Introduction to Network Security

Unit -3 [4 H]

Outlines

- Fundamentals of Network Security
- Principal methods of Protecting Network (Encryption, Decryption, Encryption in network)
- Network organization (Firewalls and Proxies, Analysis of the Network Infrastructure)
- DMZ
- Types of Firewalls (Packet Filtering, State-full Filtering, Circuit Level Gateway, Application level/proxy)
- IPSec
- VPN

Network Security

- Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

- “Network security is any activity to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network” - Cisco

Network Security

The top network security fundamental are:

1. Keep patches and update current versions.
2. Use strong passwords
   - Don’t use any words from the dictionary.
   - Don’t use anything related to your name, nickname, family members or pets.
   - Don’t use any numbers someone could guess by looking at your mail like phone numbers and street numbers.
   - Choose a phrase that means something to you, take the first letters of each word and convert some in characters.
3. Secure your VPN.
4. Actively manage user access privileges.
5. Clean up inactive accounts.

Network Security Model

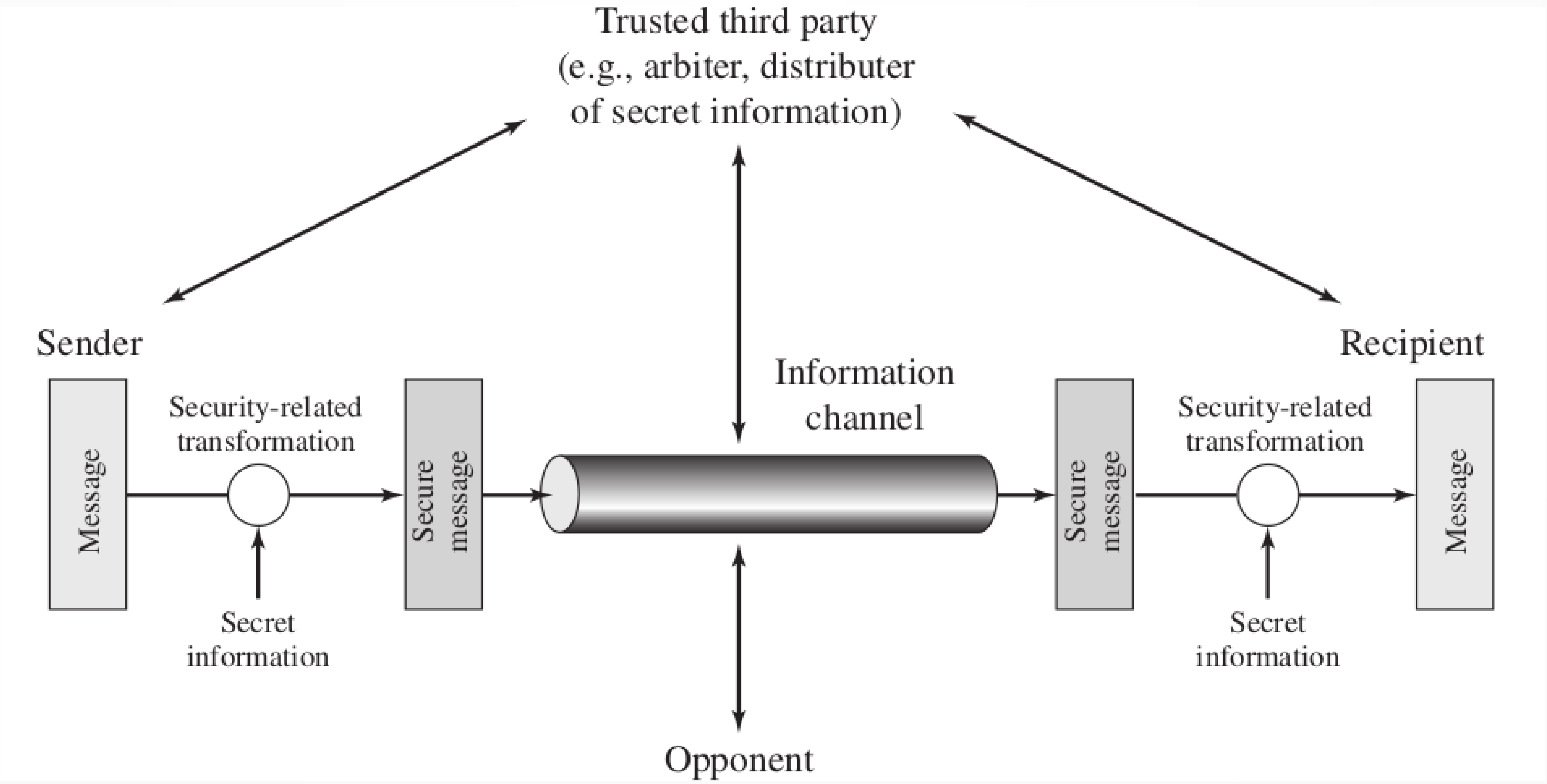


Figure: Model for Network Security

Network Security Model

Techniques for providing security have two components:

I. A security related transformation on the information to be sent. For example, the encryption of the message, MAC

II. Some secret information shared by two principals only. For example, an encryption key.

A third party may be needed to achieve secure transmission. For example, distributing the secret information to the two principals, settlement of disputes between two principals about the authenticity.

