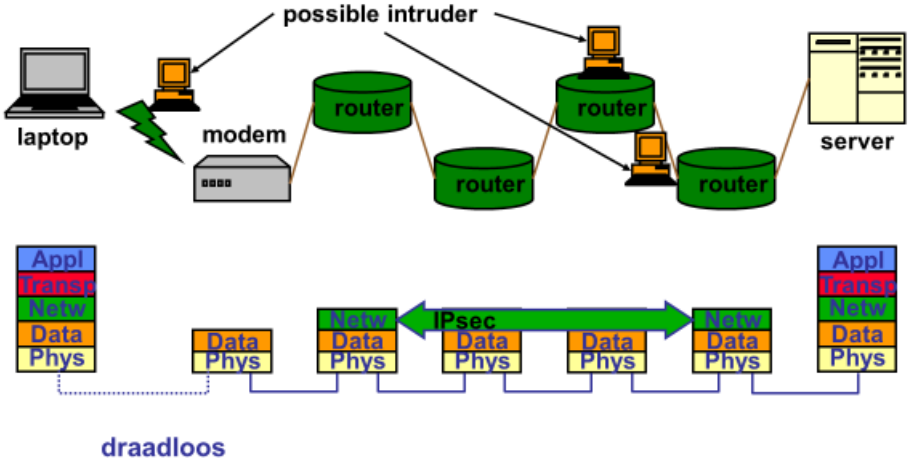
Overview

- Network model
- Secure configuration of devices
- Exchanging keys
- Secure networking protocols
  - Transport layer: TLS & SSL
  - **Network layer: IPSec & VPN**
  - Data link layer: WEP & WPA
- Firewalls

2

Network layer security



3

Network layer security

- IP security?
  - source spoofing
  - replay packets
  - no data integrity or confidentiality

  → DOS attacks, Replay attacks, Spying, and more...
- Routing applications
  - Authentication of routing messages
    - Advertisements
    - Updates
    - etc.
  - Without IPsec forged routing information could be sent
- IPsec
  - Secure IP connections
  - Application independent!

4

IPsec: applications

- LAN-to-LAN
  - VPN (virtual private network) for a company:
    - Behaves as if subnetworks were connected using an ordinary LAN (inaccessible to outer world) instead of a public network
    - Enabling secure communication over public networks between geographically disseminated company locations
- Client-to-LAN
  - Secure LAN access over the Internet
  - Remote access to a trusted source from an untrusted network
  - Often also called a VPN

