TÉCNICO LISBOA

IPsec and VPNs

Segurança Informática em Redes e Sistemas
2024/25

Ricardo Chaves, David R. Matos

Ack: Carlos Ribeiro, André Zúquete,
Miguel P. Correia, Miguel Pardal

Roadmap

- VPNs and tunneling
- IPsec
  - Main mechanisms
  - Key distribution

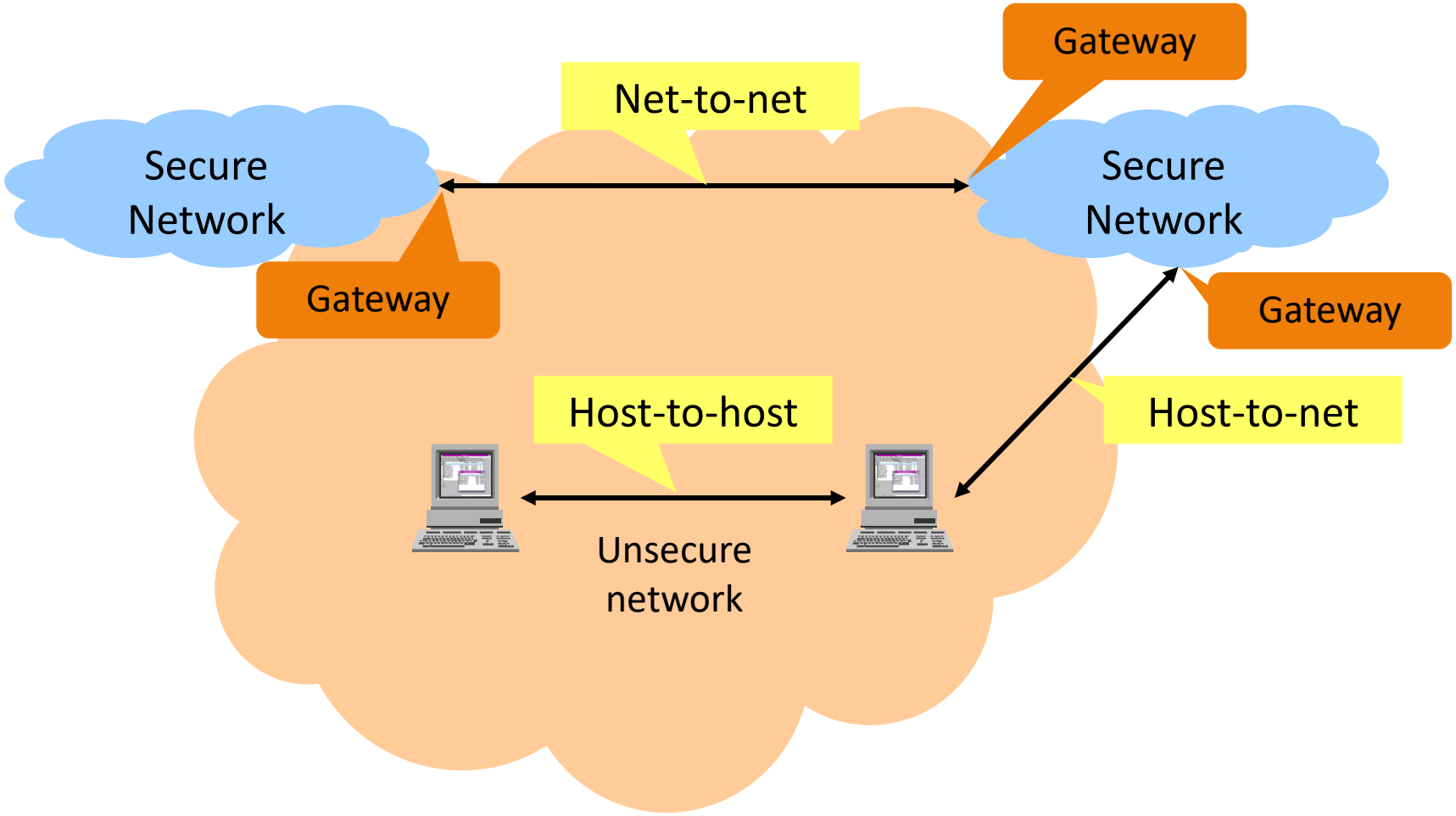
Roadmap

- **VPNs and tunneling**
- IPsec
  - Main mechanisms
  - Key distribution

VPN (Virtual Private Network)

- A **VPN** extends a private network across a public network
  - Enables users to send and receive data across shared or public networks
  - **As if** their computing devices were **directly connected** to the private network
- Applications running across a VPN may benefit from the functionality, security, and management of the private network

