CprE 530

Lecture 13

General countermeasures

- Since IP is so ingrained in the Internet it is hard to provide security. There are a few general countermeasures.
  - IP Filtering
  - Network Address Translation (NAT)
  - Virtual Private Network (VPN)
  - Encrypted IPV4 & IPV6 (IPSec)

IP Filtering

- Routers can be configured to filter out packets based on:
  - IP Address (black listing)
    - Hard to keep list current
    - Hard to get off the list (DOS)
  - Port numbers
    - Rogue protocols use multiple ports
  - Protocol types (TCP, UDP, ICMP)
    - Course grain filtering

Network Address Translation

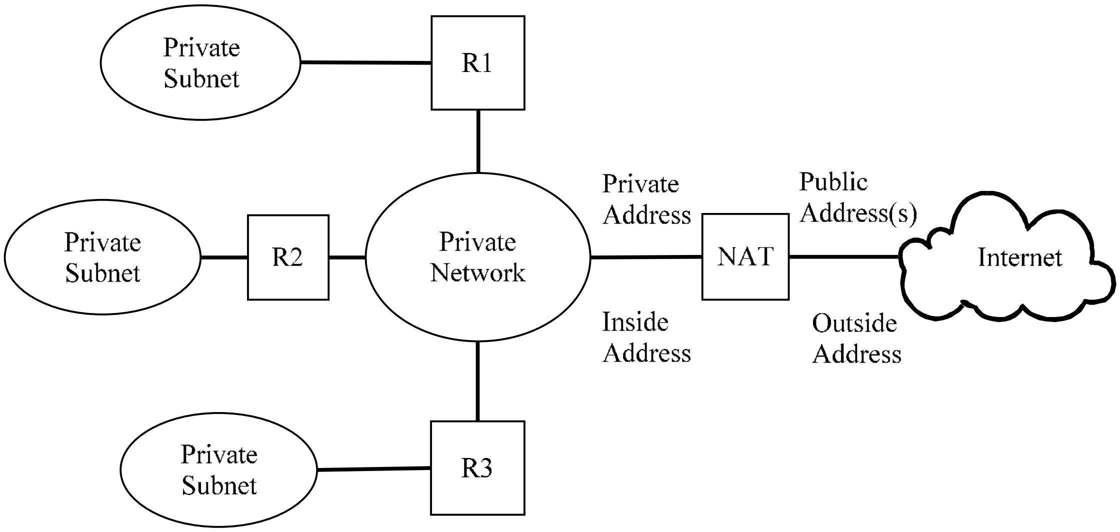


Figure 6.30 Private Network

Network Address Translation

- Used to extend the address space
  - Internal address ranges
    - 10/8 10.0.0.0
    - 172.16/12 172.16.0.0 (16 class B networks)
    - 192.168/16 192.168.0.0 (class B network)
- Static NAT
- Dynamic NAT

NAT

- Not really designed as a security device
- Does not provide security and is often coupled with a firewall

Static NAT

- One to one mapping of external addresses to internal addresses
- Used when a small number of machines need Internet access.
- NAT looks like a router to the inside machines and the destination to outside machines

