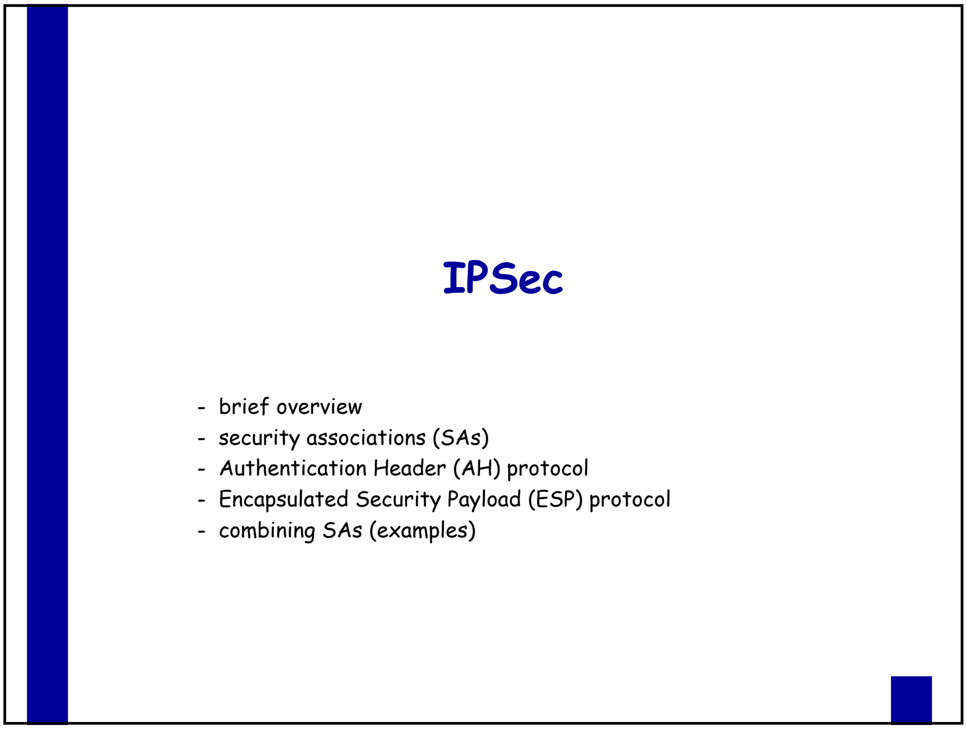
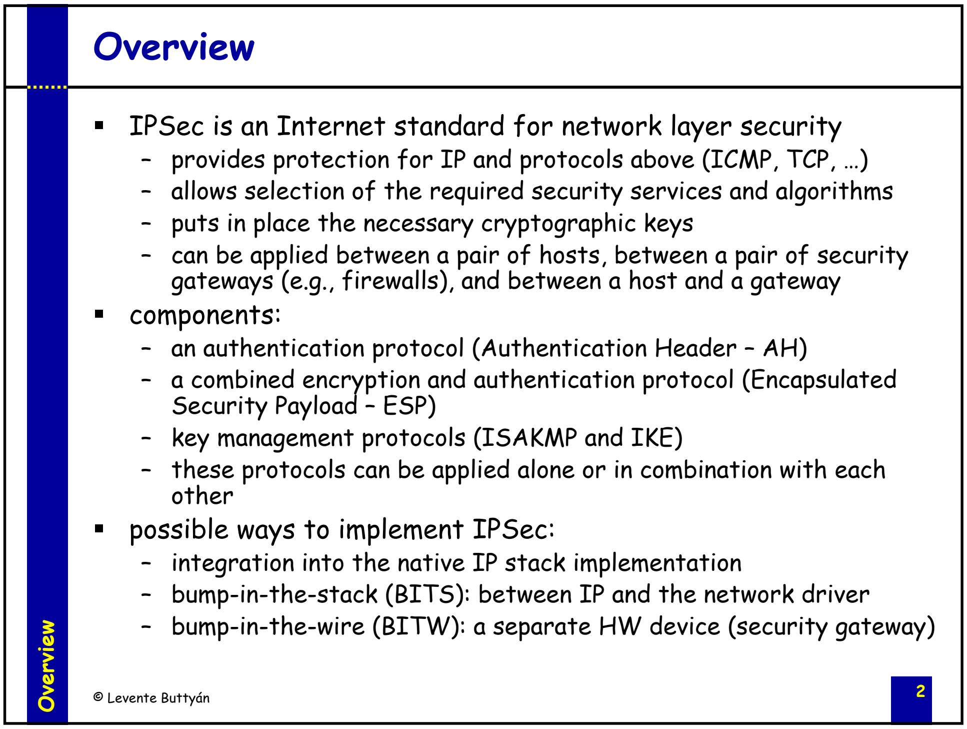


