VPN,

IPSEC, &

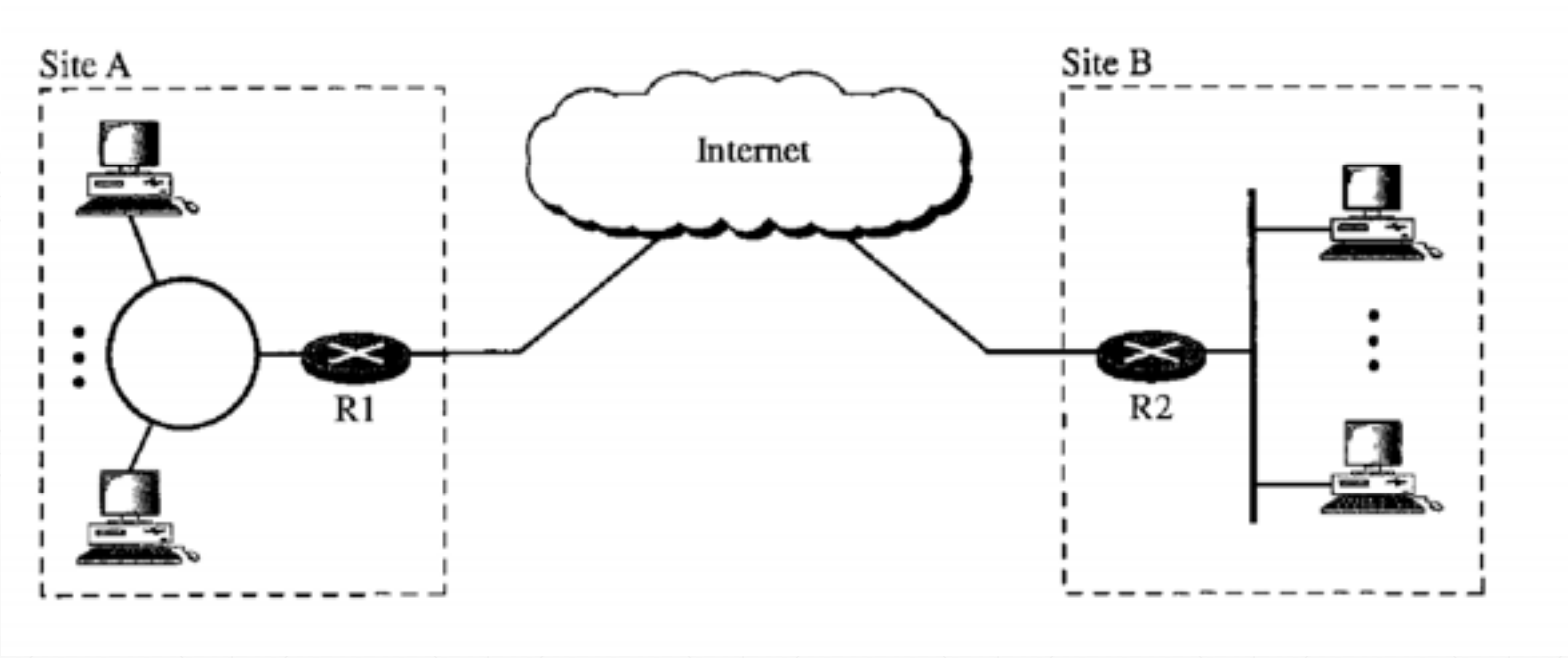
FIREWALL.

Usman Zafar (CT-063)
Ibad Ahmed (CT-071)
Fahad Ali Khan (CT-304)

VPN

- A **VPN**, or **Virtual Private Network**, allows you to create a secure connection to another network over the Internet.

- These days VPNs are really popular, but not for the reasons they were originally created for.



Virtual Private Networks (VPNs)

- Service to access the internet SAFELY and PRIVATELY
- ROUTES our connection through a SERVER

- CHANGES IP Address
- ENCRYPTS data

- In very simple terms, a VPN connects your PC, smartphone, or tablet to another computer (called a server) somewhere on the internet, and allows you to browse the internet using that computer's internet connection. So if that server is in a different country, it will appear as if you are coming from that country, and you can potentially access things that you couldn't normally.

