Advanced Networking

IPsec
Security Architecture for IP

Csaba Kiraly
kiraly@disi.unitn.it

based on slides from Prof. Giuseppe Bianchi

Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)
- **VPN**

Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)

Topics

- ***Overview of security services***
  - *Based on ISO OSI security reference model*
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)

Networking & Security

Security services as defined by ISO

- ⇨Defined in the same set of standards as the famous ISO OSI 7 layers (ISO 7498-1) (*1984*)
- ⇨ISO 7498-2 OSI Basic Reference Model Part 2: Security Architecture (*1989*)
  - →Security **services**: what to do
  - →Security **mechanism**: how to achieve it
  - →**Mapping** between services and mechanisms
  - →Potential **mapping** to 7 layers: where to implement

Further reading: ISO 7498-2 in not free, but you can download free equivalent from ITU as ITU-T X.800

Security Services (what?)

Authentication

- ⇨ To know who it is: the process of **proving** identity
  - → Mutual: both parties identified
  - → One-way: only one side proves identity

Access control

- ⇨ Control access rights to a resource (communication; read/write/delete of data)
  - → Good authentication is a pre-condition!

Data confidentiality

- ⇨ protection of data from unauthorized disclosure

Data integrity

- ⇨ Preventing/detecting modification of the data

Non-repudiation

- ⇨ Preventing an individual or entity from denying having performed a particular action
- ⇨ The recipient of data is provided with proof of the origin of data
- ⇨ The sender of data is provided with proof of delivery of data.

Security Mechanisms (how?)

Some examples only!

➔ Encryption

- ⇨ symmetric key cryptography
  - ➔ knowledge of the encryption key implies knowledge of the decryption key and vice versa;
- ⇨ asymmetric (or “public”) key cryptography
  - ➔ knowledge of the decryption key (public key) does not imply knowledge of the encryption key (private key).

Used in: mainly in confidentiality, but also in authentication

➔ Digital signatures

Used in: authentication, data integrity, non-repudiation

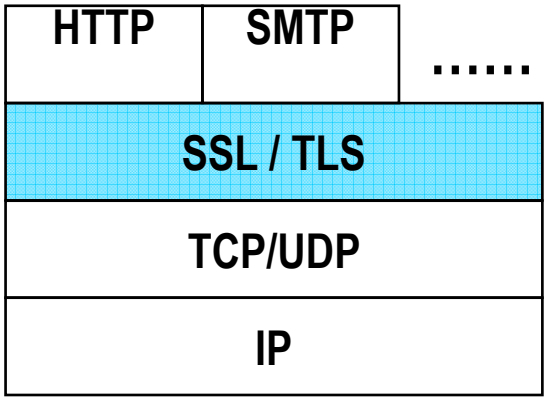
Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- ***How some known protocols map to the ISO OSI model?***
  - *To layers*
  - *To security model*
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)

Protocols you might use (or know) layer 3 and above

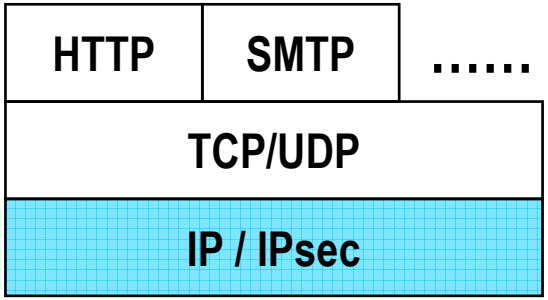
➔SSL/TLS over TCP

- ⇨Layer: 4+ (above TCP)
- ⇨Security services:
  - ➔Authentication (mutual / one-way)
  - ➔Data confidentiality
  - ➔Data integrity



➔IPsec

- ⇨Layer: 3
- ⇨Security services:
  - ➔Authentication (mutual)
  - ➔Access control
  - ➔Data confidentiality
  - ➔Data integrity



Protocols you might use (or know) layer 1,2

Wired

➔ physical protection of the wire!

Wireless

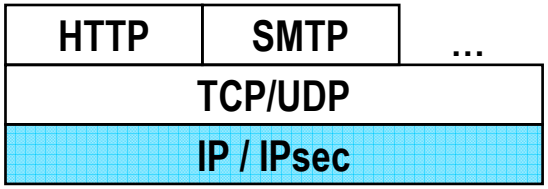
➔ WEP (Wired Equivalent Privacy)

- ⇨ Layer: 2
- ⇨ Security services:
  - →Authentication (weak)
  - →Data confidentiality (weak)
  - →Data integrity (weak)

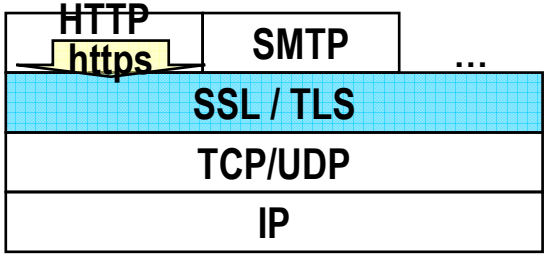
➔ 802.1x (port-based Network Access Control)

- ⇨ "port" is the LAN port (not the TCP/UDP one)
- ⇨ Layer: 2
- ⇨ Security services:
  - →Access control

SSL/TLS: why layer 4



Network layer security



Transport layer security

😐 **TLS is transparent for routers**

- ⇨ It operates over TCP … well above IP
  - → IP header is the same => IP routing is not affected
  - → The TCP stream is encrypted, but a router should not look at that
  - → There are some port numbers typically used with TLS, but this is not mandatory (443:https, 993:imaps)

☺ **TLS is implemented above Layer 4, in the application**

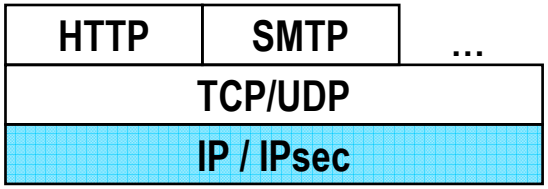
- ⇨ No need to change the OS => fast deployment
  - → Early versions (1994) came as part of Netscape browser
- ⇨ Easy to come up with new modified versions
  - → Dangerous for security protocols!

☹ **TLS relies on TCP's reliable stream delivery service**

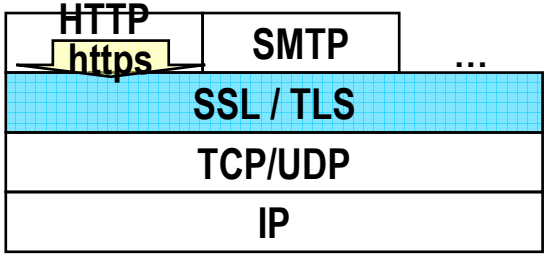
- ⇨ What about security for applications using UDP?
- ⇨ What about other protocols over IP?