VPN usage modes



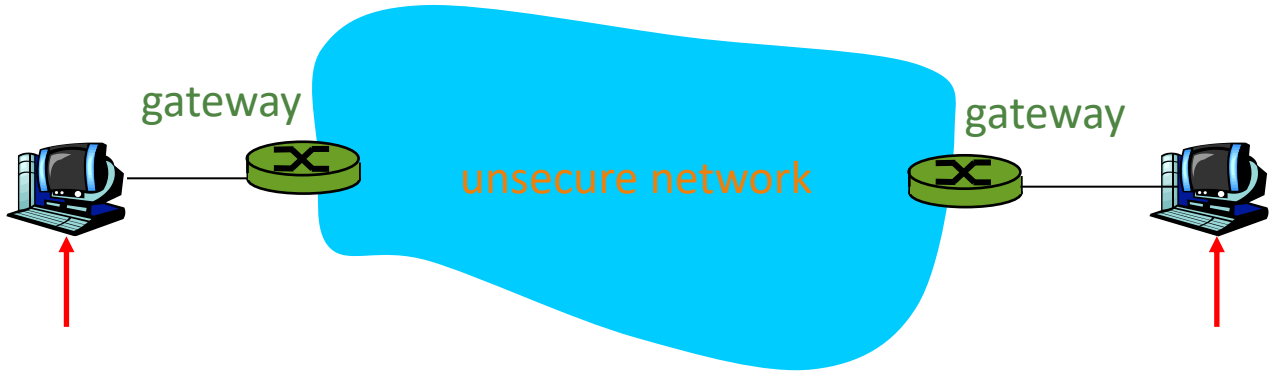
Tunneling

- Objective
  - Encapsulating a protocol inside another protocol

- Security benefits
  - Allows to associate security to the tunneling operation
  - Without interfering with the management infrastructure of the core protocol

VPN Gateway

- Communication unprotected in **internal networks**
  - Where it is assumed that no risk exists
- When data flows into an **unsecure network**, a **VPN gateway** transforms it to assure security
- Additional benefits
  - Intermediate nodes, e.g., Internet routers, can be unaware of secure channel
  - Firewall between gateway and node has access to data in cleartext



A VPN can hide traffic routes

- The traffic can be redirected by a gateway to a final destination
- A VPN is a type of overlay network
  - Virtual network built on top of existing network infrastructure
  - Enables custom routing, independent of the physical network layout
  - The VPN tunnel obscures the data's original routing information
    - Providing more security and privacy

Roadmap

- VPNs and tunneling
- **IPsec**
  - **Main mechanisms**
  - Key distribution

Secure communication: Network layer

Layers		Responsibility	Approach	Solutions
	Transaction	Local data manipulation applications	End-to-end security	PGP, PEM, S/MIME
OSI Layers	Application	Applications for remote data exchange		HTTPS, IMAPS SSH
	Presentation			
	Session			
	Transport	Operating Systems		TLS
	Network			IPsec
	Link	Devices	Link security	IEEE 802.11*
	Physical			

IP security

- Goals
- Operational scenarios
- Gateway
- Establishment of SA (Security Associations)

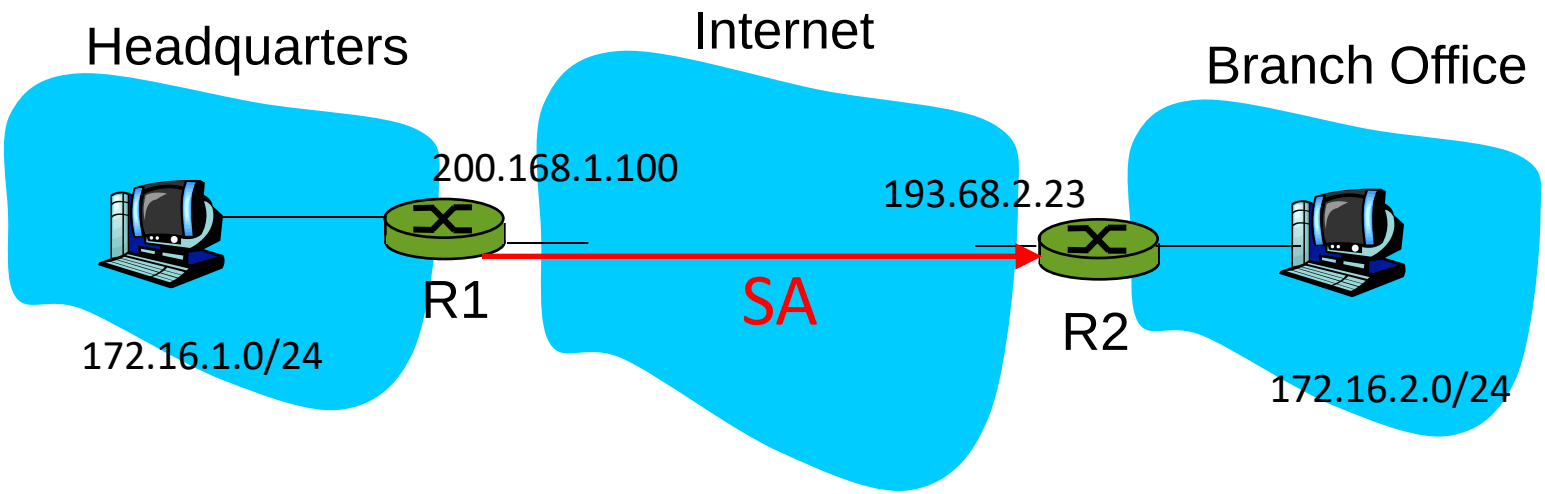
IPsec goals

- Protect all IP traffic between nodes:
  confidentiality, integrity, freshness, authenticity
- Two modes of operations:
  - **Transport Mode**: the original IP header is used for routing
  - **Tunnel Mode**: the original IP header is encapsulated
- Benefits
  - Provides secure channels
  - Only affects the network layer; transparent to higher-layer protocols
  - Avoids the update/modification of existing distributed applications
  - Uses the existing IP routing infrastructure; IP header is in plaintext
  - Security between endpoints is independent of the ISPs

SAs (Security Associations)

- Before sending data, **security associations (SAs)** are established at sending and receiving entity
- SAs are **simplex**, i.e., one for each direction
- Gateways maintain *state information* about SAs
  - IP is connectionless; **IPsec is connection-oriented**!