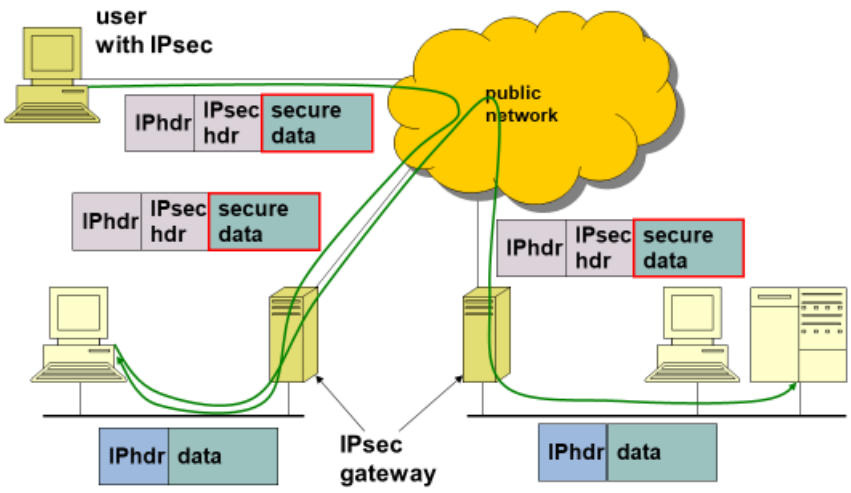
5

IPsec network level security

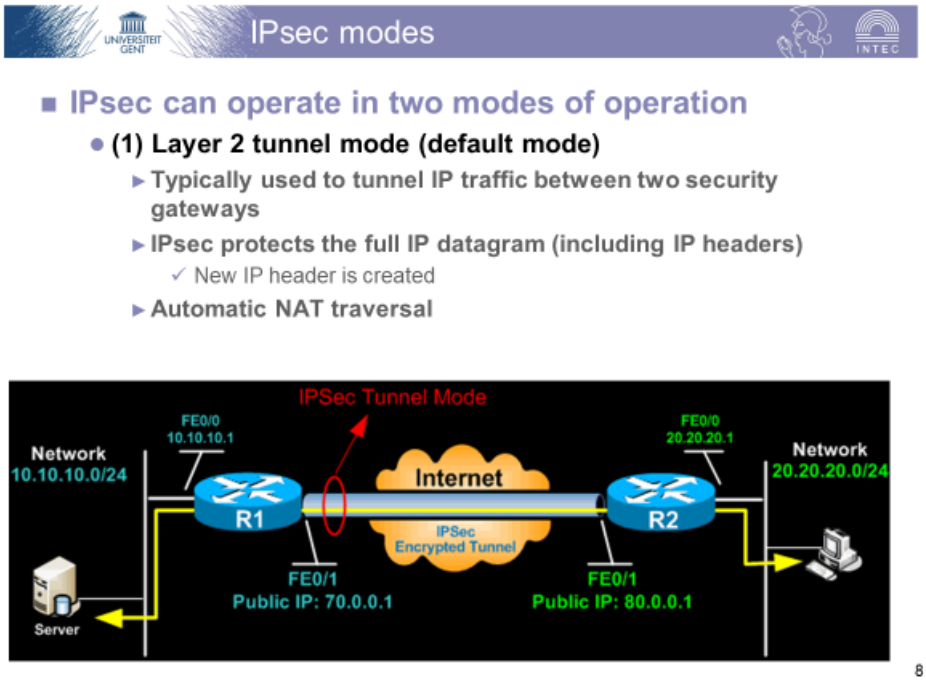
- **Advantages**
  - **Application independent**
    - Transparent for application layer
    - Provides security to applications that don't provide security themselves
  - **Security mechanisms limited to a few access points**
    - When implemented on firewall or router
    - Offers strong security for all traffic crossing perimeter, without burdening the internal traffic
  - **Possibly transparent to end users**
    - End users (almost) needn't worry about security services
  - **Individual user security is possible**
    - OK for teleworkers
- **Drawbacks**
  - **No message security beyond secure gateway**
    - E.g. at mail server
    - No secure storage
  - **Use of system resources**
    - Computation time required for cryptographic functions
  - **Complexity of specification**

6

IPsec: typical scenario



7

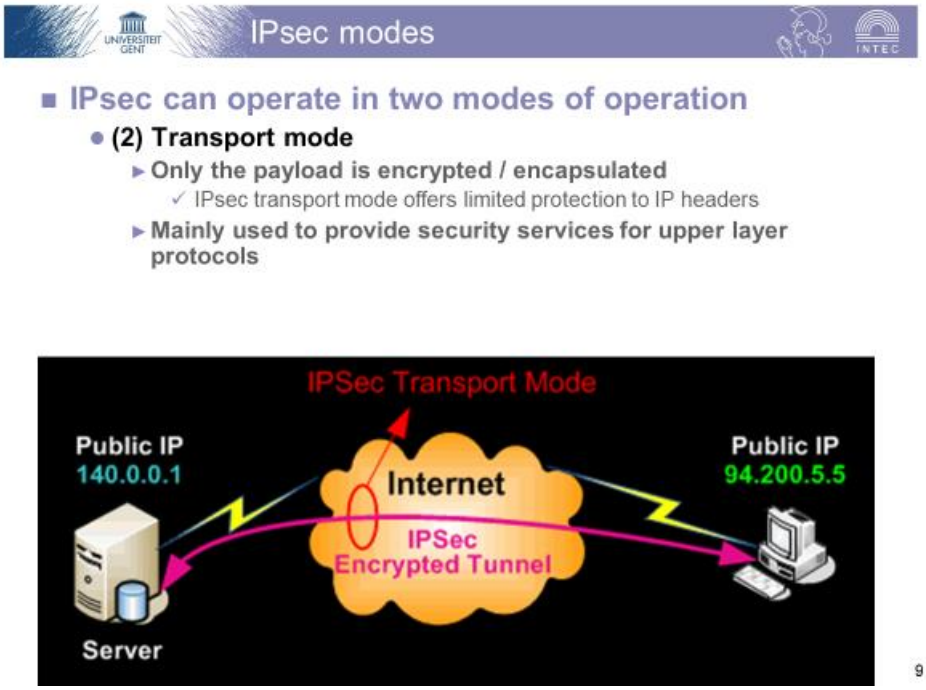


IPsec can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

Tunnel mode

IPSec tunnel mode is the **default mode**. The tunnel mode protects any internal routing info by encrypting the IP header of the ENTIRE packet. This means IPSec wraps the original packet, encrypts it, adds a new IP header and sends it to the other side of the VPN tunnel (IPSec peer). As such, the entire IP packet is encrypted and/or authenticated. Since additional headers are added to the packet there is less space available for payload.

Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat). NAT traversal is supported with the tunnel mode. In the example, the client connects to the IPSec Gateway. Traffic from the client is encrypted, encapsulated inside a new IP packet and sent to the other end. Once decrypted by the firewall appliance, the client's original IP packet is sent to the local network.



Transport mode

In transport mode, only the payload of the IP packet (and the ESP trailer) is usually encrypted and/or authenticated. The IP header of the original packet is neither modified nor encrypted, thus leaving the routing intact.
The transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers). Transport mode is implemented for client-to-site VPN scenarios.

