Firewalls

Firewalls

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet.
- Firewalls protect you from potential hackers and offensive websites.

Firewall Design Principles

- The firewall is inserted between the premises network and the Internet
- Aims:
  - Establish a controlled link
  - Protect the premises network from Internet-based attacks
  - Provide a single choke point

Firewall Characteristics

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security police) will be allowed to pass

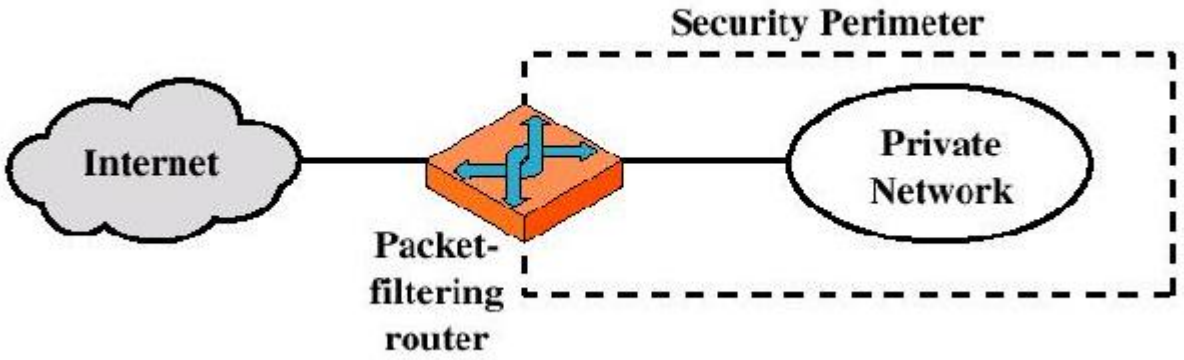
Types of Firewalls

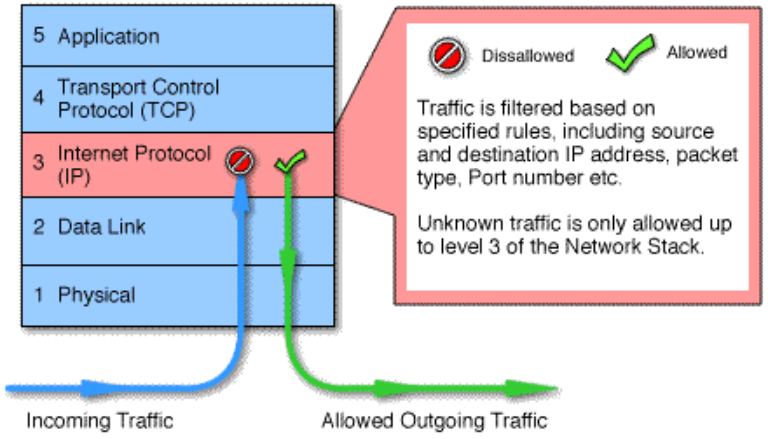
Four major types of firewalls in OSI

- Packet filters
- Circuit level gateways
- Application level gateways
- Stateful multilayer inspection firewalls

Types of Firewalls

- Packet-filtering Router

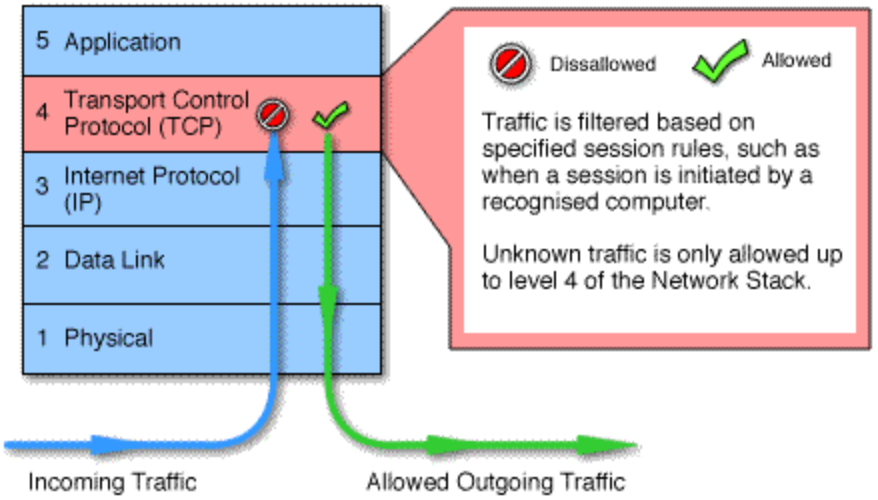




Types of Firewalls

- Packet filters –
- work at the network level.
- compared to a set of criteria before it is forwarded
- Advantages: low cost, low impact on network performance.
- Disadvantages: does not support sophisticated rule based models.

