



Network Security

CSC 512 – Networks: Architectures and Protocols

Instructor: Dr. Frye

frye@kutztown.edu

Computer Science & Information Technology
Department, Kutztown University

Network Security

■ Definition?

“Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users, and programs to perform their permitted critical functions within a secure environment.”



Network Attacks

- What are some examples of attacks against networks?



Security Overview

- Integrity
- Confidentiality
- Availability
- Authorization
- Authentication
- Nonrepudiation
- Replay Avoidance



Phases of Network Security

- Protection

- Detection

- Reaction



Network Security Components

- What are some examples of network security components / devices / services?



Network Security Components

- Antivirus Software
- Access Control
- Multifactor Authentication
- Encryption
- VPN
- Firewalls
- Wireless Security
- Email Security
- Web Security
- IDS / IPS
- Honeypots
- Network Segmentation
- Policies



Network Security Tools

- What are some tools that can be beneficial for managing network security?



Firewalls

■ Purpose

- ☐ Restrict people to enter at a carefully controlled point
- ☐ Prevent attackers from getting close to your other defenses
- ☐ Restrict people to leave at a carefully controlled point

■ Design goals

- ☐ All traffic from inside to outside and vice versa must travel through the firewall
- ☐ Only authorized traffic can pas through the firewall
- ☐ The firewall must be immune to penetration



Access Control

- Service control
- Direction control
- User control
- Behavior control



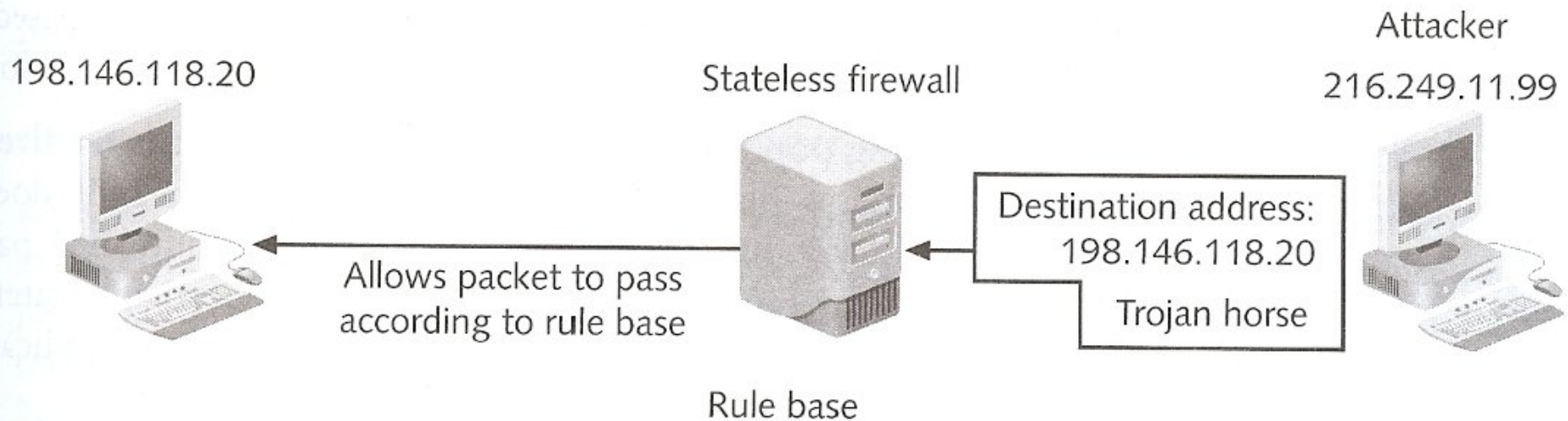
Firewall Management Cycle

- Draft a written security policy
- Design the firewall to implement the security policy
- Implement the firewall design by installing selected hardware or software
- Test the firewall
- Review new threats, requirements for additional security, and updates to adopted systems and software.



Stateless Packet Filter

- Rule Base
- Forward or Discard
- Advantages?
- Disadvantages?



| Rule | Transport | Protocol | Source IP | Source Port | Destination IP | Destination Port | Action | Time |
|------|-----------|----------|-----------|-------------|----------------|------------------|--------|------|
| 1 | TCP | HTTP In | Any | 80 | 198.146.118.20 | 80 | Allow | Any |

Example Rules

Table 9-1 Stateless packet-filtering rules

| Rule | Source IP | Source Port | Destination IP | Destination Port | Action |
|------|---------------|-------------|----------------|------------------|--------|
| 1 | Any | Any | 192.168.120.0 | Above 1023 | Allow |
| 2 | 192.168.120.1 | Any | Any | Any | Deny |
| 3 | Any | Any | 192.168.120.1 | Any | Deny |
| 4 | 192.168.120.0 | Any | Any | Any | Any |
| 5 | Any | Any | 192.168.120.2 | 25 | Allow |
| 6 | Any | Any | 192.168.120.3 | 80 | Allow |
| 7 | Any | Any | Any | Any | Deny |

Current states

| Source IP | Destination IP |
|----------------|----------------|
| 198.146.118.20 | 206.23.19.4 |

No current relationship
between 198.146.118.20
and 216.249.118.20

198.146.118.20



Stateless firewall



Destination address:
198.146.118.20

Trojan horse

Denies packet
because it is not
requested by user

Attacker

216.249.11.99



Rule base

| Rule | Transport | Protocol | Source IP | Source Port | Destination IP | Destination Port | Action | Time |
|------|-----------|----------|-----------|-------------|----------------|------------------|--------|------|
| 1 | TCP | HTTP In | Any | 80 | 198.146.118.20 | 80 | Allow | Any |

Stateful Packet Filter Connection Table

Table 9-2 State table example

| Source IP | Source Port | Destination IP | Destination Port | Connection State |
|-----------------|-------------|-----------------|------------------|------------------|
| 192.168.120.101 | 1037 | 209.233.19.22 | 80 | Established |
| 192.168.120.104 | 1022 | 165.66.28.22 | 80 | Established |
| 192.168.120.107 | 1010 | 65.66.122.101 | 25 | Established |
| 192.168.120.102 | 1035 | 213.136.87.88 | 79 | Established |
| 223.56.78.11 | 1899 | 192.168.120.101 | 80 | Established |
| 206.121.55.8 | 3558 | 192.168.120.101 | 80 | Established |
| 224.209.122.1 | 1079 | 192.168.120.105 | 80 | Established |

Firewall Rules

- Allow all, deny specific
- Deny all, allow specific
- Processed in order
- Keep simple and short



Establish Effective Rules

- Based on Security Policy
 - Firewall Policy
- Simple and short
- Restrict access to internal network
- Control Internet services