IPSec Transport mode is most commonly used for end-to-end communications between devices with public IP addresses, for example for communication between a client and a server or between a workstation and a gateway (if the gateway is being treated as a host and is thus the actual destination). A good example would be an encrypted Telnet or Remote Desktop session from a workstation to a server. By default, NAT traversal **IS NOT** supported with the transport mode, but a means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

IPSec transport mode is also used when another tunneling protocol (like GRE) is used to first encapsulate the IP data packet, then IPSec is used to protect the GRE tunnel packets. IPSec protects the GRE tunnel traffic in transport mode.

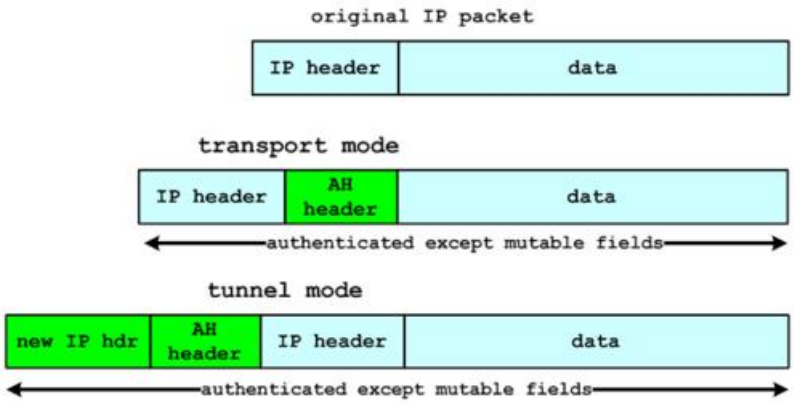
IPsec protocols: AH & ESP

- IPSec consists of two main protocols:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)
- Tunnel or transport mode can be implemented using the AH, ESP protocol or a combination of both
  - Both modes can provide data-integrity, authentication and/or confidentiality, depending on the choice of the protocols

10

IPsec : authentication header (AH)

- Authentication header
  - Used for both transport and tunnel modes



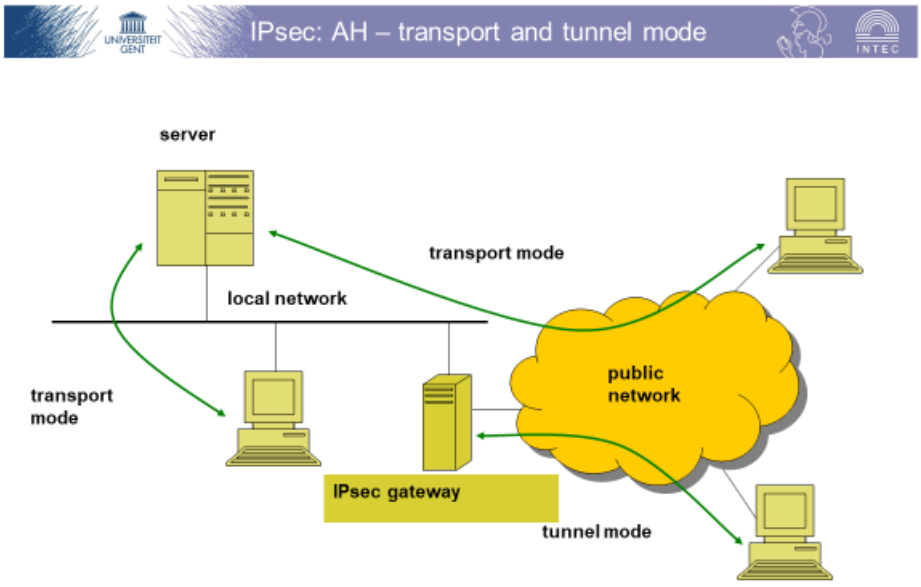
11

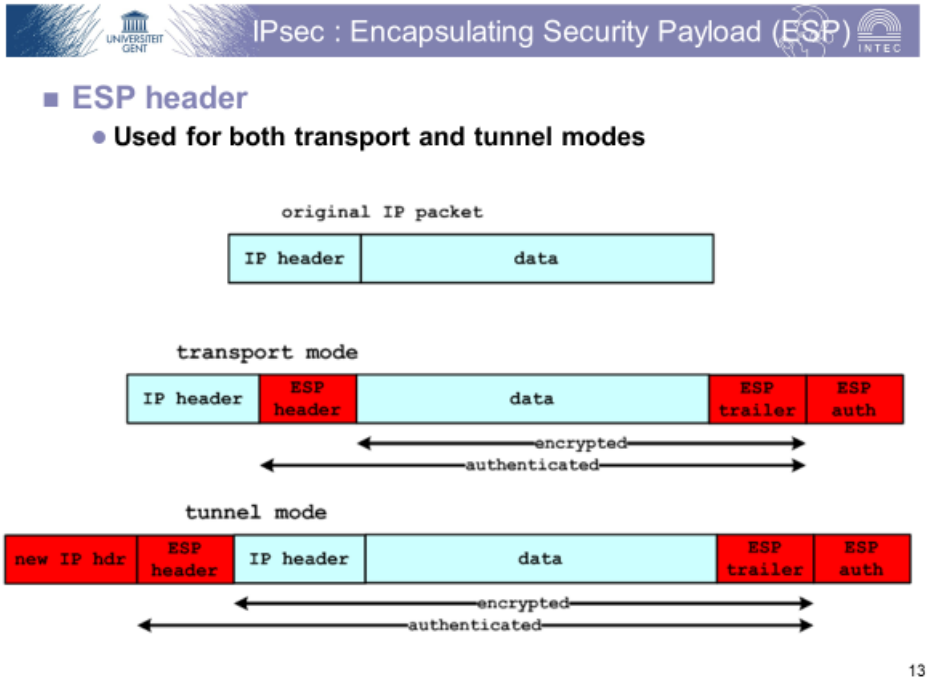
The *Authentication Header* (AH) [RFC2402] provides authentication and data integrity to the datagrams passed between two systems. This enables router/workstation to authenticate users or applications. The authentication prevents IP spoofing and implements an anti-replay mechanism.

