Firewalls

Introduction

- Seen evolution of information systems
- Now everyone want to be on the Internet
  and to interconnect networks
- Has persistent security concerns
  - can’t easily secure every system in org
- Need "harm minimisation"
- a **Firewall** usually part of this

What is a Firewall?

- a **choke point** of control and monitoring

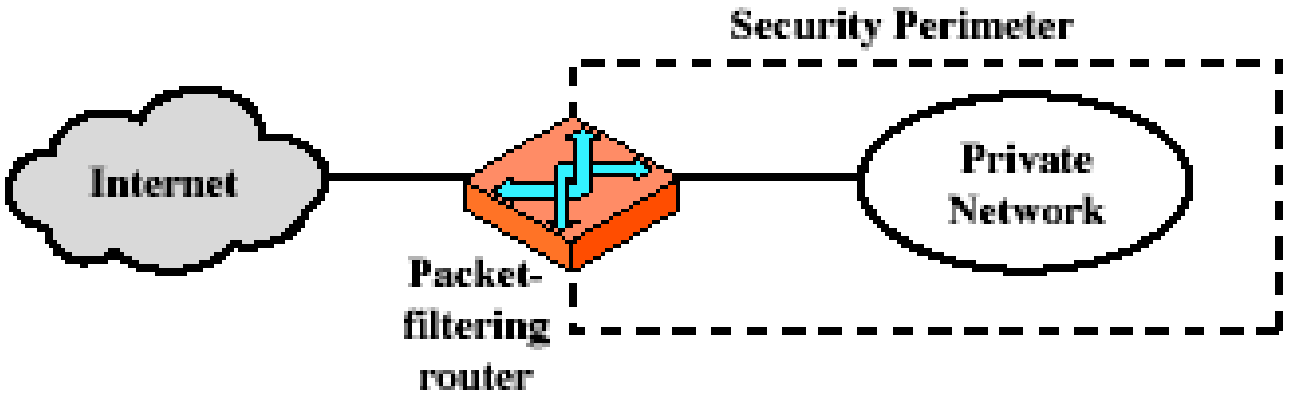
interconnects networks with differing trust

- Imposes restrictions on network services
  - only authorized traffic is allowed
- Auditing and controlling access
  - can implement alarms for abnormal behavior
- Is itself immune to penetration
- Provides **perimeter defence**

Firewall Limitations

- cannot protect from attacks bypassing it
  - eg sneaker net, utility modems, trusted organizations, trusted services (eg SSL/SSH)
- cannot protect against internal threats
  - eg disgruntled employee
- cannot protect against transfer of all virus infected programs or files
  - because of huge range of O/S & file types

Firewalls – Packet Filters



(a) Packet-filtering router

Firewalls – Packet Filters

- Simplest of components
- Foundation of any firewall system
- Examine each IP packet (no context) and permit or deny according to rules
- Hence restrict access to services (ports)
- Possible default policies
  - that not expressly permitted is prohibited
  - that not expressly prohibited is permitted

Firewalls – Packet Filters

A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

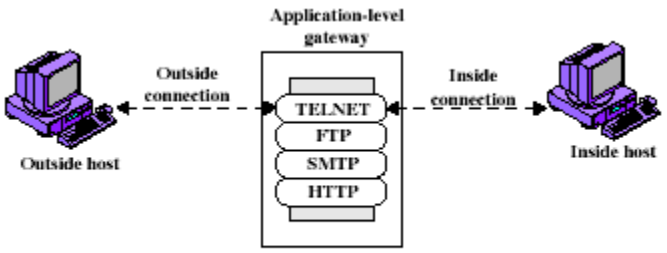
Attacks on Packet Filters

- IP address spoofing
  - fake source address to be trusted
  - add filters on router to block
- Source routing attacks
  - attacker sets a route other than default
  - block source routed packets
- Tiny fragment attacks
  - split header info over several tiny packets
  - either discard or reassemble before check

Firewalls – Stateful Packet Filters

- Examine each IP packet in context
  - keeps tracks of client-server sessions
  - checks each packet validly belongs to one
- Better able to detect bogus packets out of context

Firewalls - Application Level Gateway (or Proxy)

