KF School of Computing and Information Sciences
Florida International University

CNT 4403
Computing and Network Security

Network Security – Firewalls

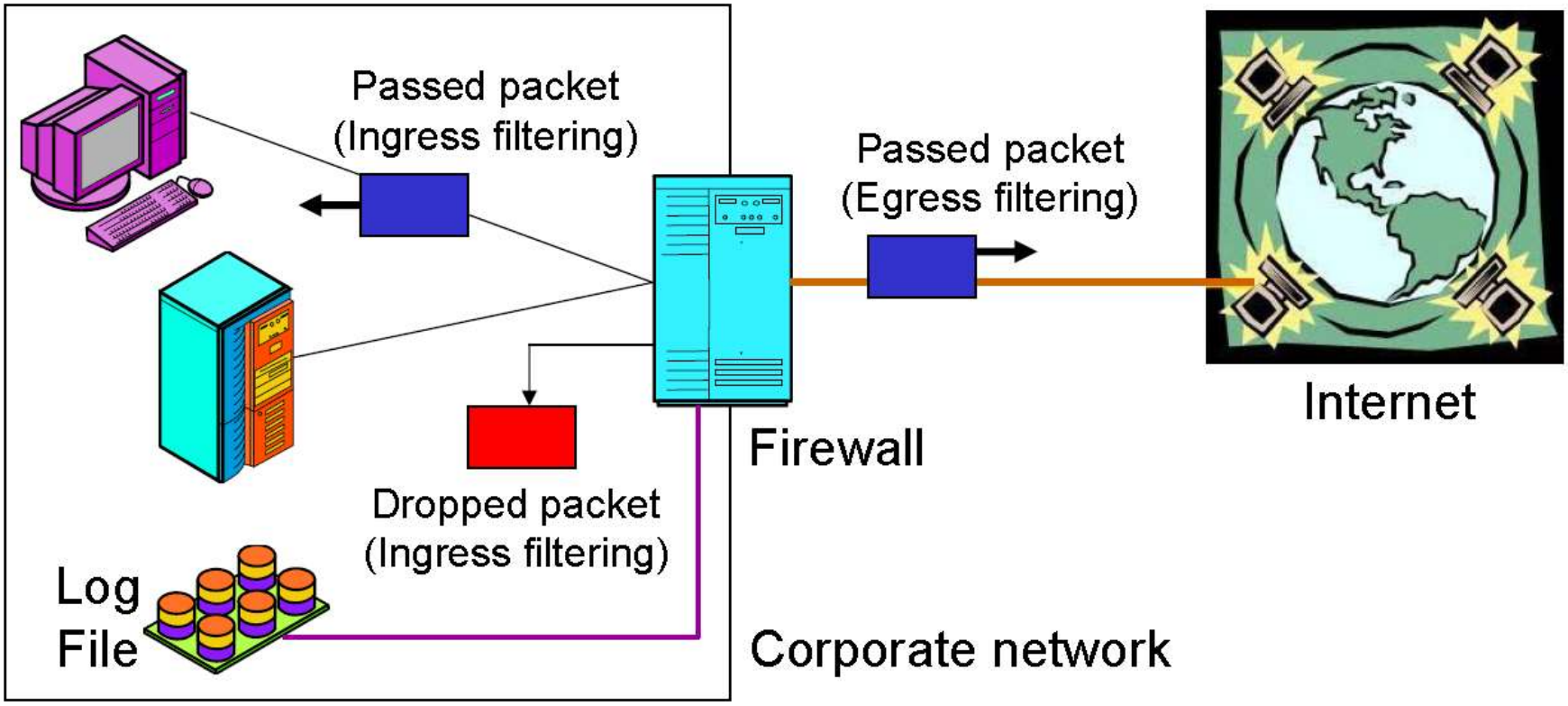
Dr. Kemal Akkaya

E-mail: *kakkaya@fiu.edu*

Firewalls

- **Prevent specific types of information from moving between the outside world (untrusted network) and the inside world (trusted network)**
- **May be separate computer system; a software service running on existing router or server; or a separate network containing supporting devices**
- **Five processing modes that firewalls can be categorized by are:**
  - Application gateways
  - Circuit gateways
  - Packet filtering
  - MAC layer firewalls
  - Hybrids