☹ **Each application should be changed**

IPsec: why layer 3



Network layer security



Transport layer security

😐 **IPsec is transparent for routers**

- ⇨ IPsec operates within (as an upper sub-layer of) layer 3
  - → Uses extension header mechanism: seen by routers as "next protocol" in IP header
  - → packets are routed just as plain IP packets

☺ **Applications/terminals unaware of IPsec**

- ⇨ IPsec can protect all protocols that rely on IP (but it is hard to differentiate between applications, only TCP/UDP port based differentiation)
- ⇨ It can protect the traffic of whole subnets (tunnel mode, VPN)

☹ **Works only if IP routing works**

- ⇨ Has difficulties passing NAT/NAPT
- ⇨ Not suitable if application level (e.g. HTTP) proxies are used

☹ **Should be implemented in layer 3**

- ⇨ In the kernel of the operating system, not in the application

Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- ***IPsec***
  - *Introduction (operation modes)*
  - *Architecture (much more than a protocol)*
  - *protocols (ESP, AH)*
  - *Management (SAD, SPD)*
  - *Signaling (IKE)*

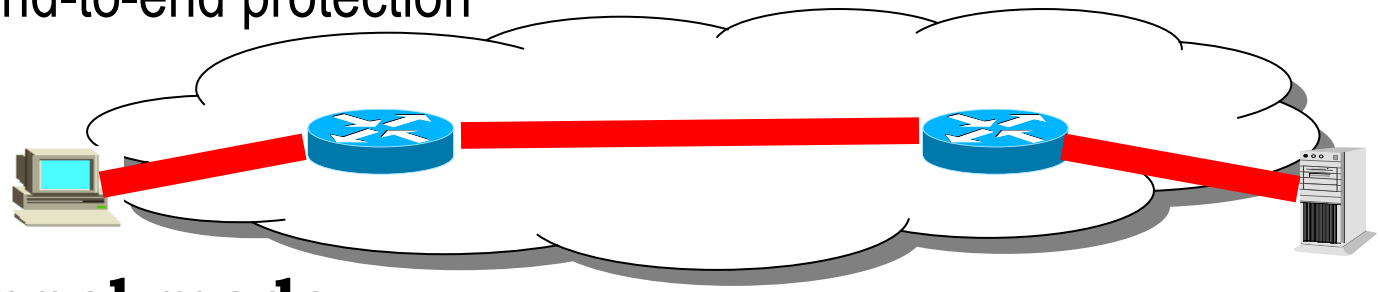
Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - *Introduction (operation modes)*
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)

IPsec operation modes

➔Transport mode

⇨End-to-end protection



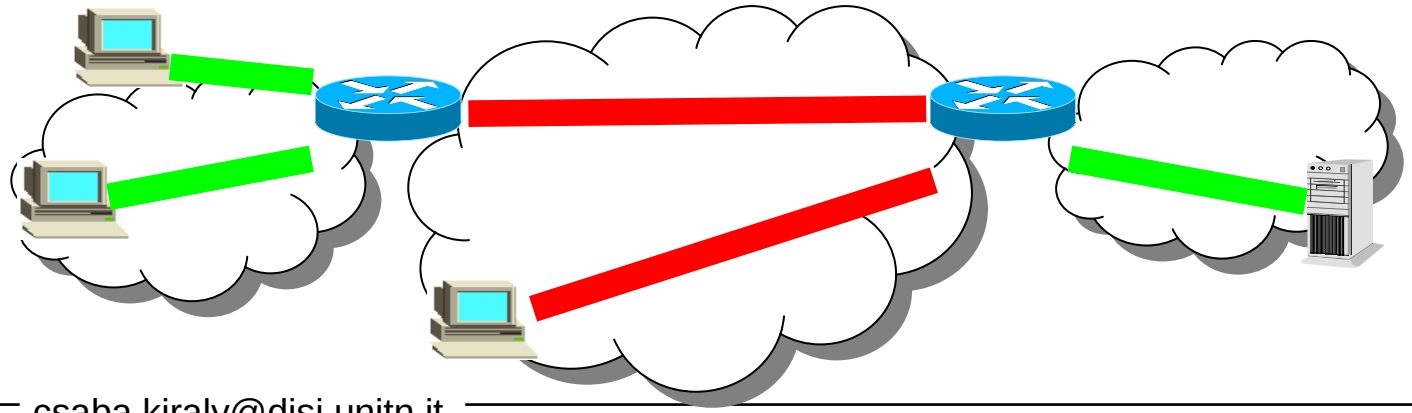
➔Tunnel mode

⇨Security gateway to Security gateway protection

➔E.g. to connect corporate sites

⇨Host to Security gateway protection

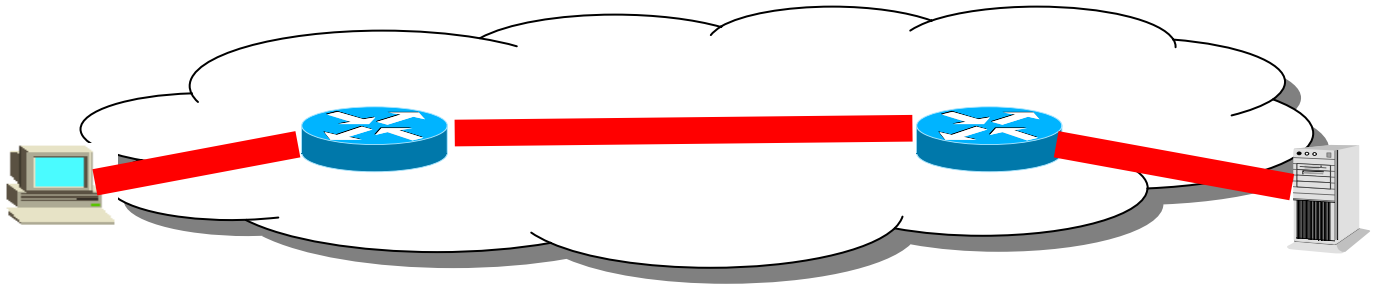
➔E.g. roaming users to connec to to home network