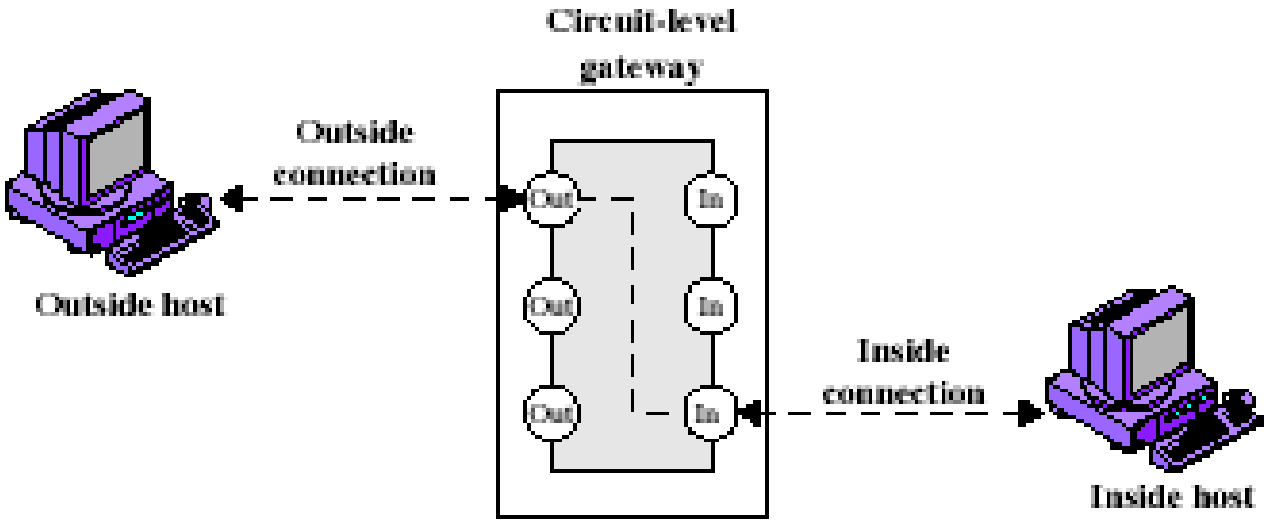


(b) Application-level gateway

Firewalls - Application Level Gateway (or Proxy)

- Use an application specific gateway / proxy
- Has full access to protocol
  - user requests service from proxy
  - proxy validates request as legal
  - then actions request and returns result to user
- Need separate proxies for each service
  - some services naturally support proxying
  - others are more problematic
  - custom services generally not supported