Network Access Security Model

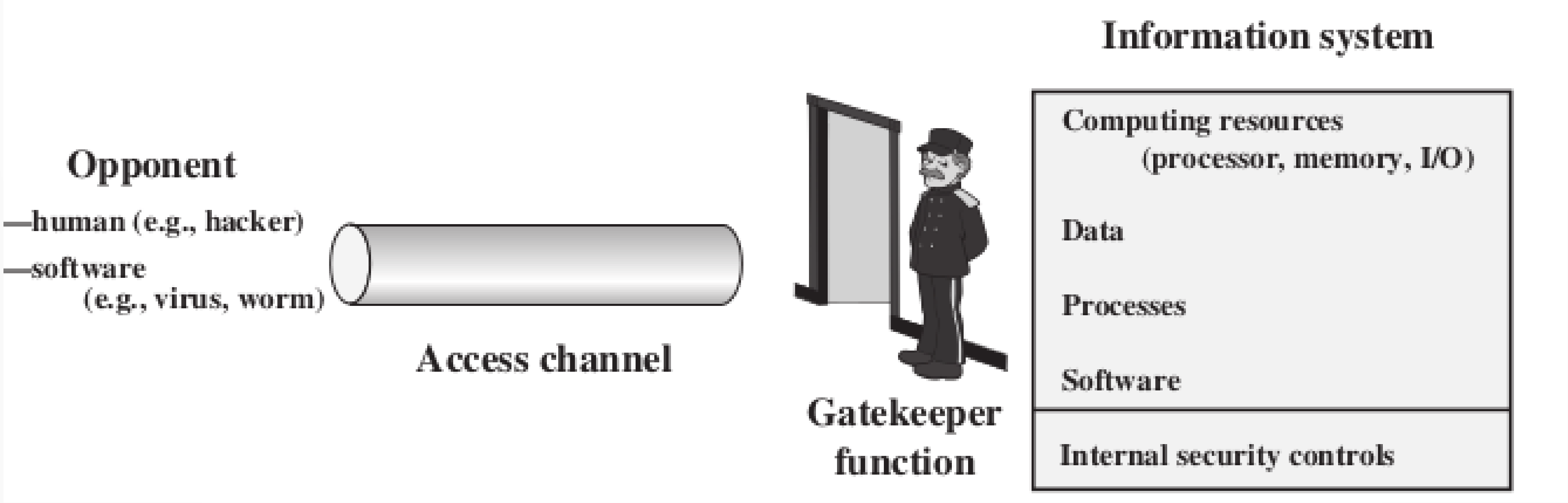


Figure: Network Access Security Model

Network Access Security Model

- Gatekeeper function includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

Network Access Security Model

- This model reflects a concern for protecting an information system from unwanted access like:
  - Hackers' attempt to penetrate systems that can be accessed over a network.
  - Intruders' wish to do damage or exploit computer assets for financial gain.
  - Placement of a logic that exploits vulnerabilities in the system and affects application and/or utility program.

Principals methods of protecting networks

- Encryption
- Decryption
- Encryption in network

Principals methods of protecting networks

- Network encryption is the process of encrypting or encoding data and messages transmitted or communicated over a computer network.
- It is a broad process that includes various tools, techniques and standards to ensure that the message are unreadable when in transit between two or more network nodes.
- Network encryption is primarily implemented on the network layer of the OSI model.

Principals methods of protecting networks

- The encryption services are generally provided by encryption software or through an integrated encryption algorithm on network devices and/or in software.
- On an IP-based network, network encryption is implemented through Internet Protocol Security (IPSec)-based encryption techniques and standard.
- Each message sent is in an encrypted form and is decrypted and converted back into plain text/original form at the recipeint’s end using encryption/decryption keys.

Principals methods of protecting networks

- Using the existing network services and application software, network encryption is invisible to the end user and operates independently of any other encryption processes used.
- Network encryption products and services are offered by a number of companies, such as cisco.

