g. IPsec)

ISAKMP payload types

- ISAKMP has several payload types
  - Chaining (each payload points to the next one)
  - They are used to carry different types of information for SA generation and management
- Some payload types
  - SA payload (to exchange the DoI information)
  - Proposal & Transform payloads (to exchange the security and cryptographic capabilities in the DoI)
  - Key Exchange payload (to exchange the key exchange info)
- Other payload types (nonce, identification, certificate, certificate request, signature, …)

ISAKMP exchanges: base

- The *Base Exchange* is designed to allow to transmit together
  - Key Exchange related information
  - Authentication related information

- As a result, reduces the number of round-trips at the expense of not providing identity protection
  - Identities are exchanged before a common shared secret has been established
  - Therefore, encryption of the identities is not possible

ISAKMP exchanges: base

Step	Host-1		Host-2	Notes
1	HDR | SA | NONCE	→		▪ Begin ISAKMP SA negotiation ▪ NONCE protects from replay attacks (used by AUTH)
2		←	HDR | SA | NONCE	▪ Basic SA accepted by Host-2 ▪ NONCE protects from replay attacks (used by AUTH)
3	HDR | KE | ID-1 | AUTH	→		▪ Key material is used to derive a shared secret ▪ Host-1 identity verified by Host-2
4		←	HDR | KE | ID-2 | AUTH	▪ Key material is used to derive a shared secret ▪ Host-2 identity verified by Host-1

ISAKMP exchanges: id protection

- The *Identity Protection Exchange* is designed to
  - Separate *Key Exchange* information from
  - *Identity* and *Authentication* related information

- As a result, provides identity protection of the communicating identities at the expense of two additional messages
  - Identities are exchanged under the protection of a previously established common shared secret

ISAKMP exchanges: id protection

Step	Host-1		Host-2	Notes
1	HDR | SA	→		▪ Begin ISAKMP SA negotiation
2		←	HDR | SA	▪ Basic SA (protection suite) accepted by Host-2
3	HDR | KE | NONCE	→		▪ Key material is used to derive a shared secret ▪ NONCE protects from replay attacks (used by AUTH)
4		←	HDR | KE | NONCE	▪ Key material is used to derive a shared secret ▪ NONCE protects from replay attacks (used by AUTH)
5	HDR | ID-1 | AUTH	→		▪ Secured Host-1 identity verified by Host-2
6		←	HDR | ID-2 | AUTH	▪ Secured Host-2 identity verified by Host-1

ISAKMP exchanges: aggressive

- The *Aggressive Exchange* is designed to transmit together the following payloads
  - Authentication,
  - Security Association, and
  - Key Exchange
- As a result, reduces the number of round-trips at the expense of not providing identity protection
  - Identities are exchanged before a common shared secret has been established
  - Therefore, encryption of the identities is not possible
- Attempts to establish all security relevant information in a single exchange

ISAKMP exchanges: aggressive

Step	Host-1		Host-2	Notes
1	HDR | SA | KE | NONCE | ID-1	→		▪ Begin ISAKMP SA negotiation ▪ Key material is used to derive a shared secret ▪ NONCE protects from replay attacks (used by AUTH) ▪ There can only be one Proposal and one Transform offered
2		←	HDR | SA | KE | NONCE | ID-2 | AUTH	▪ Basic SA (protection suite) accepted by Host-2 ▪ Key material is used to derive a shared secret ▪ NONCE protects from replay attacks (used by AUTH) ▪ Host-1 identity has been verified by Host-2
3	HDR | AUTH	→		▪ Host-1 transmits the results of the agreed upon authentication function ▪ Information is transmitted under the protection of the common shared secret ▪ Host-2 identity has been verified by Host-1

Oakley key determination

- Algorithm is characterized by five important features

1. It employs a mechanism known as cookies to thwart clogging attacks
2. It enables the two parties to negotiate a group; this, in essence, specifies the global parameters of the Diffie-Hellman key exchange
3. It uses nonces to ensure against replay attacks
4. It enables the exchange of Diffie-Hellman public key values
5. It authenticates the Diffie-Hellman exchange to thwart man-in-the-middle-attacks