Firewall


Passed packet
(Ingress filtering)
Passed packet
(Egress filtering)
Internet
Firewall
Dropped packet
(Ingress filtering)
Log
File
Corporate network

Packet Filtering

- **Examine header information of data packets**
- **Most often based on combination of:**
  - IP source and destination address
  - Direction (inbound or outbound)
  - TCP or UDP source and destination port requests
- **Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses**
- **Three subsets of packet filtering firewalls:**
  - Static filtering: requires that filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed
  - Dynamic filtering: allows firewall to react to emergent event and update or create rules to deal with event
  - Stateful inspection: firewalls that keep track of each network connection between internal and external systems using a state table

Filtering Example

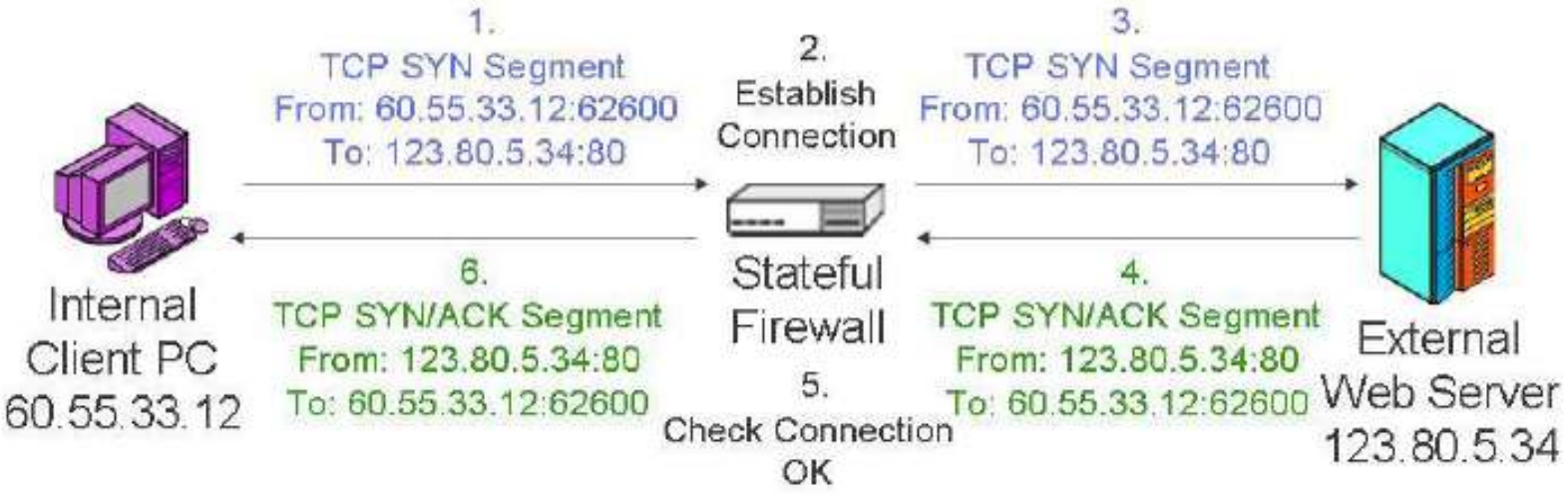
Rule	Source IP	Source Port	Destination IP	Destination Port	Action	Comments
1	192.168.120.1	Any	Any	Any	Deny	Prevents the firewall itself from making any connections
2	Any	Any	192.168.120.1	Any	Deny	Prevents anyone from connecting to the firewall
3	Any	Any	192.168.120.*	>1023	Allow	Accepts responses from external hosts that are contacted by an internal host from a port above 1023
4	192.168.120.*	Any	Any	Any	Allow	Allows internal users to access external computers
5	Any	Any	192.168.120.2	25	Allow	Allows external and internal users to access the email server
6	Any	Any	192.168.120.3	80	Allow	Enables both external and internal users to connect to the Web server
7	Any	Any	Any	Any	Deny	Blocks all traffic not covered by previous rules

