Chapter 6:
FIREWALL

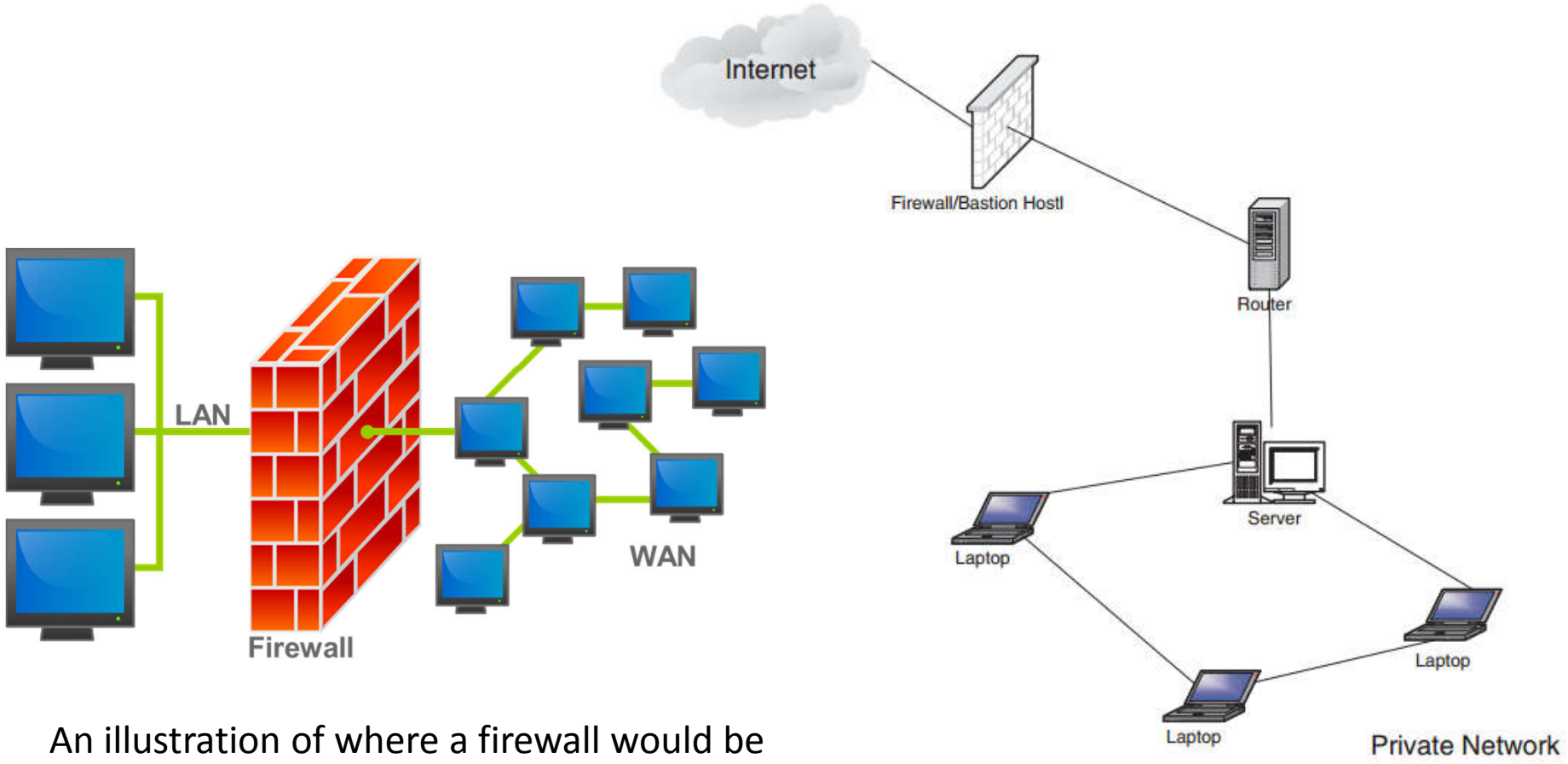
Content

- Definition
- Types of Firewalls
- The Demilitarized Zone (DMZ)
- Firewall Services & Limitations

Definition

- A firewall is a hardware, software, or a combination of both that monitors and filters traffic packets that attempt to either enter or leave the protected private network.
- According to Wikipedia, a firewall is a network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted

Definition



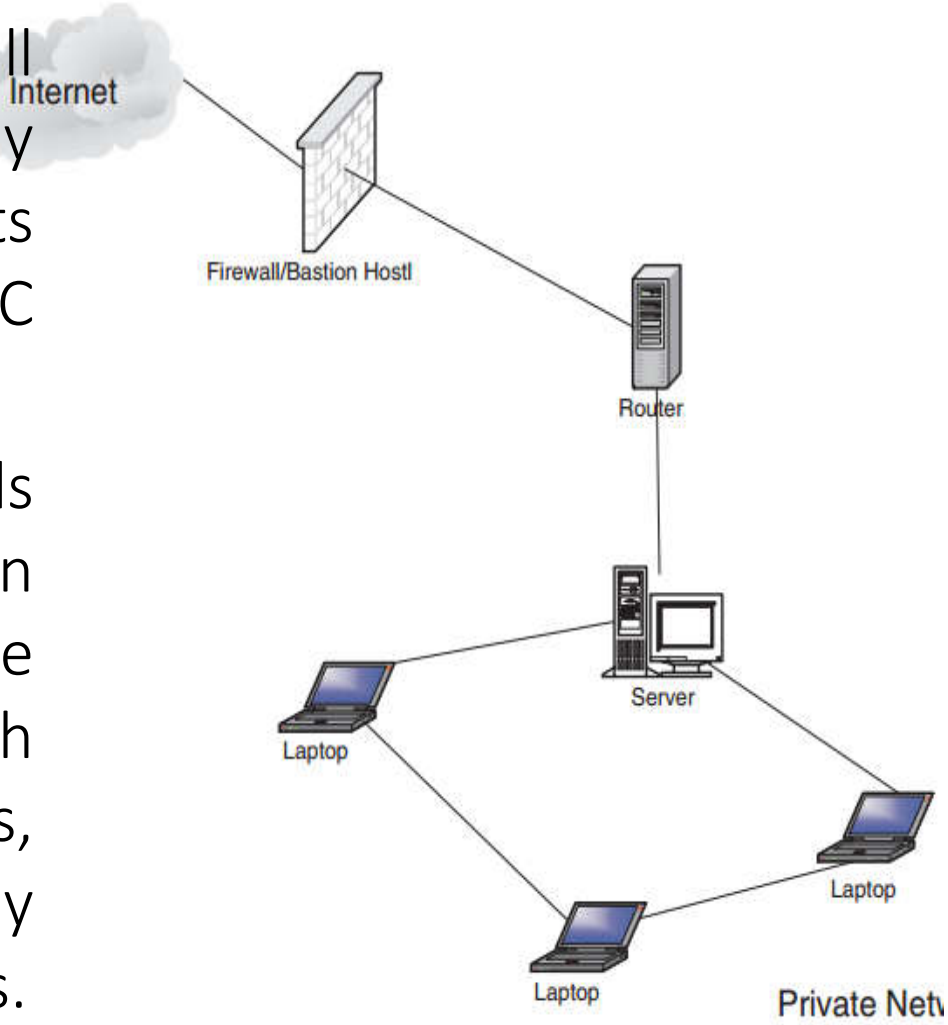
An illustration of where a firewall would be located in a network.