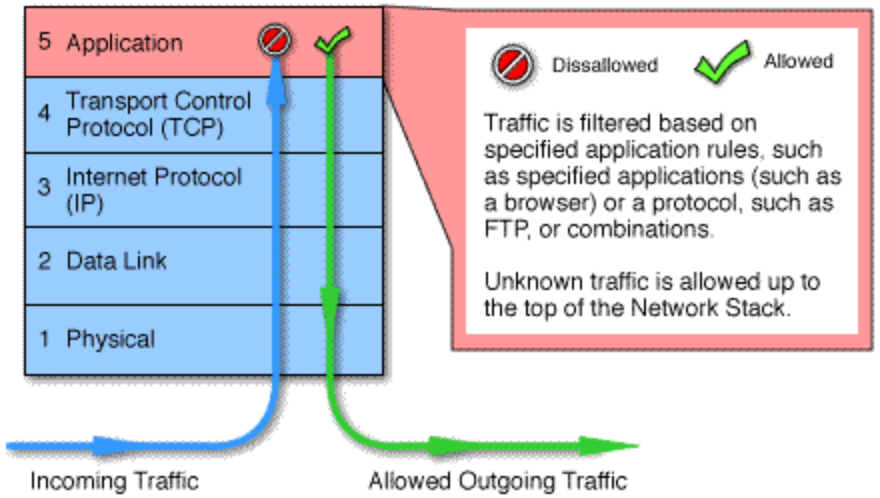
Circuit level gateways



Four major types of firewalls in OSI

- Circuit level gateways
- work at the session layer
- monitor TCP handshaking between packets to determine whether a requested session is legitimate
- Information passed to remote computer through a circuit level gateway appears to have originated from the gateway.
- Advantages: relatively inexpensive , hiding information about the private network Disadvantages: they do not filter individual packets.

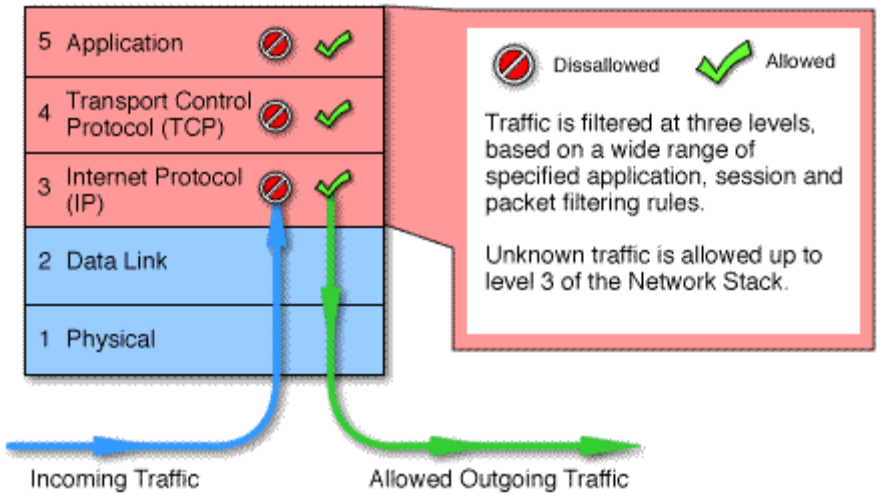
Four major types of firewalls in OSI



Four major types of firewalls in OSI

- Application level gateways
- work at the application layer
- Incoming or outgoing packets cannot access services for which there is no proxy
- filter application specific commands
- can also be used to log user activity and logins.
- Advantages: a high level of security
- Disadvantages: having a significant impact on network performance, not transparent to end users and require manual configuration of each client computer.

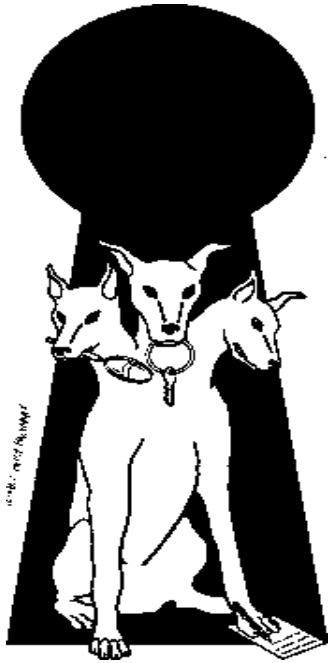
Four major types of firewalls in OSI



Four major types of firewalls in OSI

- Stateful multilayer inspection firewalls
- work at the application , session, network layer.
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer
- They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways. can also be used to log user activity and logins.
- They rely on algorithms to recognize and process application layer data instead of running application specific proxies.
- Advantages: a high level of security, good performance, transparency to end users
- Disadvantages: they are expensive and complex.