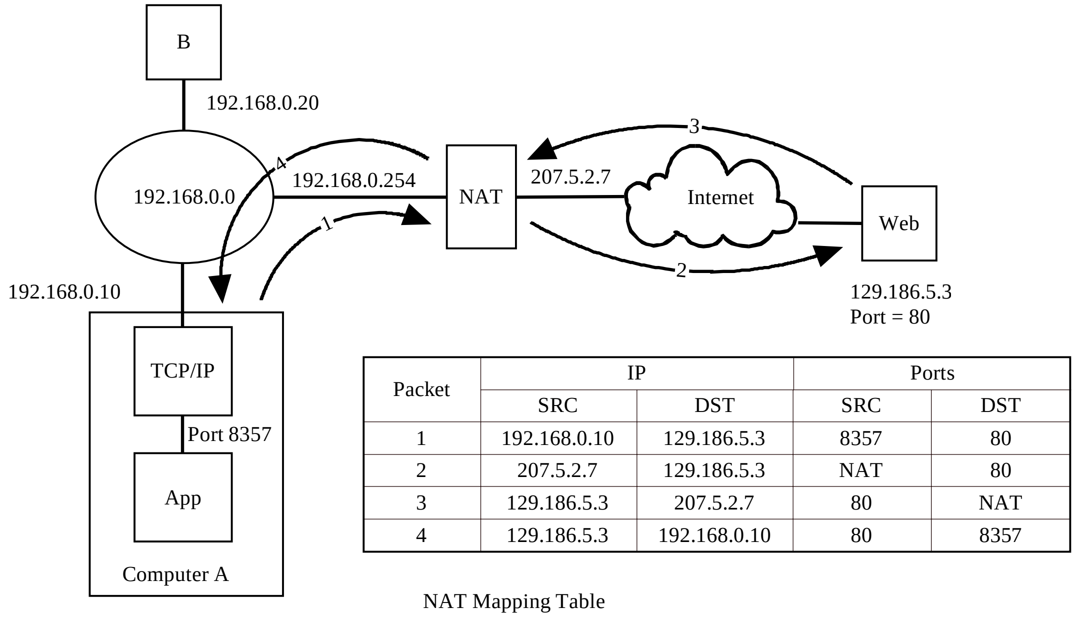
Static NAT

Public	Port	Private	Port
129.186.5.100	80	192.168.20.30	80
129.186.5.150	25	192.168.20.50	80

Dynamic NAT

- More machines on the inside than IP addresses on the outside.
- Used for outgoing access
- Can use tunnels for servers or combine with static NAT
- Inside can have same address range as a valid outside network (overlapping)

Dynamic NAT (Port mapping)



Packet	IP		Ports	
	SRC	DST	SRC	DST
1	192.168.0.10	129.186.5.3	8357	80
2	207.5.2.7	129.186.5.3	NAT	80
3	129.186.5.3	207.5.2.7	80	NAT
4	129.186.5.3	192.168.0.10	80	8357

NAT Mapping Table

Public IP	Ports		Private IP	Ports	
	SRC	DST		SRC	DST
129.186.5.3	NAT	80	192.168.0.10	8357	80