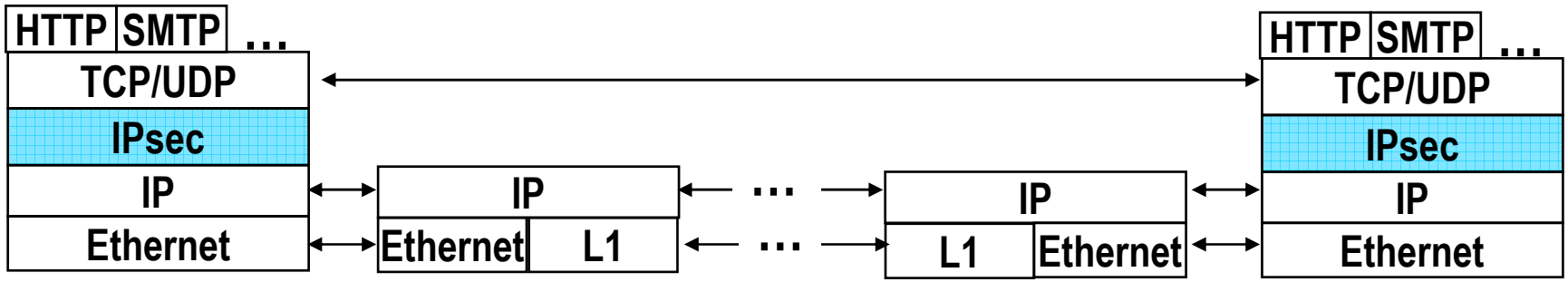


IPsec operation modes

➔Transport mode

⇨End-to-end protection

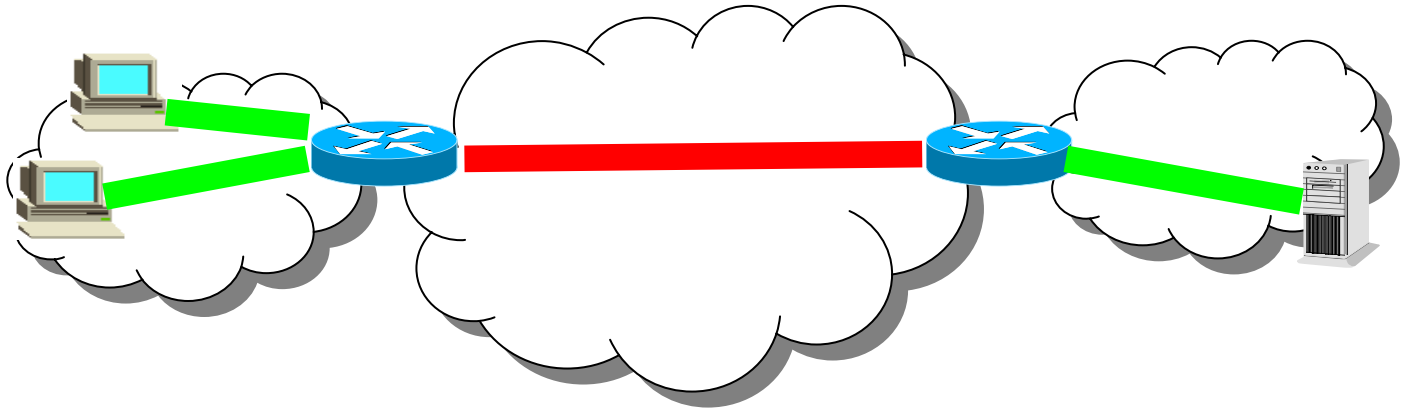




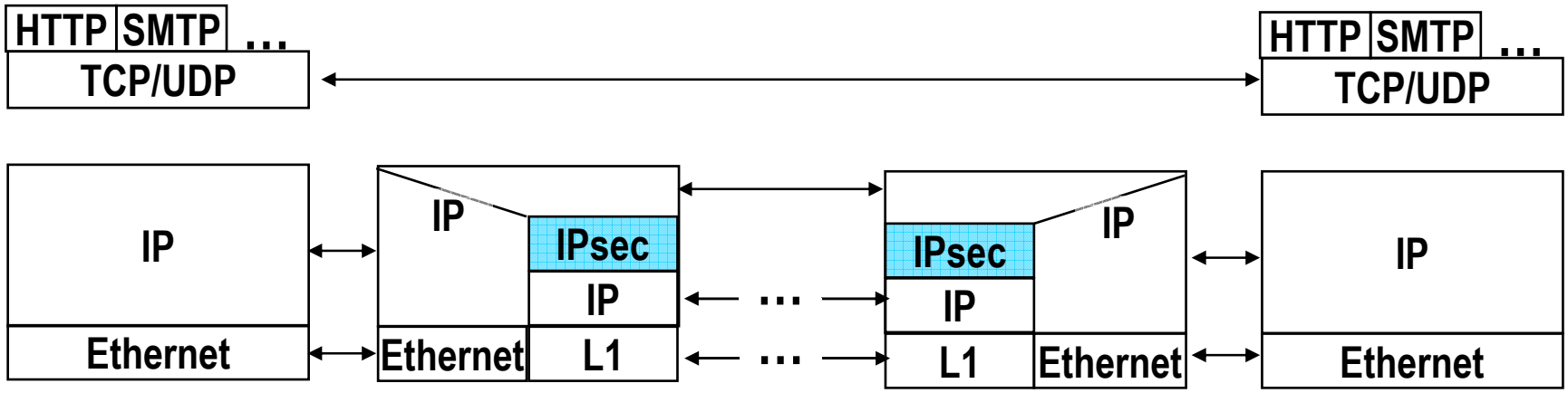
IPsec operation modes

➔ Tunnel mode

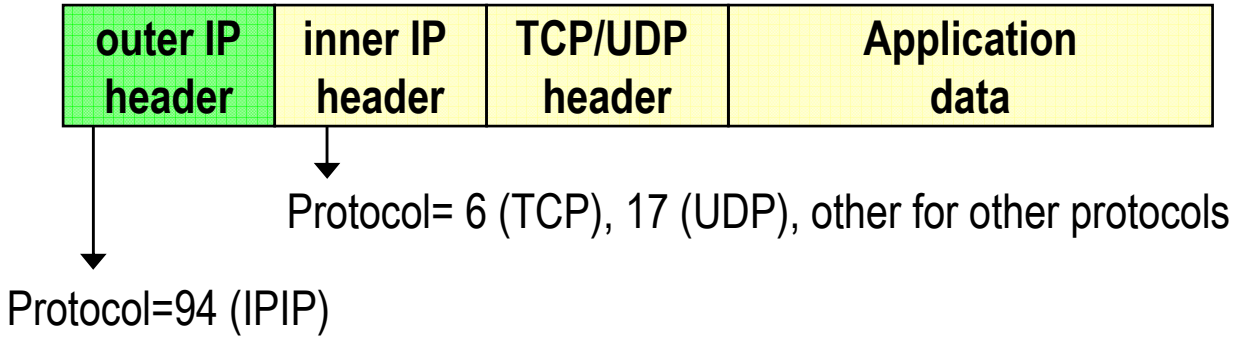
⇨ Security gateway to Security gateway protection



⇨ protocol stacking with IP-in-IP tunneling



IP-in-IP tunneling



➔ **Encapsulate an IP packet in an IP packet**
- ⇨ IP can encapsulate other PDUs, not just TCP/UDP/ICMP
- ⇨ Why not IP itself?
- ⇨ the “protocol” field should be filled: 94=IPIP

➔ **Routing is done based on the outer header’s destination IP**
- ⇨ Internal IP header is not checked by routers
- ⇨ Protocol field not used in routing (firewalls are problematic)

➔ **Once this IP packet arrives to its destination (outer), the internal IP packet is decapsulated**
- ⇨ Routing can continue based on internal destination IP

Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - *Architecture (much more than a protocol)*
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)
  - History (RFC series)

IPsec: Security Architecture for IP

➔ **IPsec is not a protocol, but a complete architecture! Components:**

1. Security Protocols (ESP, AH), each having different
   - ➔ Protocol header
   - ➔ Implemented security mechanisms
   - ➔ Provided security services
2. Cryptographic Algorithms (3DES, etc.)
   - ➔ Used by security protocols
   - ➔ Each having advantages/disadvantages, e.g.
     - » Computational complexity
     - » Block size
3. Management concepts and local management databases
   - ➔ Security Policies (SP):
     - » established and maintained by a user or system administrator
     - » select IP packets where IPsec should be applied
   - ➔ Security Associations (SA):
     - » simplex "connection" that affords security services to the traffic carried by it
4. Signaling protocols
   - ➔ Internet Key Exchange (IKEv2)

Topics

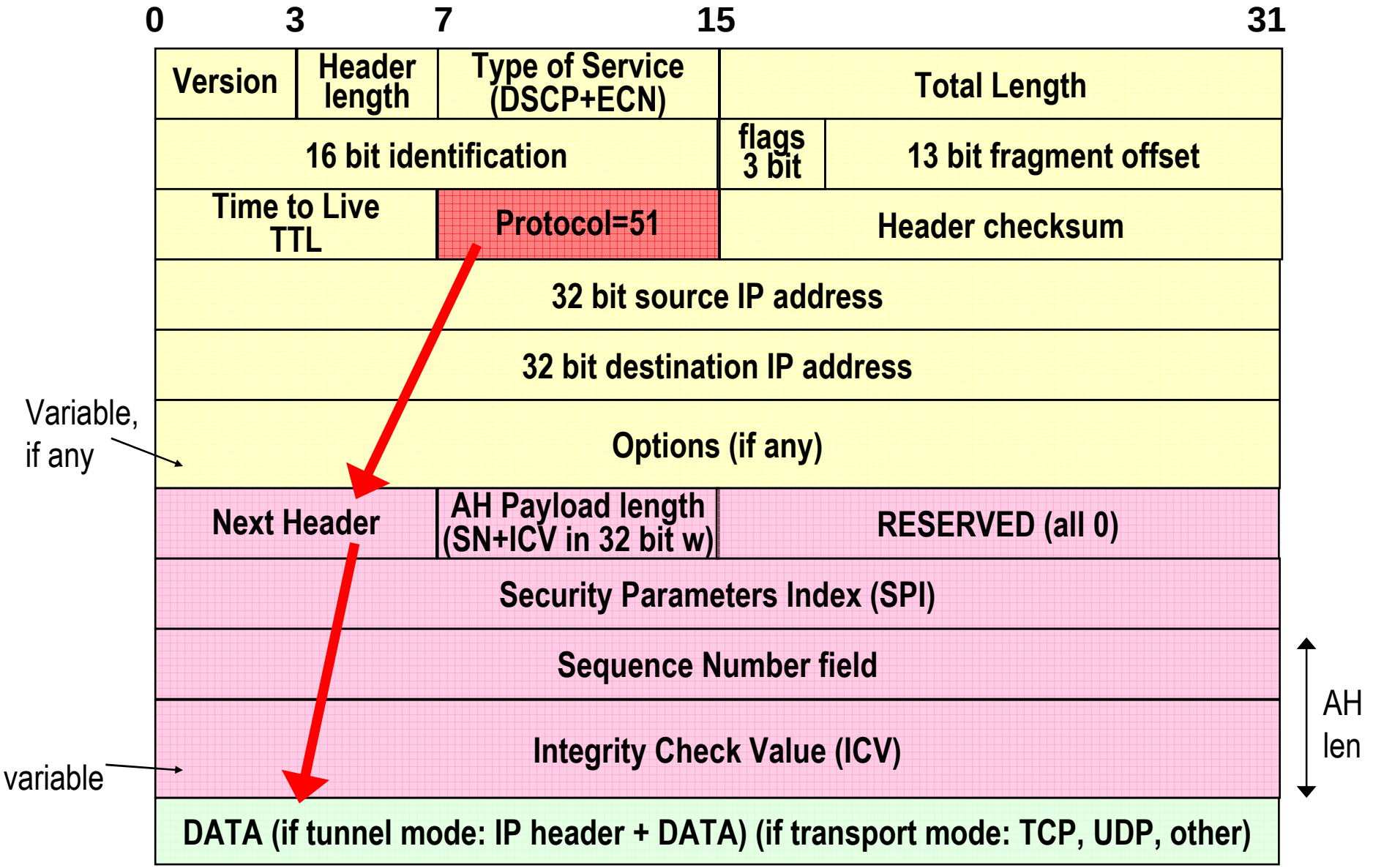
- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - Architecture (much more than a protocol)
  - *Protocols (ESP, AH)*
  - Management (SAD, SPD)
  - Signaling (IKE)
  - History (RFC series)