Authentication and data integrity is achieved by applying a keyed one-way hash function to the datagram to create a MAC message digest (this requires a shared secret key). If any part of the datagram is changed during transit, this will be detected by the receiver when it performs the same one-way hash function on the datagram and compares the value of the message digest that the sender has supplied. The fact that the one-way hash also involves the use of a secret shared between the two systems means that authenticity can be guaranteed.

The AH function is applied to the entire datagram except for any mutable IP header fields that change in transit, such as Time To Live (TTL) fields that are modified by the routers along the transmission path. AH works as follows:

- The IP header and data payload is hashed.
- The hash is used to build a new AH header, which is appended to the original packet.
- The new packet is transmitted to the IPSec peer router.
- The peer router hashes the IP header and data payload, extracts the transmitted hash from the AH header, and compares the two hashes. The hashes must match exactly. If even one bit is changed in the transmitted packet, the hash output on the received packet will change and the AH header will not match.





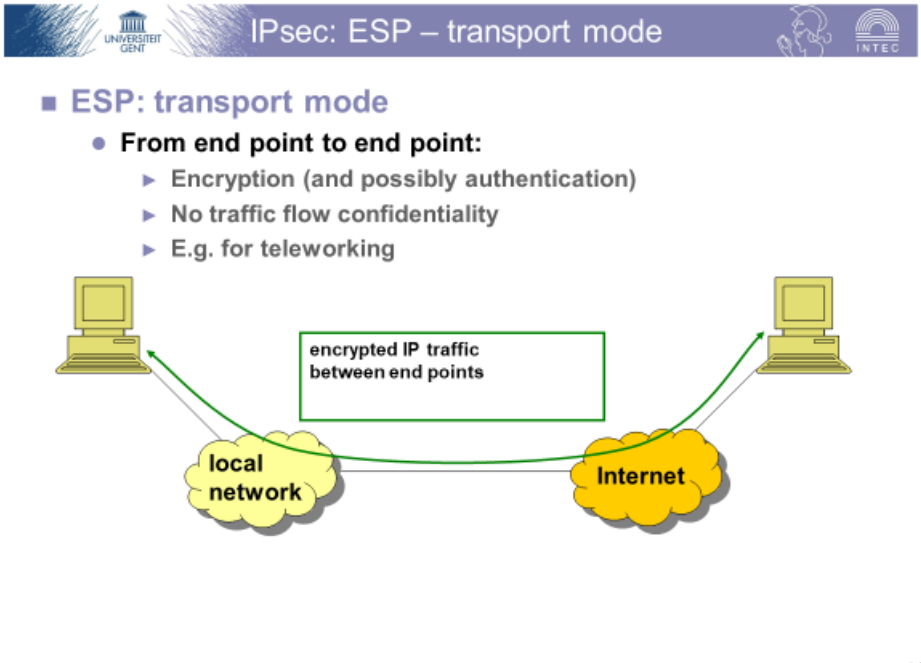
Encapsulating Security Payload (*ESP*) [RFC2406] is a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional anti-replay service, and limited traffic-flow confidentiality by defeating traffic-flow analysis. The data payload is encrypted with ESP.

