Internet Firewalls for Trusted Systems

Internet Firewalls for Trusted Systems

Internet Firewalls for Trusted Systems

- Firewall
  - Widely accepted Protective device or devices
  - Provide a choke point where security can be imposed
  - Act as outer security wall or perimeter for a network
  - Protect the intranet from Internet-based attacks
    - Internet access provides benefits but often creates a threat
  - Block traffic, it believes to be inappropriate, dangerous, or both
  - Consists of filters and gateway(s)
    - 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

Internet Firewalls for Trusted Systems

- Firewall
  - It act as an intermediate server in handling SMTP and HTTP
  - Use an access negotiation and encapsulation protocol such as SOCKS to gain access to the Internet, the intranet, or both
    - *SOCKS* is as a circumvention tool, allowing traffic to bypass Internet filtering to access content otherwise blocked
  - Many firewalls support tri-homing, allowing use of a DMZ network (**virtual perimeter network)**
  - Classified into three main categories:
    - Packet filters
    - Circuit-level gateways
    - Application-level gateways

Tri-homed

- Some firewalls, such as **Microsoft Internet Security and Acceleration (ISA) Server**, allow the creation of a **virtual perimeter network**
  - This is by using a third network adapter in the firewall
    - The Internet is attached to the first adapter
    - The private network to the second
    - The perimeter network to the third
- These firewalls are sometimes referred to as being tri-homed or as having DMZ support

DMZ

- **DMZ (demilitarized zone)**
  - Physical or logical sub-network
  - Separates an internal local area network (LAN) from other untrusted networks, usually the Internet
  - External-facing servers, resources and services are located in the DMZ
  - They are accessible from the Internet but the rest of the internal LAN remains unreachable
  - This provides an additional layer of security to the LAN
  - Restricts the ability of hackers to directly access internal servers and data via the Internet

Role of Firewalls

- **Imposes restrictions**
  - Only authorised traffic will be allowed to pass
  - Allowed packet must conform to a filtering specification, or some sort of authentication
  - The firewall itself must be immune to attack
- **Create checkpoints** (or choke points)
  - Check point – between internal private network and an untrusted Internet
  - Once the choke points have been clearly established, the device can monitor, filter and verify all inbound and outbound traffic
- **Filter**
  - Based on IP source and destination addresses and TCP port number

Role of Firewalls

- **Applied at any layer**
  - Application, network, data link
- **Log**
  - Logging help in traffic monitor and generates alarm
  - Good logging strategies are one of the most effective tools for proper network security
- **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

Role of Firewalls

- **Services**
  - Security-related
    - Ipsec
    - Virtual Private Networks
  - security-unrelated events
    - Network address translator
      - Maps local addresses to Internet addresses
      - The majority of NATs map multiple private hosts to one publicly exposed IP address
    - Network management function that accepts or logs Internet usage
- **Limit network exposure**
  - Hide the internal network systems and information from the public Internet

Role of Firewalls

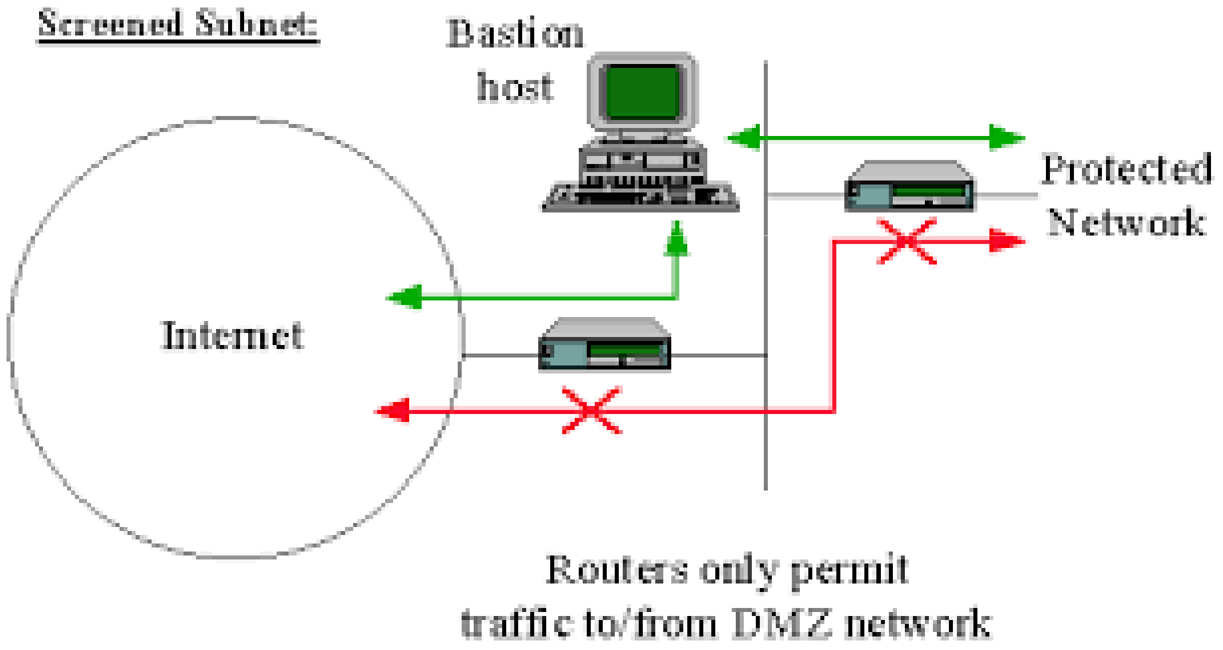
- **Negative aspects:**
  - Cannot protect against **internal threats** such as an employee who cooperates with an external attacker
  - it is also unable to protect against the transfer of **virus-**infected programs or files because it is impossible for it to scan all incoming files, e-mail and messages for viruses
  - Some firewall mechanisms are **less appropriate for multicast**

Firewall-Related Terminology

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

Firewall-Related Terminology

Bastion Host



Firewall-Related Terminology

Bastion Host

- Directly connected to a public network such as the Internet
- Serves as a platform for any types of firewalls
  - Packet filter, circuit-level gateway or application-level gateway
- Check all incoming and outgoing traffic and enforce the rules specified in the security policy
- They must be prepared for attacks from external and possibly internal sources
- Armed with Logging and alarm features to prevent attacks

Firewall-Related Terminology

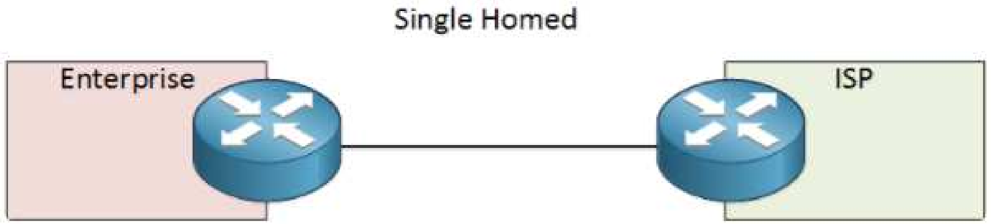
Bastion Host

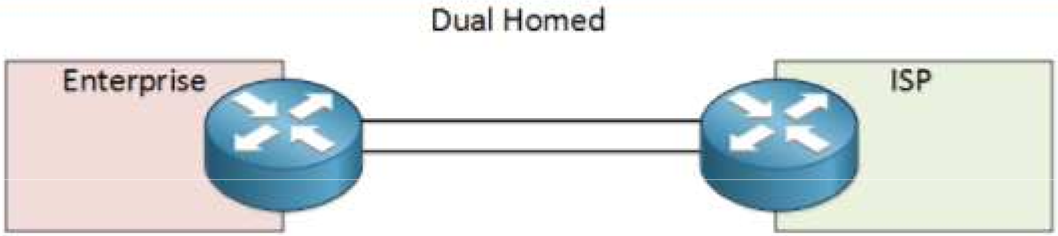
3 types of role

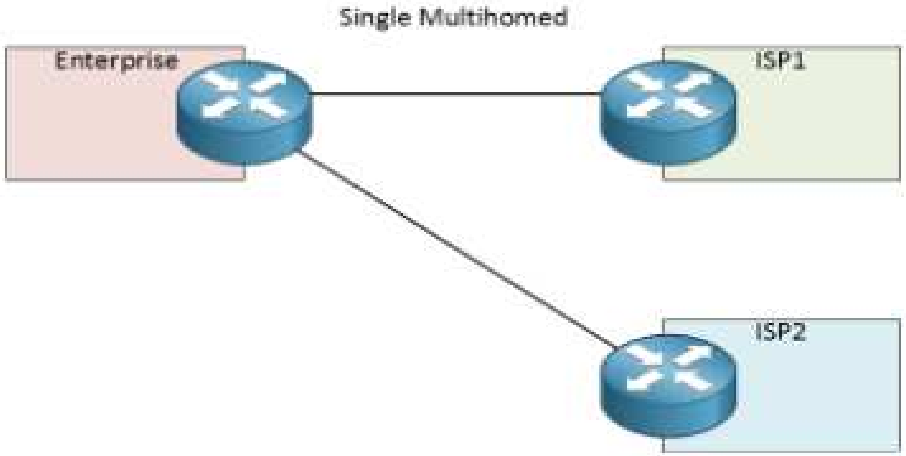
Single-homed bastion host:

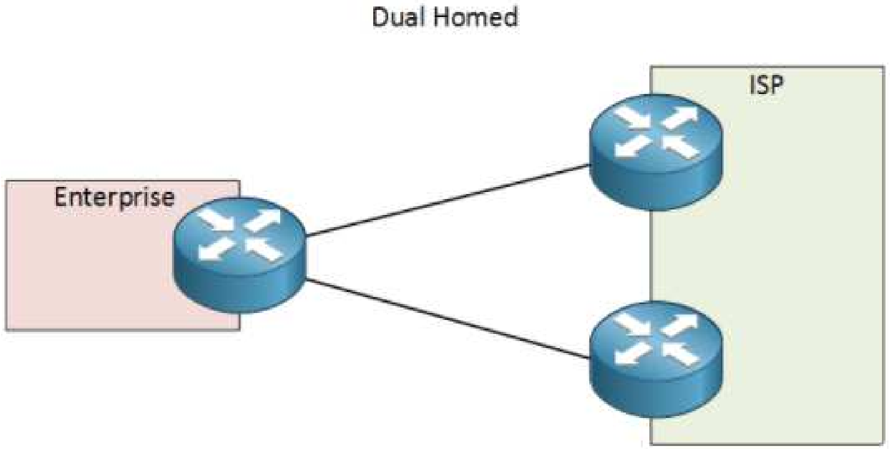
Dual-homed bastion host:

Multihomed bastion host:

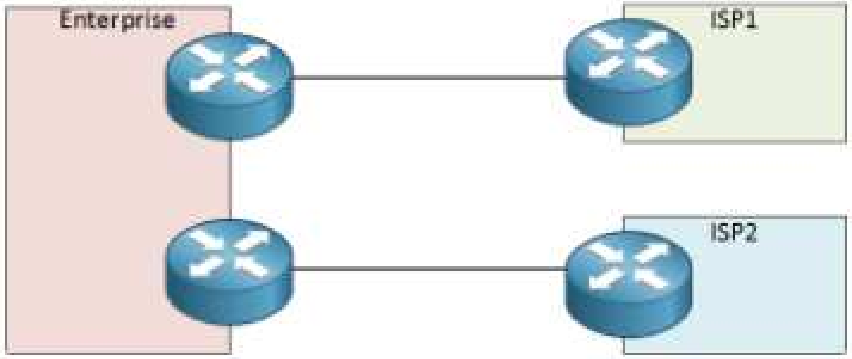




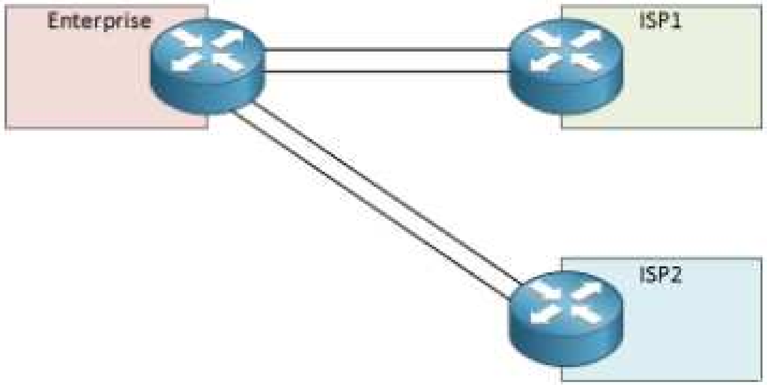




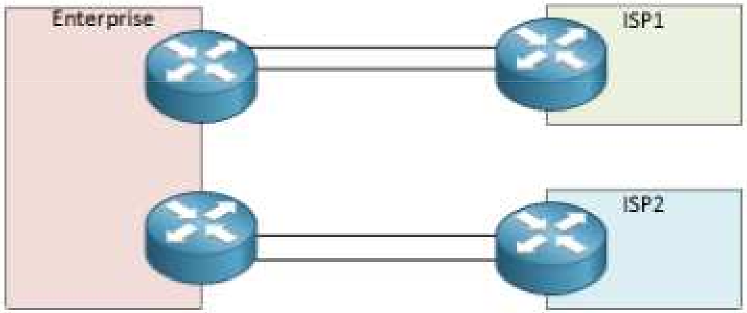
Single Multihomed



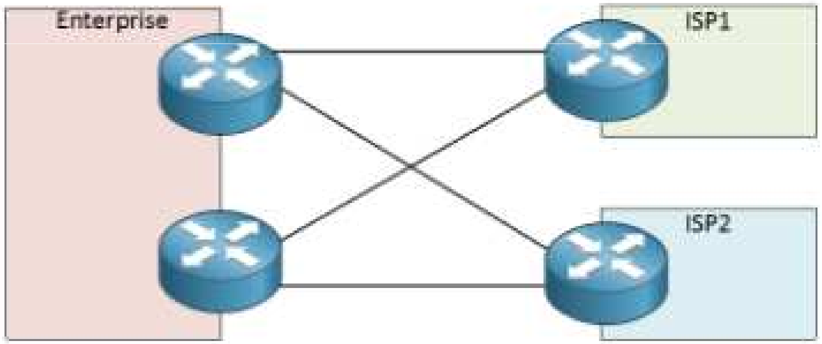
Dual Multihomed



Dual Multihomed



Dual Multihomed



Firewall-Related Terminology

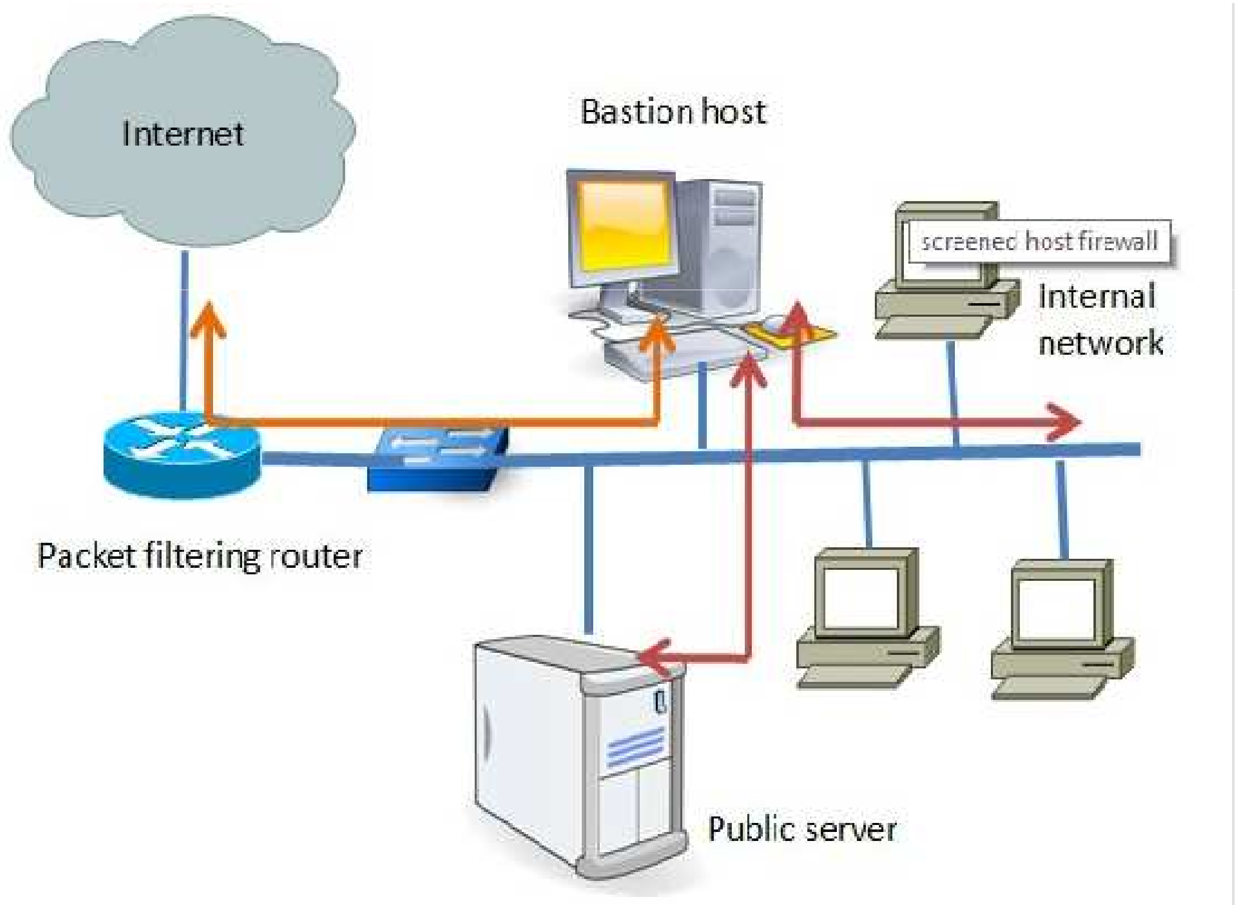
Bastion Host

- **Single-homed bastion host:**
  - A device with only **one network interface**
  - Normally used for an **application-level gateway**
  - The external router is configured to send all incoming data to the bastion host
  - All internal clients are configured to send all outgoing data to the host
  - Bastion host will test the data according to security guidelines

