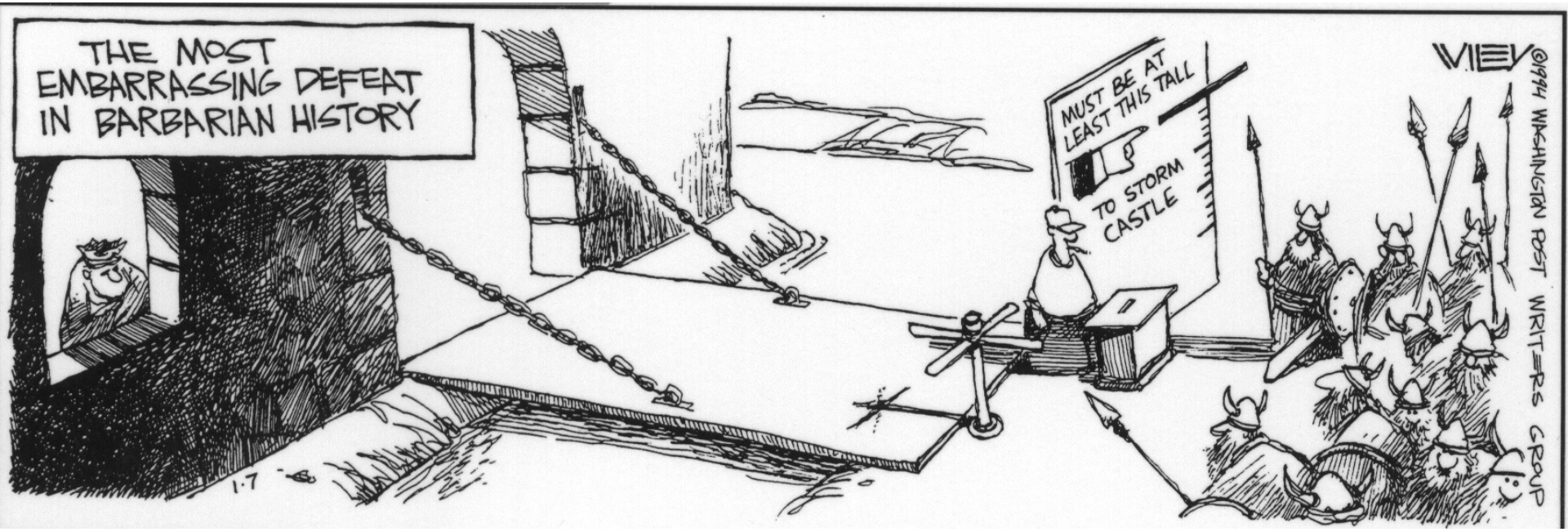
# Perimeter-based Defense for Network Security

# Components of Network Security Perimeter Defense

- Firewalls
  - DMZ
  - Bastion Host
  - Packet Filtering Firewalls
  - Stateful Filtering
  - Circuit level gateway
  - Application Proxies
- Virtual Private Networks (VPNs):
  - IPSec
- Intrusion Detection Systems (IDS)
  - Network-based  Vs. Host-based IDS
  - Anomaly-based Vs. Signature-based IDS

# Firewall


THE MOST EMBARRASSING DEFEAT IN BARBARIAN HISTORY
MUST BE AT LEAST THIS TALL
TO STORM CASTLE
VIEW
©1994 WASHINGTON POST WRITERS GROUP
1·7

# Why Firewalls?

- Internet connectivity is no longer an option for most corporation
- The Internet allows you access to worldwide resources, but…
  …the Internet also allows the *world* to try and access your resources
- This is a grave risk to most organizations
- A firewall is inserted between the premises network and the Internet
- Establishes a perimeter
- Provides a choke point where security and audits can be imposed
- Single computer system or a set of systems can perform the firewall function

# Design Goals

- All traffic, from inside to outside and vice versa, must pass through the firewall
- Only authorized traffic (defined by the security policy) is allowed to flow
- Firewall is immune to penetration – uses a trusted system

# Scope of Firewalls

- Single choke point - to protect vulnerable services from various kinds of attack (spoofing, DOS)
- Singular monitoring point – location for monitoring, auditing and event triggering
- Platform for non-security functions – can be used for network address translation and network management
- Platform for IPSec – implements VPN via tunnel mode

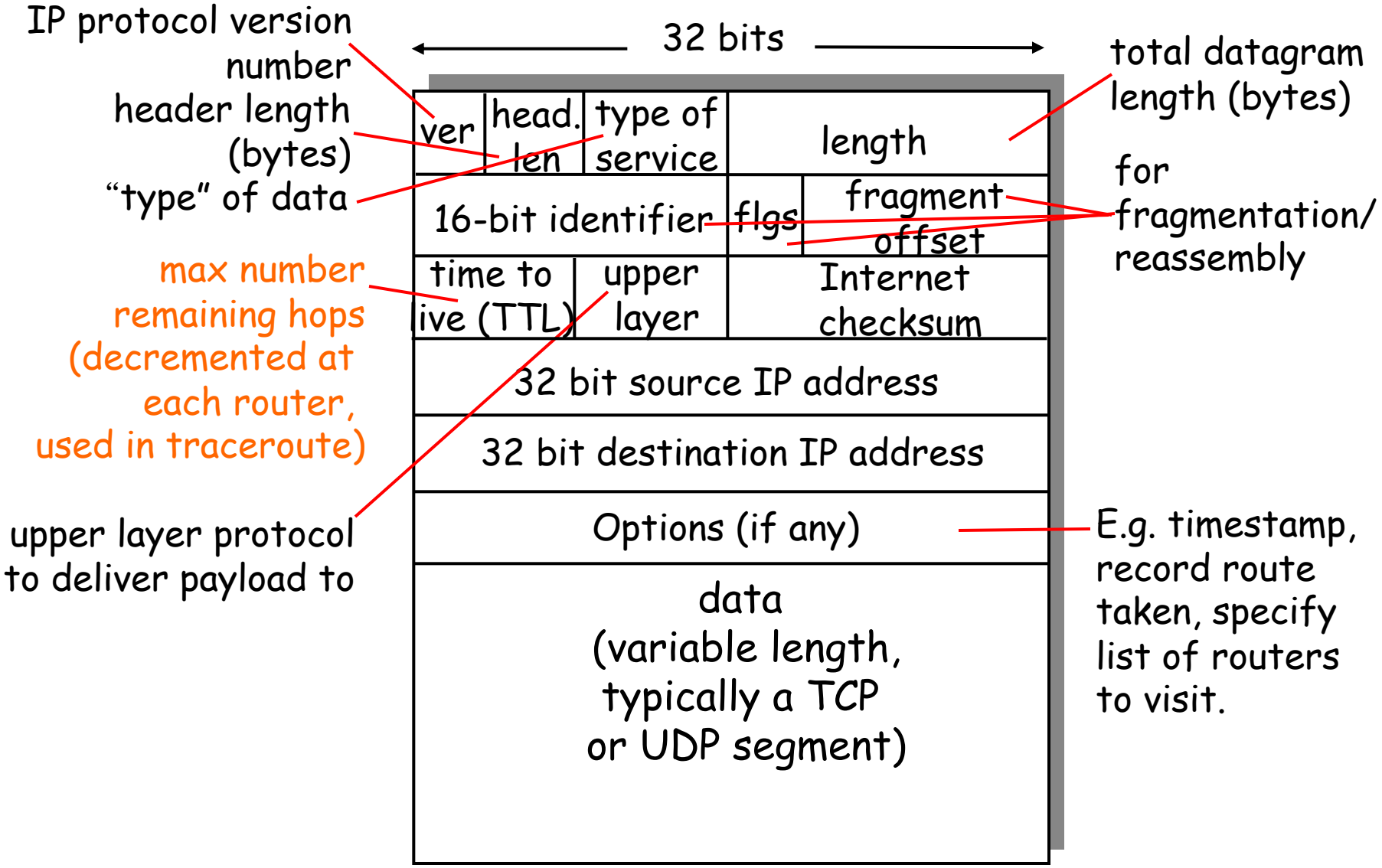
# Limitations of Firewalls

- Cannot protect against attack that bypasses the firewall – bypass attack
- Does not protect against internal threats
- Cannot protect against the transfer of virus-infected programs
- The increasing popularity of "firewall-friendly" protocols, e.g. http, and Web service related protocols

# Types of Firewalls

- Packet Filtering Firewall
- Stateful Firewall
- Application Level Gateway
- Circuit Level Gateway