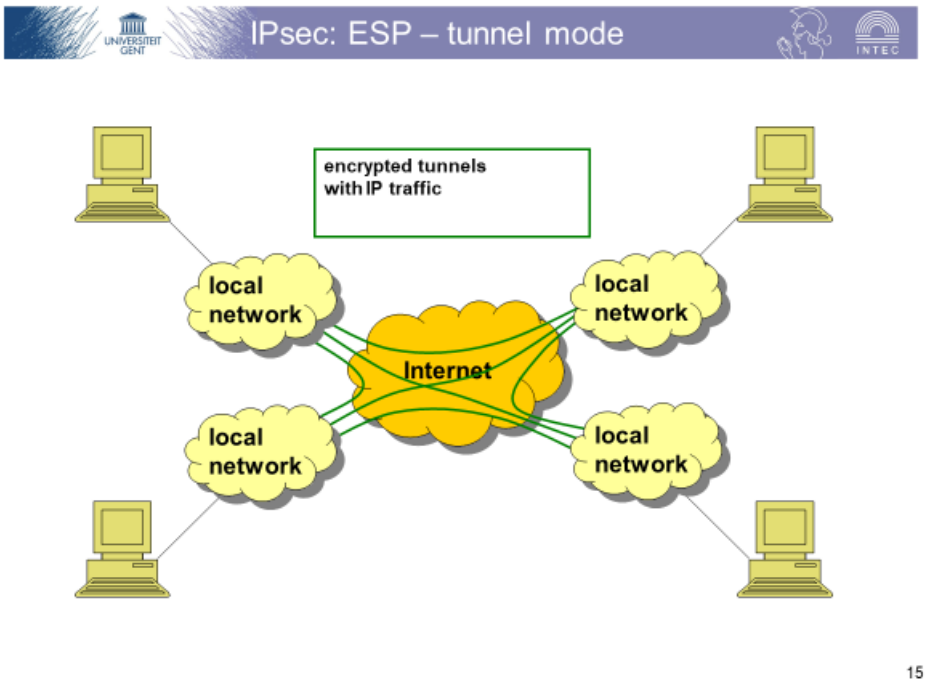
ESP ("Encapsulating Security Payload") achieves 2 security features:

(i) Confidentiality function. By encrypting the data and (optionally) IP header, confidentiality is guaranteed, and to some extent even traffic flow confidentiality is

realized. For this purpose, traditional encryption algorithms are used, such as AES-128-CBC (MUST), AES-GCM , DES (obsolete)

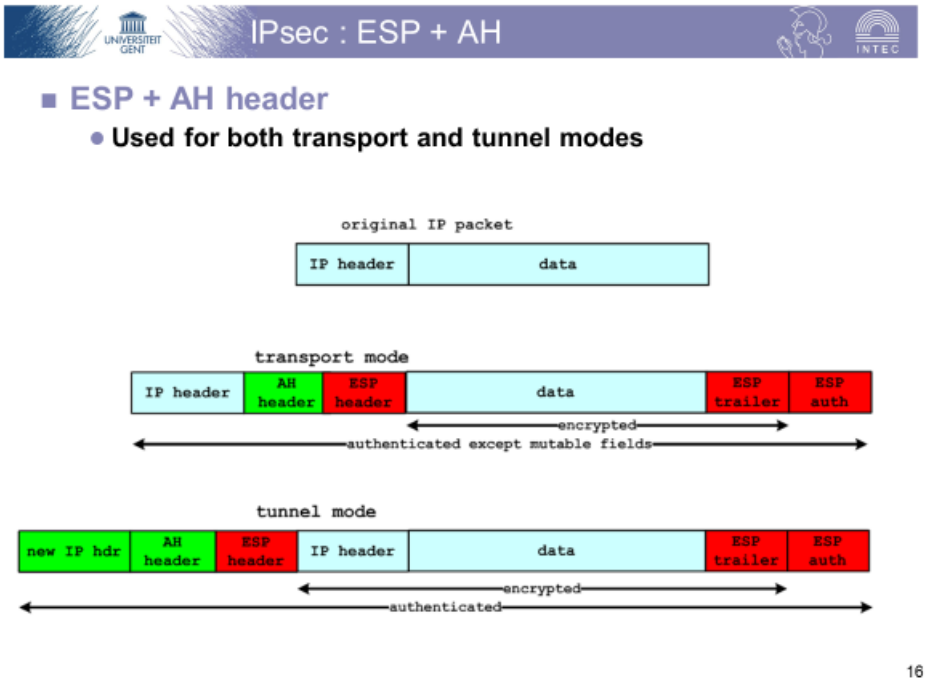
(ii) (Optional) authentication. Using the same principles as for AH. Algorithms used include HMAC-SHA-1-96, AES-GMAC and "optional" support for other MACs.





