INFORMATION SECURITY MANAGEMENT

NETWORK SECURITY

DAY-3, SESSION-3

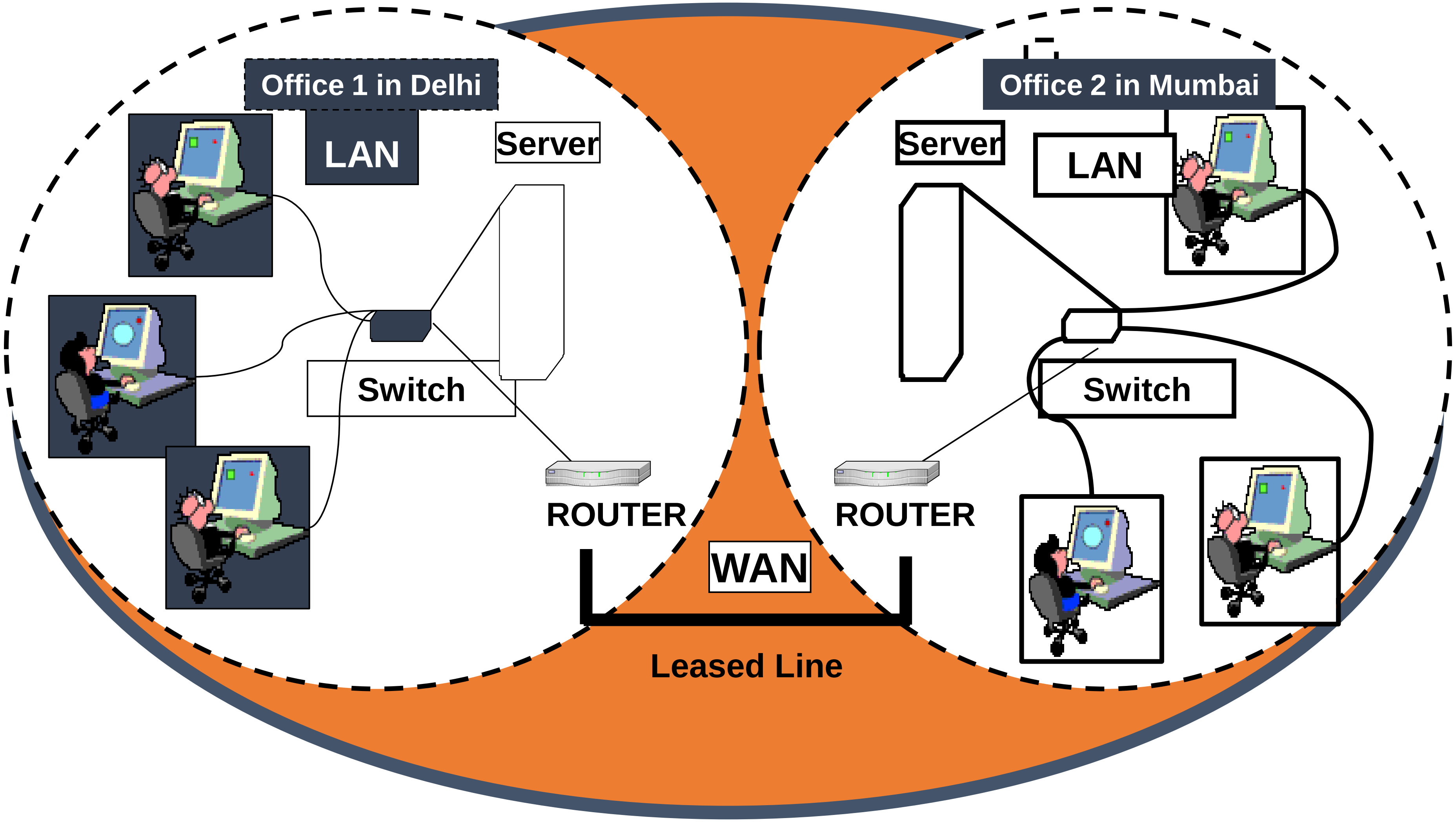
AGENDA

- Introduction to Data Networks, LAN and WAN
- Introduction to infrastructure elements of LAN and WAN
- Introduction to Data Center and IT infrastructure elements in a Data Center
- Security challenges and risks surrounding LAN and WAN environments
- Security challenges and risks surrounding IT Infrastructure in Data Center environments
- Information security measures and solutions for securing LAN, WAN and Data Center

SOME NETWORK TERMINOLOGIES

- **Network : A network is a group of computers/IT components connected together in such a way as to facilitate:**
  - Data/voice/video Communication among people within and across building, locations, cities and countries
  - Sharing of data/files/documents within office, across offices (in the same city or across the cities)
  - Accessing the software applications and databases for performing business functions
- **LAN (Local Area Network)**
  - A group of computers and associated devices that share a common communications line and typically share resources within a small geographic area (for example, within an office building)
  - Used for connecting IT infrastructure (computers, printers, servers, scanners etc) existing in a particular office or building or a campus to facilitate sharing of information among the users
- **WAN - (Wide Area Network)**
  - Connecting systems or networks (LANs) spread across multiple locations/geographies /cities/countries
  - Relies on a shared or a common communication backbone
  - Used for connecting the IT infrastructure/LANs across multiple locations to facilitate sharing of information among users spread across different locations

LAN AND WAN


Office 1 in Delhi
LAN
Server
Switch
ROUTER
Office 2 in Mumbai
Server
LAN
Switch
ROUTER
WAN
Leased Line