Firewall-Related Terminology

Bastion Host

- Single-homed bastion host:



Screened host firewall (single-homed bastion host)

Firewall-Related Terminology

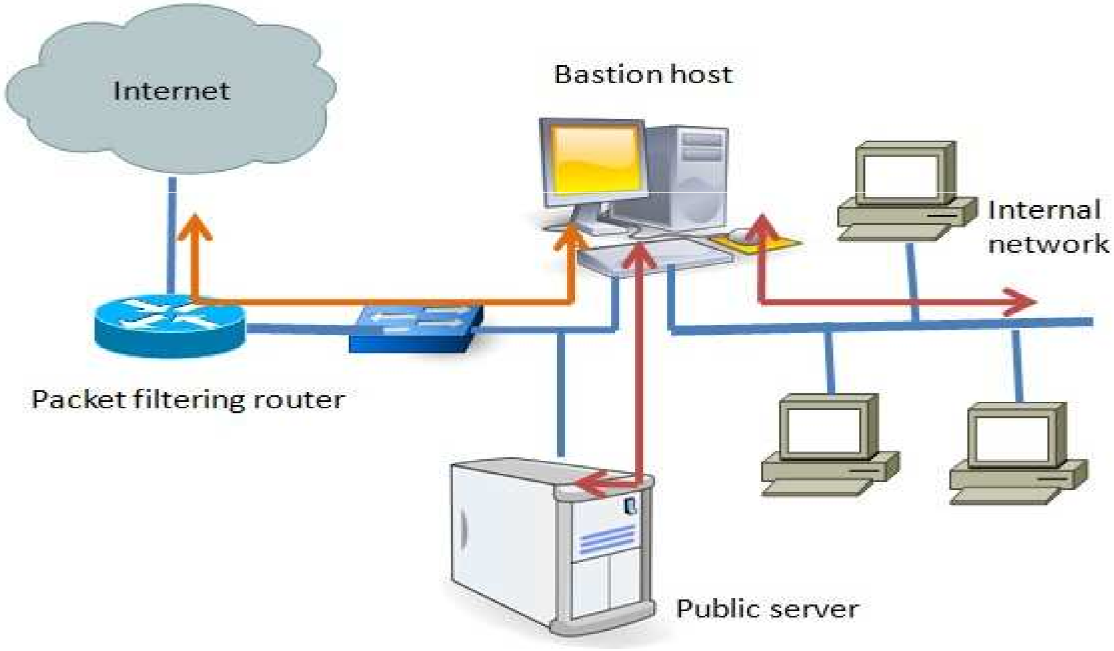
Bastion Host

- **Dual-homed bastion host:**
  - A device with **two network interface**
  - Serves as
    - Application-level gateways
    - Packet filters
    - Circuit-level gateways
  - The advantage
    - Create a complete break between the external network and the internal network
    - This break forces all incoming and outgoing traffic to pass through the host
    - Prevent a security break-in when a hacker tries to access internal devices

Firewall-Related Terminology

Bastion Host

- **Dual-homed bastion host:**



Screened host firewall (Dual-homed bastion host)

Firewall-Related Terminology

Bastion Host

- **Multihomed bastion host**
  - Single-purpose
  - Internal bastion hosts
    - Must reside inside the organisation’s internal network
    - Application gateways
    - Receive all incoming traffic from external bastion hosts
    - internal network devices are configured to communicate only with the internal bastion host
    - Provide an additional level of security in case the external firewall devices are compromised
  - Allow the user to enforce strict security mechanisms

Firewall-Related Terminology

Bastion Host

- A tri-homed firewall
  - Connects three network segments with different network addresses
  - Provides more security over firewalls with two interfaces
    - An attacker can compromise hosts on the DMZ, not any hosts on the protected internal network

Firewall-Related Terminology

Proxy Server

- Small software package
- Specifically designed for network security
- It is easier to check such modules for security flaws
- Communicate with external servers on behalf of internal clients
- Configured to allow access only to specific host systems
- A proxy service is not static
  - It is set up and torn down in response to a client request

Firewall-Related Terminology

Proxy Server

- The gateway configured to support Proxy service
- **Application-level gateway (proxy)**
  - Configured on inbound connection
  - Forward packets only when a connection has been established using some known protocol
  - When the connection closes, a firewall using application proxies rejects individual packets, even if they contain port numbers allowed by a rule set
- **Circuit-level gateway (proxy)**
  - It is also a form of proxy server
  - Configured on outbound connection
  - Circuit proxies always forward packets containing a given port number if that port number is permitted by the rule set
- **Thus, the key difference between application and circuit proxies is that the latter are static and will always set up a connection**

Firewall-Related Terminology

Proxy Server

- Logging
  - Maintains detailed audit information by logging all traffic
  - It is essential tool for detecting and terminating intruder attacks
- Each proxy is independent of other proxies on the bastion host
  - If there is a problem with the operation of any proxy, or if future vulnerability is discovered, it is easy to replace the proxy without affecting the operation of the proxy's applications
  - If the support of a new service is required, the network administrator can easily install the required proxy on the bastion host
  - A proxy generally performs no disk access other than to read its initial configuration file
  - This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host

Firewall-Related Terminology

SOCKS

- Version 4
- Provides unsecured firewall traversal for TCP-based client/server applications - HTTP, TELNET and FTP
- Extended model - include UDP
- Provide framework for generalised strong authentication schemes, and extends the addressing scheme to encompass domain name and IPv6 addresses
- Its implementation involves the recompilation or relinking of TCP-based client applications so that they can use the appropriate encapsulation routines in the SOCKS library
- RFC 1928

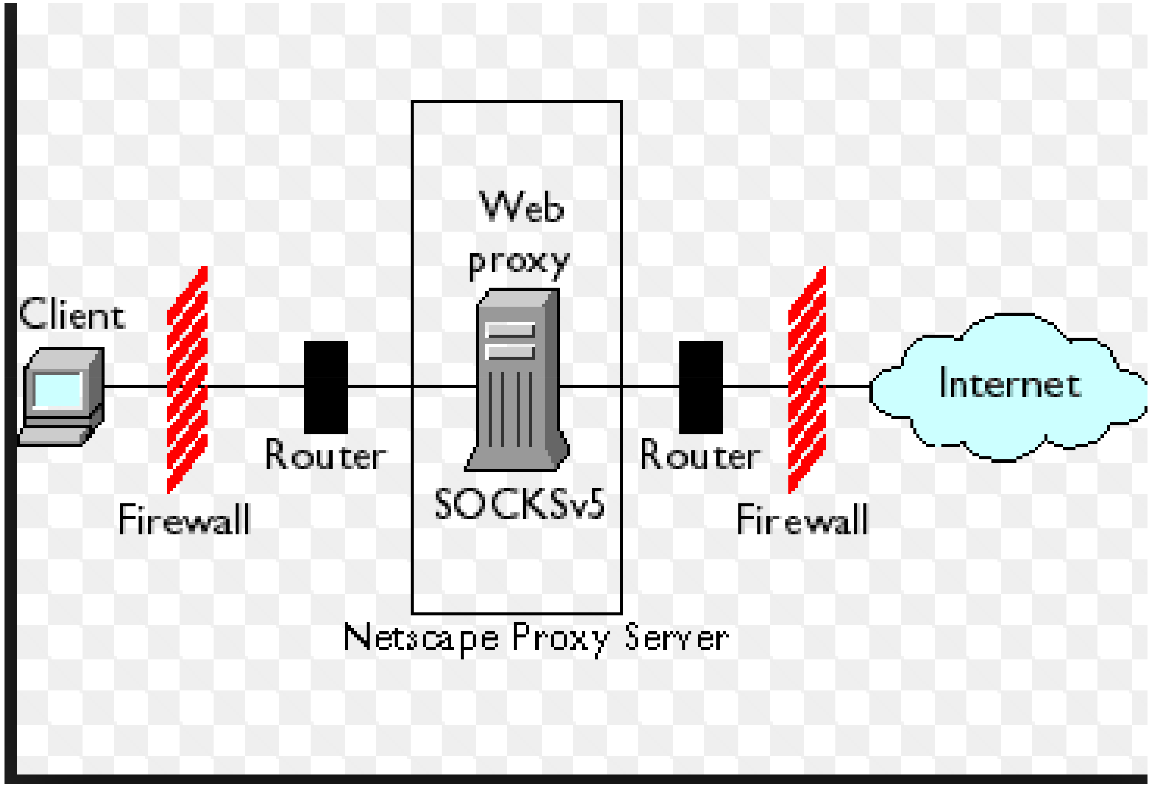
Firewall-Related Terminology

SOCKS

- TCP-based client - to establish a connection to an object that is reachable only via a firewall, it must open a TCP connection to the appropriate SOCKS port on the SOCKS server system
- TCP port 1080
- If the connection request succeeds, the client enters negotiation for the authentication method to be used, authenticates with the chosen method, and then sends a relay request
- The SOCKS server evaluates the request, and either establishes the appropriate connection or denies it
- SOCKS
  - Defines authenticated connections
  - Does not provide a clear-cut solution to the problem of encrypting the data traffic
  - IPSec can be used

