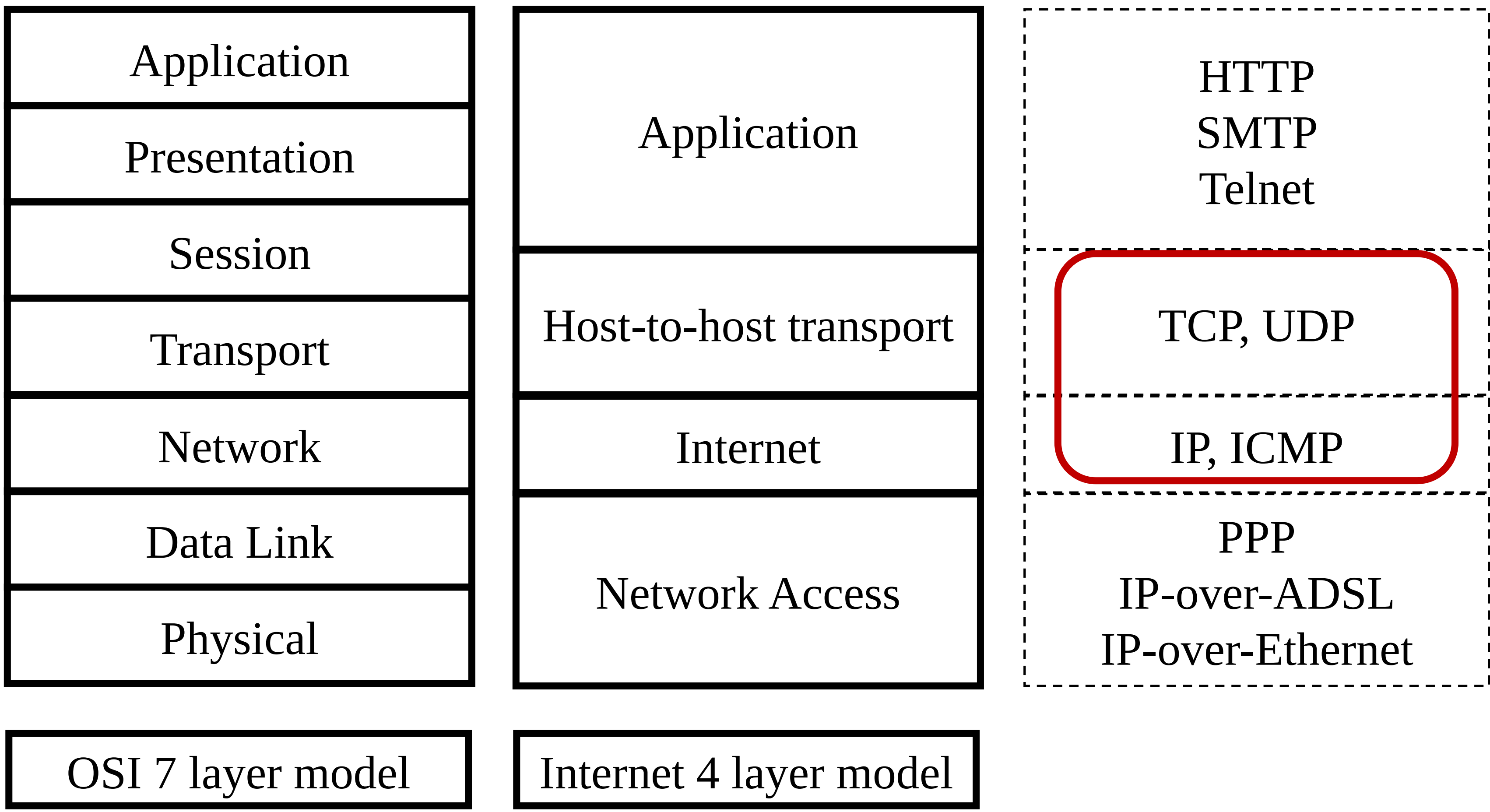
Security Protocols and Private Network

Dr Sana Belguith

TCP/IP (Internet) versus OSI



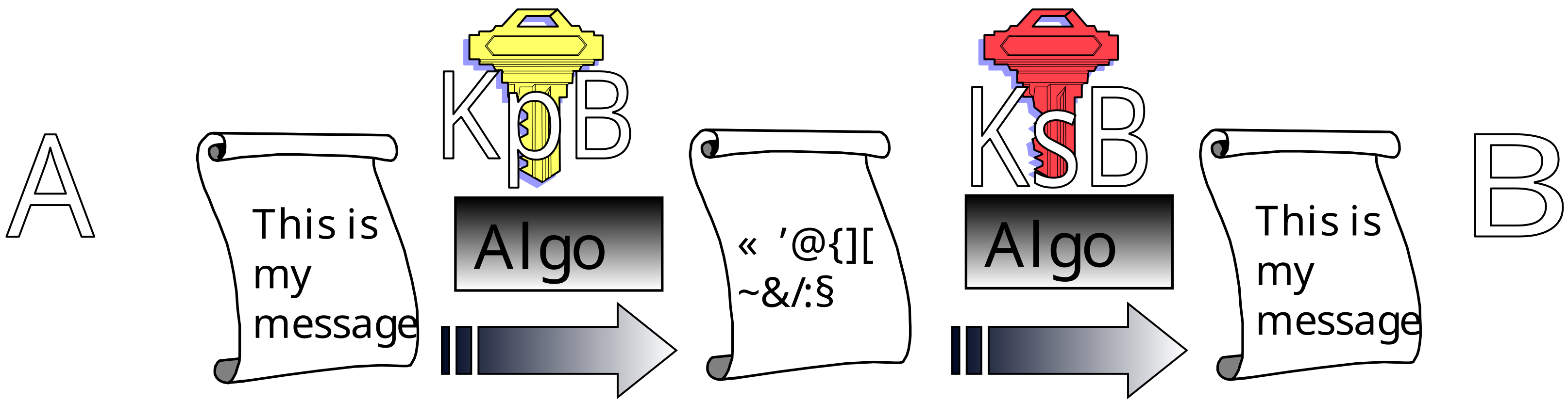
Cryptographic Systems

Using cryptography in security protocols:

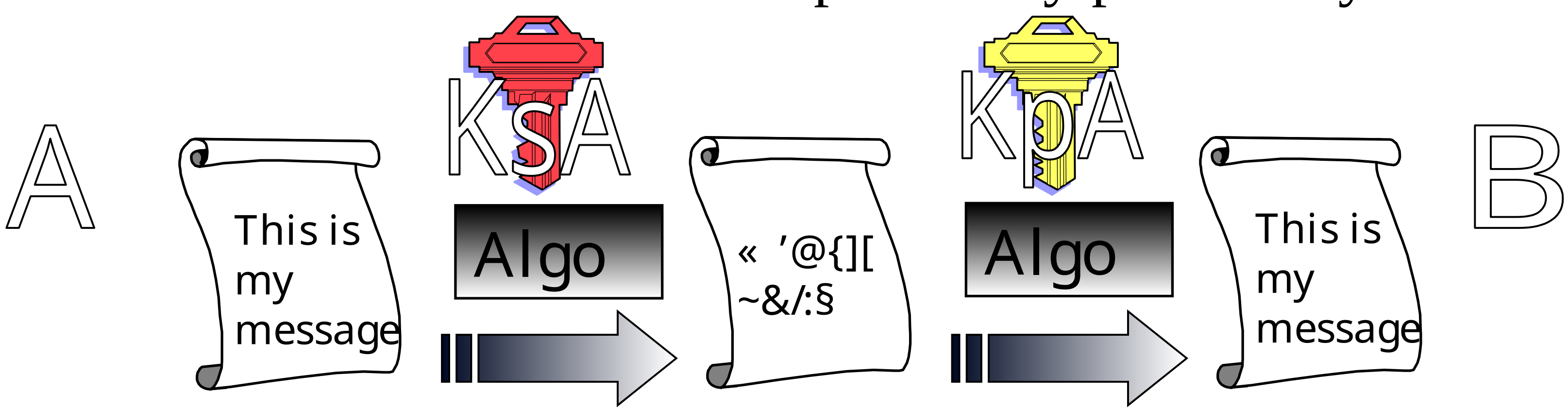
- Symmetric cryptography:
  - Intensive protection of data (due to fast processing) for encryption and MAC computation
- Asymmetric cryptography
  - Initializing a secure communication between two entities
    - to authenticate partners entities,
    - to agree on a secret key in a confidential way

Cryptographic Systems

Message ’s confidentiality: receiver’s public key/private key



Sender ’s authentication: sender ’s public key/private key



Cryptographic Systems

Use of symmetric cryptography:

- Data confidentiality
- Integrity/authentication of data with introduction of a MAC (Message Authentication Code)

Use of asymmetric cryptography:

- During connection establishment: mutual authentication, exchange of symmetric encryption keys

Secure Socket Layer

SSL *(Secure Socket Layer)* protocol:

- Developed by Netscape Communications
- Idea: introduces one security layer between the transport and application layers to protect data exchanges
- Ensures the protection of TCP-based applications (http, telnet, ftp…)
- Secure applications are renamed: https, telnets, ftps
- Applications are identified with port numbers

Applications	**Port number**
https	**443**
telnets	**992**
ftps	**990**
ftps-data	**989**

Secure Socket Layer

SSL version 3.0

- Last SSL version released in 1996
- Integrated in Netscape Navigator and Microsoft Internet Explorer
- Broadly used over Internet to protect exchanges to online web services (bank, electronic commerce…)
- SSLv3 deprecated by Internet Engineering Task Force (IETF) standard organisation in June 2015 (RFC 7568) as non sufficiently secure

Transport Layer Security

TLS *(Transport Layer Security)* protocol:

- Developed by the Internet Engineering Task Force (IETF) standard organisation

- TLS 1.0 is similar to SSL 3.0 with the following modifications:
  - the HMAC construction considered is adopted (**HMAC**: MAC using symmetric cryptography)
  - the key exchange mechanism is not proprietary and is based on Data Security Standard

- TLS sub-protocols are similar to the SSL ones: *TLS handshake protocol*, *TLS cipher spec protocol*, *TLS alert protocol*