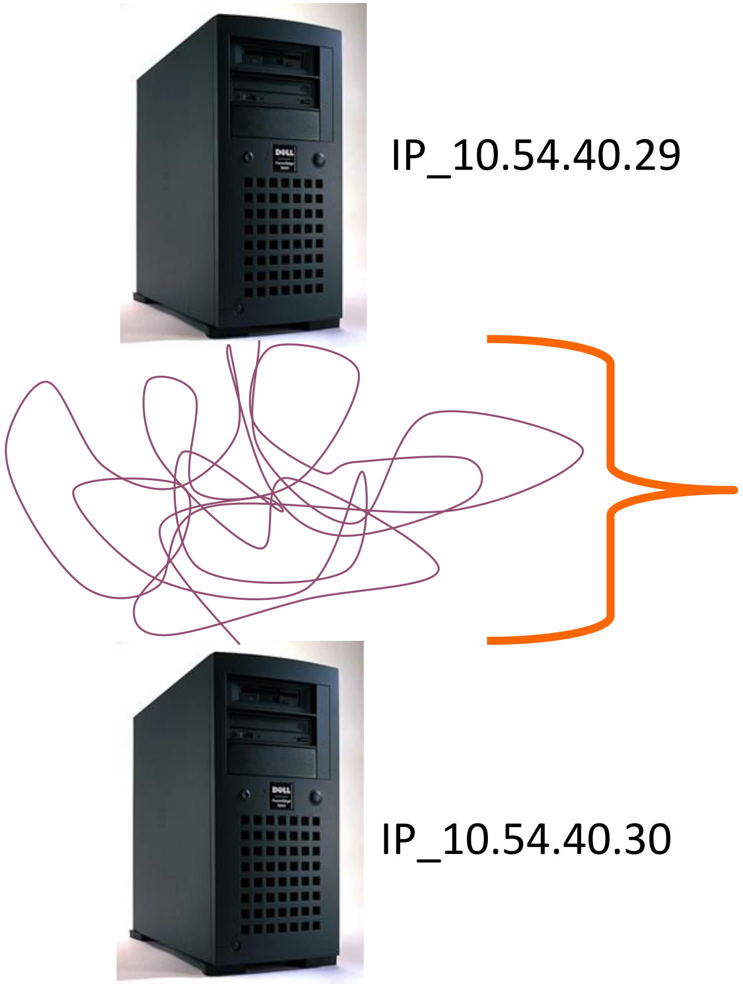
WHAT IS INTERNET

- A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.

- Internet is a public network for facilitating communication among the group of networks connected to the public network

- An intranet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or operational systems within that organization across multiple locations/geographies.

HOW ARE COMPUTERS CONNECTED ON A NETWORK?



IP_10.54.40.29

IP_10.54.40.30

- **IP (Internet Protocol)**: unique address that devices use in order to identify and communicate with each other on a computer network using the IP standard

IMPORTANCE OF SECURITY – THREAT TO DATA

- The Internet is the largest public data network, enabling and facilitating both personal and business communications worldwide. The volume of traffic moving over the Internet, as well as corporate networks, is expanding exponentially every day.
- While the Internet has transformed and greatly improved the way we do business, this vast network and its associated technologies have opened the door to an increasing number of security threats from which corporations must protect themselves.
- An attack may directly cause several hours of downtime for employees, and networks must be taken down in order for damage to be repaired or data to be restored. Clearly, loss of precious time and data can greatly impact employee efficiency and morale !!!
- A single hacker working from a basic computer can generate damage to a large number of computer networks that wreaks havoc around the world. Perhaps even more worrisome is the fact that the threats can come from people we know.
- In fact, most network security experts claim that the majority of network attacks are initiated by employees who work inside the corporations where breaches have occurred. Employees, through mischief, malice, or mistake, often manage to damage their own companies' networks and destroy data.
- Remote employees and partners pose the same threats as internal employees, as well as the risk of security breaches if their remote networking assets are not properly secured and monitored.

WHO ARE THE ENEMIES?

Hackers

- The computer enthusiasts who take pleasure in gaining access to other people’s computers or networks.
- Many hackers are content with simply breaking in and leaving their “footprints,” which are joke applications or messages on computer desktops. Other hackers, often referred to as “crackers,” are more malicious, crashing entire computer systems, stealing or damaging confidential data, defacing Web pages, and ultimately disrupting business. Some amateur hackers merely locate hacking tools online and deploy them without understanding of how they work or their effects.

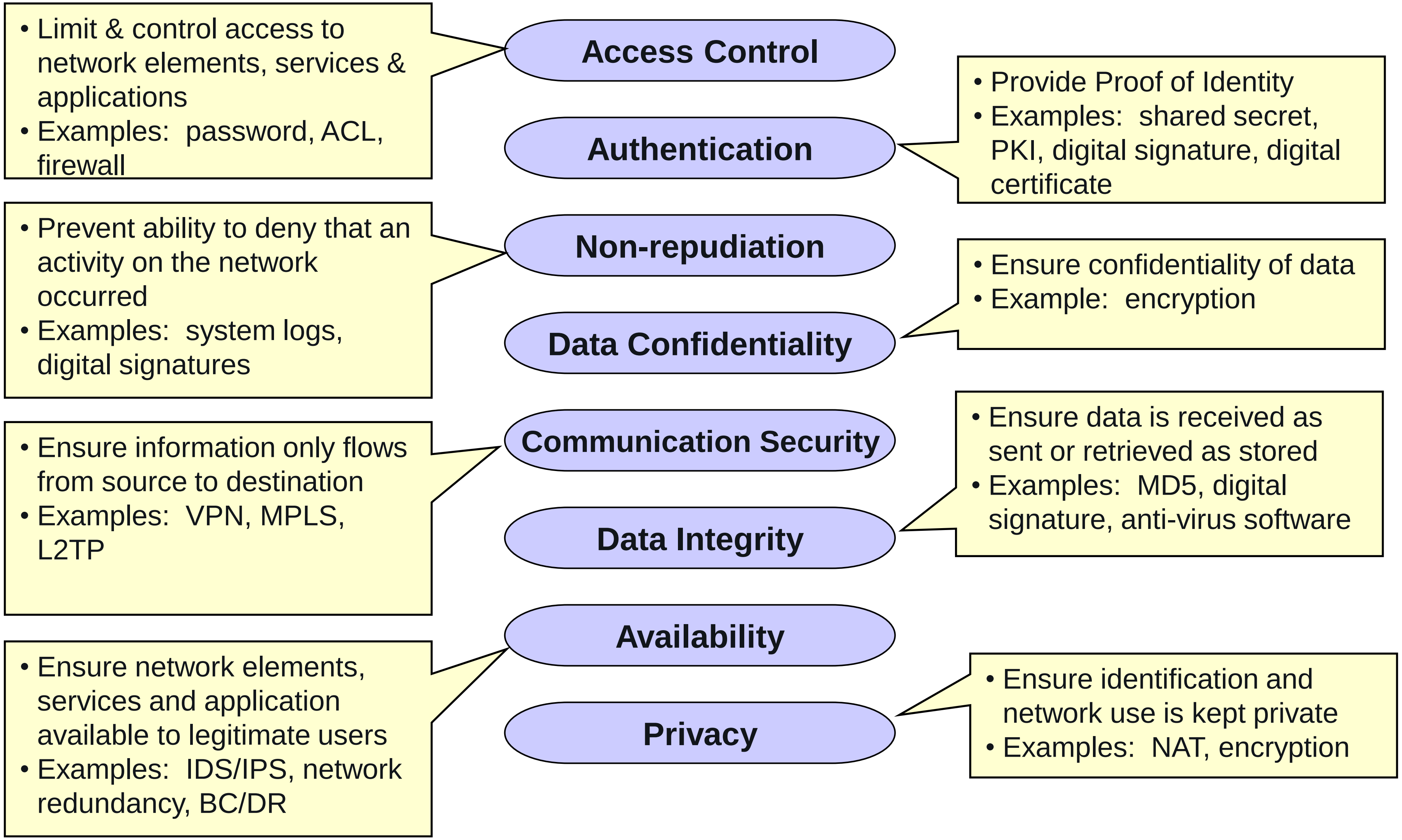
Unaware Staff

- As employees focus on their specific job duties, they often overlook standard network security rules, they might choose passwords that are very simple to remember so that they can log on to their networks easily, such passwords might be easy to guess or crack by hackers using simple common sense or a widely available password cracking software utility
- Employees can unconsciously cause other security breaches including the accidental contraction and spreading of computer viruses
- One of the most common ways to pick up a virus is from a floppy disk or by downloading files from the Internet. Employees who transport data via floppy disks can unwittingly infect their corporate networks with viruses they picked up from computers in copy centers or libraries. They might not even know if viruses are resident on their PCs. Corporations also face the risk of infection when employees download files, such as PowerPoint presentations, from the Internet

