Internet Firewalls for Trusted Systems

Internet Firewalls for Trusted Systems

Internet Firewalls for Trusted Systems

- Firewall
  - Security gateway
    - It is a secure computer system placed between a trusted network and an untrusted internet
    - Controls access between the public Internet and an intranet

Role of Firewalls

- **Imposes restrictions**
  - Only authorised traffic will be allowed to pass
- **Create checkpoints** (or choke points)
  - Check point – between internal private network and an untrusted Internet
- **Filter**
  - Based on IP source and destination addresses and TCP port number
- **Applied at any layer**
  - Application, network, data link
- **Log**
  - Logging help in traffic monitor and generates alarm
- **Block**
  - TELNET or RLOGIN connections from the Internet to the intranet
  - SMTP and FTP connections to the Internet from internal systems not authorised to send e-mail or to move files
- **Protect from attacks**
  - IP spoofing , routing attacks
- **Services**
  - Security-related - Ipsec, Virtual Private Networks
  - security-unrelated events - NAT, Network management
- **Limit network exposure**
  - Hide the internal network systems and information from the public Internet

Firewall-Related Terminology

- Bastion Host
- Proxy Server
- SOCKS
- Choke Point
- De-militarised Zone (DMZ)
- Logging and Alarms
- VPN

Types of Firewalls

- Firewalls are classified into three common types:
  - Packet filters
  - Circuit-level gateways
  - Application-level gateways

Types of Firewalls

- **Packet Filters**
  - Process network traffic on a **packet-by-packet** basis
  - Device – Inspect or Filters traffic (on IP address)
  - Resides in a screening router
  - **Screening router (external filter)**
    - Filter packets from entering (remote IP host)or leaving the internal network

Types of Firewalls

Packet Filters

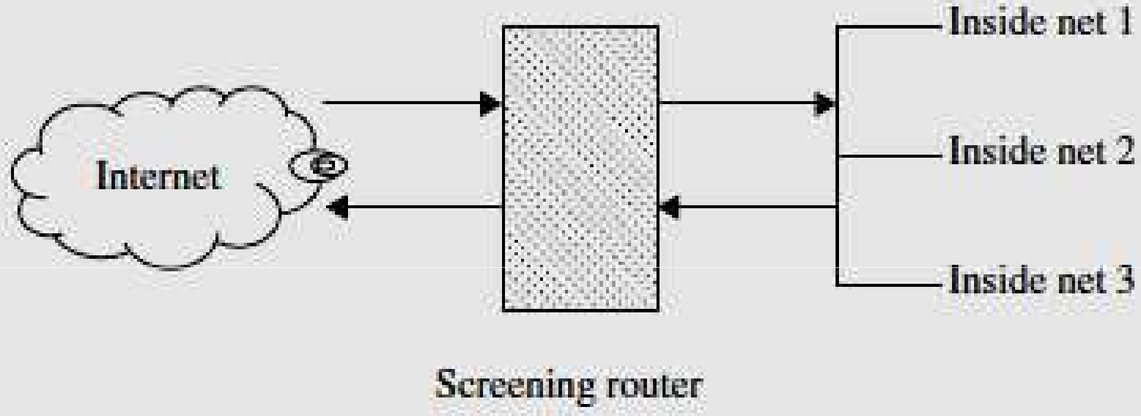


Figure 10.1 A screening router for packet filtering.

Types of Firewalls

Packet Filters

- Filtering rules
  - Rules are Set
  - Read sequentially line by line
  - Applied
    - on source and destination IP addresses
    - Network addresses
    - TCP or UDP ports
  - Actions
    - Forward :
      - Route the packet as normal if all conditions within the rule are met
    - Discard
      - Block all packets if the conditions in the rule are not met

Types of Firewalls

Packet Filters

- *Packet-Filtering Rules*
  - **TELNET packet filtering**
  - **FTP packet filtering**
  - **SMTP packet filtering**