Figure 6.31 Sample Private Network

Public servers

- Servers need a public address
  - Two networks
  - Tunneling

Public & Private Networks

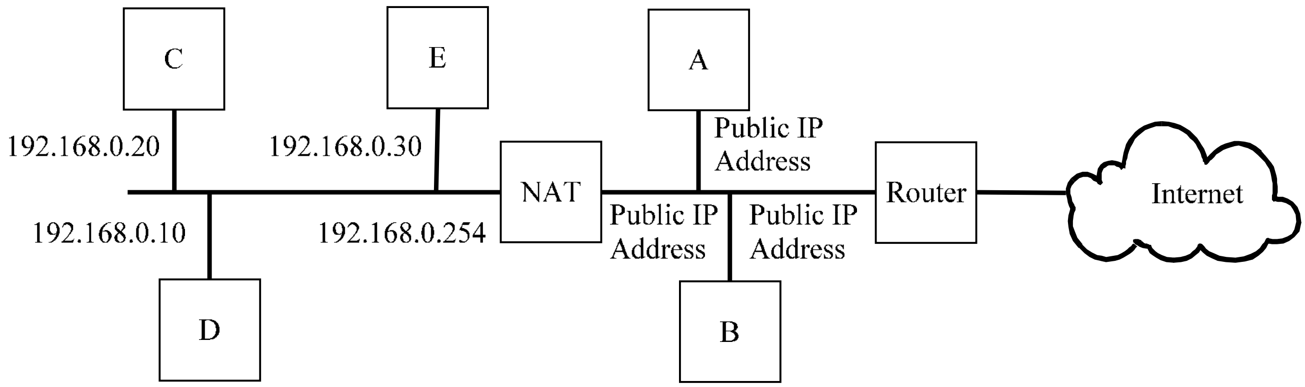
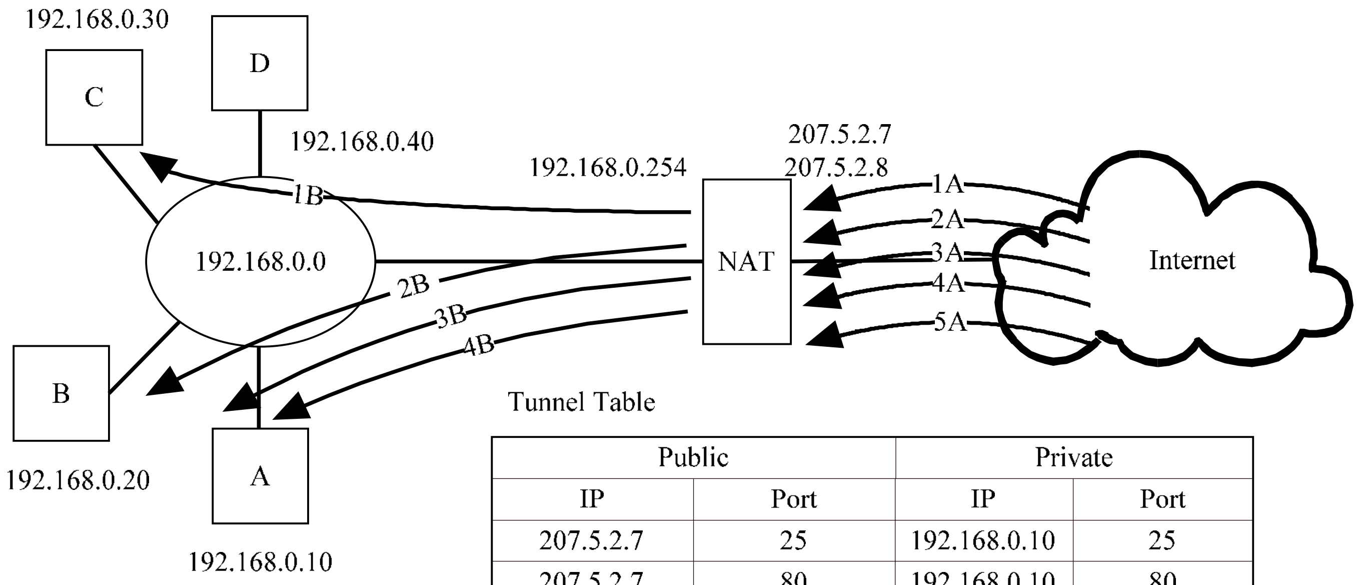


Figure 6.32 Public Servers and a Private Network

Tunneling through a NAT



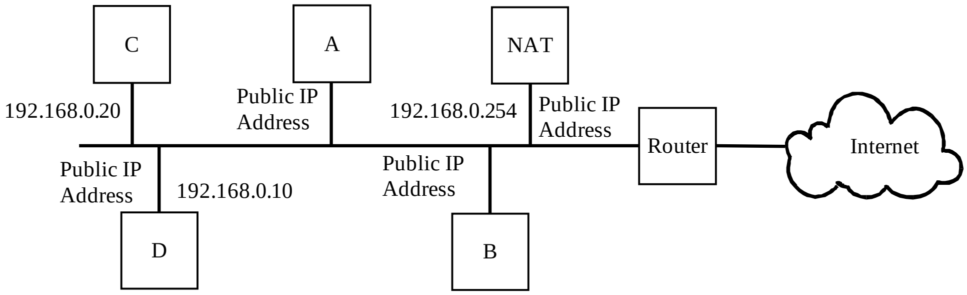
Tunnel Table

Public		Private	
IP	Port	IP	Port
207.5.2.7	25	192.168.0.10	25
207.5.2.7	80	192.168.0.10	80
207.5.2.8	80	192.168.0.20	80
207.5.2.8	100	192.168.0.30	80