IPsec Security Protocols
AH,ESP
(discuss IPv4 only)

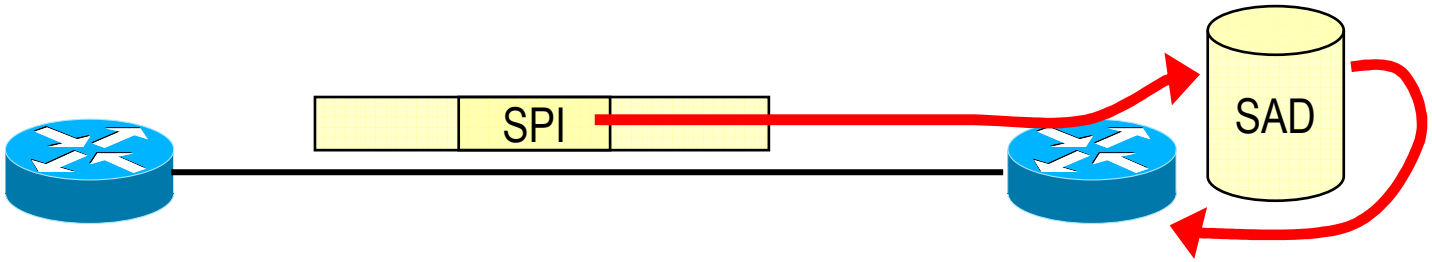
Services provided

- **AH: Authentication Header**
  - Data integrity protection and data origin authentication
    - Covers both payload and parts of IP header that do not modify in transfer
  - Protection against replays
    - Optional, through extended sequence numbers
- **ESP: Encapsulated Security Payload**
  - Same services as AH
    - authentication limited to IP payload only!
  - Confidentiality through encryption
  - Traffic flow confidentiality
    - Improved privacy against eavesdropping
    - Through padding and dummy traffic generation

Authentication Header



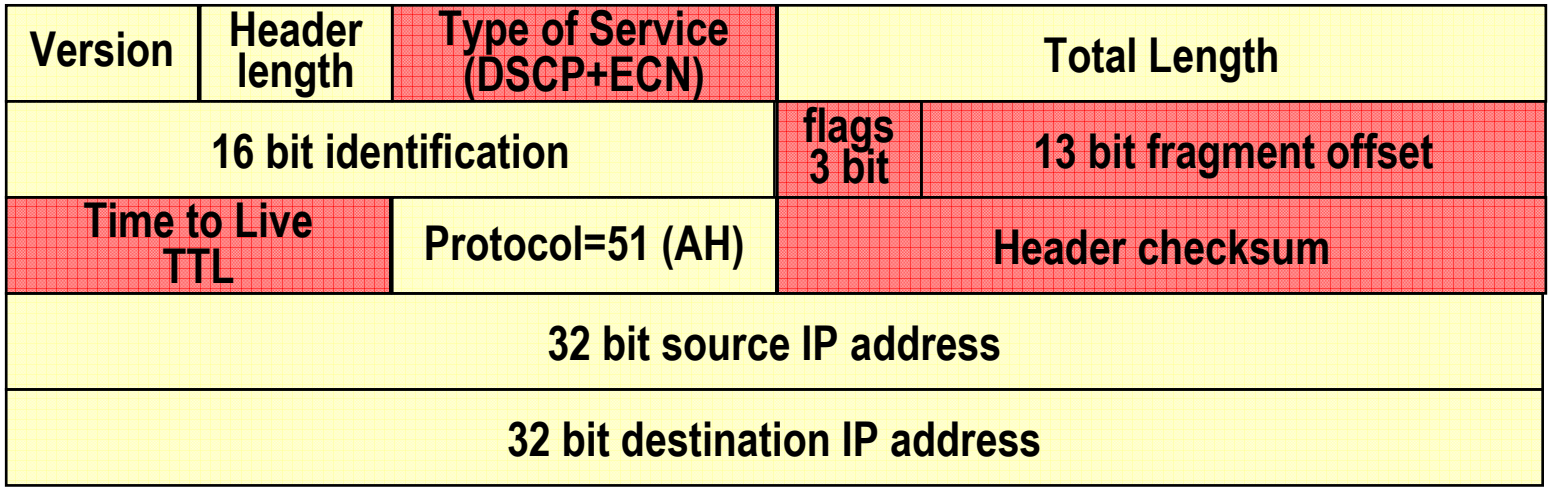
Security Parameters Index



- **32 bit index**
- **Role: like port number in TCP and UDP**
- **Used to lookup the SAD at destination**
  - Lookup also uses
    - destination address
    - source address
    - security protocol (AH/ESP)
- **Retrieves algorithms and parameters that allow to process received packet**

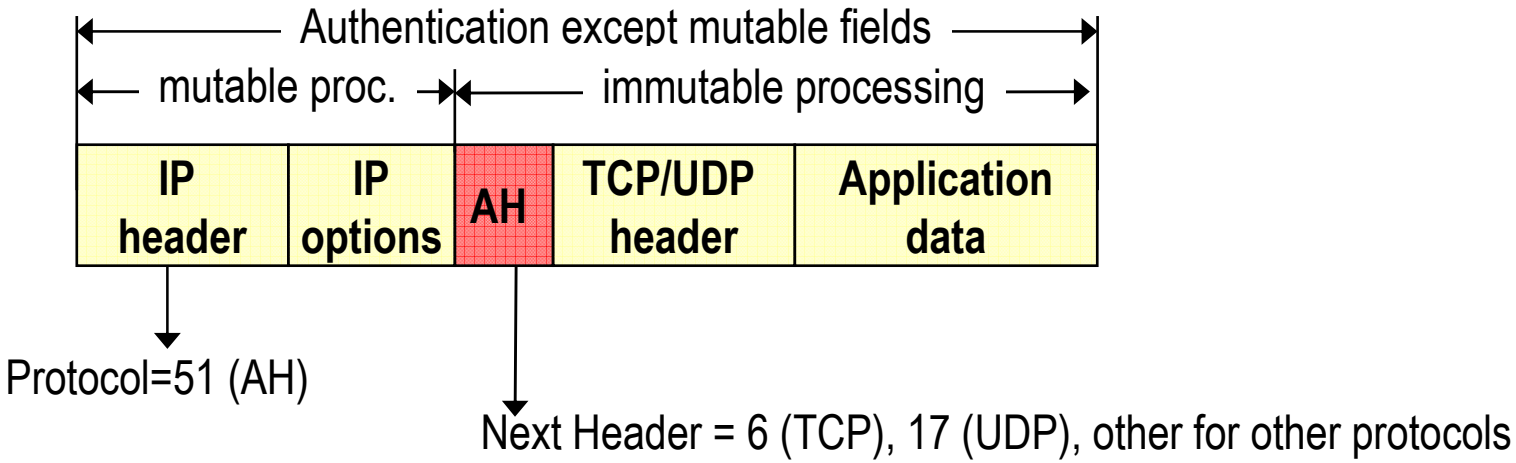
Integrity Check Value computation

- **Only on immutable fields in the IP header**
  - Or mutable but predictable
    - e.g. destination address with strict/loose source routing option
- **Mutable fields set to 0 during ICV computation**
  - Highlighted in red in next figure
    - Note: AH apply before fragmentation, and checked after reassembly
- **Options classified as either mutable or not**
    - Mutable options: details in appendix A RFC 4302
    - mutable options = all zeroed