Firewalls - Circuit Level Gateway



(c) Circuit-level gateway

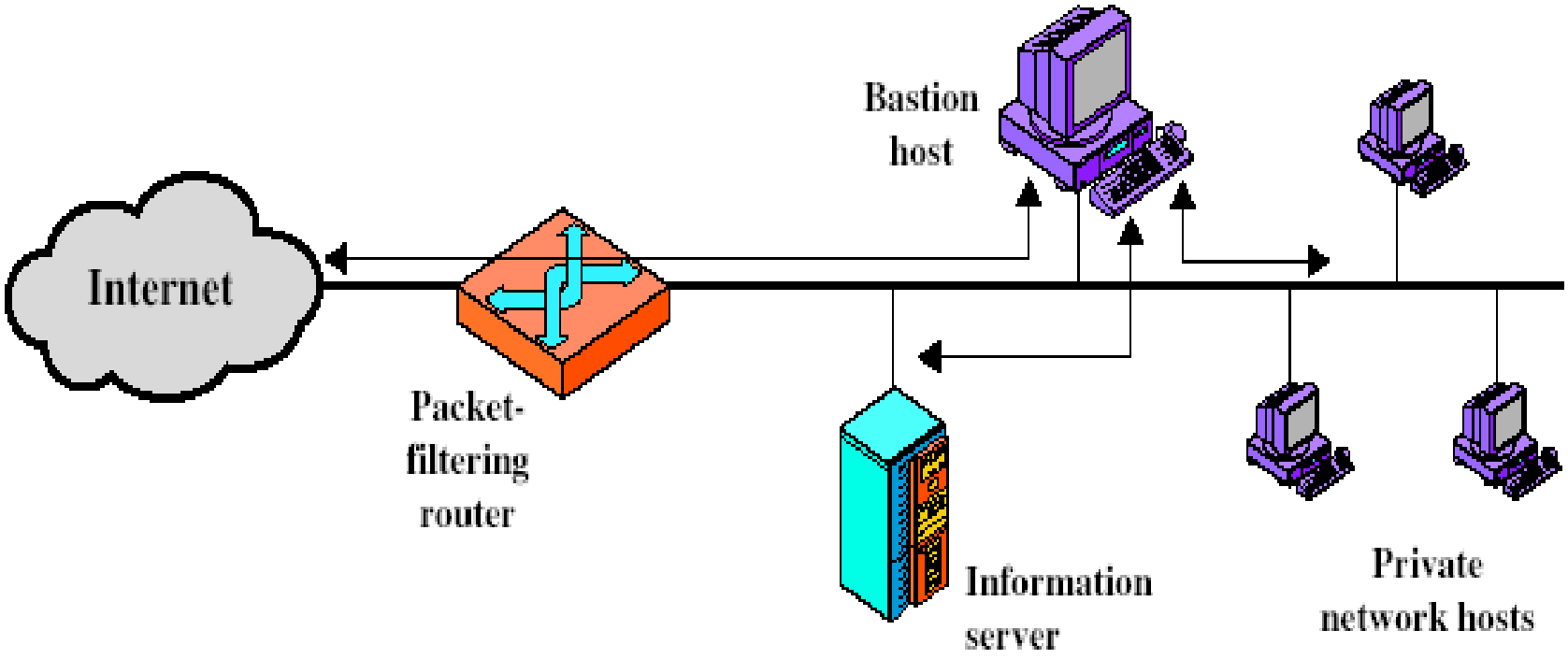
Firewalls - Circuit Level Gateway

- Relays two TCP connections
- Imposes security by limiting which such connections are allowed
- Once created usually relays traffic without examining contents
- Typically used when trust internal users by allowing general outbound connections
- SOCKS commonly used for this

Bastion Host

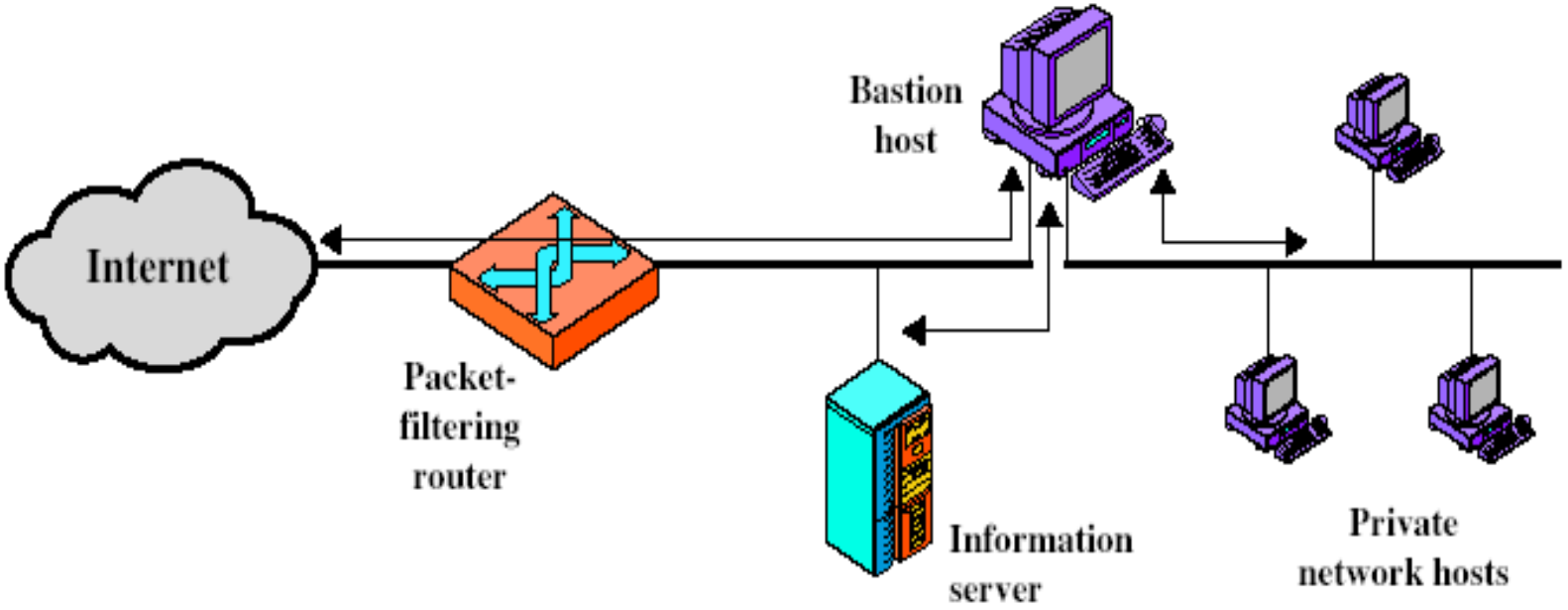
- Highly secure host system
- Potentially exposed to "hostile" elements
- Hence is secured to withstand this
- May support 2 or more net connections
- May be trusted to enforce trusted separation between network connections
- Runs circuit / application level gateways or provides externally accessible services