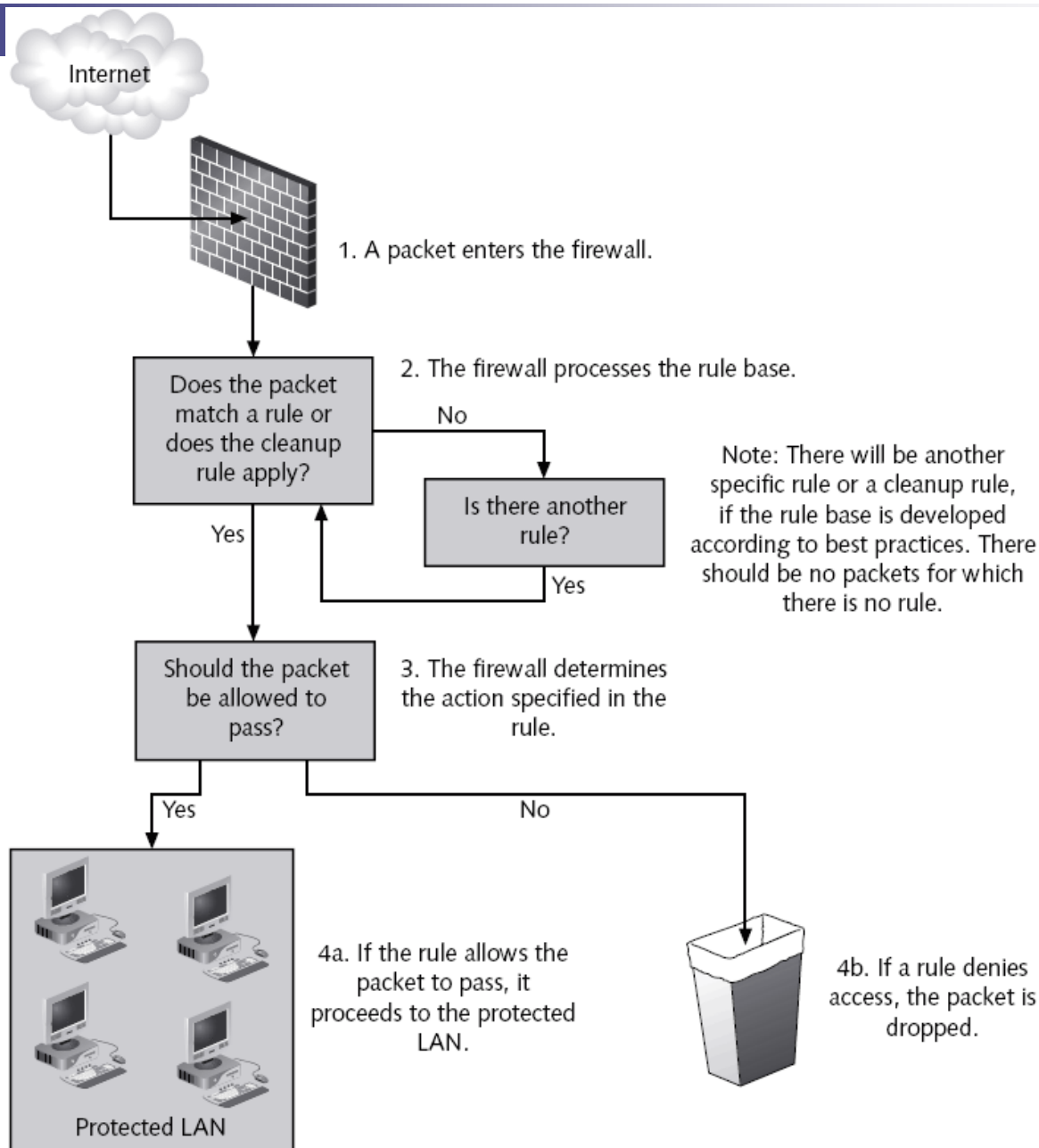


Figure 9-11 Firewalls process rules in order until a match is found
CSC512 - Dr. Lisa Frye, Kutztown University

Example Rules

Table 9-11 A typical packet-filtering rule base

| Rule | Source IP | Source Port | Destination IP | Destination | Action | What It Does |
|------|---------------|-------------|----------------|-------------|--------|--|
| 1 | 192.168.120.1 | Any | Any | Any | Deny | Prevents the firewall itself from making any connections |
| 2 | Any | Any | 192.168.120.1 | Any | Deny | Prevents anyone from connecting to the firewall |
| 3 | 192.168.120.0 | Any | Any | Any | Allow | Allows internal users to access external computers |
| 4 | 192.168.120.0 | Any | 192.168.120.4 | 53 | Allow | Enables internal users to connect to the DNS server |

Table 9-11 A typical packet-filtering rule base (continued)

| Rule | Source IP | Source Port | Destination IP | Destination | Action | What It Does |
|------|---------------|-------------|----------------|-------------|--------|---|
| 5 | Any | Any | 192.168.120.2 | 25 | Allow | Allows external and internal users to access the e-mail server via SMTP port 25 |
| 6 | 192.168.120.0 | Any | 192.168.120.2 | 110 | Allow | Enables internal users to connect to the e-mail server using POP3 port 110 |
| 7 | Any | Any | 192.168.120.3 | 80 | Allow | Enables both external and internal users to connect to the Web server |
| 8 | Any | Any | Any | Any | Deny | Blocks all traffic not covered by previous rules |



IPSec Services

- Access control
- Connectionless security
- Origin authentication
- Replay protection
- Privacy / Confidentiality

Benefits

- Provides strong security applied to all IP traffic
- IPSec in a firewall can be resistant to bypass
- Transparent to applications
- Can be transparent to end users
- Can provide security for individual users if needed

