Definition of Intrusion

- A significant security problem for networked systems; hostile, or at least unwanted, trespass by users or software
- Trespass
  - Unauthorized login (user)
  - Authorized user: acquisition of privileges beyond authorization (user)
  - Take the form of virus, worm or Trojan horse (software)

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the **behavior of legitimate users** over a period of time
- Then current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

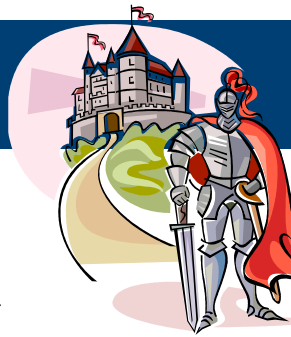
- Uses a set of **known malicious data patterns** or attack rules that are compared with current behavior
- Can only identify known attacks for which it has patterns or rules

- Host-based intrusion detection
- Network-based intrusion detection
- Distributed/hybrid intrusion detection

Host-Based IDS

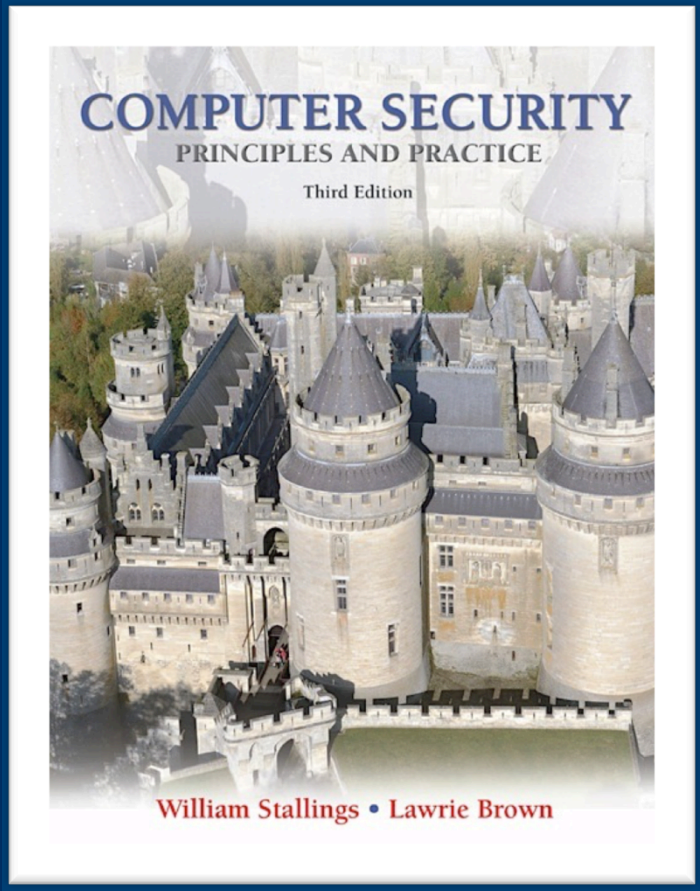
- adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- monitors activity to detect suspicious behavior
  - primary purpose is to detect intrusions, log suspicious events, and send alerts
  - can detect both external and internal intrusions

Network-Based IDS (NIDS)



- monitors traffic at selected points on a network
- examines traffic packet by packet in real or close to real time
- may examine network, transport, and/or application-level protocol activity
- comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface
- **analysis of traffic patterns** may be done at the sensor, the management server or a combination of the two

Lecture 19
Firewalls



modified from slides of Lawrie Brown

The Need For Firewalls

- Internet connectivity is essential
  - however it creates a threat
- To equip each workstation and server with strong security features? (host-based security services)
  - Hundreds of systems; once a security flaw is found, all services need to be upgraded—not scalable
- Alternative approach-- firewalls

The Need For Firewalls

- Inserted between the premises network and the Internet to establish a controlled link
  - Aim--protect the premise network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed
  - can be a single computer or a set of two or more systems working together to perform firewall function

Firewall Characteristics

Design goals

All traffic from inside to outside, and vice versa, must pass through the firewall

Only authorized traffic as defined by the local security policy will be allowed to pass

