Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

PGP - IP SEC – VPN

Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services *(www.bydesign-project.eu)*

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo Information & Communication Technologies

This presentation has been based on material provided by Dr. K. Limniotis (HDPA)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Pretty Good Privacy (PGP)

- Invented by Phil Zimmerman
- Available for any platform
  - GPG: http://www.gpg4win.org/ (Gnu Privacy Guard)
  - The same design principles with the GPG
- Implements several known cryptographic algorithms (AES, RSA etc.)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

PGP

- PGP (Pretty Good Privacy)
  - The users are able to “sign” the public keys of the other users, once they are sure for their identities
    - Hence, each user is a CA
  - Users trust a public key that is being found on a public PGP key server if it has been signed by another user who is trusted
- The PGP software is a nice option for encrypting files or e-mails
  - Its main version it not currently free
    - Provided by Symantec
  - Instead: GPG (free application), OpenPGP

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

PGP Operation – Authentication

- Sender creates a message
- SHA-2 used to generate the hash code of message
- The hash code is encrypted with RSA using the sender's private key, and result is attached to message
- The receiver uses RSA with sender's public key to decrypt and recover hash code
- Receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

PGP Operation – Confidentiality

- The sender generates message and random 256-bit number to be used as session key for this message only
  - uses random inputs taken from previous uses and from keystroke timing of user
- The message is encrypted, using AES with session key
- The session key is encrypted using RSA with recipient's public key, then attached to message
- The receiver uses RSA with its private key to decrypt and recover session key
- The session key is used to decrypt message

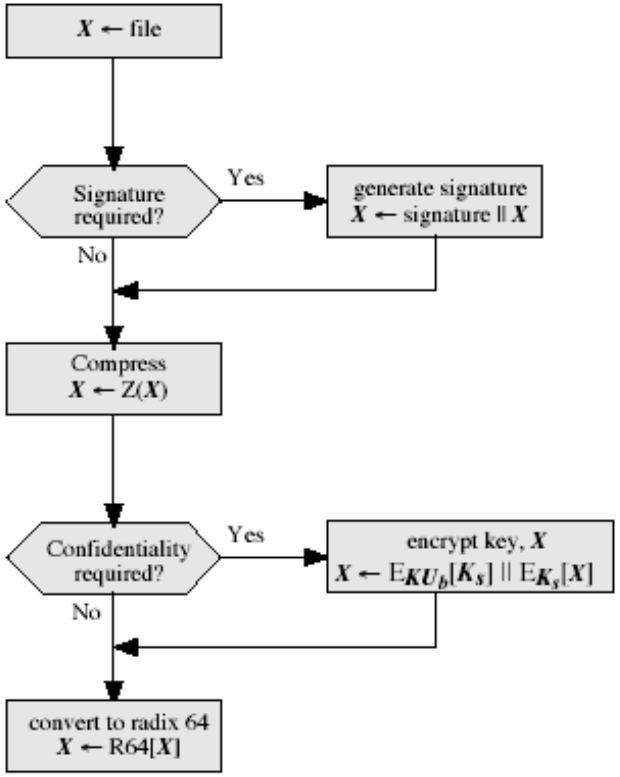
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

PGP Operation – Confidentiality & Authentication

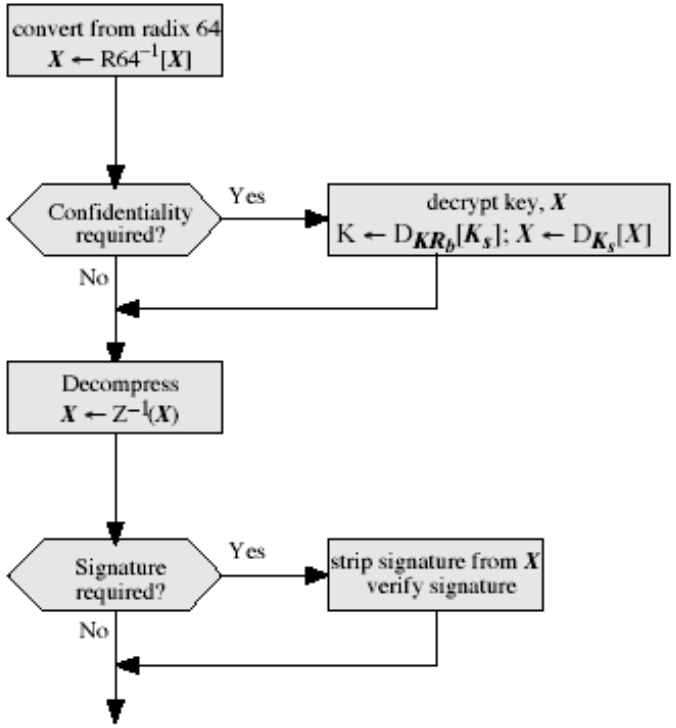
- uses both services on same message
  - create signature & attach to message
  - encrypt both message & signature
  - attach RSA encrypted session key
- By default, PGP compresses message after signing but before encrypting
  - uses ZIP compression algorithm

