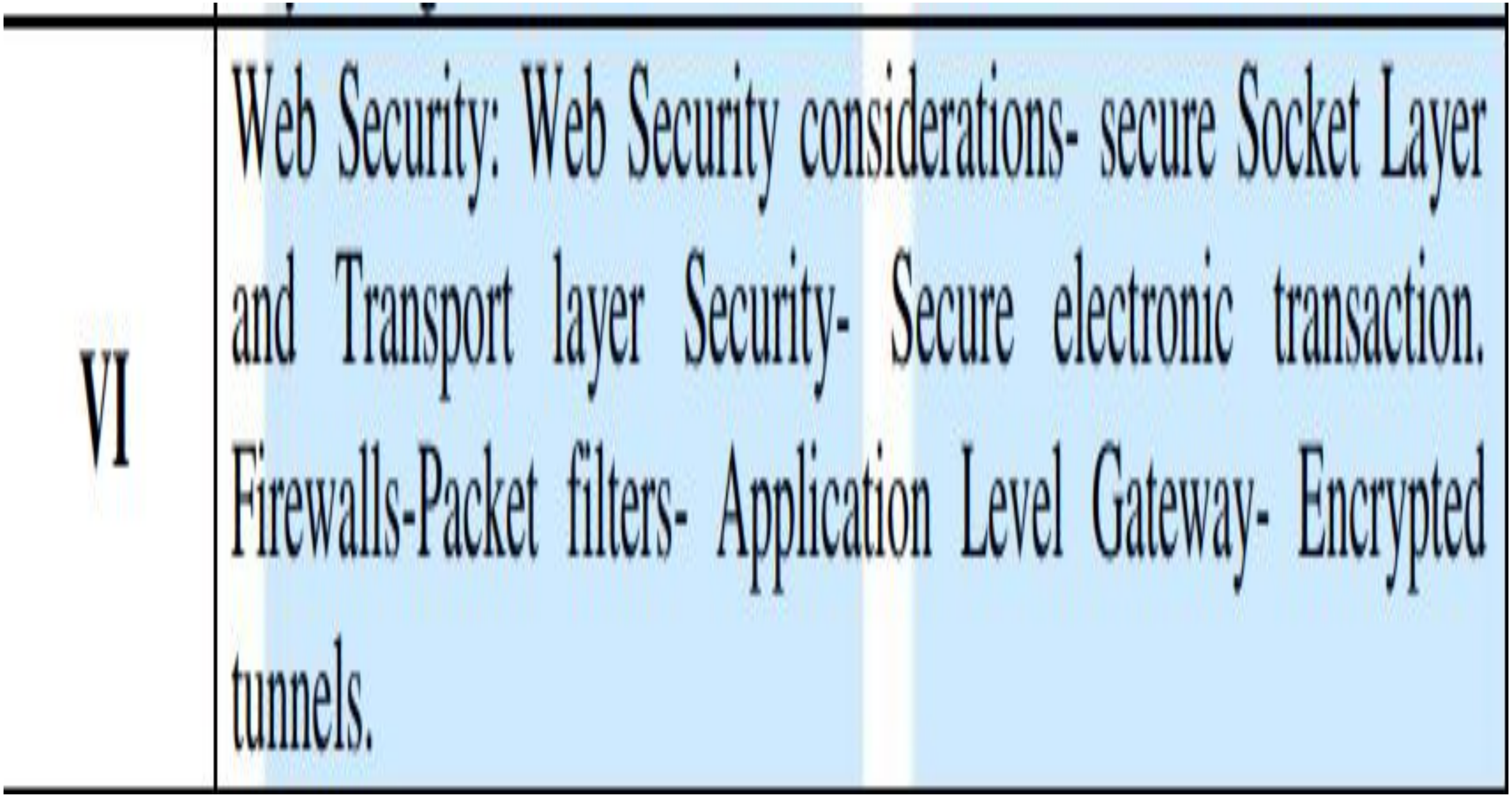
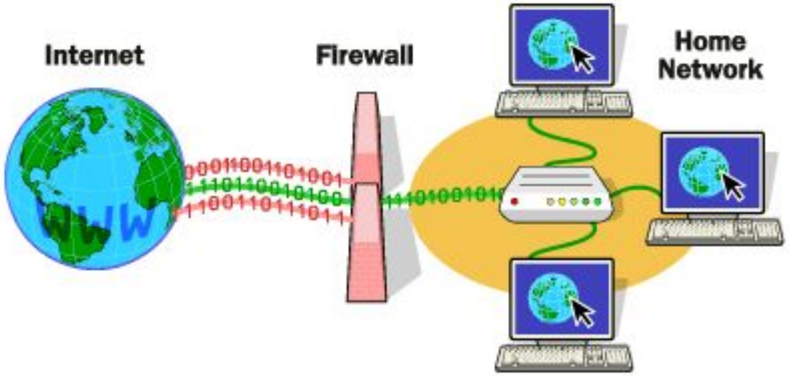


VI	Web Security: Web Security considerations- secure Socket Layer and Transport layer Security- Secure electronic transaction. Firewalls-Packet filters- Application Level Gateway- Encrypted tunnels.