Types of Firewalls

Circuit-Level Gateways

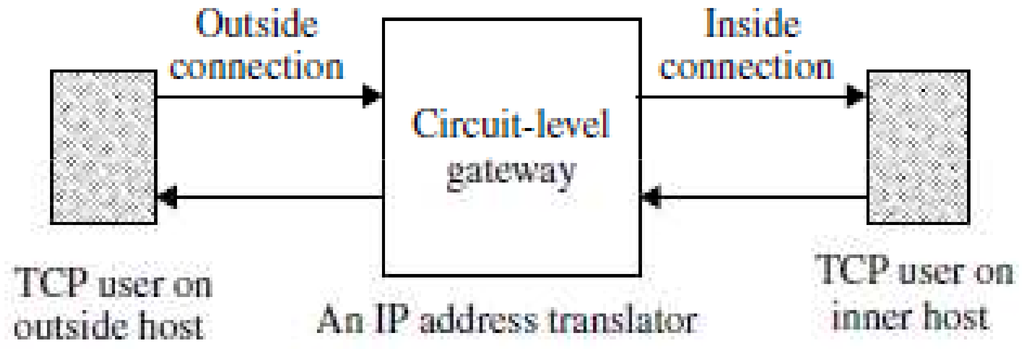
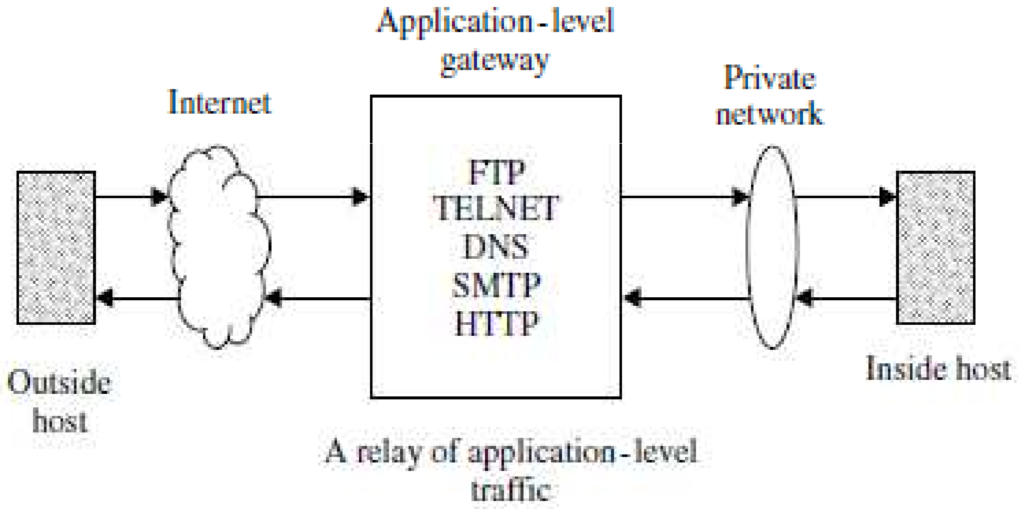


Figure 10.2 Circuit-level gateway for setting up two TCP connections.

Types of Firewalls

Application-Level Gateways



3 Application-level gateway for acting as a relay of application-level traffic.

Firewall Designs

- Three basic firewall designs are
  - a single-homed bastion host
  - a dual-homed bastion host
  - a screened subnet

Firewall Designs

Screened Host Firewall (Single-Homed Bastion Host)

- Uses a single-homed bastion host plus a packet-filtering router
- Configured as either circuit-level or application-level gateways
- Called a proxy server
- Hide the configuration of the internal network
- NAT is used
  - It is a critical component of any firewall strategy
  - It translates the internal IP addresses to IANA registered addresses to access the Internet
- All incoming and outgoing information is passed through the bastion host

Firewall Designs

Screened Host Firewall (Single-Homed Bastion Host)