Definition

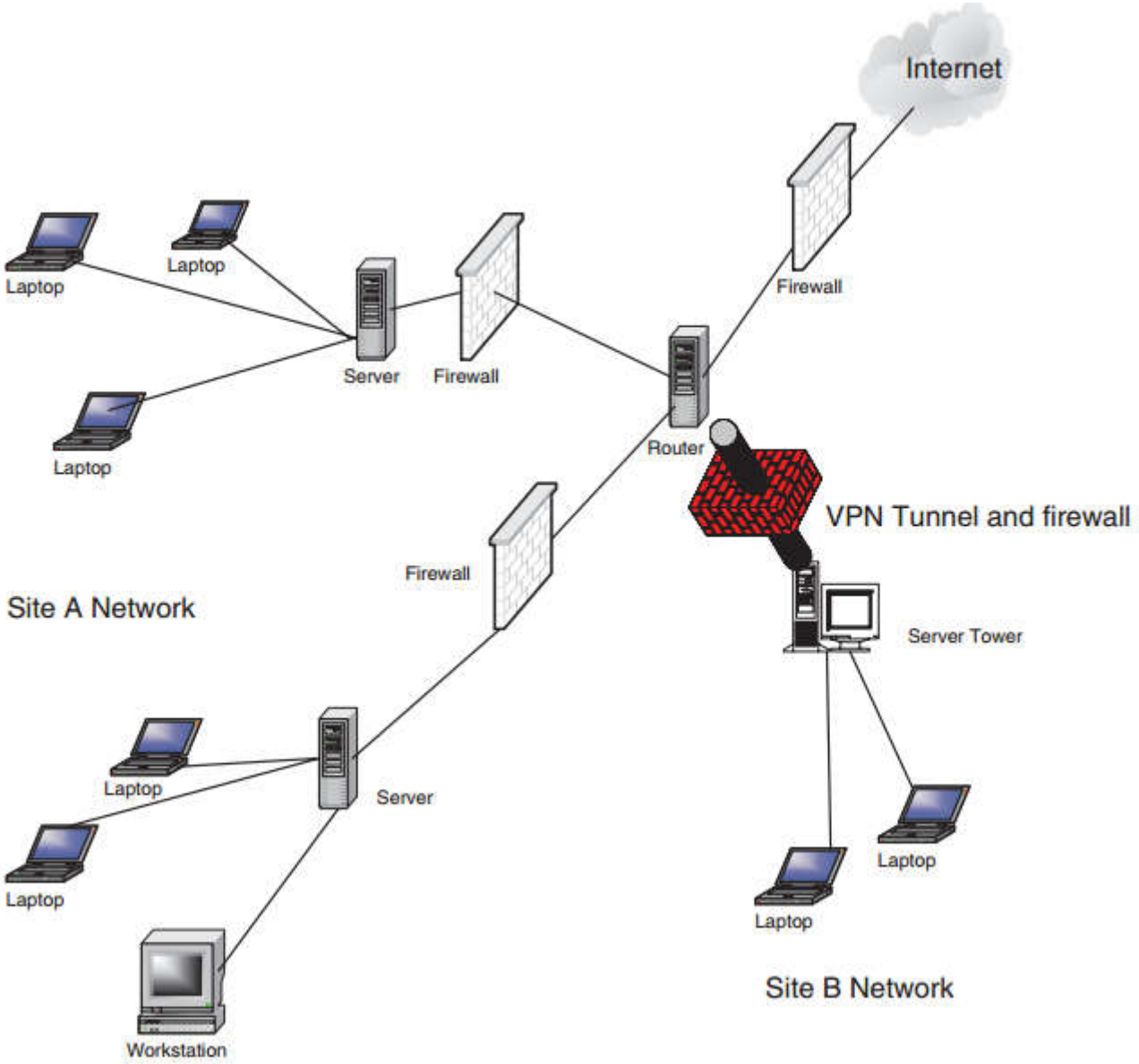
- By definition, a “firewall,” is a tool that provides a filter of both incoming and outgoing packets. Most firewalls perform two basic security functions:
  - Packet filtering based on accept or deny policy that is itself based on rules of the security policy.
  - Application proxy gateways that provide services to the inside users and at the same time protect each individual host from the “bad” outside users.

Definition

- In its simplest form, a firewall can be implemented by any device or tool that connects a network or an individual PC to the Internet.
- Most organization firewalls are bastion host. A bastion host is one computer on the organization network with bare essential services, designated and strongly fortified to withstand attacks.



Definition



Firewalls in a changing parameter security

Definition

- Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet. Many routers that pass data between networks contain firewall components and, conversely, many firewalls can perform basic routing functions.

Definition

- The accept/deny policy used in firewalls is based on an organization's security policy. These policies are consolidated into two commonly used firewall security policies:
  - Deny-everything-not-specifically-allowed
  - Allow-everything-not-specifically-denied

Definition

The firewall is supposed to:

- Prevent intruders from entering and interfering with the operations of the organization's network.
- Prevent intruders from deleting or modifying information either stored or in motion within the organization's network.
- Prevent intruders from acquiring proprietary organization information.
- Prevent insiders from misusing the organization resources by restricting unauthorized access to system resources.
- Provide authentication.
- Provide end-points to the VPN.

Types of Firewalls

- Firewalls can be set up to offer security services to many TCP/IP layers. The many types of firewalls are classified based on the network layer it offers services in and the types of services offered

Table 12.1 Firewall services based on network protocol layers

Layer	Firewall services
Application	Application-level gateways, encryption, SOCKS Proxy Server
Transport	Packet filtering (TCP, UDP, ICMP)
Network	NAT, IP-filtering
Data link	MAC address filtering
Physical	May not be available

Types of Firewalls

- 1st type is the packet inspection or filtering router. This type of firewall uses a set of rules to determine whether to forward or block individual packets. A packet inspection router could be a simple machine with multiple network interfaces or a sophisticated one with multiple functionalities.

- 2nd type is the application inspection or proxy server. The proxy server is based on specific application daemons to provide authentication and to forward packets.

Types of Firewalls

- 3rd type is the authentication and virtual private networks (VPN). A VPN is an encrypted link in a private network running on a public network.
- 4th firewall type is the small office or home (SOHO) firewall.
- 5th is the network address translation (NAT).

Types of Firewalls - Packet Inspection Firewalls

- Packet filter firewalls are routers that inspect the contents of the source or destination addresses and ports of incoming or outgoing TCP, UDP, and ICMP packets being sent between networks and accept or reject the packet based on the specific packet policies set in the organization's security policy.
- A router is a machine that forwards packets between two or more networks, working at the network level, is programmed to compare each packet to a list of rules set from the organization's security policy, before deciding if it should be forwarded or not. Data is allowed to leave the system only if the firewall rules allow it.