The firewall itself is immune to penetration

Firewall Access Policy

- A critical component in the planning & implementation of a firewall is specifying a suitable access policy
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

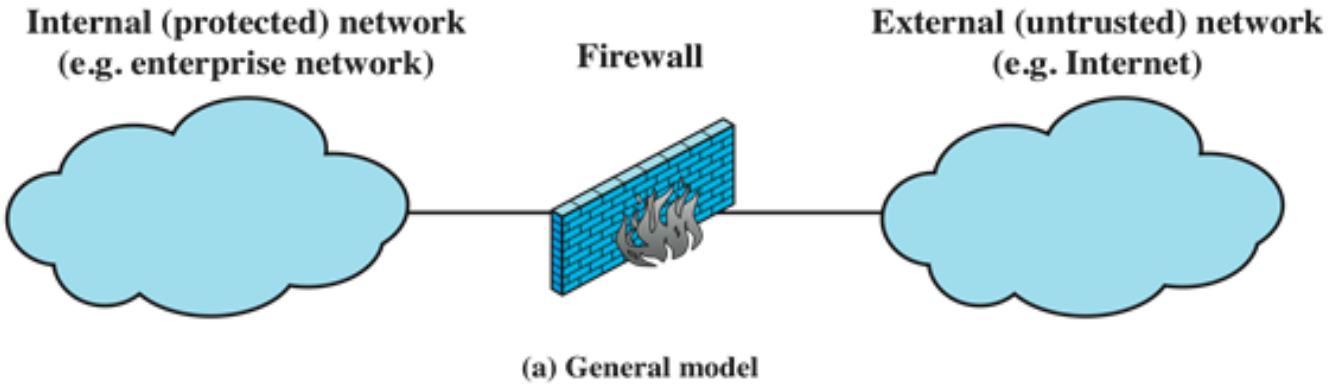
IP address and protocol values	Application protocol	User identity	Network activity
This type of filtering is used by packet filter and stateful inspection firewalls	This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols	Typically for inside users who identify themselves using some form of secure authentication technology	Controls access based on considerations such as the time or request, rate of requests, or other activity patterns
Typically used to limit access to specific services			

Firewall Capabilities And Limits

- capabilities:
  - defines a single choke point
  - provides a location for monitoring security events
  - can serve as the platform for IPSec
- limitations:
  - cannot protect against attacks bypassing firewall
  - may not protect fully against internal threats
  - laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls
- Circuit-level firewalls



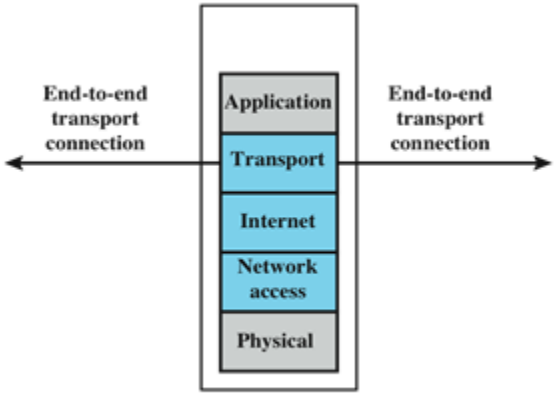
(a) General model

Packet Filtering Firewall

- applies rules to each incoming and outgoing IP packet
  - typically a list of rules based on matches in the TCP/IP header
  - forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface



(b) Packet filtering firewall

- two default policies:
  - **discard** - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - **forward** - permit unless expressly prohibited
    - easier to manage and use but less secure

Packet Filtering Rule Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

- Inbound mail is allowed (port 25 is for SMTP incoming)
- Allow a response to an inbound SMTP connection
- Outbound mail to an external source is allowed
- Allow a response to an inbound SMTP connection
- Discard default policy

SMTP-basic knowledge

- Simple mail transfer protocol
- By setting TCP connections between clients and the server
- The TCP server port number is 25 (fixed); the TCP client port is 1024-65,535 (temporarily allocated)