Network Organization

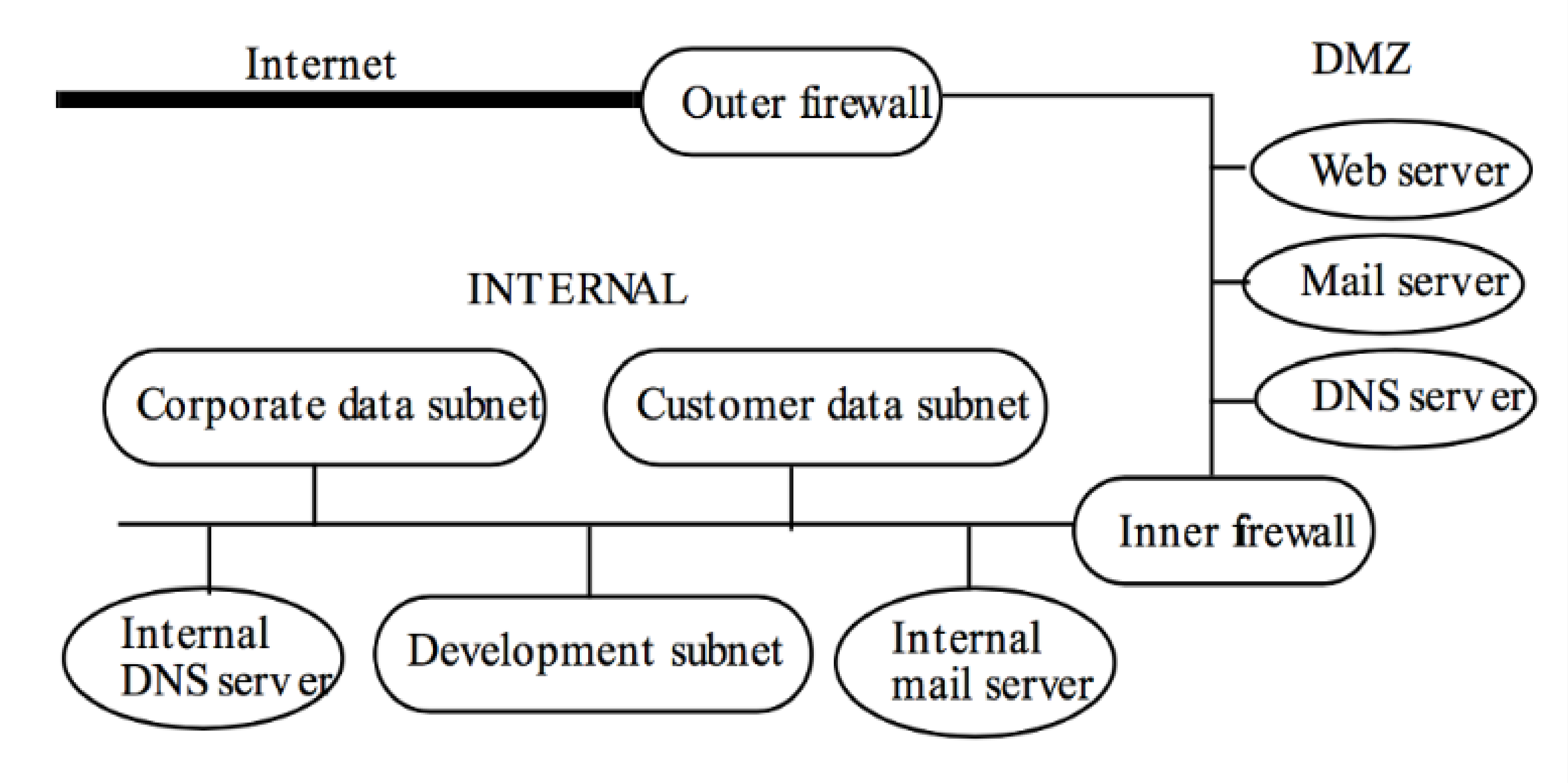


Figure: Network Designed for Dribble Corporation

Firewalls and Proxies

- A firewall is a host that mediates access to a network, allowing and disallowing certain types of access on the basis of a configured security policy.
- The firewall accepts or rejects messages on the basis of external information, such as destination addresses or ports, rather than on the basis of the contents of the messages.

Filtering Firewall

- A *filtering firewall* performs access control on the basis of attributes of the packet header, such as destination addresses, source addresses, and options.
- Routers and other infrastructure systems are typical examples of filtering firewalls. They allow connections through the firewall, usually on the basis of source and destination and ports.

Proxy

- A *proxy* is an intermediate agent or server that acts on behalf of an end point without allowing a direct connection between two endpoints.
- Proxy never allows such a direct connection between two endpoints.
- A proxy (or application level) firewall uses proxies to perform access control.

Demilitarized Zone (DMZ)

- The DMZ is a physical or logical subnet portion of a network that separates a purely internal network from an external network.
- The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled.
- The DMZ functions as a small, isolated network positioned between the Internet and the private network.
- It is often refereed to as a *perimeter network* or *screened subnet*.
- Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are:
  - Web servers
  - Mail servers
  - FTP servers
  - VoIP servers
  - DNS server

Demilitarized Zone (DMZ) Design

There are many different ways to design a network with a DMZ. Two of the most basic methods are with a *single firewall*, also known as the three legged model, and with *dual firewalls*, also known as back to back.

- **Single Firewall:**
  - A single firewall with at least 3 network interfaces can be used to create a network architecture containing a DMZ.
  - The external network is formed from the ISP to the firewall on the first network interface, the internal network is formed from the second network interface, and the DMZ is formed from the third network interface.
  - The firewall becomes a single point of failure for the network and must be able to handle all of the traffic going to the DMZ as well as the internal network.

Demilitarized Zone (DMZ) Design

Dual Firewall

- The most secure approach is to use two firewalls to create a DMZ. The first firewall (also called the "front-end" or "perimeter firewall) must be configured to allow traffic destined to the DMZ only.
- The second firewall (also called "back-end" or "internal" firewall) only allows traffic to the DMZ from the internal network.
- This setup is considered more secure since two devices would need to be compromised.

DMZ

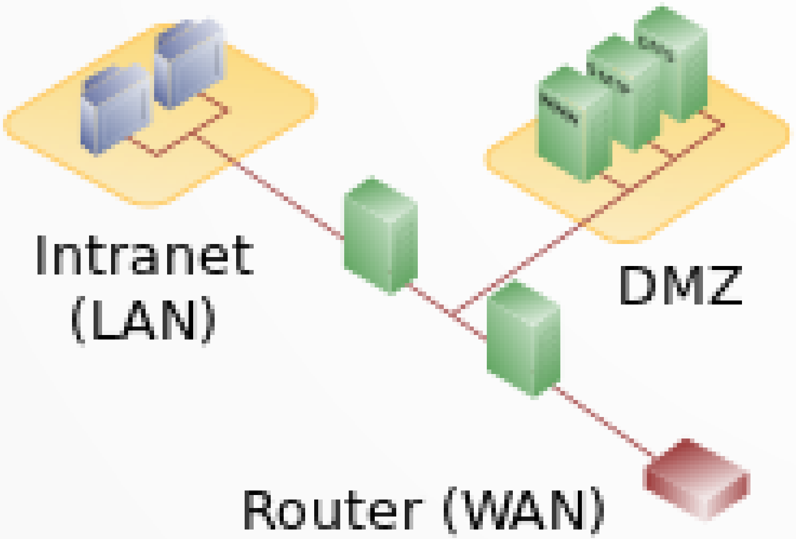


Figure: Dual DMZ

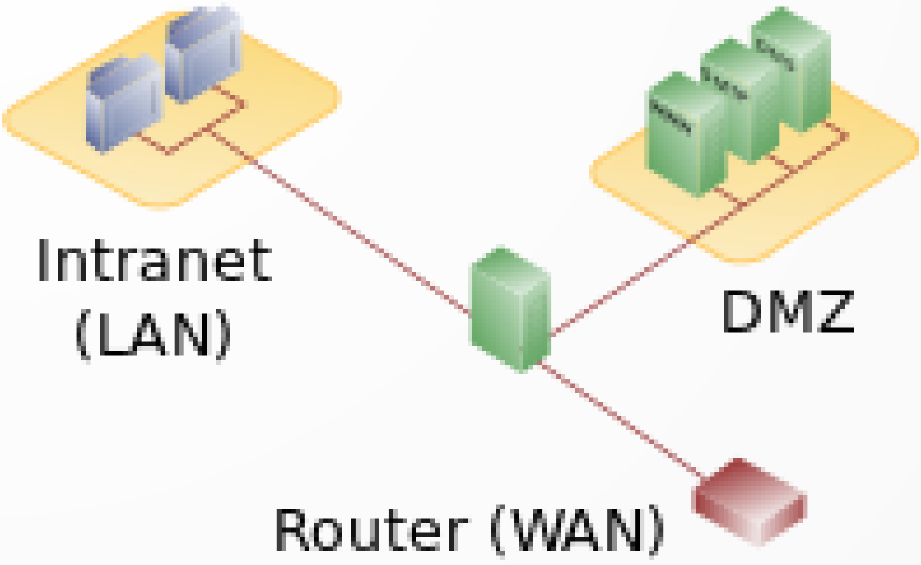


Figure: Single DMZ

Demilitarized Zone (DMZ) Design

- For example, a network intrusion detection and prevention system located in a DMZ that only contains a Web Server can block all traffic except HTTP and HTTPS requests on ports 80 and 443.