Types of Firewalls - Packet Inspection Firewalls

- Two types of packet filtering are used during packet inspection: static or stateless filtering (layer 1-3) and stateful filtering (layer 4)
- Filtering based on the following information in the packet:
  - Source address
  - Destination address
  - TCP or UDP source and destination port number
  - ICMP message type
  - Payload data type
  - Connection initialization and datagram using TCP ACK bit.

  => different ways of implementing the filtering firewall based on IP address, TCP/UDP port numbers, and sequence numbers and ACK filtering.

Types of Firewalls - Packet Inspection Firewalls

- IP Address Filtering:
  - IP address filtering rules are used to control traffic into and out of the network through the filtering of both source and destination IP addresses.

Table 12.2 Destination IP filtering

Application protocol	Source IP	Destination IP	Action
HTTP	Any	198.124.1.0	Allow
Telnet	Any	198.213.1.1	Deny
FTP	Any	198.142.0.2	Allow

- TCP and UDP Port Filtering

Table 12.3 Filtering rules based on TCP and UDP destination port numbers

Application	Protocol	Destination port number	Action
HTTP	TCP	80	Allow
SSL	UDP	443	Deny
Telnet	TCP	23	Allow

Types of Firewalls - Packet Inspection Firewalls

- Packet Filtering Based on Initial Sequence Numbers (ISN) and Acknowledgement (ACK) Bits

Table 12.4 Rules for filtering based on ACK field bit

Sequence number	IP Destination address	Port number	ACK	Action
15	198.123.0.1	80	0	Deny
16	198.024.1.1	80	1	Allow

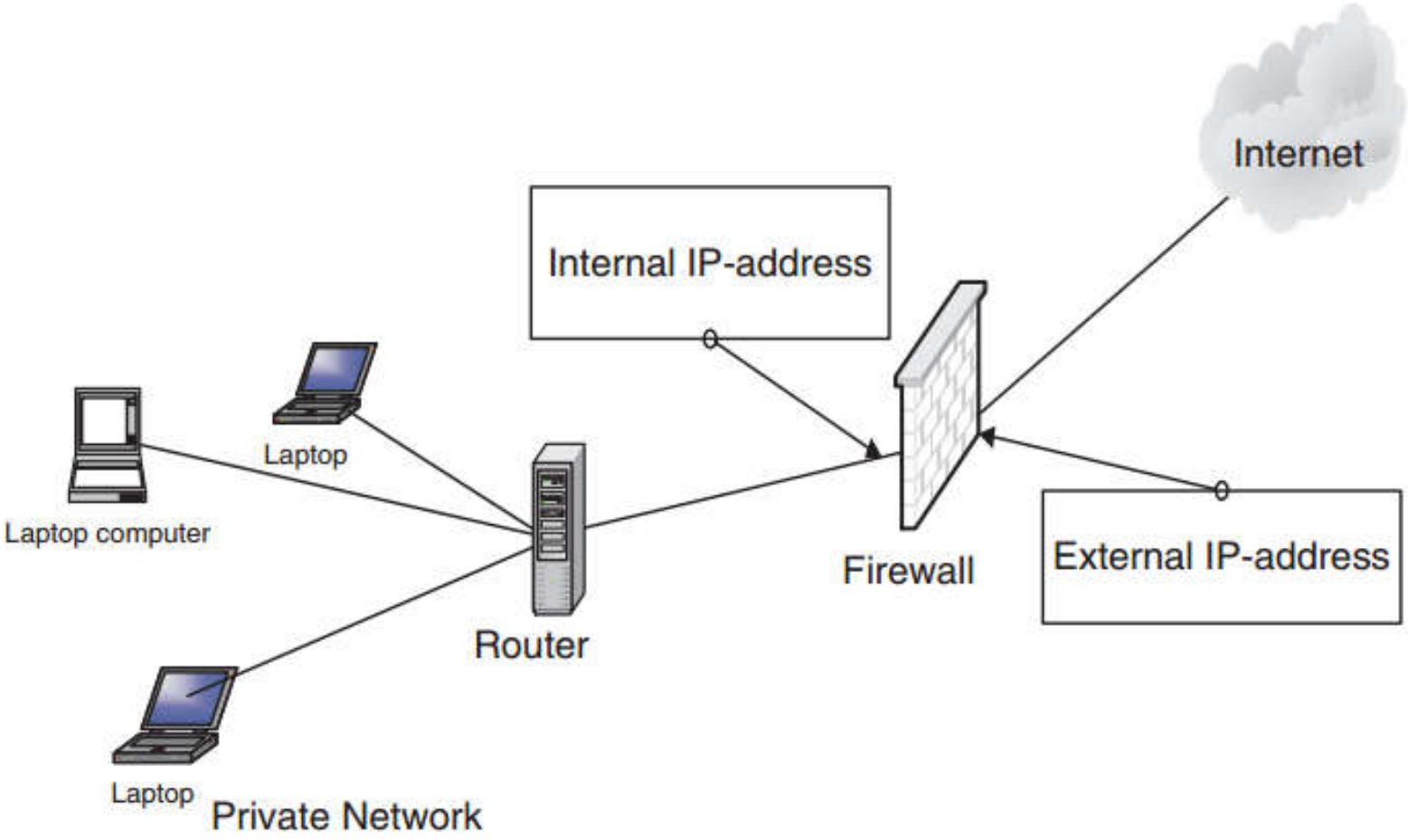
Types of Firewalls - Application Proxy Server