Example SA from R1 to R2



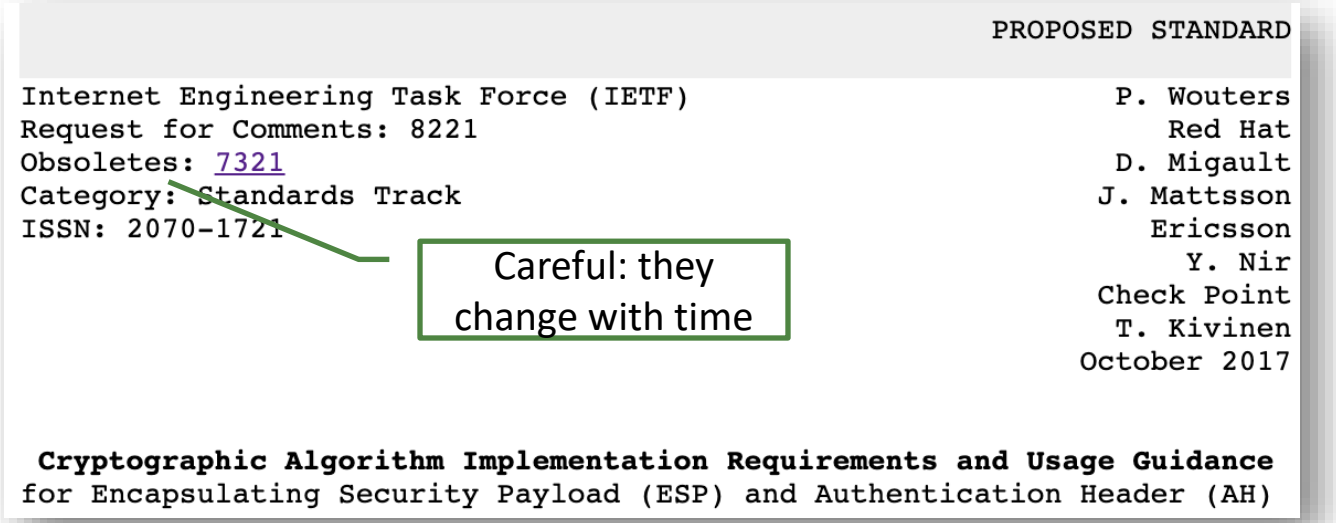
Router 1 stores for an SA:

- 32-bit SA identifier called **SPI (Security Parameter Index)**
- Origin SA interface IP address (200.168.1.100)
- Destination SA interface IP address (193.68.2.23)
- Type of encryption used (e.g., AES with CBC)
- Encryption key
- Type of integrity check used (e.g., HMAC with SHA-2)
- Authentication key (for obtaining HMACs)

SAD (Security Association Database)

- Endpoint holds SA state in the **SAD database**, where it can locate them during processing
  - The SAD is indexed using the **SPI (Security Parameter Index)**
- When **sending** IPsec datagram:
  - R1 accesses SAD to determine how to process the datagram
- When IPsec datagram **arrives** to R2:
  - R2 fetches the **SPI** from the IPsec datagram
  - indexes SAD with the **SPI**
  - and processes datagram accordingly

IPsec cryptographic techniques



PROPOSED STANDARD

Internet Engineering Task Force (IETF)
Request for Comments: 8221
Obsoletes: 7321
Category: Standards Track
ISSN: 2070-1721

P. Wouters
Red Hat
D. Migault
J. Mattsson
Ericsson
Y. Nir
Check Point
T. Kivinen
October 2017

Careful: they change with time

Cryptographic Algorithm Implementation Requirements and Usage Guidance
for Encapsulating Security Payload (ESP) and Authentication Header (AH)

- RFC 8221 (Oct 2017) essentially mandates:
  - ESP Encryption Algorithms: AES, ChaCha20
  - ESP and AH Authentication Algorithms: HMAC w/SHA-2
- In fact, it is more complicated:
  - It defines specific configurations of the algorithms
  - It makes “should”, “must”, “must not” statements

IPsec sub-protocols

- IPsec has two sub-protocols: AH and ESP

- **Authentication Header (AH)**
  - Can provide source authentication, data integrity, freshness, but ***not*** confidentiality
- **Encapsulating Security Payload (ESP)**
  - Can provide source authentication, data integrity, freshness, ***and*** *confidentiality*

AH vs ESP

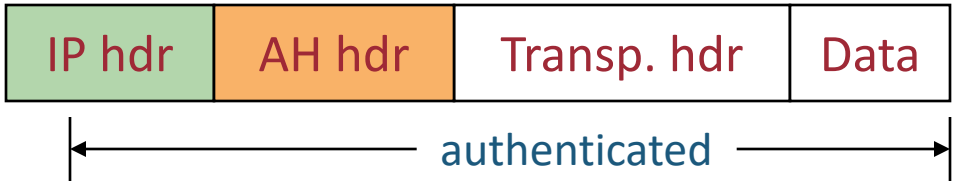
- **Authentication Header**
  - Can prevent IP spoofing (packet tampering) but **not** eavesdropping
  - Simpler and lower overhead than ESP

- **Encapsulating Security Payload**
  - Can prevent IP spoofing (packet tampering) and eavesdropping
  - ESP provides encryption and optional authentication

