SEMENAR SECURITY

NETWORK DEFENSE TOOLS

...

PREPARATION BY

MUTHANA SALIH - ISRAA ABDALSATAR

...

SUPERVISION

DR.BASHAR.M.NEMA

What is Network Defense Tools

- network defense is a set of processes and protective measures that use computer networks to detect, monitor, protect, analyze and defend against network infiltrations resulting in service/network denial, degradation and disruptions.

Continue

- enables a government or military organization to defend against malicious network attacks .

TOOLS TYPE

- FIREWALLS .
- FILTERS .
- INTRUSION DETECTION .
- VPNS .

What is a Firewalls

- Firewall is anything, hardware or software, that monitors transmission of packets of digital information that attempt to pass the perimeter of a network .
- Firewalls allow traffic only to legitimate hosts and services .
- Traffic to the legitimate hosts/services can have attacks .

Continue

- A computer firewall is a router or other communications device which filters access to a protected network.
- Firewall is also a program that screens all incoming traffic and protects the network from unwelcome intruders.

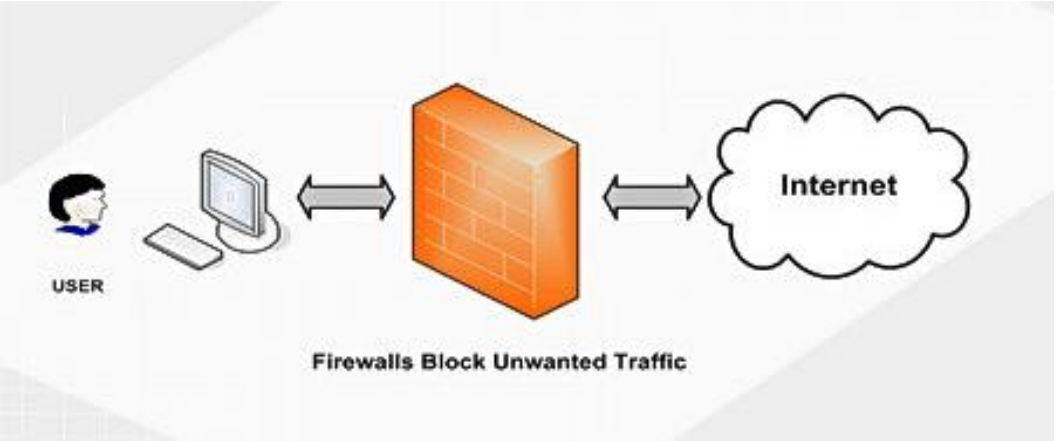
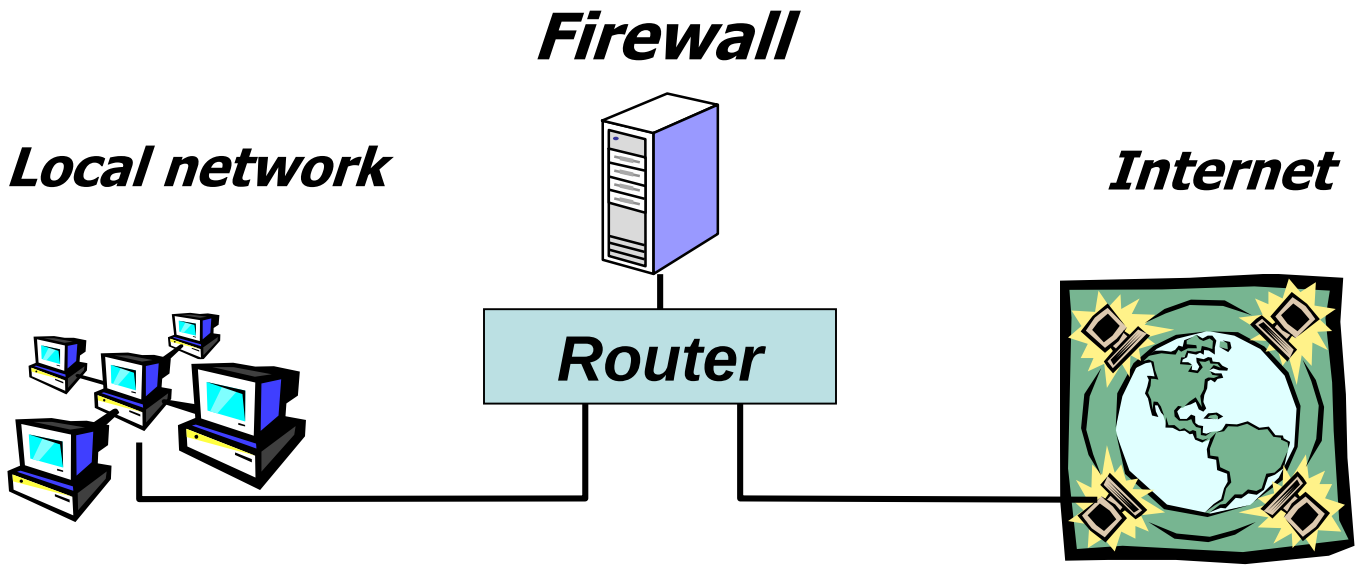