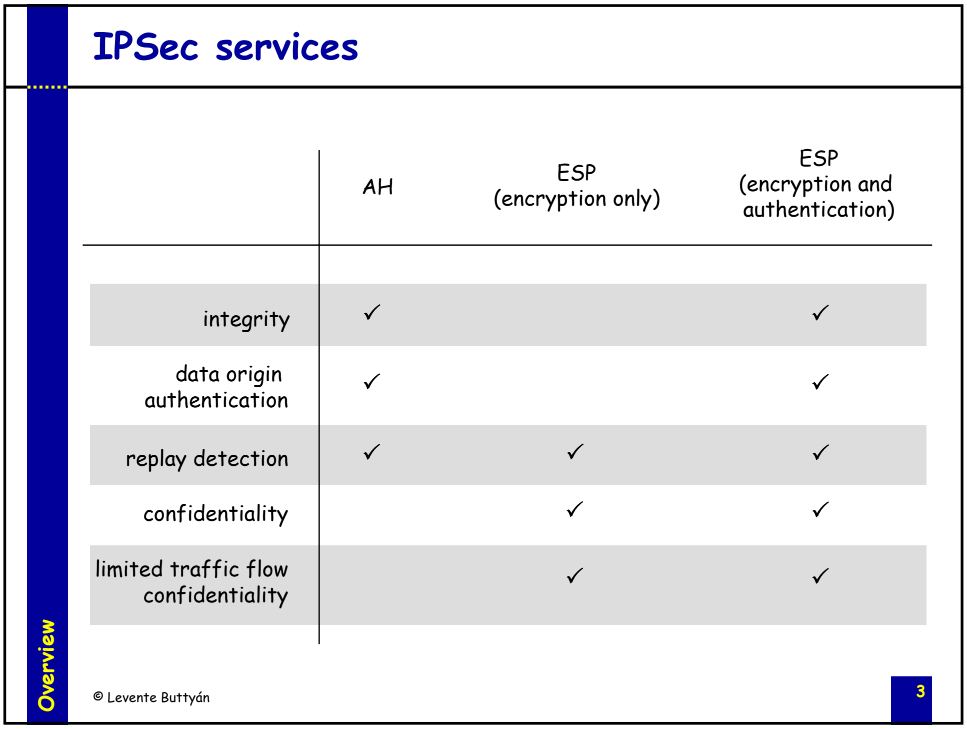
IPSec

- brief overview
- security associations (SAs)
- Authentication Header (AH) protocol
- Encapsulated Security Payload (ESP) protocol
- combining SAs (examples)