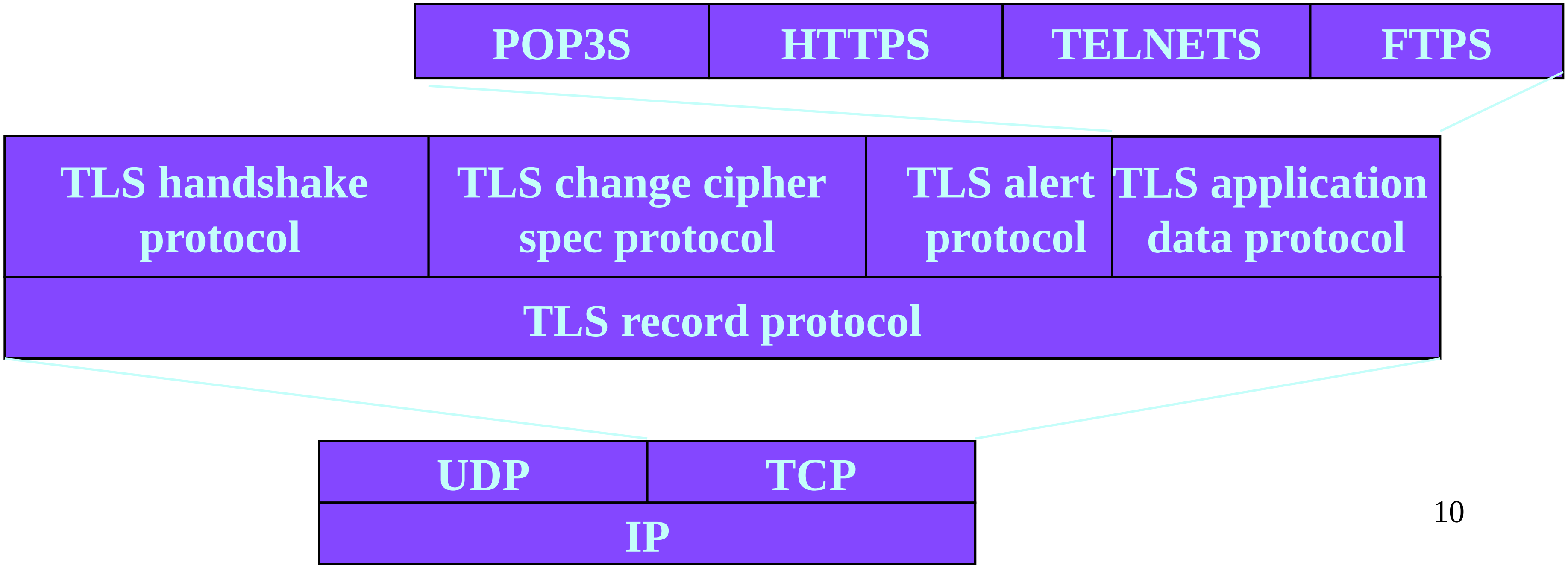
Transport Layer Security

- Initialization phase:
  - The server must authenticate to the client thanks to its public key certificate
  - The client optionally can authenticate itself to the server (public key certificate)
  - Negotiation of security services and mechanisms
  - Establishment of a secret key (master key)
  - Messages of the initialization phase are protected in integrity and authenticity
  - Phase implemented by a software sub-module of TLS *(TLS Handshake Protocol)*
- Data protection phase (for TLS 1.0 – TLS1.2):
  - Data confidentiality
  - Data integrity/authentication
  - Usage of symmetric cryptography to protect this phase
  - Phase implemented by a sub-module of TLS *(TLS Record Protocol)*

Transport Layer Security

TLS organized into 2 parts:

- *TLS record protocol*: user data protection
- TLS sub-protocols: establishment and management of TLS sessions (security parameters negotiation, errors processing…)