Firewall Configurations



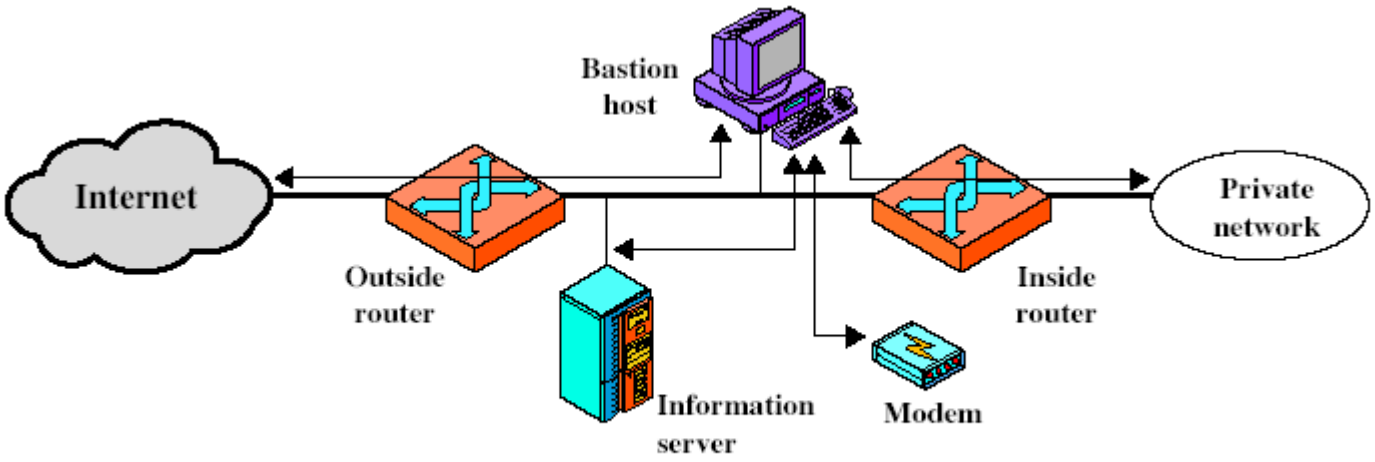
(a) Screened host firewall system (single-homed bastion host)