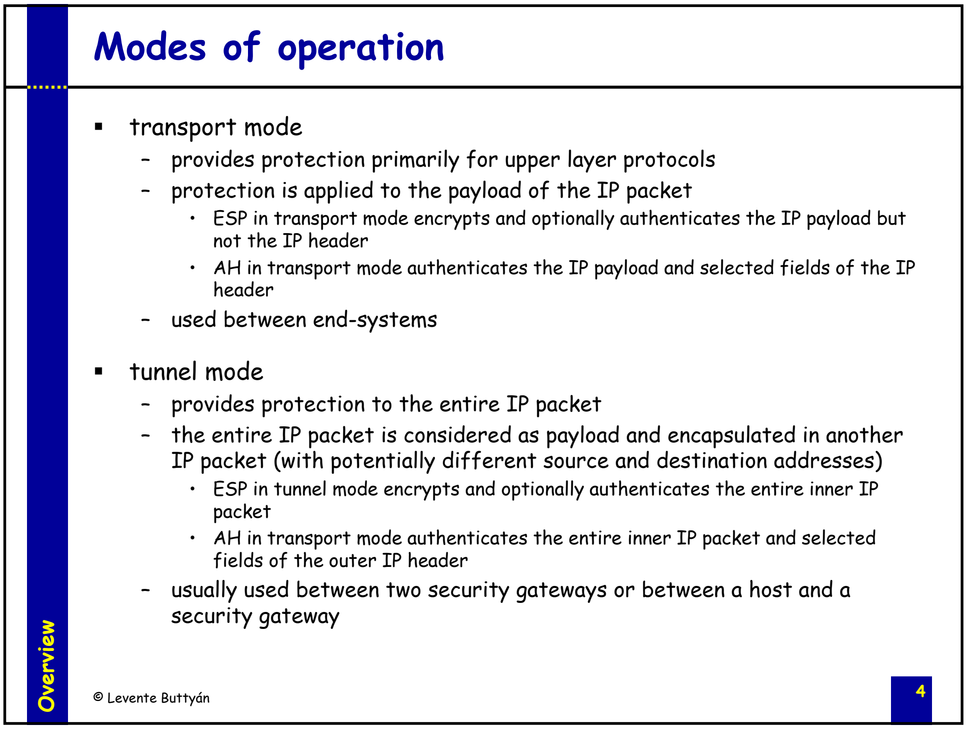
Overview

- IPSec is an Internet standard for network layer security
  - provides protection for IP and protocols above (ICMP, TCP, …)
  - allows selection of the required security services and algorithms
  - puts in place the necessary cryptographic keys
  - can be applied between a pair of hosts, between a pair of security gateways (e.g., firewalls), and between a host and a gateway
- components:
  - an authentication protocol (Authentication Header – AH)
  - a combined encryption and authentication protocol (Encapsulated Security Payload – ESP)
  - key management protocols (ISAKMP and IKE)
  - these protocols can be applied alone or in combination with each other
- possible ways to implement IPSec:
  - integration into the native IP stack implementation
  - bump-in-the-stack (BITS): between IP and the network driver
  - bump-in-the-wire (BITW): a separate HW device (security gateway)