Firewall-Related Terminology

SOCKS



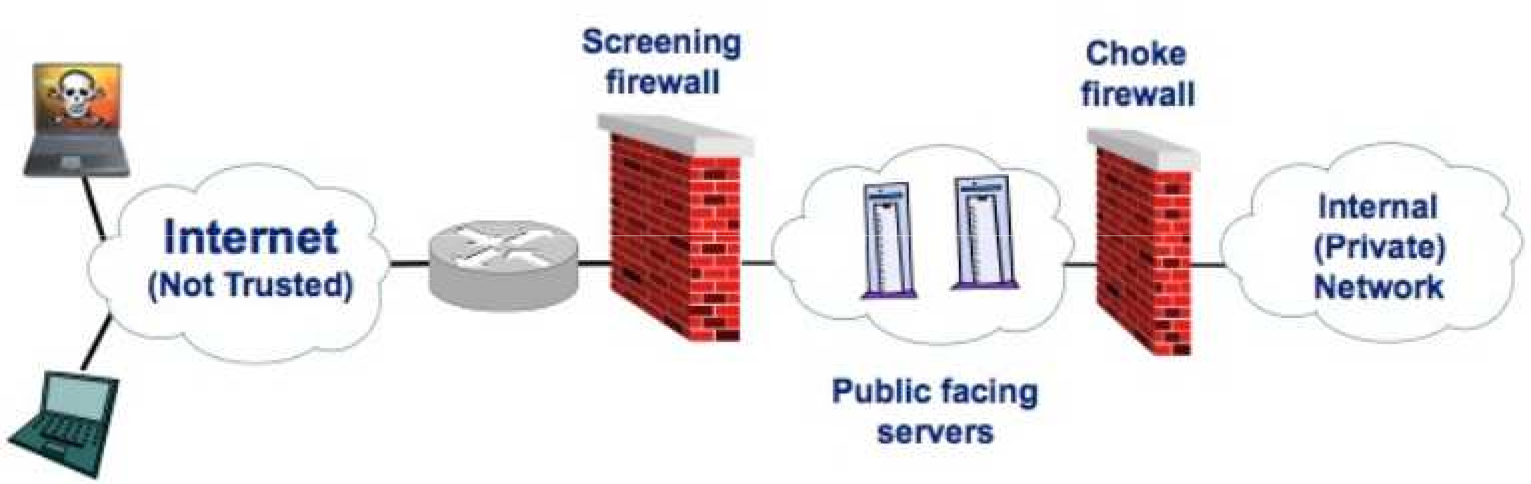
Firewall-Related Terminology

Choke Point

- Important aspect of firewall placement is to create choke points
- Point at which a public internet can access the internal network
- The most comprehensive and extensive monitoring tools should be configured on the choke points
- Proper implementation requires that all traffic be funnelled through these choke points
- It can monitor, filter and verify all inbound and outbound traffic
- Will detect exactly what a hacker is doing

Firewall-Related Terminology

Choke Point



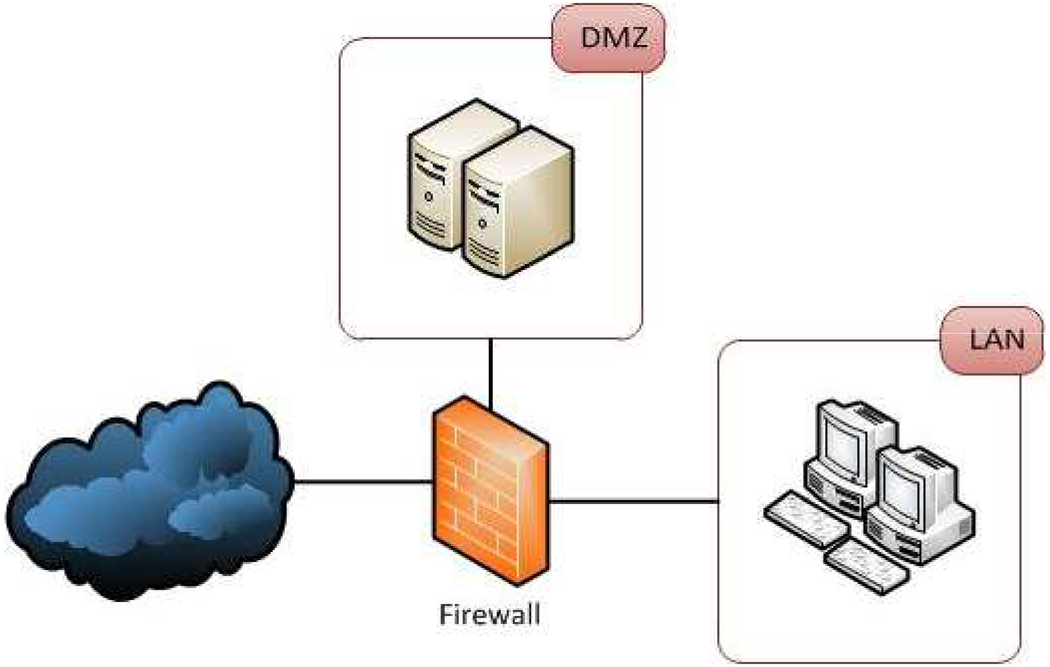
Firewall-Related Terminology

De-militarised Zone (DMZ)

- Network that lies between an internal private network and the external public network
- Called perimeter networks
- Separate the public network from the internal network
- Network inhabited by the gateway
- A gateway in the DMZ is sometimes assisted by an internal gateway
- Internal filter is used to guard against the consequences of a compromised gateway, while the outside filter can be used to protect the gateway from attack
- Many firewalls support tri-homing, allowing use of a DMZ network
- It is possible for a firewall to accommodate more than three interfaces, each attached to a different network segment

Firewall-Related Terminology

De-militarised Zone (DMZ)



Firewall-Related Terminology

Logging and Alarms

- Logging is usually implemented at every device in the firewall
- Individual logs combine to become the entire record of user activity
- Packet filters normally do not enable logging by default so as not to degrade performance
- Packet filters as well as circuit-level gateways log only the most basic information
- All traffic pass through the choke point- creates comprehensive logging
- Capture all hacker activities, including all user activities as well
- The user can then tell exactly what a hacker is doing, and have such information available for audit

Firewall-Related Terminology

Logging and Alarms

- The audit log is an essential tool for detecting and terminating intruder attacks
- Preconfigure responses to unacceptable activities in firewall can protect from attack
- The firewall should alert the user by several means
  - The two most common actions are for the firewall to break the TCP/IP connection, or to have it automatically set off alarms

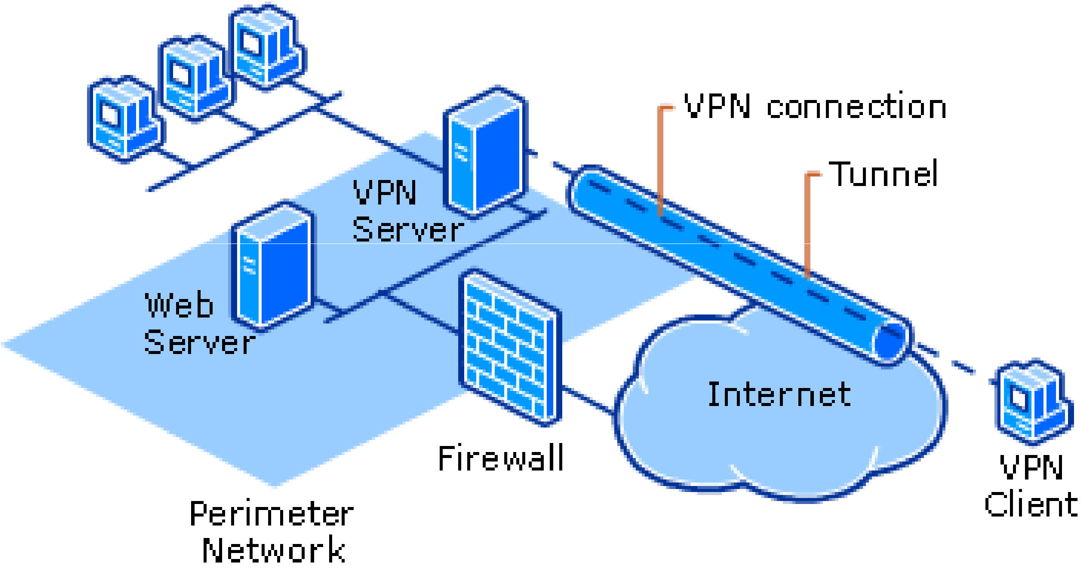
Firewall-Related Terminology

VPN

- Some firewalls are now providing VPN services
- VPNs are appropriate for any organisation requiring secure external access to internal resources
- All VPNs are **tunnelling protocols** in the sense that their information packets or payloads are encapsulated or tunnelled into the network packets
- All data transmitted over a VPN is usually encrypted because an opponent with access to the Internet could eavesdrop on the data as it travels over the public network
- The VPN **encapsulates all the encrypted data** within an IP packet
- Authentication, message integrity and encryption are very important fundamentals for implementing a VPN
- Without such authentication procedures, a hacker could impersonate anyone and then gain access to the network