Filtering disadvantages

- **Can be difficult to configure**
  - Easy to accidentally configure a packet to be denied to get in
  - Difficult to test
- **Most packet filters do not support advanced user authentication**
- **They do not examine application-level data**
  - They cannot prevent attacks that employ application specific vulnerabilities
- **Vulnerable to attacks that exploit protocol weaknesses such as IP spoofing**

Stateful Inspection

- Maintains a table for established outbound connections
- It will allow traffic to high numbered ports only for those packets that fit the profile of one of the entries in the connection table

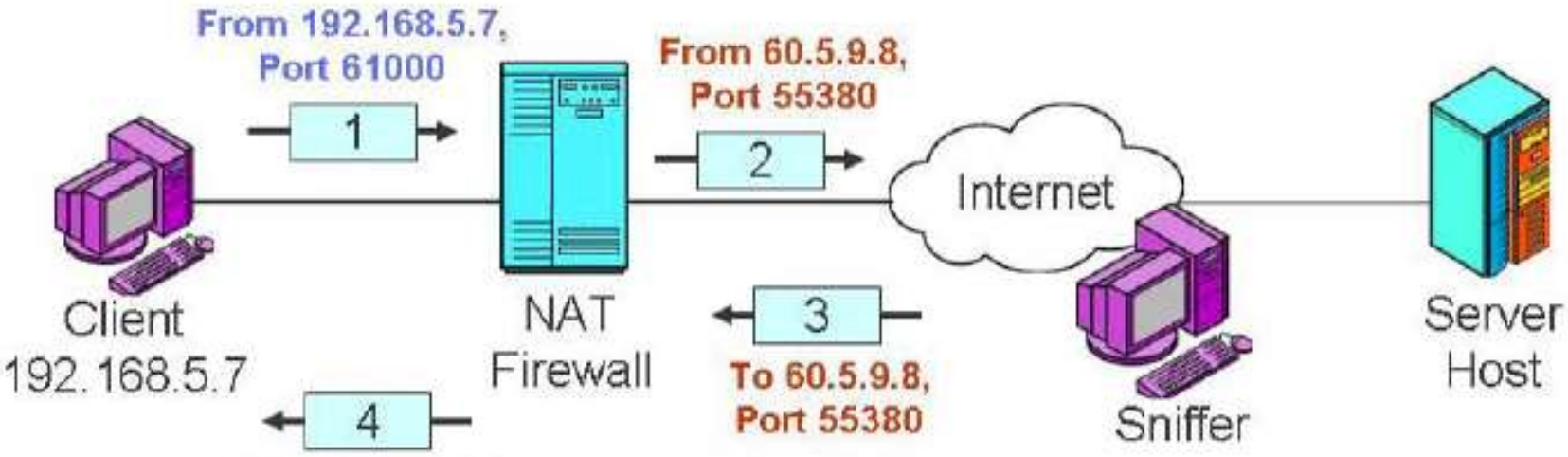


Connection Table

Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	62600	123.80.5.34	80	Established
UDP	60.55.33.12	63206	1.8.33.4	69	Established

Network Address Translation

- **Packet Filters offer a second form of protection called Network Address Translation**
  - Prevent external sniffers to learn internal IP and port numbers