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A diagram of PGP operation



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

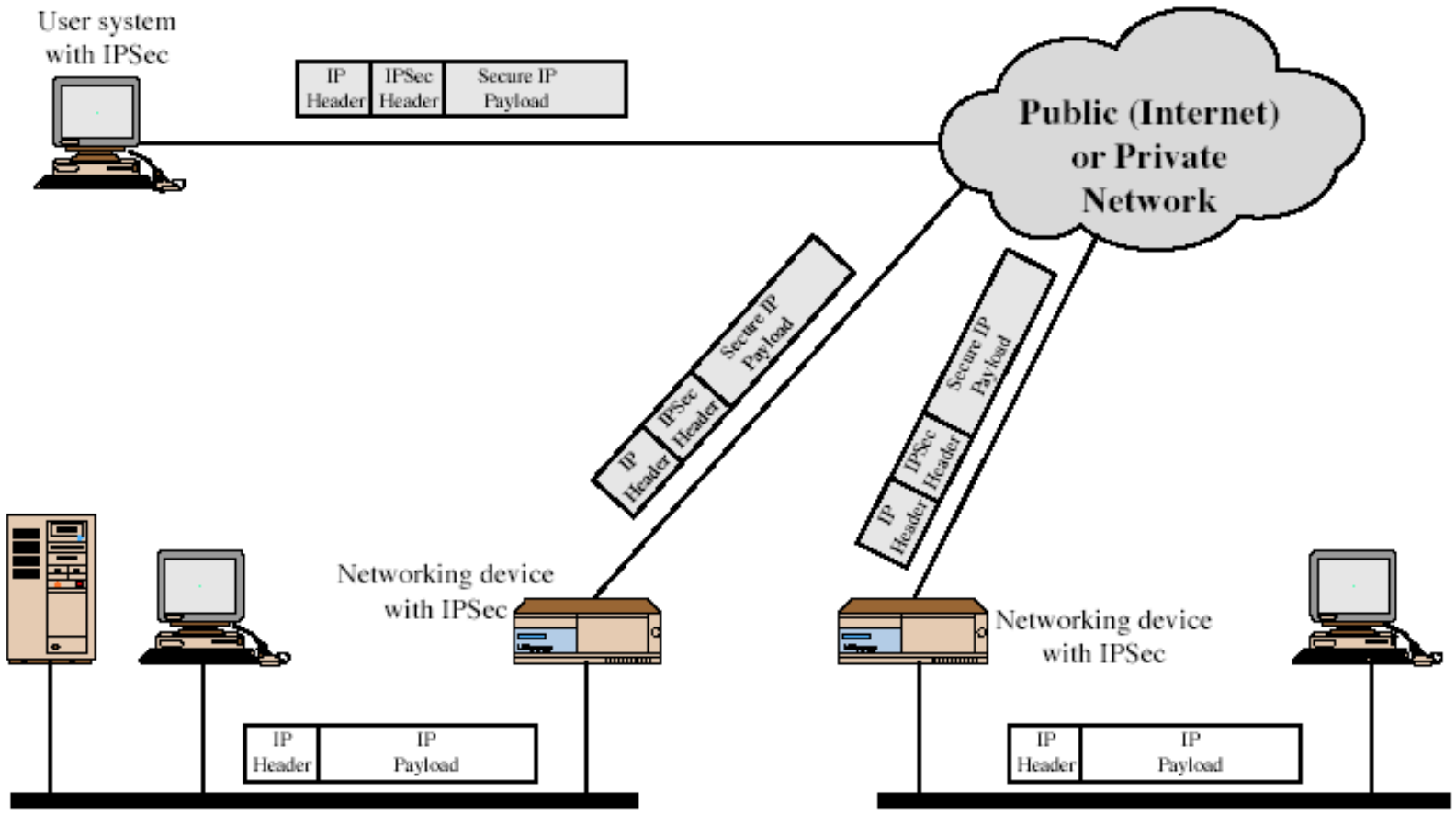
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

IPSec

- Protocol for “forcing” security in the Internet Protocol (IP) level
- Being determined in a set of RFCs (2401/2402/2406/2408)
- Ensures
  - Authentication
  - Confidentiality
  - Key management
- All these are being implemented into the IP packets, so any higher-level applications (mail, file transfer) may rely on this lower-level security
- Applications
  - Setting up a secure Virtual Private Network (VPN) over the Internet or over a public WAN
    - Less cost for the organization than using leased lines for a private network
  - Remote users (employees / external workers) may securely connect to the organization’s network