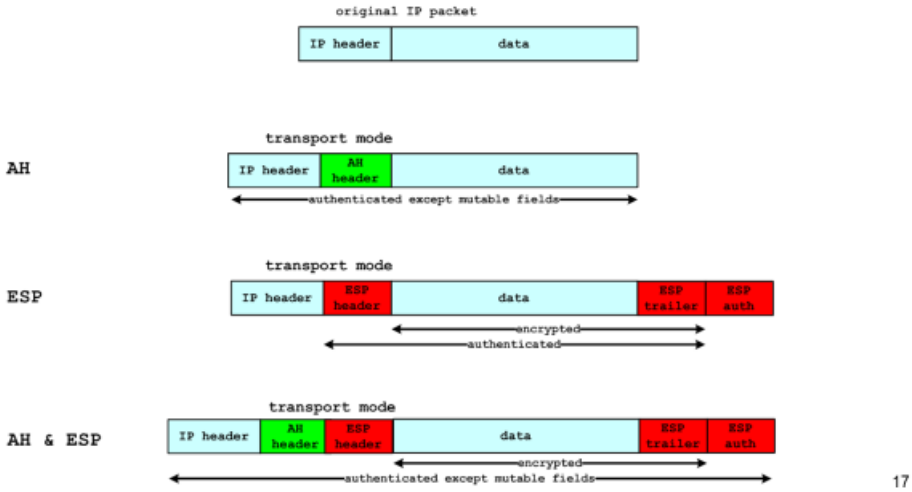
The tunnel mode can prove useful if we want to create a VPN between different locations of a company. Not every single connected device requires IPSec capabilities. Only a

security gateway, which connects the (reputedly safe) local network to the Internet, requires IPSec capabilities. In this case, the local traffic will not use IPSec, while outgoing traffic (to some other company location) will be encrypted by the security gateway. In this way, possibly confidential data will be transmitted securely over the Internet from one location to another. This configuration allows some traffic flow confidentiality, as an attacker outside one of the local networks can only observe between which local networks the traffic is flowing, but not between which workstations precisely. In practice, the security gateway will also contain a firewall to achieve other security services.



IPsec transport mode

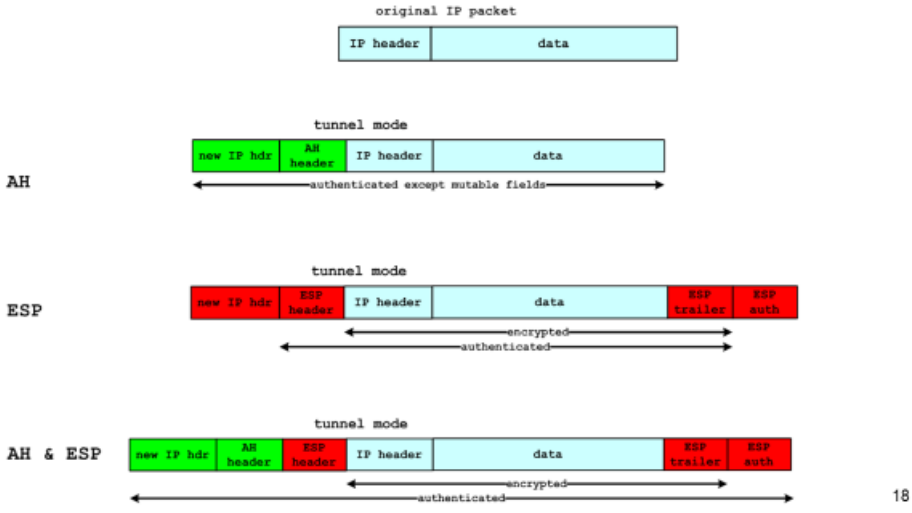
- **IPsec transport mode summary**
  - **Different AH, ESP or AH+ESP combinations**



17

IPsec tunnel mode

- **IPsec tunnel mode summary**
  - **Different AH, ESP or AH+ESP combinations**



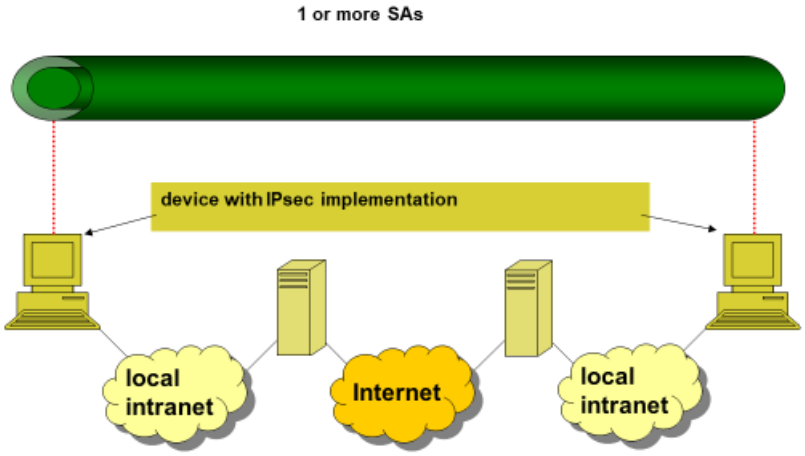
18

IPsec: security associations

- **Security associations (SA)**
  - **One-way relationship between sender and receiver**
    - Provides security services to traffic carried
    - Two associations needed for bidirectional traffic
  - **Identified by**
    - SPI ("Security Parameters Index")
    - IP destination address (end user, firewall, router, etc.)
    - Security protocol identification (AH or ESP)
    - Obvious bundle: AH + ESP for single IP stream
- **Combining tunnels**
  - **Not necessarily identical end points for each tunnel**
  - **Several levels possible**
  - **"Iterated tunneling"**