Why use VPNs?

You can use a VPN to:

- Bypass geographic restrictions on websites or streaming audio and video.
- Watch streaming media like Netflix and Hulu.
- Protect yourself from snooping on untrustworthy Wi-Fi hotspots.
- Gain at least some anonymity online by hiding your true location.
- Protect yourself from being logged while torrenting.

- Beside the role of creating a “private scope of computer communications,” VPN technology has many other advantages, for example; enhanced security. When you connect to the network through a VPN, the data is kept secured and encrypted. In this way, the information is away from the hackers' eyes.

IP SECURITY (IPSEC)

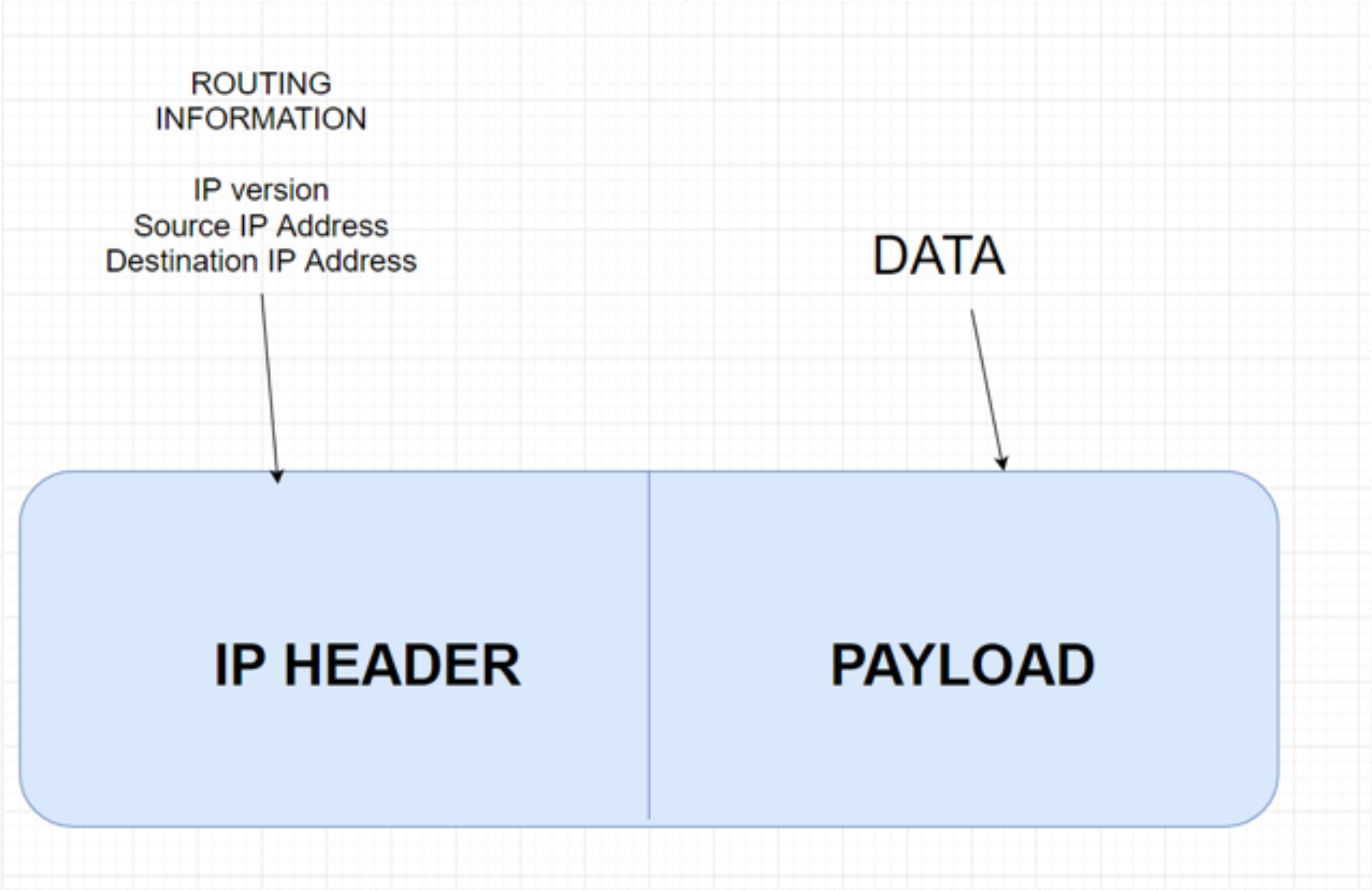
- Set of protocols to provide security for a packet at the NETWORK LEVEL
- IPSEC describes the framework for providing security at the IP layer, as well as the suite of protocols designed to provide that security, through authentication and encryption of IP network packets.
- It provides:
  - CONFIDENTIALITY by encrypting data
  - INTEGRITY by using algorithms like checksum or hashing
  - AUTHENTICATION by verifying identities
  - ANTI REPLAY PROTECTION by making sure all the packets aren’t duplicates