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An IPSec case



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

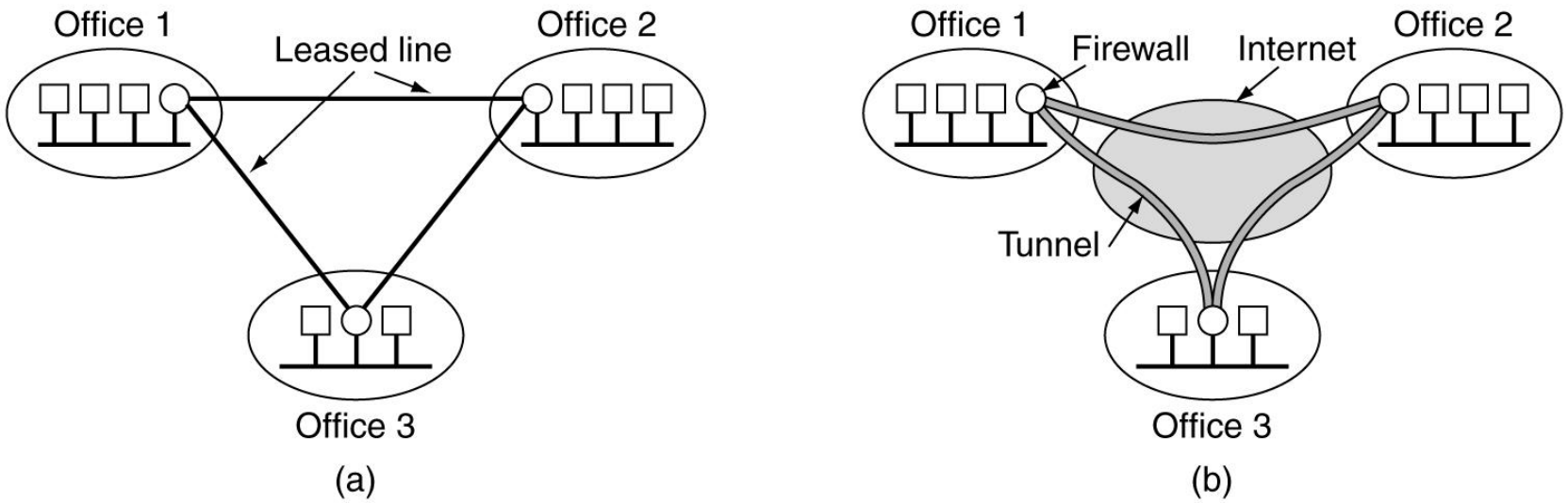
Virtual Private Networks – VPNs

- A safe and encrypted connection over a less secure **network**, such as the public internet.
- A **VPN** works by using the shared public infrastructure while maintaining security features (confidentiality, integrity, authentication) through security procedures and tunneling protocols

- Desired goals
  - Security
  - No degradation in QoS

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

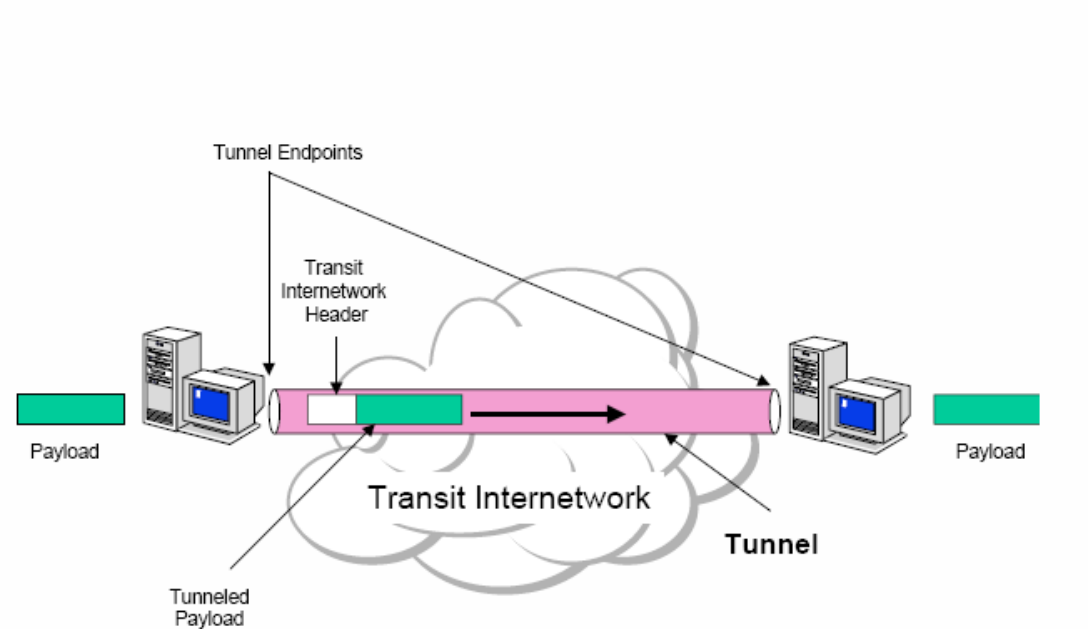
Virtual Private Networks



(a) A leased-line private network. (b) A virtual private network

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

What is a tunnel



- The virtual connections are being implemented by creating “special” IP packets. By these means, a so-called tunnel is being built (the network in which these special secure packets are being sent)