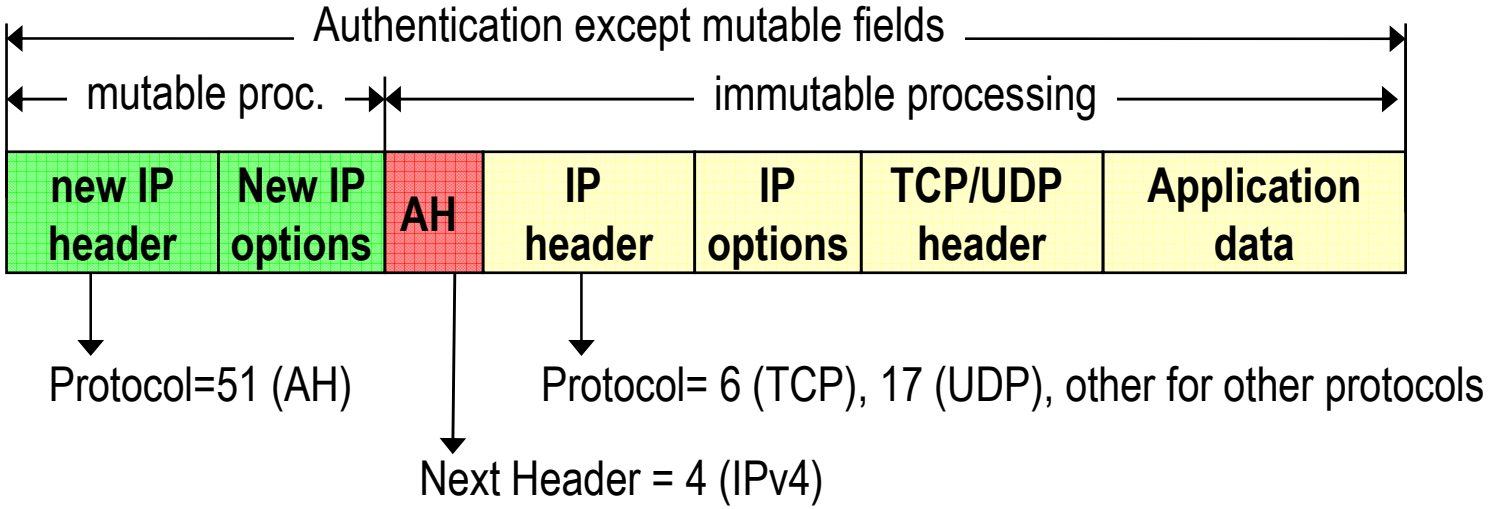


Transport mode, tunnel mode

Transport mode:



Tunnel mode:



Why sequence number?

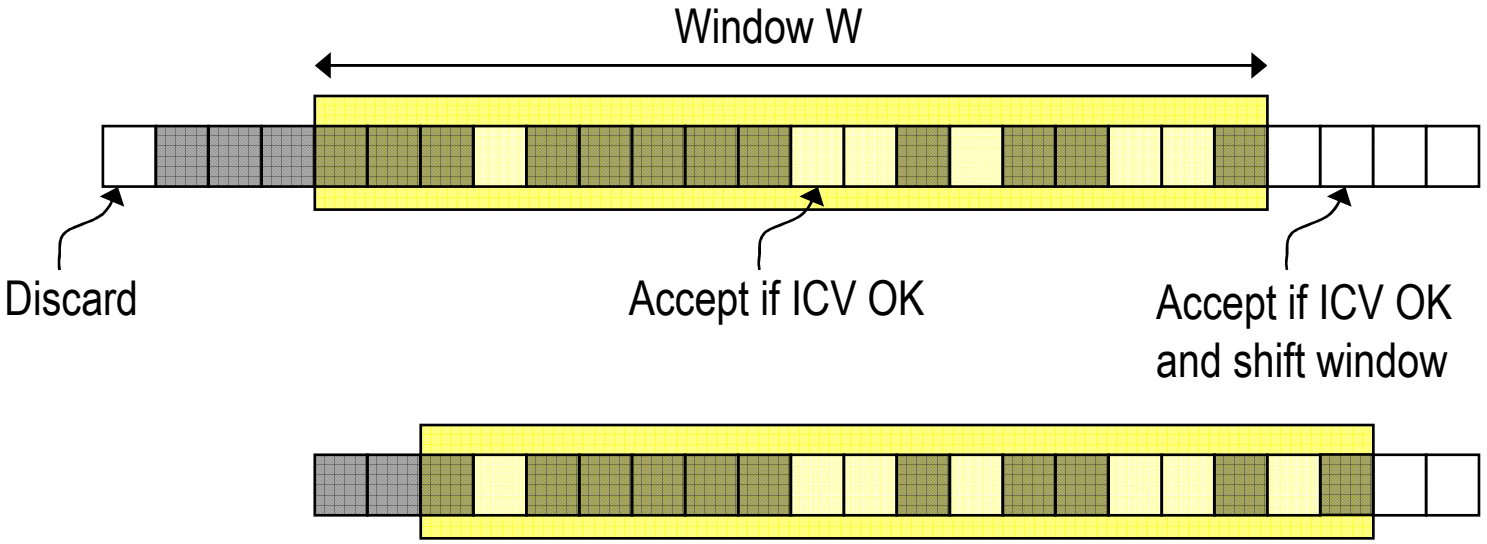
- **IP header DOES NOT contain a sequence number!**
  - Hence replay of an authenticated IP packet is possible
    - And may alter in an unpredictable manner the overlaying service (e.g. ICMP replies can be dangerous ☺)
- **Sequence number: 32 bit counter**
  - Initialized to 0 when the Security Association is established
  - Increments of 1 per each transmitted packet
    - First transmitted packet: SN=1
  - Maximum value 2^{32}-1, afterwards Security Association must be terminated
    - No counter cycling allowed when anti-replay service active
    - Anti-replay: optional (but default = on)
      - » Anti-replay typically OFF when manual (static) keys configured

Extended Sequence Number

- **2^{32} ~ 4.3 billion**
  - A lot, but not REALLY al lot!
    - Packet size = 1500 (1460 bytes payload)
    - 2^{32} x 1460 bytes = 6270 GB
    - About 14 h transmission of a 1 Gbps link
- **Extended Sequence Number:**
  - 64 bits - this should be enough, now ☺
  - Transmit only low order 32 bits
  - But use high order 32 bits in ICV computation!