Firewall-Related Terminology

VPN



Firewall-Related Terminology

VPN

- Several methods exist to implement a VPN
- RSA connection through a VPN
- Specialised firewalls or routers can be configured to establish a VPN over the Internet
- New protocols such as IPsec are expected to standardise on a specific VPN solution
  - Several VPN protocols exist, but the Point-to-Point Tunnelling Protocol (PPTP) and IPsec are the most popular

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

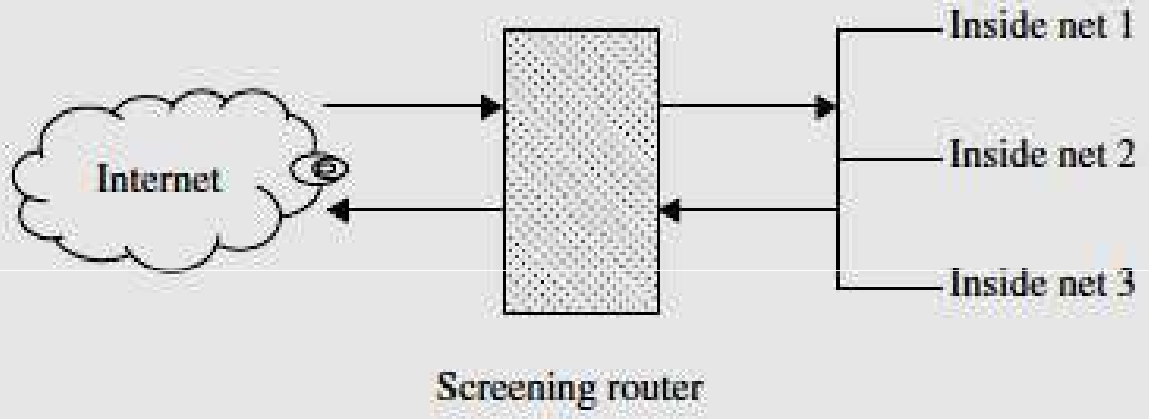


Figure 10.1 A screening router for packet filtering.

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

- Adv:
  - Restrict all inbound traffic to a specific host, preventing other host from hackers
- Disadv:
  - Cannot discriminate between good and bad packets
  - Cannot verify the content of the packet
  - Susceptibility to spoofing

Types of Firewalls

Packet Filters

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

Types of Firewalls

Packet Filters

Packet-Filtering Rules

TELNET packet filtering

- Simple “remote terminal access “
- TELNET **client software** allows user to log onto a computer by giving its domain name or IP address
- Used most often for remote management
  - For the initial setup - network hardware like switches, access points, etc.
- Working
  - Establishes a TCP connection
  - Passes keystrokes from the user’s keyboard directly to the remote computer
  - Carries output from the remote machine back to the user’s screen

Types of Firewalls

Packet Filters

Packet-Filtering Rules

TELNET packet filtering

- User names and passwords are send in plaintext
- Experienced hackers can hijack a TELNET session in progress

- Used when the user can verify the entire network connecting the client and server
- It is not allowed to connect over the Internet

- All TELNET traffic should be filtered at the firewall

Types of Firewalls

Packet Filters

Packet-Filtering Rules

TELNET packet filtering

- TELNET runs on TCP port 23
- It runs completely in open
  - non-encryption, with no authentication other than the user name and password that are transmitted in clear
- The packet-filtering rule sets are executed sequentially, from top to bottom
- Firewall discard all packets with port 23

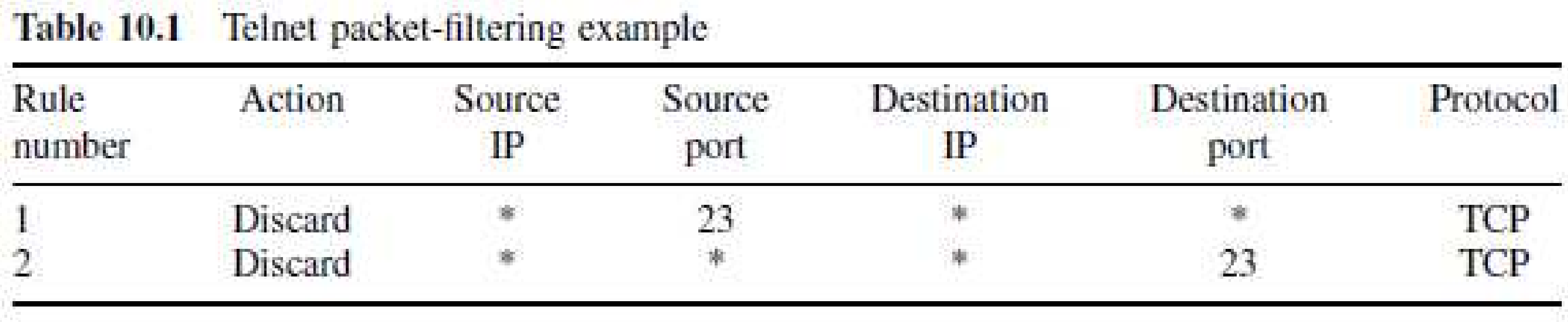


Table 10.1 Telnet packet-filtering example

Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Discard	*	23	*	*	TCP
2	Discard	*	*	*	23	TCP

Types of Firewalls

Packet Filters

Packet-Filtering Rules

FTP packet filtering

- TCP ports 20 and 21
- Rule 1 allows any host with the network address 192.168.10.0 to initiate a TCP session on any destination IP address on port 21
- Rule 2 blocks any packet originating from any remote address with a source port of 20 and contacting a host with a network address 192.168.10.0 on any port less than 1024
- Rule 3 allows any remote address that has a source port of 20 and is contacting any host with a network address of 192.168.10.0 on any port
- Once a connection is set up, the ACK flag (ACK = 1) of a TCP segment is set to acknowledge segments sent from the other side
- If any packet violates rule 2, it will be immediately discarded, and rule 3 will never be executed

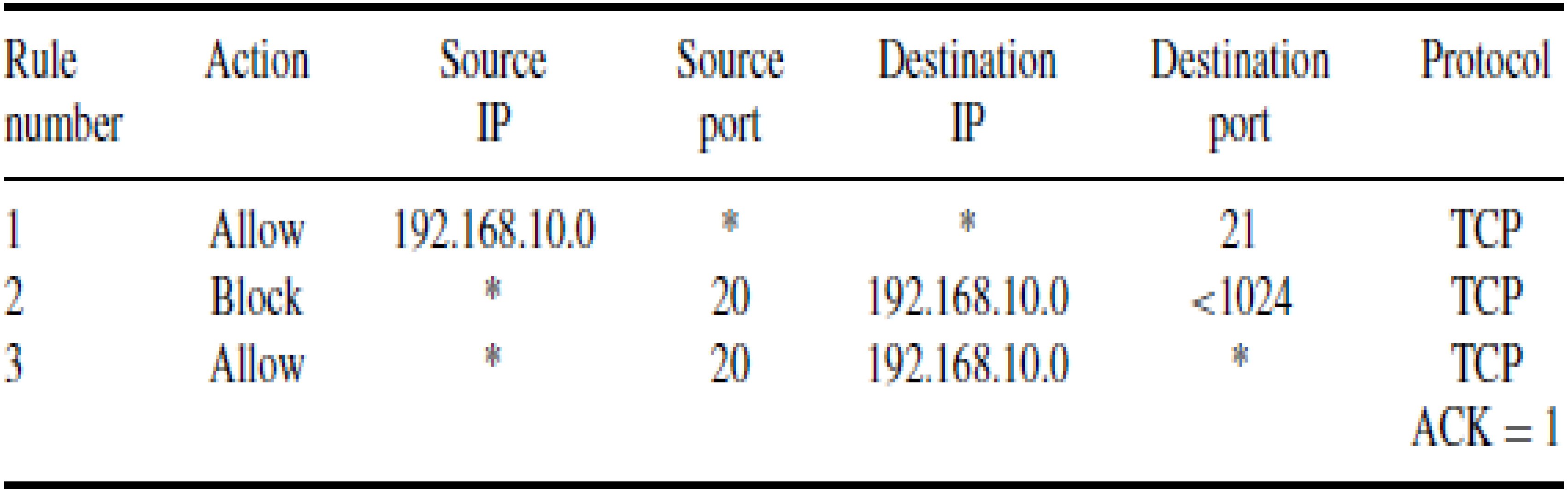
Types of Firewalls

Packet Filters

Packet-Filtering Rules

FTP packet filtering

Table 10.2 FTP packet-filtering example



Rule number	Action	Source IP	Source port	Destination IP	Destination port	Protocol
1	Allow	192.168.10.0	*	*	21	TCP
2	Block	*	20	192.168.10.0	<1024	TCP
3	Allow	*	20	192.168.10.0	*	TCP ACK = 1