Disgruntled Staff

- Far more unsettling than the prospect of employee error causing harm to a network is the potential for an angry or vengeful staff member to inflict damage. Angry employees, often those who have been reprimanded, fired, or laid off, might vindictively infect their corporate networks with viruses or intentionally delete crucial files.
- This group is especially dangerous because it is usually far more aware of the network, the value of the information within it, where high-priority information is located, and the safeguards protecting

SECURITY DIMENSIONS : BREADTH OF NETWORK VULNERABILITIES



Access Control

- Limit & control access to network elements, services & applications
- Examples: password, ACL, firewall

Authentication

- Provide Proof of Identity
- Examples: shared secret, PKI, digital signature, digital certificate

Non-repudiation

- Prevent ability to deny that an activity on the network occurred
- Examples: system logs, digital signatures

Data Confidentiality

- Ensure confidentiality of data
- Example: encryption

Communication Security

- Ensure information only flows from source to destination
- Examples: VPN, MPLS, L2TP

Data Integrity

- Ensure data is received as sent or retrieved as stored
- Examples: MD5, digital signature, anti-virus software

Availability

- Ensure network elements, services and application available to legitimate users
- Examples: IDS/IPS, network redundancy, BC/DR

Privacy

- Ensure identification and network use is kept private
- Examples: NAT, encryption

These Security Dimensions applied to each Security Perspective (layer and plane)

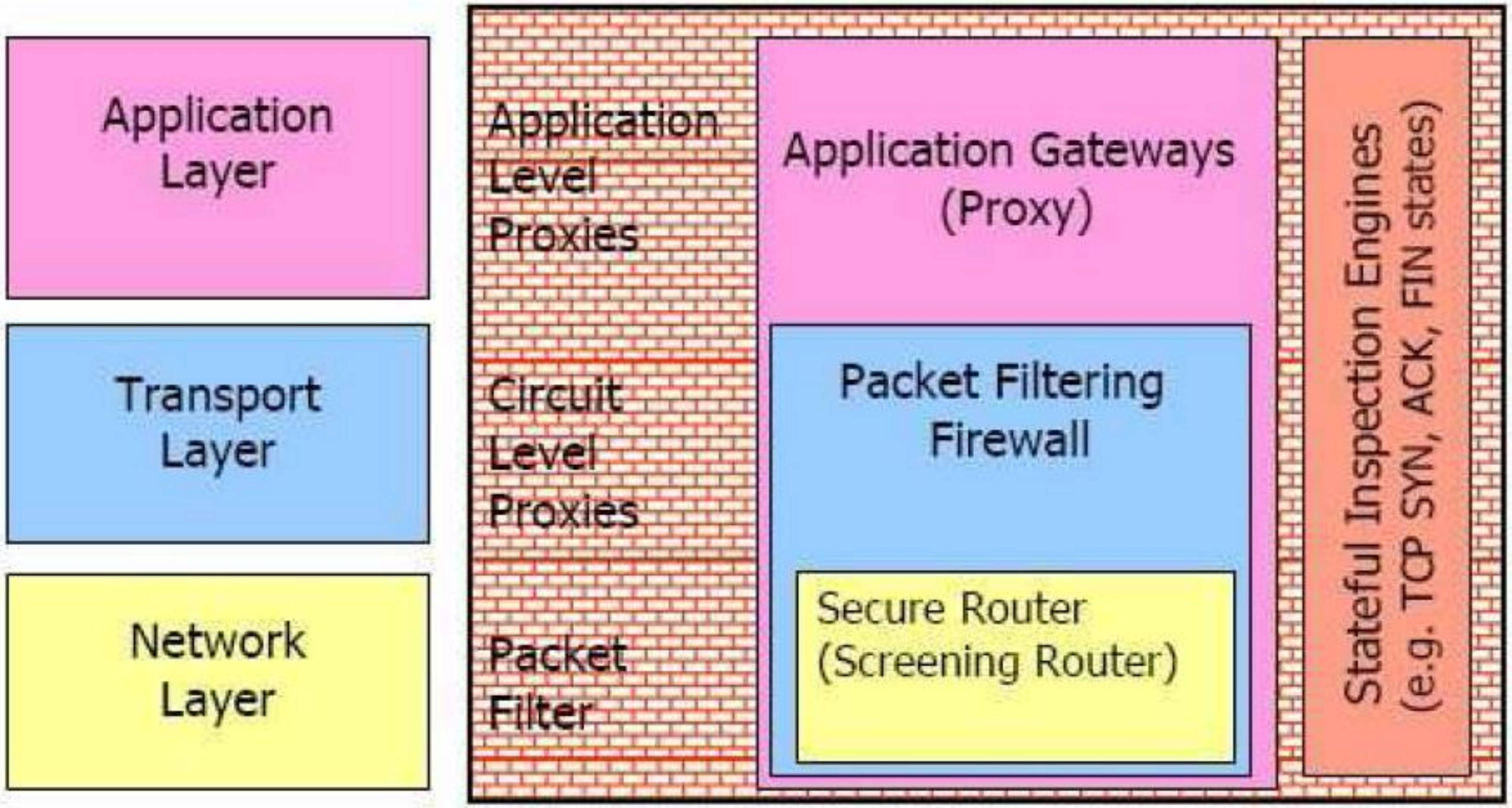
MAJOR NETWORK SECURITY COMPONENTS

1. Firewalls
2. Intrusion Detection System
3. Intrusion Prevention Systems
4. Quarantine
5. Routers
6. AAA Server
7. Antivirus Gateway
8. Virtual Private Networks
9. Network Monitoring Tools

WHAT IS A FIREWALLS

- **A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.**
- **Frequently used to prevent unauthorized internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.**
- **A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.**

CONTROL CAPABILITIES OF FIREWALLS


Application Layer
Transport Layer
Network Layer
Application Level Proxies
Circuit Level Proxies
Packet Filter
Application Gateways (Proxy)
Packet Filtering Firewall
Secure Router (Screening Router)
Stateful Inspection Engines (e.g. TCP SYN, ACK, FIN states)

TYPES OF FIREWALLS

- **Packet filter firewalls:** Evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet.
- **Stateful inspection firewalls:** Are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial “handshake” communicated through TCP flags in the header information. When a connection is established the firewall adds the connection information to a table. The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall.
- **Proxy Server Firewall:** Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network. Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices. They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution’s security policy.
- **Application-level firewalls** perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application. They capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc. Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.