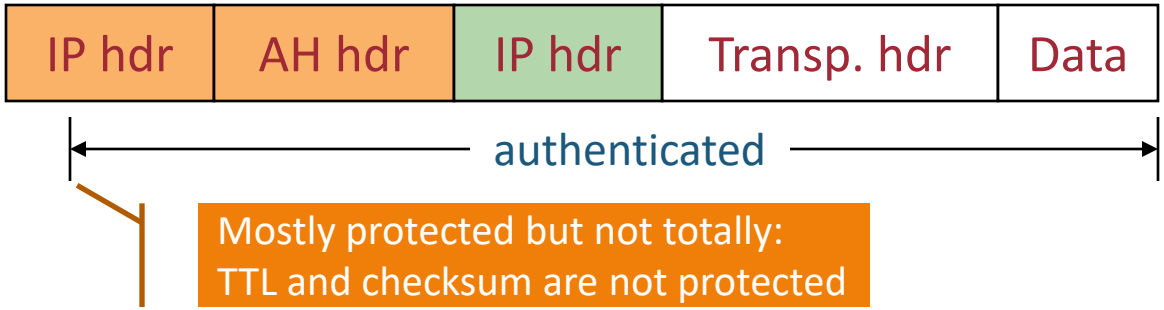
IPsec AH (Authentication Header)

Original packet

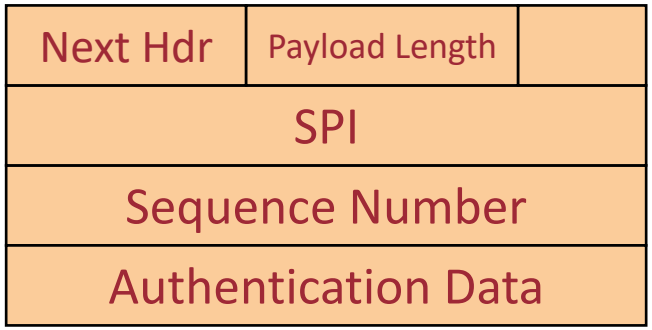
Transport mode



Tunnel mode



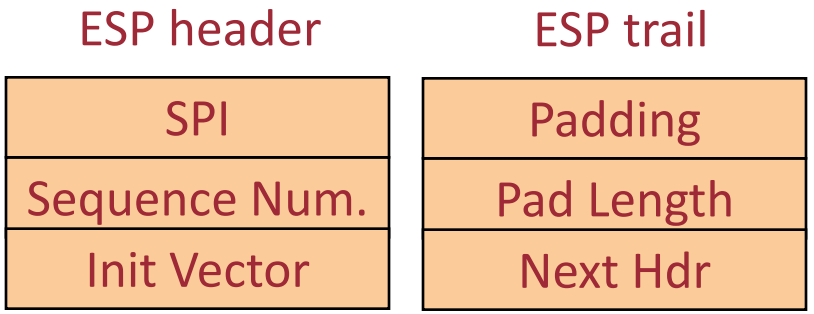
AH header



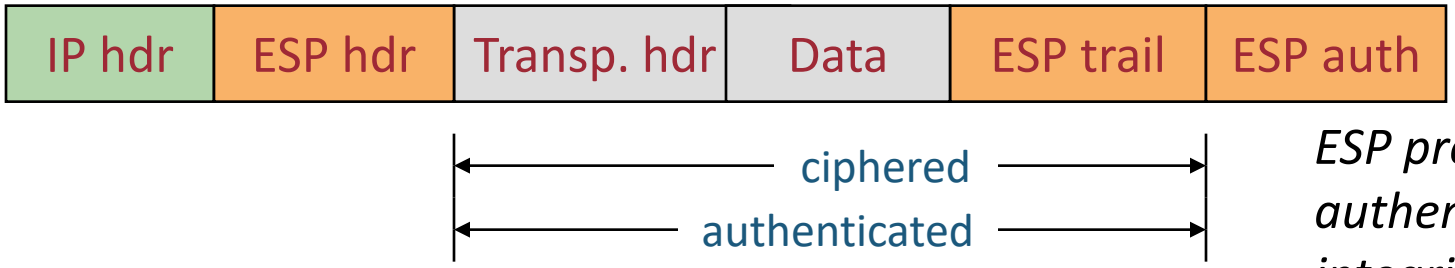
AH provides source authentication, data integrity, freshness, but not confidentiality

IPsec ESP (Encapsulating Security Payload)