Translation Table

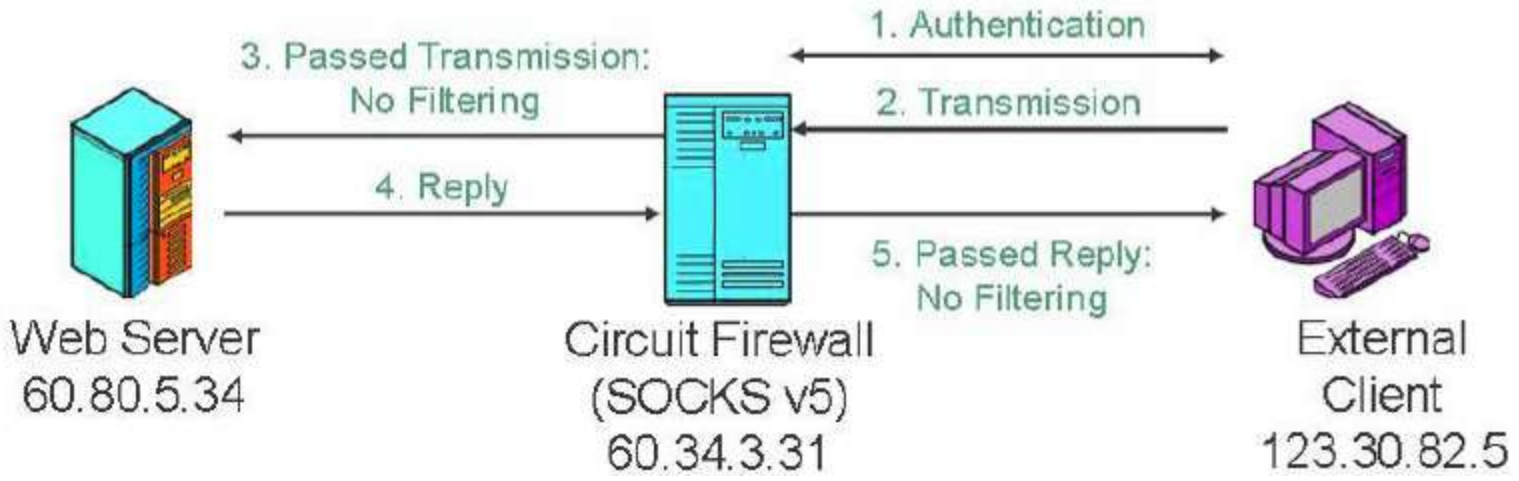
Internal		External	
IP Address	Port	IP Address	Port
192.168.5.7	61000	60.5.9.8	55380
. . .	. . .	. . .	. . .

Application Gateways

- Frequently installed on a dedicated computer; also known as a proxy server (or reverse proxy)
- Used in conjunction with filtering router
- Examines application-level traffic
  - E.g. A proxy can be configured to block HTTP communication with ActiveX control
- Since proxy server is often placed in unsecured area of the network, it is exposed to higher levels of risk from less trusted networks
- Additional filtering routers can be implemented behind the proxy server, further protecting internal systems

Circuit Gateways

- **Circuit gateway firewall operates at transport layer**
- **Prevents direct connections between one network and another**
  - Accomplished by creating tunnels connecting specific processes or systems on each side of the firewall, and allow only authorized traffic in the tunnels
  - Does not examine messages but can log or cache them



MAC Layer Firewalls

- Designed to operate at the media access control layer of OSI network model
- Able to consider specific host computer's identity in its filtering decisions
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked

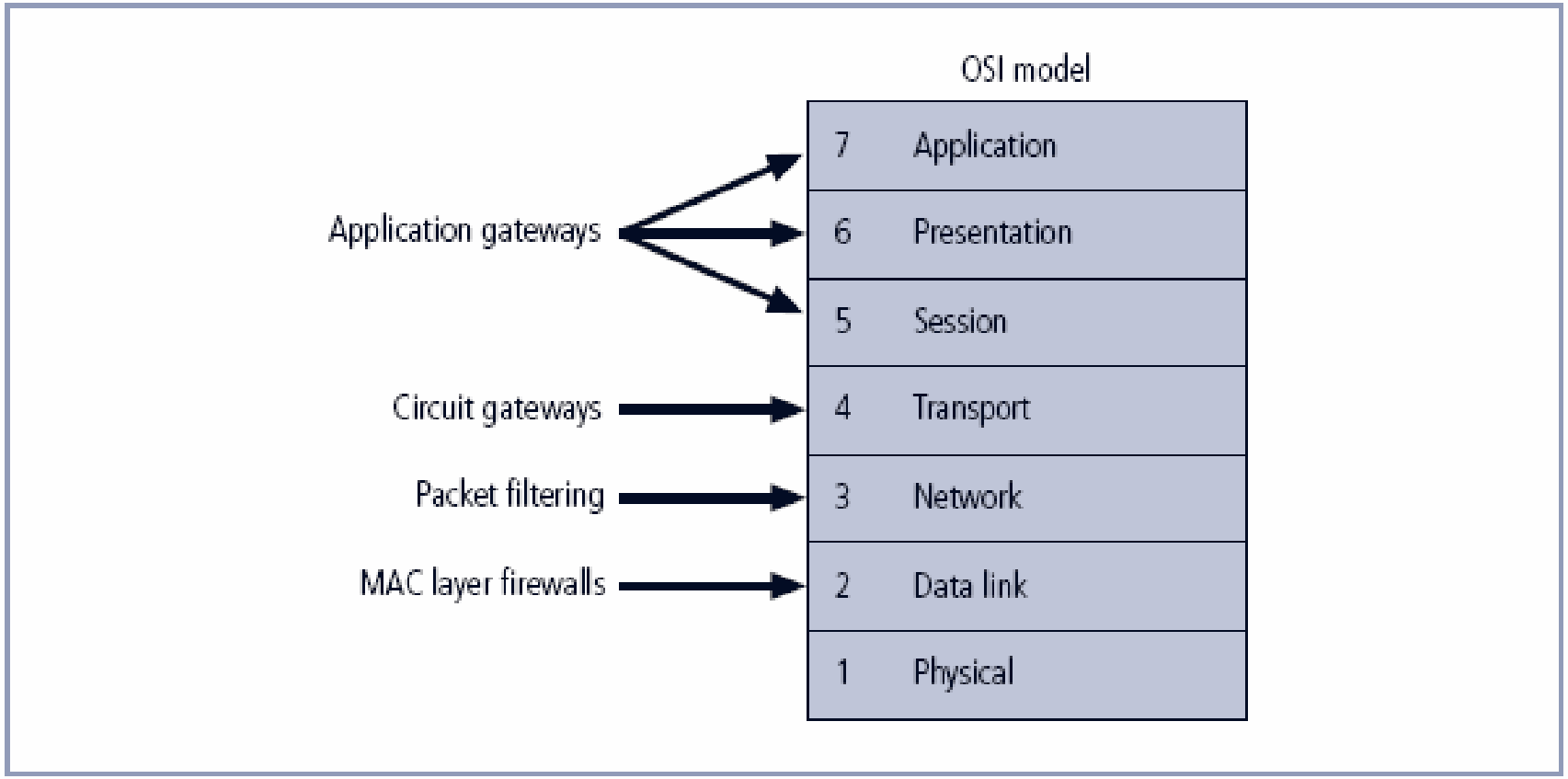


FIGURE 6-5 Firewall Types and the OSI Model

Hybrid Firewalls

- Combine elements of other types of firewalls; i.e., elements of packet filtering and proxy services, or of packet filtering and circuit gateways
- Alternately, may consist of two separate firewall devices; each a separate firewall system, but connected to work in tandem

Firewalls Categorized by Structure

- Most firewalls are appliances: stand-alone, self-contained systems
- Commercial-grade firewall system consists of firewall application software running on general-purpose computer
- Small office/home office (SOHO) or residential-grade firewalls, aka broadband gateways or cable modem routers, connect user's local area network or a specific computer system to Internetworking device
- Residential-grade firewall software is installed directly on the user's system