Firewall Configurations

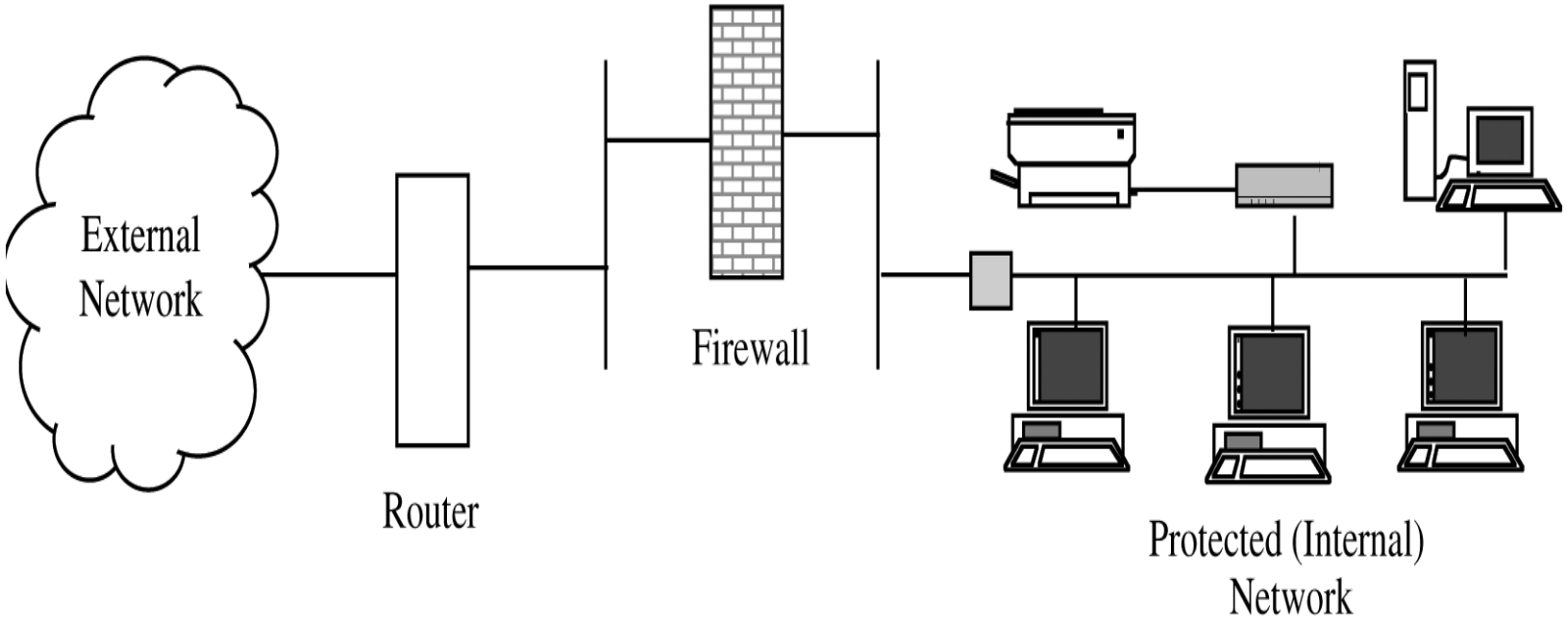


(b) Screened host firewall system (dual-homed bastion host)