Anti-replay

- **Sliding Window W**
  - Size locally decided at receiver
    - Minimum = 32; default = 64; higher values recommended for high speed links
    - eventually very large: maximum 2^{31}-1 with SN and 2^{32}-1 with ESN
  - Window right margin = highest NS packet received
- **Duplicates discarded**
- **Packets out of left window edge discarded**
- **Packets greater than right window margin make W shift**



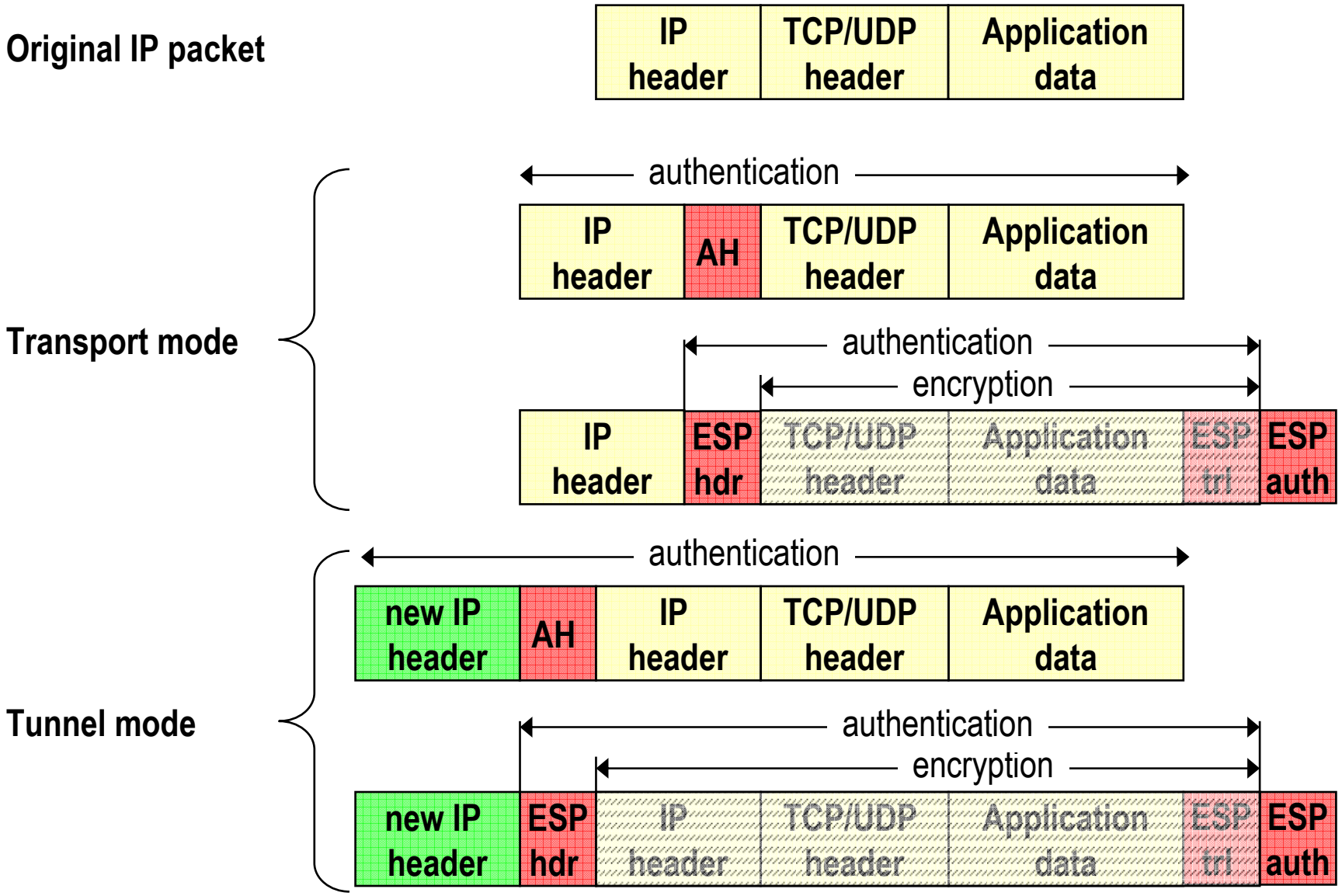
ESP
Encapsulated Security Payload

Encapsulated Security Payload

➔Security services

- ⇨Same services as AH
  - ➔authentication limited to IP payload only!
- ⇨Confidentiality through encryption
- ⇨Traffic flow confidentiality
  - ➔Improved privacy against eavesdropping
  - ➔Through padding and dummy traffic generation

Transport vs Tunnel – AH and ESP



Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - *Management (SAD, SPD)*
  - Signaling (IKE)
  - History (RFC series)

IPsec management

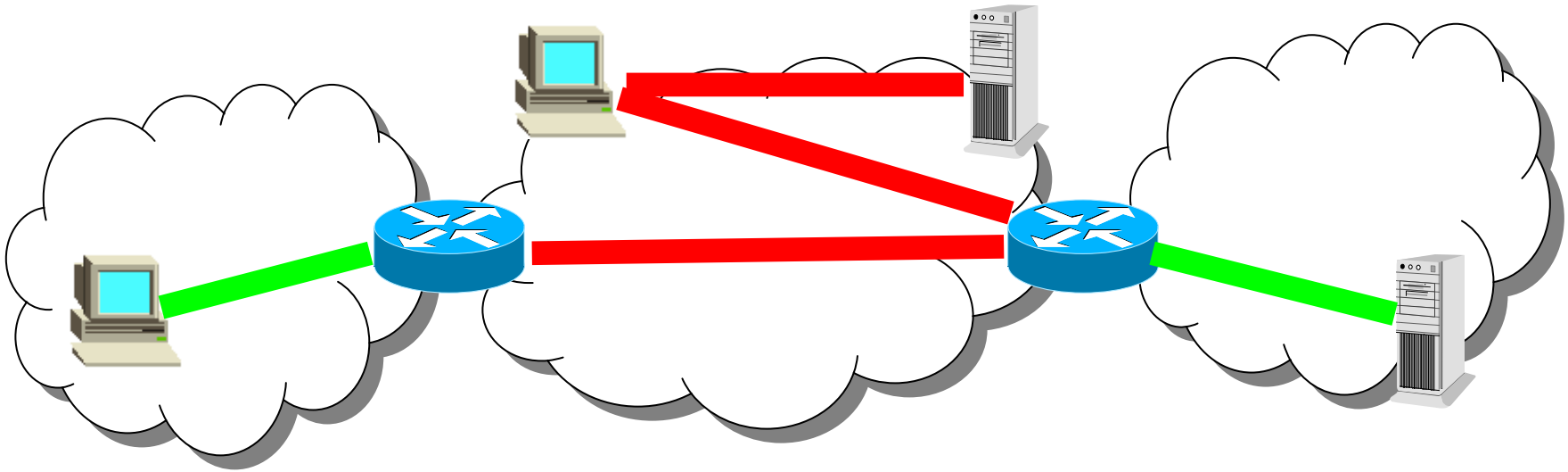
SA: Security Association
SAD: SA Database

SP: Security Policy
SPD: SP Database

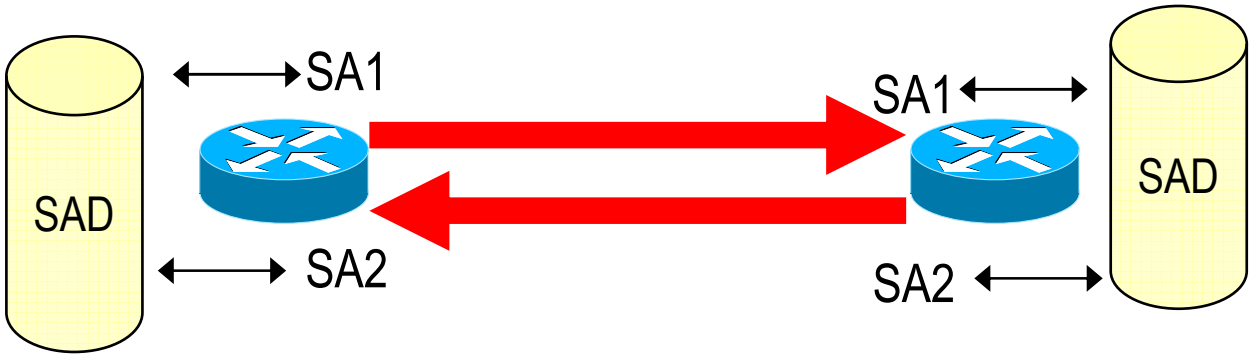
SPI: Security Parameters Index

Security Association (SA)

- **Fundamental concept in IPsec**
- **May involve:**
  - Host to host
  - Host to intermediate router (security gateways)
  - Security gateway to security gateway
- **Defines the boundaries for IP packets authentication/encryption**
  - A “connection” with active security services



SA: unidirectional!