The phases of IKE

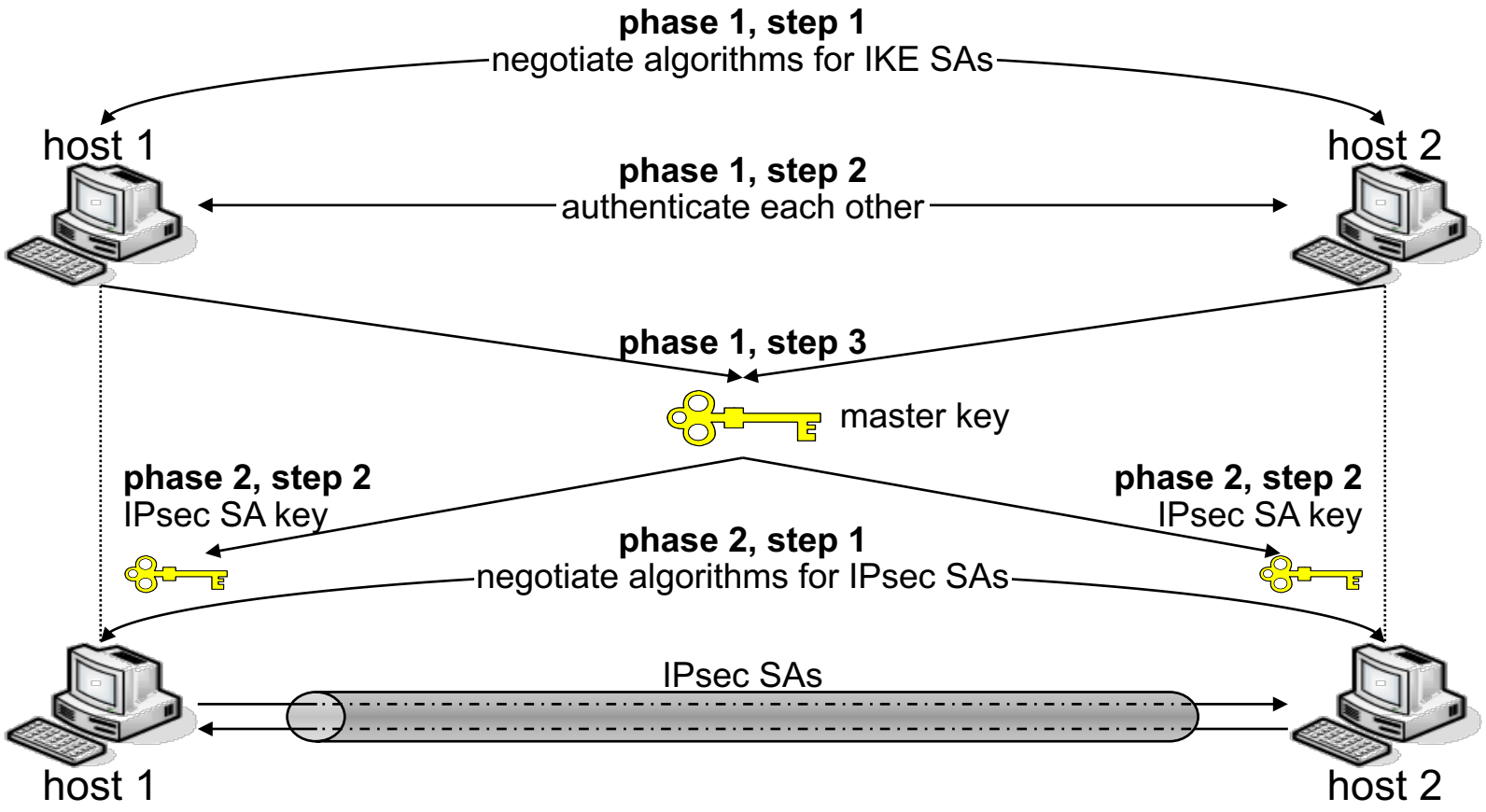
PHASE I

- Establish a secure channel
  - Used to define encryption & authentication of IKE traffic
  - Multiple IPsec SAs can be established with one IKE SA
- Authenticate host identity
- Establishes session key
  - Diffie-Hellman key exchange