Firewalls

Introduction

- Now everyone want to be on the internet
  - Has persistent security concerns
  - Can’t easily secure every system in org
- Typically use a **firewall**
- To provide **perimeter defence**



What is a Firewall?

- A **choke point** of control and monitoring
- Interconnects networks with differing trust
- Imposes restrictions on network services
  - Only authorized traffic is allowed
- Auditing and controlling access
  - Can implement alarms for abnormal behavior

- A firewall is a **network security** device that monitors incoming and outgoing network traffic and permits or blocks data **packets** based on a set of security rules.
- Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) in order to block malicious traffic like viruses and hackers.

What is a Firewall...

- Provide NAT & usage monitoring
- Implement VPNs using IPSec
- Must be immune to penetration

Firewall Properties

- Service Control
- Direction Control
- User Control
- Behavior Control

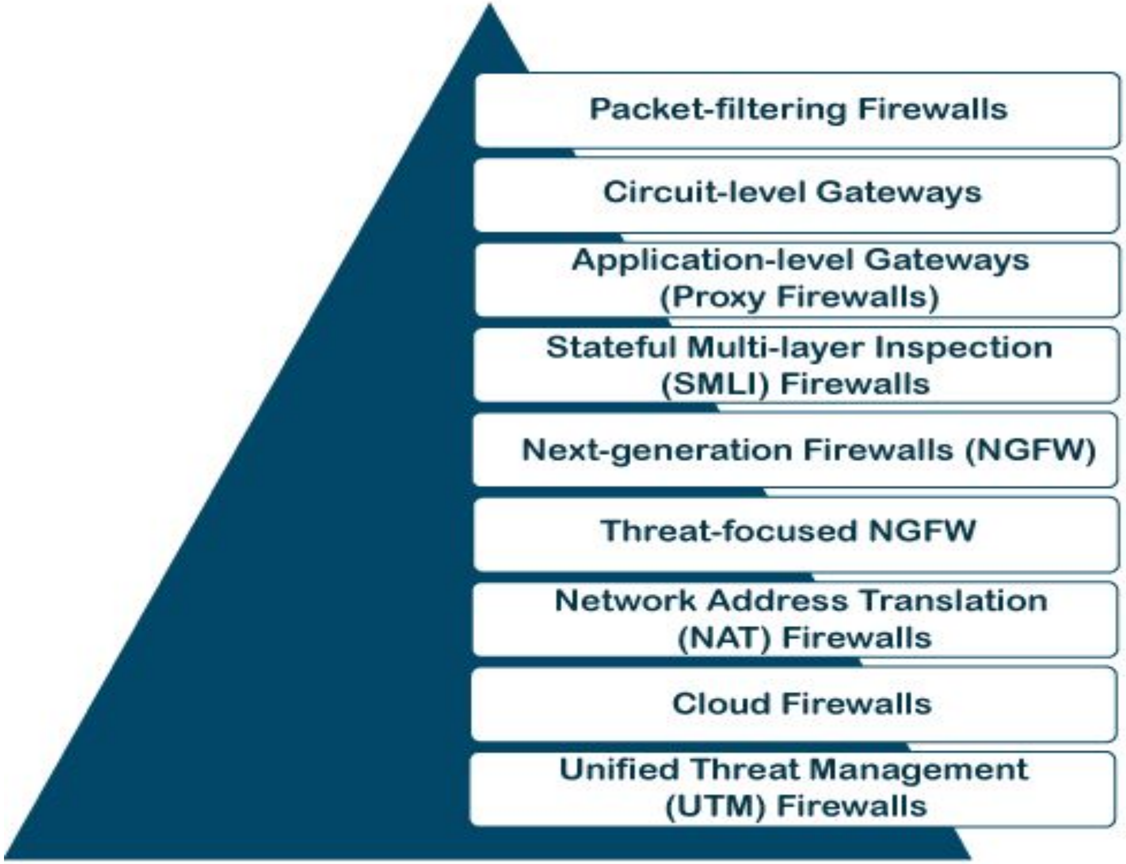
Firewall Limitations

- Cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organisations, trusted services (eg SSL/SSH)
- Cannot protect against internal threats
  - eg disgruntled or colluding employees
- Cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