FIREWALL POLICY

- A firewall policy states management’s expectations for how the firewall should function and is a component of the overall security policy.
- It should establish rules for traffic coming into and going out of the security domain and how the firewall will be managed and updated.
- Therefore, it is a type of security policy for the firewall and forms the basis for the firewall rules.
- The firewall selection and the firewall policy should stem from the ongoing security risk assessment process.
- Accordingly, management needs to update the firewall policy as the institution's security needs and the risks change.

WHAT THE FIREWALL POLICY SHOULD ADDRESS?

- Firewall topology and architecture,
- Type of firewall(s) being utilized,
- Physical placement of the firewall components,
- Monitoring firewall traffic,
- Permissible traffic ,
- Firewall updating,
- Coordination with security monitoring and intrusion response mechanisms,
- Responsibility for monitoring and enforcing the firewall policy,
- Protocols and applications permitted,
- Regular auditing of a firewall’s configuration and testing of the firewall’s
- effectiveness, and
- Contingency planning.

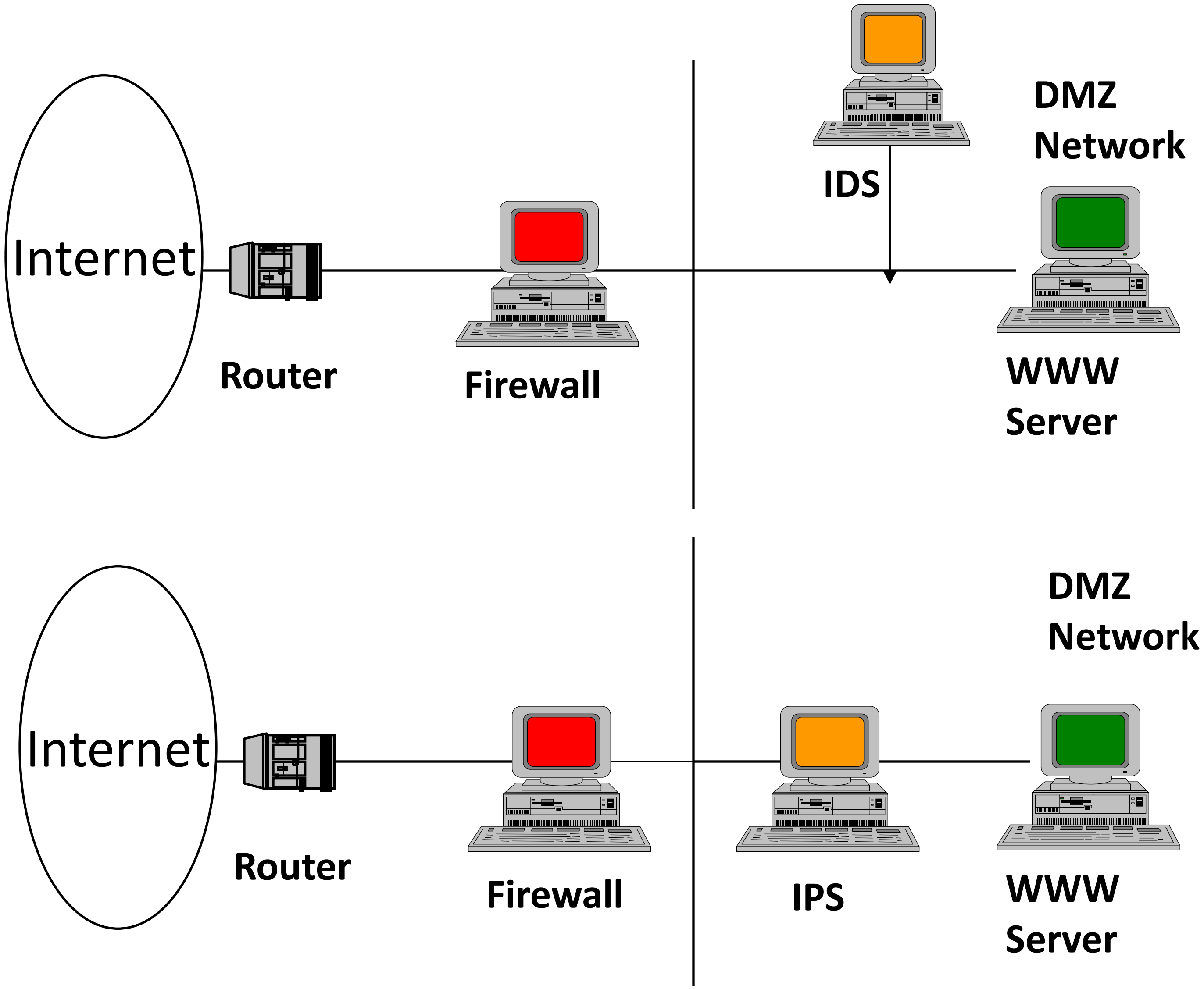
INTRUSION DETECTION SYSTEM (IDS) & INTRUSION PREVENTION SYSTEMS (IPS)

- **Intrusion detection:** is a technique of detecting unauthorized access to a computer system or a computer network. An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system.