Figure 1 : Show Firewall block Unwanted Traffic

Basic Firewall Concept

- Separate local area net from internet



All packets between LAN and internet routed through firewall

Figure 2 : Show Basic Firewall Concept

Use of Firewalls

- firewall is used to secure the network of an organization.
- It is a device that attempts to prevent unauthorized access to a network.
- It is usually located at the boundary where a private network interfaces with the external world

Continue

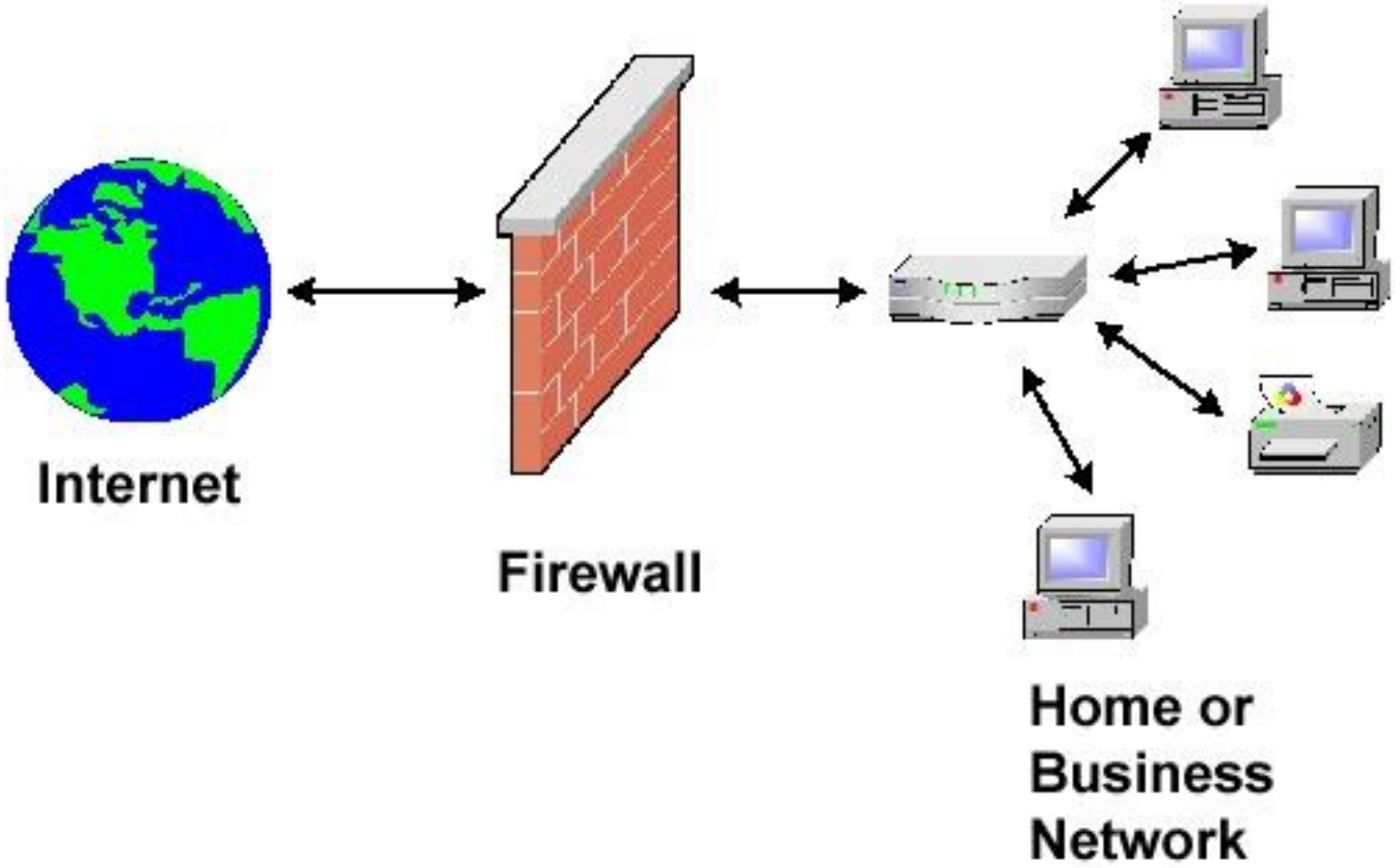


Figure 3 : Show Use of Firewalls

Packet Filtering Firewalls

- Packet Filtering is the type of firewall built into the Linux kernel
- A filtering firewall works at the network level. Data is only allowed to leave the system if the firewall rules allow it. As packets arrive they are filtered by their type, source address, destination address, and port information contained in each packet