Types of firewalls

- Packet filtering router
- Application level gateway
- Circuit-level gateway

Types of Firewall

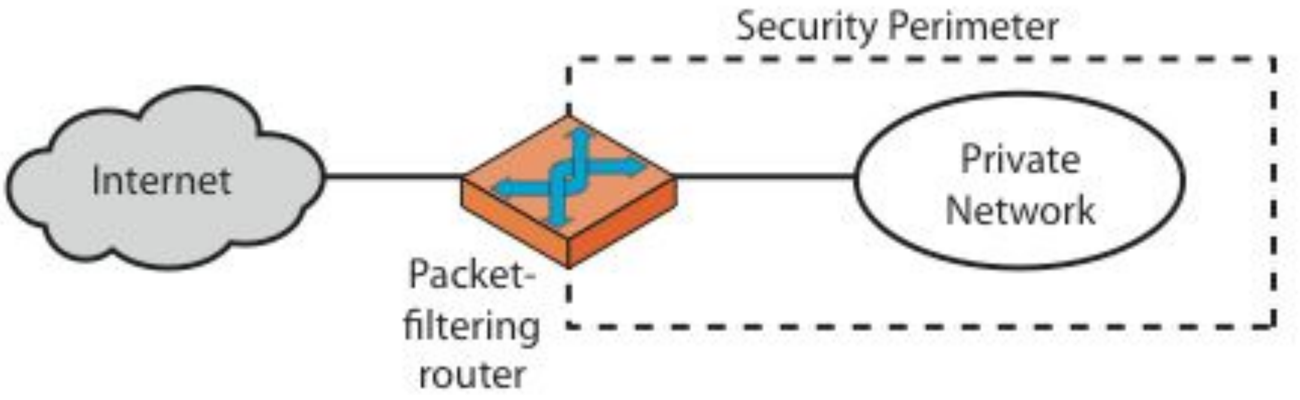


- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

Firewalls – Packet Filters

- Simplest, fastest firewall component
- Foundation of any firewall system
- Examine each IP packet (no context) and permit or deny according to rules
- Hence restrict access to services (ports)

Firewalls – Packet Filters



(a) Packet-filtering router

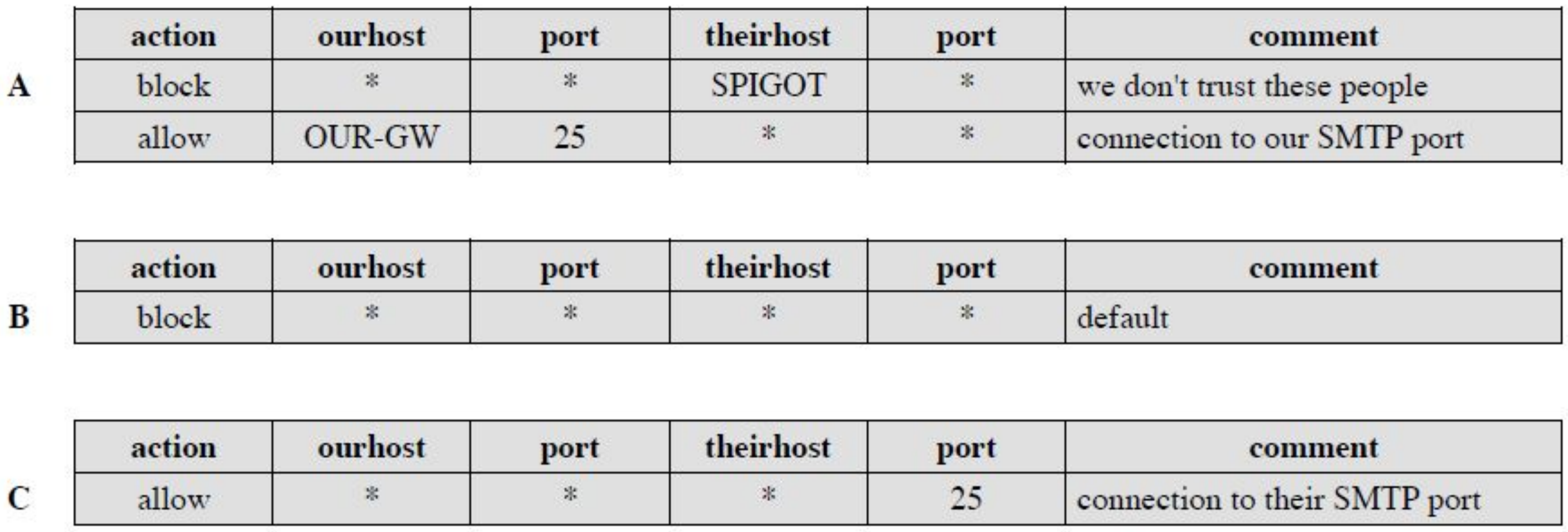
Filtering rules – Packet Filters

- Rules are based on info contained in a packet
  - Source IP Address
  - Destination IP Address
  - Source and destination transport-level address
  - IP protocol field
  - Interface

Firewalls – Packet Filters

- Possible default policies
  - **Default = Discard** : that not expressly permitted is prohibited
  - **Default = Forward** : that not expressly prohibited is permitted

Table 20.1 Packet-Filtering Examples



A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Attacks on Packet Filters

- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- Source routing attacks
  - attacker sets a route other than default
  - block source routed packets
- Tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check

Firewalls – Stateful Packet Filters

- Traditional packet filters do not examine higher layer context
  - ie matching return packets with outgoing flow
- Stateful packet filters address this need
- They examine each IP packet in context
  - keep track of client-server sessions
  - check each packet validly belongs to one
- Hence are better able to detect bogus packets out of context