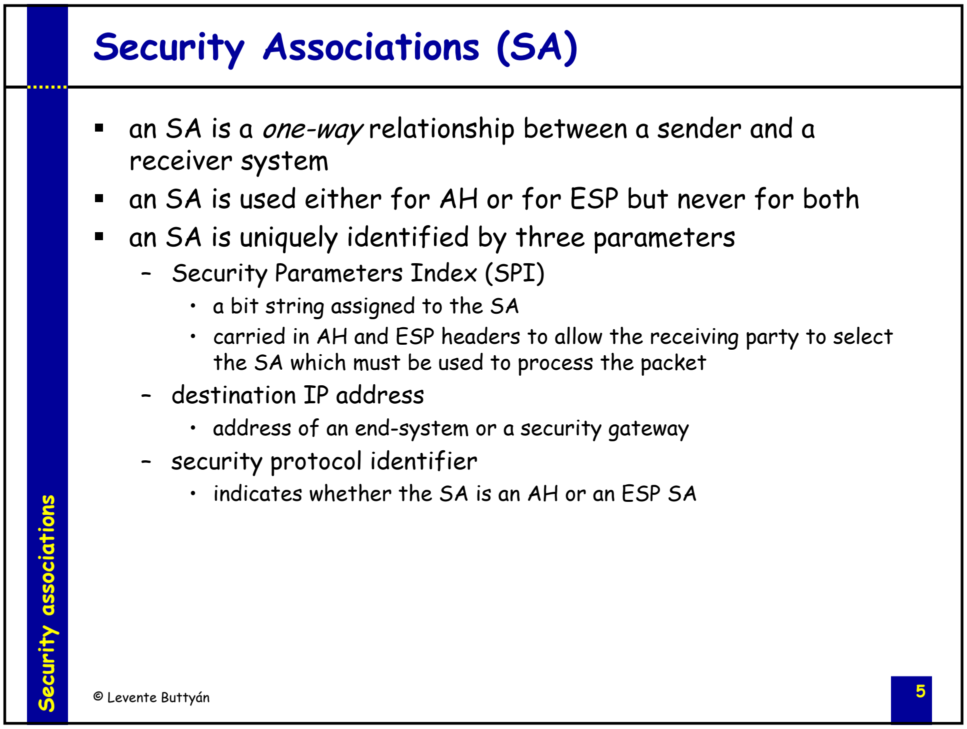
IPSec services

	AH	ESP (encryption only)	ESP (encryption and authentication)
integrity	✓		✓
data origin authentication	✓		✓
replay detection	✓	✓	✓
confidentiality		✓	✓
limited traffic flow confidentiality		✓	✓



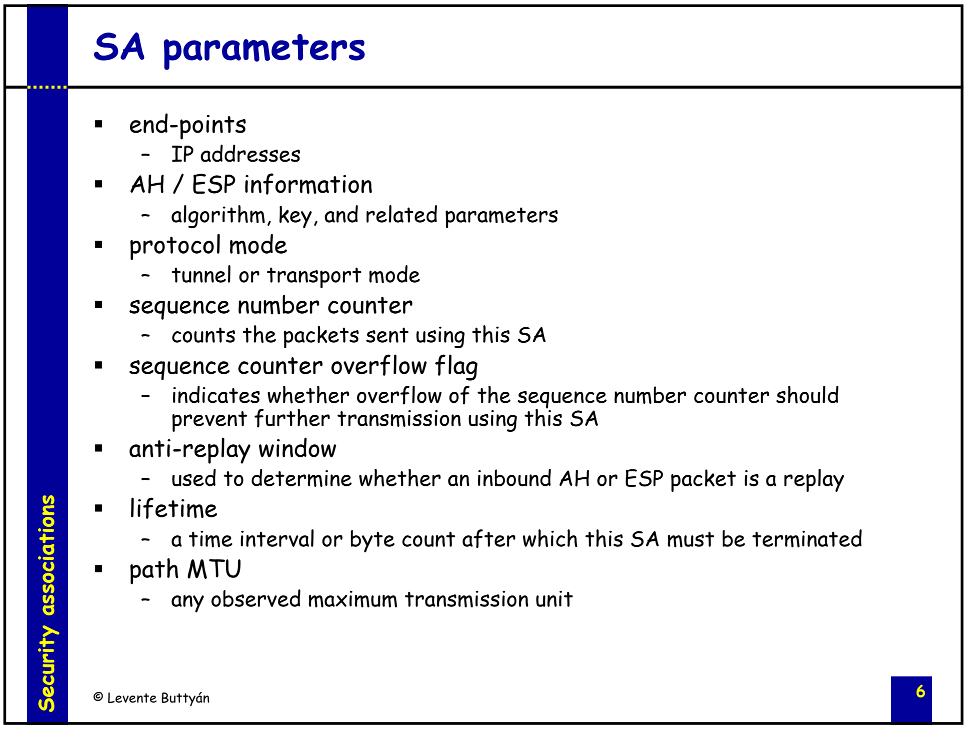
Modes of operation

- transport mode
  - provides protection primarily for upper layer protocols
  - protection is applied to the payload of the IP packet
    - ESP in transport mode encrypts and optionally authenticates the IP payload but not the IP header
    - AH in transport mode authenticates the IP payload and selected fields of the IP header
  - used between end-systems
- tunnel mode
  - provides protection to the entire IP packet
  - the entire IP packet is considered as payload and encapsulated in another IP packet (with potentially different source and destination addresses)
    - ESP in tunnel mode encrypts and optionally authenticates the entire inner IP packet
    - AH in transport mode authenticates the entire inner IP packet and selected fields of the outer IP header
  - usually used between two security gateways or between a host and a security gateway



Security Associations (SA)