What is Network Infrastructure?

- **Network infrastructure** refers to all of the resources of a network that make network or internet connectivity, management, business operations and communication possible.
- Network infrastructure comprises hardware and software, systems and devices, and it enables computing and communication between users, services, applications and processes.
- Anything involved in the network, from servers to wireless routers, comes together to make up a system’s network infrastructure.
- Network infrastructure allows for effective communication and service between users, applications, services, devices and so forth.
- Network infrastructure are critical to the success of a business.

Analysis of Network Infrastructure

- The security policy distinguishes “**public**” entities from those internal to the corporation, but recognizes that some corporate resources must be allowed to the public.
- The public entities may enter the corporate perimeter (bounded by the “**outer firewall**”) but are confined to the DMZ area (bounded inside by the “**inner firewall**”)
- The key decision is to limit the flow of information from the internal network to the DMZ.

Analysis of Network Infrastructure

- The public cannot communicate directly with any system in the internal network, nor can any system in the internal network communicate directly with other systems on the Internet.
- The systems in the DMZ serve as mediators with the firewalls providing the guards.
- The firewalls and the DMZ systems control all access to and from the Internet and filter all traffic in both directions.

Analysis of Network Infrastructure

- The first step is to hide the addresses of the internal network.
- In general, the internal network address can be any IP addressess, and the inner firewall can use a protocol such as the ***Network Address Translator (NAT)*** to map these internal host addresses to the firewall's Internet address.
- A more common method is to assign each host an address but not allow those addresses to leave the corporate network.

Analysis of Network Infrastructure

- All services are implemented as proxies in the outer firewall. However, electronic mail presents a special problem.
- The **DMZ mail server** must know an address in order for the internal mail server to pass mail back and forth.
- This need not be the actual address of the internal mail server. It could be a distinguished address that the inner firewall will recognize as representing the internal mail server.
- Similarly, the internal mail server must know an address for the DMZ mail server.
- The web server lies in the DMZ for the same reasons that a mail server lies in the DMZ. External connections to the Web Server go into the DMZ and no farther.
- If any information is to be transmitted from the web server to the internal network (for example, the customer data subnet), the transmission is made separately, and not as part of Web Transaction.

Analysis of Network Infrastructure

- The goals of the **outer firewall** is to restrict public access to the internal network and to restrict internal network to Internet.
- To implement the required access control the firewall uses an *access control list*, which binds source addresses and ports and destination addresses and ports to access rights.
- The public needs to be able to access the Web server and mail server, and no other services. The firewall therefore presents an interface that allows connections to WWW services (HTTP and HTTPS) and to electronic mail (SMTP).

Analysis of Network Infrastructure

- Like the outer firewall , the **inner firewall** allows a limited set of traffic through it.
- It allows SMTP connection using proxies, but all electronics mail is sent to the DMZ mails server for disposition.
- It allows a limited transfer of information to the DNS server in the DMZ.
- It allows system administrators to access the systems in the DMZ from a trusted administrative server. All other traffic, including Web access is blocked.

Analysis of Network Infrastructure

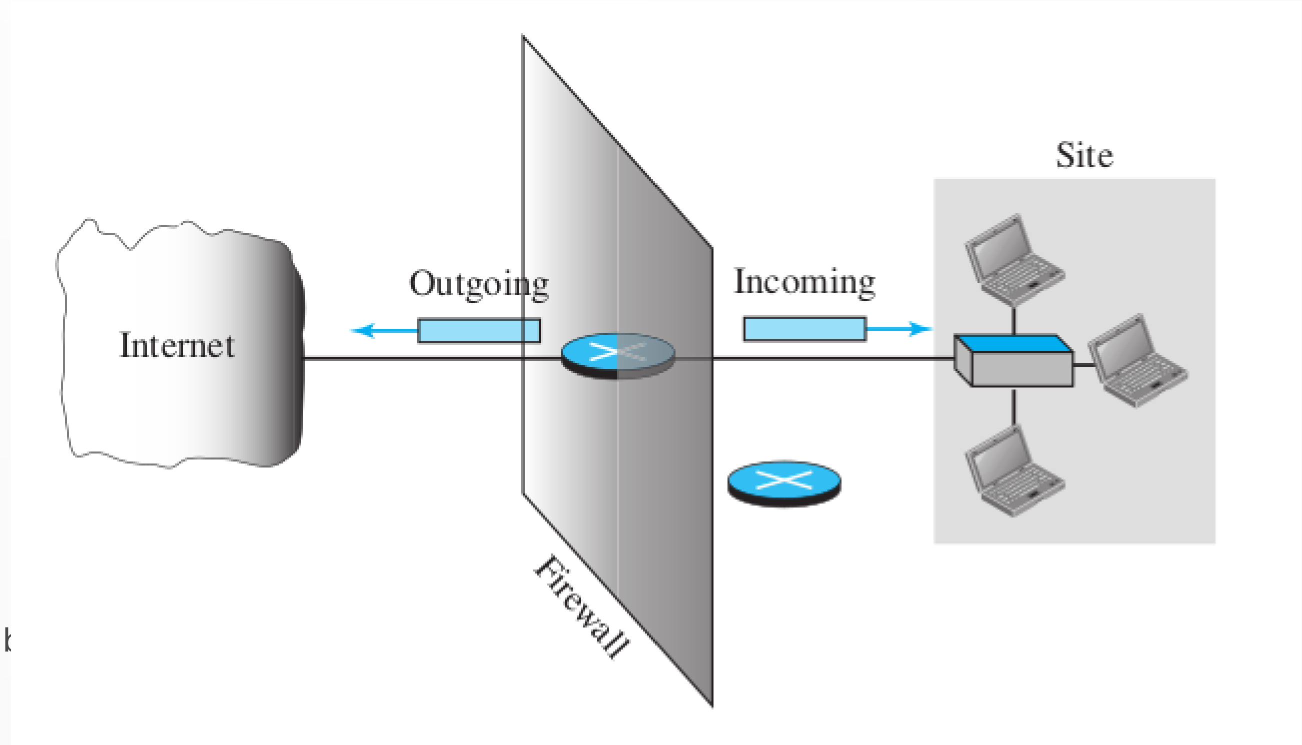
- The **mail server** in the DMZ performs address and content checking on all electronic mail messages.
- The goal is to hide internal information from the outside while being transparent to the inside.
- The web server accepts and services requests from the Internet. It does not contact any servers or information sources within the internal network.
- This means that if the web server is compromised, the compromise cannot affect internal hosts.