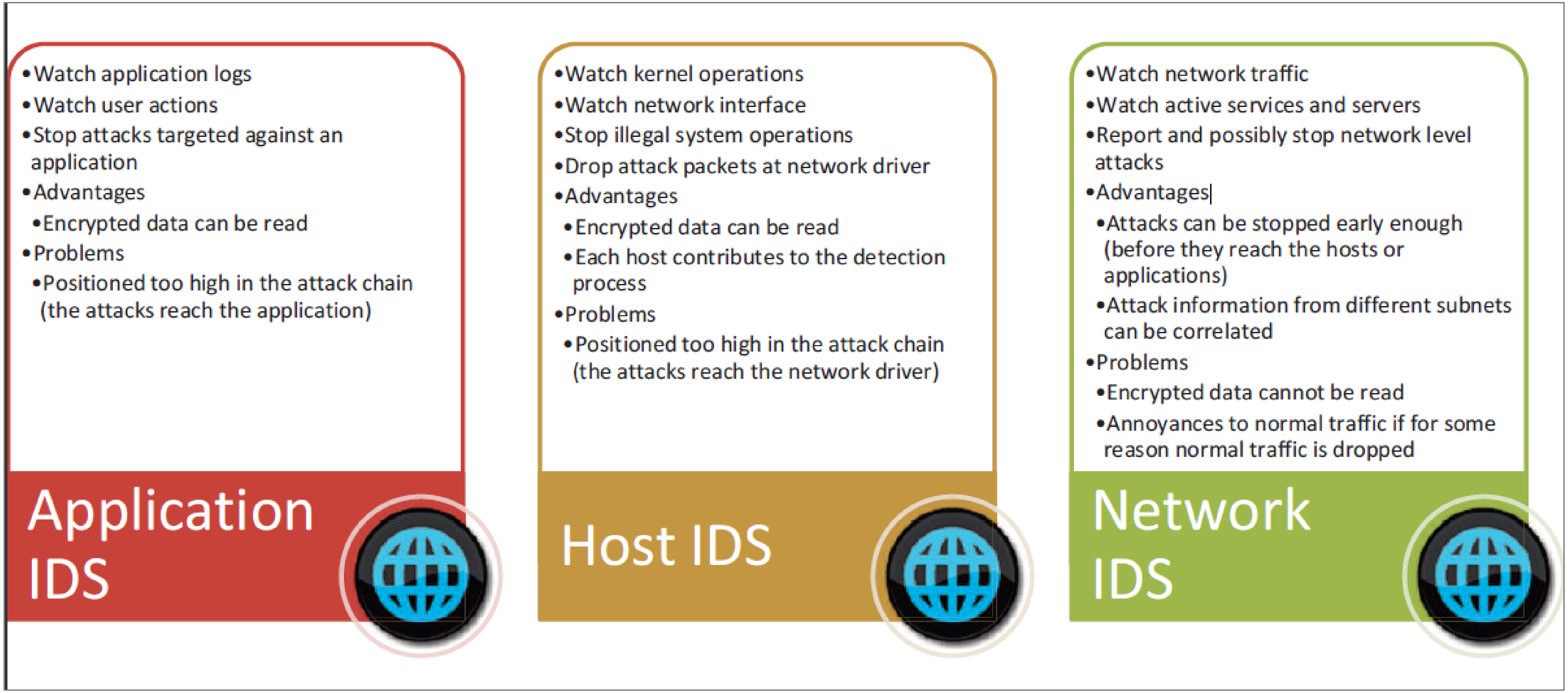
- **Intrusion prevention:** on the other hand, is the art of preventing an unauthorized access of a system's resources.

- The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.

POSITIONING OF IDS / IPS



TYPES OF IDS



Application IDS

- Watch application logs
- Watch user actions
- Stop attacks targeted against an application
- Advantages
  - Encrypted data can be read
- Problems
  - Positioned too high in the attack chain (the attacks reach the application)

Host IDS

- Watch kernel operations
- Watch network interface
- Stop illegal system operations
- Drop attack packets at network driver
- Advantages
  - Encrypted data can be read
  - Each host contributes to the detection process
- Problems
  - Positioned too high in the attack chain (the attacks reach the network driver)

Network IDS

- Watch network traffic
- Watch active services and servers
- Report and possibly stop network level attacks
- Advantages
  - Attacks can be stopped early enough (before they reach the hosts or applications)
  - Attack information from different subnets can be correlated
- Problems
  - Encrypted data cannot be read
  - Annoyances to normal traffic if for some reason normal traffic is dropped

FUNCTIONS OF IDS

The functions of Intrusion detection includes:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations.

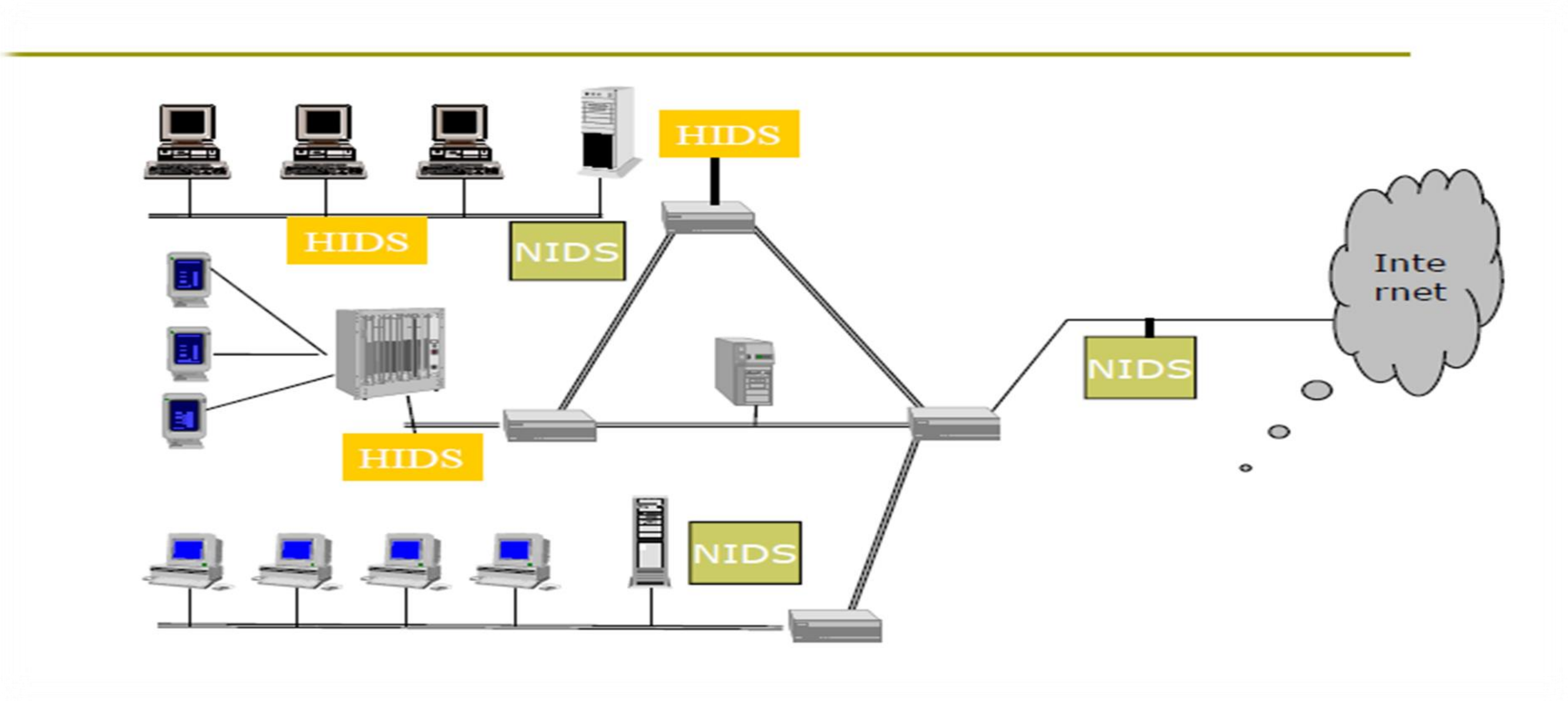
WHAT CAN AN IPS DO?