- Proxy servers: filter traffic based on popular services in the organization, only packets from well known and popularly used services are allowed into the organization network, and reject any packets that are not from specific applications
- A proxy server,
  - is a machine server that sits between a client application and the server (offering the services the client application may want)
  - It behaves as a server to the client and as a client to the server
  - providing a higher level of filtering than the packet filter server by examining individual application packet data streams.

Types of Firewalls - Application Proxy Server

- A proxy firewall works by first intercepting a request from a host on the internal network and then passing it on to its destination, usually the Internet.
- Before passing it on, the proxy replaces the IP source address in the packet with its own IP address and then passes it on.
- On receipt of packet from an external network, the proxy inspects the packet, replaces its own IP destination address in the packet with that of the internal host, and passes it on to the internal host.
- The internal host does not suspect that the packet is from a proxy.

Types of Firewalls - Application Proxy Server



Types of Firewalls - Application Proxy Server

- An example of a proxy server is a Web application firewall server. Popular web applications are filtered based on their port numbers as below.
  - HTTP (port 80)
  - FTP (port 20 and 21)
  - SSL (port 443)
  - Gopher (port 70)
  - Telnet (port 23)
  - Mail (port 25)
- Proxy firewalls fall into two types: application and SOCKS proxies

Types of Firewalls - Virtual Private Network (VPN) Firewalls

- A virtual private network (VPN) extends a private network across a public network, such as the Internet. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryptions.
- VPNs can be created using a single remote computer connecting on to a trusted network or connecting two corporate network sites. In either case and at both ends of the tunnels, a VPN server can also act as a firewall server.