KERBEROS



In Greek mythology, a many headed dog, the guardian of the entrance of Hades

KERBEROS

- Users wish to access services on servers.
- Three threats exist:
  - User pretend to be another user.
  - User alter the network address of a workstation.
  - User eavesdrop on exchanges and use a replay attack.

KERBEROS

- It is Network Authentication Protocol
- Provides a centralized authentication server to authenticate users to servers and servers to users.
- Relies on conventional encryption, making no use of public-key encryption
- Two versions: version 4 and 5
- Version 4 makes use of DES

Kerberos Version 4

- Terms:
  - C = Client
  - AS = authentication server
  - V = server
  - ID_C = identifier of user on C
  - ID_V = identifier of V
  - P_c = password of user on C
  - ADc = network address of C
  - K_V = secret encryption key shared by AS an V
  - TS = timestamp
  - || = concatenation

A Simple Authentication Dialogue

(1) C → AS: $ID_c \| P_c \| ID_v$

(2) AS → C: Ticket

(3) C → V: $ID_c \| Ticket$

$Ticket = E_{Kv}[ID_c \| P_c \| ID_v]$

Version 4 Authentication Dialogue

- Problems:
  - Lifetime associated with the ticket-granting ticket
  - If to short → repeatedly asked for password
  - If to long → greater opportunity to replay
- The threat is that an opponent will steal the ticket and use it before it expires

Version 4 Authentication Dialogue

Authentication Service Exhange: To obtain Ticket-Granting Ticket

(1) C → AS: IDc || IDtgs ||TS1

(2) AS → C: $E_{Kc}[K_{c,tgs}|| ID_{tgs} || TS_2 || Lifetime_2 || Ticket_{tgs}]$

Ticket-Granting Service Echange: To obtain Service-Granting Ticket

(3) C → TGS: IDv ||Ticket$_{tgs}$ ||Authenticatorc

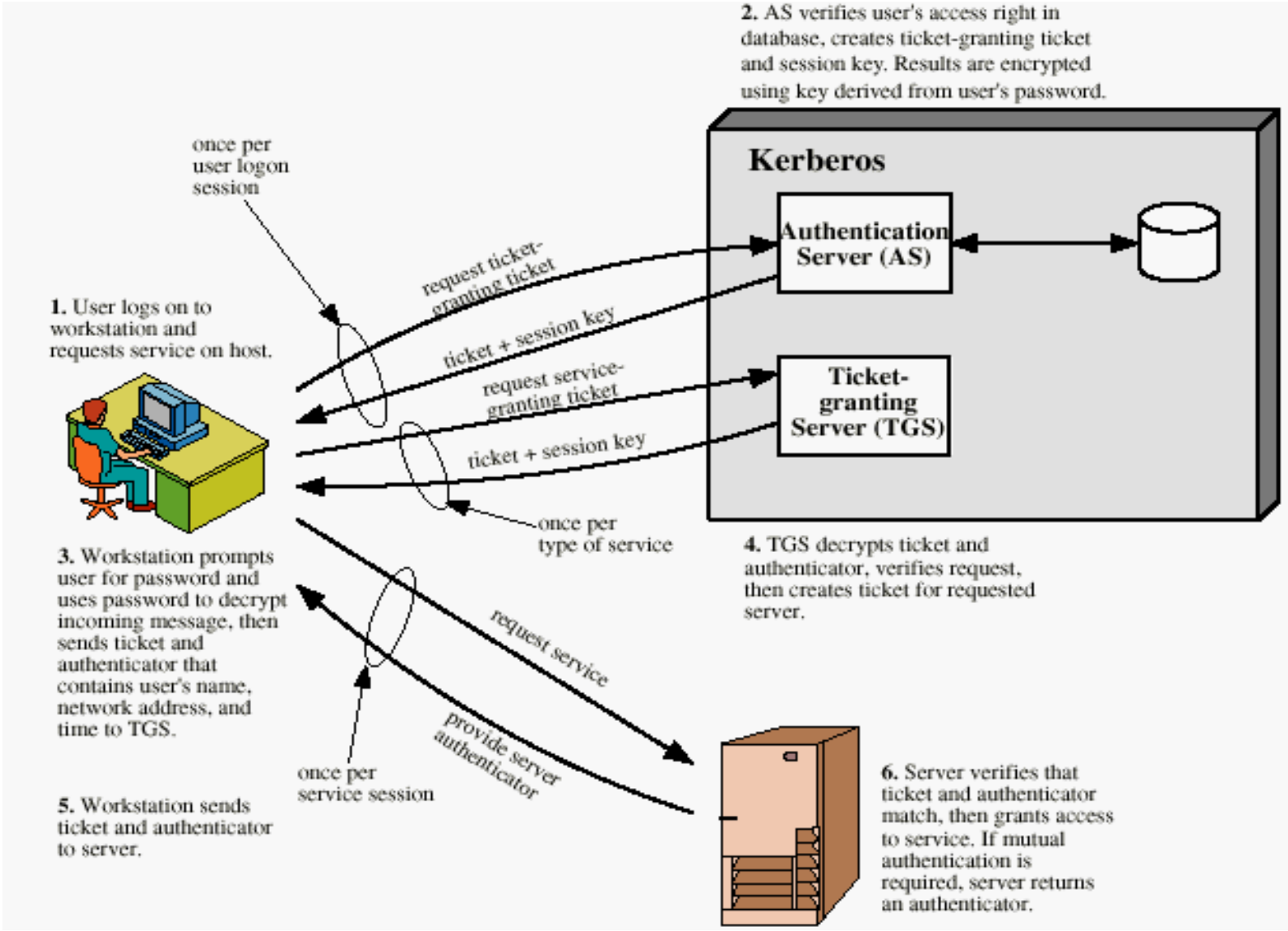
(4) TGS → C: $E_{Kc}[K_{c,v} || IDv || TS_4 || Ticket_v]$