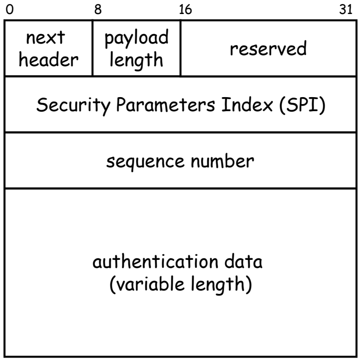
- an SA is a *one-way* relationship between a sender and a receiver system
- an SA is used either for AH or for ESP but never for both
- an SA is uniquely identified by three parameters
  - Security Parameters Index (SPI)
    - a bit string assigned to the SA
    - carried in AH and ESP headers to allow the receiving party to select the SA which must be used to process the packet
  - destination IP address
    - address of an end-system or a security gateway
  - security protocol identifier
    - indicates whether the SA is an AH or an ESP SA



SA parameters

- end-points
  - IP addresses
- AH / ESP information
  - algorithm, key, and related parameters
- protocol mode
  - tunnel or transport mode
- sequence number counter
  - counts the packets sent using this SA
- sequence counter overflow flag
  - indicates whether overflow of the sequence number counter should prevent further transmission using this SA
- anti-replay window
  - used to determine whether an inbound AH or ESP packet is a replay
- lifetime
  - a time interval or byte count after which this SA must be terminated
- path MTU
  - any observed maximum transmission unit

Authentication Header – AH



0 8 16 31

next header | payload length | reserved

Security Parameters Index (SPI)

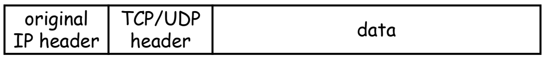
sequence number

authentication data (variable length)

- next header
  - type of header immediately following this header (e.g., TCP, IP, etc.)
- payload length
  - length of AH (in 32 bit words) minus 2
  - e.g., 4 if Authentication data is 3x32 bits long
- Security Parameters Index
  - identifies the SA used to generate this header
- sequence number
  - sequence number of the packet
- authentication data
  - a (truncated) MAC (default length is 3x32 bits)