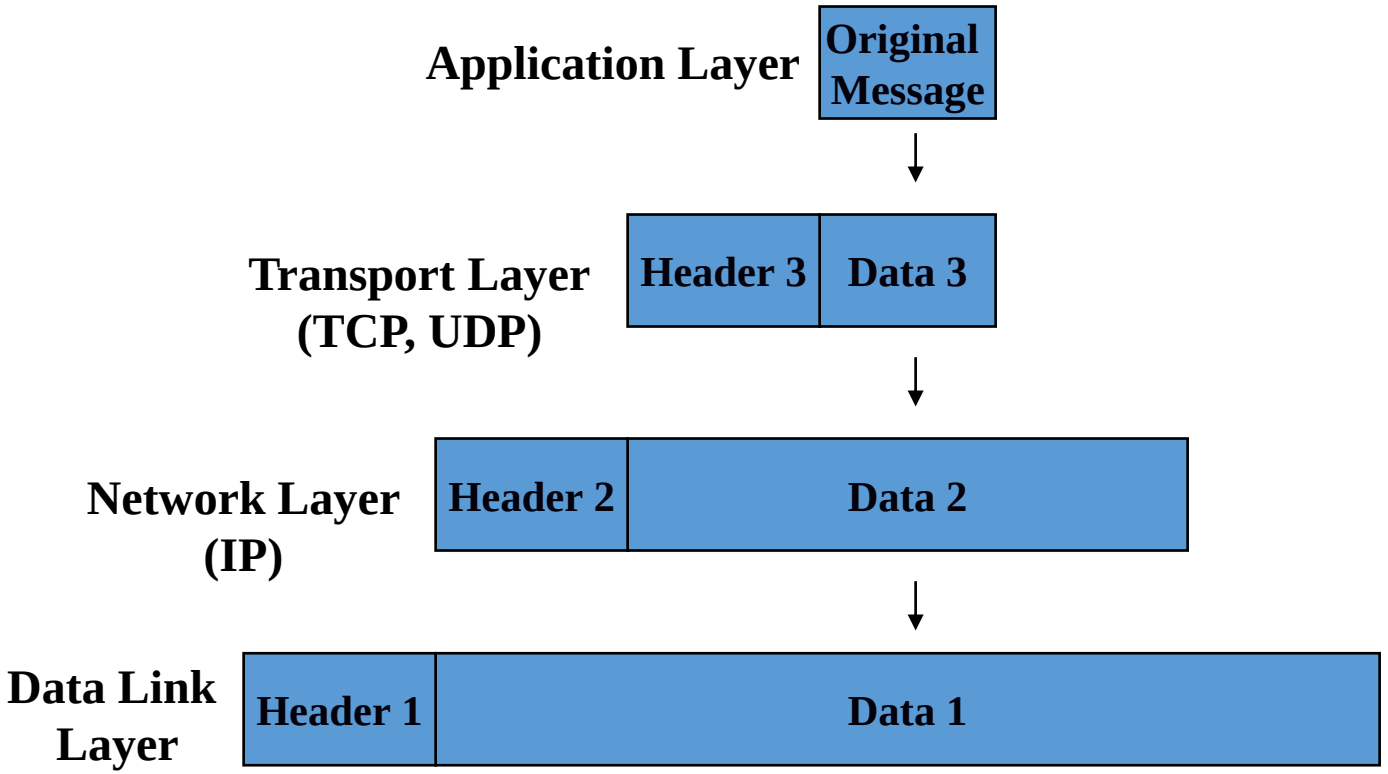
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Benefits of IPSec

- IPSec provides strong security that can be applied to all traffic crossing the network perimeter
- IPSec is below the transport layer (TCP/UDP) and, thus, is transparent to applications
  - There is no need to change software on a user's system when IPSec is implemented in a router
- IPSec can be transparent to end users
  - There is no need to train users on security mechanisms or revoke material when users leave the organisation
- IPSec can provide security for individual users if needed
  - Useful for offsite workers

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Encapsulation in TCP/IP



- IPSec defines a new set of headers, which are being attached to the original IP packets, thus producing "new" IP packets in such a way that security requirements are met

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Basic IPSec functionalities

- Two protocols (each of them has its own headers):
  - **The Authentication Header (AH) Protocol,**
  - **The Encapsulating Security Payload (ESP)**
- The AH protocol provides source authentication and data integrity, but not confidentiality.
- The ESP protocol was designed after the AH protocol was already in use. ESP does whatever AH does with an additional functionality: confidentiality.
- IPSec supports both IPv4 and IPv6
- Known cryptographic primitives are also used:
  - Diffie-Hellman key exchange algorithm
  - AES or other block ciphers for encryption
  - Hash functions for message integrity
  - Digital certificates for validating the public keys