Types of Firewalls - Virtual Private Network (VPN) Firewalls

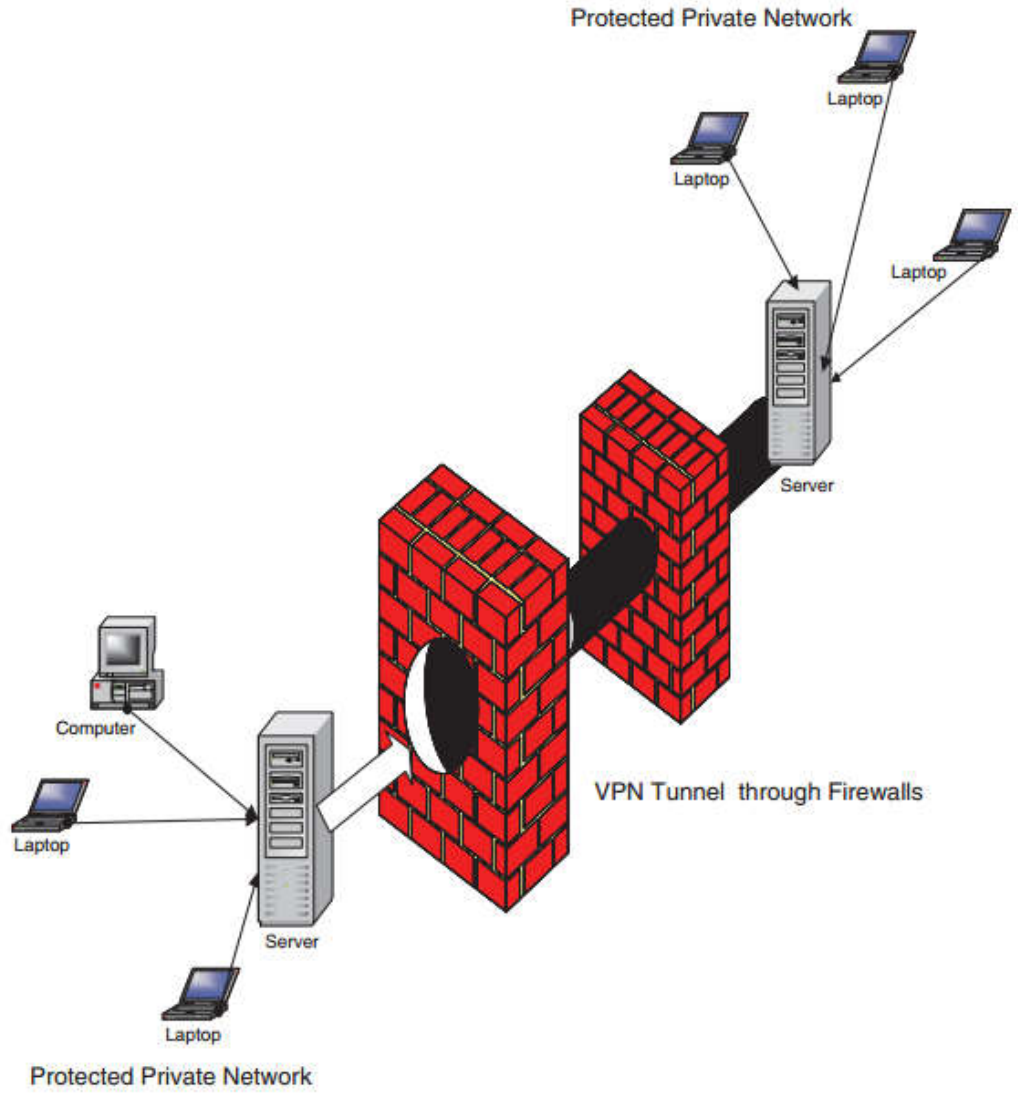
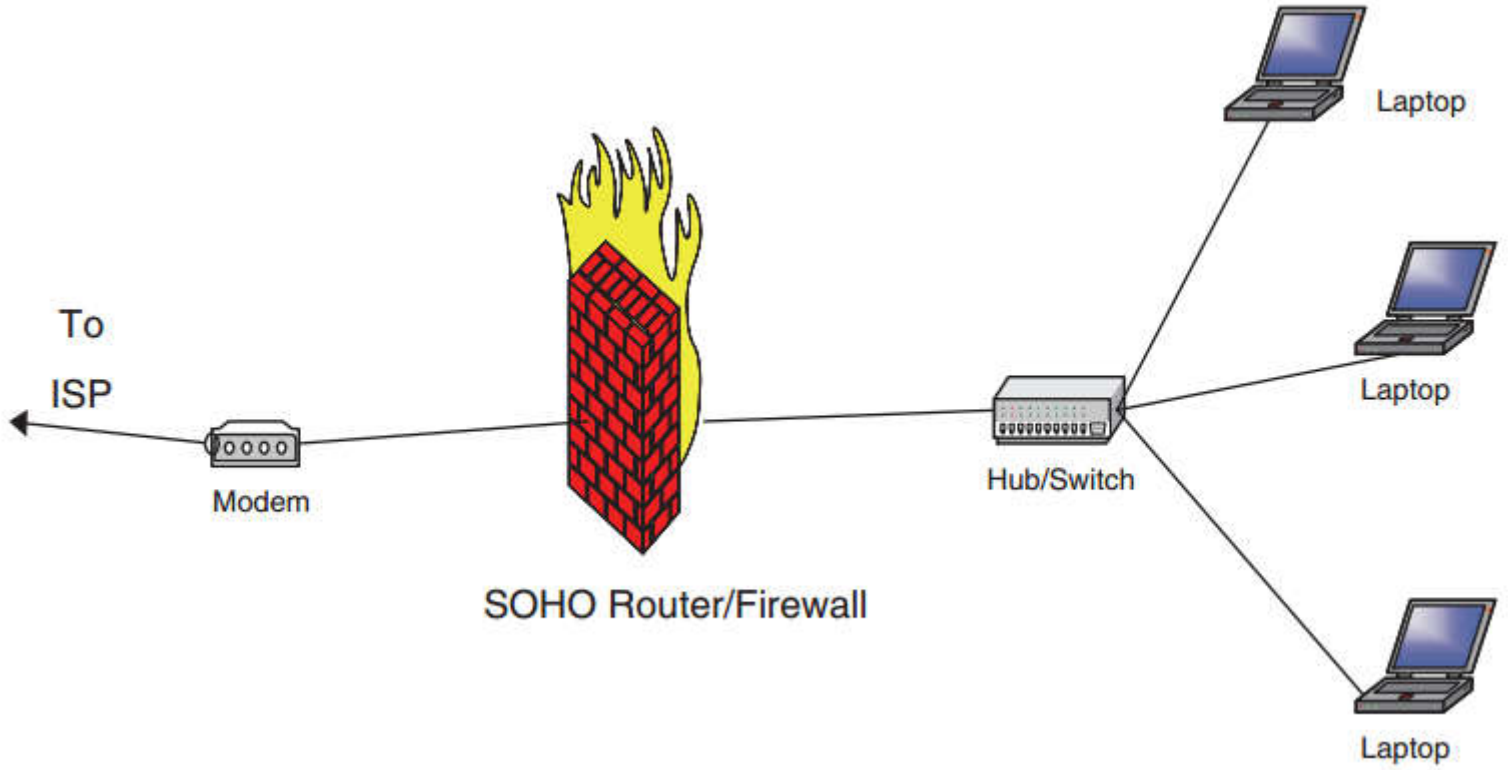