IPS can detect and block:

- OS, Web and database attacks
- Spyware / Malware
- Instant Messenger
- Peer to Peer (P2P)
- Worm propagation
- Critical outbound data loss (data leakage)

IDS WORKING PROCEDURES

- Types of IDS
    - Host Based IDS
    - Network Based IDS
    - Hybrid Intrusion Detection
    - Network-Node Intrusion Detection (NNID)



HOST-BASED IDS AND ADVANTAGES

- **Host-based Intrusion Detection Systems (HIDS):** are designed to monitor, detect, and respond to user and system activities and attacks on a given host, Host Intrusion can be used to fight out internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host.

- **Some of the HIDS advantages are:**
  - **Host Level protection:-**They are better than NIDS at monitoring and keeping track of local system events. Because Host-based only protects a single system, switches, VPN, and routers do not affect their functionality.
  - **Encrypted Attacks:-**They aren't typically hindered by encrypted attacks. Host-based IDS can read transmitted packets before they are encrypted and received packets after they are decrypted.
  - **Integrity Breaches:-**They can help to detect software integrity breaches, such as Trojan horse software, file modifications, and so on.

NETWORK IDS

- **Network Intrusion Detection Systems:** deals with data packets flowing through the wire between the hosts. They are also referred to as “packet- sniffers,”NID devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP
- **Network Based IDS Advantages-**
  - Increase overall security
  - Protect multiple systems
  - Allow monitoring traffic inside your firewall
  - Alert you to incoming attacks
  - Detect slow attacks
  - Delayed analysis
  - Take corrective action

HYBRID INTRUSION DETECTION

- **Hybrid IDS:** is a combination of host-based IDS and network IDS technologies. Hybrid intrusion detection provides attack recognition on the network packets flowing to and from a single and is host system-based.

- **Advantages:** Hybrid IDS offer management and alert notification from both network and host based intrusion detection devices. A Hybrid IDS offers the best of HIDS and NIDS technologies providing attack recognition on the network packets flowing to and from single hosts.

NETWORK-NODE INTRUSION DETECTION

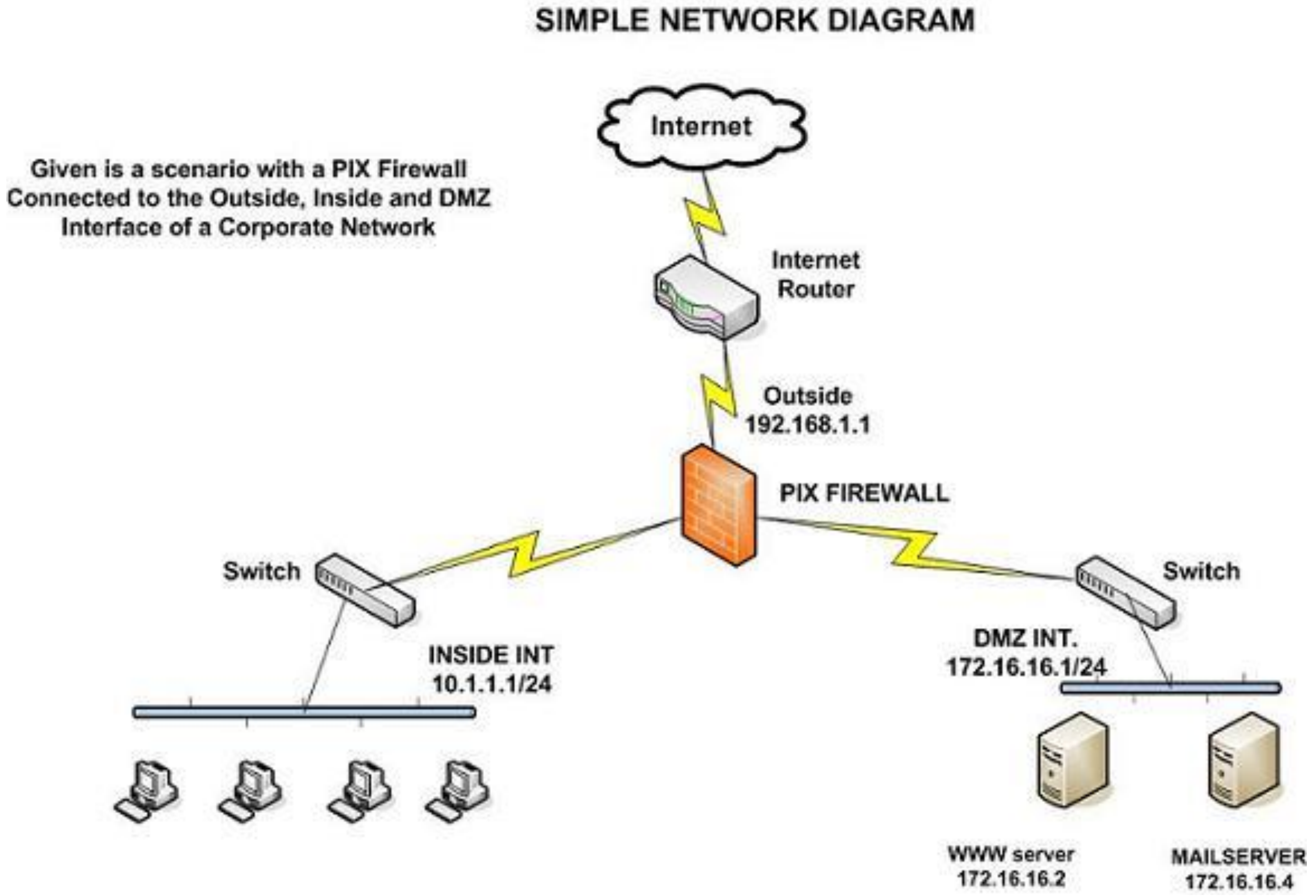
- **Network-node Intrusion Detection:** captures the packet-intercepting technology of the wire and puts it on the hosts. With NNID, the *packet-sniffer* is positioned in such a way that it captures packets after they destination host.
- **Advantages of NNIDS**
  - The advantage to NNID is its ability to defend specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.
  - Since the NNIDS system is not expected to examine individual packet on the wire it is relatively much faster and also less resource intensive. Thus it can be installed on existing servers without imposing too much burden.
  - NNID is suitable for heavy traffic networks, switched network environments, or VPN implementations with encrypted traffic on the wire

QUARANTINE

- Quarantining a device protects the network from potentially malicious code or actions.
- Typically, a device connecting to a security domain is queried for conformance to the domain’s security policy.
- If the device does not conform, it is placed in a restricted part of the network until it does conform.
- For example, if the patch level is not current, the device is not allowed into the security domain until the appropriate patches are downloaded and installed.

ROUTERS

A router (including a wireless router) is a specialized networking device connected to two or more networks running software that allows the router to move data from one network to another. Router functions in an Internet protocol based network operate at the network layer (OSI Model's layer 3). The primary function of a router is to connect networks together and keep certain kinds of broadcast traffic under control.