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

IPSec modes of operation

- Transport Mode:

Initial IP packet

IP Header	TCP Header	Data

Transport Mode protected packet

IP Header	IPSec Header	TCP Header	Data

protected

- Tunnel Mode (especially in VPN set-ups):

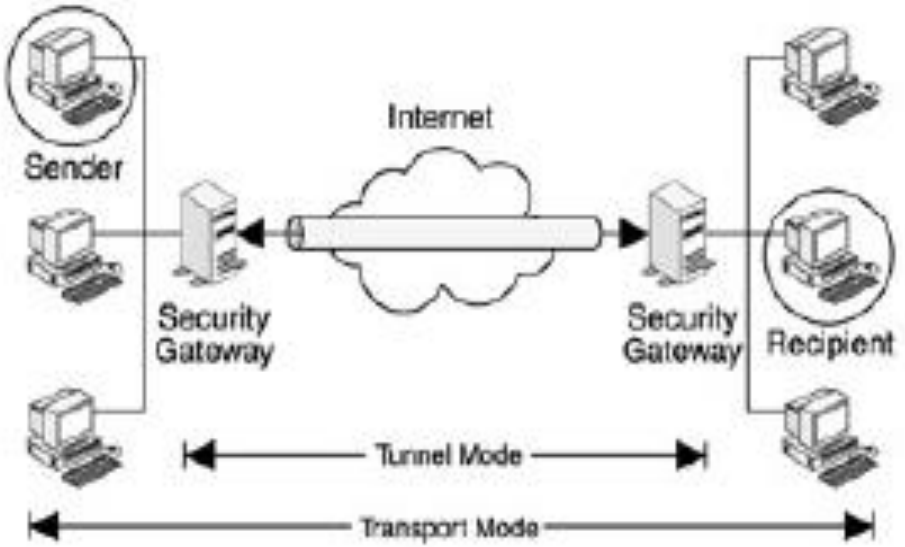
Tunnel Mode protected packet

New IP Header	IPSec Header	Original IP Header	TCP Header	Data

protected