Original packet

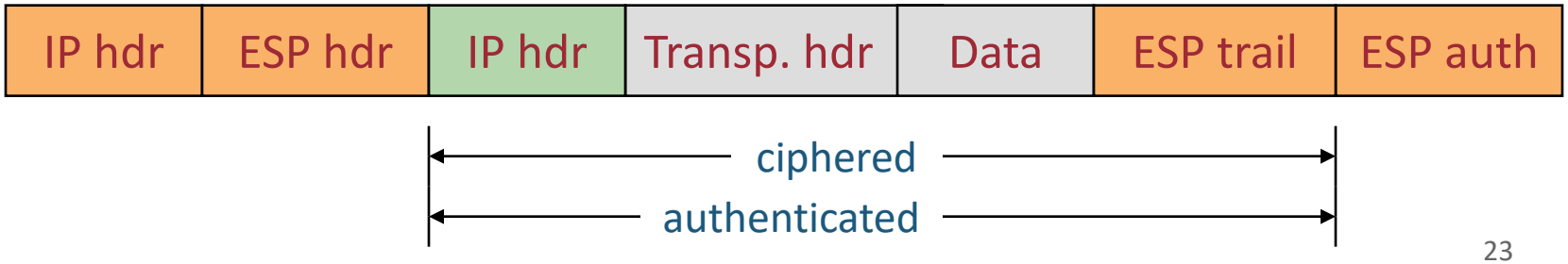


Transport mode

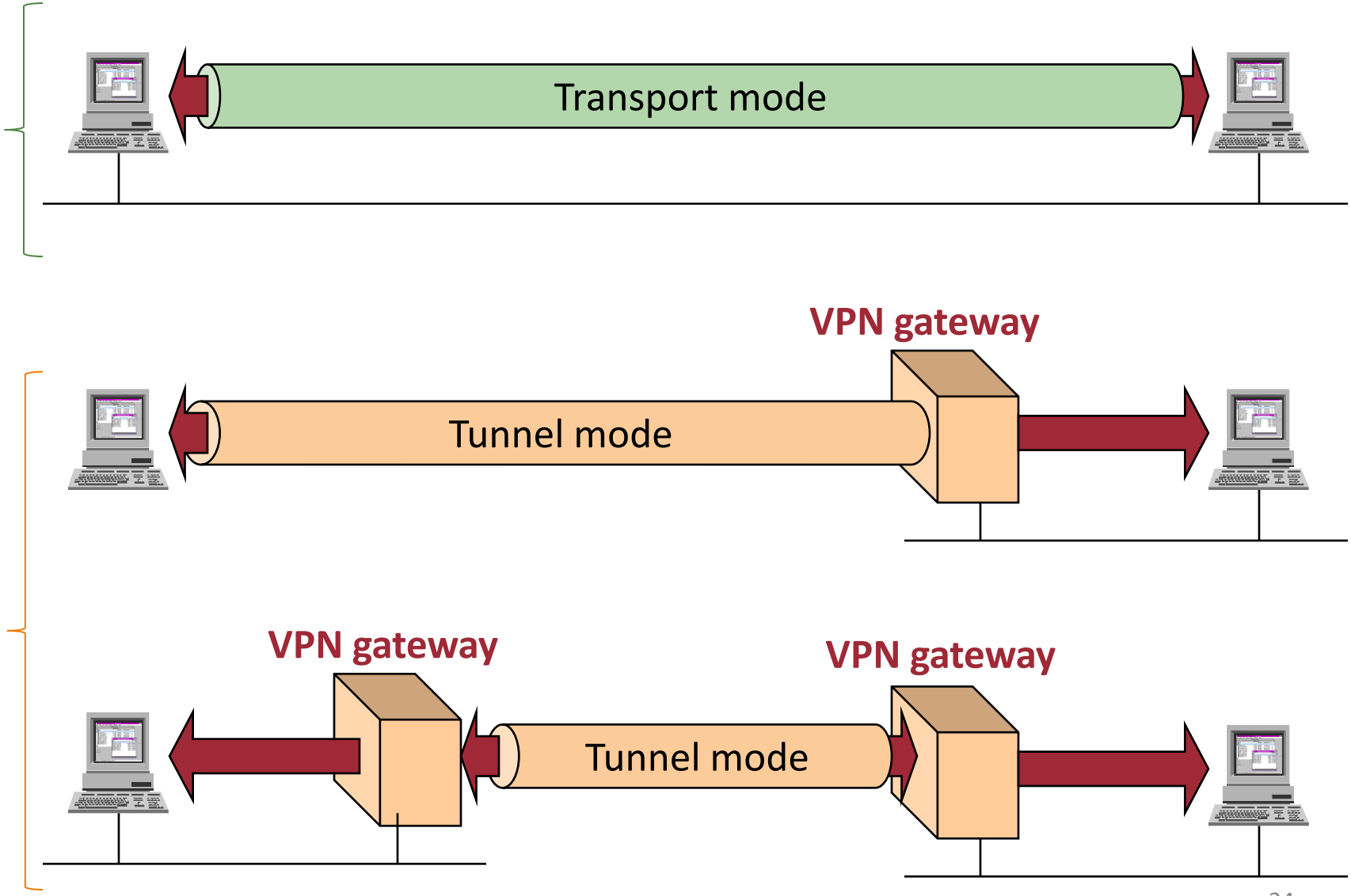


ESP provides source authentication, data integrity, freshness, and confidentiality