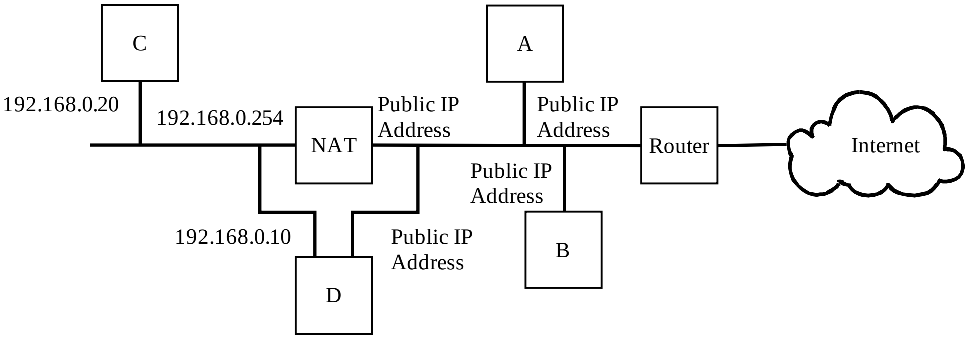
Tunneling through a NAT

Packet	IP		Ports	
	SRC	DST	SRC	DST
1A	Internet	207.5.2.8	8357	100
1B	Internet	192.168.0.30	8357	80
2A	Internet	207.5.2.8	7384	80
2B	Internet	192.168.0.20	7384	80
3A	Internet	207.5.2.7	2345	80
3B	Internet	192.168.0.10	2345	80
4A	Internet	207.5.2.7	2554	25
4B	Internet	192.168.0.10	2554	25
5A	Internet	207.5.2.7	6623	22

Pass-by NAT



Physical Configuration



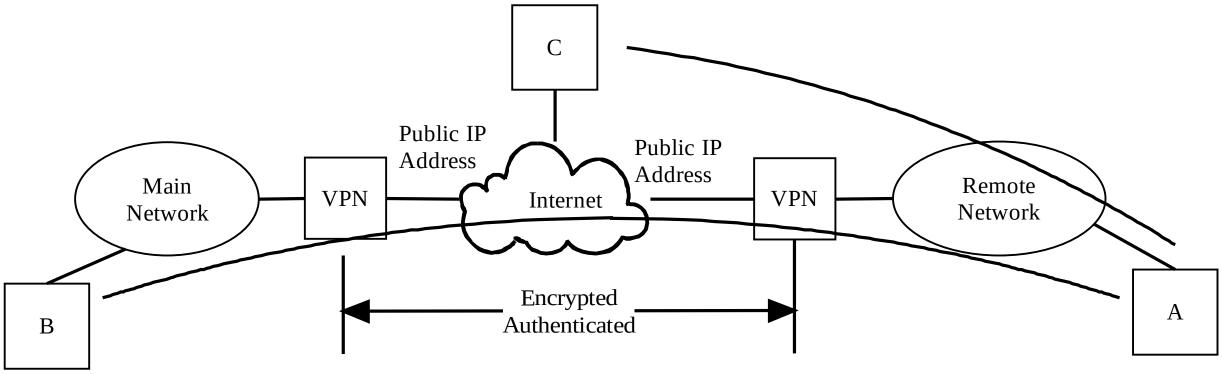
Logical Configuration

Virtual Private Network

- Used to created encrypted tunnels between devices
- Uses many different protocols
  - SSH
  - IPSEC
  - Proprietary