# Review on IP datagram format

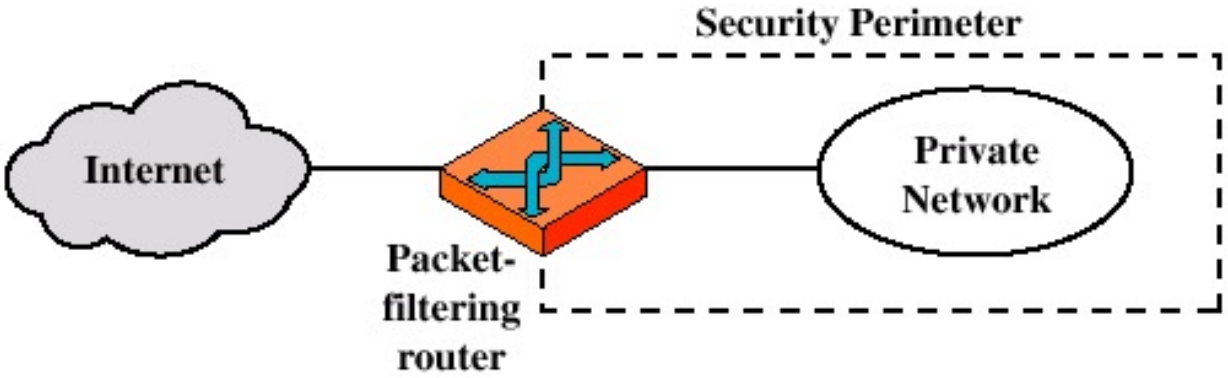


# Packet Filtering

- Applies a set of rules to each incoming IP packet and *forwards* or *discards* the packet
- Filters packets in *both directions*
- Rules based on *source* and *destination* IP addresses and *port* numbers

  => Make decisions based on Layer 3 and Layer 4 information
- *List of rules* looking for a match
- Decisions made on a per-packet basis

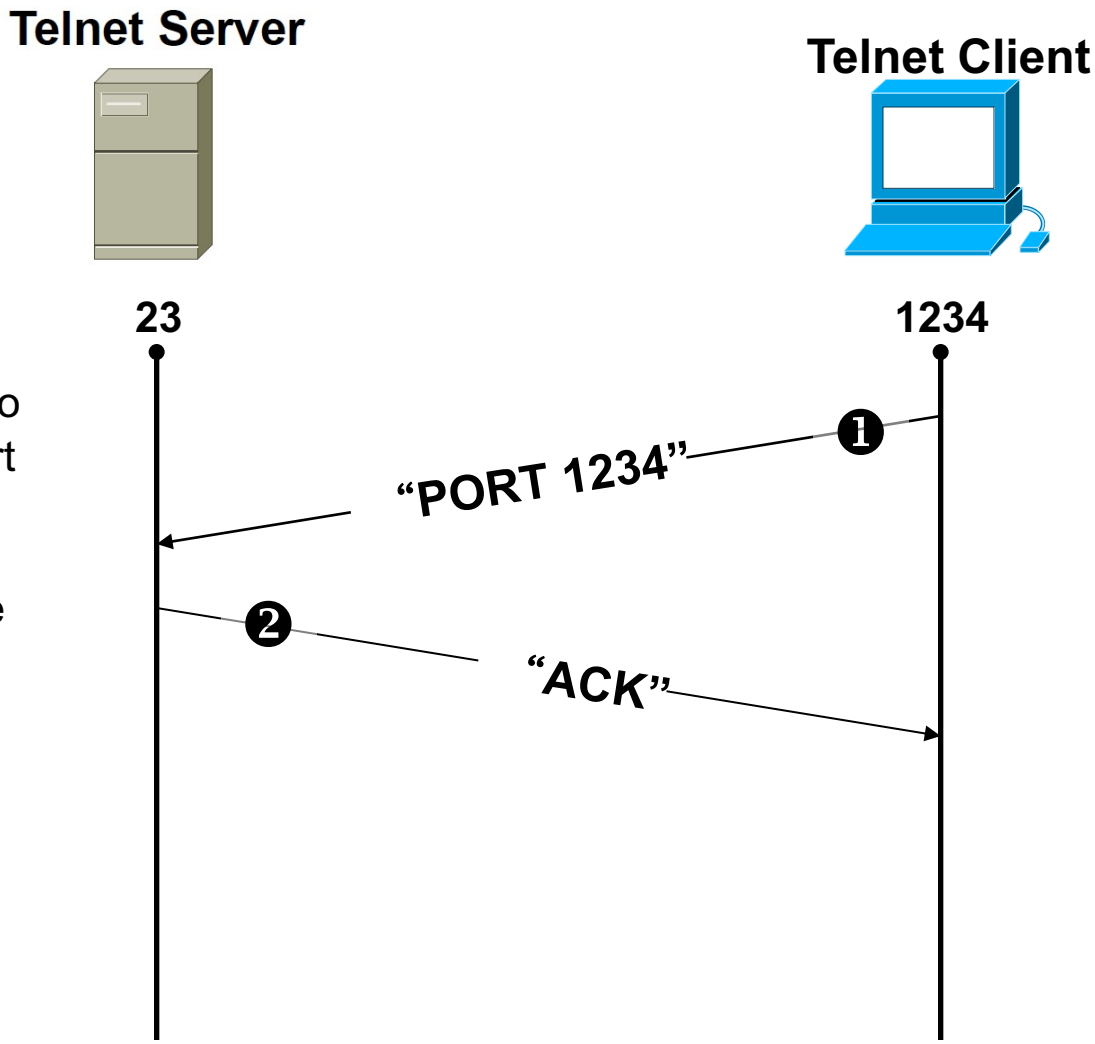
  => No state information saved across multiple packets
- Typically, incoming traffic with Dest. Ports > 1023 is permitted to allow returning TCP traffic for the clients behind the firewall
- If dynamic protocols, Netmeeting, Real-audio etc, are in use, *entire ranges of ports must be allowed* for the protocol to work.



# Telnet

❶ Client opens channel to server; tells server its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets.

❷ Server acknowleges.



# Sample Packet Filtering Rules

| | Source Address | Source Port | Destination Address | Destination Port | Action | Description |
|---|---|---|---|---|---|---|
| 1 | Any | Any | 192.168.1.0 | > 1023 | Allow | Rule to allow return TCP Connections to internal subnet |
| 2 | 192.168.1.1 | Any | Any | Any | Deny | Prevent Firewall system itself from directly connecting to anything |
| 3 | Any | Any | 192.168.1.1 | Any | Deny | Prevent External users from directly accessing the Firewall system. |
| 4 | 192.168.1.0 | Any | Any | Any | Allow | Internal Users can access External servers |
| 5 | Any | Any | 192.168.1.2 | SMTP | Allow | Allow External Users to send email in |
| 6 | Any | Any | 192.168.1.3 | HTTP | Allow | Allow External Users to access WWW server |
| 7 | Any | Any | Any | Any | Deny | "Catch-All" Rule - Everything not previously allowed is explicitly denied |