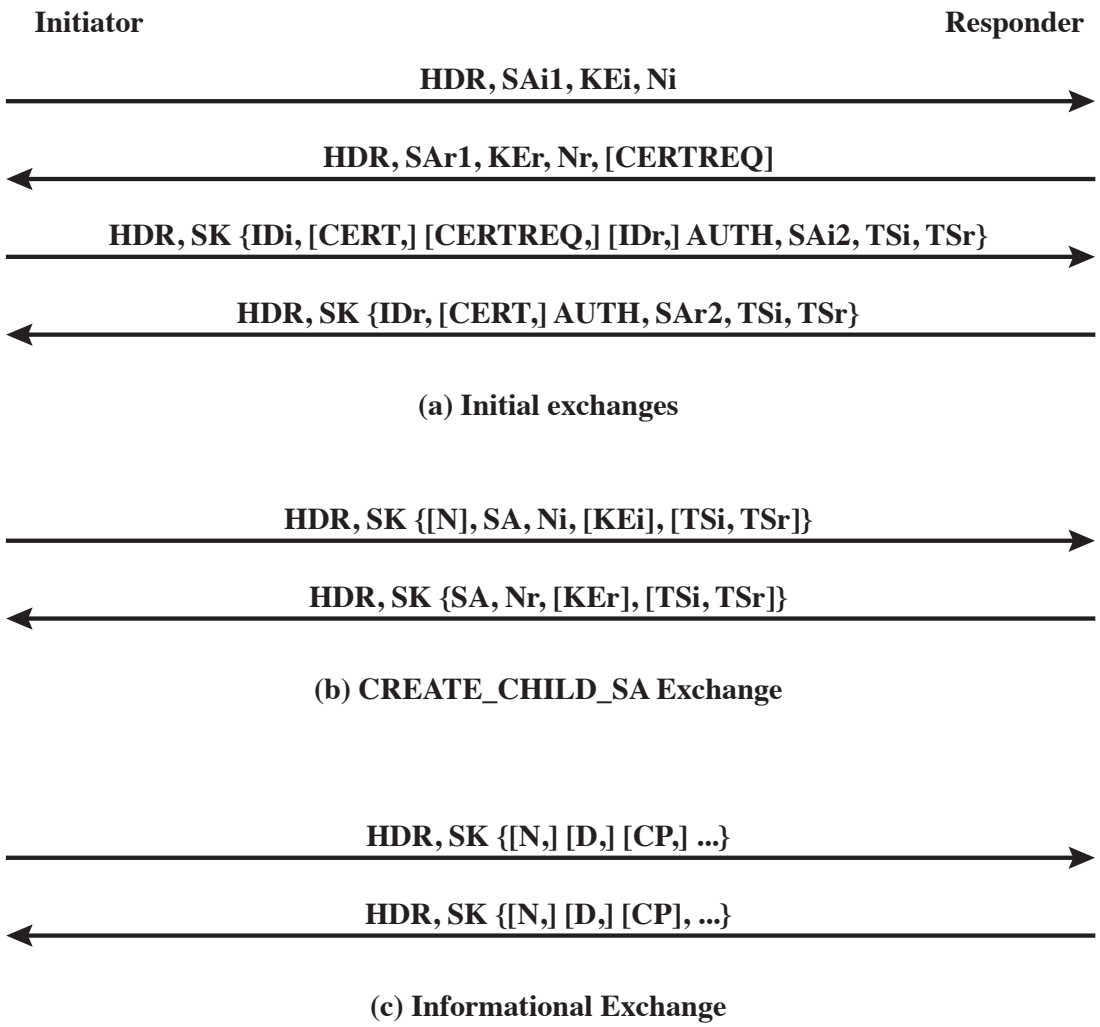
PHASE II

- Use IKE SA to negotiate IPsec SAs
  - Establish a secure channel between computers intended for the transmission of data
  - Can establish multiple session keys (ESP SA, AH SA, …)
- IKE SA is used to protect this exchange

Overview of IKE



IKE v2 exchanges



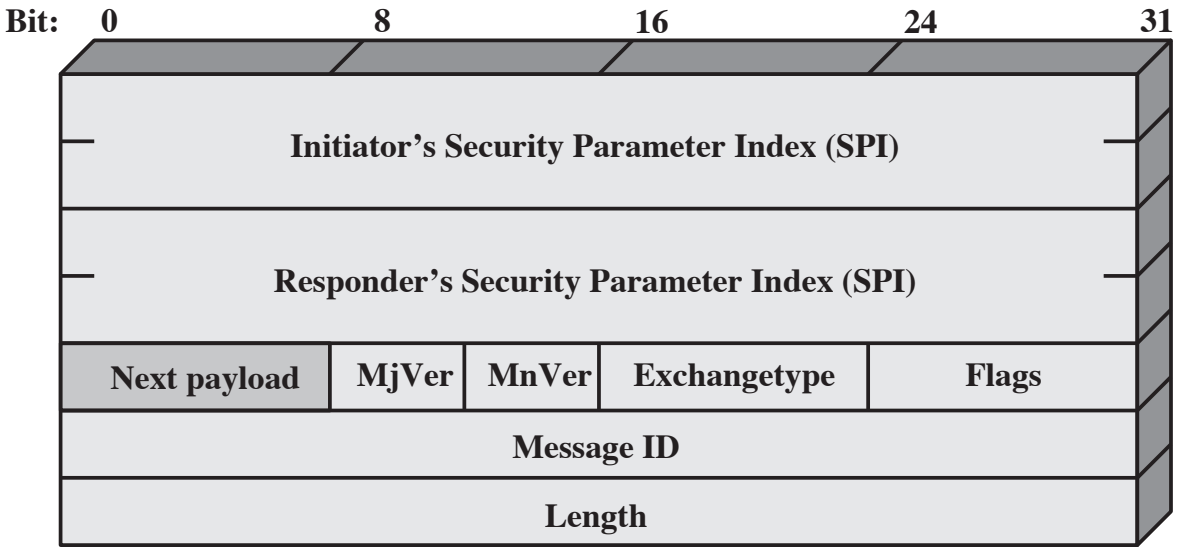
HDR = IKE header
SAx1 = offered and chosen algorithms, DH group
KEx = Diffie-Hellman public key
Nx= nonces
CERTREQ = Certificate request
IDx = identity
CERT = certificate

SK {...} = MAC and encrypt
AUTH = Authentication
SAx2 = algorithms, parameters for IPsec SA
TSx = traffic selectors for IPsec SA
N = Notify
D = Delete
CP = Configuration