Packet Filtering Rule Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

- Security threats: Rule 4 allows external traffic to any destination port above 1023—an external attacker can open a connection from **its port (e.g., 5150)** to an internal Web proxy server on port 8080 (not for mail).
- Countermeasure—add source port field for each row

Packet Filter Firewalls: Advantages And Weaknesses

- advantages
  - simplicity
  - typically transparent to users and are very fast
- weaknesses
  - cannot prevent attacks that employ application specific vulnerabilities or functions
  - do not support advanced user authentication
  - improper configuration can lead to breaches

Attacks to Packet Filtering Firewalls

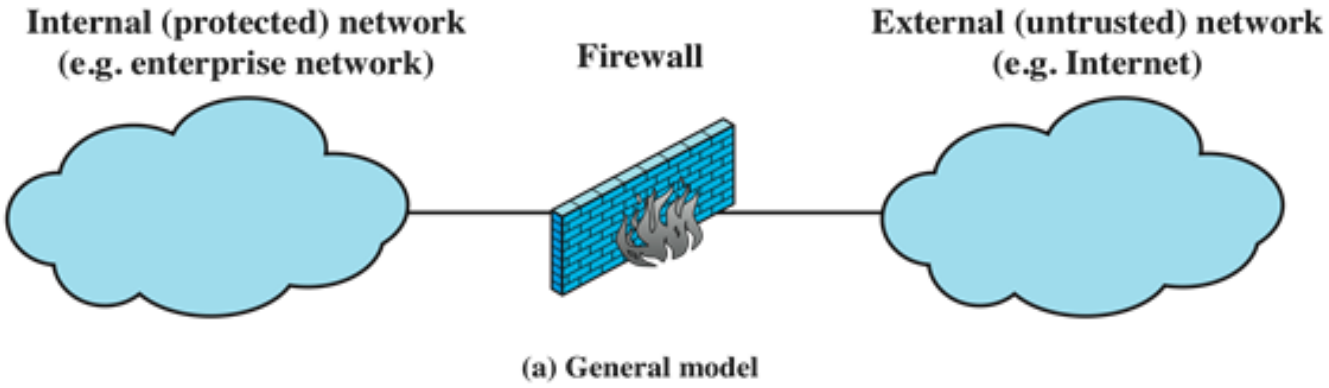
- IP address spoofing
  - The intruder transmits packets from the outside with a source IP address field containing an address of an internal host
  - Countermeasure– discard packets with an inside source address if the packet arrives on an external interface

Attacks to Packet Filtering Firewalls

- Tiny fragment attack
  - The intruder uses the IP fragment option to create small fragments; in some datalink protocol (Ethernet), the packet information is only contained in the first fragment packet; once the first fragment passes the test of firewall, the rest can pass as well
  - Countermeasure– enforce all the fragment packets contain necessary information

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Stateful Inspection Firewall

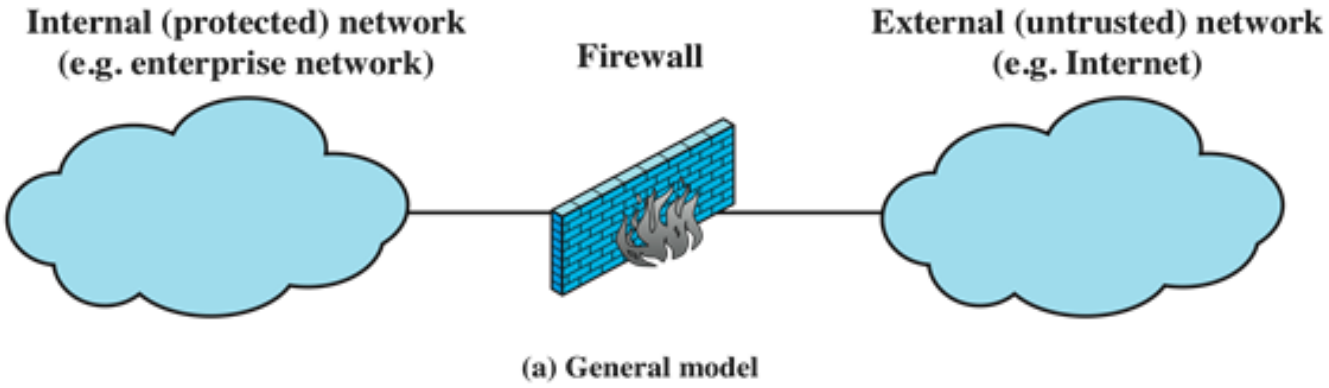
- tightens rules for TCP traffic by creating a directory of current TCP connections and their information (stateful)
  - there is an entry for each currently established connection
  - packet filter allows incoming packets that fit the profile of one of the entries
  - Consider the SMTP example ; the TCP client port value is valid if it belongs to 1024-65,535—wide accepting range for firewall filter; the attacker can exploit this property→stateful inspection
  - How about the first packet?