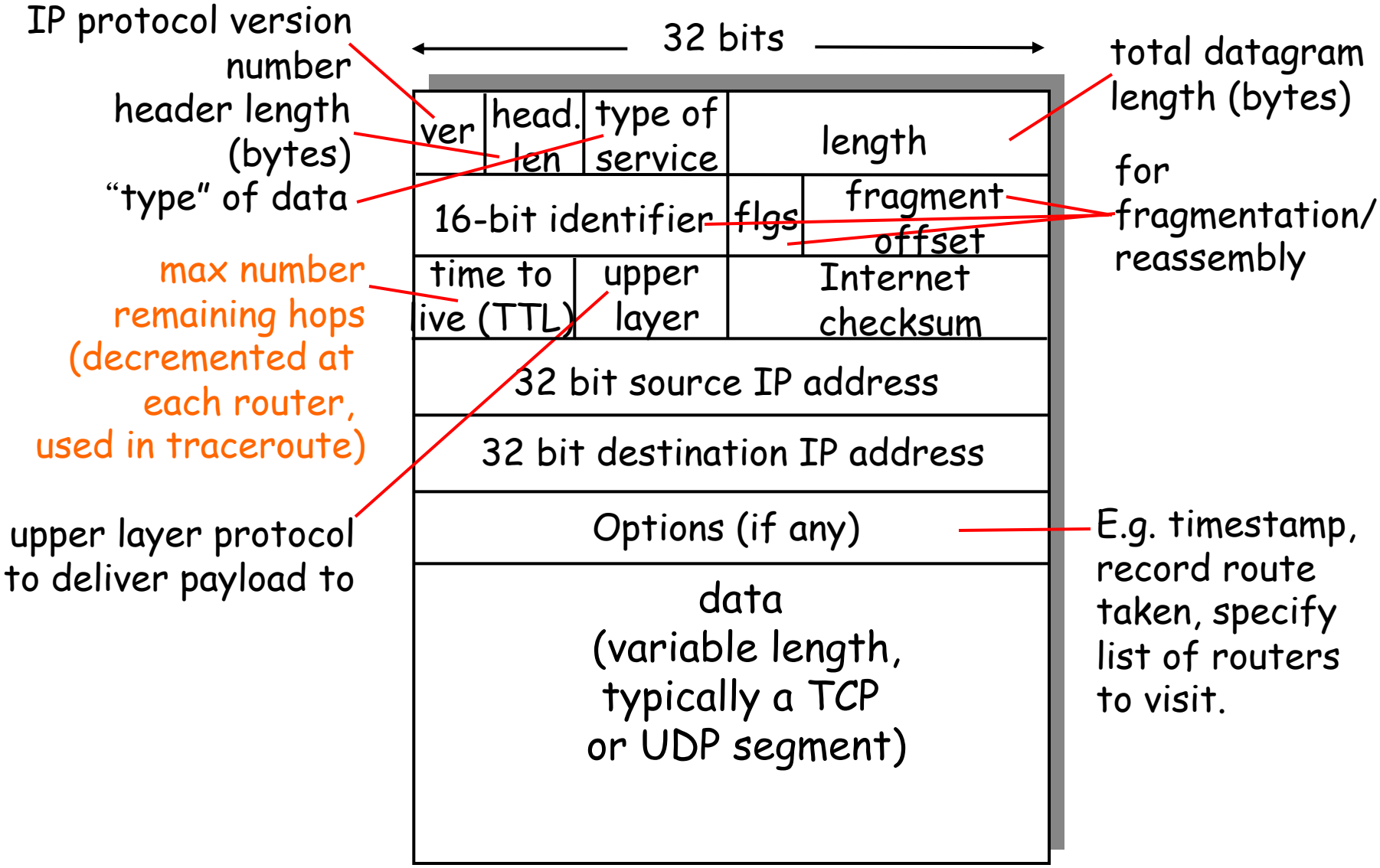
# Packet Filtering

- *Advantage:* simple, transparent and very fast
- *Disadvantage:*
  - difficulty in setting up rules correctly
  - Require to open all ports > 1023 for incoming traffic, especially, in order to support dynamic protocols

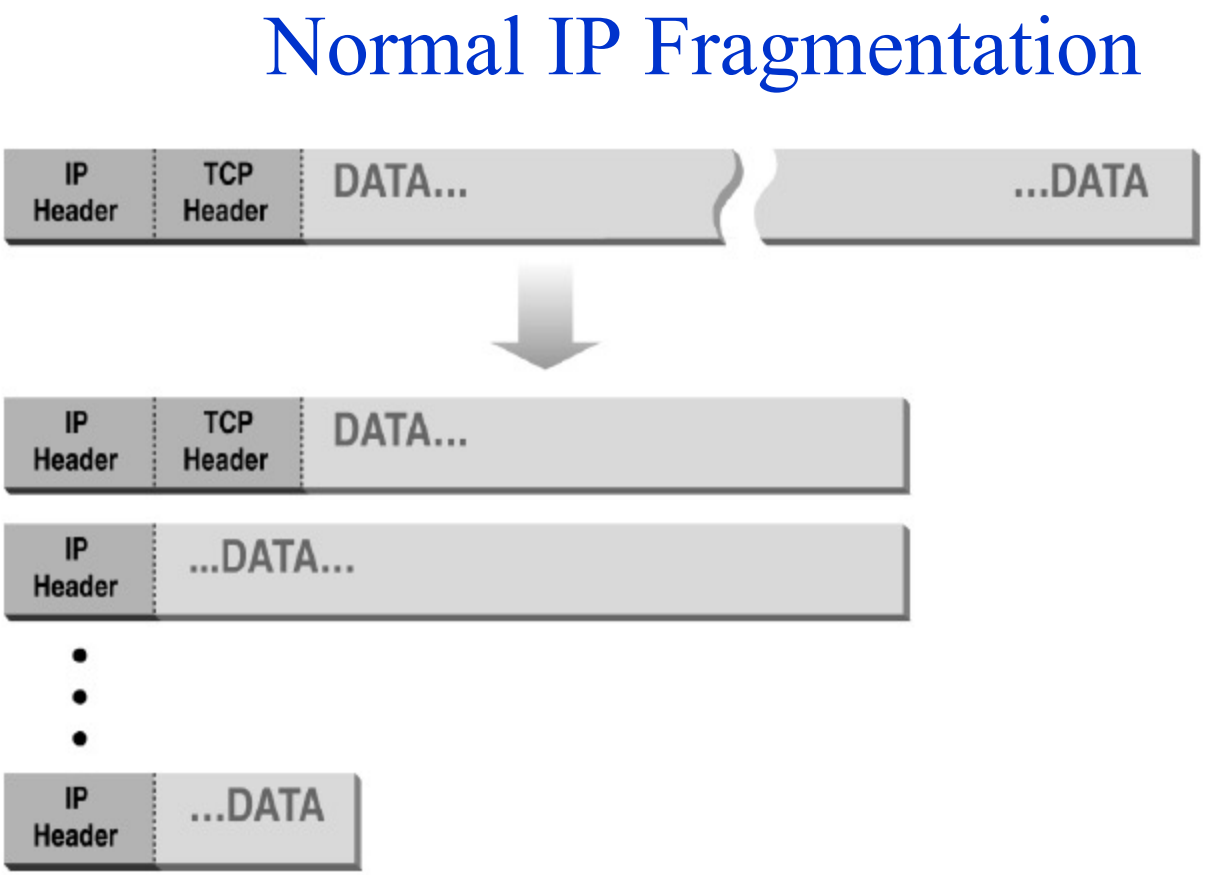
# Packet Filtering Attacks

- IP address spoofing – packets from the outside have internal addresses in their source IP address field
- Source routing attacks – route of packet is specified to bypass security measures
- Tiny fragment attack – designed to circumvent filtering rules that depend on TCP header information