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Basic IPSec functionalities

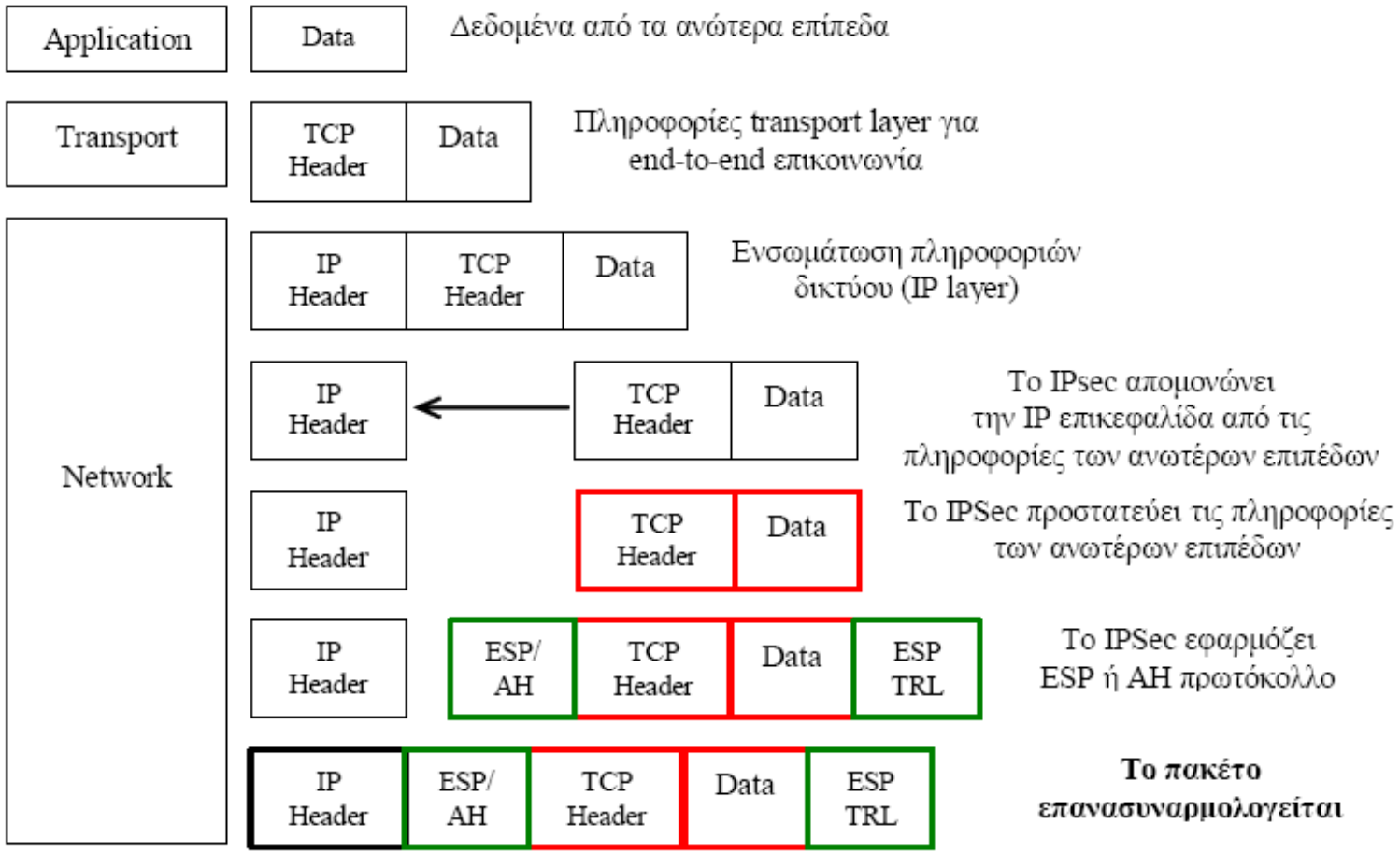


- Tunnel mode:
  - Between gateways (routers/firewalls)
- Transport mode:
  - For end-to-end security (e.g. Client-server applications).

In both modes, either AH or ESP can be used (thus resulting in 4 possible combinations)

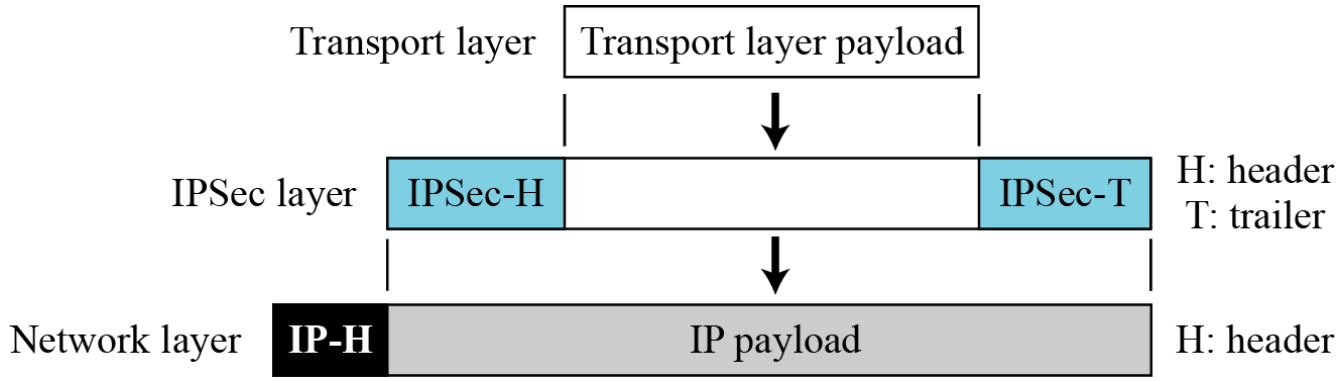
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