Stateful Firewall Connection State

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

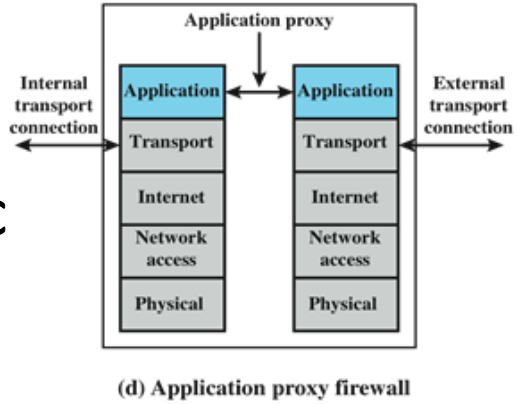
Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Application-Level Gateway



(d) Application proxy firewall

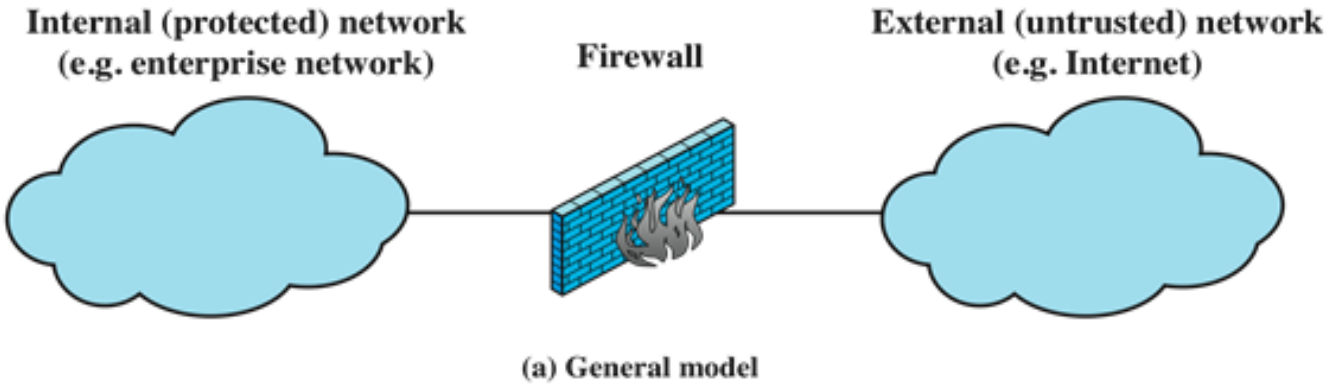
- also called an **application proxy**
- acts as a relay of application-level traffic
  - user contacts gateway using a TCP/IP appl.
  - user is authenticated
  - gateway contacts application on remote host and relays TCP segments between server and user
- tend to be more secure than packet filters
  - The application-level gateway only needs to check a few allowable applications

Application-Level Gateway

- Disadvantage
  - Two split connections, one from external user to the gateway, the other from the gateway to the internal user
  - additional processing overhead on each connection