Network to network VPN

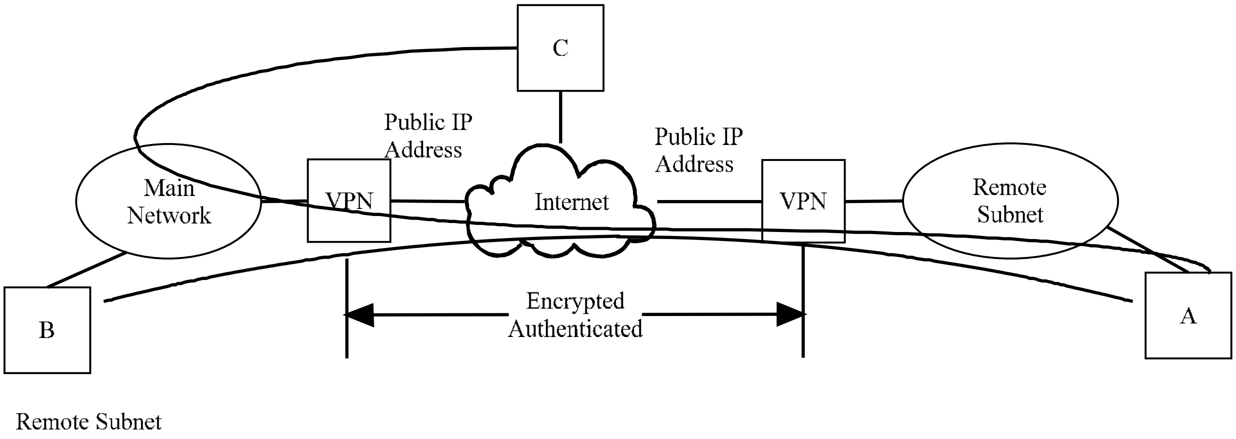
VPN only when talking to target network
Other traffic goes directly to destination



Remote Network

Network to network VPN

Always uses VPN
All traffic is routed through target network



Client to client VPN

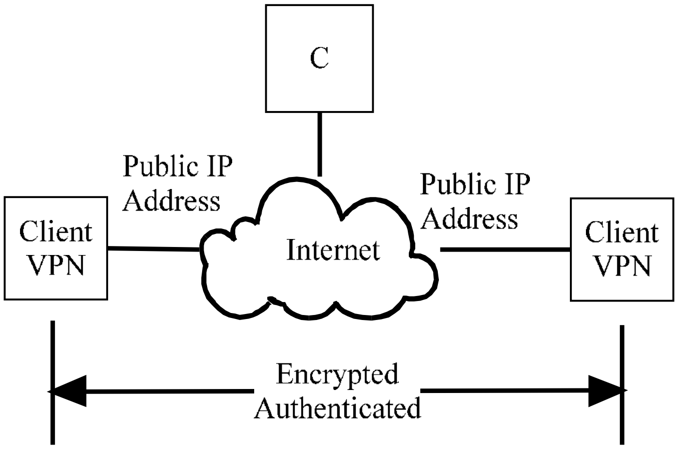
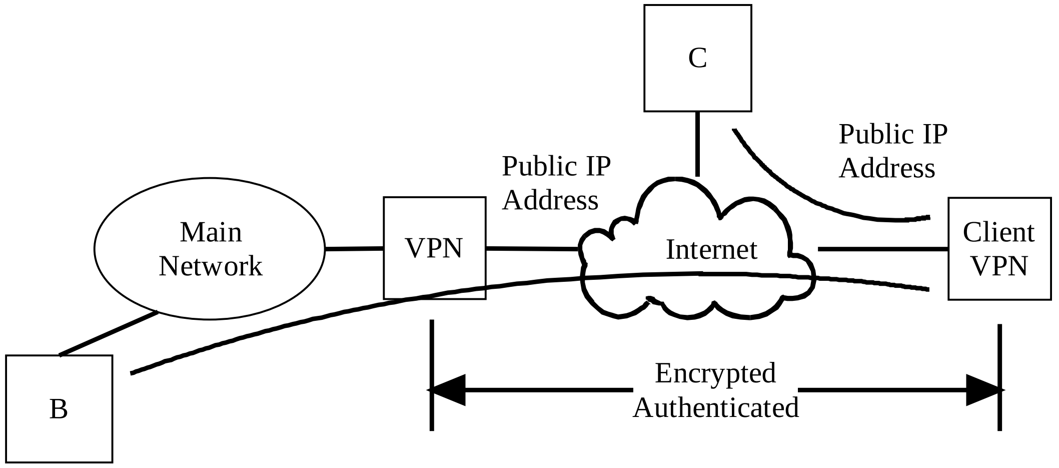