Analysis of Network Infrastructure

- The **DMZ DNS** host contains directory name service information about those hosts that the DMZ servers must know.
- It contains entries for the following:
  - DMZ mail, Web hosts
  - Internal trusted administrative host
  - Outer firewall
  - Inner firewall

Types of Firewalls

- Packet Filtering firewall
- Stateful Inspection Firewall
- Application Proxy Firewall
- Circuit-Level Firewall



Packet Filtering Firewall

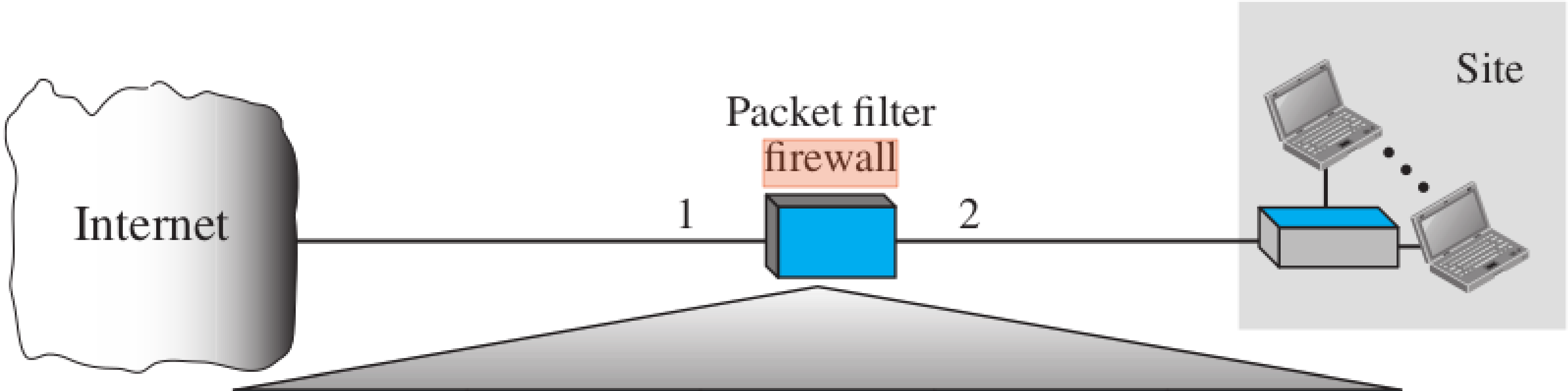
- A packet filtering firewall is a router that uses filtering table to decide which packet must be discarded (not forwarded).
- Filtering rule are based on information contained in a network packet such as:
  - Source IP address
  - Destination IP address
  - Source and destination port address
  - IP protocol field
  - interface

Packet Filtering Firewall

- Advantages of packet filtering firewall is its simplicity. Also, packet filter typically are transparent to users and are very fast.
- Because packet-filter firewalls do not examine upper-layer data, they cannot specify attacks the employ application specific vulnerabilities or functions.

Packet Filtering Firewall

Example



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

Packet Filtering Firewall

- According to the figure, the following packets are filtered:
  1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means “any.”
  2. Incoming packets destined for any internal TELNET server (port 23) are blocked.
  3. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.
  4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

Circuit Level Gateway Firewall

- The circuit level gateway firewall works at the transport and session layer of the OSI model.
- Circuit level gateways verify established TCP connections to determine whether the session being initiated is legitimate -- whether the remote system is considered truste and keep track of active sessions.
- They don't inspect the packets themselves
- Primarily, they determine the security of an established connection.
- When an internal device initiates a connection with a remote host, circuit-level gateways establish a virtual connection on behalf of the internal device to keep the identity and IP address of the internal user hidden.

Circuit Level Gateway Firewall

- Once the two connections are established the gateway typically relays TCP segments from one connection to the other without examining the contents.
- The security function consists of determining which connections will be allowed.
- Circuit-level gateways are cost-efficient, simplistic and have barely any impact on a network’s performance. However, their inability to inspect the content of data packets makes them an incomplete security solution on their own. A data packet containing malware can bypass a circuit-level gateway easily if it has a legitimate TCP handshake. That is why another type of firewall is often configured on top of circuit-level gateways for added protection.

Application Level Gateway

- Sometimes referred to as a *proxy firewall* it is mplemented at the application layer via proxy device.
- Instead of an outsider accessing your internal network directly, the connection is established through the proxy firewall.
- The external client sends a request to the proxy firewall. After verifying the authenticity of the request, the proxy firewall forwards it to one of the internal devices or servers on the client’s behalf.
- Alternatively, an internal device may request access to a webpage, and the proxy device will forward the request while hiding the identity and location of the internal devices and network.
-

Application Level Gateways

- Unlike packet filtering firewalls, proxy firewalls perform stateful and deep packet inspection to analyze the context and content of data packets against a set of user-defined rules. Based on the outcome, they either permit or discard a packet.
- They protect the identity and location of your sensitive resources by preventing a direct connection between internal systems and external networks.
- However, configuring them to achieve optimal network protection can be a bit hard. You must also keep in mind the tradeoff—a proxy firewall is essentially an extra barrier between the host and the client, causing considerable slowdowns. (introduce a delay in communications.)