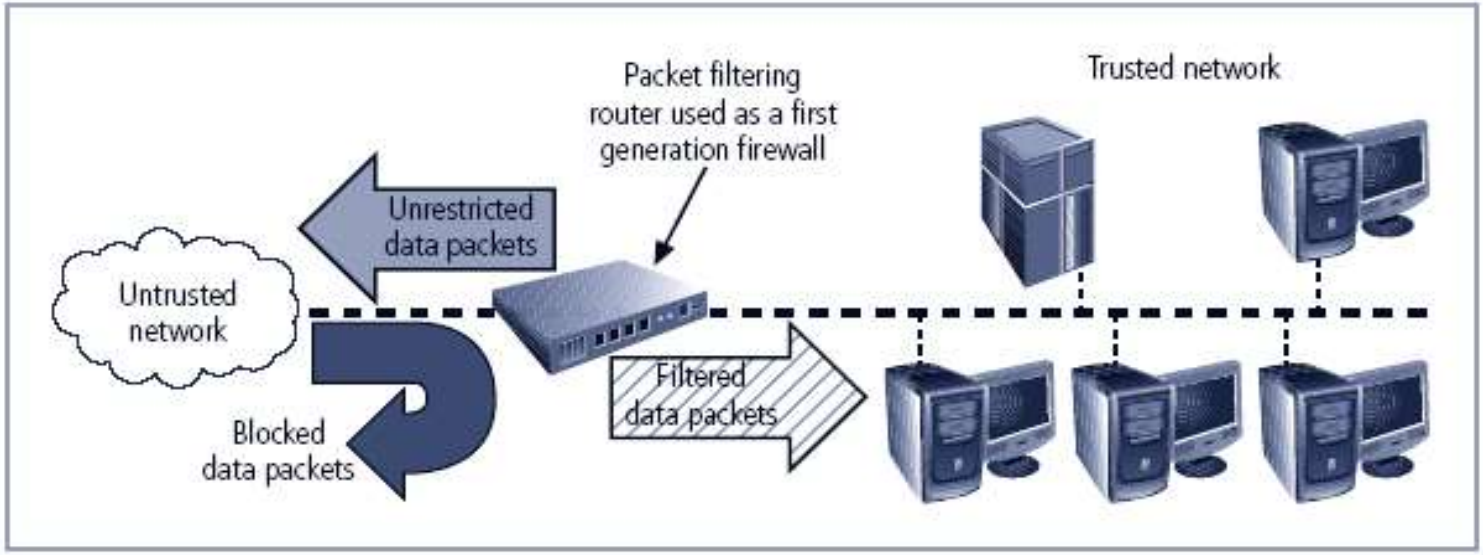
FIGURE 6-6 SOHO Firewall Devices

Firewall Architectures

- **Firewall devices can be configured in a number of network connection architectures**
- **Configuration that works best depends on three factors:**
  - Objectives of the network
  - Organization's ability to develop and implement architectures
  - Budget available for function
- **Four common architectural implementations of firewalls:**
  - packet filtering routers, screened host firewalls, dual-homed firewalls, screened subnet firewalls