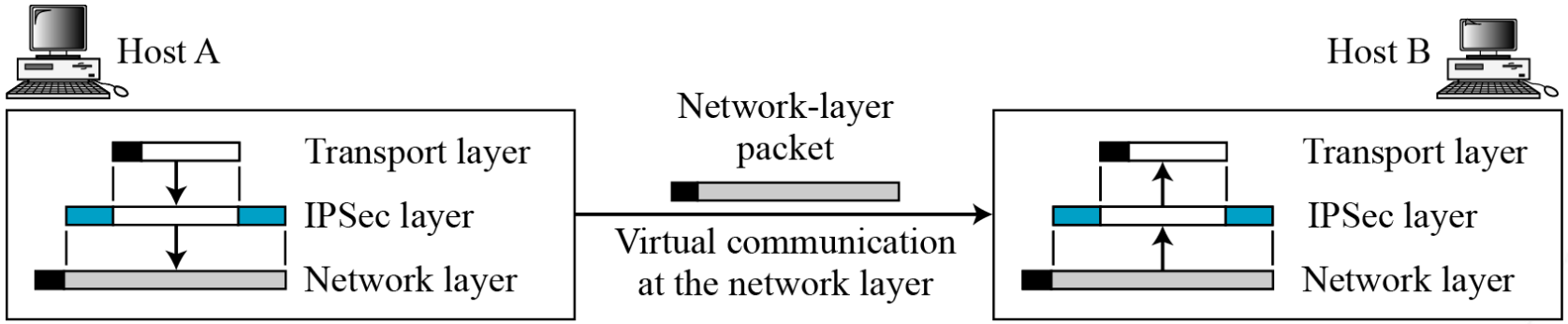
IPSec in transport mode



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

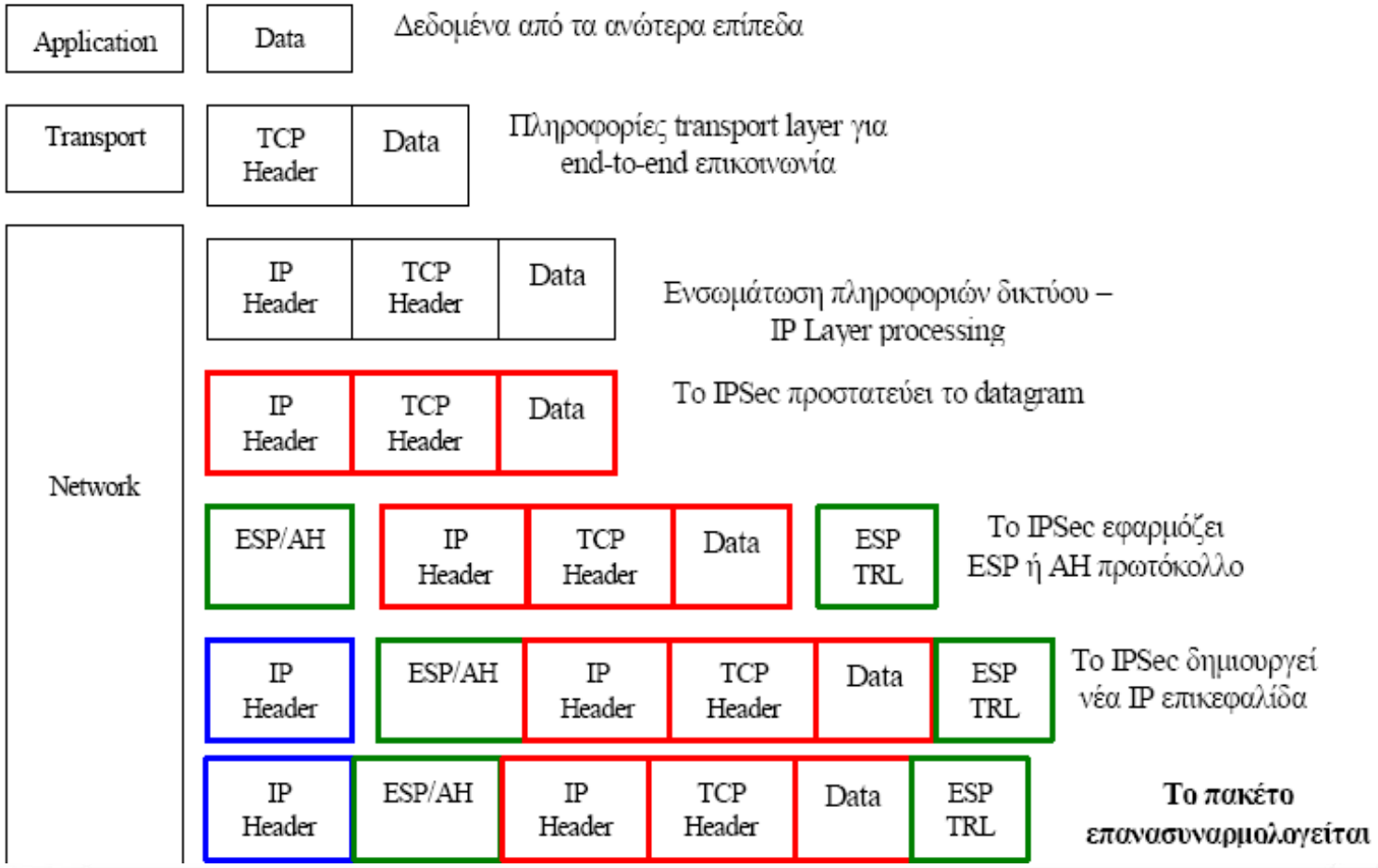
Transport mode





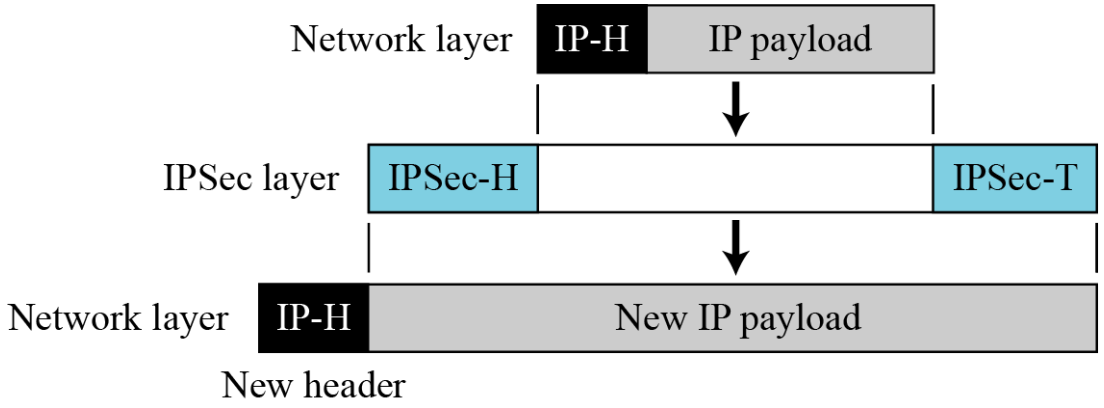
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