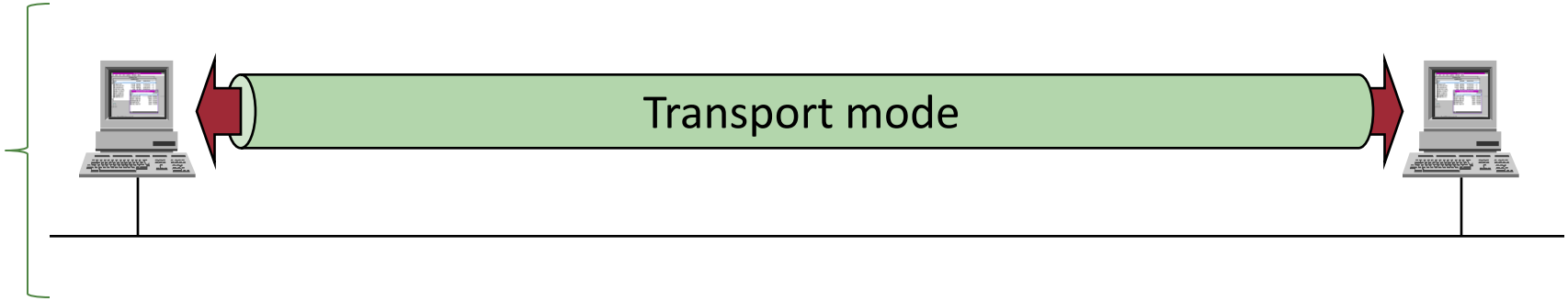
Tunnel mode



IPsec operational scenarios



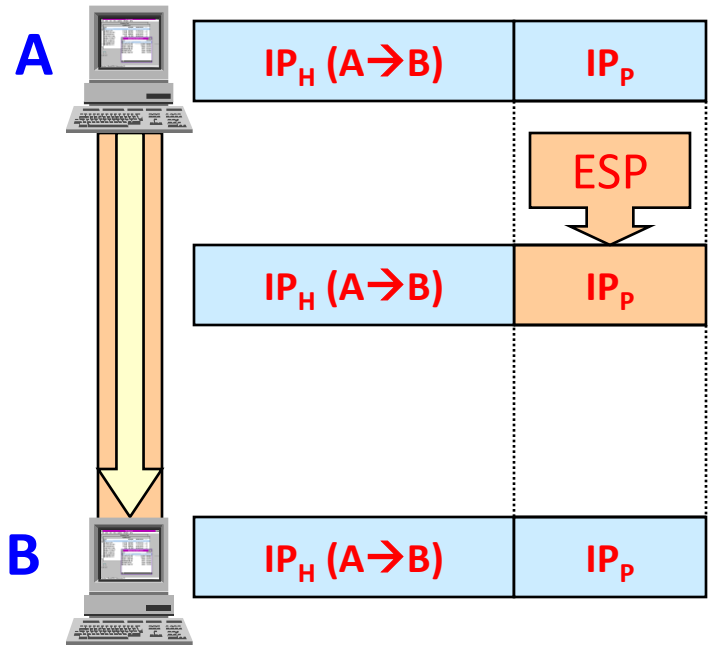
IPsec operational scenarios: host-to-host



ESP Transport Mode

- **Transport Mode**: the original IP header is used for routing
- ESP is deciphered by the destination host
  - Deciphers the ESP and reconstructs the original datagram
- ESP auth (MAC) is verified by the destination host
- SA in use is indexed by the SPI of the datagram

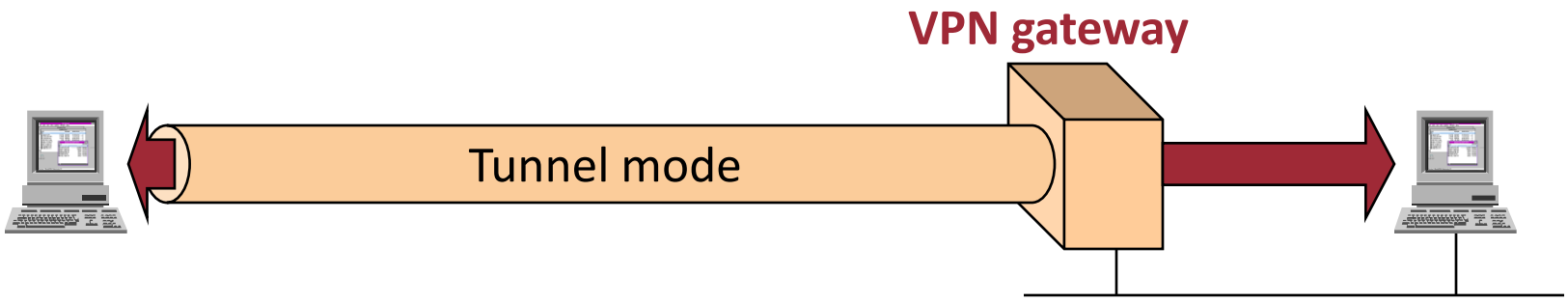
Host-to-host using ESP Transport Mode



IP_H – IP header
IP_P – IP payload

- **Host-to-host**
  - IPsec security exists between A and B
  - Both machines need to to know how to use IPsec
- Machine A and B take the initiative of using IPsec between them
  - Two SAs must exist between A and B

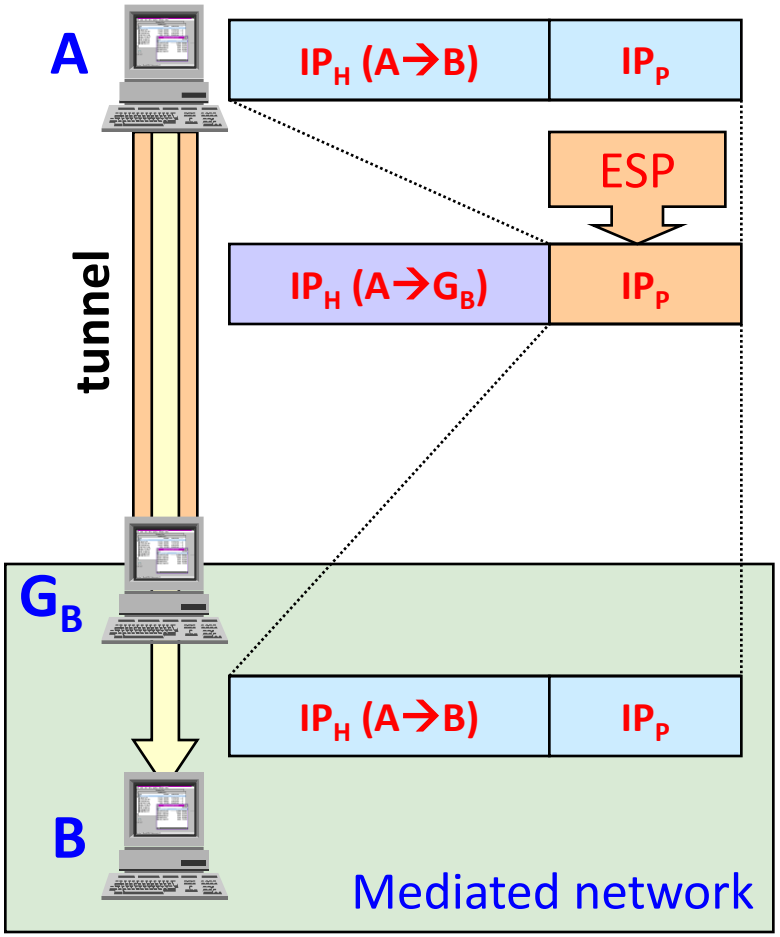
IPsec operational scenarios: host-to-net