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



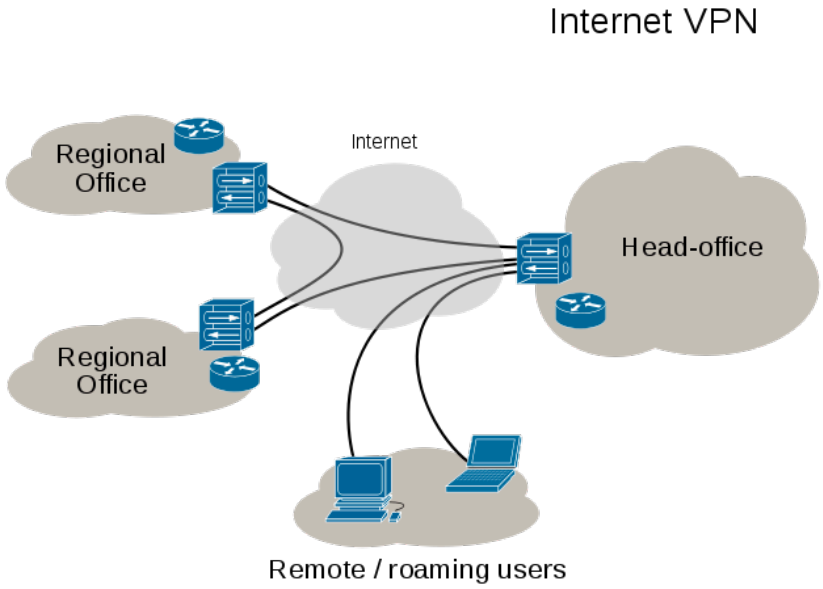
(a) General model

Bastion Hosts

- system identified as a critical strong point in the network's security
- serves as a platform for an application-level or circuit-level gateway
- common characteristics:
  - runs secure O/S, only essential services
  - may require user authentication to access proxy or host
  - each proxy can restrict features, hosts accessed
  - each proxy is small, simple, checked for security
  - each proxy is independent, non-privileged
  - limited disk use, hence read-only code

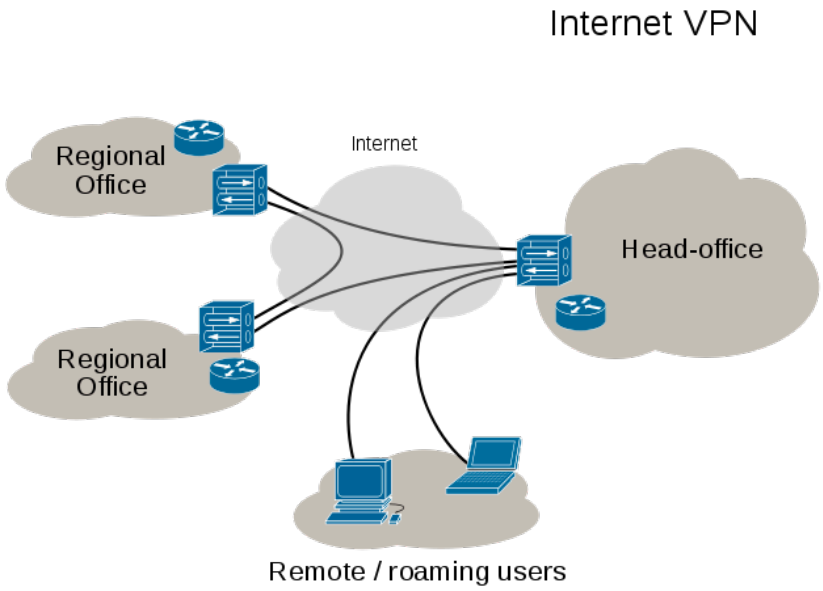
Virtual Private Networks (VPNs)

- A VPN extends a private network across a public network (Internet). It enables users to send and receive data across public networks as if their computing devices were directly connected to the private network, and thus are benefiting from the functionality, security and management policies of the private network