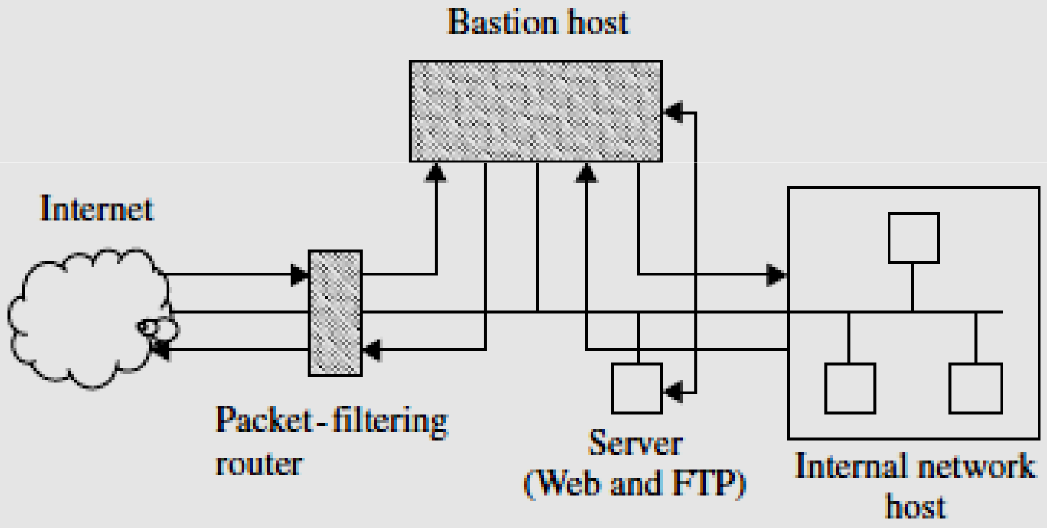


Figure 10.4 Screened host firewall system (single-homed bastion host).

Firewall Designs

Screened Host Firewall (Dual-Homed Bastion Host)

- Dual-homed bastion host adds significant security, compared with a single-homed bastion host
- Has two network interfaces
- It creates a complete break between the internal network and the external Internet
- NAT is used

Firewall Designs

Screened Host Firewall (Dual-Homed Bastion Host)

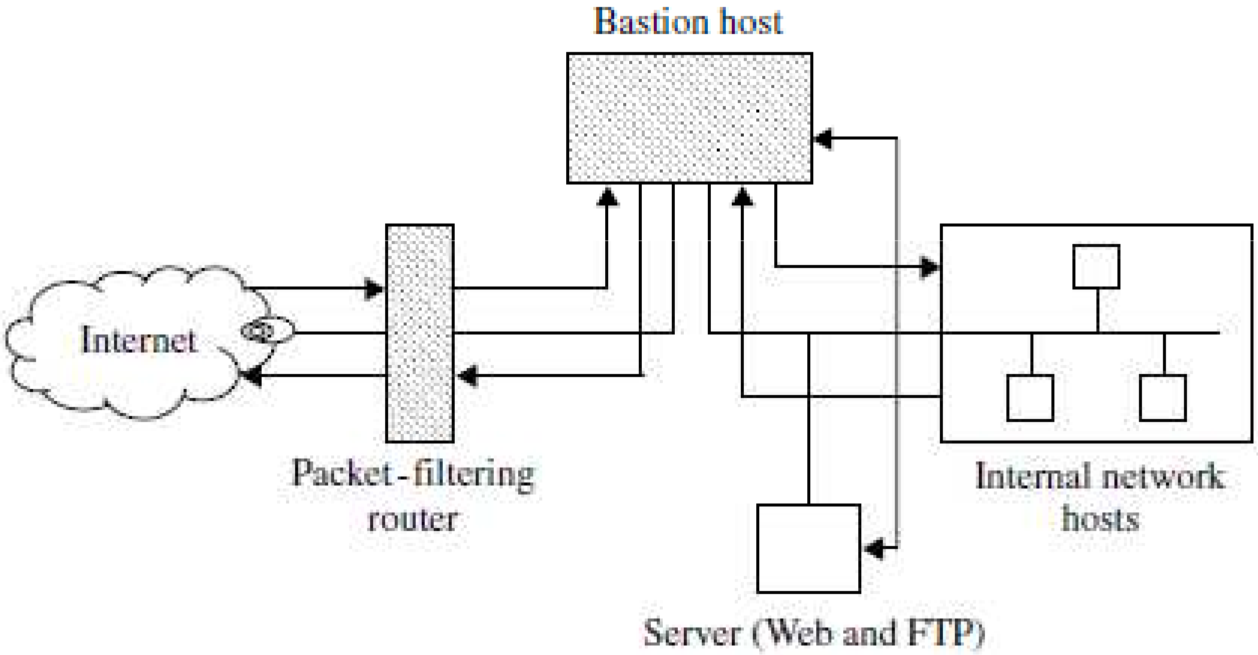


Figure 10.5 Screened host firewall system (dual-homed bastion host).