Types of Firewalls

Packet Filters

Packet-Filtering Rules

FTP packet filtering

- Two TCP connections are used
  - a control connection to set up the file transfer
  - a data connection for the actual file transfer

- Each FTP server has
  - Command channel
    - where the requests for data and directory listings are issued
  - Data channel
    - over which the requested data is delivered

Types of Firewalls

Packet Filters

Packet-Filtering Rules

FTP packet filtering

- Two different modes of operations
  - Active
  - Passive

- In active mode
  - An FTP server receives commands on TCP/IP port 21 and exchanges data with the client
  - To send or receive data, the client picks an unused local TCP port between 1024 and 65 535, tells the server over the command channel, and listens for the server to connect on the chosen port
  - The server opens a connection from TCP port 20 to the specified port on the client machine
  - Once the connection is established, the data is passed across

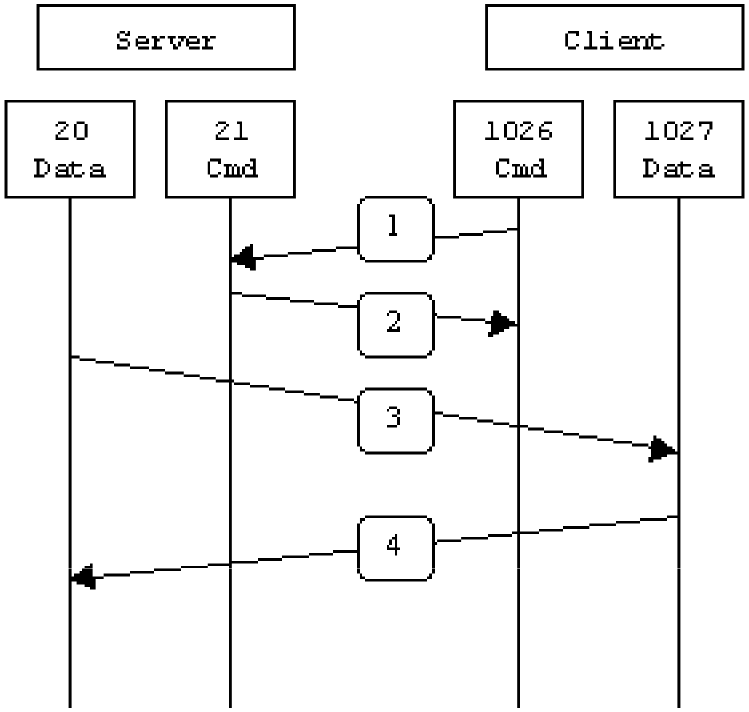
Types of Firewalls

Packet Filters

Packet-Filtering Rules

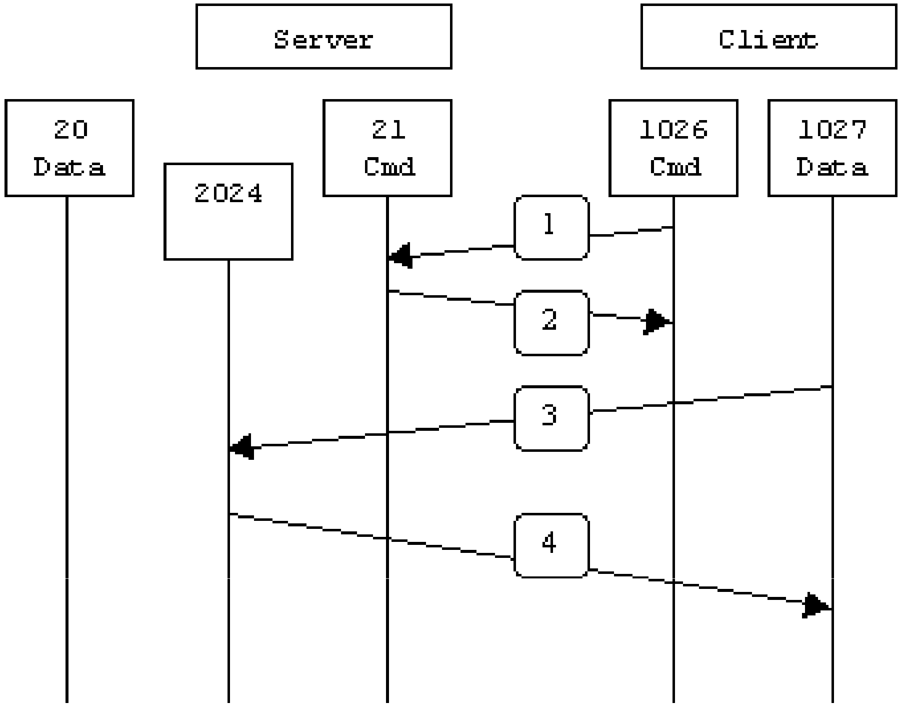
FTP packet filtering

- In passive mode,
  - The command channel is still port 21 on the server
  - The traditional data channel on port 20 is not used
  - The server picks an unused local TCP port between 1024 and 65 535 and tells the client
  - The client opens a connection to that port on the server
  - The server is listening on that port for the inbound connection from the client
  - Once the connection is established, the data flows across
  - Thus, since the client is initiating both the command and data channel connections to the server, most modern browsers use passive mode FTP for data accessing



In active mode

FTP server's port 21 from anywhere (Client initiates connection)
FTP server's port 21 to ports > 1023 (Server responds to client's control port)
FTP server's port 20 to ports > 1023 (Server initiates data connection to client's data port)
FTP server's port 20 from ports > 1023 (Client sends ACKs to server's data port)



In passive mode

FTP server's port 21 from anywhere (Client initiates connection)
FTP server's port 21 to ports > 1023 (Server responds to client's control port)
FTP server's ports > 1023 from anywhere (Client initiates data connection to random port specified by server)
FTP server's ports > 1023 to remote ports > 1023 (Server sends ACKs (and data) to client's data port)

Types of Firewalls

Packet Filters

Packet-Filtering Rules

SMTP packet filtering

- Mail Transport Agent (MTA)
  - Responsible for sending mail
  - Based on SMTP and its extension ESMTP
    - SMTP handle e-mail exchanges between mail servers
    - A host’s SMTP server accepts mail and examines the destination IP address to decide whether to deliver the mail locally or to forward it to some other machine
    - SMTP receivers use TCP port 25
    - SMTP senders use port above 1023

Types of Firewalls

Packet Filters

Packet-Filtering Rules

SMTP packet filtering

- E-mail messages are addressed with hostnames instead of IP addresses
- SMTP server uses DNS (Directory and Naming Services) to determine the matching IP address
- If the same machines handle internal and external mail delivery,
  - a hacker who can spoof DNS information may deliver internal mail to external host
- Better to use separate internal and external mail delivery machine