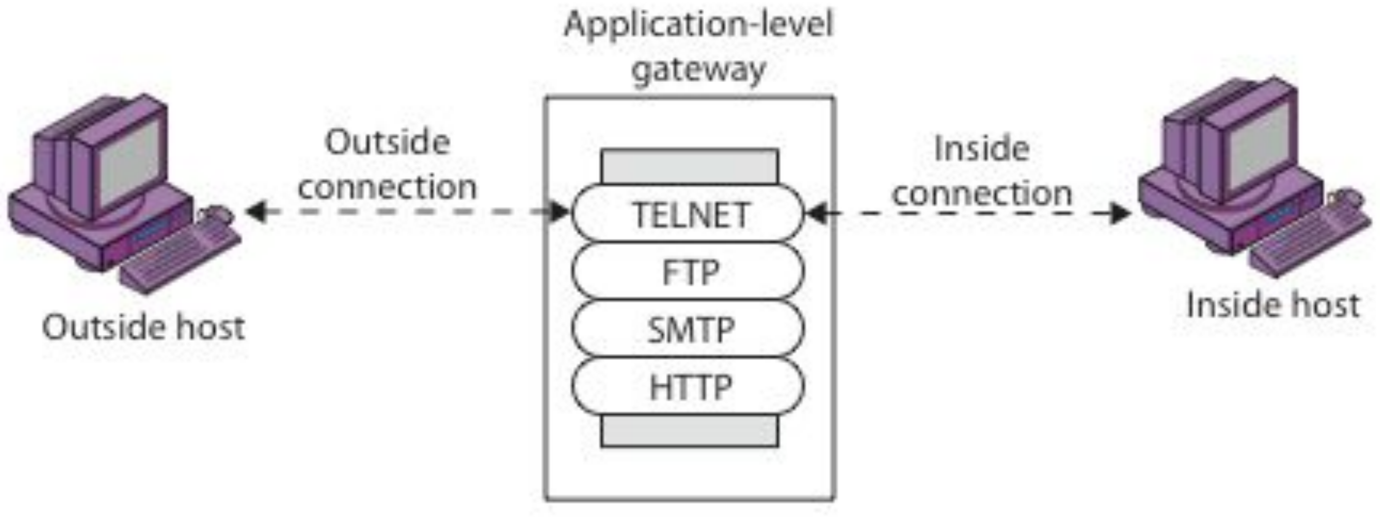
- Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.
- In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.
- In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls. This is why stateful packet inspection is implemented along with many other firewalls to track statistics for all internal traffic. Doing so increases the load and puts more pressure on computing resources. This can give rise to a slower transfer rate for data packets than other solutions.

Firewalls - Application Level Gateway (or Proxy Server)

- Have application specific gateway / proxy
- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
  - can log / audit traffic at application level
- Need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic

- Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.
- Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks.
- Once the connection is established, the proxy firewall inspects data packets coming from the source.
- If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

Firewalls - Application Level Gateway (or Proxy Server)

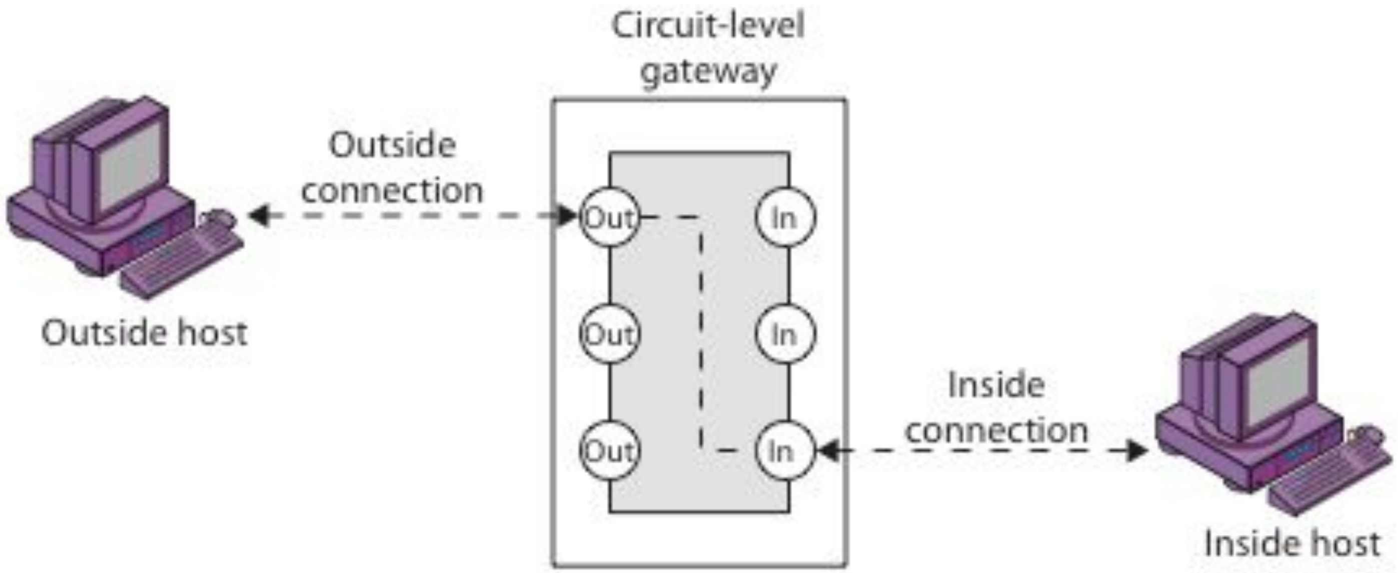


(b) Application-level gateway

Firewalls - Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting which such connections are allowed
- Once created usually relays traffic without examining contents
- Typically used when trust internal users by allowing general outbound connections