Continue

- Many network routers have the ability to perform some firewall services. Filtering firewalls can be thought of as a type of router

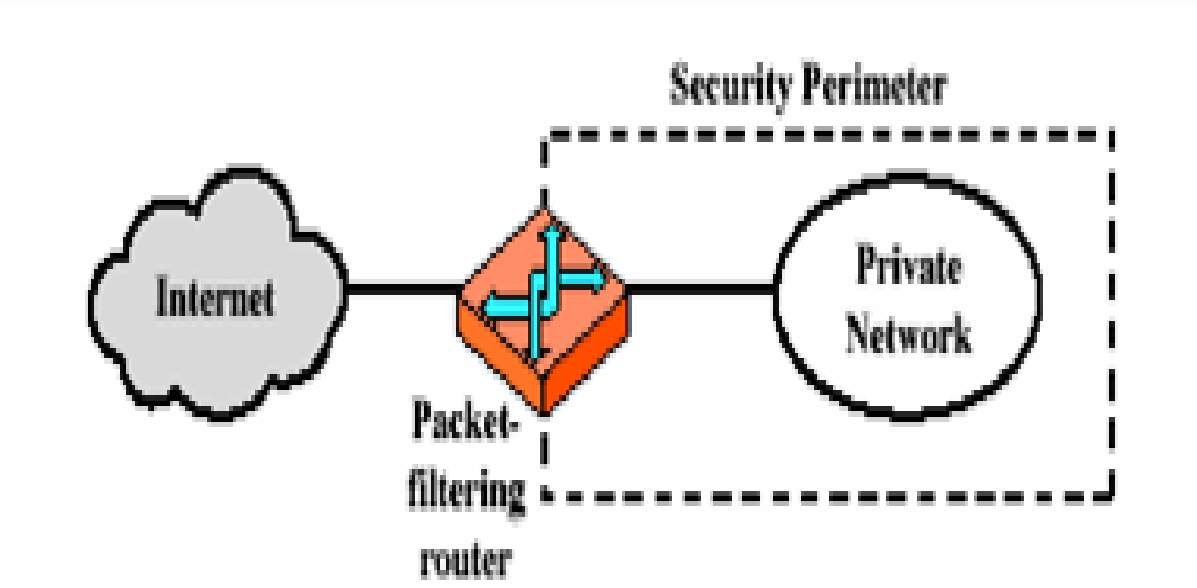


Figure 4 : Show Packet Filtering router

INTRUSION DETECTION SYSTEMS

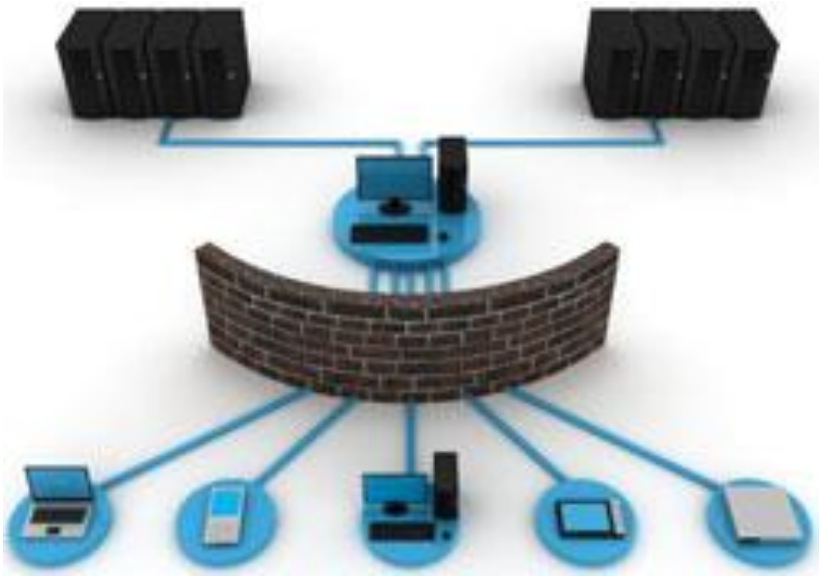
- What is an intrusion ?
- What is an Intrusion Detection Systems ?
- how is Intrusion prevention ?
- What is Principles of Intrusion Detection Systems ?

