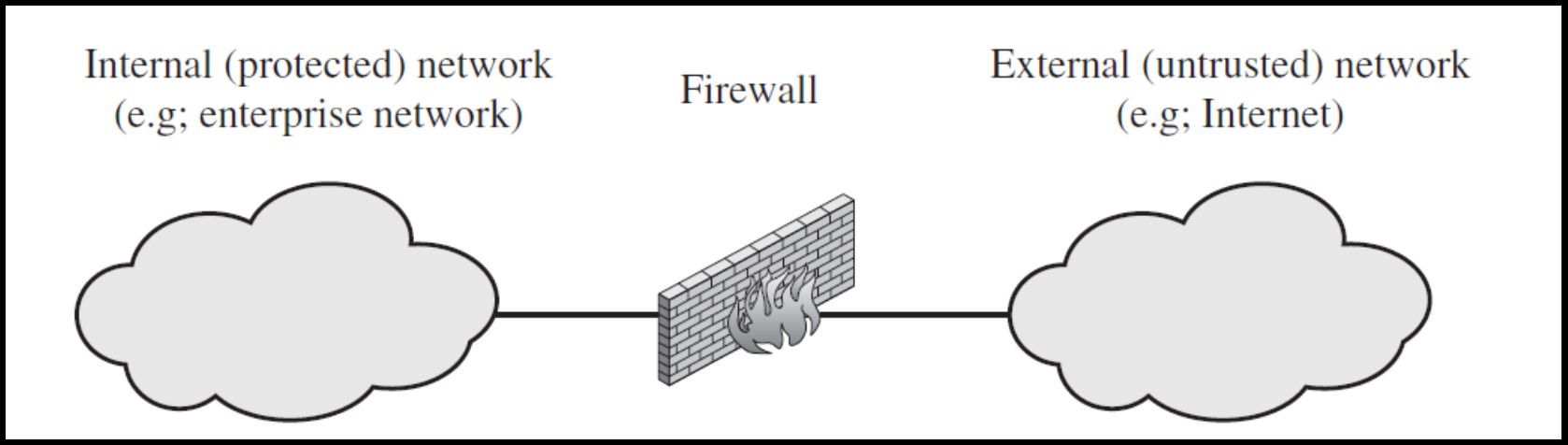
Firewall/IPS

What is Firewall

- The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter.
- The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed.
- The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function

What is Firewall



Design goals for a firewall

- 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.

Characteristics that a firewall access policy could use to filter traffic

- **IP Address and Protocol Values**: Controls access based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics
- **Application Protocol**: Controls access on the basis of authorized application protocol data
- **User Identity**: Controls access based on the users identity, typically for inside users
- **Network Activity**: Controls access based on considerations such as the time or request, e.g., only in business hours; rate of requests, e.g., to detect scanning attempts; or other activity patterns