Figure 6.36 Client to Client VPN

Client to Network

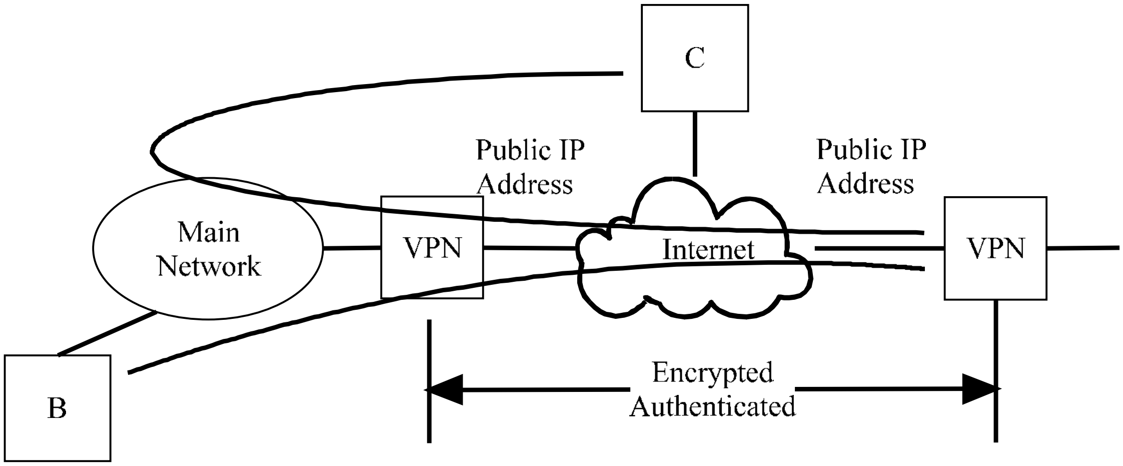
Always uses VPN
All traffic is routed through target network



Remote Access

Client to network

Always uses VPN
All traffic is routed through target network



Remote Subnet

IPSEC

- Two Purposes
  - Authentication: sender & receiver (prevents IP spoofing)
  - Encryption: data privacy
- IPSEC is not end-to-end

IPSEC

- AH = Authentication Header Not used much)
- ESP = Encapsulating Security Payload
- Not Specified in IPSEC Policy
  - Encryption Algorithms
  - Key Management
  - Domain of Interpretation

IPSEC Services

AH	ESP	BOTH	IPSEC Service
X	X	X	Access Control
X			Connectionless Integrity
X			Data Origin Authentication
X	X	X	Reject of Replay
	X		Confidentiality
	X		Limited Traffic Flow Confidentiality