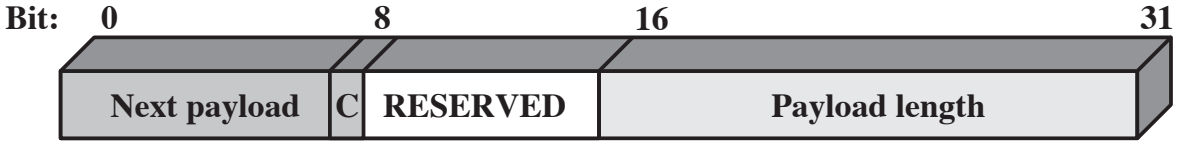
IKE authentication methods

- Authentication methods of IKE
  - Certificate-based public key signature
    - Certificates are exchanged
  - Public-key encryption
    - Some key material exchanged using previously known public keys
    - No certificates, so no non-repudiation
  - Pre-shared keys
    - Symmetric method
    - Simplest, no public key crypto
- Material to be authenticated is derived from the messages exchanged

IKE formats



(a) IKE Header



(b) Generic Payload Header

IPsec messages

Error Messages	Status Messages
Unsupported Critical Payload	Initial Contact
Invalid IKE SPI	Set Window Size
Invalid Major Version	Additional TS Possible
Invalid Syntax	IPCOMP Supported
Invalid Payload Type	NAT Detection Source IP
Invalid Message ID	NAT Detection Destination IP
Invalid SPI	Cookie
No Proposal Chosen	Use Transport Mode
Invalid KE Payload	HTTP Cert Lookup Supported
Authentication Failed	Rekey SA
Single Pair Required	ESP TFC Padding Not Supported
No Additional SAS	Non First Fragments Also
Internal Address Failure	
Failed CP Required	
TS Unacceptable	
Invalid Selectors	

IKE payload types

Type	Parameters
Security Association	Proposals
Key Exchange	DH Group #, Key Exchange Data
Identification	ID Type, ID Data
Certificate	Cert Encoding, Certificate Data
Certificate Request	Cert Encoding, Certification Authority
Authentication	Auth Method, Authentication Data
Nonce	Nonce Data
Notify	Protocol-ID, SPI Size, Notify Message Type, SPI, Notification Data
Delete	Protocol-ID, SPI Size, # of SPIs, SPI (one or more)
Vendor ID	Vendor ID
Traffic Selector	Number of TSs, Traffic Selectors
Encrypted	IV, Encrypted IKE payloads, Padding, Pad Length, ICV
Configuration	CFG Type, Configuration Attributes
Extensible Authentication Protocol	EAP Message

Cryptographic suites for IPsec

- (a) Virtual private networks (RFC 4308)

	VPN-A	VPN-B
ESP encryption	3DES-CBC	AES-CBC (128-bit key)
ESP integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE encryption	3DES-CBC	AES-CBC (128-bit key)
IKE PRF	HMAC-SHA1	AES-XCBC-PRF-128
IKE Integrity	HMAC-SHA1-96	AES-XCBC-MAC-96
IKE DH group	1024-bit MODP	2048-bit MODP

Cryptographic suites for IPsec

- (b) NSA Suite B (RFC 6379)

	GCM-128	GCM-256	GMAC-128	GMAC-256
ESP encryption/ Integrity	AES-GCM (128-bit key)	AES-GCM (256-bit key)	Null	Null
ESP integrity	Null	Null	AES-GMAC (128-bit key)	AES-GMAC (256-bit key)
IKE encryption	AES-CBC (128-bit key)	AES-CBC (256-bit key)	AES-CBC (128-bit key)	AES-CBC (256-bit key)
IKE PRF	HMAC-SHA-256	HMAC-SHA-384	HMAC-SHA-256	HMAC-SHA-384
IKE Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192	HMAC-SHA-256-128	HMAC-SHA-384-192
IKE DH group	256-bit random ECP	384-bit random ECP	256-bit random ECP	384-bit random ECP

Επιθέσεις στο IPsec

Είναι το IPsec ασφαλές?

- Η κεφαλίδα AH είναι προαιρετική
- Δηλ. υπάρχει η δυνατότητα στους μηχανικούς δικτύων να υλοποιήσουν IPsec όπου δεν γίνεται αυθεντικοποίηση
  - Πολλές φορές μία τέτοια προσέγγιση είναι αυτή που προτείνεται, για λόγους ταχύτητας
- Δημιουργεί αυτό πρόβλημα στην ασφάλεια?

