
# Cryptography and Network Security



## Chapter 8

# IP Security



*Lectured by*
**Nguyễn Đức Thái**

# Outline

- IP Security Overview
- IP Security Policy
- Encapsulating Security Payload (ESP)
- Combining Security Associations
- Internet Key Exchange (IKE)
- Cryptographic Suits

# Key Points (1/2)

- IP security (IPsec) is a ***capability*** that ***can be added*** to either current version of the Internet Protocol (IPv4 or IPv6) by means of additional headers.
- **IPsec** encompasses three functional areas:
  - authentication,
  - confidentiality, and
  - key management.

# Key Points (2/2)

- ***Authentication*** makes use of the HMAC message authentication code.
- Authentication can be applied to the ***entire original IP packet*** (tunnel mode) or to all of the packet except for the IP header (transport mode).
- ***Confidentiality*** is provided by an encryption format known as encapsulating security payload. Both tunnel and transport modes can be accommodated.
- IKE defines a ***number of techniques*** for key management.

# IP Security Overview (1/2)

- In **1994**, the Internet Architecture Board (IAB) issued a report titled "Security in the Internet Architecture" (RFC 1636).
- The report identified ***key areas*** for security mechanisms.
- Among these were the need to ***secure the network infrastructure*** from ***unauthorized monitoring*** and ***control of network traffic*** and the need to secure end-user-to-end-user traffic using authentication and encryption mechanisms

# IP Security Overview (2/2)

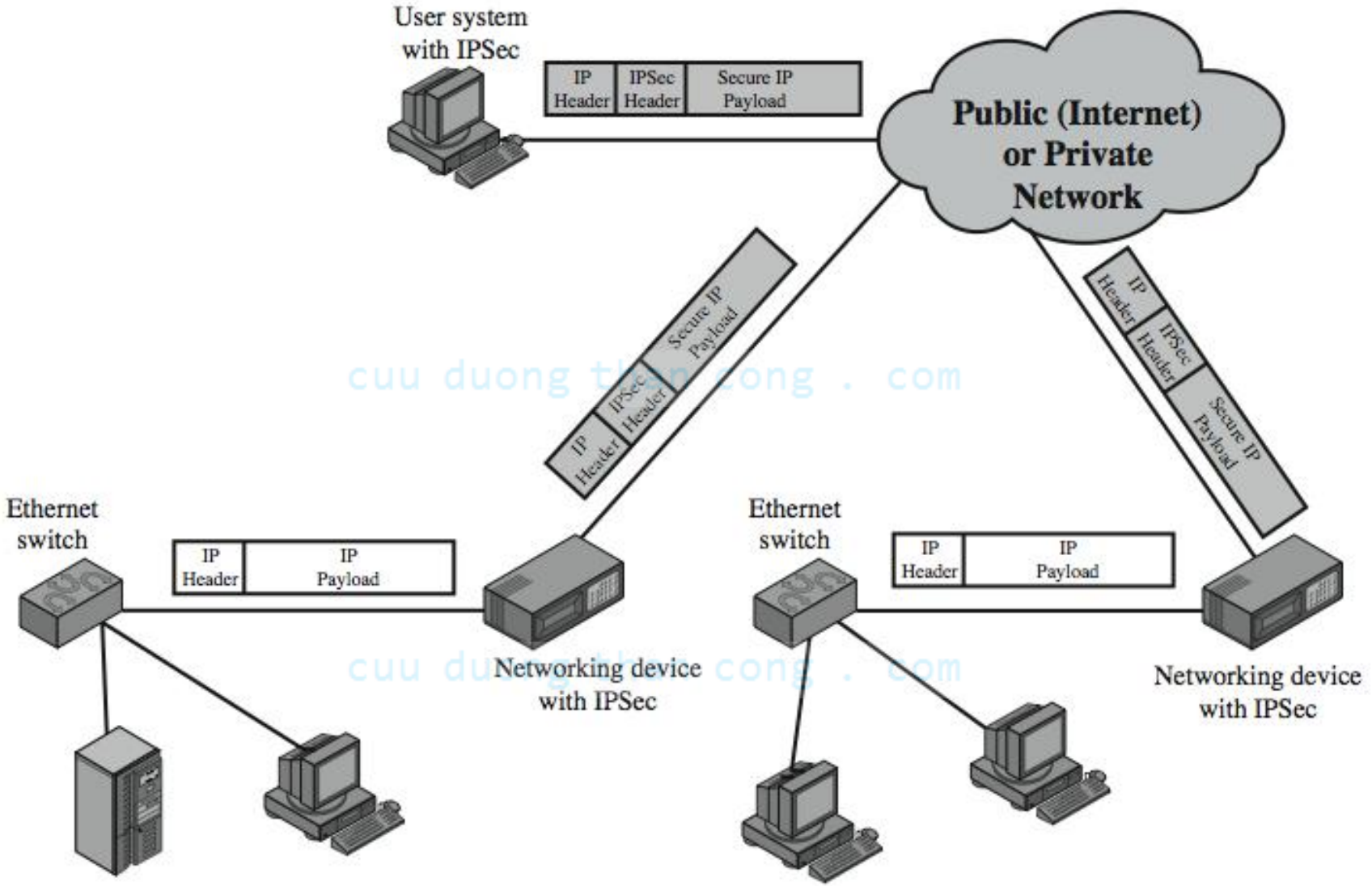
- To provide security, the IAB included ***authentication*** and ***encryption*** as necessary security features in the next-generation IP, which has been issued as IPv6
- Fortunately, these security capabilities were designed to be usable both with the current IPv4 and the future IPv6.
- This means that vendors can begin offering these features now, and many vendors now do have some ***IPsec capability*** in their products.
- The IPsec specification now exists as a set of Internet standards.