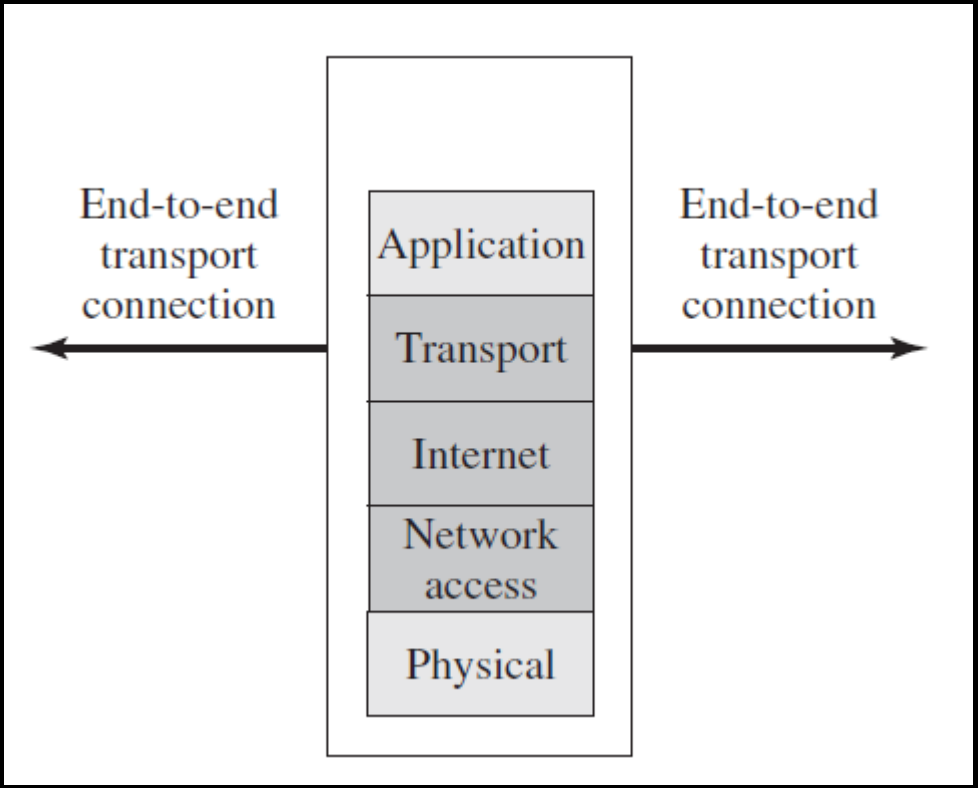
Types of Firewalls

- Packet filtering firewall
- Stateful inspection firewall
- Application proxy firewall
- Circuit-level proxy firewall

Packet Filtering Firewall

- A **packet filtering firewall** applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address
  - IP protocol field
  - Interface