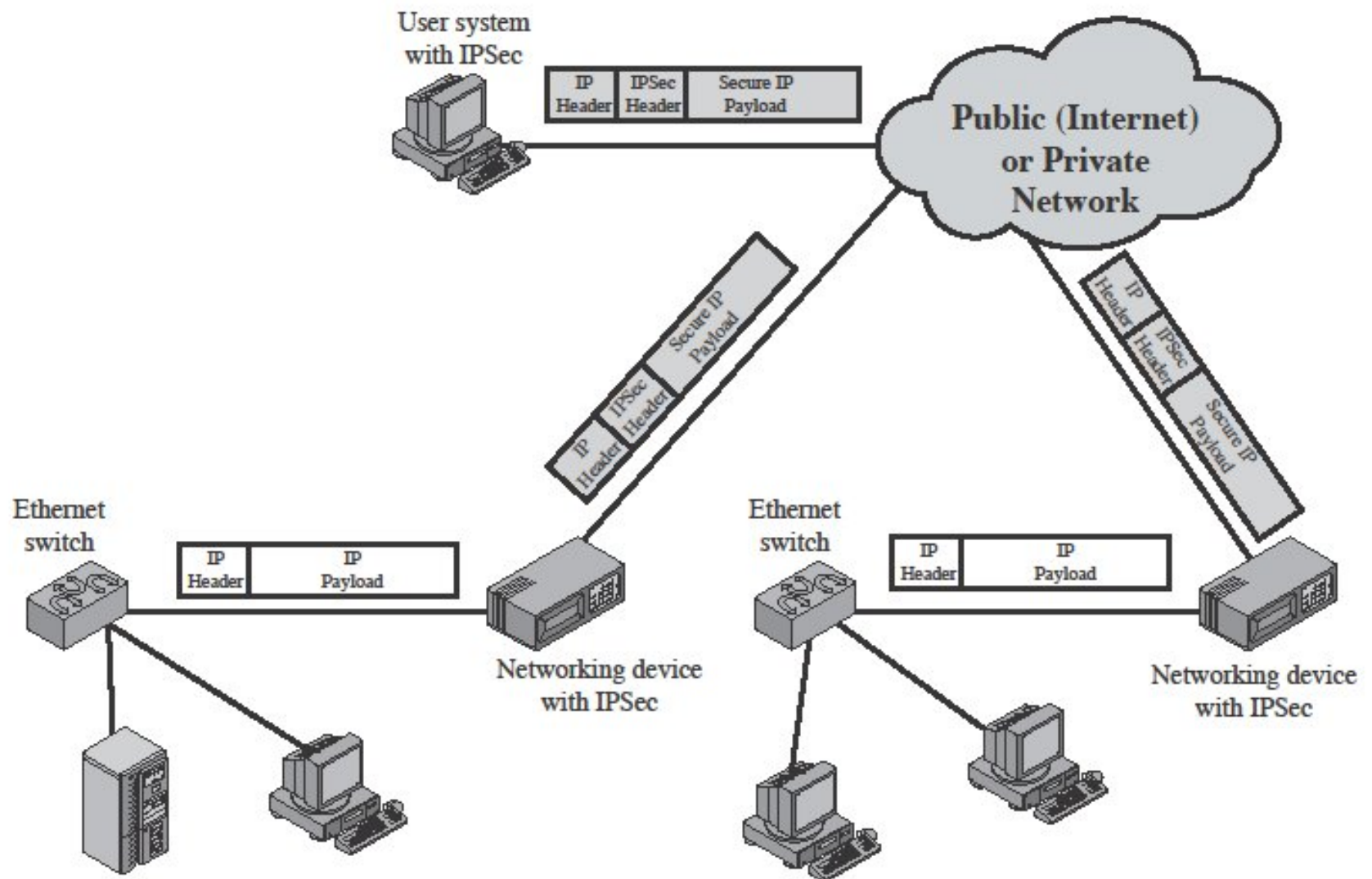


Figure 8.1 An IP Security Scenario

Protocols

- Authentication Header (AH)
 - ☐ Access control
 - ☐ Integrity
 - ☐ Authentication
- Encapsulating Security Payload (ESP)
 - ☐ Access Control
 - ☐ Confidentiality
 - ☐ Integrity (optional)
 - ☐ Authentication (optional)

Authentication Header

| Next header | Payload length | Reserved |
|---------------------------------|----------------|----------|
| Security Parameters Index (SPI) | | |
| Sequence Number | | |
| Authentication Data (variable) | | |

Encapsulating Security Payload

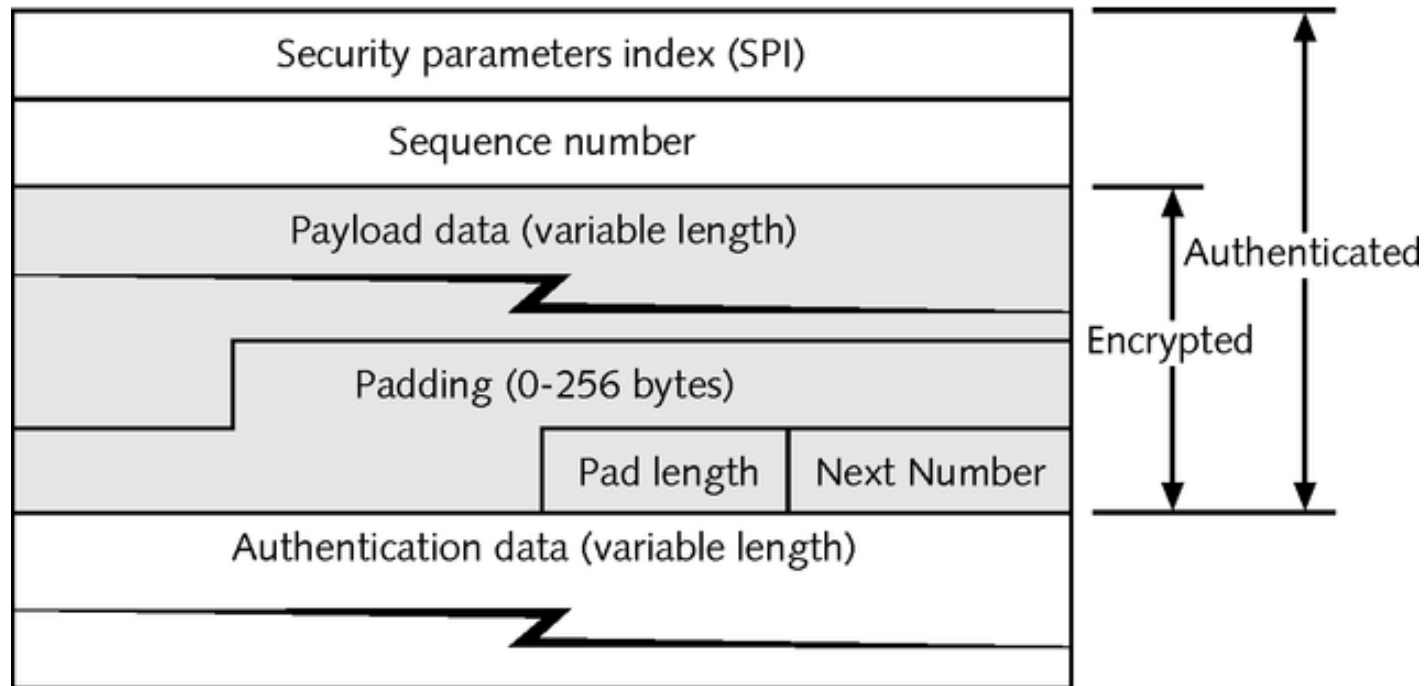


Figure 4-8 IPsec security payload



Security Associations

- Contract between two communicating entities
- One-way relationship
- Protocol specific
- What and how of IPSec protection