# Recap: IP datagram format

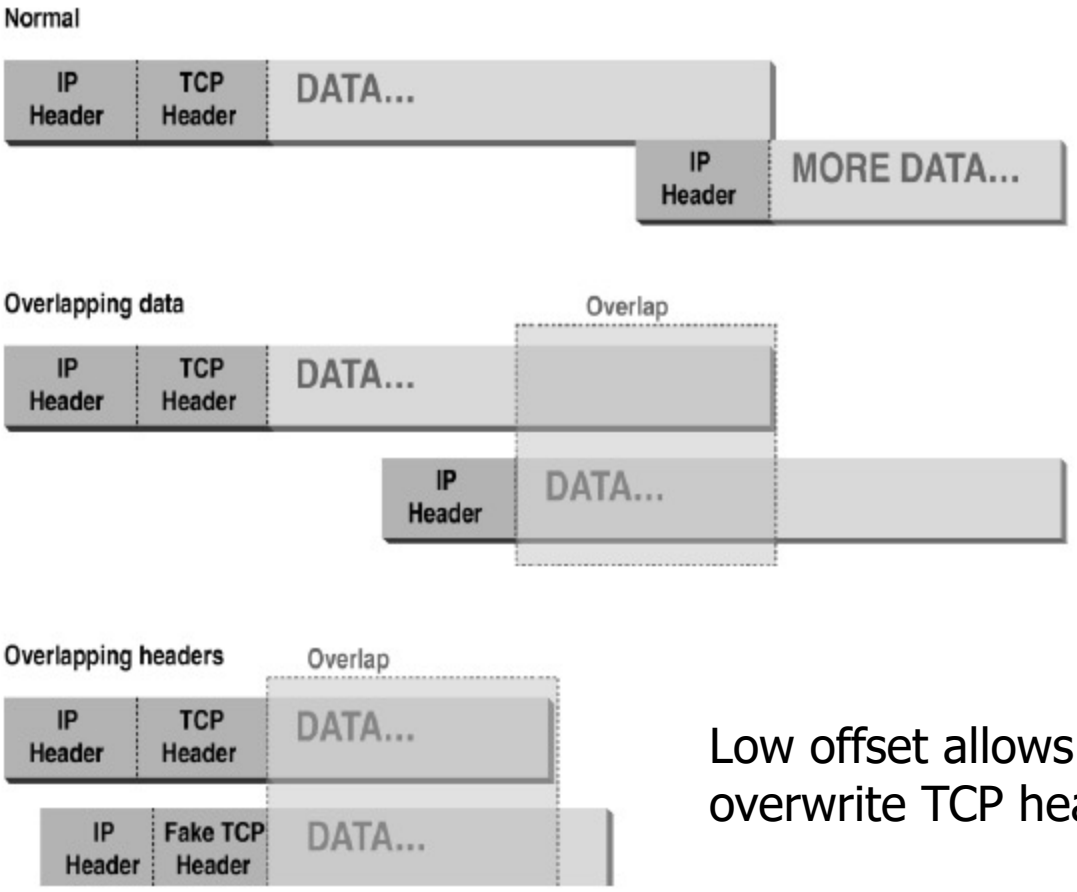


Complication for firewalls




Flags and offset inside IP header indicate packet fragmentation

# Abnormal Fragmentation




Low offset allows second packet to overwrite TCP header at receiving host

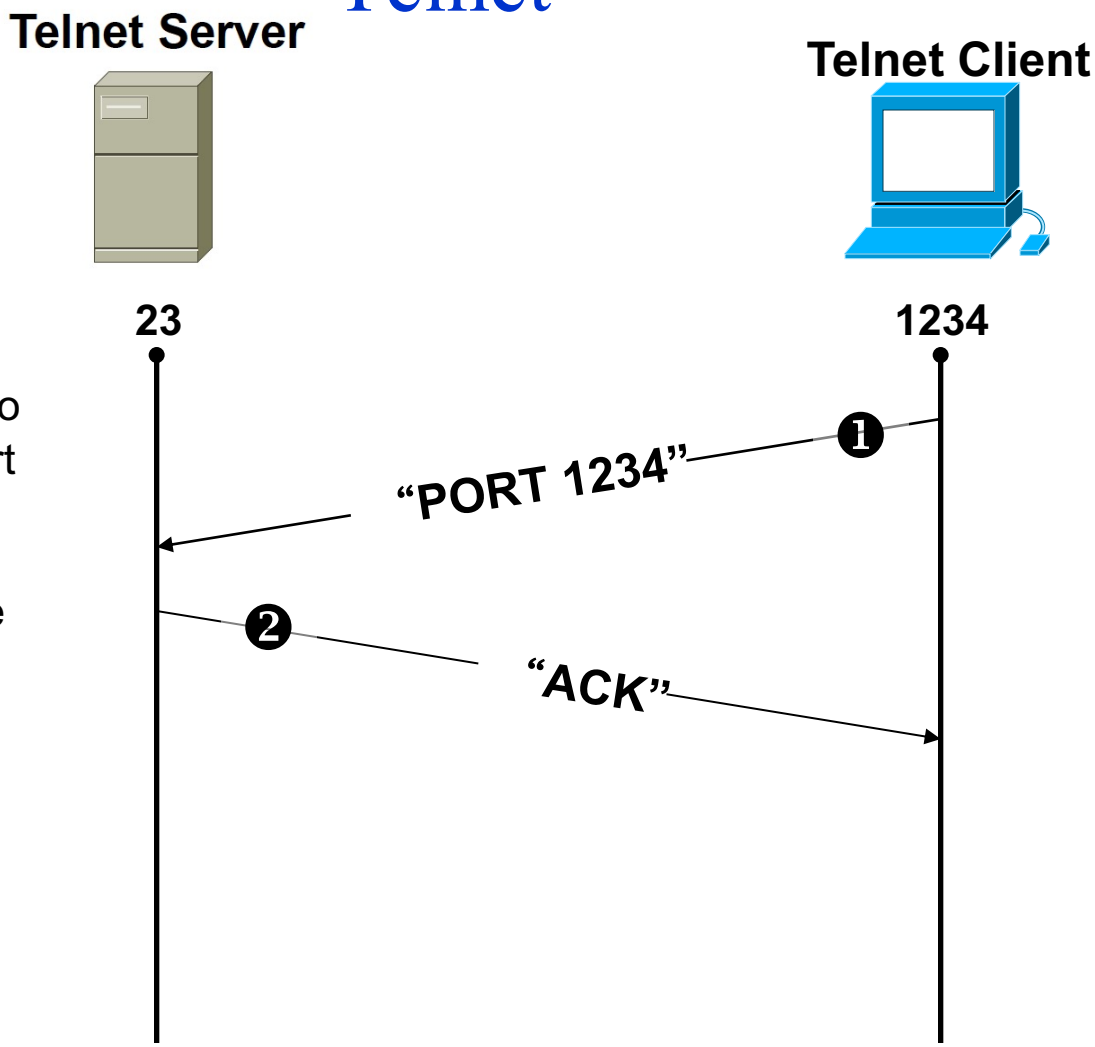
# Packet Fragmentation Attack

- Firewall configuration
  - TCP port 23 is blocked but SMTP port 25 is allowed
- First packet
  - Fragmentation Offset = 0.
  - DF bit = 0 : "May Fragment"
  - MF bit = 1 : "More Fragments"
  - Destination Port = 25. TCP port 25 is allowed, so firewall allows packet
- Second packet
  - Fragmentation Offset = 1: second packet overwrites all but first 8 bits of the first packet
  - DF bit = 0 : "May Fragment"
  - MF bit = 0 : "Last Fragment."
  - Destination Port = 23. Normally be blocked, but sneaks by!
- What happens
  - Firewall ignores second packet “TCP header” because it is fragment of first
  - At host, packet reassembled and received at port 23

# Stateful Inspection

- Packet decision made in the context of a connection
- If packet is a new connection, check against security policy
- If packet is part of an existing connection, match it up in the state table & update table
- Mainly to handle Inbound connections above port 1023
- Solve this problem by creating a directory of outbound TCP connections, along with each session's corresponding high-numbered client port
- State Table - used to validate any inbound traffic.
- Some commercial stateful firewalls do keep even more sophisticated state-info tracking, e.g.
  - track the ongoing port no. negotiations for some applications such as streaming channels for H.323 video conferencing or data-connection of FTP, to open/close the necessary ports in the firewall dynamically

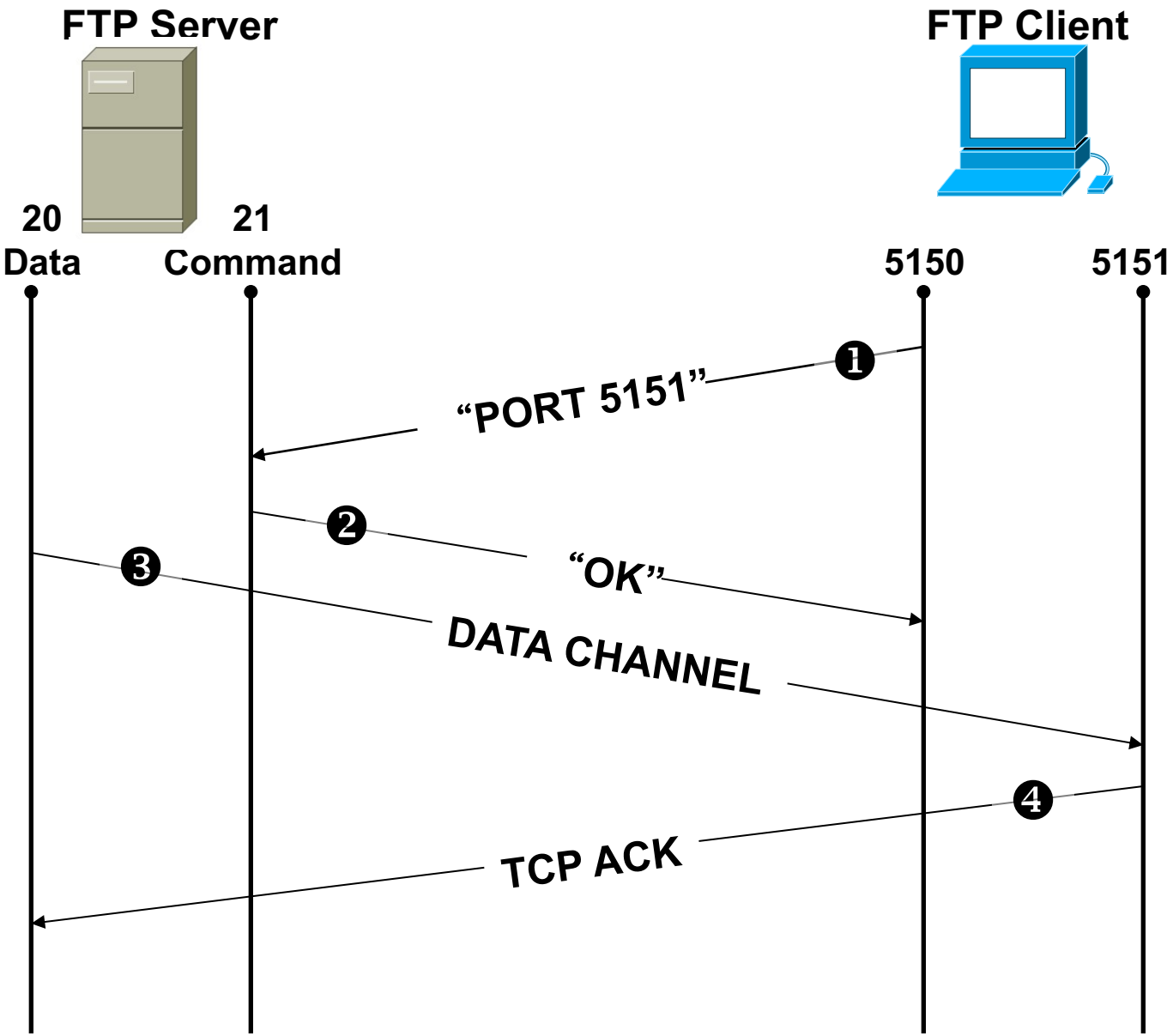
# Telnet




❶ Client opens channel to server; tells server its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets.