AUTHENTICATION, AUTHORIZATION AND ACCOUNTING

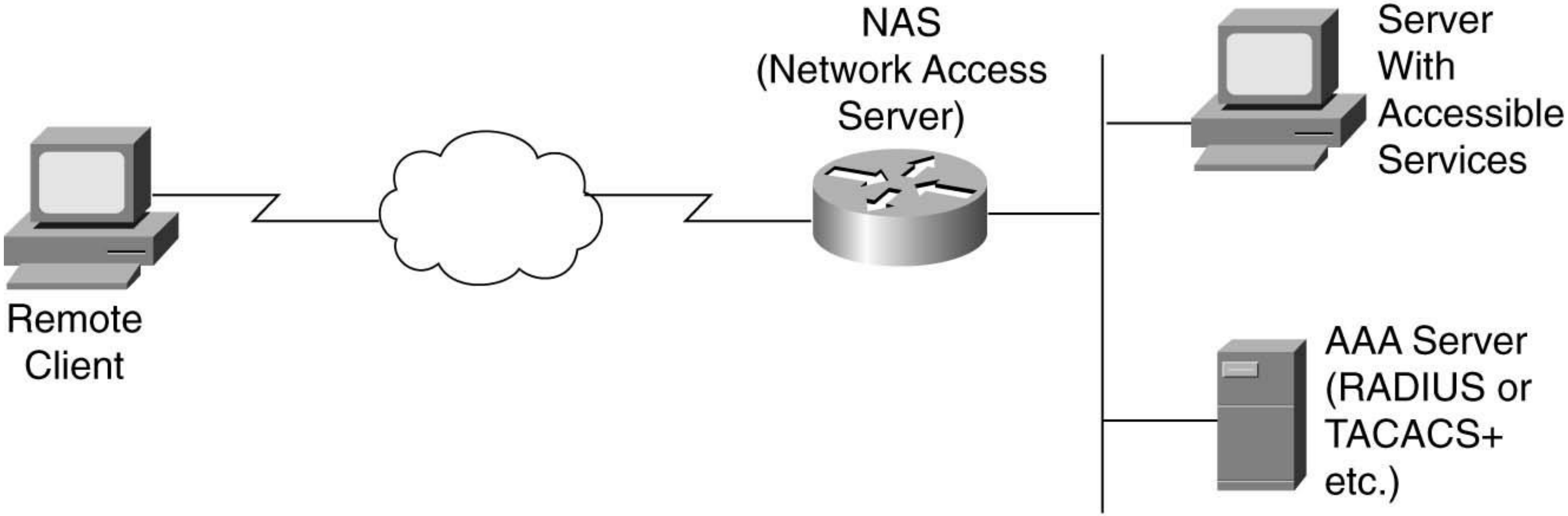
It is a system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.

- **Authentication** is the process of identifying an individual, usually based on a username and password. Authentication is based on the idea that each individual user will have unique information that sets him or her apart from other users.
- **Authorization** is the process of granting or denying a user access to network resources once the user has been authenticated through the username and password. The amount of information and the amount of services the user has access to depend on the user's authorization level.
- **Accounting** is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing and cost allocation.

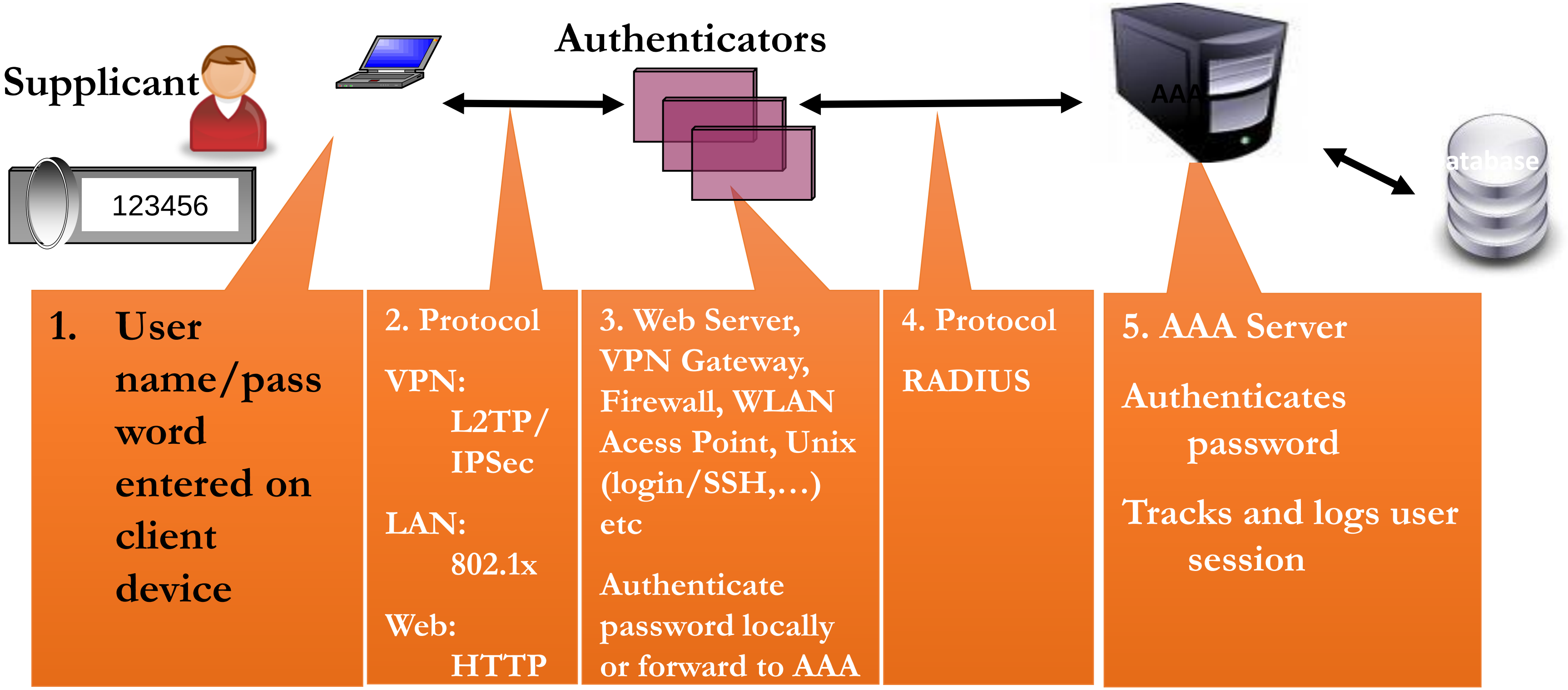
AAA COMPONENTS

- **AAA server**
    - Authenticates users accessing a device or network
    - Authorizes user to perform specific activities
    - Performs accounting of device or user activities
- **Network Access Server (NAS) or Access Device**
    - A router, switch, or other network device that can perform AAA functions on users or devices connecting to it
- **RADIUS or TACACS+**
    - Protocols that can be used by an access device to communicate with the AAA server

AAA NETWORK COMPONENTS


Remote Client
NAS (Network Access Server)
Server With Accessible Services
AAA Server (RADIUS or TACACS+ etc.)