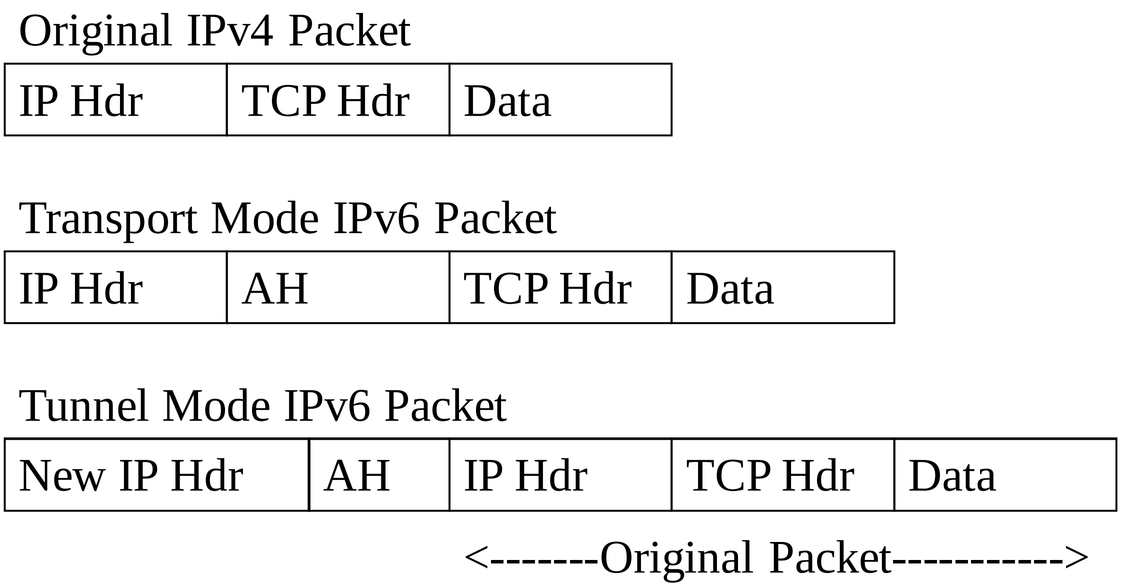
AH

Size	Field
8 bits	Next
8 bits	Length of Header
16 bits	Reserved
32 bits	Security Parameters
32 bits	Sequence Number
Variable	Authentication Data

Authentication Data: MD5 (1-way Hash)

AH Use: End-to-End or End-to-Intermediate Node

IPv4 Use of AH in IPSEC



Original IPv4 Packet

IP Hdr | TCP Hdr | Data

Transport Mode IPv6 Packet

IP Hdr | AH | TCP Hdr | Data

Tunnel Mode IPv6 Packet

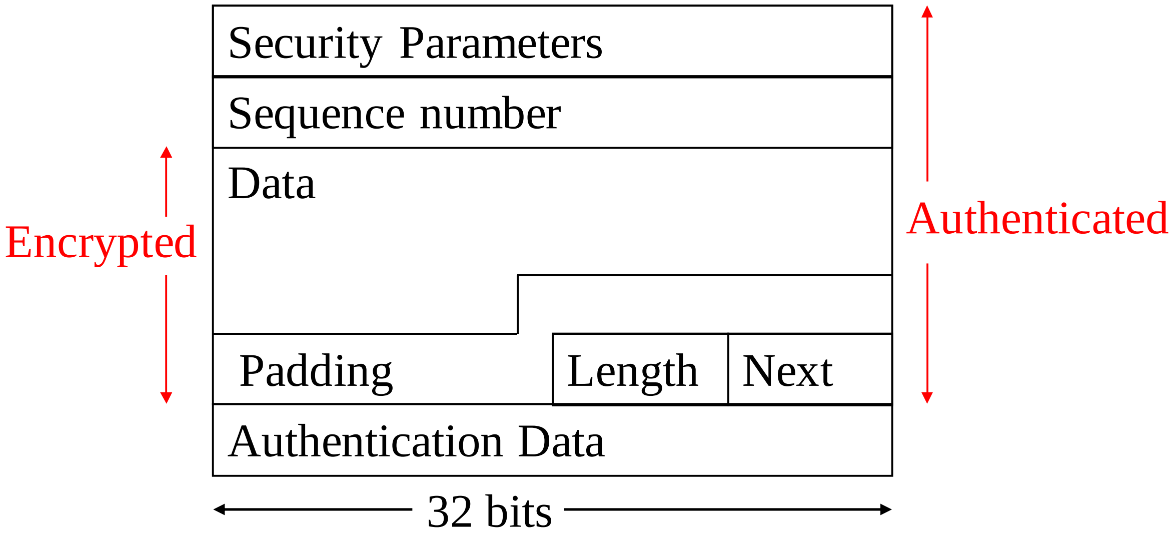
New IP Hdr | AH | IP Hdr | TCP Hdr | Data