ESP Tunnel Mode with gateway

- **Encapsulating Security Payload (ESP)** created with a **full IP datagram**
- Operation
  - Sender or gateway generates ESP with datagram addressed to machine B
  - The final datagram is sent to the gateway of B
    - Host IP addresses may be private
  - The ESP is deciphered; integrity is checked by the gateway of B, then sent to B
- Additional advantages
  - Conceals the real IP addresses from the intermediate nodes
- Disadvantages
  - Increases the IP packet size

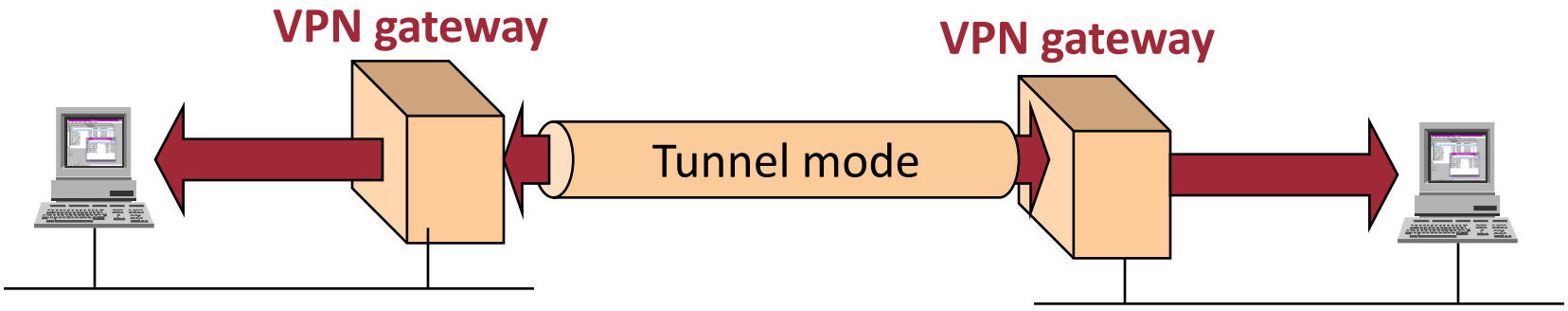
Host-to-net VPN using ESP Tunnel Mode



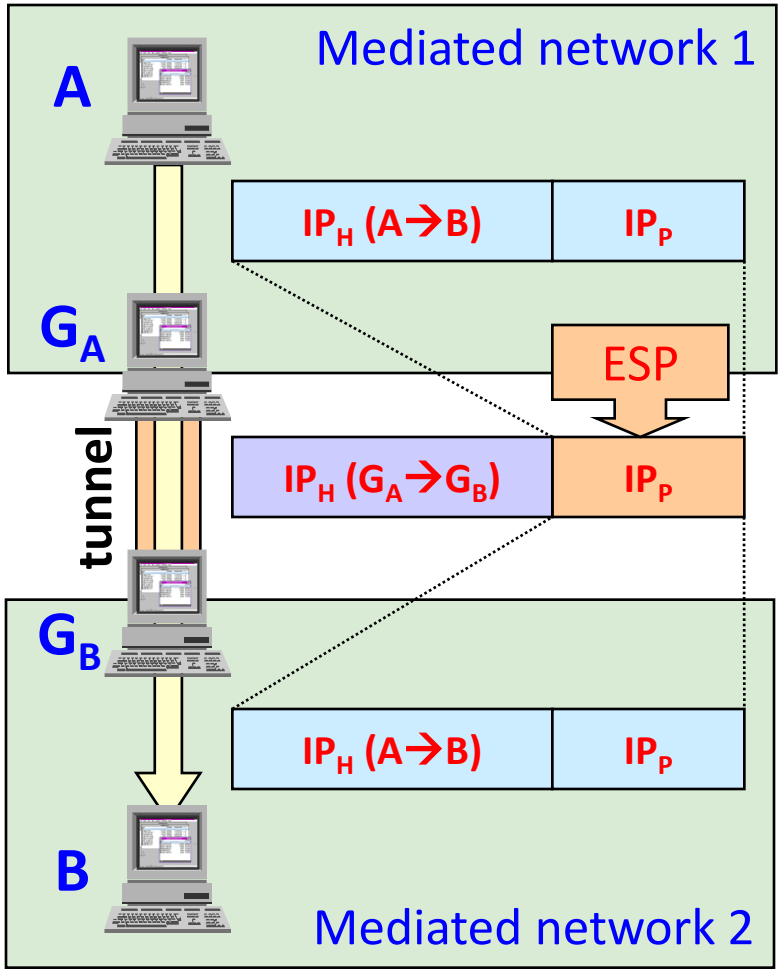
IP_H – IP header
IP_P – IP payload

- **Host-to-net VPN**
  - IPsec security exists between A and gateway G_B
  - Machine B does not need to know how to use IPsec
  - The address of B does not have to be public
- Host A and gateway G_B take the initiative of using IPsec tunneling between them
  - Two SAs must exist between A and G_B