Firewall Designs

Screened Subnet Firewall

- Also known as a DMZ
  - A small isolated network positioned between the Internet and the internal network
  - All publicly accessible devices, including modem and server, are placed inside the DMZ

Firewall Designs

Screened Subnet Firewall

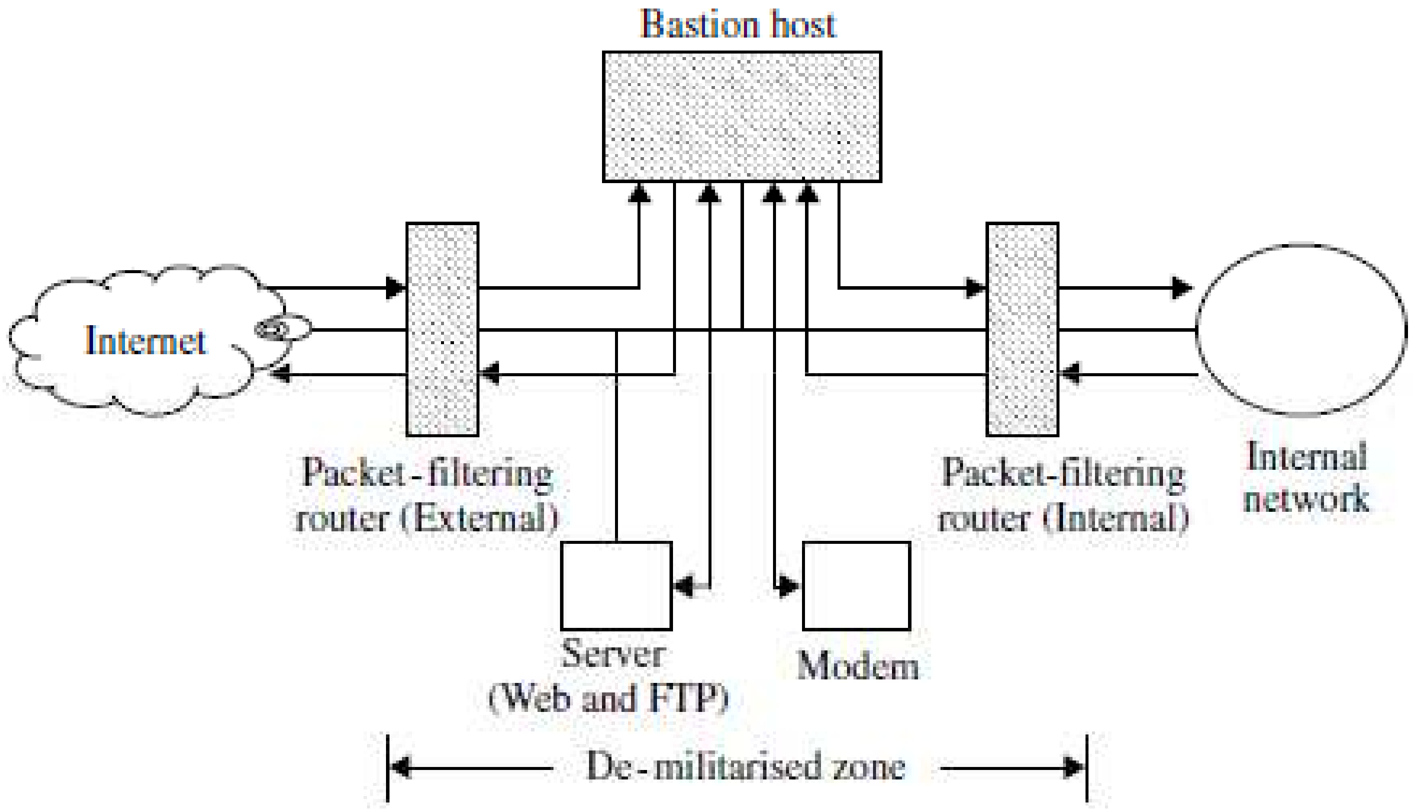


Figure 10.6 Screened subnet firewall system.