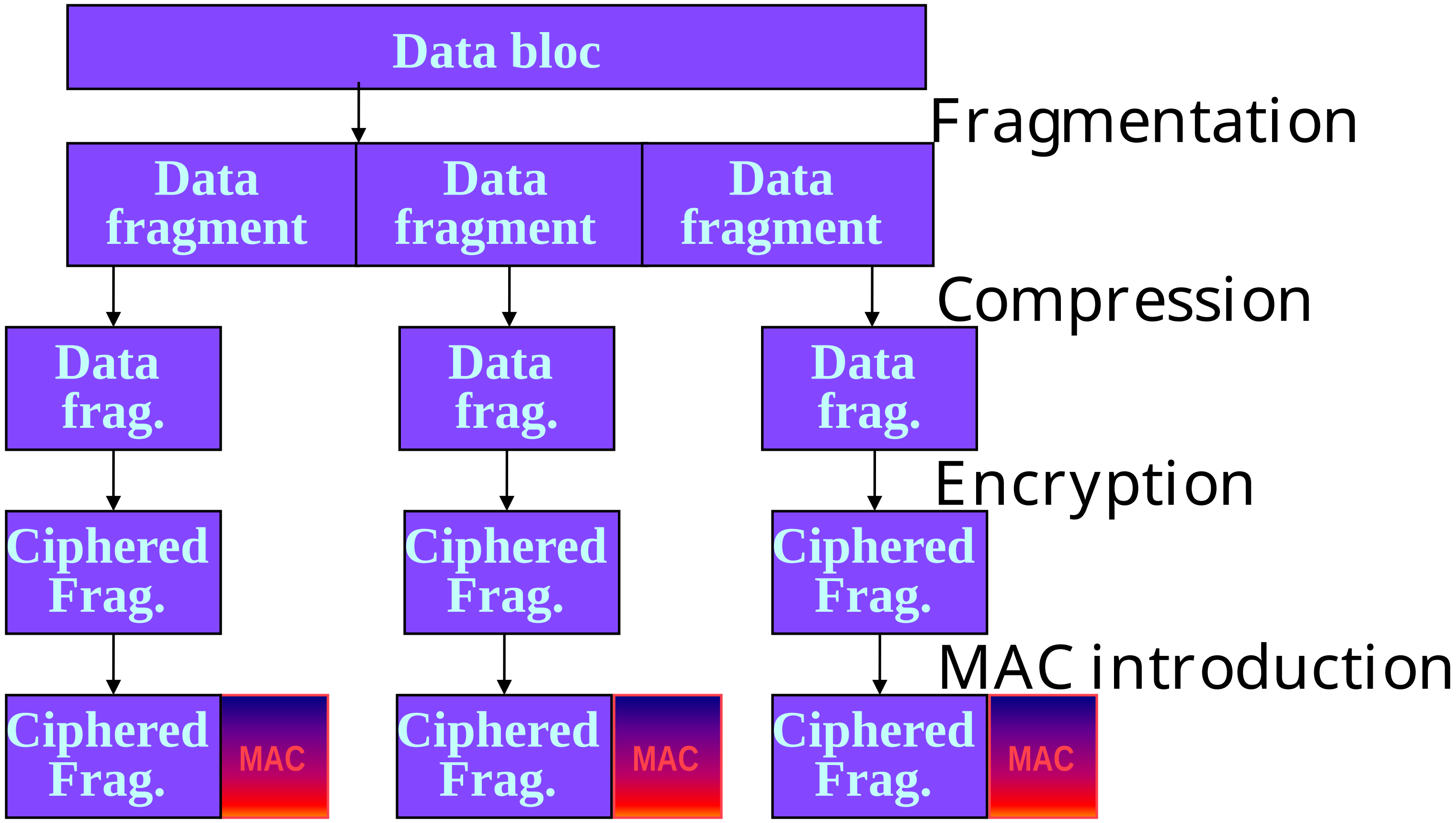
Transport Layer Security

TLS sub-protocols:

- *TLS alert protocol*: alarms transmission through the *TLS record protocol*
- *TLS change cipher-spec protocol*: moves to the new security context by the sender
- *TLS application data protocol*: directs data communication to the *TLS record protocol* layer
- *TLS handshake protocol*: authentication and security parameters establishment

Transport Layer Security

TLS record protocol :



Many mechanisms that need negotiation during the TLS initialization

Transport Layer Security

TLS handshake protocol enables the server and client to:

- agree on the TLS version
- agree on security parameters (compression method, encryption algorithms) for the confidentiality, authentication, integrity services
- authenticate each other (optional authentication of clients)
- exchange of master keys (used to derive session keys)
- replay detection (thanks to the *Random*)
- detection of message integrity problems

Transport Layer Security

TLS exchanges:

Client Server

(1) Handshake : ClientHello

(2) Handshake : ServerHello

(2) Handshake : Certificate

(2) Handshake : ServerHelloDone

(3) Handshake : ClientKeyExchange

ChangeCipherSpec

(5) Handshake: Finished

ChangeCipherSpec

(6) Handshake : Finished

application_data

application_data

Alert: warning, close_notify

Transport Layer Security

TLS1.2 algorithms/methods:

Key exchange methods	Ciphering algorithms	Hash functions
RSA	RC4_128	MD5
DH-DSS	3DES_EDE	SHA-1
DH_RSA	AES_128_CBC	SHA-256
DHE_DSS	AES_256_CBC	
DHE_RSA		
DH_anon		

A number of Cipher Suites are defined under the format:
TLS_RSA_WITH_AES_256_CBC_SHA256 (mandatory cipher suite)

IP security

Security protocol IPsec *(IP security)*:

- Defined by the IETF *(Internet Engineering Task Force)*
  - 1st standards in 1995
  - 2nd standards in 1998, improved in 2005 and largely implemented
- Very much used to protect IP traffic between two remote networks

IP security

- Initialization phase:
  - Both IPsec entities must authenticate each other (e.g. public key certificate, but also shared secret)
  - Negotiation of security services and mechanisms
  - Establishment of a secret key
  - Initialization phase messages protected in integrity and authenticity
  - Phase implemented by the application level module IKE *(Internet Key Exchange)*

- Data protection phase:
  - Data confidentiality
  - Data integrity/authentication
  - Usage of symmetric cryptography to protect this phase
  - Phase implemented by an IPsec sub-protocol: AH *(Authentication Header)* or ESP *(Encapsulating Security Payload)*
  - Possibility to create a protected tunnel or to secure an IP packet flow

IP security

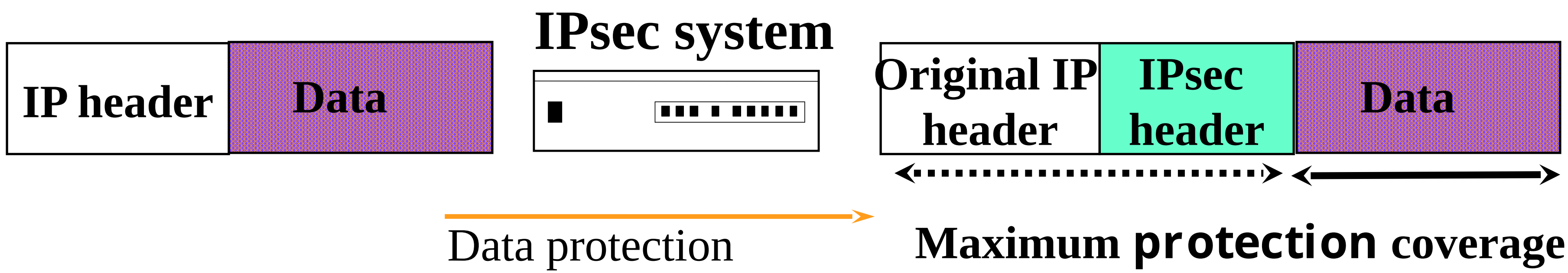
Security services supported by IPsec thanks to two sub-protocols:

- AH *(Authentication Header)* :
  - » integrity and authentication of data origin and optionally replay detection (optional)
  - » protection over the packet content and part of the header
  - » protocol number: 51
- ESP *(Encapsulating Security Payload)* :
  - » data confidentiality (optional)
  - » integrity, authentication of data origin and optionally replay detection (optional)
  - » protection over the packet content only