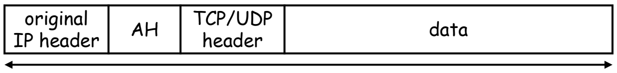
AH in transport and tunnel mode

original IPv4 packet



original IP header | TCP/UDP header | data

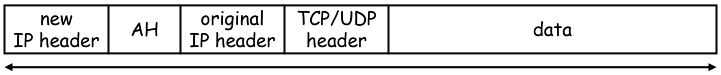
AH in transport mode



original IP header | AH | TCP/UDP header | data

authenticated except for mutable fields in the IP header

AH in tunnel mode

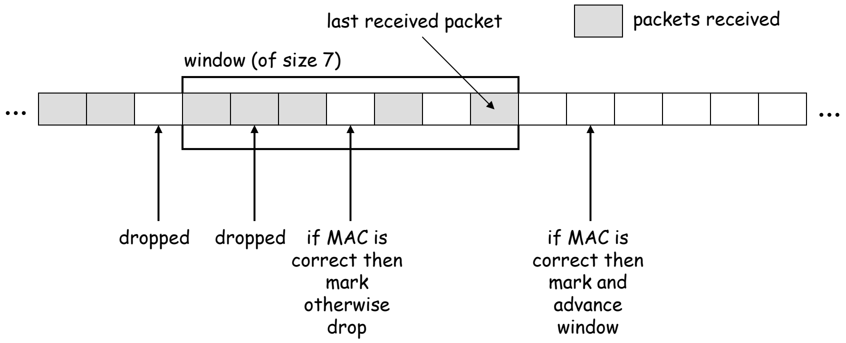


new IP header | AH | original IP header | TCP/UDP header | data

authenticated except for mutable fields in the outer IP header

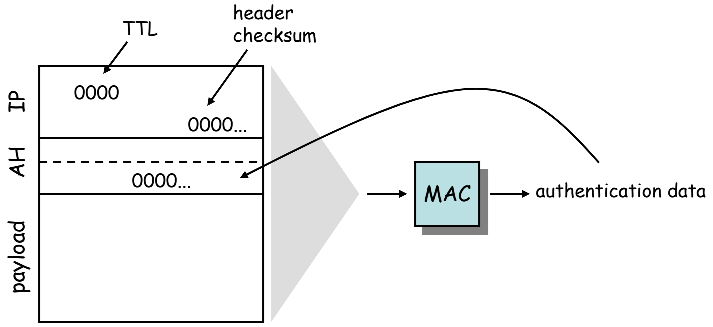
Replay detection

- replay: the attacker obtains an authenticated packet and later transmits (replays) it to the intended destination
- receiver has an anti-replay window of default size W = 64

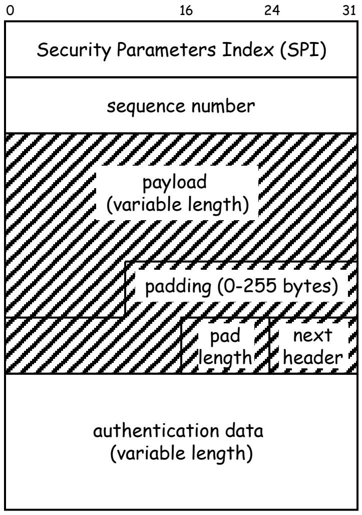

last received packet
packets received
window (of size 7)
…
…
dropped
dropped
if MAC is correct then mark otherwise drop
if MAC is correct then mark and advance window

MAC

- implementations must support
  - HMAC-MD5-96
  - HMAC-SHA1-96
- the MAC is calculated over
  - IP header fields that do not change in transit
  - the AH header fields (Authentication data field is set to 0)
  - entire upper layer protocol data
- the fields not covered by the MAC are set to 0 for the calculation



Encapsulating Security Payload – ESP



0 16 24 31

Security Parameters Index (SPI)

sequence number

payload (variable length)

padding (0-255 bytes)

pad length

next header

authentication data (variable length)

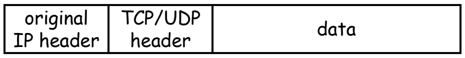
- Security Parameters Index
  - identifies the SA used to generate this encrypted packet
- sequence number
- payload
  - transport level segment (transfer mode) or encapsulated IP packet (tunnel mode)
- padding
  - variable length padding
- pad length
- next header
  - identifies the type of data contained in the payload
- authentication data
  - a (truncated) MAC computed over the ESP packet (SPI … next header)

Encryption and MAC algorithms

- encryption
  - applied to the payload, padding, pad length, and next header fields
  - if an IV is needed, then it is explicitly carried at the beginning of the payload data (the IV is not encrypted)
  - implementations must support DES-CBC
  - other suggested algorithms: 3DES, RC5, IDEA, 3IDEA, CAST, Blowfish
- MAC
  - default length is 3x32 bits
  - implementations must support HMAC-MD5-96 and HMAC-SHA1-96
  - MAC is computed over the SPI, sequence number, and encrypted payload, padding, pad length, and next header fields
  - unlike in AH, here the MAC does not cover the preceding IP header

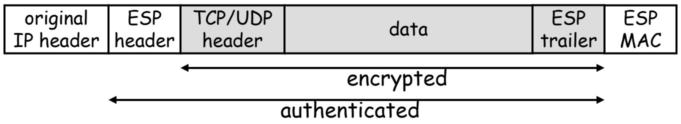
ESP in transport and tunnel mode

original IPv4 packet



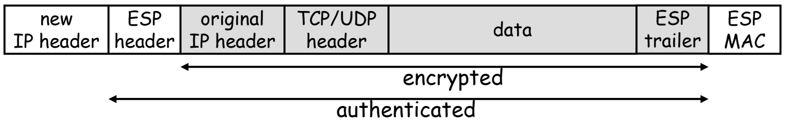
original IP header	TCP/UDP header	data

ESP in transport mode



original IP header	ESP header	TCP/UDP header	data	ESP trailer	ESP MAC

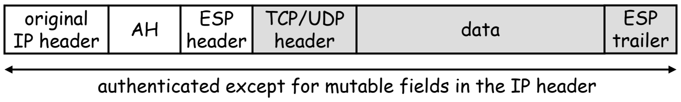
ESP in tunnel mode



new IP header	ESP header	original IP header	TCP/UDP header	data	ESP trailer	ESP MAC