19

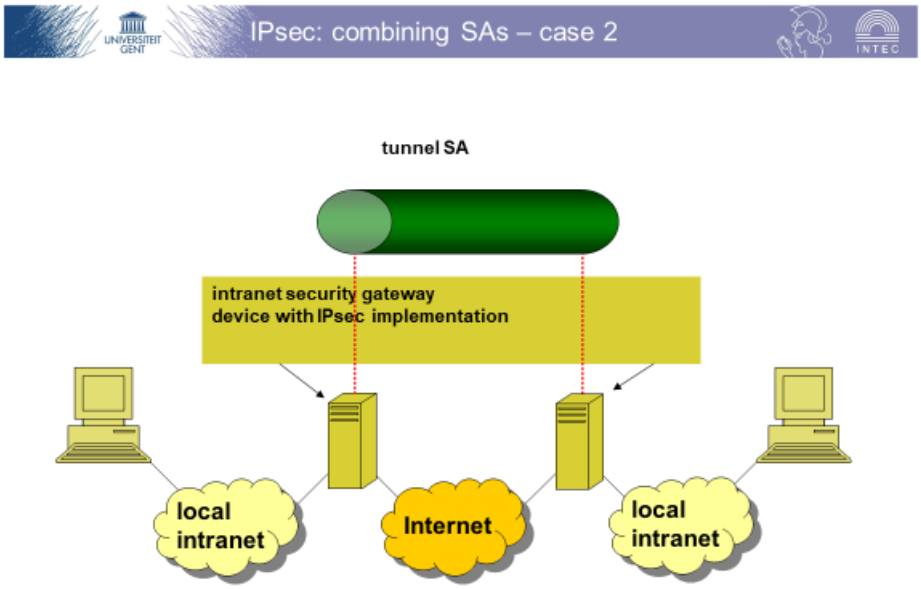
IPsec: combining SAs – case 1



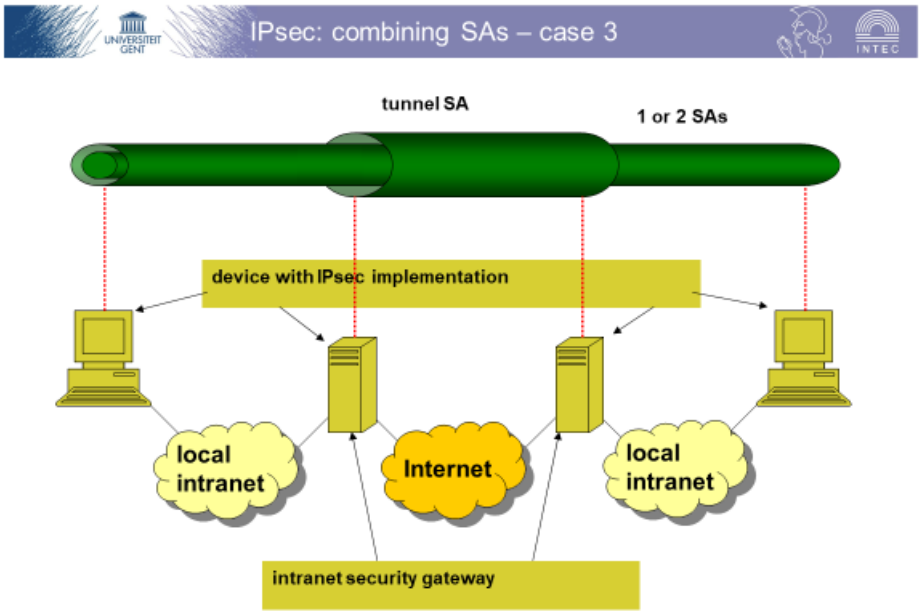
20

Security between two end points. Possible combinations:

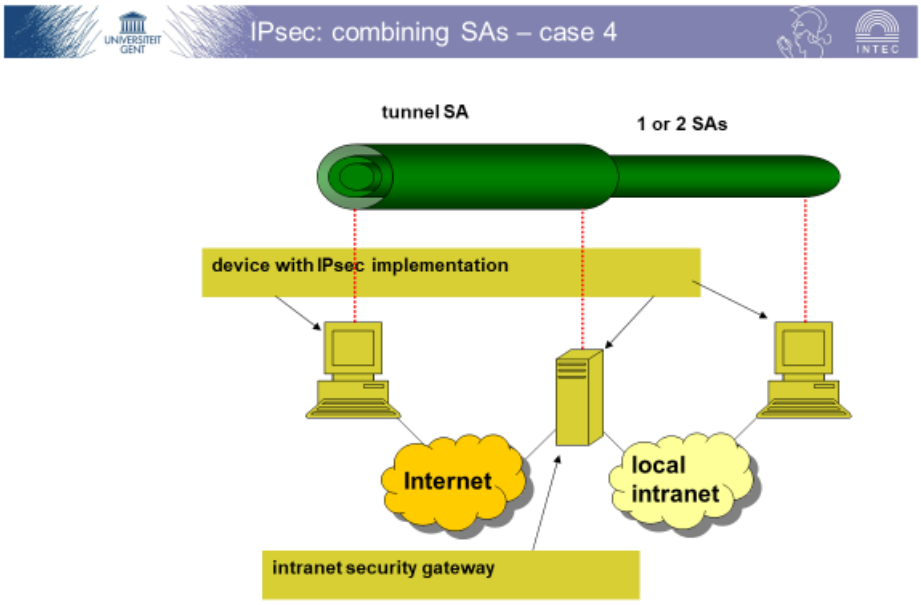
- AH in transport mode
- ESP in transport mode
- AH, followed by ESP in transport mode (an ESP SA within an AH SA)
- one of the previous within an AH or ESP in tunnel mode