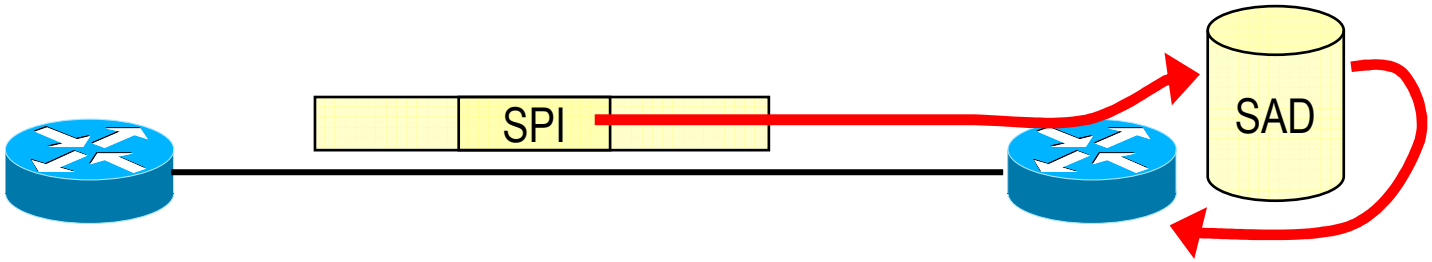
➔ **SPI = Security Parameters Index**

- ⇨ The (somewhat) unique “name” of an SA

➔ **SAD = Security Associations Database**

- ⇨ SPI = search key (at least)
- ⇨ Stores type of security protocol per each SA, with related parameters
  - ➔ E.g. which encryption algorithm; shared key for encryption, SA lifetime, Sequence number counter, etc.
- ⇨ SA should be in SAD on both sides, at sender and at receiver!

Security Parameters Index

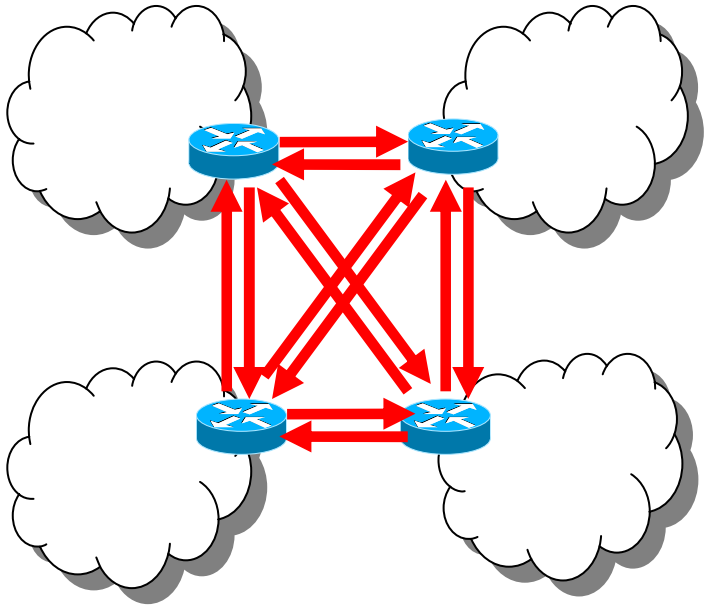


- **32 bit index**
- **Role: like port number in TCP and UDP**
  - Allows multiple SAs between the same two hosts
- **Used to lookup the SAD at destination**
  - Lookup also uses
    - destination address
    - source address
    - security protocol (AH/ESP)
- **Retrieves algorithms and parameters that allow to process received packet**

Security Association and Key management

➔ Manual

- ⇨ Manually configure each SA and related crypto keys
  - → static, symmetric
- ⇨ Typical in small-scale VPNs
  - → Few security gateways, e.g. one per site
  - → Meshed SA connections

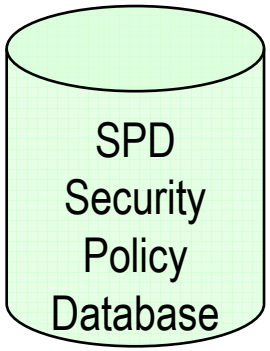


➔ Automatic

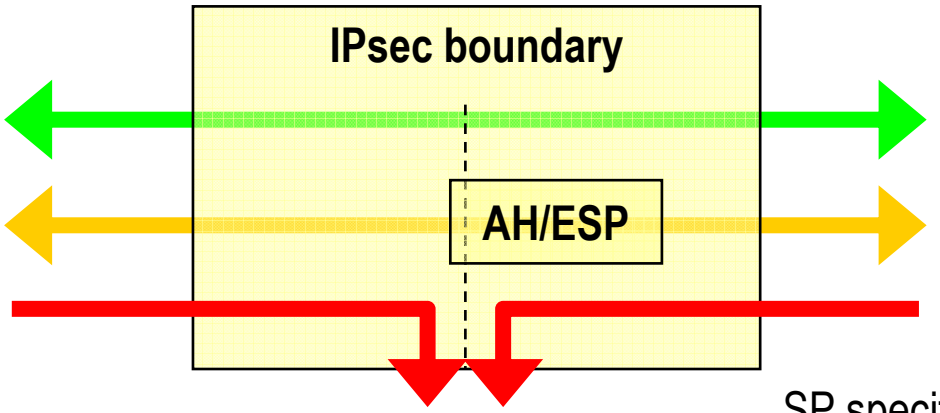
- ⇨ SA management through IKEv2
- ⇨ On-demand SA creation
- ⇨ Session-oriented keying/rekeying

IPsec protection & access control

Protected Interface
- Internal Network with IPsec Security GW;
- Host OS with IPsec Host



Unprotected Interface
- The external network



BYPASS
PROTECT
DISCARD

Three rules

Outbound Traffic

Inbound Traffic

SP specifies:
- On which packets/traffic relations
- Which security protocols (AH, ESP)
- Which mode (tunnel, transport)
- Which granularity
  - single shared tunnel
  - different tunnels per TCP conn

IPsec processing

1. **PDU enters IPsec processing: two posibilities**
   - ⇨ Host: PDU from upper layer arrives, or
   - ⇨ Security GW: IP packet arrives
2. **SPD searched for matching SP**
   - ⇨ Search based on IP addresses, higher layer protocol, port number, etc.
3. **If SP found:**
   - a) If BYPASS: no IPsec processing needed
   - b) If DISCARD: PDU dropped (like in a firewall)
   - c) If PROTECT: we know that we have to protect, but we don't know how! It is defined in an SA. Search for corresponding SA in SAD
4. **If SA found, apply it**
   - ⇨ Encapsulate in ESP or AH, with the parameters of the SA
   - ⇨ Encapsulate in IP if tunnel mode
5. **Send protected packet**

IPsec processing

What happens If SP is not found?

- ⇨No problem, IPsec treatment not needed
- ⇨PDU goes as it would go otherwise

What happens If SA is not found?