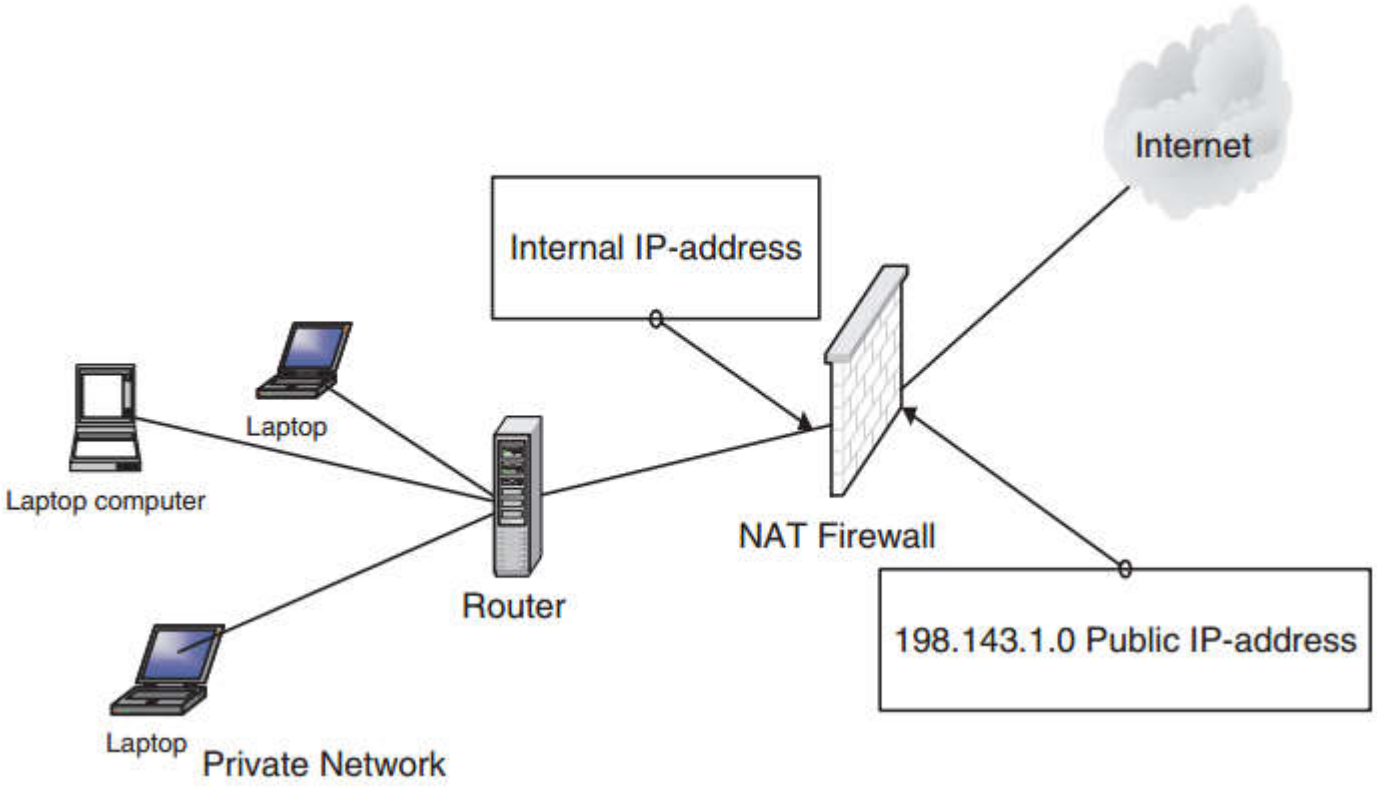
Fig. 12.6 VPN connections and firewalls

Types of Firewalls - Small Office or Home (SOHO) Firewalls

- A SOHO firewall is a relatively small firewall that connects a few personal computers via a hub, switch, a bridge, even a router on one side and connecting to a broadband modem like DSL or cable on the other.