Types of Firewalls

SMTP packet filtering

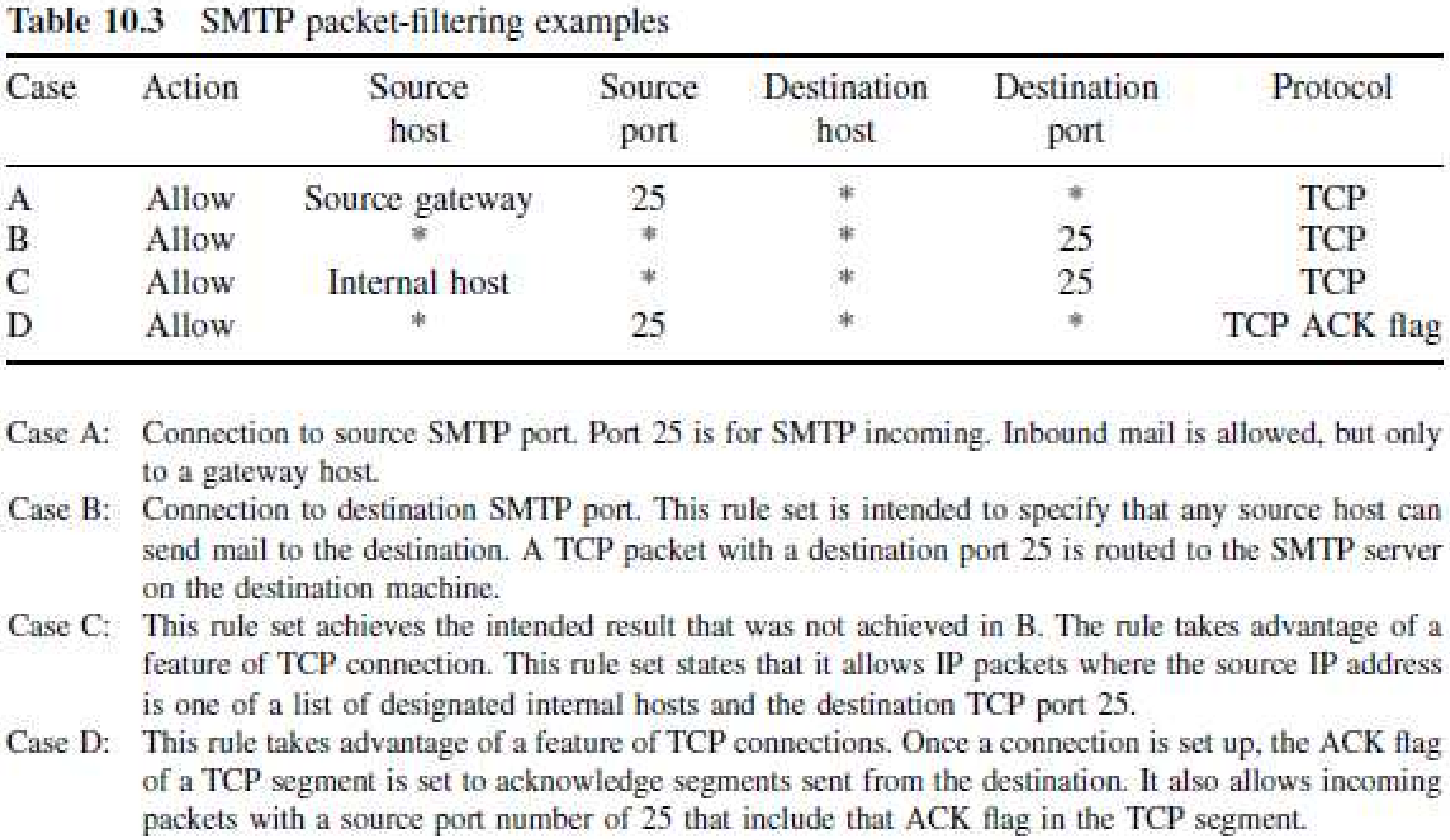


Table 10.3 SMTP packet-filtering examples

Case	Action	Source host	Source port	Destination host	Destination port	Protocol
A	Allow	Source gateway	25	*	*	TCP
B	Allow	*	*	*	25	TCP
C	Allow	Internal host	*	*	25	TCP
D	Allow	*	25	*	*	TCP ACK flag

Case A: Connection to source SMTP port. Port 25 is for SMTP incoming. Inbound mail is allowed, but only to a gateway host.

Case B: Connection to destination SMTP port. This rule set is intended to specify that any source host can send mail to the destination. A TCP packet with a destination port 25 is routed to the SMTP server on the destination machine.

Case C: This rule set achieves the intended result that was not achieved in B. The rule takes advantage of a feature of TCP connection. This rule set states that it allows IP packets where the source IP address is one of a list of designated internal hosts and the destination TCP port 25.

Case D: This rule takes advantage of a feature of TCP connections. Once a connection is set up, the ACK flag of a TCP segment is set to acknowledge segments sent from the destination. It also allows incoming packets with a source port number of 25 that include that ACK flag in the TCP segment.

Types of Firewalls

Circuit-Level Gateways

- Proxy server
- Statically defines what traffic will be forwarded
  - Forward packets containing a given port number
- Operates at the network level of the OSI model
- Provide Network Address Translation (NAT)
  - NAT hides the internal IP address from the Internet
  - Gateway sends out the packets on behalf of the internal system and receives any replies (IP address of the gateway's)
- Works on same principles as packet filter firewalls - predetermined rules set

Types of Firewalls

Circuit-Level Gateways

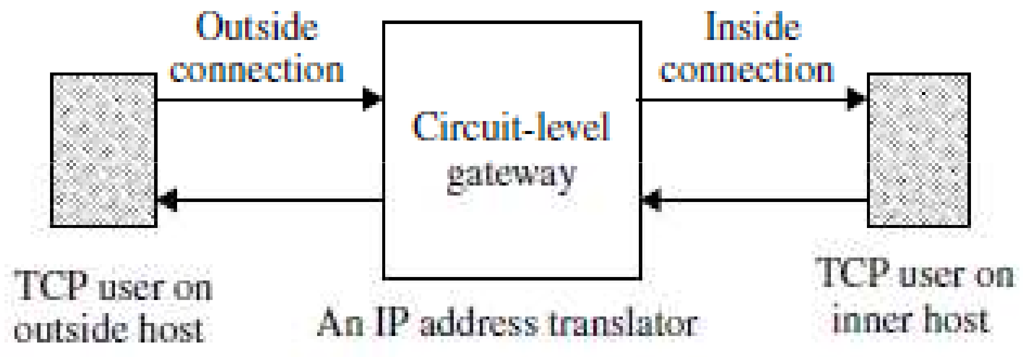
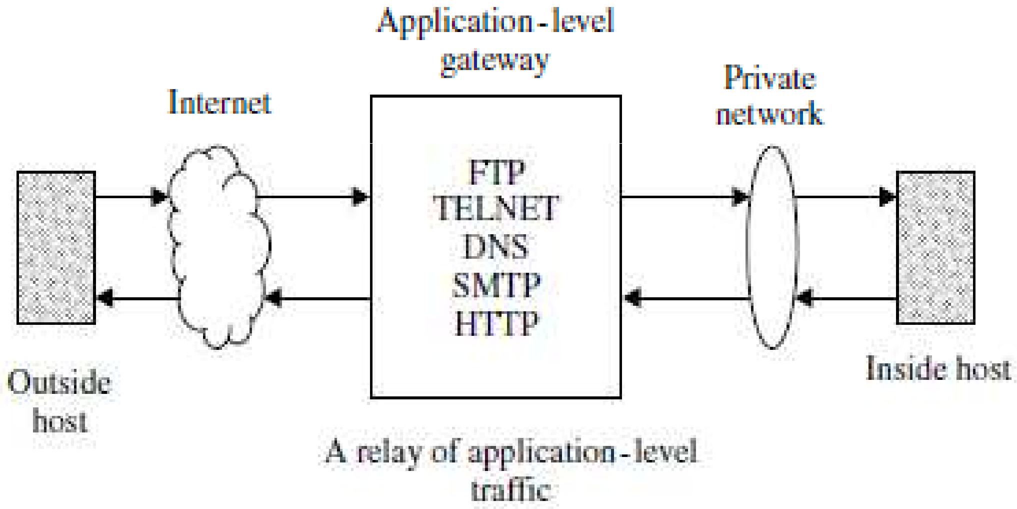


Figure 10.2 Circuit-level gateway for setting up two TCP connections.

Types of Firewalls

Application-Level Gateways



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

Types of Firewalls

Application-Level Gateways

- Proxy server
- Performing at the TCP/IP application level
- Set up and torn connections in response to a client request, rather than existing on a static basis
- Forward packets only when a connection has been established using some known protocol
- When the connection closes, a firewall using application proxies rejects individual packets, even if the packets contain port numbers allowed by a rule set.

Types of Firewalls

Application-Level Gateways

- Inside host initiates a TCP/IP connection
- The application gateway receives the request and checks it against a set of rules or filters
- Then initiate a TCP/IP connection with the remote server

- The server will generate TCP/IP responses based on the request from the proxy server

- The responses will be sent to the proxy server (application gateway) where the responses are again checked against the proxy server’s filters
- If the remote server’s response is permitted, the proxy server will then forward the response to the inside host

Types of Firewalls

Application-Level Gateways

- TCP protocol works better than UDP as it is connection based protocol
- ICMP programs are nearly impossible to proxy
  - ICMP messages do not work through an application-level gateway
- For example
  - HTTP traffic is often used in conjunction with proxy servers
  - Internal host could not ping (based on ICMP) a remote host through the proxy server

Firewall Designs

- Firewall design must prevent the firewall devices from being compromised by threat
- Three basic firewall designs are
  - a single-homed bastion host
  - a dual-homed bastion host
  - a screened subnet
- The first two options -act as screened host firewall
- Screened subnet - contains an additional packet-filtering router to achieve another level of security
- Design - simple with the fewest possible components, both hardware and software

Firewall Designs

- A bastion host
  - Publicly accessible device
  - First device - When Internet users attempt to access resources on the Internet network
  - Fewer running services on the bastion host will give a potential hacker less opportunity to overcome the firewall
  - Must check all incoming and outgoing traffic and enforce the rules specified in the security policy
  - Armed with logging and alarm features to prevent attacks

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)