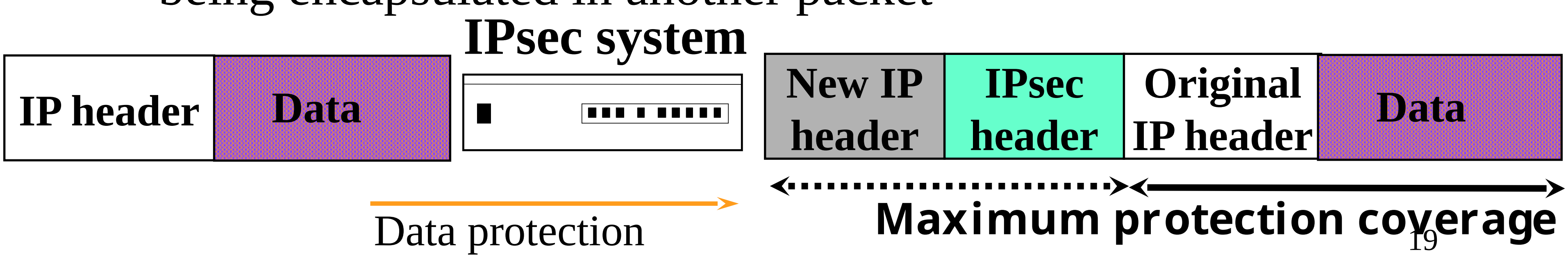
IP security

Two IPsec protection modes:

- Transport mode: only the content of the packet and some fields in the header are protected. Usable only between ends of connection



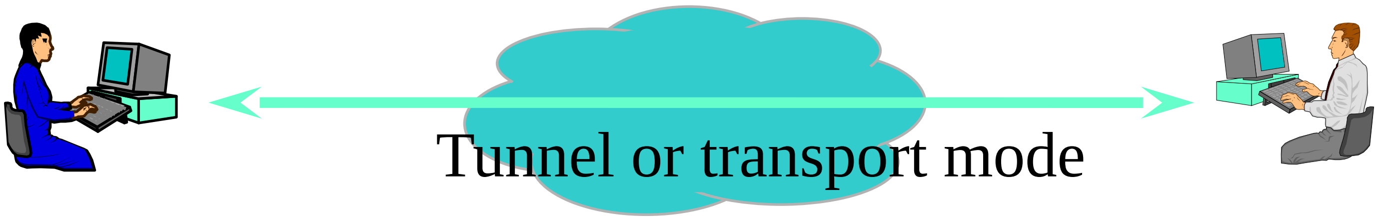
- Tunnel mode: all the fields of the packet are protected prior to being encapsulated in another packet



IP security

Combining modes/types of protection (rfc 4301)

- End-to-end protection



- Protection over network segments

IP security

- Access from a nomad

L2TP Tunnel protected by IPsec in transport mode

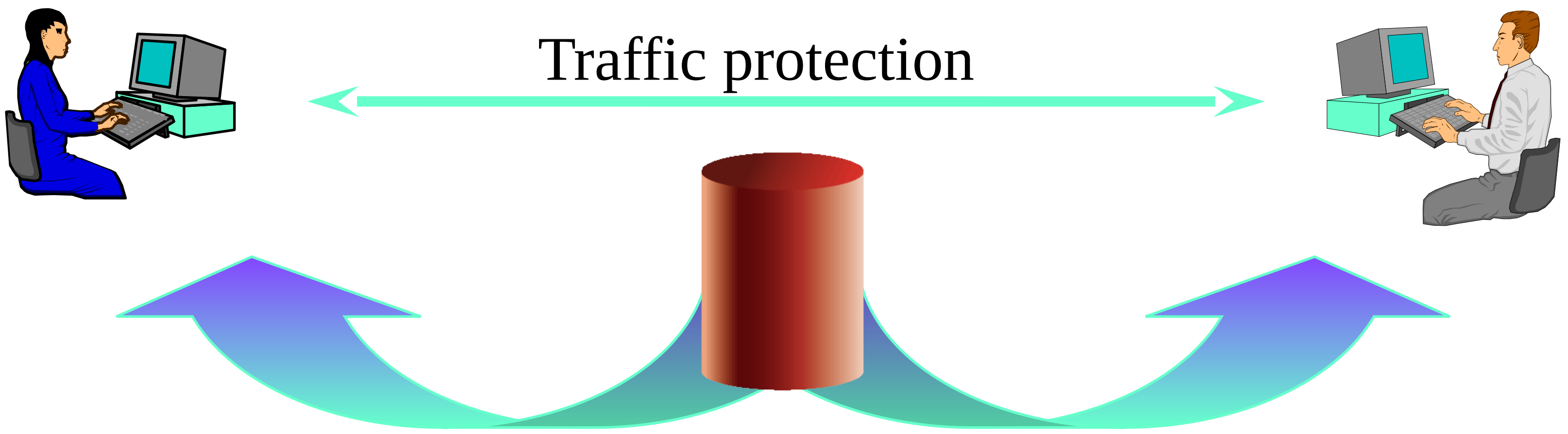
IP security

Default Ciphersuites for IPsec (rfc 4308)

Key exchange Methods (IKE, IKEv2)	IPsec
3DES-CBC (encryption) HMAC-SHA1 (PRF) HMAC-SHA1-96 (integrity check) 1024-bit MODP (DH Group)	ESP 3DES-CBC (encryption) HMAC-SHA1-96 (integrity)
AES-128-CBC (encryption) AES-XCBC-PRF-128 (PRF) AES-XCBC-MAC96 (integrity) 2048-bit MODP (DH Group)	ESP AES-128-CBC (encryption) AES-XCBC-MAC96 (integrity)

PRF = pseudo-random function
MODP = Modular Exponential

Security associations (SA)



- Definition: contract between two entities at least and that includes a set of security parameters enabling entities to establish security services for traffic protection

Security associations (SA)

A security association contains:

- Security protocol AH or ESP to be established along the security services (confidentiality, integrity, authentication, protection against replay), algorithms and encryption keys, initialization vector, hash function
- IPsec protocol mode (tunnel, transport)
- SA lifetime

Identification of SA using triplet:

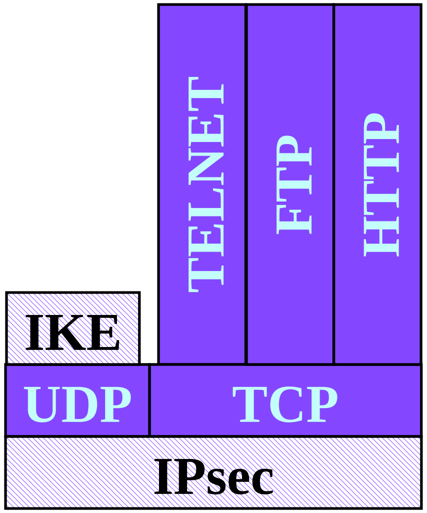
- index SPI *(Security Parameters Index)*
- address of IPsec equipment « partner »
- security protocol AH or ESP

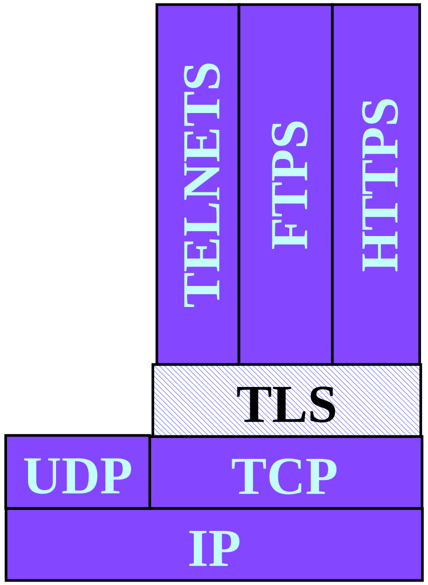
Security associations (SA)

Key and security association management done by IKE *(Internet Key Exchange)* protocol

- Services offered at connection setup:
  - » Mutual authentication between IPsec modules
  - » Negotiation of the IPsec security associations (enciphering algorithms, key length)
  - » Generation of a symmetric encryption key

Security solutions recapitulation:





IPsec

TLS

Real-world Applications of Security Protocols

Have you ever heard of VPN or used it ?

Virtual Private Network

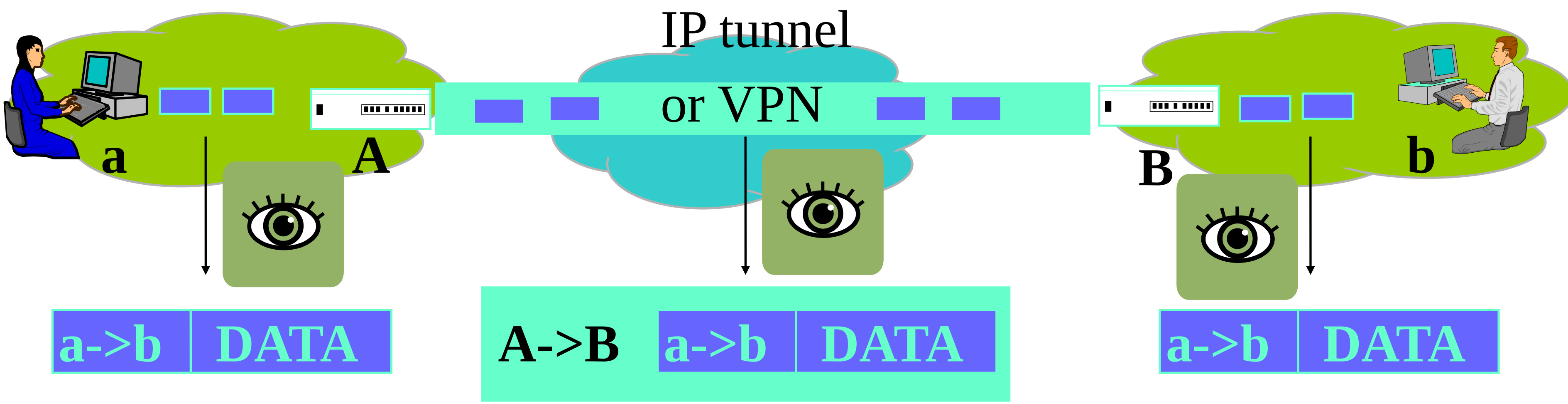
What is a VPN?

- VPN for *Virtual Private Network*
- **Primary goal:** facilitate communications between companies and their partners, internal communications of a geographically distributed company, or remote communications between a mobile and its company
- **Techniques:** establishing an IP tunnel to exchange data through the tunnel
- **Security** is optional to protect the tunnel

Virtual Private Network

What is an IP tunnel?