Επίθεση στο IPsec

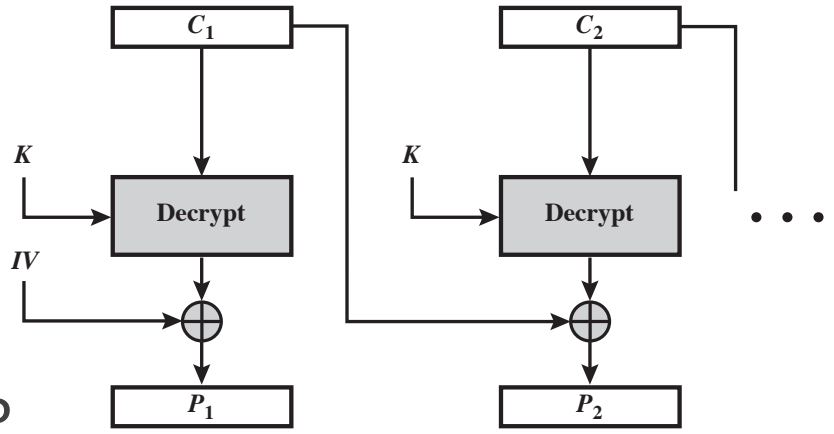
- Στην εργασία των Paterson και Yau (Eurocrypt, 2006)
  - Επιτυχής κρυπτανάλυση, χωρίς να χρειάζεται γνώση κάποιου τμήματος του αρχικού μηνύματος παρά μόνο ολόκληρη (ή τμήμα) της IP διεύθυνσης προορισμού ενός IP datagram
  - Συσκευή που υλοποιεί την κρυπτανάλυση στο IPsec δούλεψε αποδοτικά και έδωσε αποτέλεσμα, ανακαλύπτοντας τα αρχικά μηνύματα (σε περιβάλλον Linux)
  - Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιήθηκε στις υλοποιήσεις του IPsec είναι ο πολύ ισχυρός AES – ωστόσο, η κρυπτανάλυση πέτυχε
- Η επίθεση αφορά την περίπτωση ESP με κρυπτογράφηση μόνο (χωρίς αυθεντικοποίηση)

Βασική ιδέα

- Επιθέσεις αναστροφής bit (bit flipping)
  - Υποθέτουμε ότι ο επιτιθέμενος γνωρίζει τη διεύθυνση προορισμού του πακέτου
    - βρίσκεται κρυπτογραφημένη στο ενθυλακωμένο πακέτο
  - Λόγω της CBC δομής ο επιτιθέμενος μπορεί να τροποποιήσει κατάλληλα κάποια bit του κρυπτογραφημένου πακέτου
    - όταν η gateway λάβει το πακέτο και το αποκρυπτογραφήσει να το προωθήσει (αποκρυπτογραφημένο) σε λάθος διεύθυνση – σε αυτή του επιτιθέμενου!!
    - αυτό οφείλεται σε εγγενή αδυναμία της CBC δομής των block ciphers
    - μεταβάλλοντας το i-ιοστό bit ενός μπλοκ κρυπτογράμματος ισοδυναμεί με μεταβολή του i-ιοστού bit μπλοκ του αρχικού μηνύματος

Πραγματοποίηση bit flipping

- Μεταβολή bit στο C_{i-1} οδηγεί σε ελεγχόμενες μεταβολές στο P_i (το P_{i-1} όμως είναι τυχαίο)
- Λόγω του τυχαίου P_i τα μηνύματα λάθους από το IP μεταφέρονται με το ICMP
  - φέρουν επίσης τμήμα των αρχικών δεδομένων
- Τα ICMP πακέτα μπορεί να καταλήξουν στον επιτιθέμενο με κατάλληλη αλλαγή bits (στη θέση της IP) του C_{i-1}



Πηγή του προβλήματος

- Λόγω έλλειψης αυθεντικοποίησης (τα bit-flipping attacks δεν θα λειτουργούσαν) σε Linux υλοποιήσεις
- Το IPsec προτείνει ως προαιρετικούς κάποιους ελέγχους εγκυρότητας των δεδομένων
- Καμία έκδοση του Linux δεν τους κάνει – διαφορετικά δεν θα ήταν εφικτή η επίθεση
- Το RFC 4303 επαναλαμβάνει την προτροπή του RFC 2406
  - ESP allows encryption-only […] because this may offer considerably better performance and still provide adequate security

IPsec applications

IPsec applications

- VPNs (Virtual Private Networks)
  - Interconnected LANs over the insecure Internet
  - Secure router-to-router (i.e. routing security)
- Secure remote access, e.g. to ISPs
  - Individual-to-router
- Domain replication
  - Between domain controllers
- Packet filtering