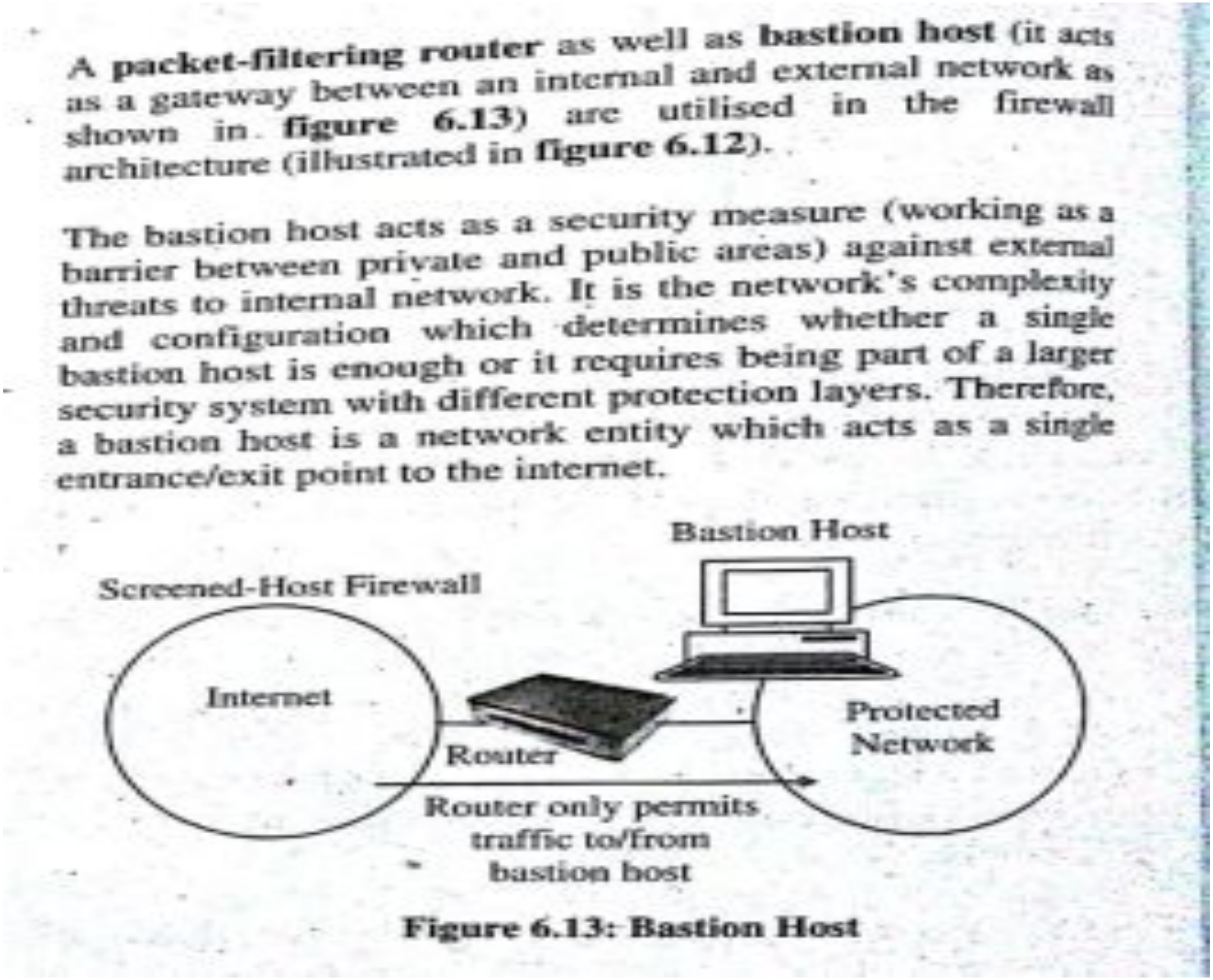
Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

Bastion Host

- Highly secure host system
- Platform for circuit / application level gateways
- It is potentially exposed to "hostile" elements
- Hence it is secured to withstand this
  - hardened O/S, essential services, extra auth
  - proxies small, secure, independent, non-privileged
- May support 2 or more net connections
- May be trusted to enforce policy of trusted separation between these net connections