- Encapsulating an IP packet into another IP packet



- Objective: two remote equipments are enabled to behave as if they were locally connected

Virtual Private Network

- The two remote local networks are virtually forming the same local network thanks to the tunnel
- The packet is going out a private network and is getting into another private network through the tunnel:
  - Lighter filtering done by private networks
  - Possibility to use private addresses a and b (at the condition that addresses spaces are compatible)

Virtual Private Network

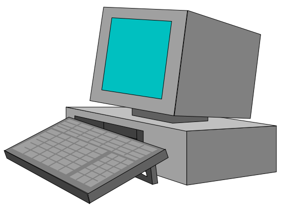
Securing the tunnel is of high importance:

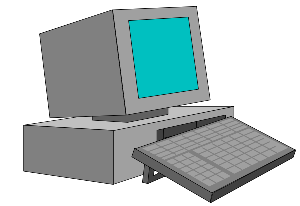
- Too much talkative machines behaving as if being locally connected
- Data exchanged through the tunnel might be confidential
- Strong need to introduce some security services:
  - Data confidentiality
  - Data integrity
  - Data origin authentication
- Services implemented by the security protocols:
  - IPsec (IP Security)
  - TLS (Transport Layer Security)

Security protocols and VPN

- Objectives of security protocol: to protect any communication over a network
- Two successive phases:
  - Initialization phase: authentication of entities, negotiation of security services, exchange of encryption keys
  - Data protection phase: activation of security services over data flows

Security protocols and VPN





<u>1st initialization phase:</u>

- Mutual authentication of entities (ex: based on the peer entity's certificate),
- Agreement on one or several secret keys,
- Negotiation of security associations (security services and mechanisms) for data protection

Control

<u>2nd data protection phase</u> with the possibility to offer the following security services (secret keys) :

- **Data confidentiality (encryption mechanism),**
- **Data integrity,**
- **Authentication of data origin**

Data

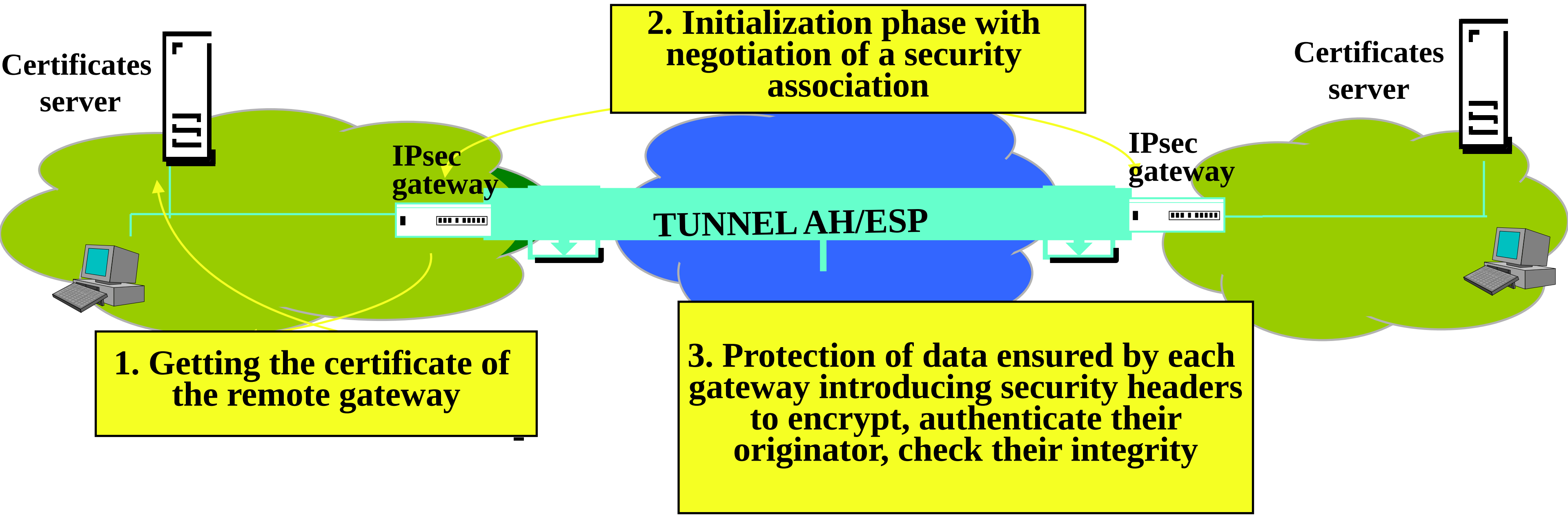
IPsec and TLS VPN

- 2 main usages:
  - Interconnecting LANs - 2 solutions:
    - VPN only supported by gateways *(Customer Equipment based)* of remote sites
    - Possible protocol: IPsec
  - Remote access to a network from a nomad
    - Possible protocols: IPsec or TLS

IPsec VPN

Interconnecting remote sites

Establishment of an IPsec tunnel (VPN)



IPsec VPN

Authentication within (IPsec) VPN

- Gateways authenticate to each other:
  - Based on a pre-shared key (password)
  - Based on a public key certificate

- Users authenticate:
  - Based on a password

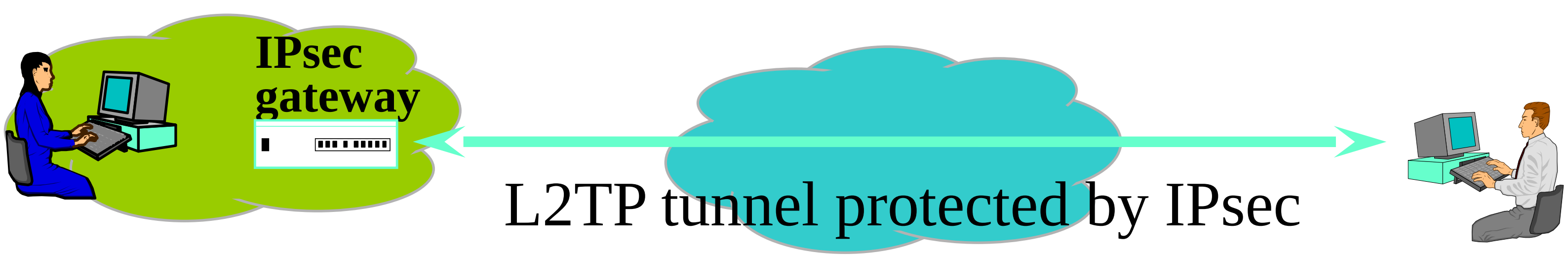
IPsec VPN

Layer Two Tunneling Protocol

L2TP/IPsec

Remote access scenario

- Establishing an IPsec session between the nomad and the IPsec gateway (every next packets are protected by IPsec)
- Establishing an L2TP tunnel between a nomad and a gateway