<-------Original Packet----------->

ESP

- Encapsulating Security Payload
  - Security Parameters: help identify the encryption algorithm (eg: DES, blowfish)
  - Sequence number: an ever increasing number used for replay
  - Authentication data: a hash of everything, proves non-alteration
  - Data, Padding, Length, and Next fields are all encrypted

Encapsulating Security Payload


Security Parameters

Sequence number

Data

Padding

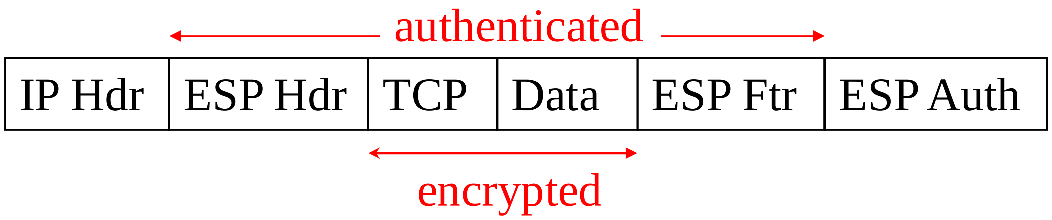
Length

Next

Authentication Data

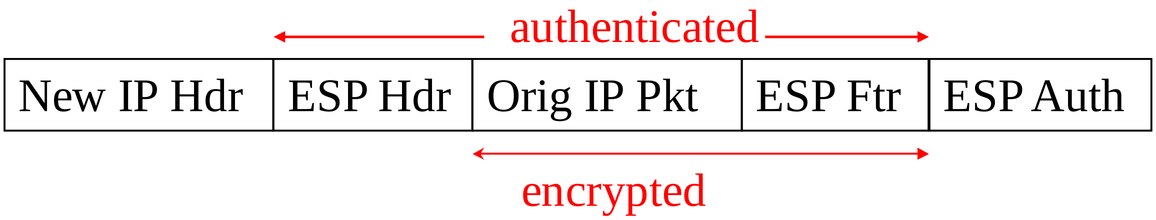
Encapsulating Security Payload

- There are two ways encryption can be handled:
  - – Transport Level (end-to-end)
  - – Tunnel mode (also referred to as VPN)
- Packet format for IPv4:


IP Hdr	ESP Hdr	TCP	Data	ESP Ftr	ESP Auth

Encapsulating Security Payload

- Packet format for IPv6:

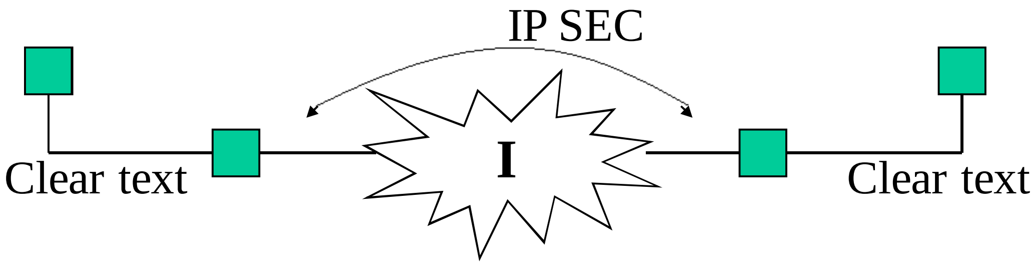


authenticated

New IP Hdr | ESP Hdr | Orig IP Pkt | ESP Ftr | ESP Auth

encrypted

- Tunneling mode:


IP SEC
I
Clear text
Clear text