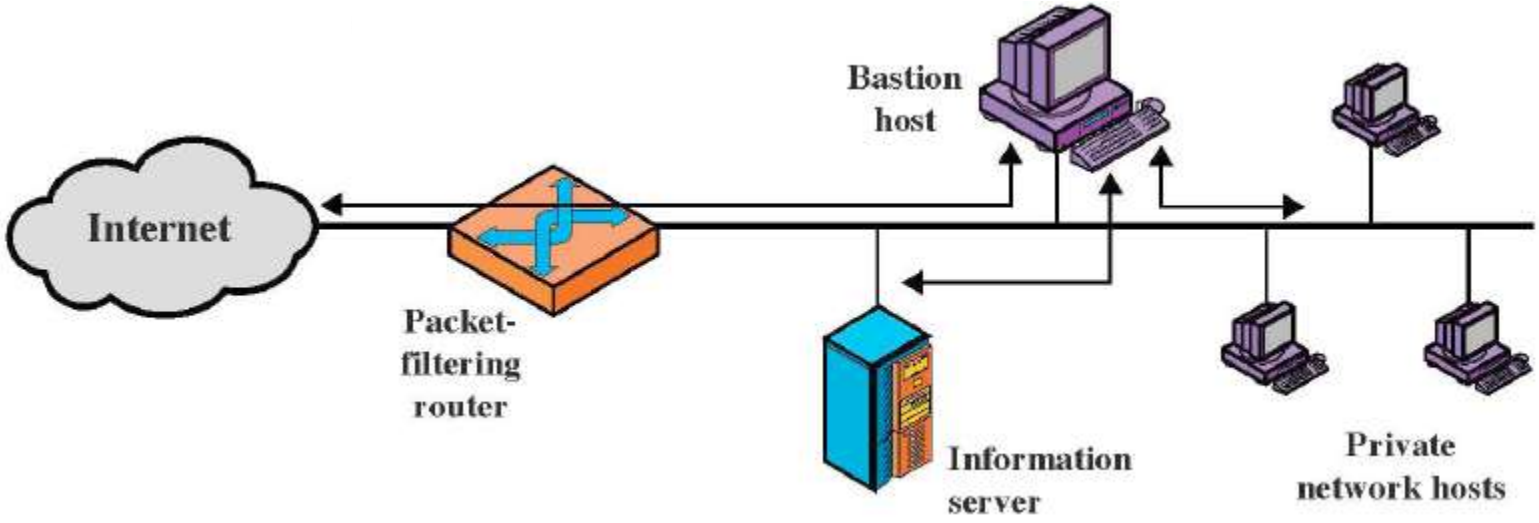
Packet Filtering Routers

- Most organizations with Internet connection have a router serving as interface to Internet
- Many of these routers can be configured to reject packets that organization does not allow into network
- Drawbacks include a lack of auditing and strong authentication



Screened Host Firewalls

- **Combines packet filtering router with separate, dedicated firewall such as an application proxy server or bastion host**
  - Router allows packets to/from bastion host
  - Bastion host performs authentication and proxy
- **Router minimizes traffic/load on bastion host**