❷ Server acknowleges.

# FTP




❶ Client opens command channel to server; tells server second port number.

❷ Server acknowleges.

❸ Server opens data channel to client's second port.

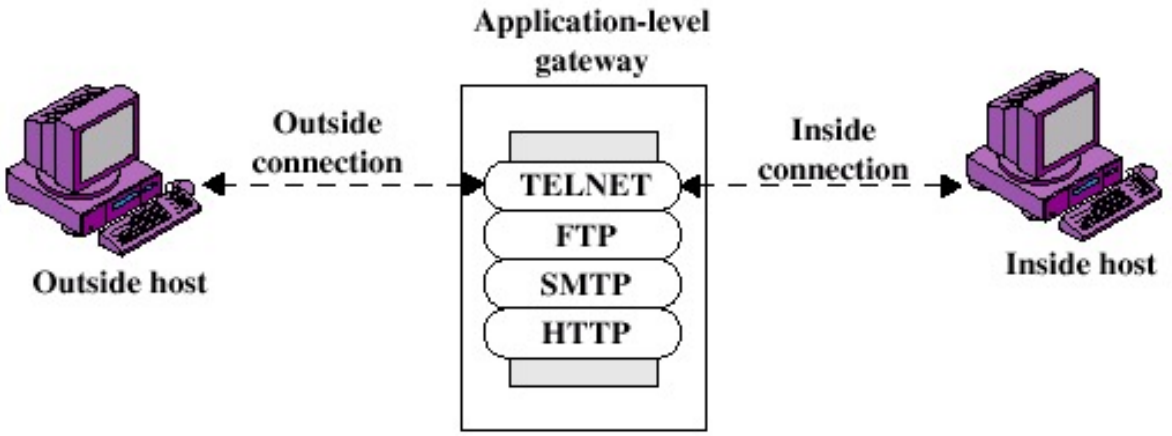
❹ Client Acknowledges.

# Stateful Inspection

- More secure because the firewall tracks client ports individually rather than opening all high-numbered ports for external access.
- Adds Layer 4 or Higher awareness to the standard packet filter architecture.
- Useful or applicable only within TCP/IP network infrastructures
- Superset of packet filter firewall functionality
- The more state-info is tracked, the bigger the challenge for support high speed communications link

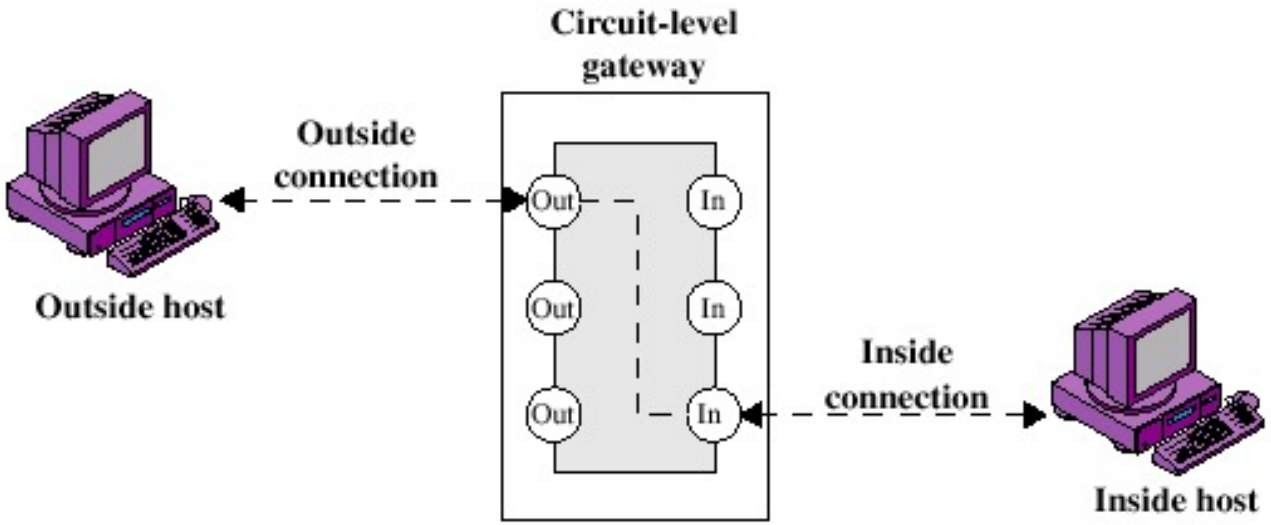
# Application Level Gateway

- Acts as a relay of application level traffic
- Also called a proxy
- User contacts gateway for TELNET to remote host, user is authenticated, then gateway contacts remote host and relays info between two end points
- Can examine the packets to ensure the security of the application – full packet awareness
- Very easy to log since entire packet seen
- *Disadvantage:* additional processing overhead for each connection – increase load, and slow



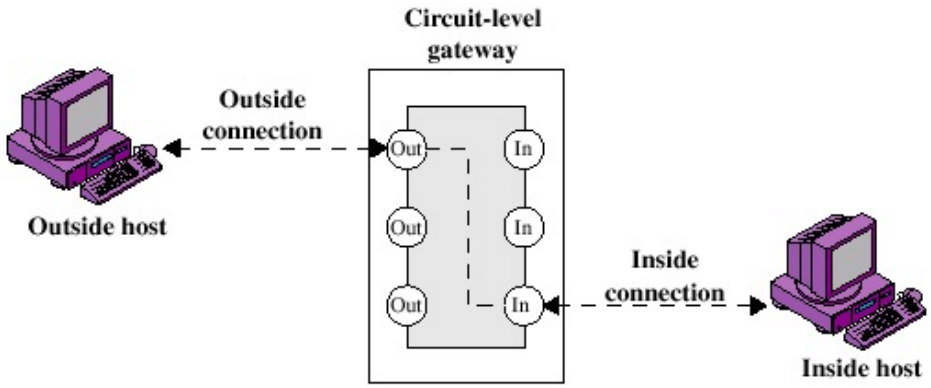
# Circuit Level Gateway

- *Does not* permit an end-to-end TCP connection
- Sets up *two TCP connections* one between itself and a TCP user on the inside and one between itself and a TCP user on the outside
- *Relays TCP segments* from one connection to the other without examining the contents
- *Security function* (implements policy) determines which connections will be allowed
- Used where *internal users are trusted* for all outbound services
- Often *combined with a proxy* for inbound services