# Applications of IPsec

- IPsec provides the capability to ***secure communications*** across a ***LAN***, across private and public ***WANs***, and across the ***Internet***. Examples of its use include:
  - Secure branch office connectivity over the Internet.
  - Secure remote access over the Internet
  - Establishing extranet and intranet connectivity with partners
  - Enhancing electronic commerce security


cuu duong than cong . com

# An IP Security Scenario



# Benefits of IPsec

- In a firewall or router, it provides ***strong security*** that can be applied to all traffic crossing the perimeter.
- IPsec in a firewall is ***resistant*** to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.
- IPsec is ***below*** the transport layer (TCP, UDP) and so is ***transparent*** to applications.
- IPsec can be transparent ***to end users***.
- IPsec can provide security for ***individual users***

# Routing Applications

**IPsec can assure that**

- A router advertisement (a new router advertises its presence) comes ***from an authorized router***.
- A neighbor advertisement (a router seeks to establish or maintain a neighbor relationship with a router in another routing domain) ***comes from an authorized router***.
- A redirect message comes from the router to which the initial IP packet was sent.
- A routing update is ***not forged***.

# IPsec Documents

- IPsec encompasses three functional areas:
  - authentication,
  - confidentiality, and
  - key management
- The totality of the IPsec specification is scattered across dozens of **RFCs** and **draft IETF documents**, making this the most complex and difficult to grasp of all IETF specifications

# IPsec Documents

- The documents can be categorized into the following ***groups***
  - Architecture
    - RFC4301 *Security Architecture for Internet Protocol*
  - Authentication Header (AH)
    - RFC4302 *IP Authentication Header*
  - Encapsulating Security Payload (ESP)
    - RFC4303 *IP Encapsulating Security Payload (ESP)*
  - Internet Key Exchange (IKE)
    - RFC4306 *Internet Key Exchange (IKEv2) Protocol*
  - Cryptographic algorithms
  - Other

# IPsec Services

- IPsec provides ***security services*** at the ***IP layer*** by ***enabling*** a system to ***select*** required security protocols, ***determine*** the algorithm(s) to use for the service(s), and ***put in place*** any cryptographic keys required to provide the requested services.
- RFC 4301 lists the following services:
  - Access control
  - Connectionless integrity
  - Data origin authentication
  - Rejection of replayed packets (a form of partial sequence integrity)
  - Confidentiality (encryption)
  - Limited traffic flow confidentiality