What is an intrusion?

Any set of actions that attempt to compromise the confidentiality, integrity, or availability of a computer resource .

What is an Intrusion Detection Systems

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.



Intrusion prevention

- Network firewall
  - Restrict flow of packets .
- System security
  - Find vulnerabilities and remove them .

Principles of Intrusion Detection Systems

- An IDS must run unattended for extended periods of time .
- The IDS must stay active and secure .
- The IDS must be able to recognize unusual activity
- The IDS must operate without unduly affecting the system’s activity .

What is VPN?

- A technology that creates a network that is physically public, but virtually private.

- VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies to prevent disclosure of private information to unauthorized parties.

Virtual Private Networks (VPN)

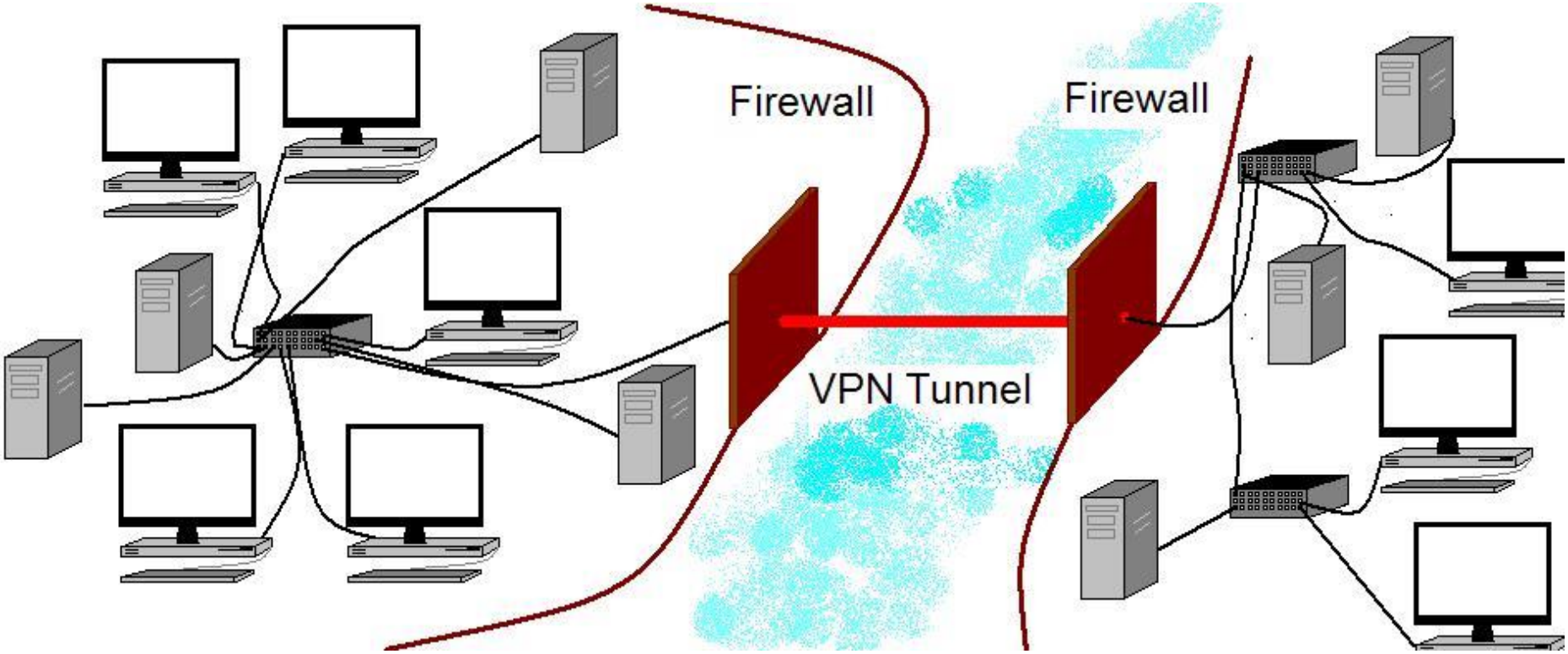


Figure 5 : Show Virtual Private Networks Tunnel

Continue

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

- Became popular as more employees worked in remote locations.

goal In VPNs

- **In VPNs, various networking technologies are applied toward the goal of providing private communications within the public Internet infrastructure**