SA Information

- Security Parameters Index (SPI)
- IP Destination Address
- Security Protocol Identifier
- Secret keys
- Encapsulation mode

SA types

- Transport Mode

- ☐ Between hosts
- ☐ One IP header

- Tunnel Mode

- ☐ Between hosts or gateways
- ☐ Two IP headers
- ☐ Protects entire IP packet

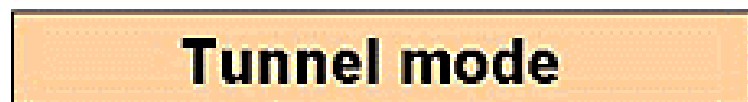
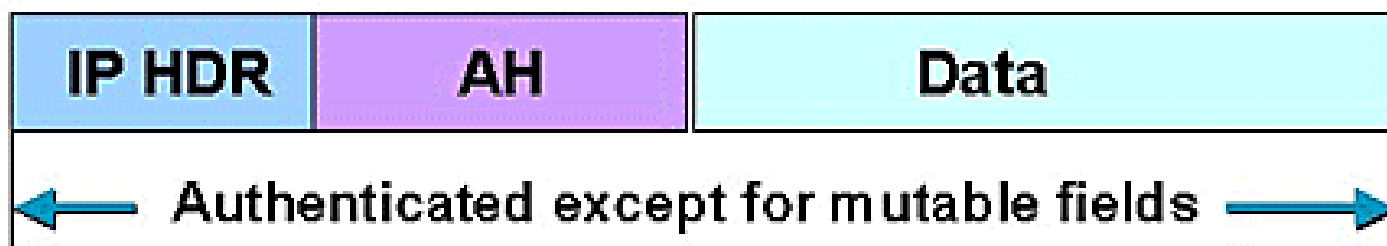
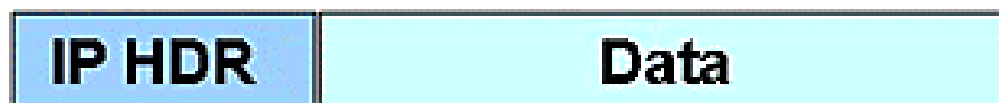
IPSec Example

- Packet routed from host A to a firewall or secure router at boundary of A's network.
- Firewall or router determines if IPSec is necessary for that packet
- If requires IPSec, firewall/router performs IPSec processing
 - Encapulates the packet in an outer IP header
 - Source IP address of outer IP packet is this firewall/router
 - Destination IP address of outer IP packet may be firewall/router that forms boundary to B's local network
- Packet is now routed to B's firewall/router
- Intermediate routers examine only the outer IP header
- B's firewall/router strips off the outer IP header
- Inner packet is delivered to host B

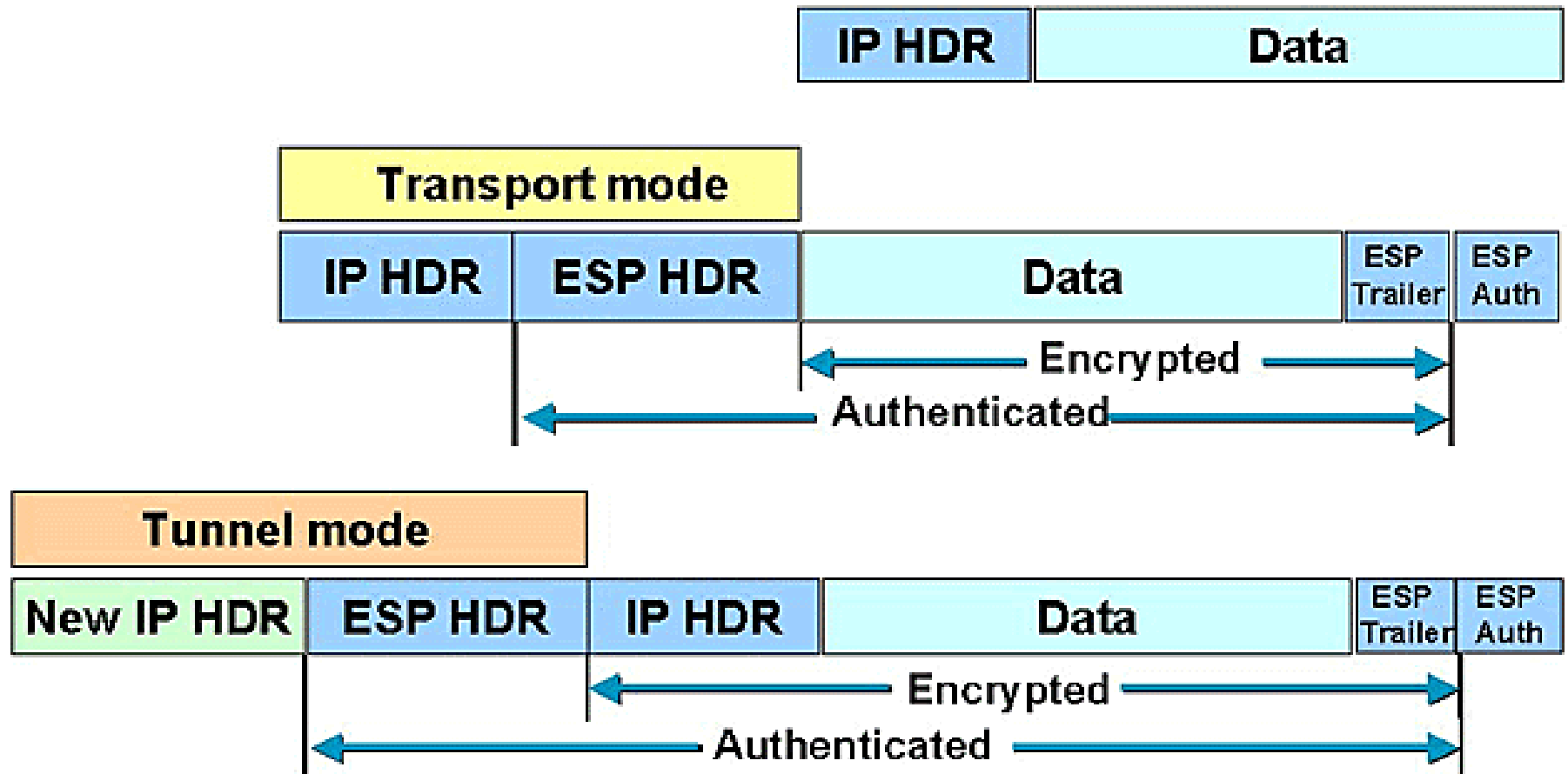
Table 8.1 Tunnel Mode and Transport Mode Functionality

| | Transport Mode SA | Tunnel Mode SA |
|--------------------------------|--|---|
| AH | Authenticates IP payload and selected portions of IP header and IPv6 extension headers. | Authenticates entire inner IP packet (inner header plus IP payload) plus selected portions of outer IP header and outer IPv6 extension headers. |
| ESP | Encrypts IP payload and any IPv6 extension headers following the ESP header. | Encrypts entire inner IP packet. |
| ESP with Authentication | Encrypts IP payload and any IPv6 extension headers following the ESP header. Authenticates IP payload but not IP header. | Encrypts entire inner IP packet. Authenticates inner IP packet. |