Uses of IPSEC

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunnelling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

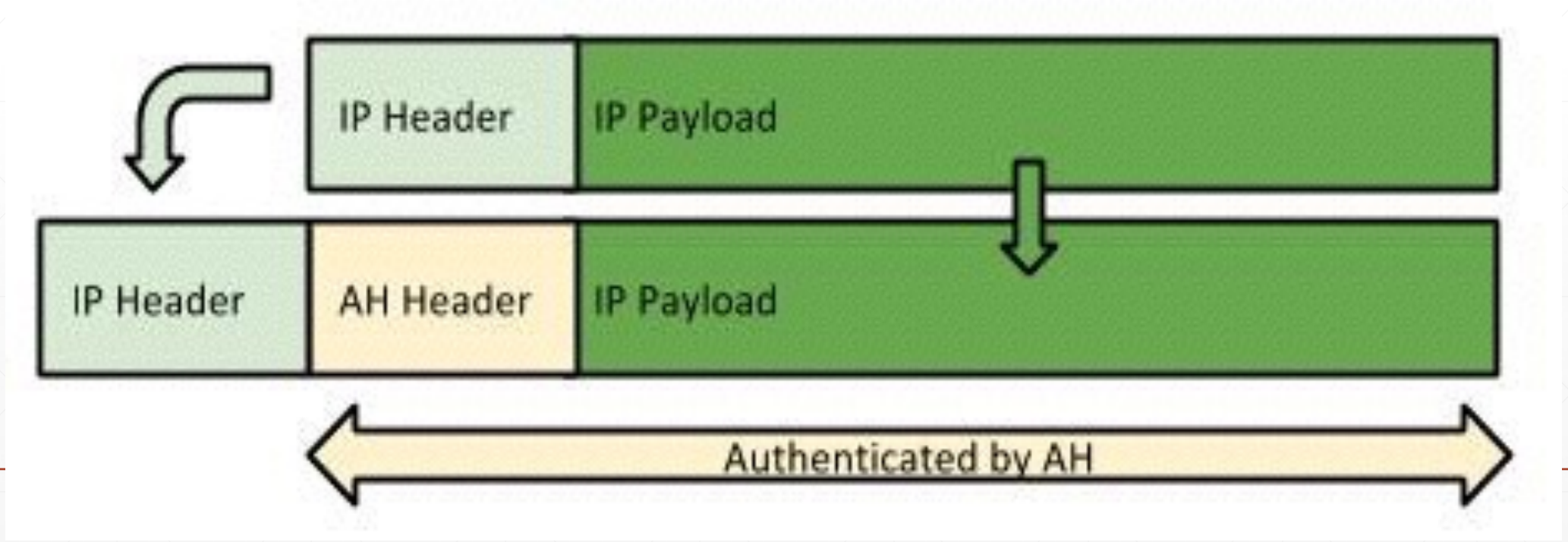
NORMAL PACKET WITHOUT IPSEC



MODES OF IPSEC

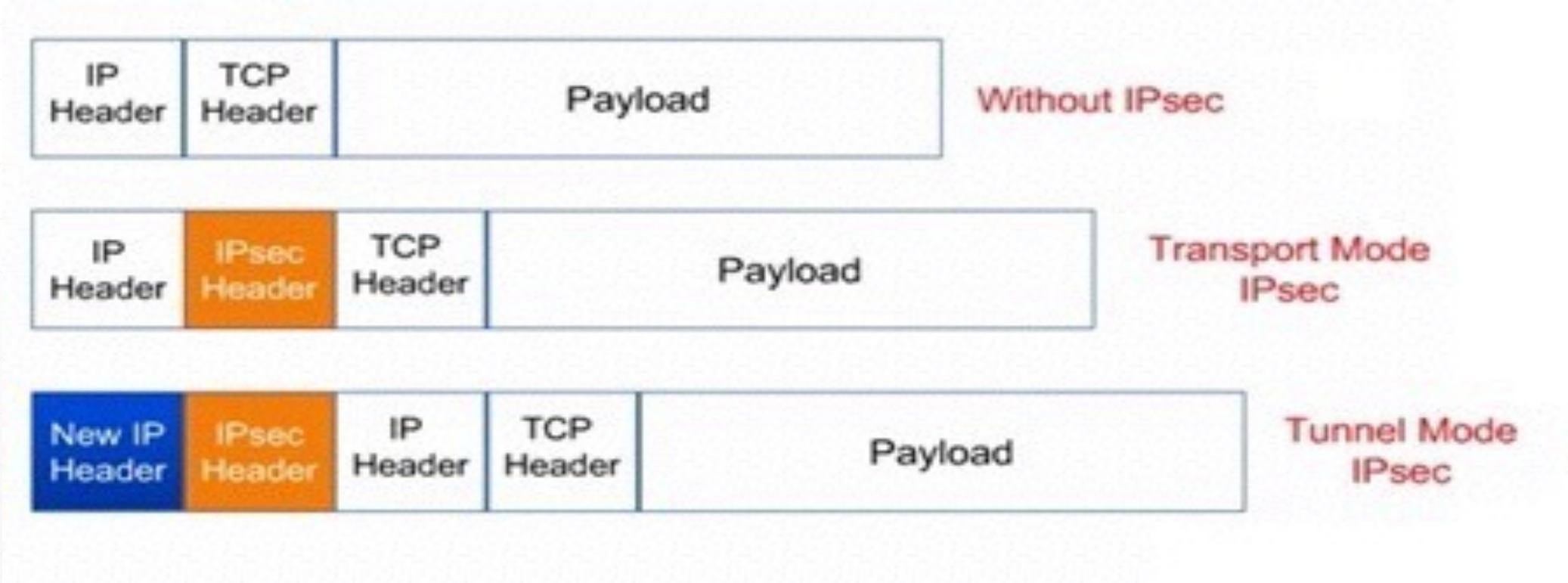
1. TRANSPORT MODE:

- ONLY the PAYLOAD is encrypted and IP header is left as it is
- Doesn’t protect the whole packet
- NEW IPSEC HEADER is added before the payload
- Used for END to END communication



2. Tunnel Mode:

- Entire packet is secured including the IP HEADER and PAYLOAD
- New IP HEADER is added to the packet
- VPNs are the practical application of tunnel mode



Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls have been a first line of defence in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.
- Device or Software installed BETWEEN the internal network and the internet to filter malicious packet or messages from entering the internal network.