Combining security associations

- transport adjacency (basic ESP-AH combination)
  1. apply ESP in transport mode without authentication
  2. apply AH in transport mode

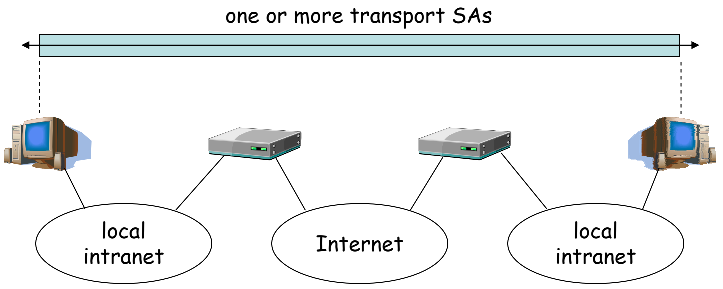


original IP header	AH	ESP header	TCP/UDP header	data	ESP trailer

- iterated tunneling (multiple nested tunnels)
  - both end-points of the two tunnels are the same (host-to-host)
  - one end-point of the two tunnels is the same (host-to-gateway)
  - neither endpoint of the two tunnels is the same (gateway-to-gateway)
- transport within tunnel

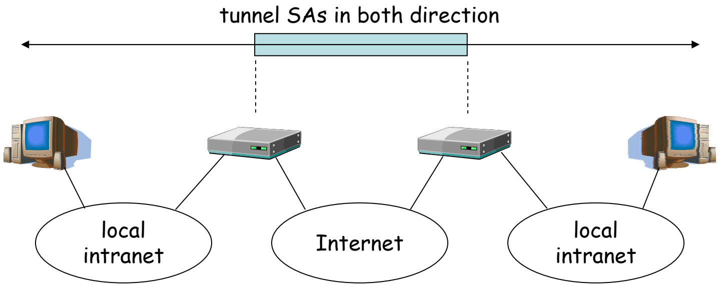
Examples

- host-to-host security with transport adjacency



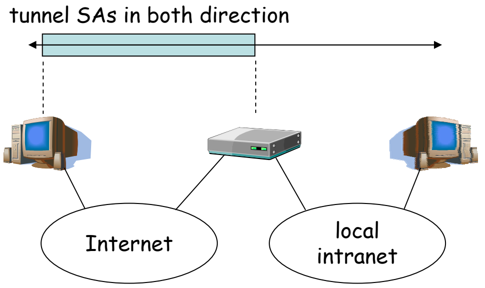
Examples

- a corporate VPN (virtual private network) with tunnel SAs



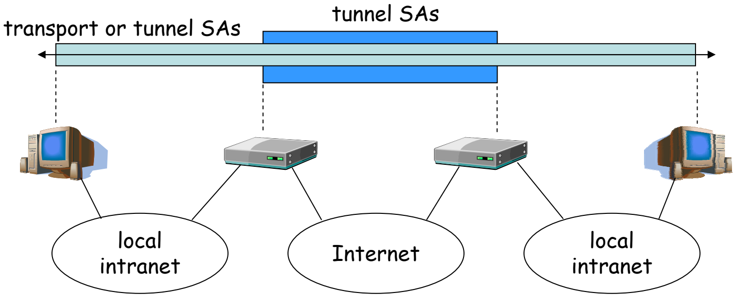
Examples

- remote access to a corporate network



Examples

- private connection within a corporate VPN



Recommended readings

- Internet RFCs:
  - **RFC 2401: an overview of the IPSec security architecture**
  - RFC 2402: specification of AH
  - RFC 2406: specification of ESP
  - RFC 2408: specification of ISAKMP
  - RFC 2409: specification of IKE