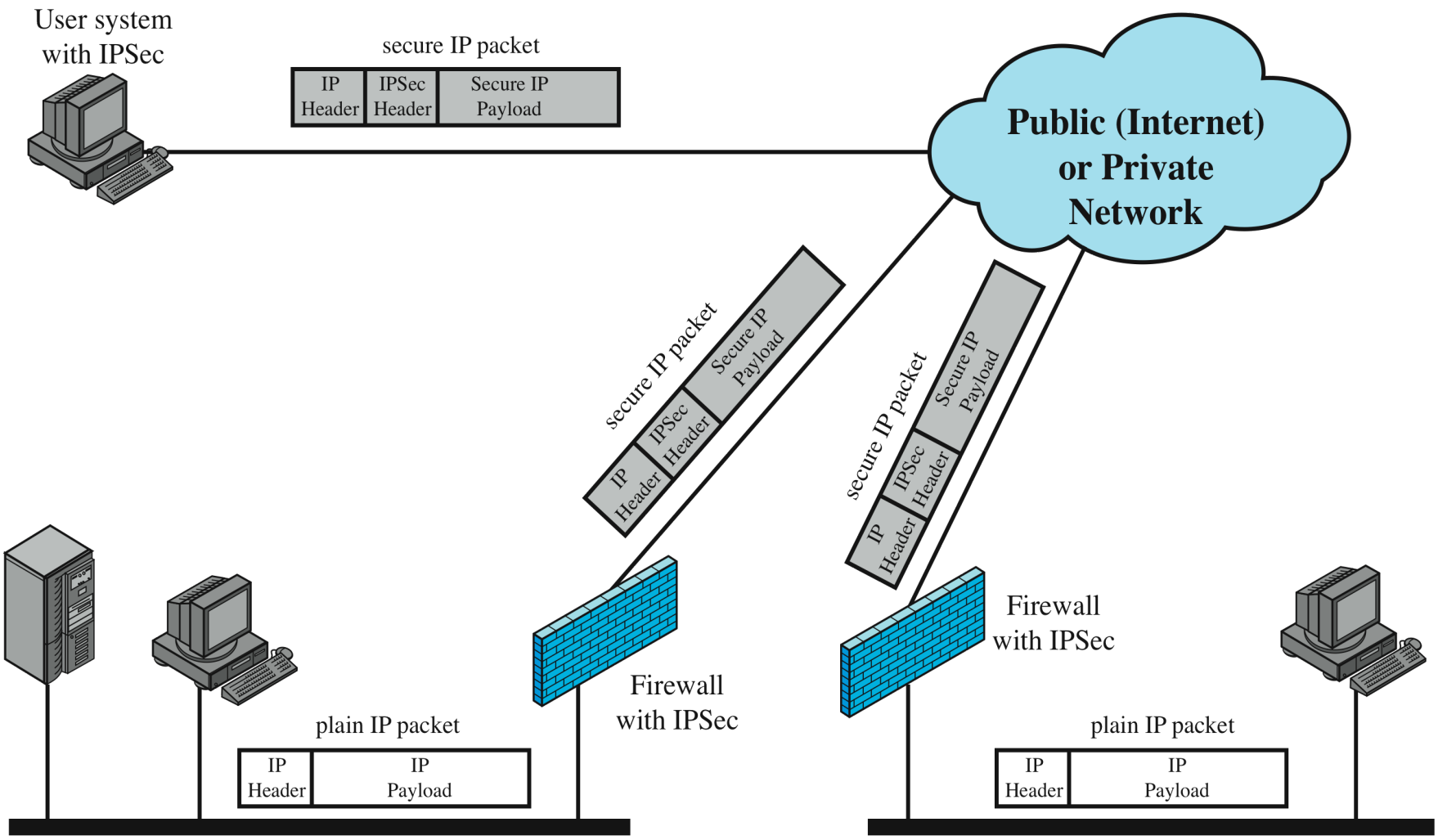


Virtual Private Networks (VPNs)

- In essence, a VPN uses encryption and authentication in the lower protocol layers to provide a secure connection through Internet. The encryption can be performed by firewall software or the routers
- The most common protocol mechanism used is at the IP level and is known as IPSec



IPSec


User system with IPSec
secure IP packet
IP Header
IPSec Header
Secure IP Payload
Public (Internet) or Private Network
secure IP packet
IP Header
IPSec Header
Secure IP Payload
secure IP packet
IP Header
IPSec Header
Secure IP Payload
Firewall with IPSec
Firewall with IPSec
plain IP packet
IP Header
IP Payload
plain IP packet
IP Header
IP Payload