HOW THE AAA SERVER WORKS



1. User name/password entered on client device

2. Protocol

VPN:
L2TP/IPSec

LAN:
802.1x

Web:
HTTP

3. Web Server, VPN Gateway, Firewall, WLAN Acess Point, Unix (login/SSH,…) etc

Authenticate password locally or forward to AAA

4. Protocol

RADIUS

5. AAA Server

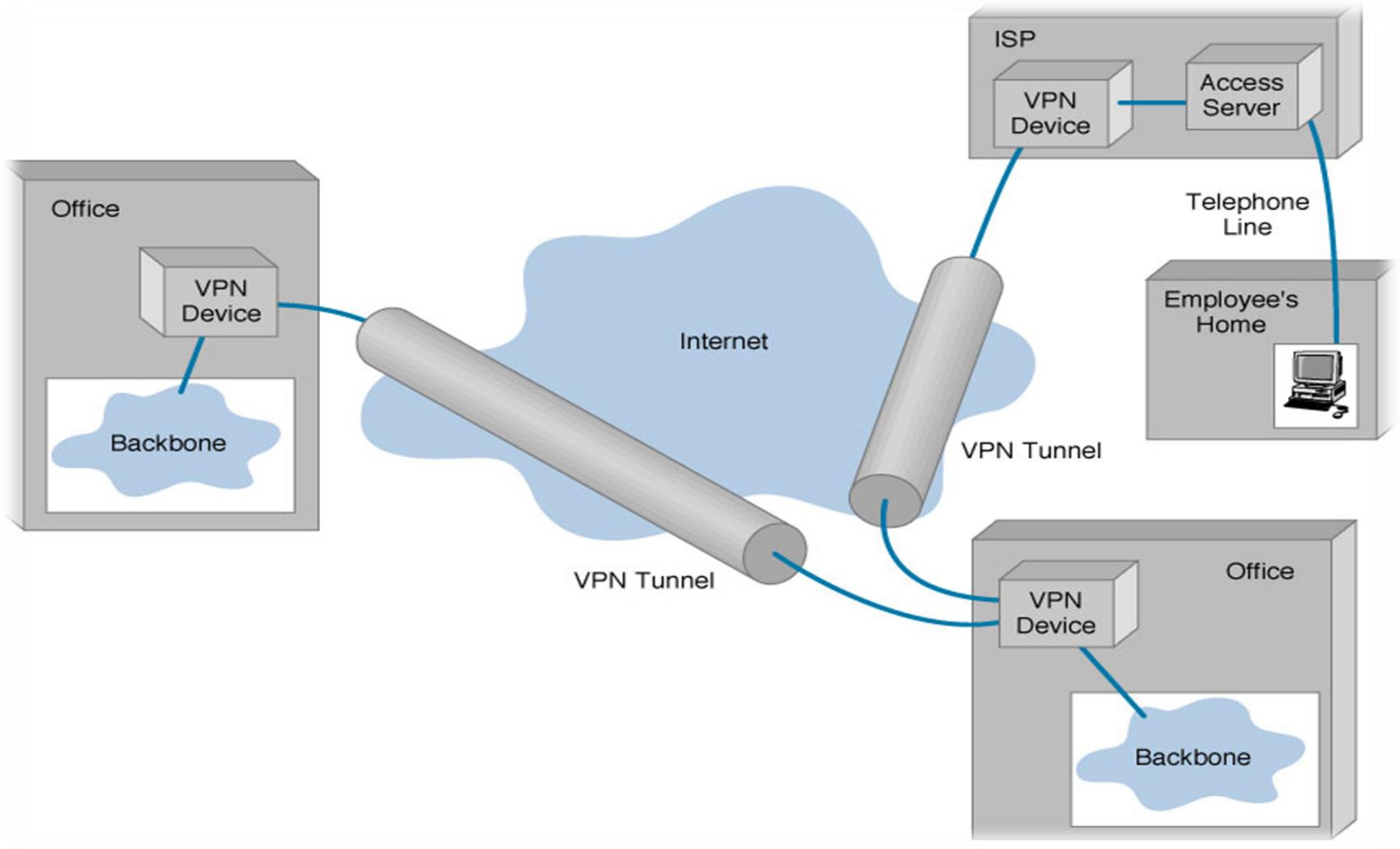
Authenticates password

Tracks and logs user session

WHAT IS VPN?

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.

BASIC ARCHITECTURE OF VIRTUAL PRIVATE NETWORKS (VPN)



PRIVATE NETWORKS VS. VIRTUAL PRIVATE NETWORKS

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability

VPN TYPES

- **Intranet VPN**
  - Provides virtual circuits between organization offices over the Internet
- **Extranet VPN**
  - Same as an intranet VPN except that the VPN connects several different organizations, e.g., customers and suppliers, over the Internet
- **Access VPN**
  - Enables employees to access an organization's networks from remote locations

ADVANTAGES AND DISADVANTAGES OF VPN

ADVANTAGES:

- Flexibility of growth
- Efficiency with broadband technology

- **DISADVANTAGES:**
- VPNs require an in-depth understanding of public network security issues and proper deployment of precautions
- Availability and performance depends on factors largely outside of their control
- Evolving standards
- VPNs need to accommodate protocols other than IP and existing internal network technology

ANTIVIRUS GATEWAY

- The most common transmission routes for viruses and worms are through email and Web traffic.
- In addition, the growing volume of unsolicited email (spam) and inappropriate Web surfing poses risks to corporate security, liability, and employee productivity.
- Effective security at every network tier—especially virus protection at the Internet gateway—is essential in today’s Internet-enabled network environments.
- Gateway Solution provides multi-layered protection against viruses, spam, and unwanted email and Web content at the Internet gateway.

NEED OF NETWORK MANAGEMENT

- It lowers costs by eliminating the need for many administrators at multiple locations performing the same function
- Makes network administration and monitoring easier and more convenient
- Coherent presentation of data.
- Performance Management – how smoothly is the network running
- Fault Management - reactive and proactive network fault management (deals with problems and emergencies in the network)
- Configuration Management – keeping track of device settings and how they function
- Accounting Management - cost management and charge back assessment
- Security Management

WHAT ARE NETWORK MONITORING TOOLS?

- They allow the administrator to know the health status of the network.
- Provides information about collected data and the analysis of such raw data with a view to using scarce or limited resources effectively.
- They use network probe. Probes let you isolate traffic problems and congestions slowing your network to a crawl.
- Network Monitoring tools can apply various security policies at the click of a mouse to all the network devices available in the network.

THANKS