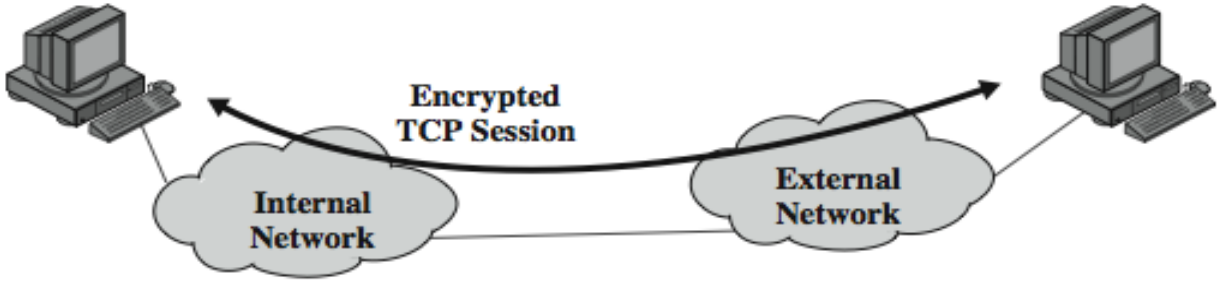
# Transport Mode

- Transport mode provides ***protection*** primarily for ***upper-layer protocols***.
- That is, transport mode protection extends to the ***payload*** of an IP packet.
- Typically, transport mode is used for ***end-to-end communication between two hosts*** (e.g., a client and a server, or two workstations)
- **to encrypt & *optionally* authenticate IP data**
  - can do traffic analysis but is efficient
  - good for ESP host-to-host traffic

# Tunnel Mode

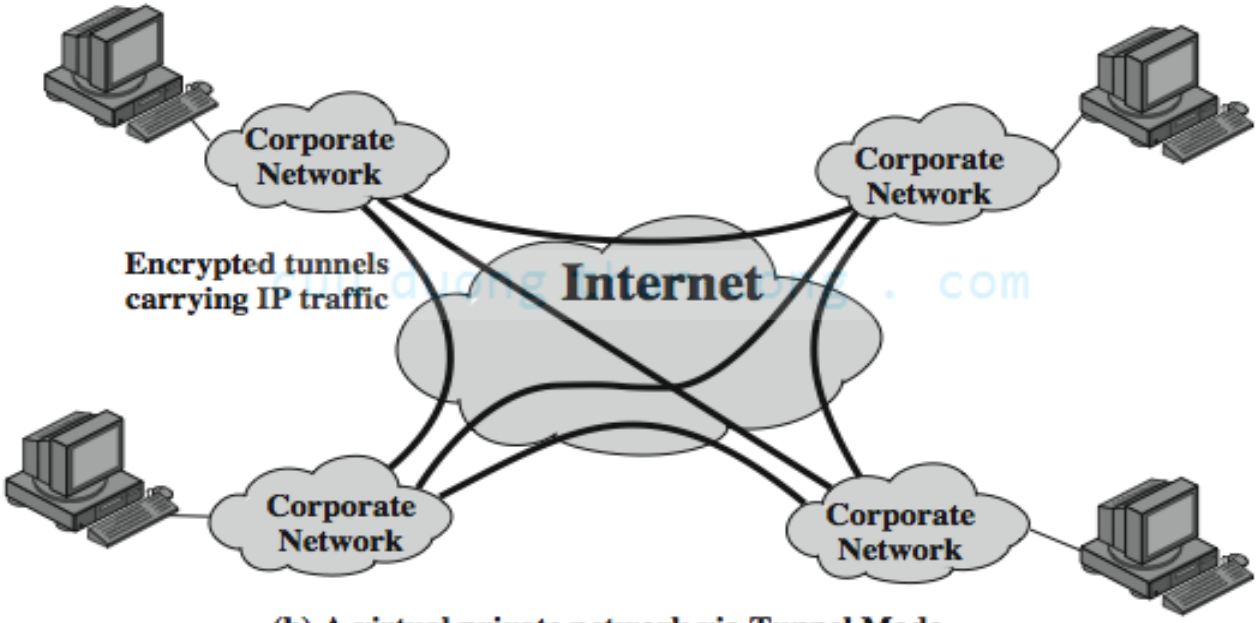
- Tunnel mode provides ***protection*** to the ***entire IP packet***.
- To achieve this, after the ***AH or ESP fields are added*** to the IP packet, the entire packet plus security fields is treated as the ***payload*** of new outer IP packet with a ***new outer IP header***
- The entire original, inner, packet travels ***through a tunnel*** from one point of an IP network to another; no routers along the way are able to examine the inner IP header
  - encrypts entire IP packet
  - add new header for next hop
  - no routers on way can examine inner IP header
  - good for VPNs, gateway to gateway security