IPsec operational scenarios: net-to-net



Net-to-net VPN using ESP Tunnel Mode



IP_H – IP header
IP_P – IP payload

- **Net-to-net VPN**
  - IPsec security exists between gateways G_A and G_B
  - Machines A and B do not need to know how to use IPsec
  - The IP addresses of A and B do not have to be public
- Gateways G_A and G_B take the initiative of using an IPsec tunnel between them
  - Two SAs must exist between them

IPsec limitations

- Performance
  - All the dataflow between two nodes is protected
    - Even if not needed
  - Tunneling size overhead
    - More headers, more processing
- Security quality
  - Some messages are more critical than others
    - Depending on the applications and the users
  - There may be need of assuring security at higher layers
    - Leading to a duplication of effort
- Key management
  - There is no unique key management protocol
    - The most common solution is manual distribution

Roadmap

- VPNs and tunneling
- **IPsec**
  - Main mechanisms
  - **Key distribution**

IPsec SA establishment (1/2)

- **Security Association (SA)**
  - Security policy, cryptographic mechanisms, and parameters used in the secure communication between a pair of machines
  - Security Parameter Index (SPI)
- Problem
  - How to create common SAs between a pair of machines?
  - Which is the SPI of those SAs?

IPsec SA establishment (2/2)

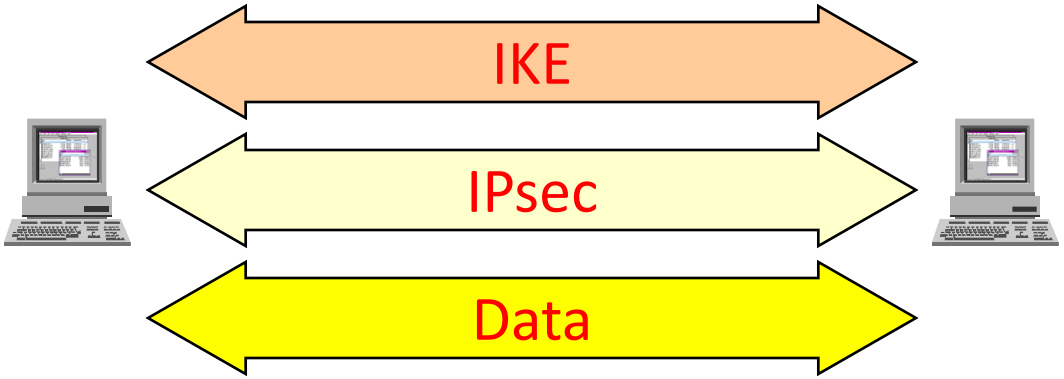
- Manual establishment
  - Manual configuration of the SAs
  - Manual attribution of SAs to IPs
- SA establishment with protocols
  - **ISAKMP** – framework
  - **IKE** – the standard protocol (IKEv2)

ISAKMP

- **ISAKMP** – Internet Security Association and Key Management Protocol
- Generic protocol (framework)
  - Allows the negotiation of keys and entity authentication
    - Does not specify any techniques
    - Only defines 5 types of information exchange
- It is an application layer protocol
  - Supports negotiations for several OSI layers
- There is only one protocol that uses it:
  - **IKE: Internet Key Exchange,** the standard for IPSEC
  - but can also be used with TLS

IKE operation

- IKE – Internet Key Exchange
- 1st phase: establishment of a bidirectional **IKE SA**
- 2nd phase: establishment of unidirectional **IPsec SAs**
  - Negotiation protected by the IKE SA
  - Several IPsec SAs can be established using the same IKE SA
- Data transmission secured by IPsec
  - Protected by unidirectional IPsec SAs



IKE negotiation modes

- Main mode (1st phase)
  - Establishment of a bidirectional IKE SA
  - Instance of the identity exchange of the ISAKMP
  - Ciphered identities (machine names)
    - The IKE SA can be negotiated by a third party rather than the machines using them
- Quick mode (2nd phase)
  - Establishment of two IPsec SAs
    - One for the outgoing data,
    - Another one for the incoming data (with its SPI)
  - Protected by an IKE SA
  - Generates a new key with DH (Diffie-Hellman) or refreshes the previous key

IKE: host authentication

- 1st Phase: two alternatives:
  - With **asymmetric cryptography**
    - DSA/RSA signatures and X.509 digital certificates
  - With a **shared secret**
    - Pre-shared key (PSK) – secret key, established manually
- 2nd Phase
  - With **shared secret** only
    - Uses secret established in the first phase

Roadmap

- IPsec
  - Main mechanisms
  - Key distribution
- **VPNs and tunneling**

Summary

- IPsec
  - Main mechanisms
  - Key distribution
- VPNs and tunneling