Packet Filtering Firewall

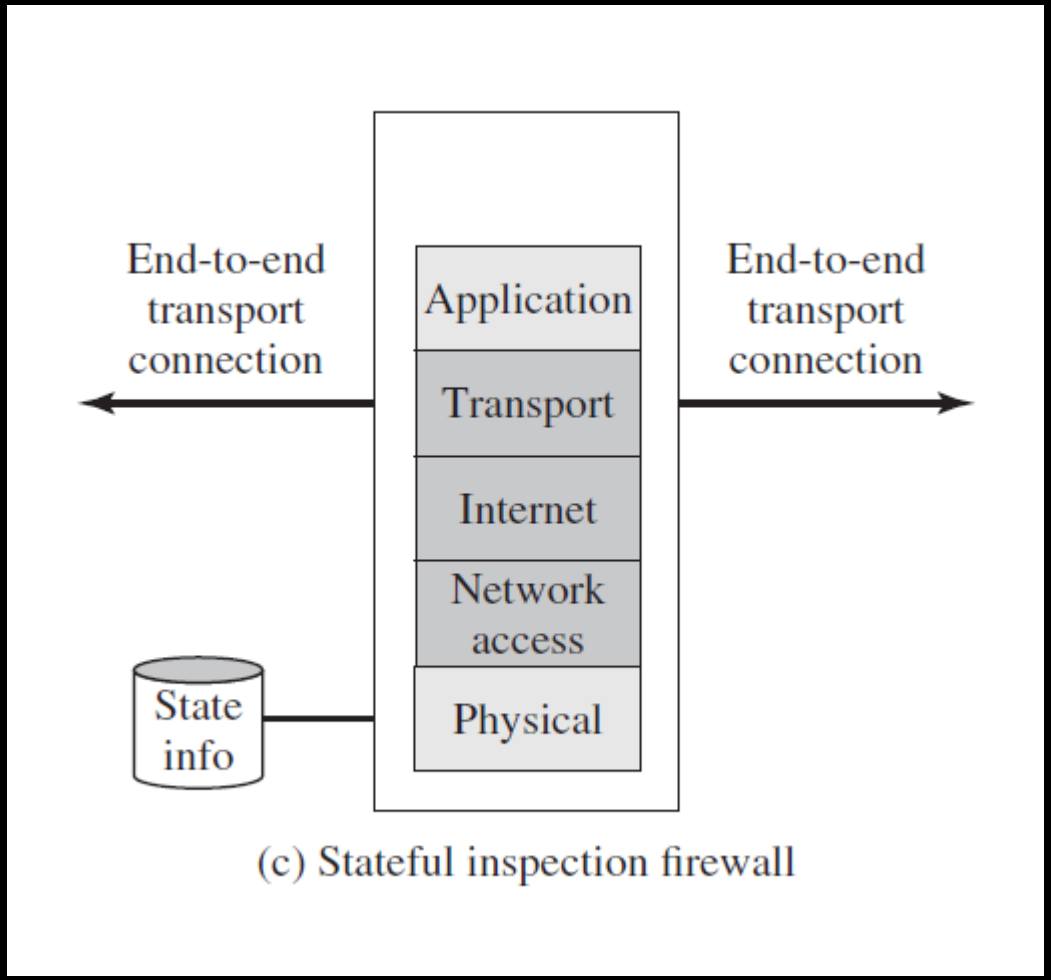


Packet Filtering Firewall

Table 9.1 **Packet-Filtering Examples**

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

Stateful inspection firewall



(c) Stateful inspection firewall

Stateful inspection firewall

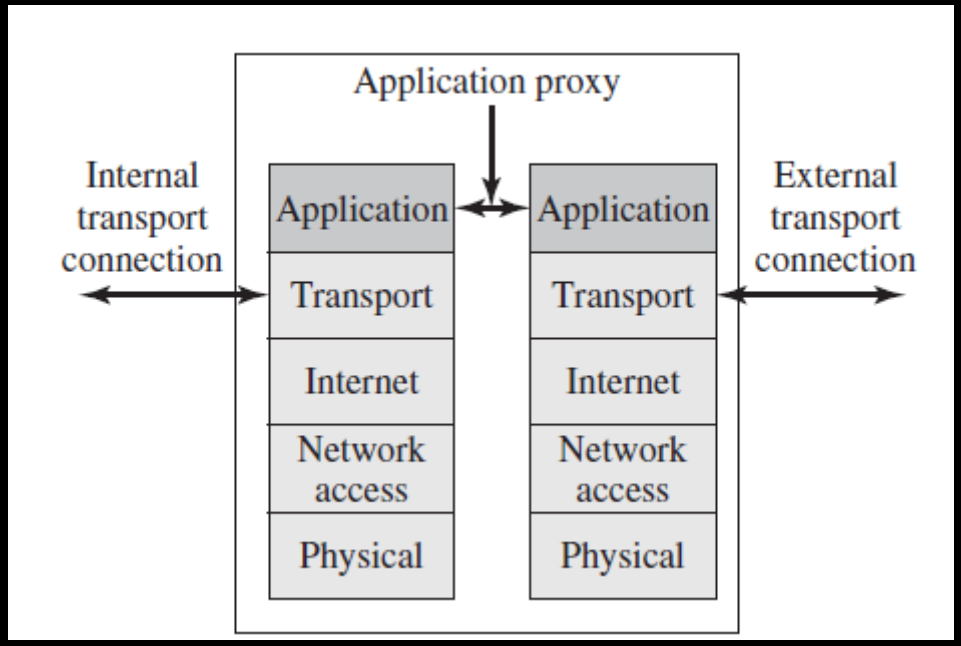
Table 9.2 Example Stateful Firewall Connection State Table

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

Application proxy firewall

- An **application-level gateway**, also called an application proxy, acts as a relay of application-level traffic. The user contacts the gateway using a TCP/IP application, such as HTTP/FTP,