# Transport and Tunnel Modes



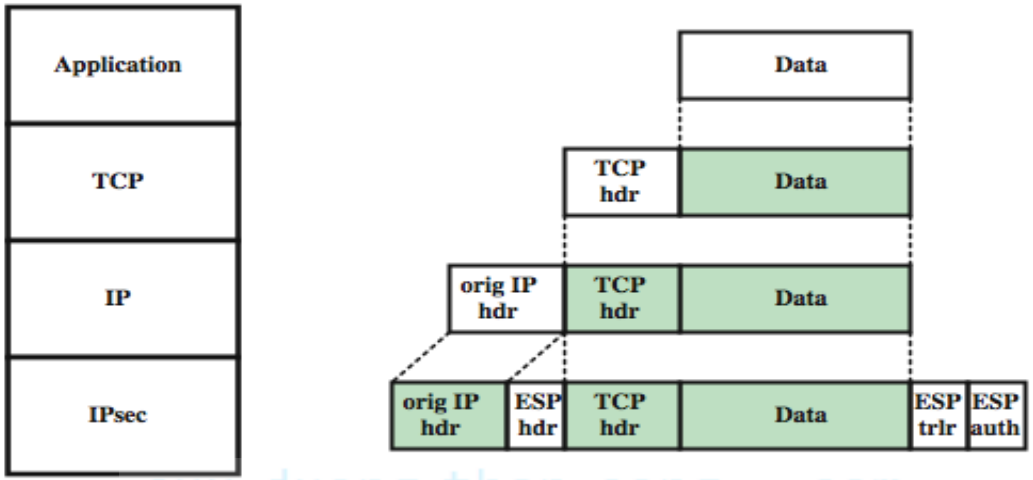

(a) Transport-level security



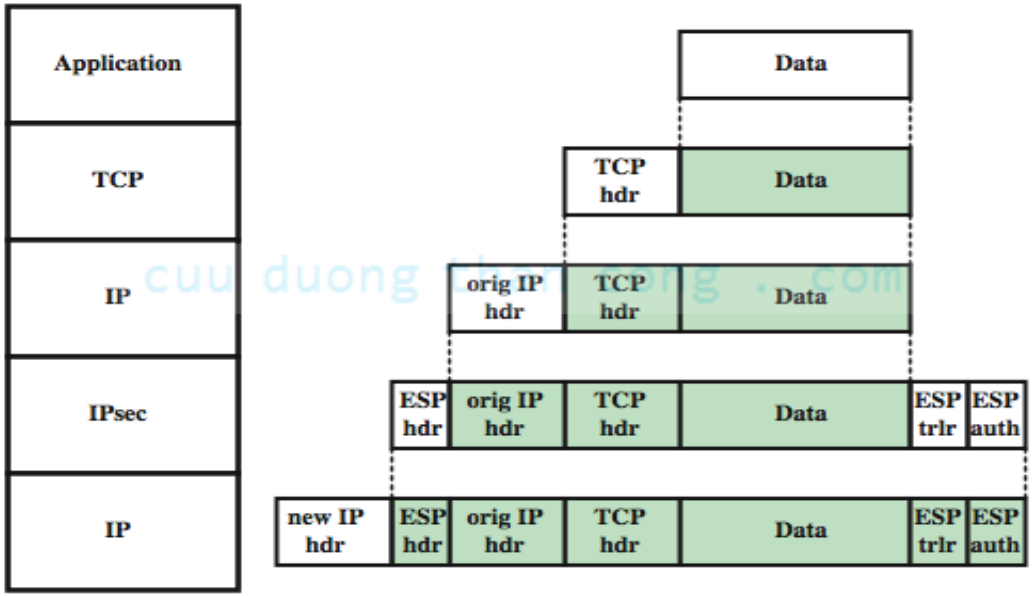



(b) A virtual private network via Tunnel Mode

# Transport and Tunnel Modes Protocols




(a) Transport mode




(b) Tunnel mode

# IP Security Policy

- Fundamental to the operation of IPsec is the ***concept of a security policy*** applied to each IP packet that transits ***from a source to a destination***.
- IPsec policy is determined primarily by the interaction of ***two databases***,
  - the security association database (SAD) and
  - the security policy database (SPD)

- Security Associations
- Security Association Database
- Security Policy Database
- IP Traffic Processing