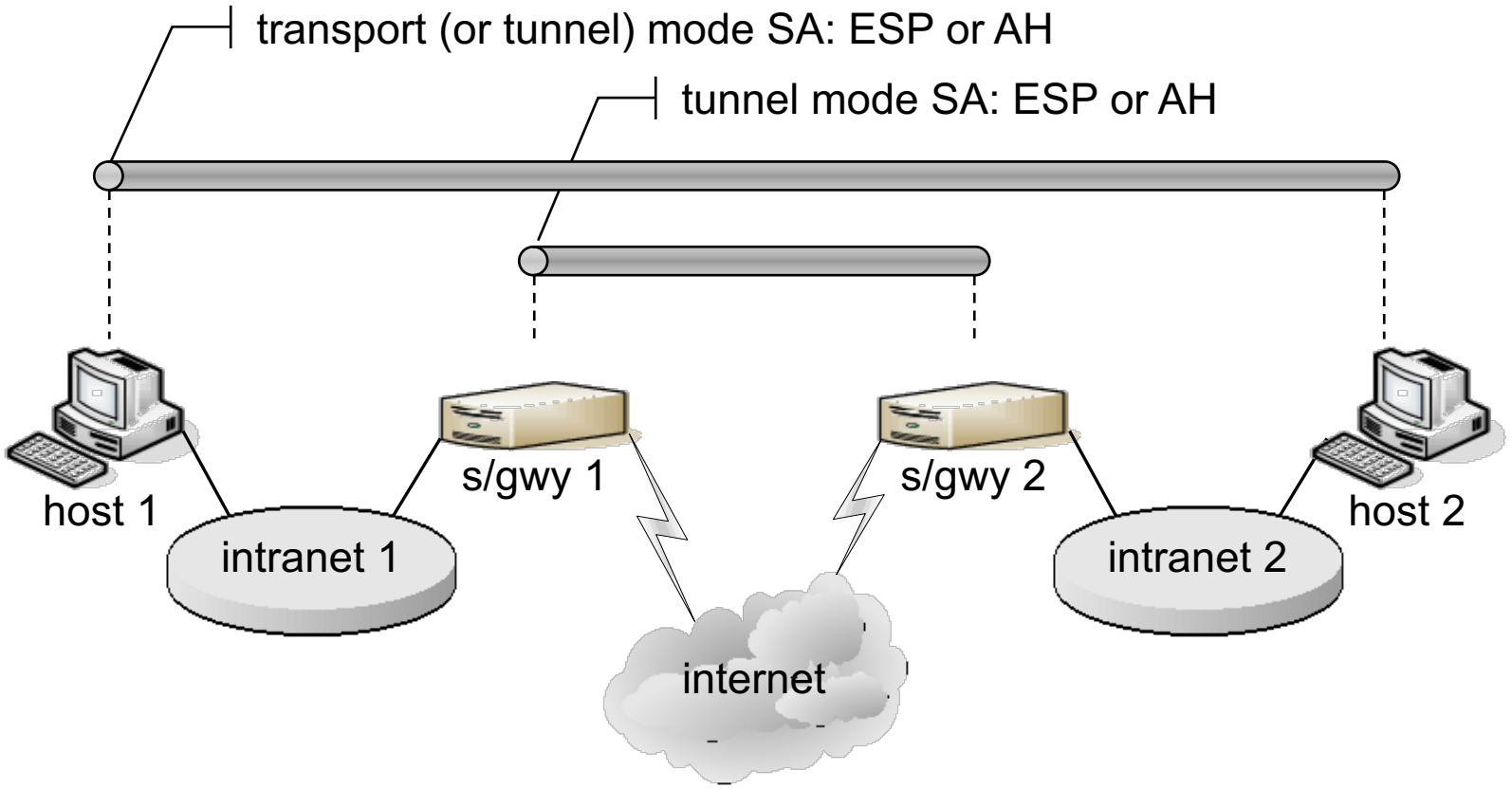
Virtual private networks

- Ορισμός
  - Δίκτυο εικονικών ζεύξεων, για τη μετάδοση ιδιωτικής πληροφορίας
  - Είναι δομημένο πάνω σε κάποιο δημόσιο υπάρχον δίκτυο (κύρια στο Internet)
    - Παύει η ανάγκη ύπαρξης μισθωμένων γραμμών (μείωση κόστους οικονομικού αλλά και διαχείρισης)
- Επιθυμητά χαρακτηριστικά / στόχοι
  - Ασφάλεια
  - Εγγυημένη ποιότητα υπηρεσιών