Traffic secured between gateways (routers, firewall, etc.). No IPsec implementation at end users. Basic support for VPN. IPsec specifies that a single tunnel (with AH, ESP, or ESP with authentication) is sufficient in this case. Nested tunnels aren't required as the IPsec service applies to the entire original packet.



Extension of case 2, offering security between the end points too. The tunnel offers authentication and/or confidentiality for traffic between intranets. Additional IPSec security may be added by the end users for the traffic within the local intranets.



This is the scenario for an external user (e.g. teleworker) using the Internet to access the security gateway of the company (secured by the tunnel SA) and further on a server or workstation within the company (internal communication secured by the internal SAs).

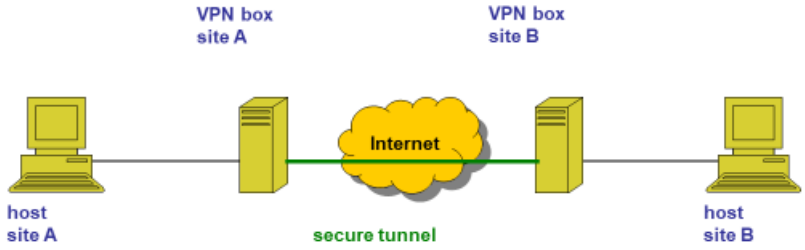
Overview

- Network model
- Secure configuration of devices
- Exchanging keys
- Secure networking protocols
  - Transport layer: TLS & SSL
  - **Network layer: IPSec & VPN**
  - Data link layer: WEB & WPA
- Firewalls

24

VPNs

- Basic principle of VPN
  - **VPN = secure tunnel from site to site**
    - Not just secure remote login



25

VPNs

- Options
  - **IPsec**
  - **PPTP**
    - Point-to-Point Tunneling Protocol (Microsoft specific)
  - **L2TP**
    - Layer 2 Tunneling Protocol (Microsoft + CISCO)
  - **SSL/TLS**
  - **SSH**
  - **SSTP**
    - Secure Socket Tunneling Protocol
    - Windows only
  - **....**

26

VPN: IPsec

- Advantages
  - **Designed for this purpose**
  - **Part of several other solutions**
- Disadvantages
  - **Complexity of IPsec**
    - **Especially key exchange (using IKE)**
  - **Interoperability issues between different (partial) implementations of the standard**
  - **Issues with NAT and (non-IPsec) firewalls**
    - **Mainly for AH**

27

VPN: PPTP

- Point-to-Point Tunneling Protocol
- Advantages
  - Client built-in to just about all platforms
  - Very easy to set up
  - Fast
- Disadvantages
  - Not at all secure (the vulnerable MS CHAPv2 authentication is still the most common in use)
  - Definitely compromised by the NSA

28

VPN: openVPN

- Build on the OpenSSL library using the SSL/TLS protocols
- Advantages
  - Highly configurable
  - Very secure (probably even against the NSA)
  - Can bypass firewalls
  - Can use a wide range of encryption algorithms
  - Open source (and can therefore be readily vetted for back doors and other NSA style tampering)
- Disadvantages
  - Needs third party software
  - Can be fiddly to set up
  - Support on mobile devices is improving, but is not as good as on the desktop
  - Security on top of transport layer
    - Instead of network layer security

29

VPN: L2TP and L2TP/IPsec

- Layer 2 Tunnel Protocol (L2TP)
  - On its own no encryption or confidentiality
  - Therefore combines with IPsec
- Advantages
  - Usually considered very secure
  - Easy to set up
  - Available on all modern platforms
- Disadvantages
  - May be compromised by the NSA
  - Likely deliberately weakened by the NSA
  - Slower than OpenVPN
  - Can struggle with restrictive firewalls

30

Test yourself

- Give 5 examples of security problems that can be solved by IPsec but not by TLS or SSH
- Which of the following security services can be achieved with IPsec: access control, integrity, authentication, confidentiality (which types)?
- Which IPsec protocols provide traffic flow confidentiality? Why is this only a limited form of confidentiality?

31