IPSec AH Packet Examples



IPSec ESP Packet Examples



IPSec Databases

- Security Associations Database (SAD)
- Security Policy Database (SPD)
 - ☐ Discard
 - ☐ Bypass
 - ☐ Protect

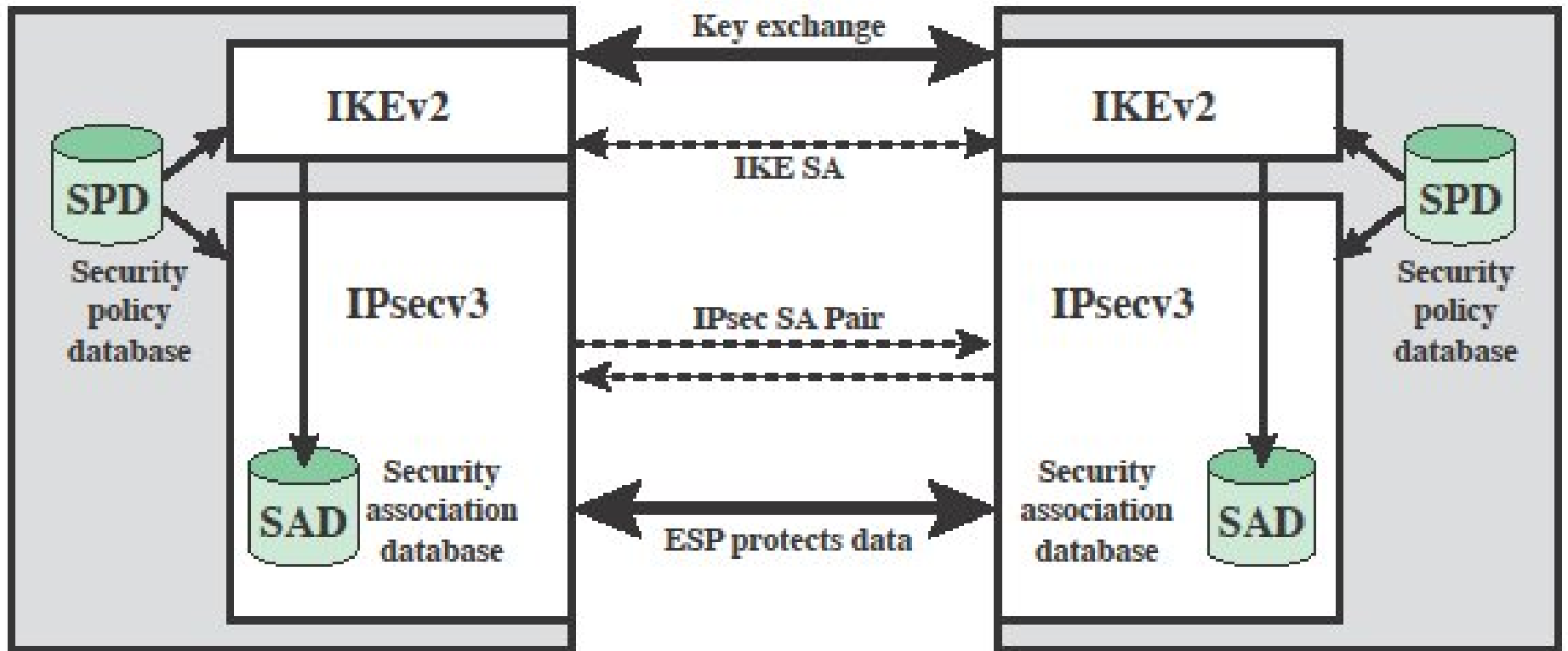
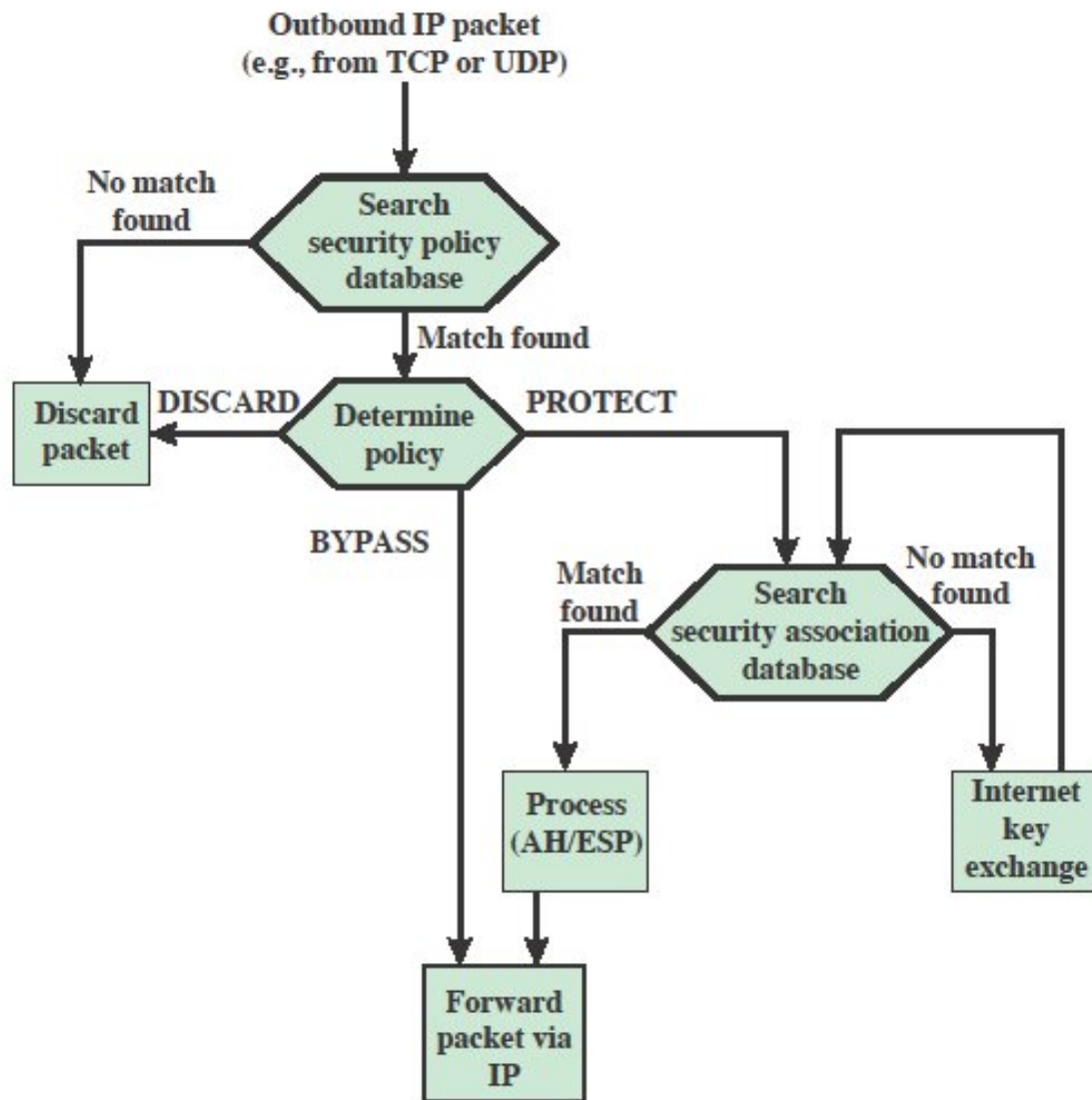