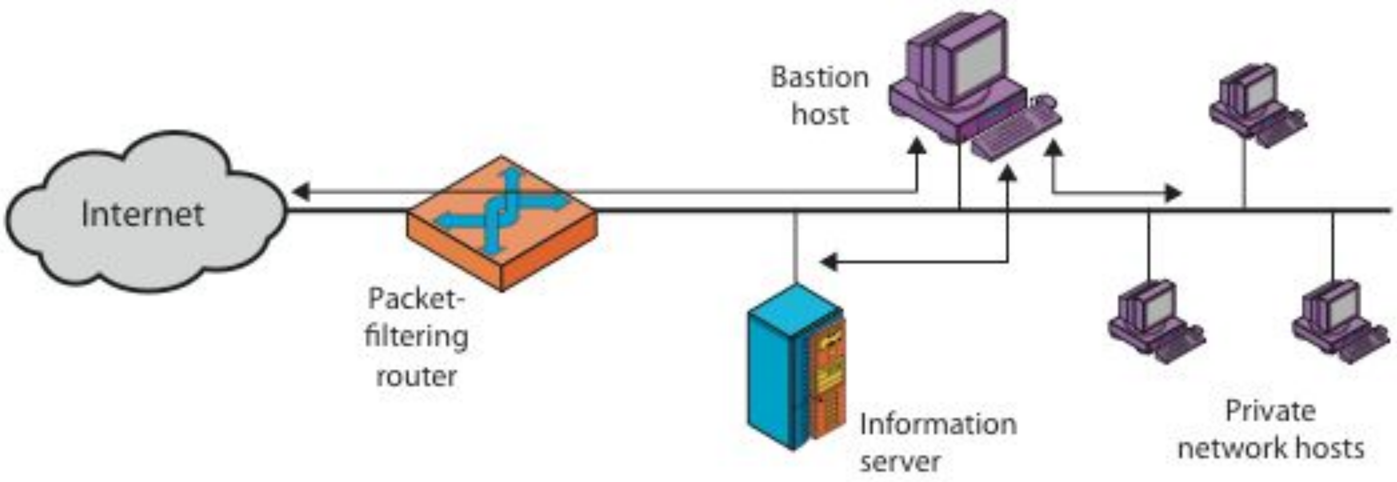


A **packet-filtering router** as well as **bastion host** (it acts as a gateway between an internal and external network as shown in **figure 6.13**) are utilised in the firewall architecture (illustrated in **figure 6.12**).

The bastion host acts as a security measure (working as a barrier between private and public areas) against external threats to internal network. It is the network's complexity and configuration which determines whether a single bastion host is enough or it requires being part of a larger security system with different protection layers. Therefore, a bastion host is a network entity which acts as a single entrance/exit point to the internet.

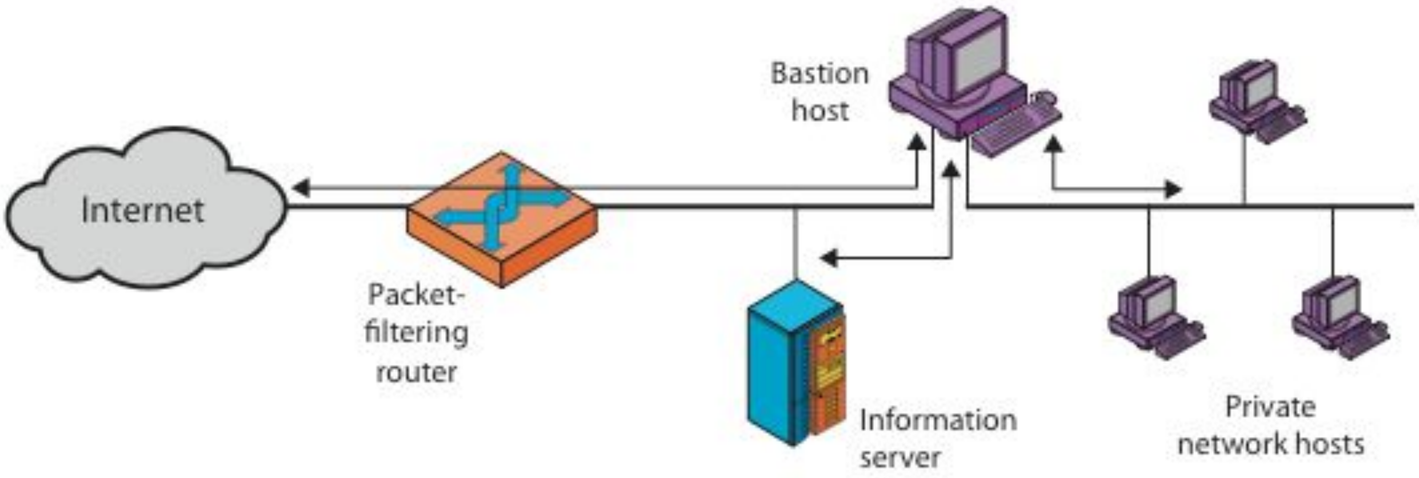
Figure 6.13: Bastion Host

Firewall Configurations



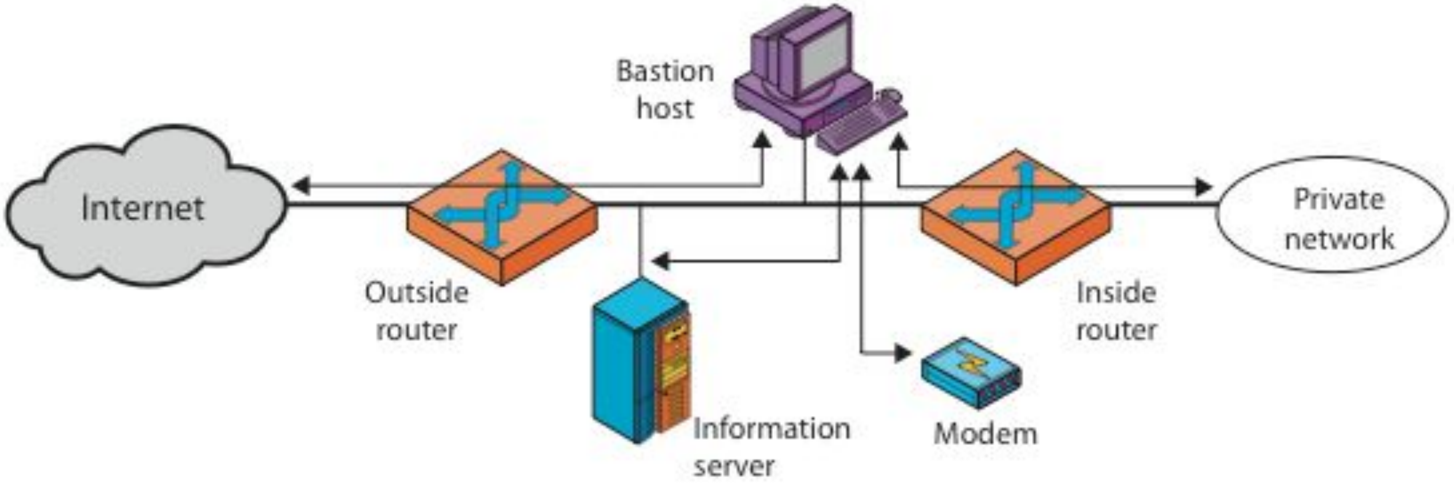
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations



(b) Screened host firewall system (dual-homed bastion host)

Firewall Configurations



(c) Screened-subnet firewall system

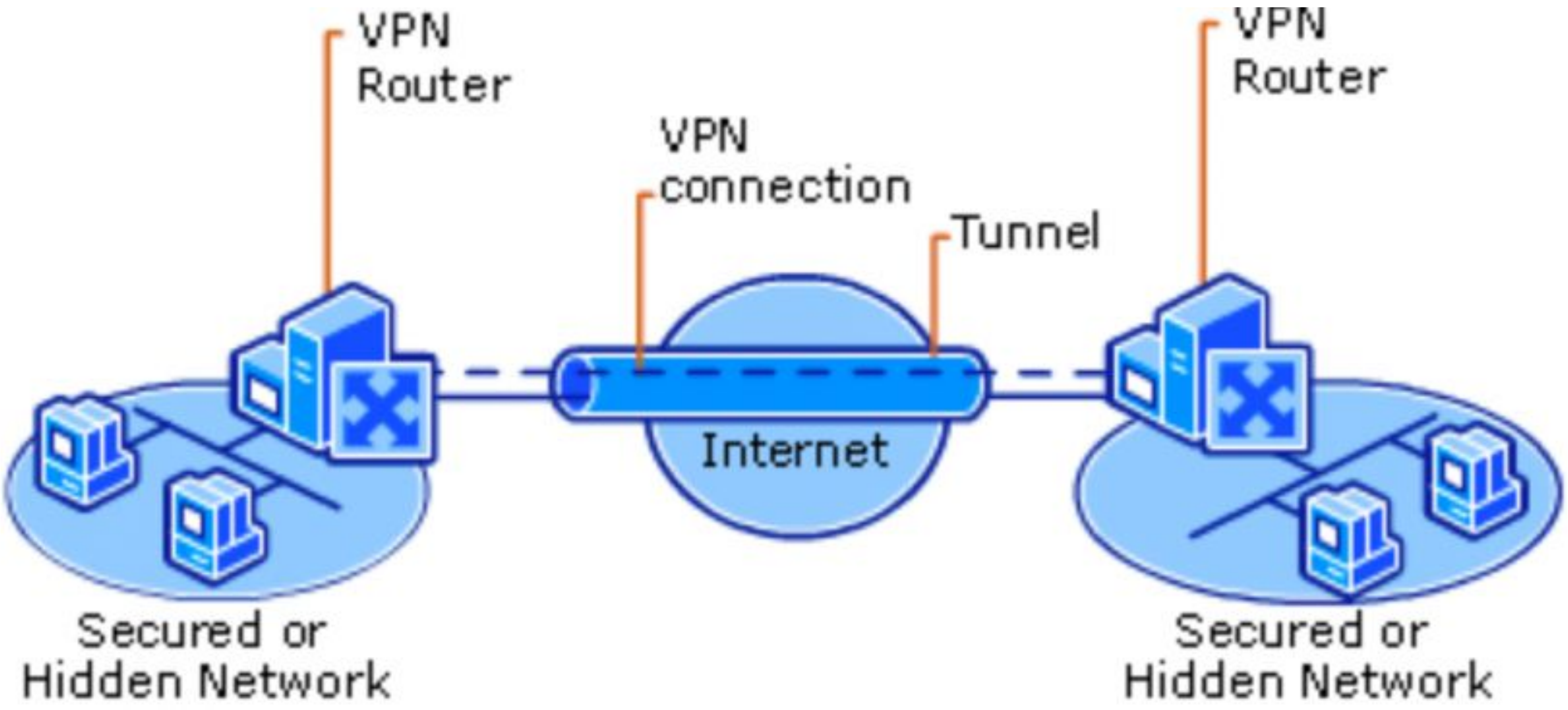
ENCRYPTED TUNNELS

ENCRYPTED TUNNELS

- Secure mechanism that is used to send data across a public network
- Security is achieved using tunneling protocol and VPN