IPsec VPN

Using a tunnel: L2TP (August 1999)

- *Layer Two Tunneling Protocol*
- Known as the standard protocol of tunneling for switched access
- Concurrent proprietary protocol:
  - PPTP *(Point-to-Point Tunneling Protocol)* from Microsoft with data encryption

IPsec VPN

L2TP

- Role:
  - » Tunnel between a nomad and private network
  - » No services to ensure data protection
- Entities:
  - » L2TP client (within the device)
  - » LNS server: *L2TP Network Server* responsible for L2TP tunnels management, and located within the company’s IPsec gateway

IPsec VPN

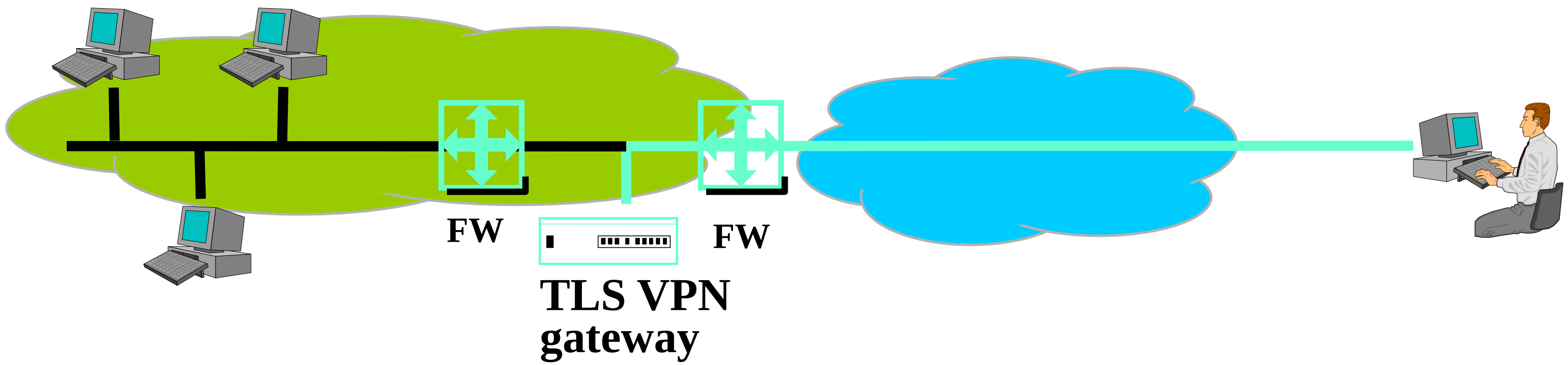
Solution L2TP/IPsec

- First establishing an IPsec session enabling:
  - » Protection of IP packets being exchanged between the device and the gateway
  - » Authentication of the nomad’s equipment
- Then, establishing an L2TP tunnel:
  - » Getting a private address for the device when establishing the L2TP tunnel
  - » Authentication of the nomadic user
- Finally, the user accesses to company’s resources

TLS VPN

Remote access (to private network):

- TLS communications between the nomad and the TLS VPN gateway
- TLS VPN gateway being used as an interface between the device and the applications within the private network



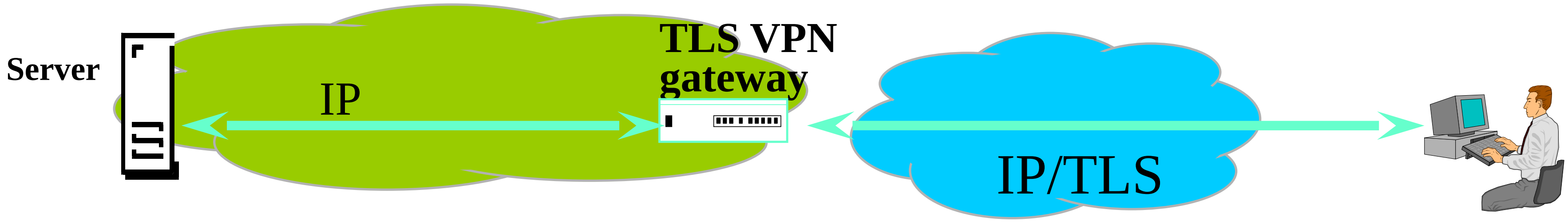
TLS VPN

Clientless solution (without client)

– Ex: Webised applications (the gateway translated data returned by the applications into web data)

Non clientless solutions (with a client)

– Ex: Heavy TLS client (solution similar to IPsec)



TLS VPN

Advantages/drawbacks of clientless TLS VPN:

- ✪ No need to install specific clients
- ✪ Easy management
- ✪ Lower costs
- ☹ Restricted access to « webised » applications

Advantages/drawbacks of IPsec VPN/TLS (with client)

- ✪ Access to private network similar to local connection
- ☹ Sometimes need to install and manage an Ipsec/VPN client within the nomad

Security protocols
Advantages and drawbacks

IPsec advantages:

- Common solution for all the applications
- Adapted to VPN (site to site and nomads)

IPsec drawbacks:

- Heavy to manage (application-level IKE module)

Security protocols
Advantages and drawbacks

TLS advantages:

- The most common solution (included by default in browsers)
- Largely used for nomads’ remote access protection (VPN)

TLS drawbacks:

- According to TLS VPN solutions, access limited to certain applications