Figure 8.2 IPsec Architecture

Selectors

- Identifies SPD entry
- IP and upper-layer protocol field values
 - Source IP address
 - Destination IP address
 - DNS name
 - IP protocol ID field
 - Source port number
 - Destination port number



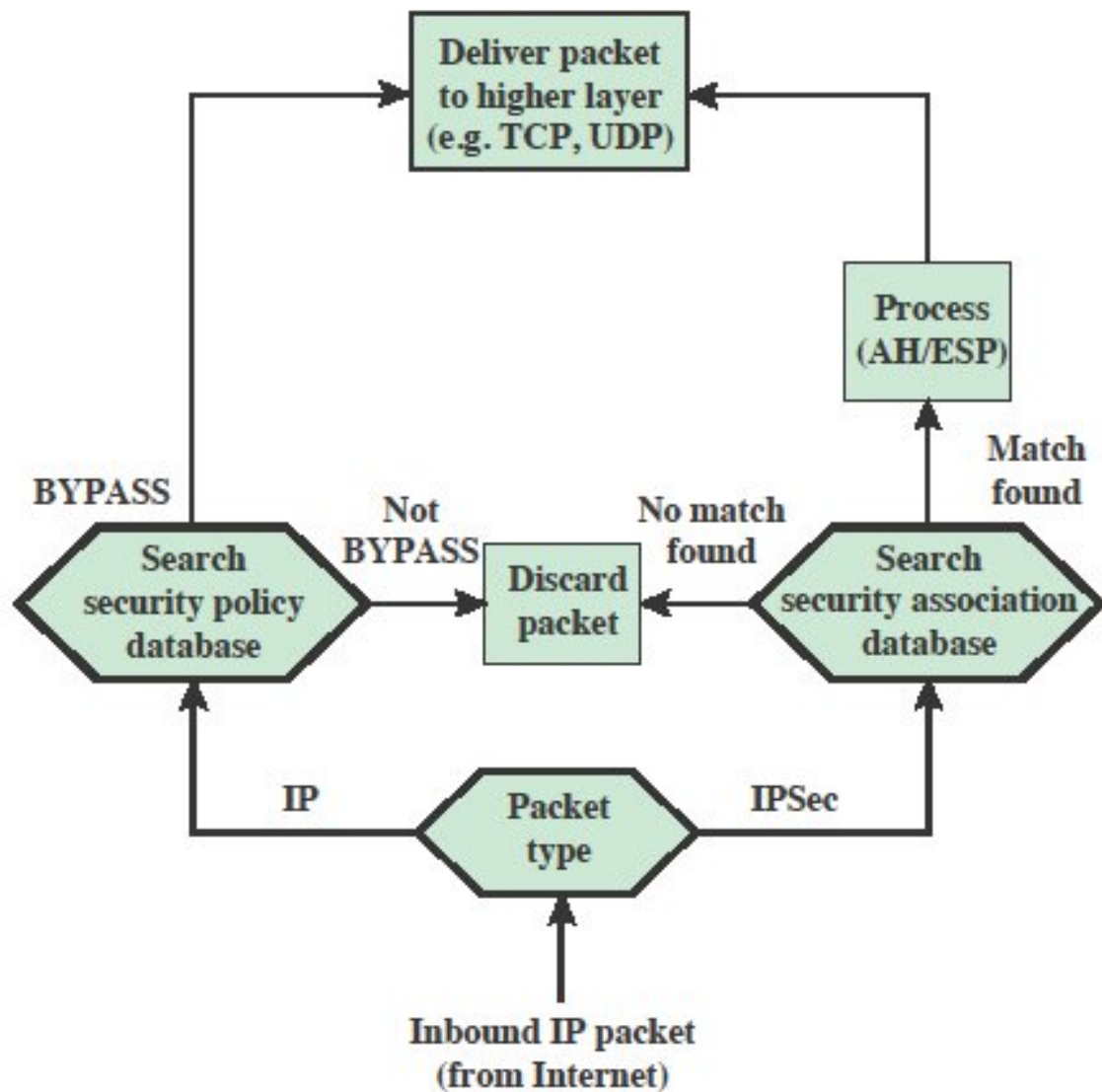
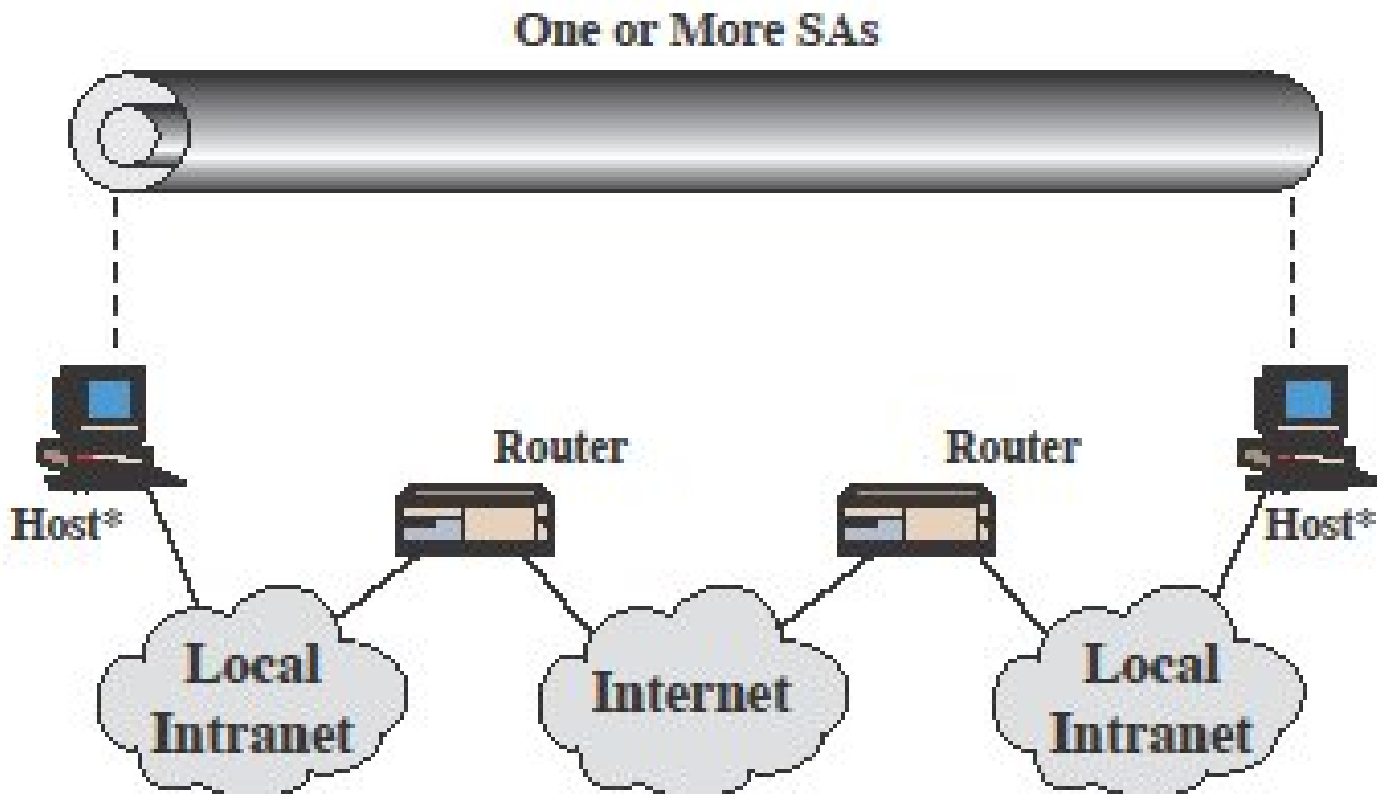