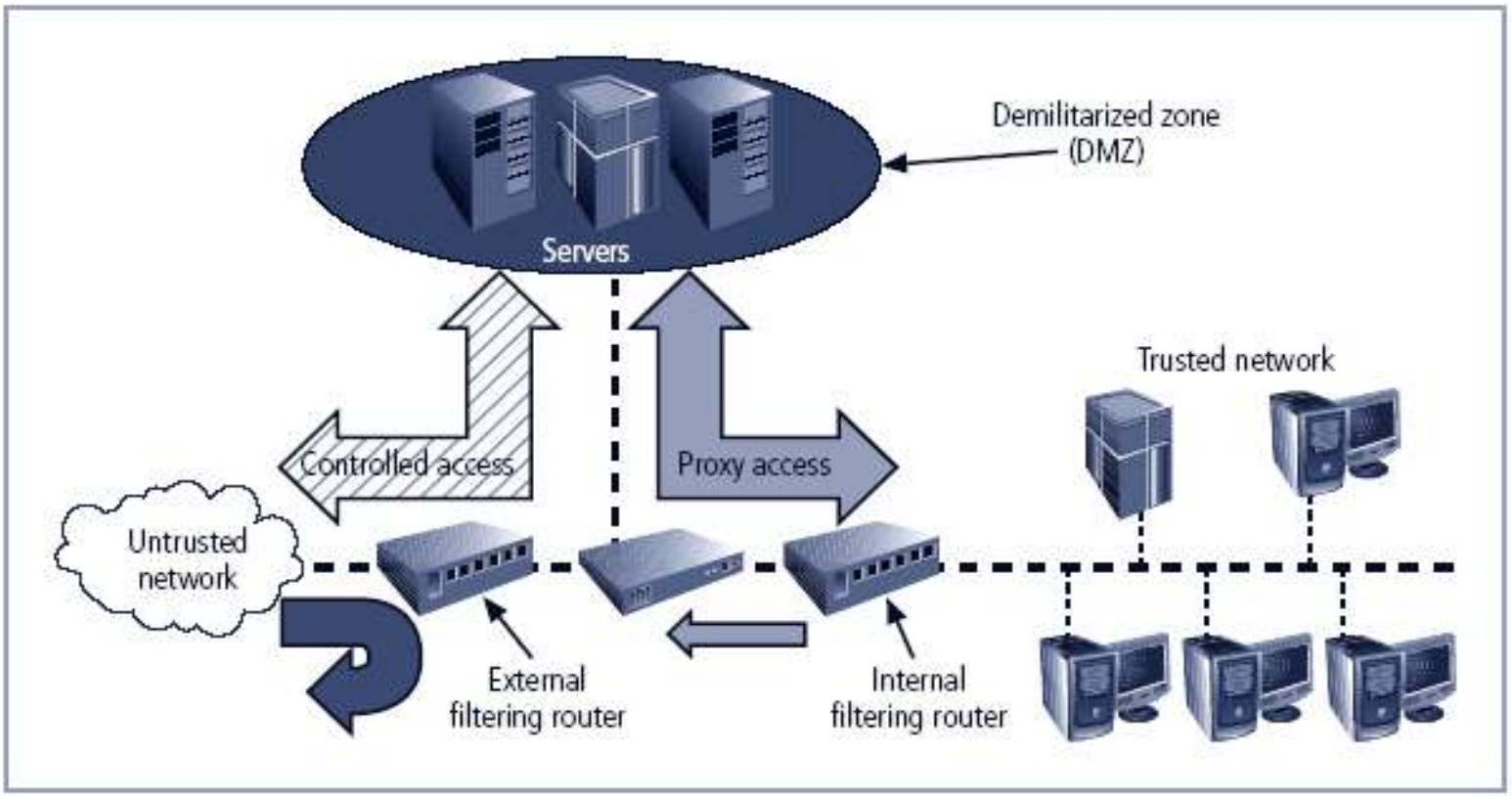


Dual-Homed Host Firewalls

- **In screened host architecture, if packet filtering router is compromised, the traffic can flow through the private network.**
- **This is not allowed in dual-homed host architecture**
  - Bastion host contains two network interface cards (NICs): one connected to external network, one connected to internal network
  - All traffic should flow through the bastion host
- **Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers**

Screened Subnet Firewalls (with DMZ)

- **Dominant architecture used today is the screened subnet firewall**
- **Commonly consists of two or more internal bastion hosts behind external packet filtering router and before the internal filtering router:**
  - Connections from outside (untrusted network) routed through external filtering router
  - The network segment in between is known as demilitarized zone (DMZ)
  - Connections into trusted internal network allowed only from DMZ bastion host servers
- **Screened subnet performs two functions:**
  - Protects DMZ systems and information from outside threats
  - Protects the internal networks by limiting how external connections can gain access to internal systems


Demilitarized zone
(DMZ)
Servers
Trusted network
Controlled access
Proxy access
Untrusted
network
External
filtering router
Internal
filtering router

Limitations of Firewalls

- **Will not protect from all the attacks**
  - E.g. insider attacks
  - Not all of the outsider attacks
- **Are effective if they control all the perimeter**
- **Do not protect outsider data once they pass through the firewalls**
  - Inaccurate data or malicious code must be controlled by other means inside
- **Most attractive target for attack and single point of failure**
  - Therefore as an option Honeypots are sometimes deployed:
    - ✓ Purposely configured with some security holes so that they look vulnerable
    - ✓ The attacks can be attracted to these fake systems