# Security Associations (SA)

- A ***key concept*** that appears in both the authentication and confidentiality mechanisms for IP is the security association (SA)
- **a *one-way logical connection* between sender & receiver that affords *security service* to the traffic carried on it**
- **identified by 3 parameters:**
  - **Security Parameters Index** (SPI): *A bit string assigned to this SA and having local significance only*
  - **IP Destination Address:** *address of the destination endpoint*
  - **Security Protocol Identifier:** *indicates whether the association is an AH or ESP security association*

# Security Association Database (SAD)

- In each IPsec implementation, there is a nominal ***Security Association Database*** that defines the parameters associated with each SA.
  - Security Parameter Index
  - Sequence Number Counter
  - Sequence Counter Overflow
  - Anti-Replay Window
  - AH Information
  - ESP Information
  - Lifetime of this Security Association
  - IPsec Protocol Mode
  - Path MTU

# Security Policy Database (SPD)

- The ***means*** by which IP traffic is related to specific SAs (or no SA in the case of traffic allowed to bypass IPsec) is the nominal ***Security Policy Database***

# Security Policy Database

| Protocol | Local IP | Port | Remote IP | Port | Action | Comment |
|---|---|---|---|---|---|---|
| UDP | 1.2.3.101 | 500 | * | 500 | BYPASS | IKE |
| ICMP | 1.2.3.101 | * | * | * | BYPASS | Error messages |
| * | 1.2.3.101 | * | 1.2.3.0/24 | * | PROTECT: ESP intransport-mode | Encrypt intranet traffic |
| TCP | 1.2.3.101 | * | 1.2.4.10 | 80 | PROTECT: ESP intransport-mode | Encrypt to server |
| TCP | 1.2.3.101 | * | 1.2.4.10 | 443 | BYPASS | TLS: avoid double encryption |
| * | 1.2.3.101 | * | 1.2.4.0/24 | * | DISCARD | Others in DMZ |
| * | 1.2.3.101 | * | * | * | BYPASS | Internet |

# Encapsulating Security Payload (ESP)

- ESP can be used to ***provide*** confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality.
- The set of services provided ***depends on options*** selected at the time of Security Association (SA) establishment and on the location of the implementation in a network topology.
- ESP can work with a ***variety of encryption*** and ***authentication algorithms***

# Encryption and Authentication Algs

- The Payload Data, Padding, Pad Length, and Next Header fields are ***encrypted*** by the ESP service.
- If the algorithm used to encrypt the payload requires cryptographic synchronization data, such as an initialization vector (IV), then these data may be carried explicitly at the beginning of the Payload Data field.
- If included, an IV is usually not encrypted, although it is often referred to as being part of the ciphertext.

# Padding

- The Padding field serves several purposes:
  - to expand plaintext to required length
  - to align pad length and next header fields
  - to provide partial traffic flow confidentiality



cuu duong than cong . com

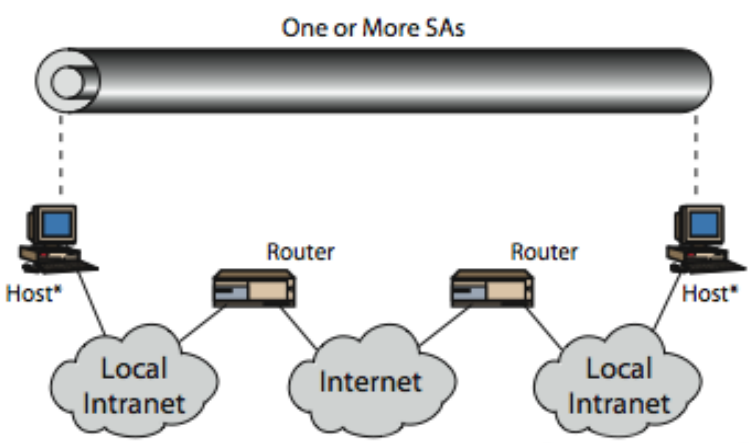
# Anti-Replay Service

- replay is when attacker ***resends*** a copy of an authenticated packet
- use sequence number to thwart this attack
- sender initializes sequence number to 0 when a new SA is established
  - increment for each packet
  - must not exceed limit of $2^{32} - 1$
- receiver then accepts packets with seq no within window of $(N - W + 1)$