Figure 8.4 Processing Model for Inbound Packets

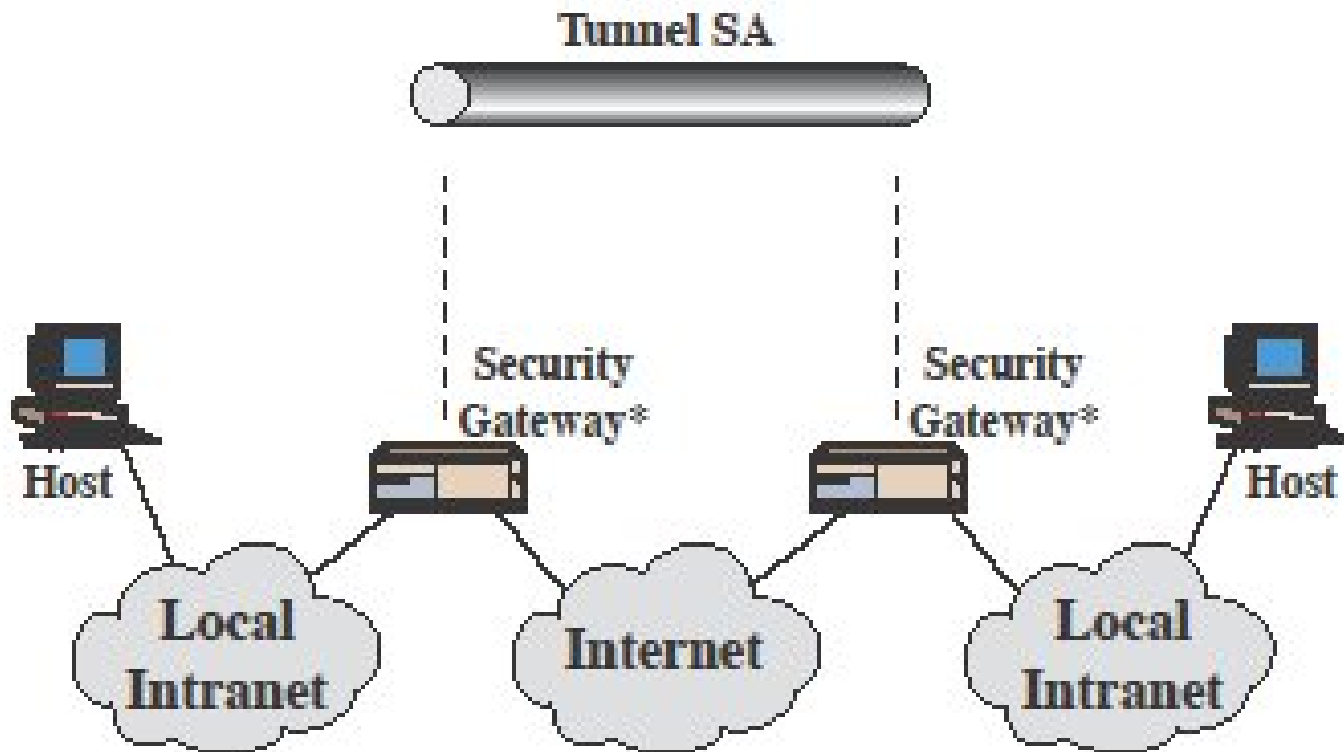


SA Bundles

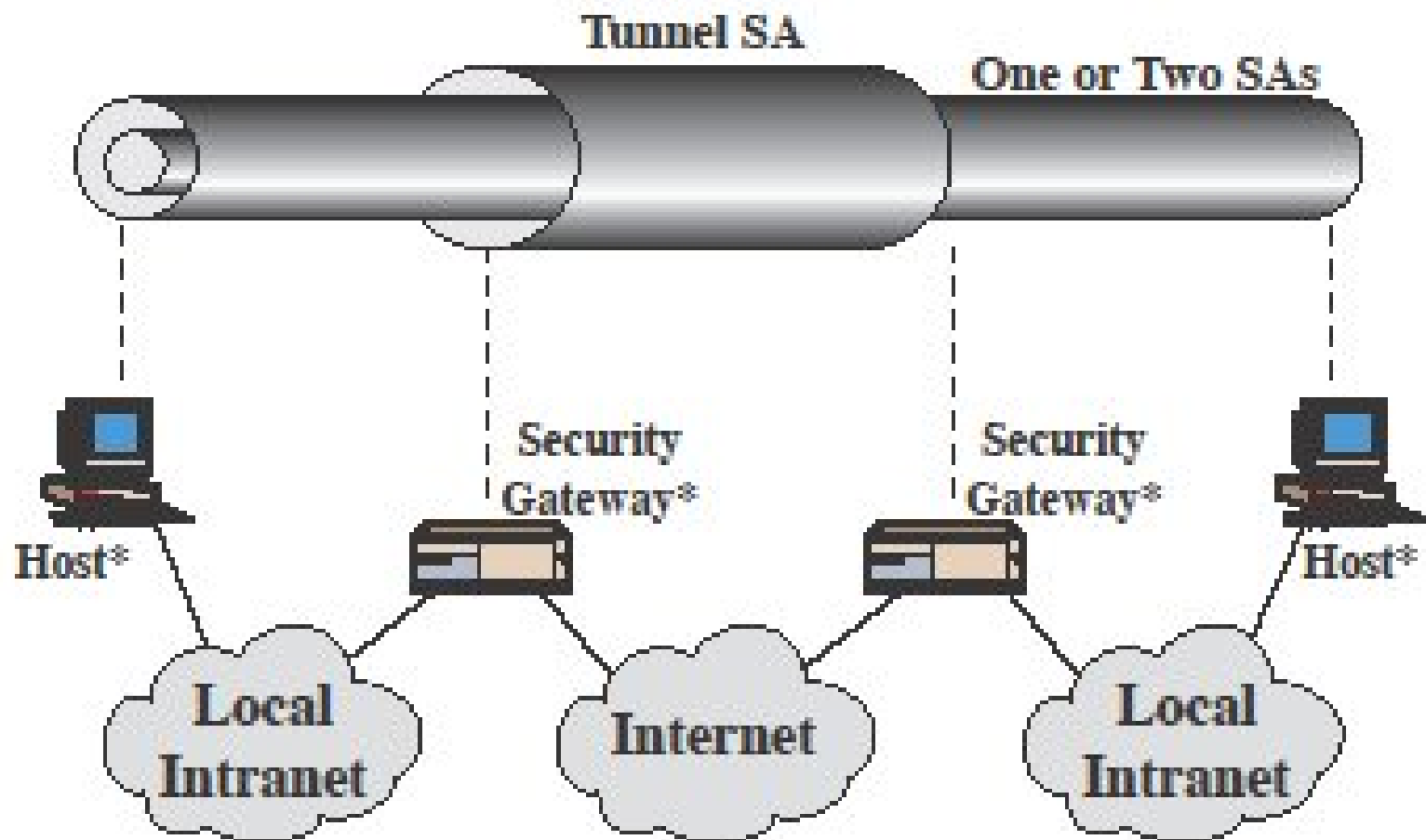
- Combine multiple SAs
- Transport Adjacency
- Iterated Tunneling
- Combination of two



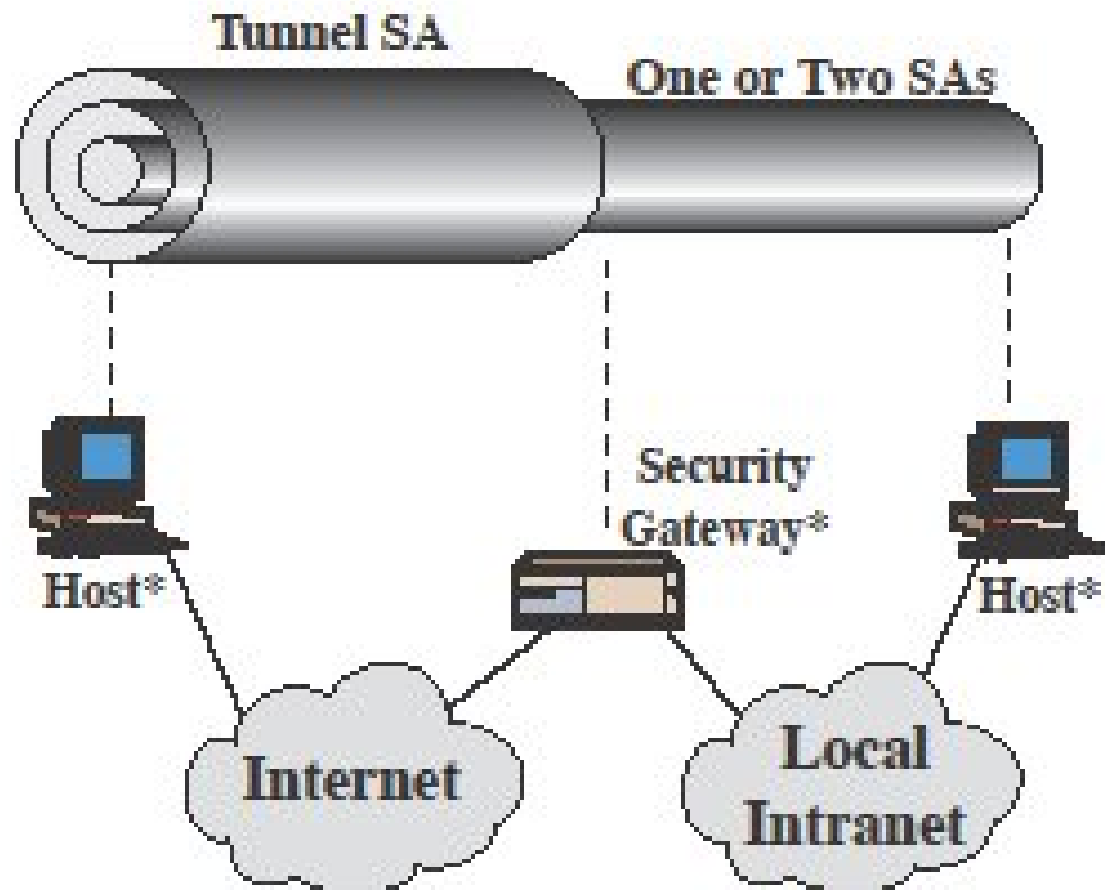
(a) Case 1



(b) Case 2



(c) Case 3



(d) Case 4



Authentication plus Confidentiality

- ESP with Authentication
- Transport Adjacency
- Transport-tunnel Bundle

ESP with Authentication

- Apply ESP to data
- Append Authentication Data field
- Transport mode ESP
 - Apply encryption and authentication to IP payload
- Tunnel mode ESP
 - Authentication applied to entire IP packet

Transport Adjacency

- Two bundled transport SAs
- Inner SA – ESP SA
- Outer SA – AH SA
- ESP without Authentication option
- Encryption applied to IP payload
- IP header then ESP header
- AH applied to ESP and original IP packet

Transport-Tunnel Bundle

- Authentication before encryption
- Inner packet – AH SA
- Outer packet – ESP SA
- Authenticate entire IP packet
- Apply ESP in tunnel mode
- Add new outer IP header



Key Management

- Manual
- Automatic