Client/Server Authentication Exhange: To Obtain Service

(5) C → V: Ticket$_v$ || Authenticator$_c$

(6) V → C: EKc,v[TS5 +1]

Overview of Kerberos



Request for Service in Another Realm

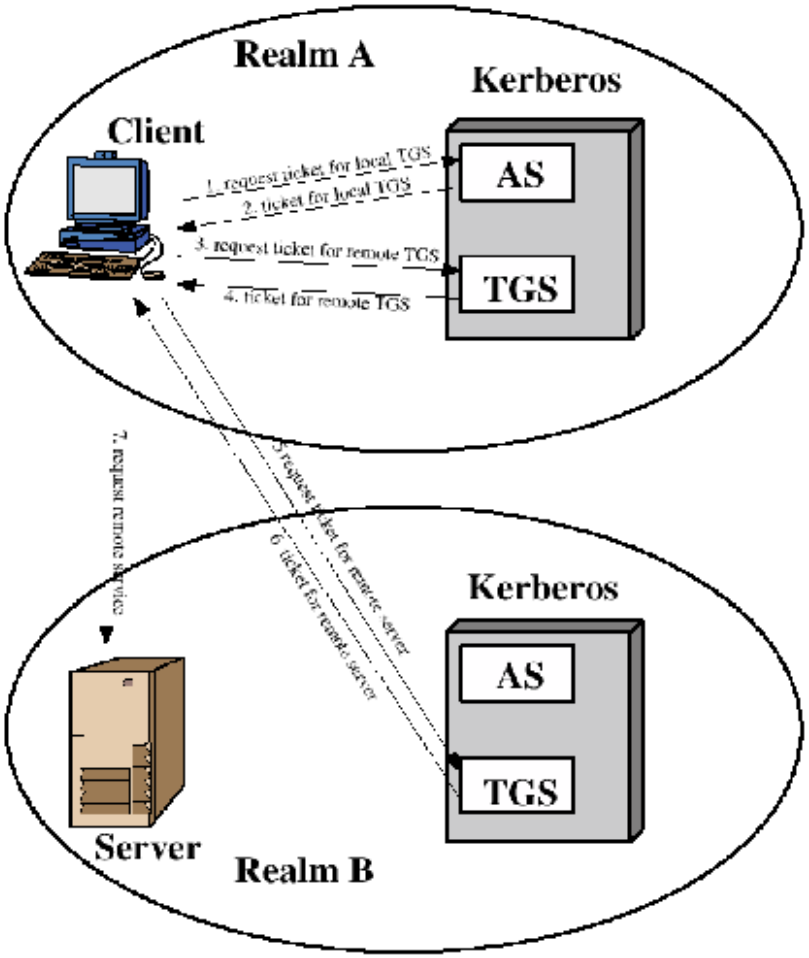


Figure 4.2 Request for Service in Another Realm

Difference Between Version 4 and 5

- Encryption system dependence (V.4 DES)
- Internet protocol dependence
- Message byte ordering
- Ticket lifetime
- Authentication forwarding
- Interrealm authentication