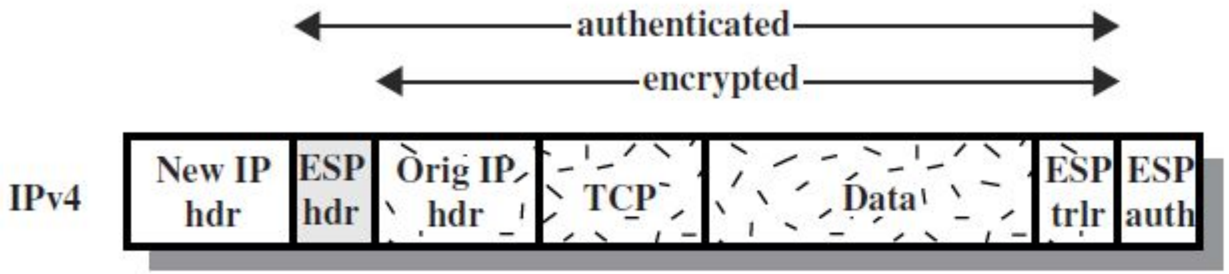
Virtual Private Network (VPN)

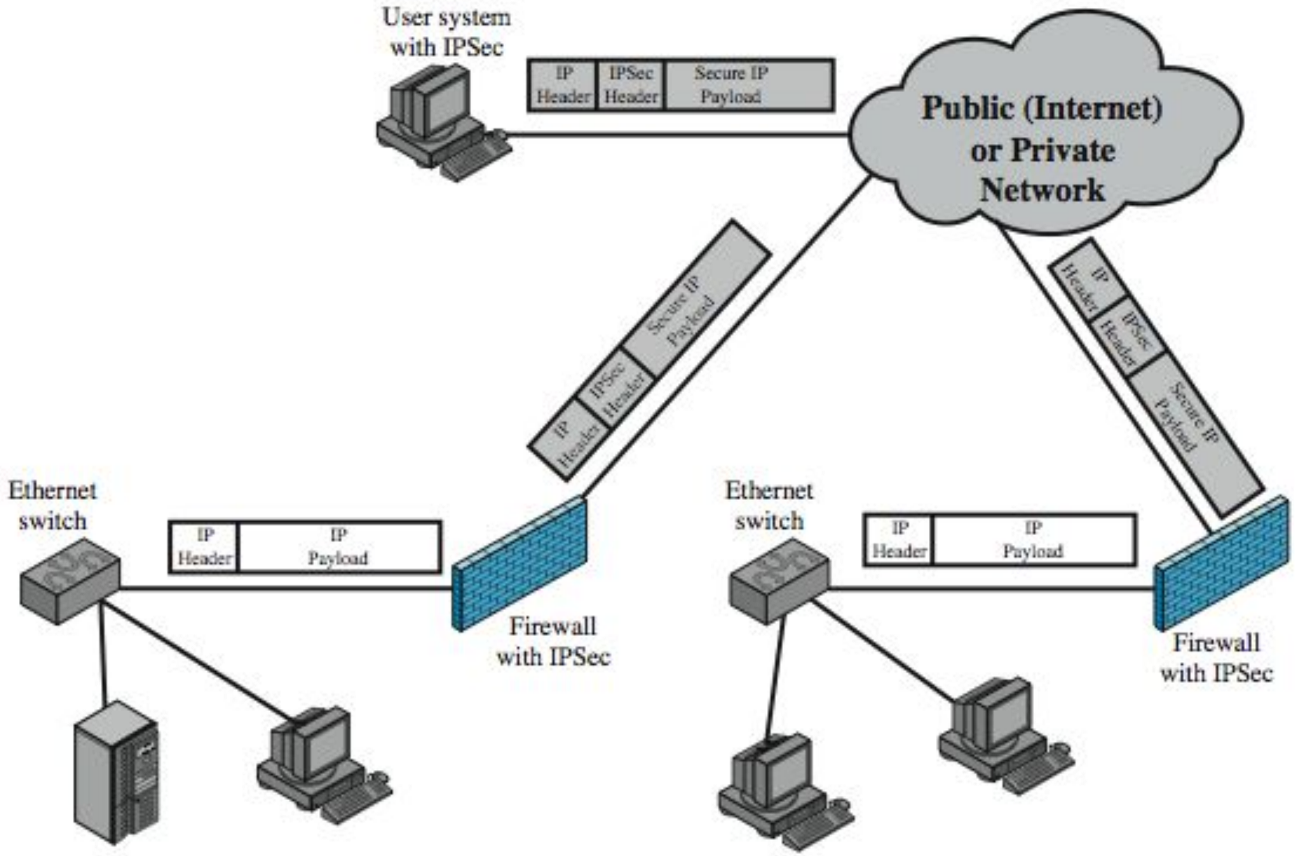
- A **VPN** extends a private network across a public network,
- Enables users to send and receive data across public networks
  - as if their computing devices were directly connected to the private network


VPN
Router
VPN
connection
Tunnel
VPN
Router
Internet
Secured or
Hidden Network
Secured or
Hidden Network

Tunneling Protocol

- Tunneling protocol uses the tunnel mode of IPSec




User system with IPSec
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
IP Header
IPSec Header
Secure IP Payload
IP Header
IPSec Header
Secure IP Payload
Ethernet switch
IP Header
IP Payload
Firewall with IPSec
Ethernet switch
IP Header
IP Payload
Firewall with IPSec