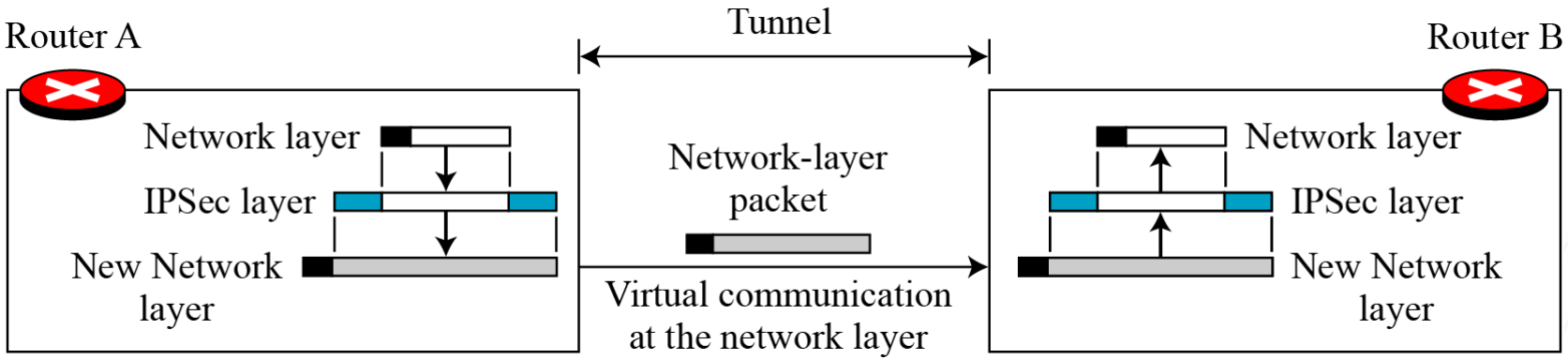
IPSec in tunnel mode



Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

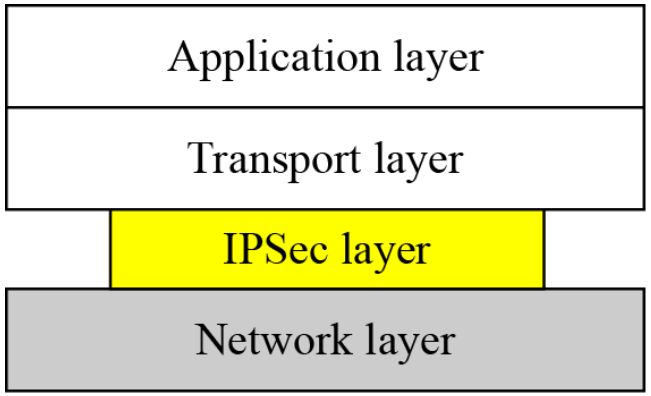
Tunnel mode



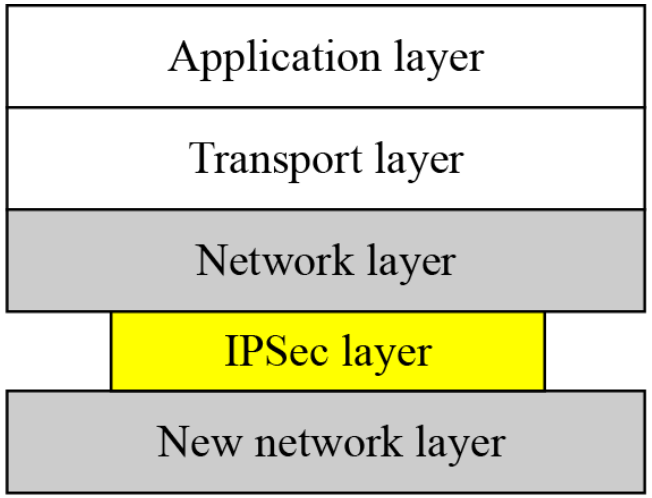


Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Transport mode vs. tunnel mode



Transport Mode



Tunnel Mode

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A comparison

- Tunnel mode: Gateways (routers) act as IPSec proxies, namely the user's operating system does not need any special software. Moreover, it provides security against traffic analysis, since the initial IP addresses are encrypted. However, it requires more computational cost than the transport mode.

- Transport mode: Less computation cost, since only a few more bytes are being added. Moreover, since the gateways "see" the initial source/destination IP addresses, routings based on desired QoS can be performed. A drawback is that traffic analysis is now achievable.