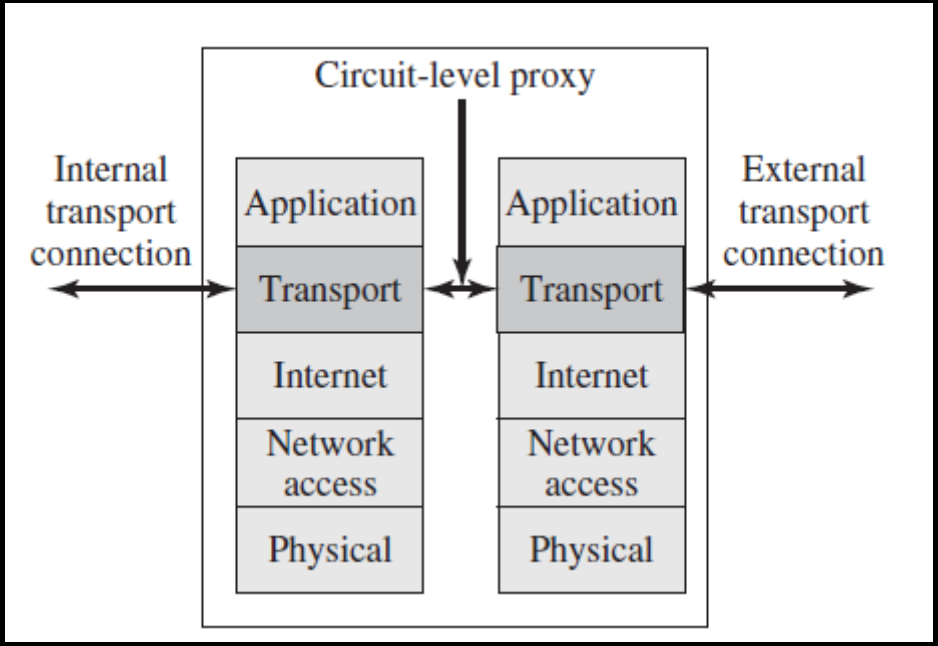
Application proxy firewall



Circuit-level proxy firewall

- As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outside host
- An example of a circuit-level gateway implementation is the SOCKS

Circuit-level proxy firewall



Firewall Basing

- **Bastion Host**
- **Host-Based Firewalls**
  - A host-based firewall is a software module used to secure an individual host.
- **Personal Firewall**
  - A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side

Firewall Location and Configurations

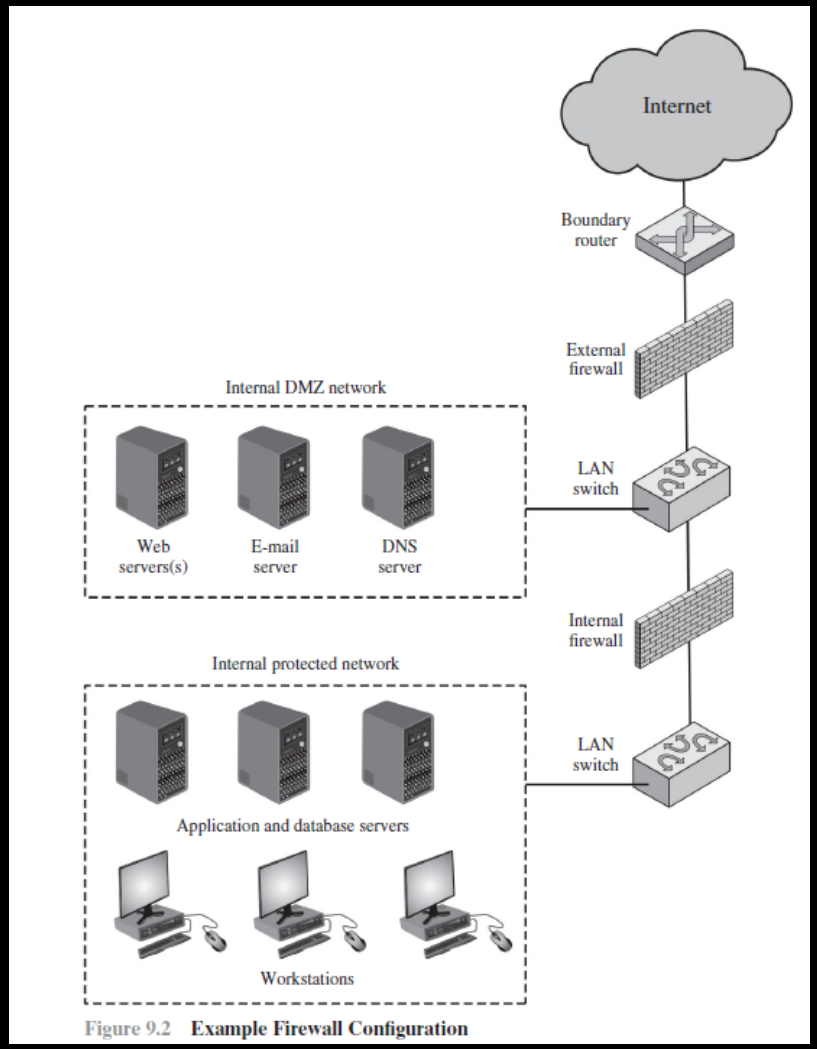


Figure 9.2 **Example Firewall Configuration**