- ⇨That is a problem: packet must be protected, but we don’t know how
- ⇨SA should be negotiated with other side
- ⇨Automatic keying is triggered, IKE starts …

Topics

- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - *Signaling (IKE)*

Rationale for IKE

- **shared state must be maintained between source and sink**
  - ⇨ Which security services (AH, ESP)
  - ⇨ Which Crypto algorithms
  - ⇨ Which crypto keys
- **Manual maintenance not scalable**
  - ⇨ Partially OK only for small scale VPNs
  - ⇨ In any case, weak approach
    - → Infinite lifetime SA → no rekeying!
- **IKE = Internet Key Exchange protocol**
  - ⇨ Goal: dynamically establish and maintain SA
  - ⇨ IKE now (december 2005, RFC 4306) in version 2
    - → Replaces protocols specified in RFCs 2407, 2408, 2409 (IKE, ISAKMP, DOI)
    - → IKEv2 quite different (and much cleaner!!) than former specifications

Topics

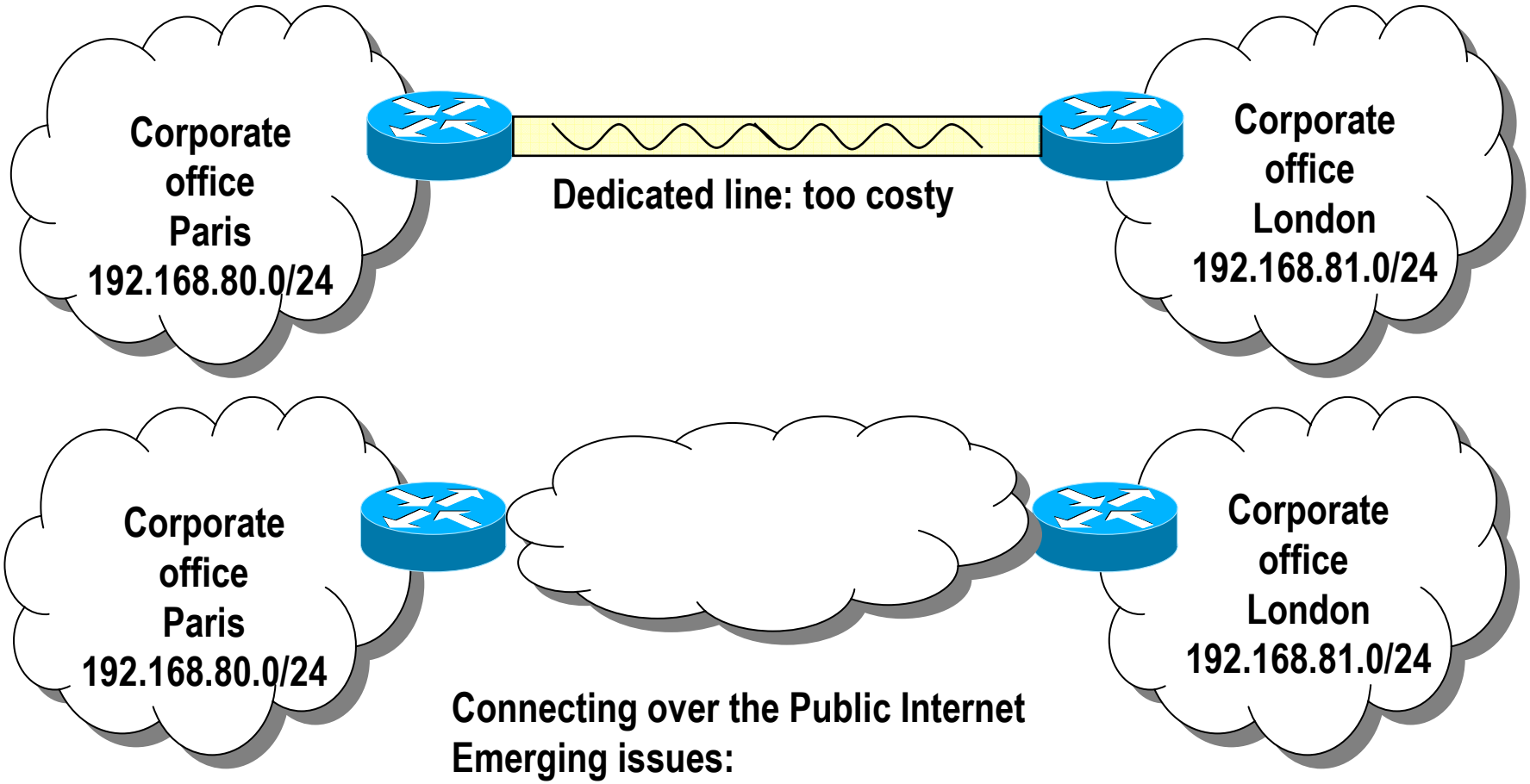
- **Overview of security services**
  - Based on ISO OSI security reference model
- **How some known protocols map to the ISO OSI model?**
  - To layers
  - To security model
- **IPsec**
  - Introduction (operation modes, relation to IPv6, extension headers)
  - Architecture (much more than a protocol)
  - protocols (ESP, AH)
  - Management (SAD, SPD)
  - Signaling (IKE)

Trying IPsec: StrongSwan virtual laboratories

http://www.strongswan.org/uml/

VPN
Virtual Private Network

Virtual Private Networks: why?

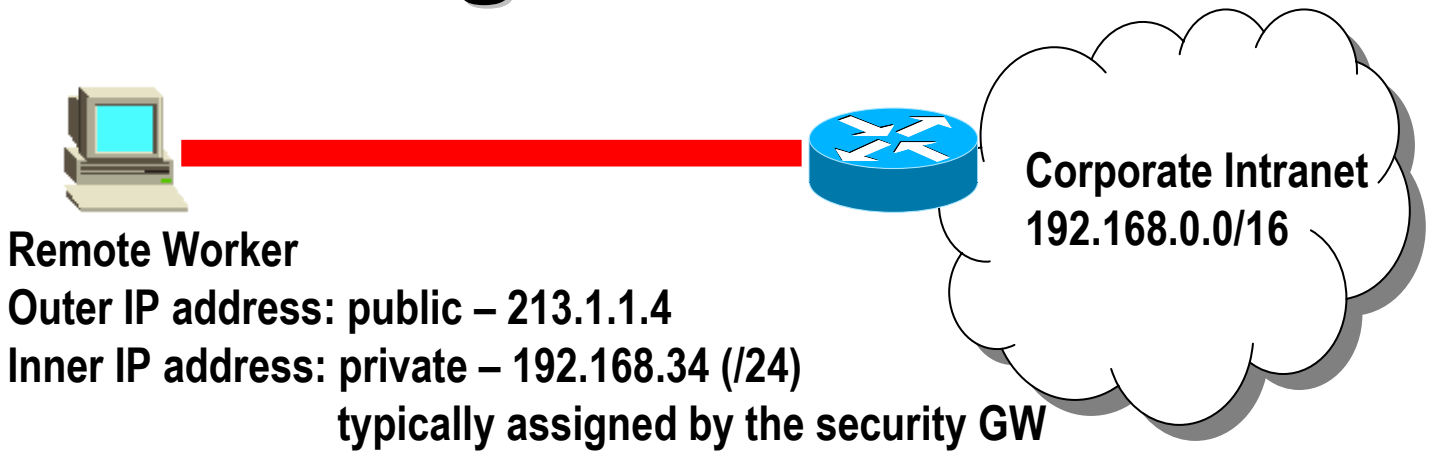


Connecting over the Public Internet

Emerging issues:

- How to manage routing across distributed sites?
- How to protect data in transit?

Virtual Private Networks: why? host-to-gw tunnels in VPN



➔Using a private IP address inside the tunnel:

- ⇨Allows to access to all services provided in the intranet, exactly like in the case the worker is connected inside the corporate

Virtual + Private Networks

➔ **VPN =**

⇨ Virtual Networks (tunnels)

+

⇨ Private Networks (authentication, encryption)

➔ **IPsec: a POSSIBLE tool for building VPN**

⇨ But IPsec and VPNs are NOT synonymous

➔ VPNs can use other technologies:

» e.g. when non-IP traffic must be transported

➔ IPsec has other uses:

» e.g. e2e encrypted/authenticated transport

➔ **VPN alternatives:**

➔ Layer 2: GRE/PPTP, L2TP

➔ Layer 3 (actually 3-): MPLS

➔ Layer 4 (actually between 4 and 7): SSL tunnels

➔ Layer 7: SSH tunnels