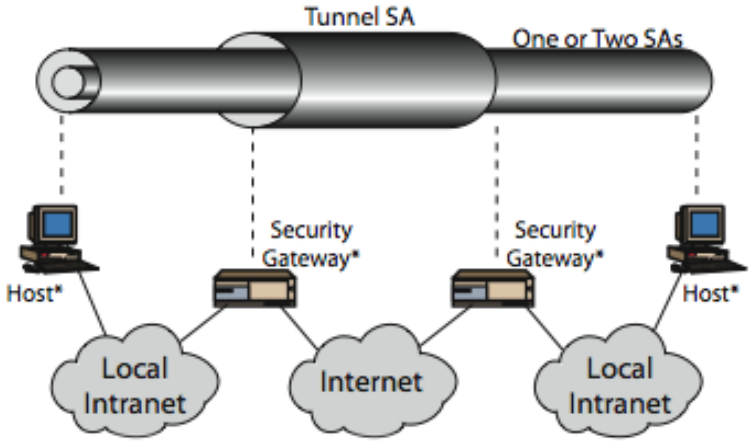
# Combining Security Associations

- **SA's can implement either AH or ESP**
- **to implement both need to combine SA's**
  - form a security association bundle
  - may terminate at different or same endpoints
  - combined by
    - o transport adjacency
    - o iterated tunneling
- **combining authentication & encryption**
  - ESP with authentication, bundled inner ESP & outer AH, bundled inner transport & outer ESP

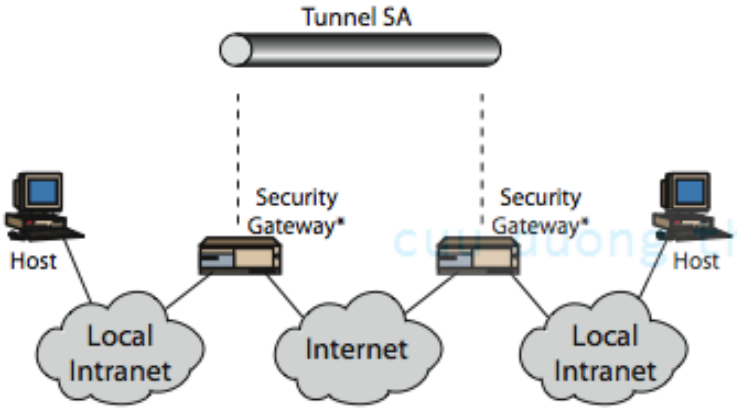
# Combining Security Associations



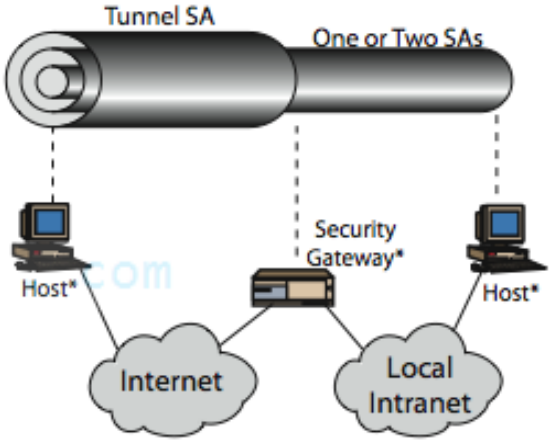

(a) Case 1




(c) Case 3




(b) Case 2




(d) Case 4

# IPSec Key Management

- **handles key generation & distribution**
- **typically need 2 pairs of keys**
  - 2 per direction for AH & ESP
- **manual key management**
  - Sys admin manually configures every system
- **automated key management**
  - automated system for on demand creation of keys for SA's in large systems
  - has Oakley & ISAKMP elements

# Cryptographic Suits

- **variety of cryptographic algorithm types**
- **to promote interoperability have**
  - RFC4308 defines VPN cryptographic suites
    - ✓VPN-A matches common corporate VPN security using 3DES & HMAC
    - ✓VPN-B has stronger security for new VPNs implementing IPsecv3 and IKEv2 using AES
  - RFC4869 defines four cryptographic suites compatible with US NSA specs
    - ✓provide choices for ESP & IKE
    - ✓AES-GCM, AES-CBC, HMAC-SHA, ECP, ECDSA

# Summary

We have discussed:

- IP Security Overview
- IP Security Policy
- Encapsulating Security Payload
- Combining Security Associations
- Internet Key Exchange
- Cryptographic Suits

# References

1. Cryptography and Network Security, Principles and Practice, William Stallings, Prentice Hall, Fifth Edition, 2011



cuu duong than cong . com