Stateful Inspection Firewall

- State-aware devices not only examine each packet, but also keep track of whether or not that packet is part of an established TCP or other network session. This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.
- It monitors the entire session for the state of the connection, while also checking IP addresses and payloads for more thorough security.
- Only packets matching the a known active connection is allowed to pass the firewall.
- It is also known as dynamic packet filtering and Stateful inspection filtering

Stateful Inspection Firewall

- In a firewall that uses stateful inspection the network administrator can set the parameters to meet specific needs.
- In a typical network, ports are closed unless an incoming packet request connection to a specific port and then only then that port is opened. This practice prevents port scanning, a well known hacking technique.
- Stateful inspection firewall is a resource intensive and requires interface with the high speed network communication Thus, more expensive than other firewalls.

Internet Protocol Security (IPSec)

- Internet Protocol Security (Ipsec) is a network protocol suite that authenticates and encrypts the packets of data sent over a network.
- It is a set of protocols to provide security for a packet at the network layer.
- It is a standard framework for ensuring private communication over public network, VPN (Virtual Private Network)

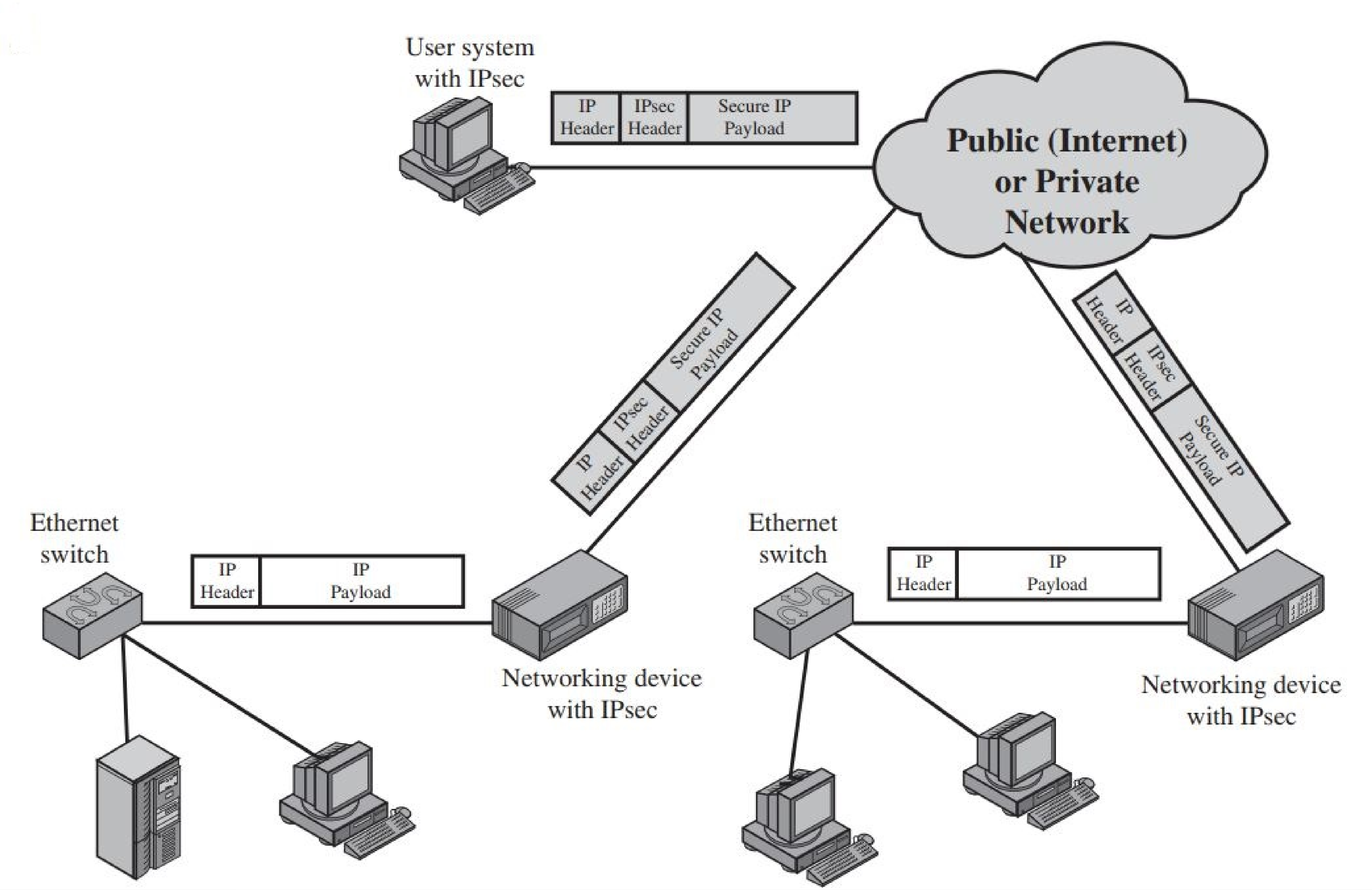


Figure: An IPsec Scenario

IPSec: Two Modes

- IPSec operates in one of two different mode: *transport mode and tunnel mode.*

  Transport Mode
  - Transport mode protects the payload to be encapsulated in the network layer i.e. it protects what is delivered from the transport layer to the network layer.
  - It does not protect the whole IP header or in other words, it does not protect the whole IP packet.