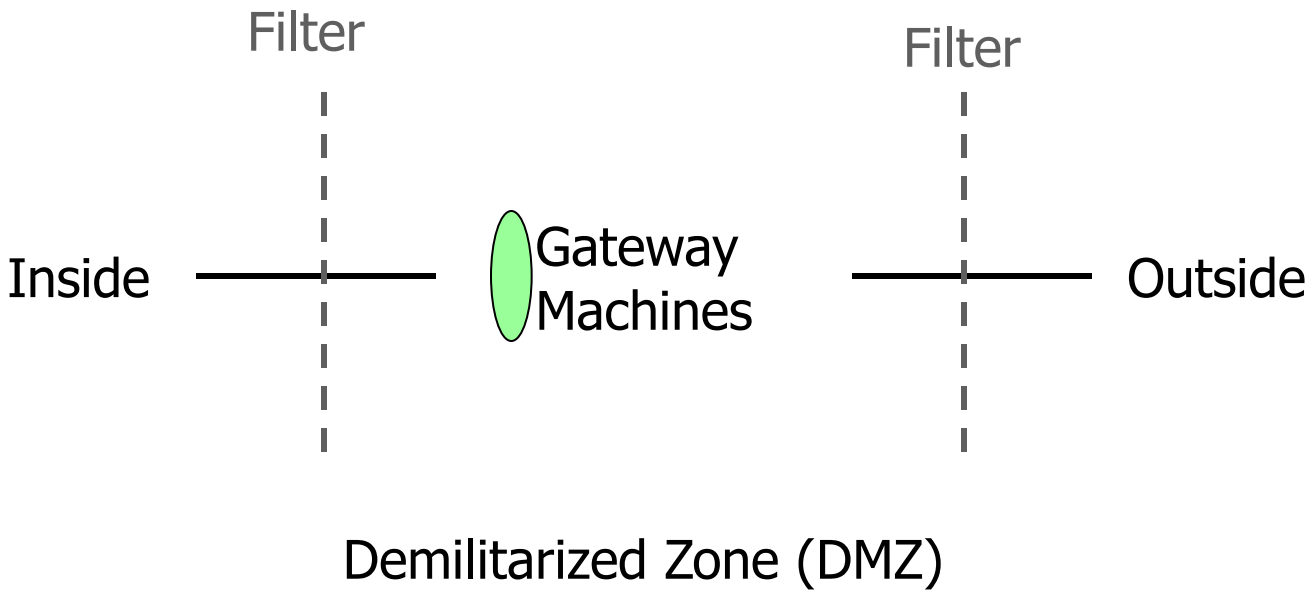


# Circuit Level Gateway

- Support more services than Application-level Gateway
- Less control over data
- Hard to handle dynamic protocols like FTP
- Clients must be aware they are using a circuit-level proxy
  - some implementations require a special client, e.g. requires *SOCKS-ified client*
- Protect against fragmentation problem
- **SOCKS** package V5 – RFC 1928
  - Uses port 1080



# Abstract view of a Typical Secure Perimeter



# Real Life Example

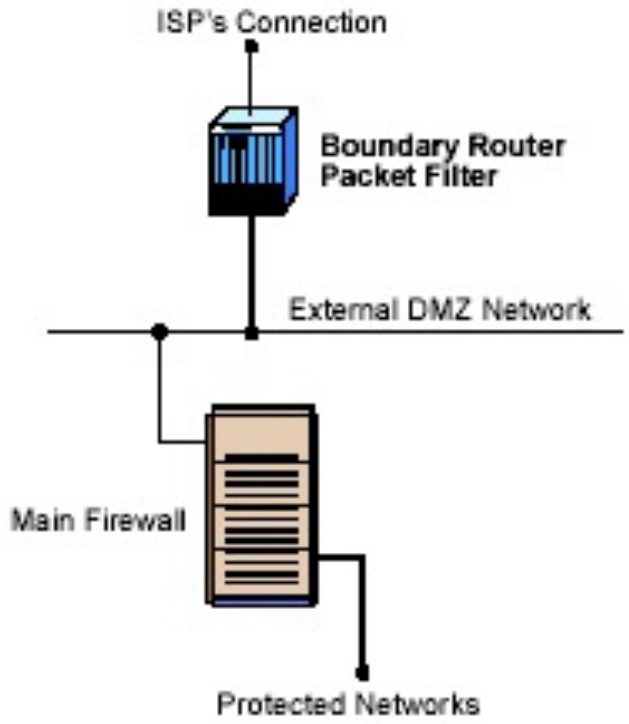
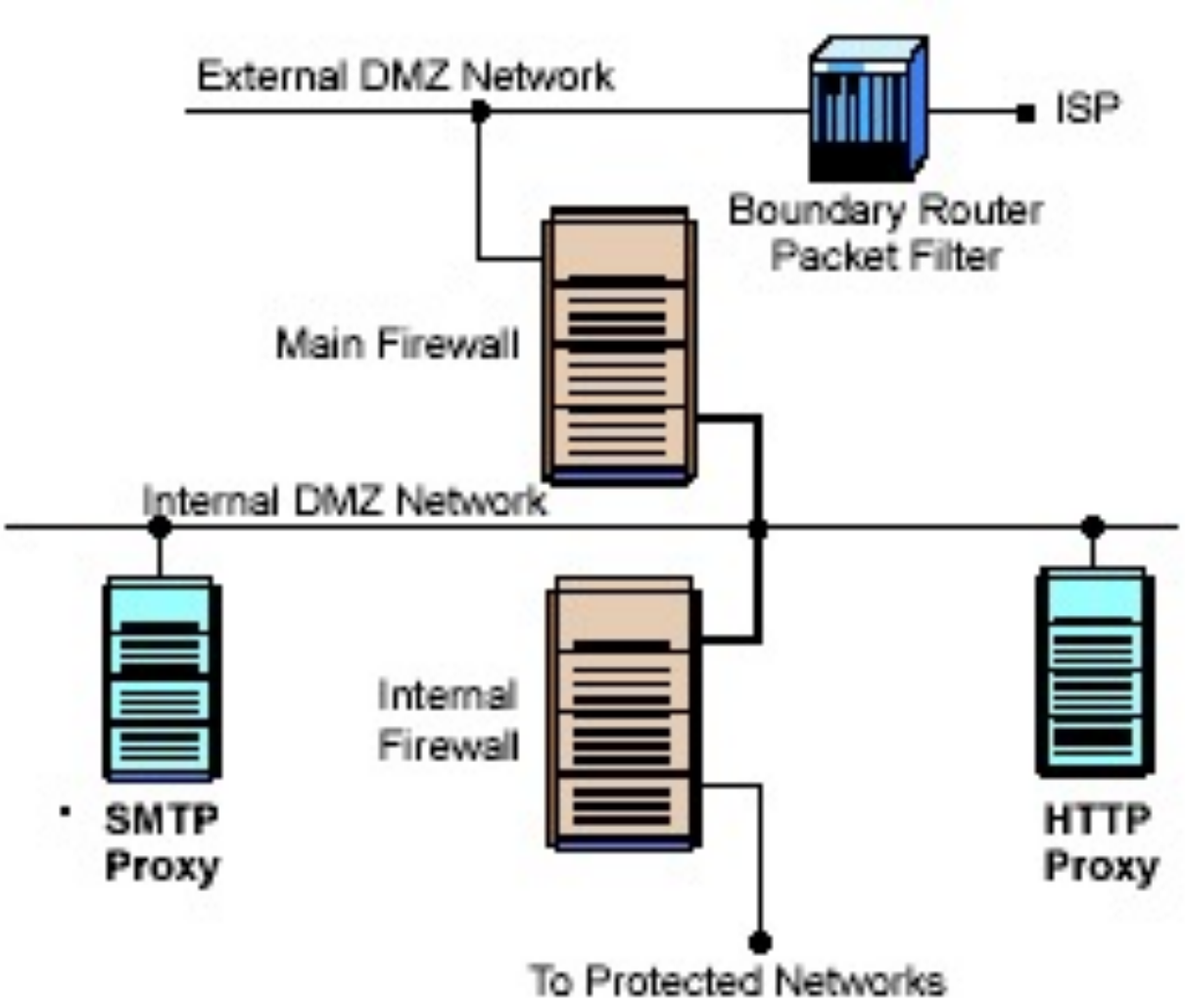