Virtual Private Networks (VPN)
Basic Architecture

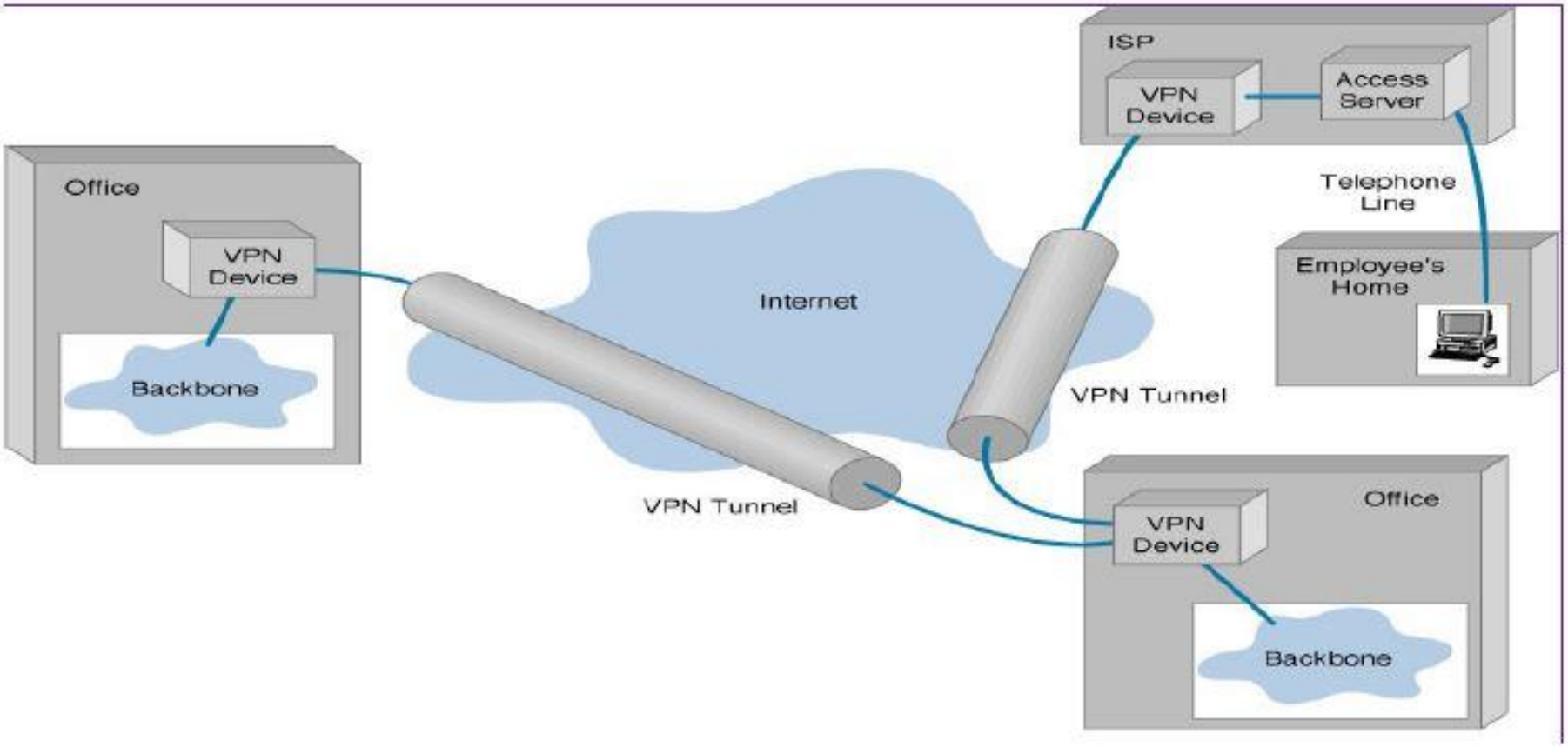


Figure 6 : Show Basic Architecture of VPN

THANK YOU

REFERENCES

Michael E. Whitman , “Principles of Information Security 4th ed” Fourth Edition, 2011 .

William Stallings, “Cryptography and Network Security Principles and Practices”, 4th Ed - William Stallings , November 16, 2005 .

Behrouz_A._Forouzan ,” TCP_IP_Protocol_Suite Virtual Private Network (VPN) “, Fourth Edition,2008 .

Charles P. Pfleeger,” Security in Computing “, Fourth Edition, October 13, 2006 .

D.Litchfield, C.Anley, J. Heasman, B. Grindlay, “ Hacker’s Handbook – Defending Database Servers”, Indianapolis: Wiley Publishing Inc, 2005.