  Tunnel Model
  - In tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header

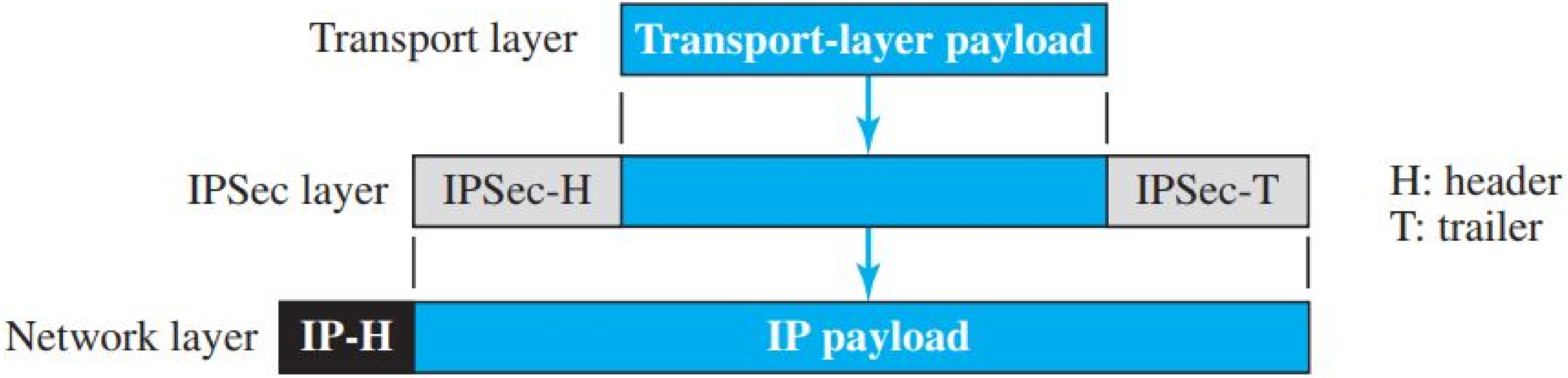


Figure: IPSec in Transport mode

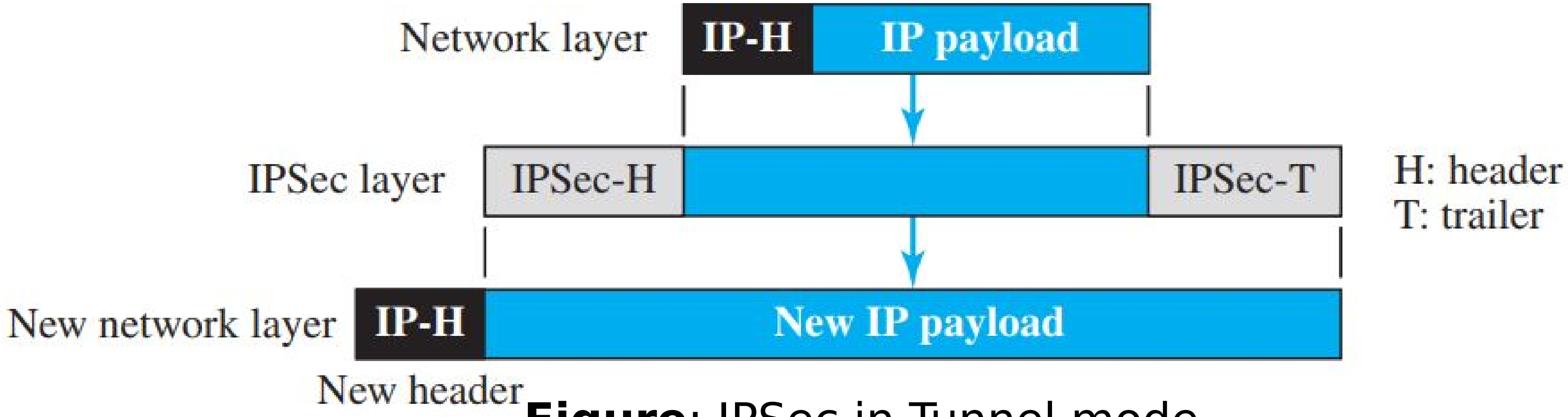


Figure: IPSec in Tunnel mode

IPSec Components

IPSec provides two security protocols :

1. **Authentication Header (AH):** AH is an extension header to provide message authentication. Because message authentication is provided by ESP, the use of AH is deprecated.
2. **Encapsulating Security Payload (ESP)**: ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication and integrity protection

- **Internet Key Exchange (IKE) protocol**
  - IPSec uses IKE to negotiate IPSec connection settings.
  - Authenticate endpoints to each other.
  - Define the security parameters of IPSec-protected connections
  - Negotiate secret keys and
  - Manage, update, and delect IPSec-protected communication channels.

IPSec Components

- IP Payload Compression Protocol (IPComp)
  - Optionally, IPSec can use IPComp to compress payloads before encrypting them.

IPSec Application

- Secure branch office connectivity over the Internet (VPN) secure remote access over the internet.
- Establishing extranet and intranet connectivity with partners.
- Enhancing electronic commerce security.

Virtual Private Network

- One of the applications of IPSec is in *virtual private networks*.
- VPN creates a network that is *private but virtual*. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.
- It is build on top of existing physical networks and provides a secure communications mechanisms for data and IP information transmitted between networks.
- VPN technology uses the ESP protocol of IPSec in the tunnel mode. Moreover, firewalls, VPNs, and IPsec with ESP in tunnel mode are a natural combination and widely used in practice .
- VPSs can use both symmetric and asymmetric forms of cryptography.