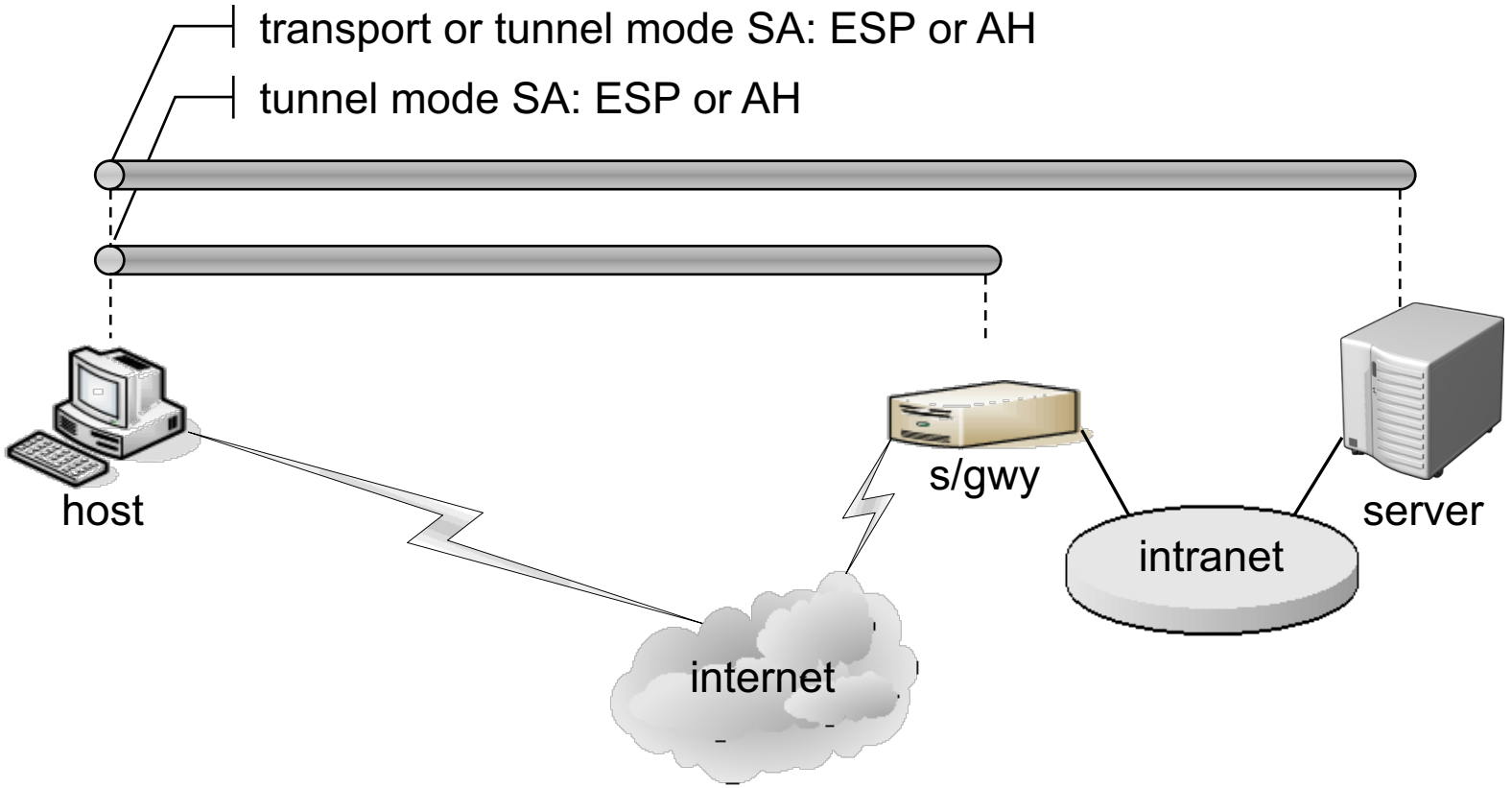
Κατηγορίες VPN βάσει των άκρων

- Το άκρο ενός tunnel μπορεί να είναι είτε ένας απλός χρήστης είτε ένα LAN
  - LAN-to-LAN tunneling (site-to-site). Μία πύλη ασφαλείας (security gateway) είναι το Interface ανάμεσα στο LAN και το tunnel
    - Πρωτόκολλο διαχείρισης IKE (ISAKMP/Oakley)
  - Client-to-LAN tunneling (remote access). Πραγματοποιείται όταν ένας κινητός χρήστης θέλει να συνδεθεί σε ένα LAN.
    - Ο χρήστης εκτελεί κατάλληλο πρόγραμμα στον υπολογιστή του για να συνδεθεί στην πύλη του LAN
    - Πρωτόκολλο διαχείρισης RADIUS (Remote Authentication Dial-In User Service)