**Figure 2.4: Packet Filter used as Boundary Router**

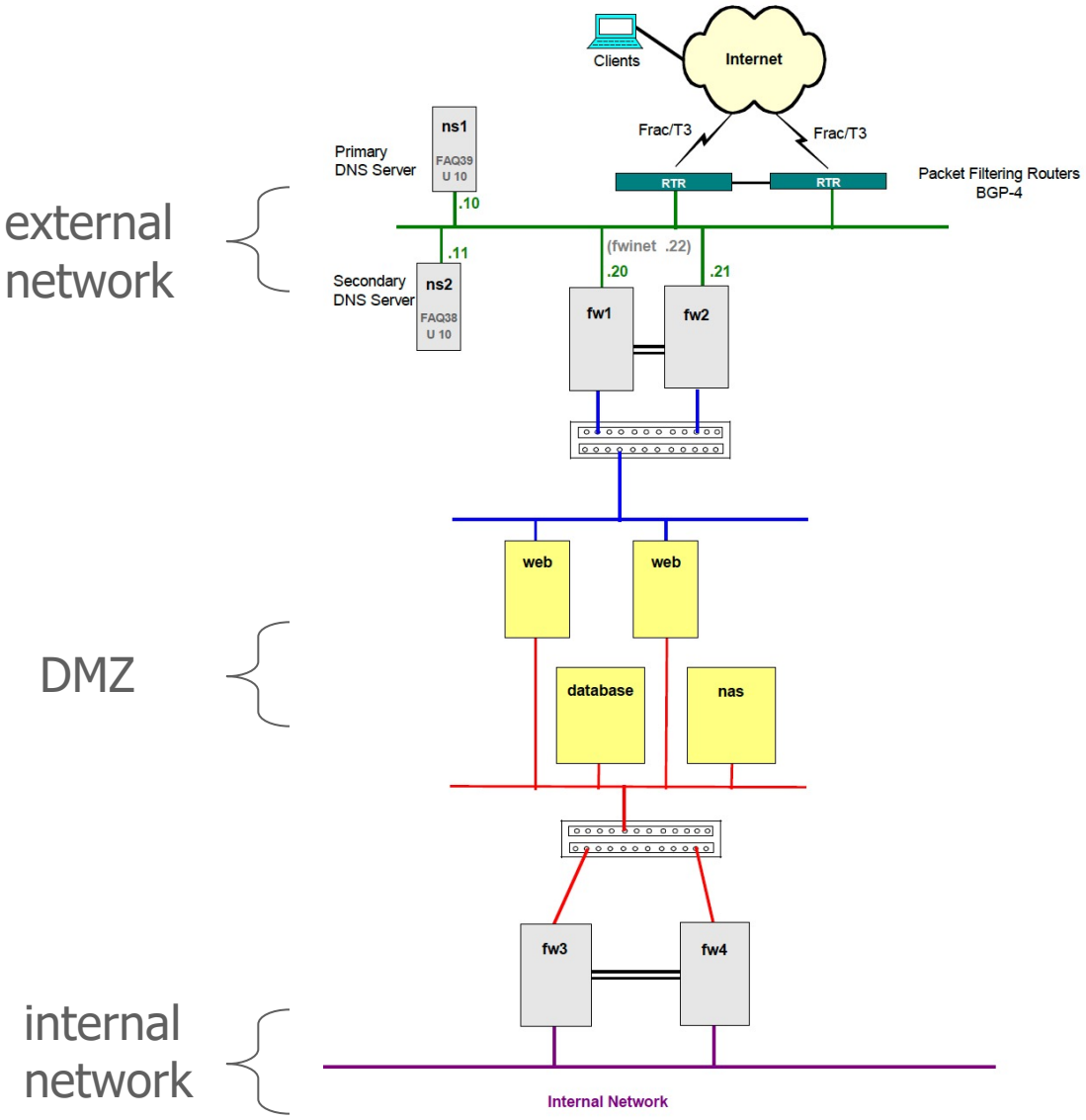
# Dedicated Proxy Servers



# Hybrid Firewalls

- "blurring of lines" that differentiate types of firewalls
- Application proxy gateway firewall vendors have implemented basic packet filter functionality in order to provide better support for UDP based applications
- Stateful inspection packet filter firewall vendors have implemented basic application proxy functionality to offset some of the weaknesses associated with packet filtering

# Typical DMZ


external network
DMZ
internal network
Clients
Internet
Frac/T3
Frac/T3
Primary DNS Server
ns1
FAQ39 U 10
.10
RTR
RTR
Packet Filtering Routers BGP-4
.11
(fwinet .22)
.20
.21
Secondary DNS Server
ns2
FAQ38 U 10
fw1
fw2
web
web
database
nas
fw3
fw4
Internal Network

# DMZ Building Guidelines

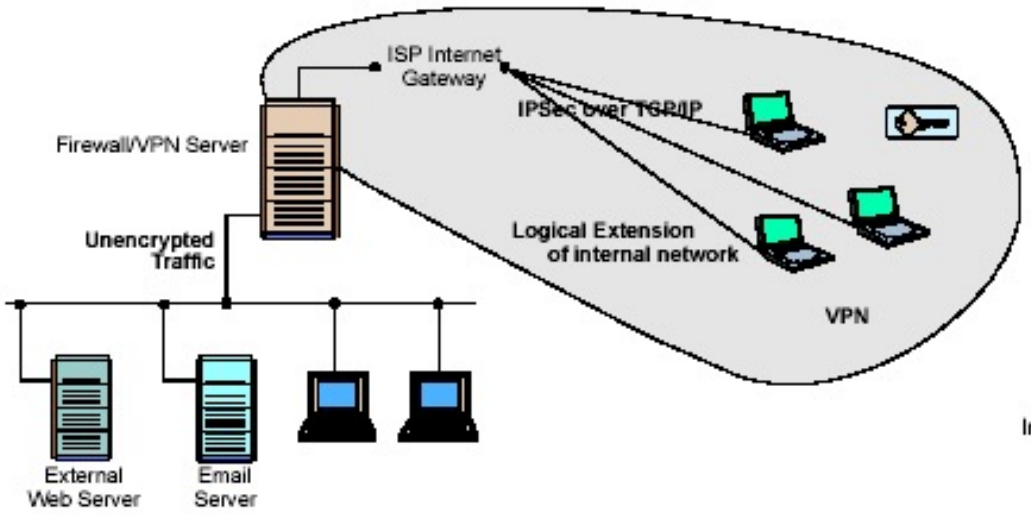
- Keep It Simple - KISS principle - the more simple the firewall solution, the more secure and more manageable
- Use Devices as They Were Intended to Be Used – don't make switches into firewalls
- Create Defense in Depth – use layers, routers and servers for defense
- Pay Attention to Internal Threats – "crown jewels" go behind internal firewall – remember: "all rules are meant to be broken"

# Other Types Of Firewalls

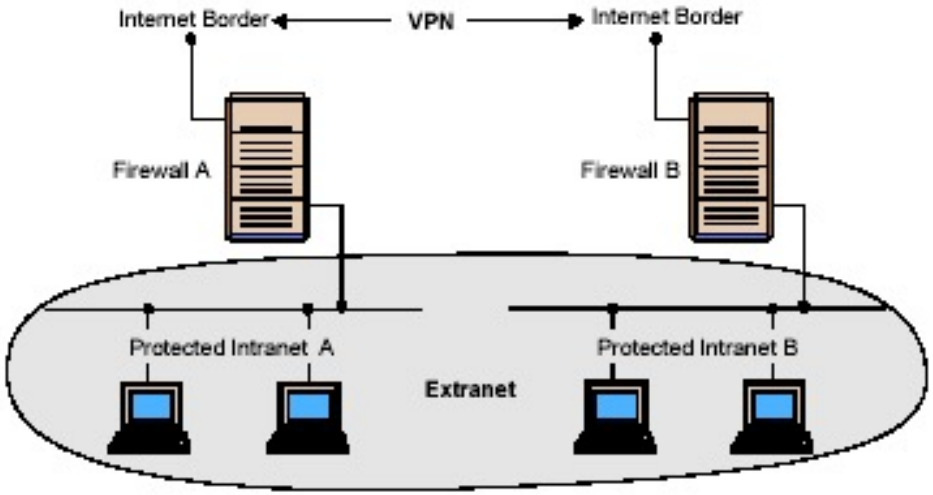
- Host Based Firewalls – comes with some operating systems (LINUX, WIN/XP), e.g.
  - Zone alarm
  - Freeware from Computer Associates


- Personal Firewalls Appliances – personal firewall appliances are designed to protect small networks such as networks that might be found in home offices
  - Provide: print server, shared broadband use, firewall, DHCP server and NAT
- Avoids Crunchy Cookie Syndrome – hard and crunchy on the outside, soft and chewy on the inside

# Virtual Private Networks (VPNs)




**Connecting remote users across the Internet**




**Connecting offices across Internet**

More details when we talk about IPSec

# Intrusion Detection Systems (IDS)

- A monitor system (mostly passive/listen-only) for system/network behavior and sends warnings/alarm if possible intrusions are detected


  - e.g. Snort is a very popular and powerful public-domain IDS http://www.snort.org
  - Some commercial firewalls do provide *limited* IDS capabilities
- Network-based IDS Vs. Host-based IDS
  - Network-based IDS monitors (sniffs at) the network traffic to find hints of intrusions/abuse/attacks
  - Host-based IDS, typically a piece of software running on the monitored host, monitors the end-system behavior, e.g. system call usage/ sequences, disk access, CPU utilization pattern etc, to find hints of intrusions/abuse/attacks