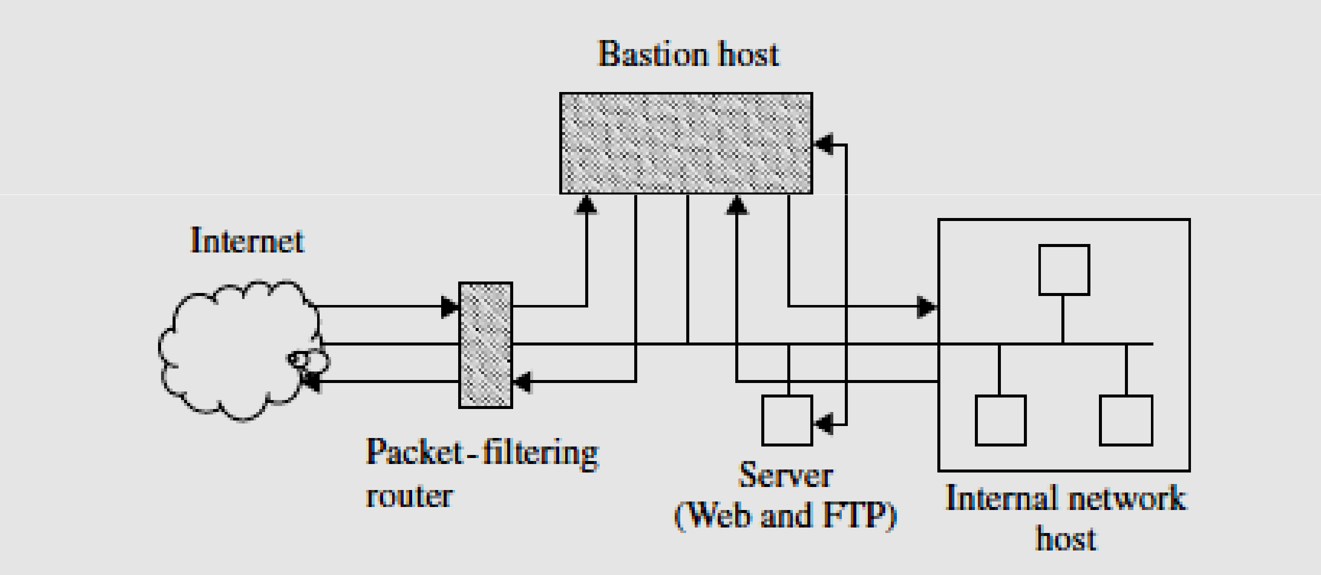


Figure 10.4 Screened host firewall system (single-homed bastion host).

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)

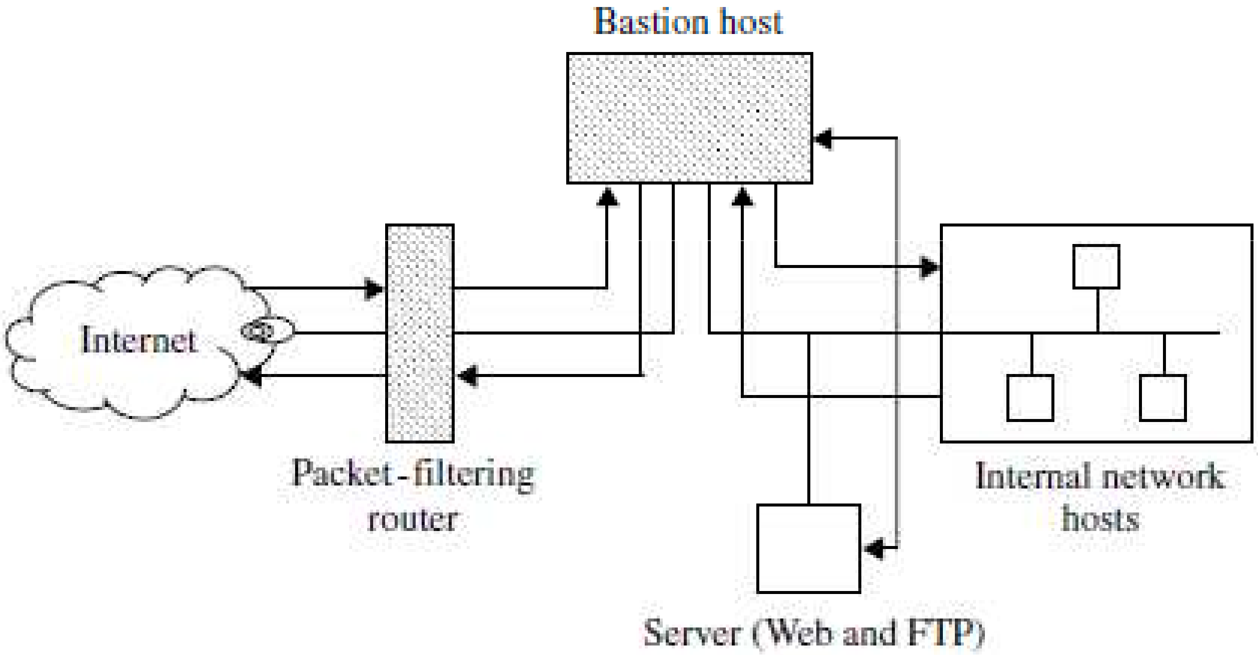


Figure 10.5 Screened host firewall system (dual-homed bastion host).

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
- Most secure
- Support both circuit- and application-level gateways
- Two screening routers
  - External and internal
  - Configured such that its traffic flows only to or from the bastion host
  - This arrangement prevents any traffic from directly traversing the DMZ subnetwork

Firewall Designs

Screened Subnet Firewall

- The external screening router
  - Uses standard filtering
  - Restrict external access to the bastion host, and rejects any traffic that does not come from the bastion host
  - Prevent IP spoofing
- The internal screening router
  - Uses rules to prevent spoofing
  - Rejects incoming packets that do not originate from the bastion host
  - Sends only outgoing packets to the bastion host

Firewall Designs

Screened Subnet Firewall

- Hacker **must subvert three separate tri-homed** interfaces when he or she wants to access the internal network. But it is almost infeasible.
- Second, the **internal network is effectively invisible** to the Internet because all inbound/outbound packets go directly through the DMZ

  This arrangement makes it impossible for a hacker to gain information about the internal systems because only the DMZ is advertised in the routing tables and other Internet information
- Third**, internal users cannot access the Internet** without going through the bastion host

Firewall Designs

Screened Subnet Firewall

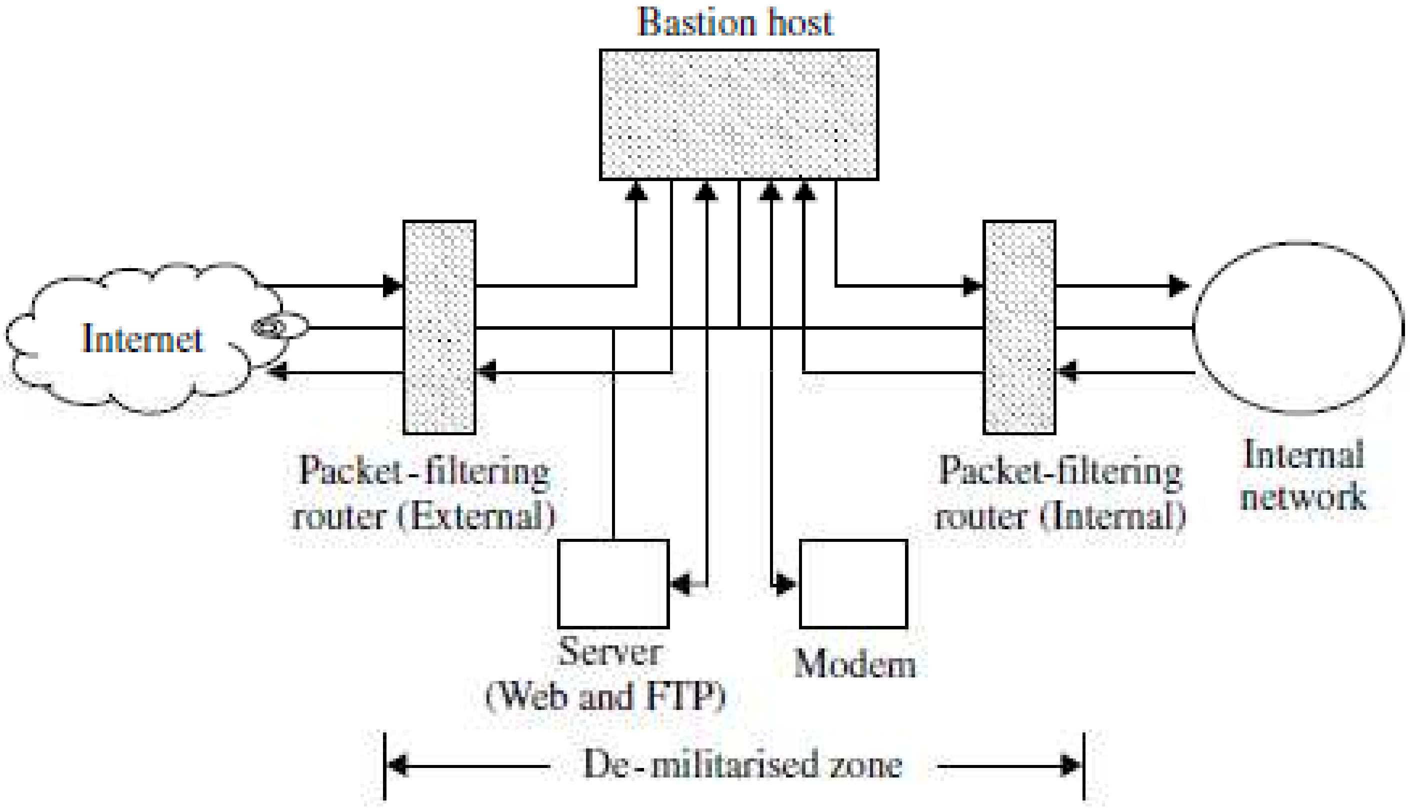


Figure 10.6 Screened subnet firewall system.