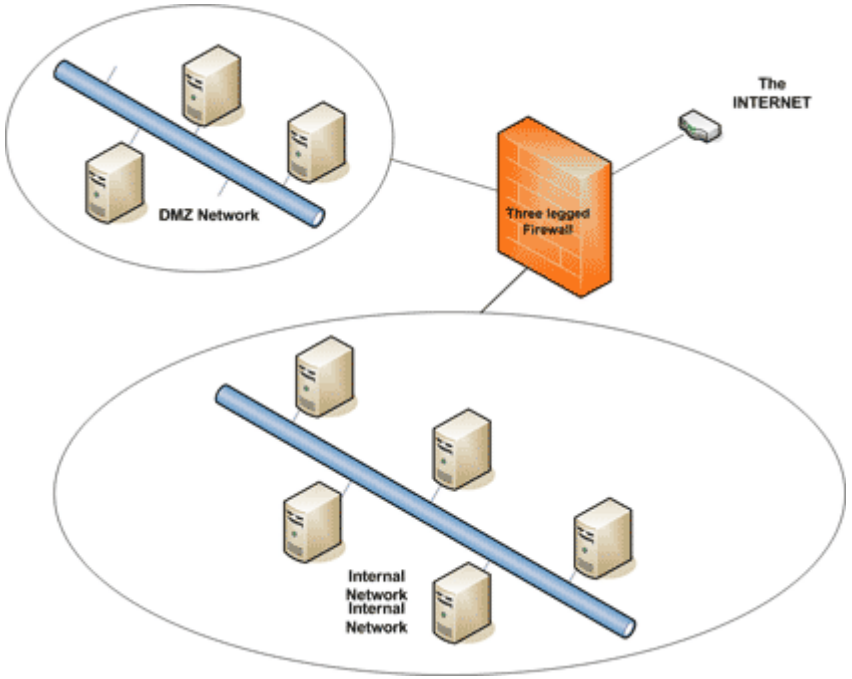


Types of Firewalls – NAT (Network address translation) Firewalls

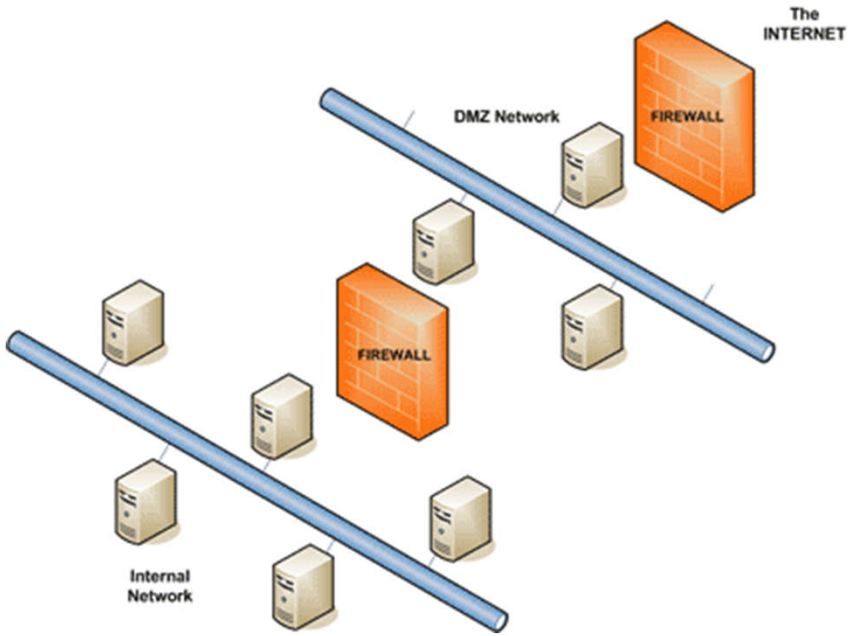


The Demilitarized Zone (DMZ)

- A DMZ is a segment of a network or a network between the protected network and the “bad external network.”



Single firewall



Dual firewall with front-end and back-end firewall

Firewall Services and Limitations

Firewall Services: services offered by the firewall are based on the following access controls:

- Service control – where the firewall may filter traffic on the basis of IP addresses, TCP, UDP, port numbers, and DNS and FTP protocols in addition to providing proxy software that receives and interprets each service request before passing it on.
- Direction control – where permission for traffic flow is determined from the direction of the requests.
- User control – where access is granted based on which user is attempting to access the internal protected network, which may also be used on incoming traffic.
- Behavior control – in which access is granted based on how particular services are used, for example, filtering e-mail to eliminate spam.

Firewall Services and Limitations

Limitations of Firewalls:

- Firewalls cannot protect against a threat that bypasses it, such as a dial-in using a mobile host.
- Firewalls do not provide data integrity because it is not possible, especially in large networks, to have the firewall examine each and every incoming and outgoing data packet for anything.
- Firewalls cannot ensure data confidentiality because, even though newer firewalls include encryption tools, it is not easy to use these tools. It can only work if the receiver of the packet also has the same firewall.
- Firewalls do not protect against internal threats.
- Firewalls cannot protect against transfer of virus-infected programs or files.

Read more

- Guide to Computer Network Security, chapter 12, page 249-269.
- http://en.wikipedia.org/wiki/Firewall_(computing)
- http://www.certificationkits.com/cisco-certification/CCNA-Security-Operational-Strength-Weaknesses-of-Firewalls.html
- http://en.wikipedia.org/wiki/DMZ_(computing)
- http://en.wikipedia.org/wiki/Virtual_private_network