Virtual Private Network

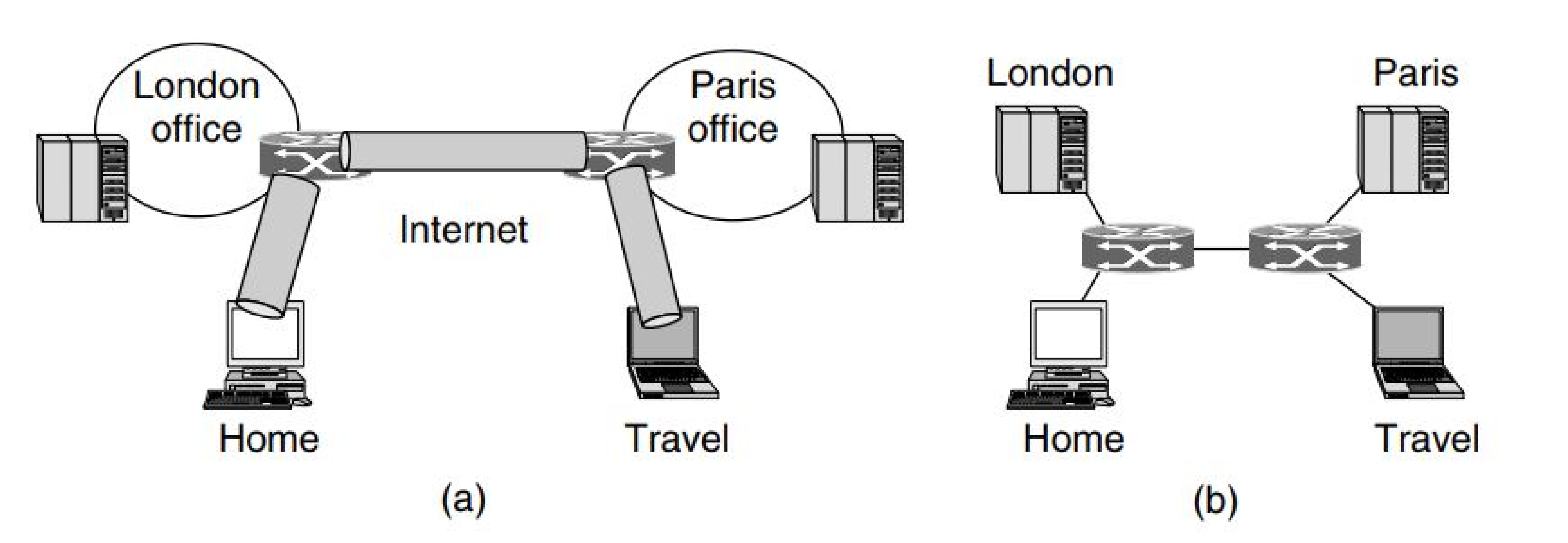


Figure: a) A VPN b) Topology as seen from the inside.

VPN

- A fundamental requirement for VPN is security.
- Use of a public network exposes corporate traffic to eavesdropping and provides an entry point for unauthorized users.
- To counter this problem, a VPN is needed. In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through an otherwise insecure network, typically the Internet.

VPN

- VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption and authentication system at both ends.
- The encryption may be performed by firewall software or possibly by routers.
- The most common protocol mechanism used for this purpose is at the IP level and is known as IPSec.
- An organization maintains LANs at dispersed locations.
- A logical means of implementing an IPSec is a firewall which is shown in figure.

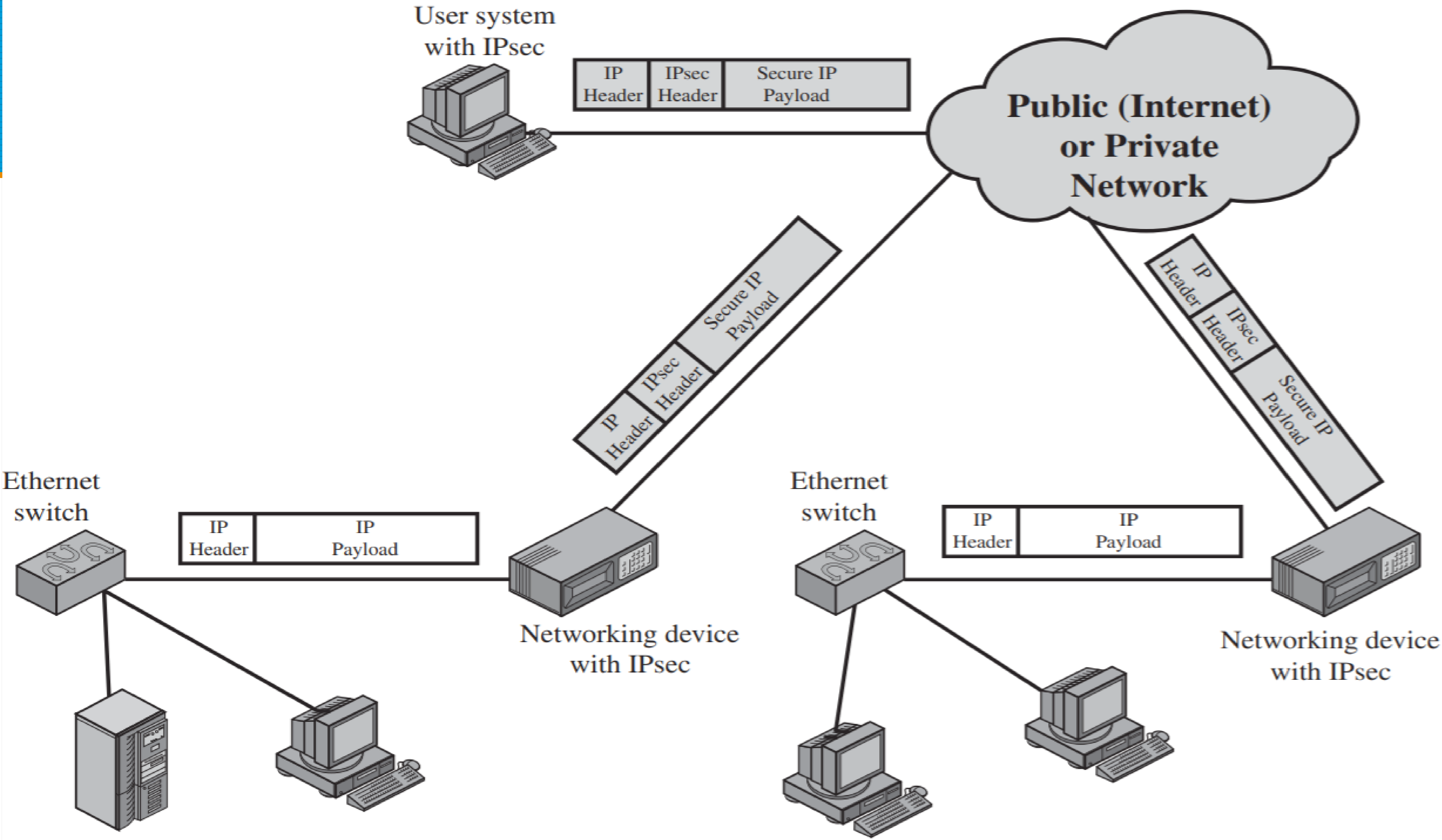


Figure: A VPN security scenario