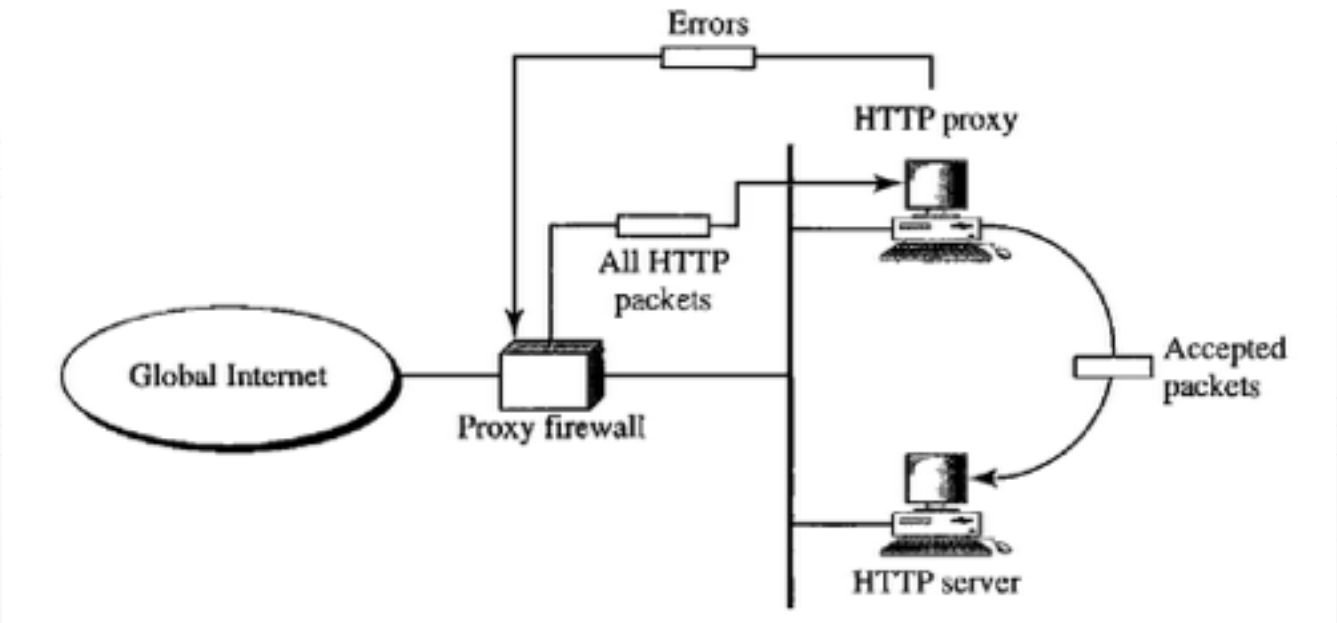
Types

Proxy firewall:

- An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application.
- Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network.
- However, this also may impact throughput capabilities and the applications they can support.

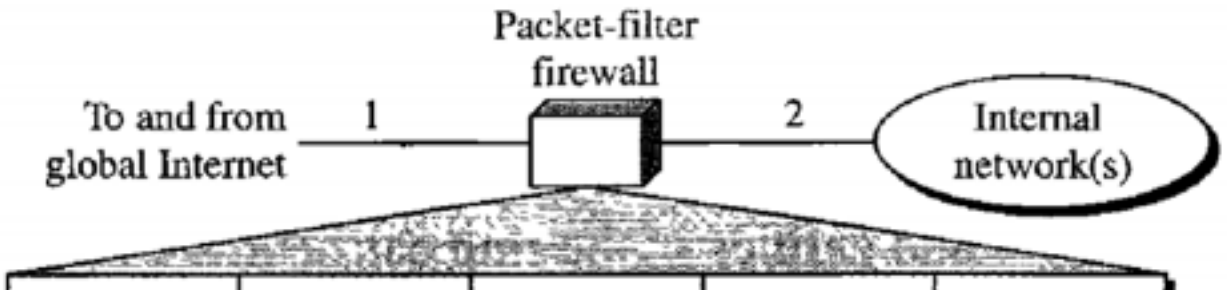
PROXY FIREWALL (contd.)

- Filtering is based on the information in the packets
- Proxy server opens the packets and see if the request is legitimate
- If the request are legitimate they are transferred to the actual server
- Else the requests are dropped



PACKET FILTER FIREWALL

- Here we filter packets based on :
  - IP Address of Source
  - IP Address of Destination
  - Source Port Address
  - Destination Port Address



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Next-generation firewall (NGFW)

- Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

- According to Gartner, Inc.'s definition, a next-generation firewall must include:
  - Standard firewall capabilities like stateful inspection
  - Integrated intrusion prevention
  - Application awareness and control to see and block risky apps
  - Upgrade paths to include future information feeds
  - Techniques to address evolving security threats

Thank You