IPsec apps: VPNs



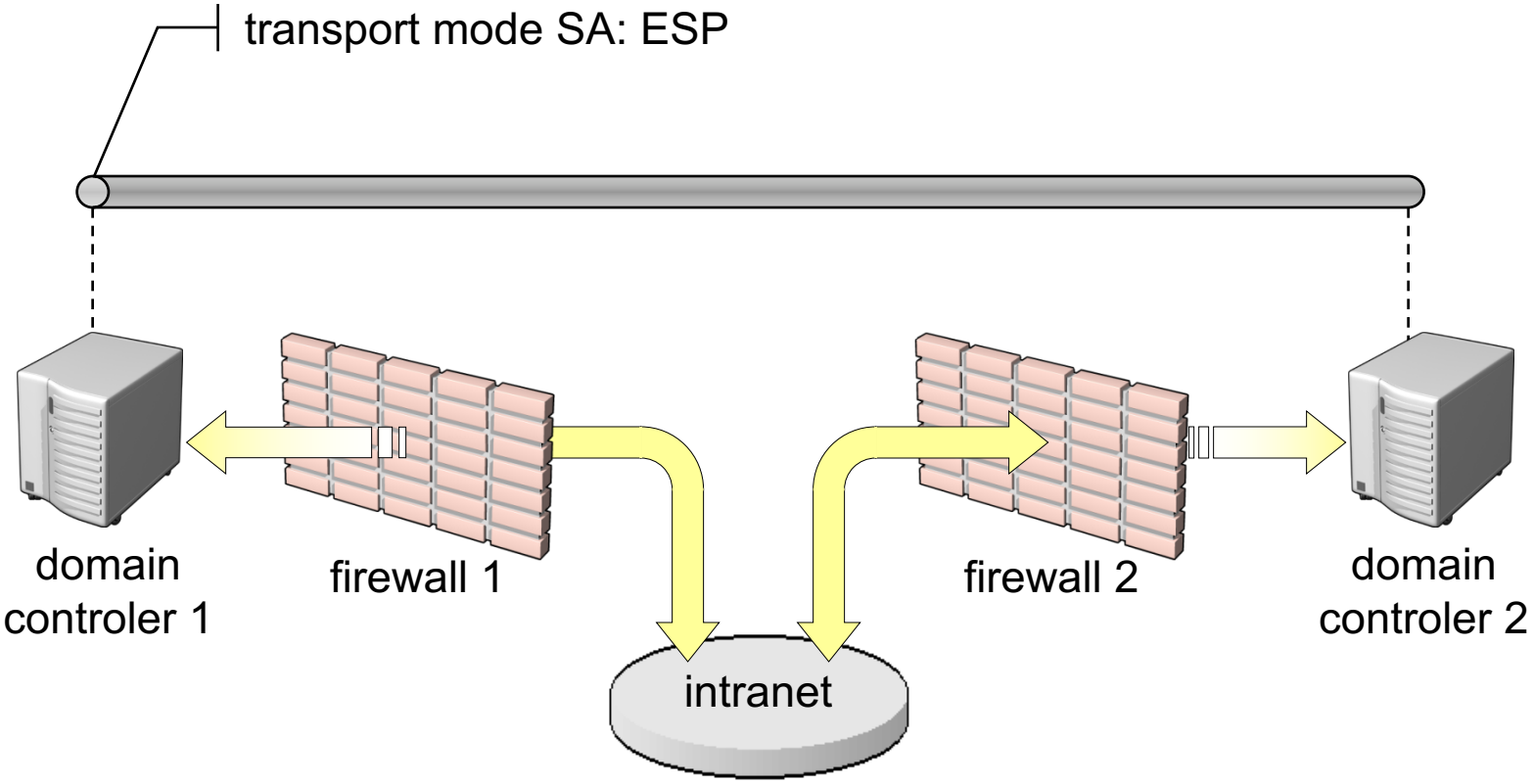
IPsec apps: remote access



Πρωτόκολλο RADIUS

- Υπεύθυνο για πιστοποίηση ταυτότητας και χρέωση
- Διατηρεί μία βάση δεδομένων για κάθε χρήστη, περιέχοντας πληροφορίες όπως
  - passwords (για πιστοποίηση ταυτότητας)
  - δικαιώματα πρόσβασης, και
  - ποσοστό χρήσης δικτύου (για χρέωση)
- Όταν ένας απομακρυσμένος χρήστης θέλει να συνδεθεί στο VPN, το δίκτυο ρωτά το RADIUS σχετικά με το αν ο χρήστης έχει δικαίωμα

IPsec apps: replication



IPsec apps: replication

- Use IPsec for replication through firewalls
  - On each domain controller, create an IPsec policy to secure all traffic to the other domain controller's IP address
- Use ESP 3DES or AES for encryption
- Allow traffic through the firewall
  - UDP Port 500 (IKE)
  - IP protocol 50 (ESP)

IPsec apps: packet filtering

- Filters for allowed and blocked traffic
- Overlapping filters - most specific match determines action

From IP	To IP	Protocol	Src Port	Dest Port	Action
Any	My Internet IP	Any	N/A	N/A	Block
Any	My Internet IP	TCP	Any	80	Permit

- Packet filtering is not sufficient to protect Servers
  - Spoofed IP packets containing queries or malicious content can still reach open ports through firewalls
  - Many hacker tools use source ports 80, 88, …, to connect to any destination port

IPsec apps: traffic not filtered

- Kerberos traffic
  - Kerberos may be used by the Internet Key Exchange (IKE) negotiation service to authenticate other computers in a domain
  - UDP source or destination port 88
- IKE traffic
  - Required to allow IKE to negotiate parameters for IPsec security
  - UDP destination port 500
- IP broadcast addresses
  - Cannot secure to multiple receivers

Προτεινόμενη βιβλιογραφία

- W. Stallings
  Cryptography and Network Security: Principles & Practice
  7th Ed., Prentice Hall, 2017
- W. Stallings and L. Brown
  Computer Security: Principles & Practice
  3rd Ed., Prentice Hall, 2015
- M. Bishop
  Computer Security: Art and Science
  Addison Wesley, 2003