# Intrusion Detection Systems (IDS) (cont'd)

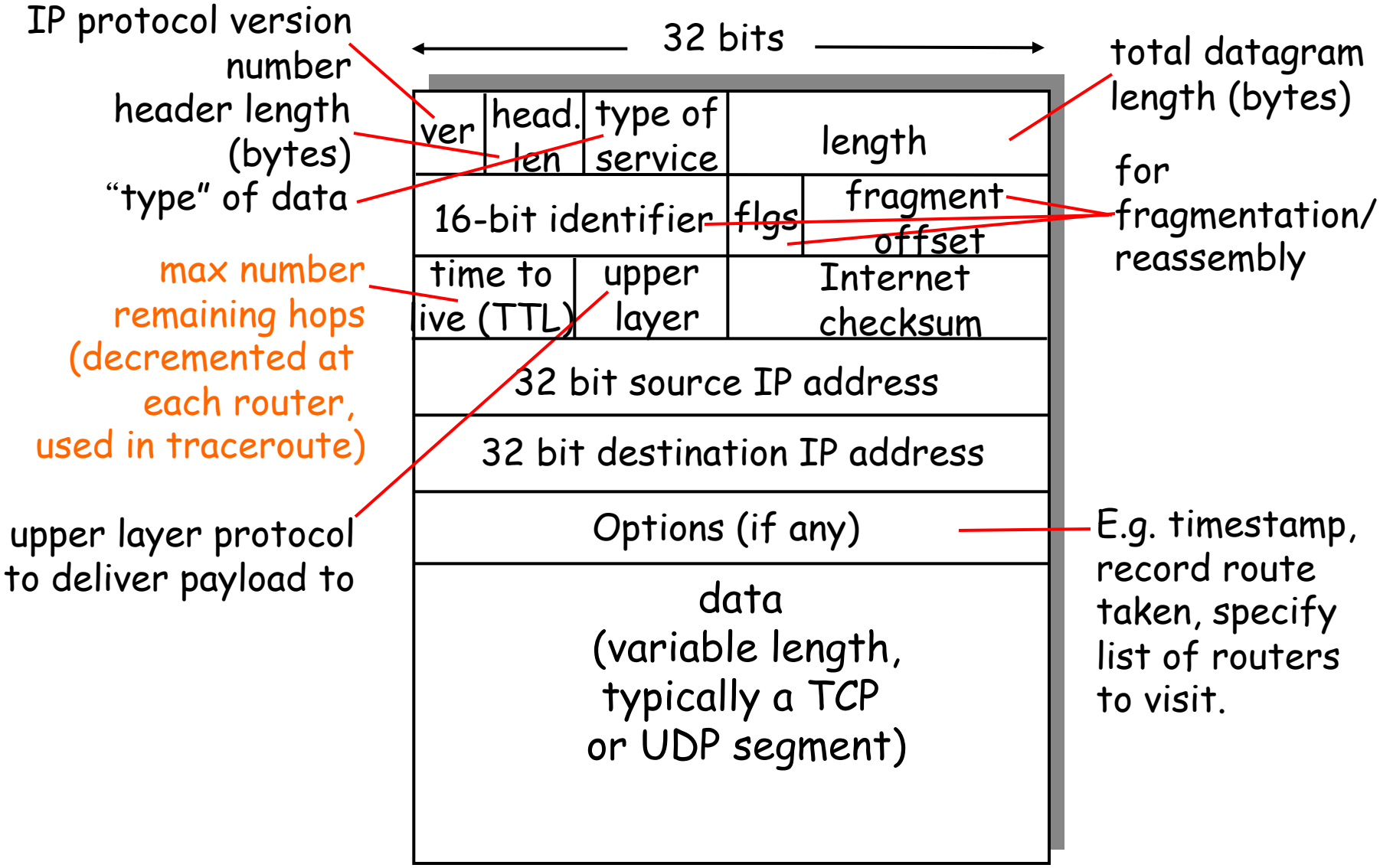
- Anomaly-based Vs. Signature-based
  - Anomaly-based IDSs compare the current "behavior" with a nominal profile of system/network
    - Can detect never-seen-before (zero-day threat) of intrusions
    - The challenge is to decide what is "normal" – need to balance between false +ve and false –ve rate
  - Signature-based IDSs compare the observed packets/system calls/commands with a database of known attack packet/system call signatures
    - Less prone to false positive but require update of signature database all the time and not effective to new attacks before new signatures are installed

# Intrusion Detection Systems (IDS) (cont'd)

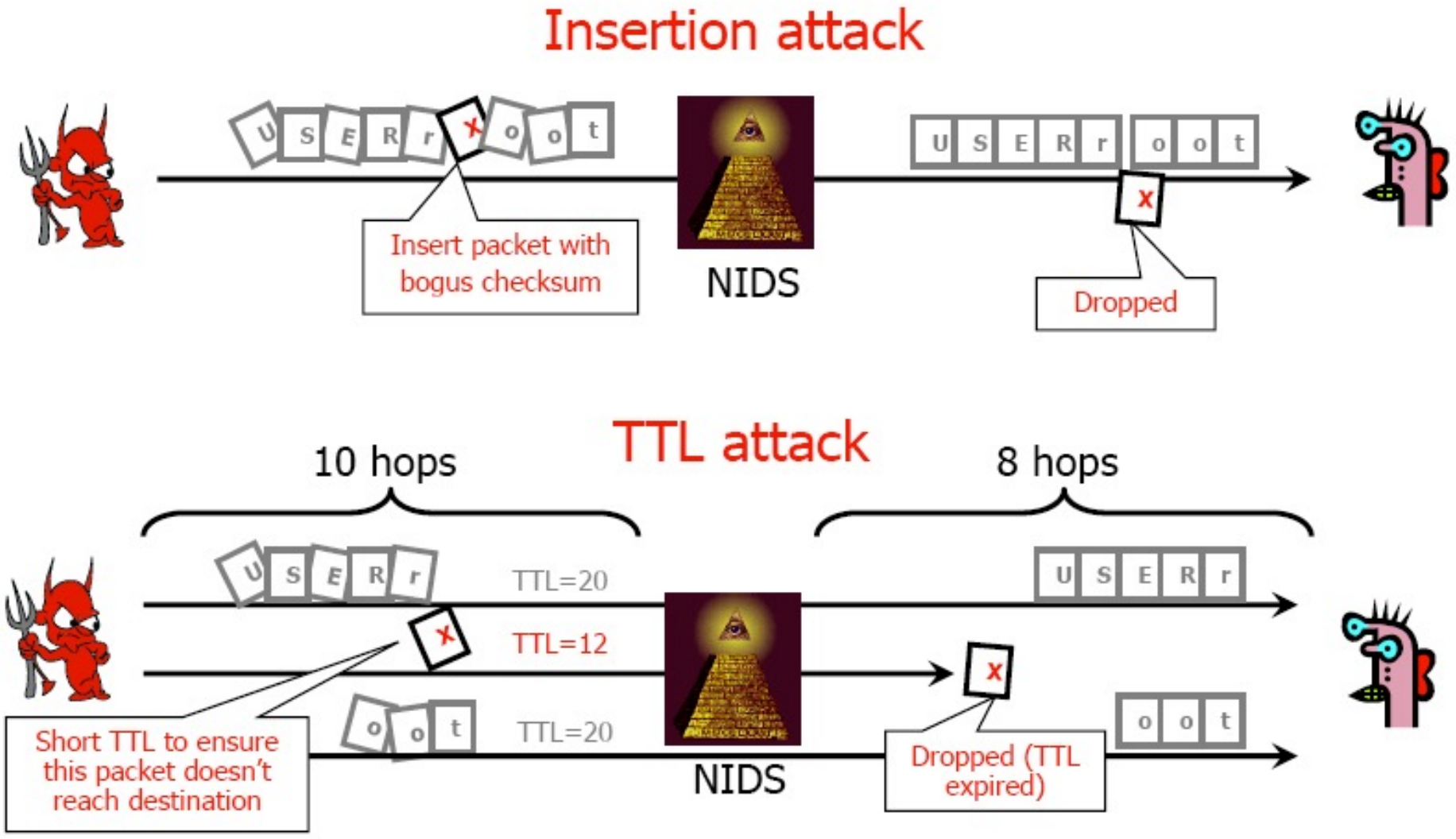
- For an IDS to be useful, the false +ve and false –ve rates must be kept to an acceptable limit
  - False +ve: an alarm is generated even when there is no intrusion
  - False –ve: fails to generate an alarm when there is an intrusion
- IDS evasive techniques include:
  - Flooding
  - Fragmentation (e.g. break an TCP segment into multiple IP fragments)
  - Encryption
  - Obfuscation (disguise, use unicode or hex to encode special keywords )
- The industry trend is for IDSs to evolving towards the so-called Intrusion Protection System (IPS) which will act as a chokepoint of network traffic or intercept system-calls within a host/OS, and take active actions, e.g. discard attacking packets, when an intrusion is identified

⇒ Further blurring the lines between Firewalls and IDSs

# Recap: IP datagram format



# IDS Evasion


Insertion attack
U S E R r X o o t
Insert packet with bogus checksum
NIDS
U S E R r o o t
X
Dropped
TTL attack
10 hops
8 hops
U S E R r
TTL=20
X
TTL=12
o o t
TTL=20
Short TTL to ensure this packet doesn't reach destination
NIDS
X
Dropped (TTL expired)
U S E R r
o o t

# A Typical Multi-tiered Web Site Architecture