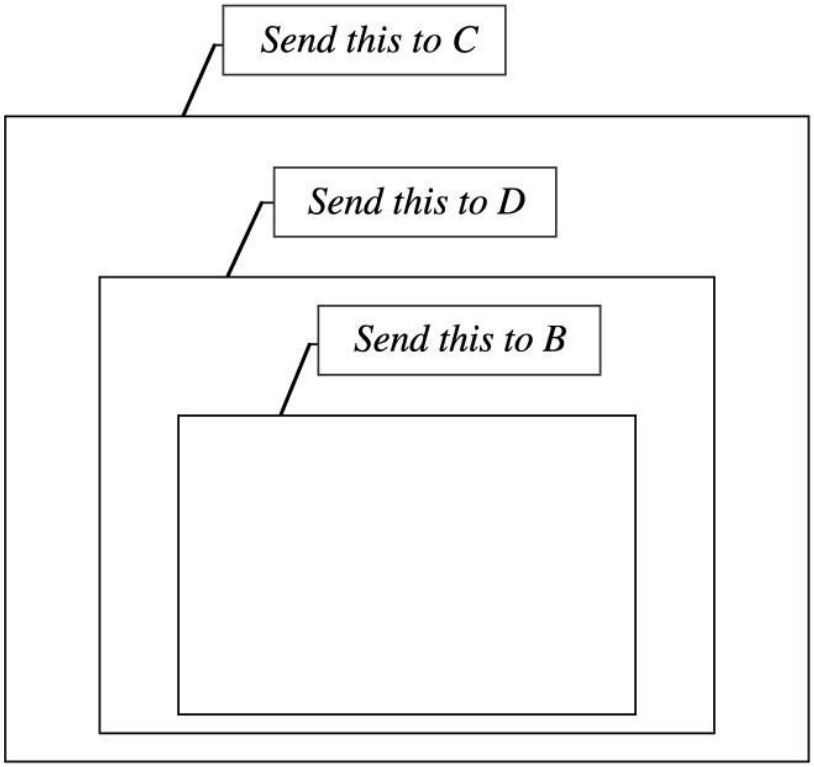
Firewall Configurations



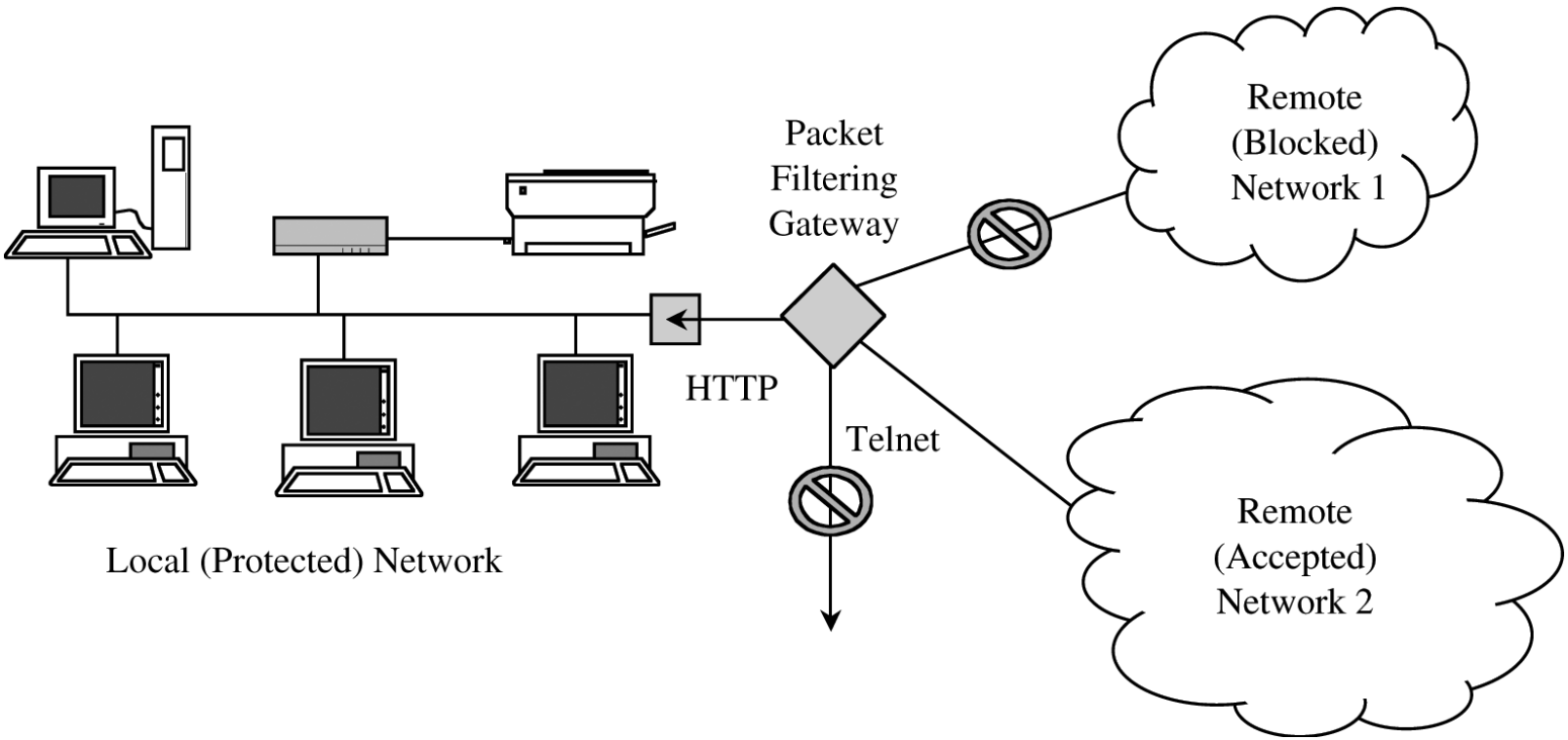
(c) Screened-subnet firewall system



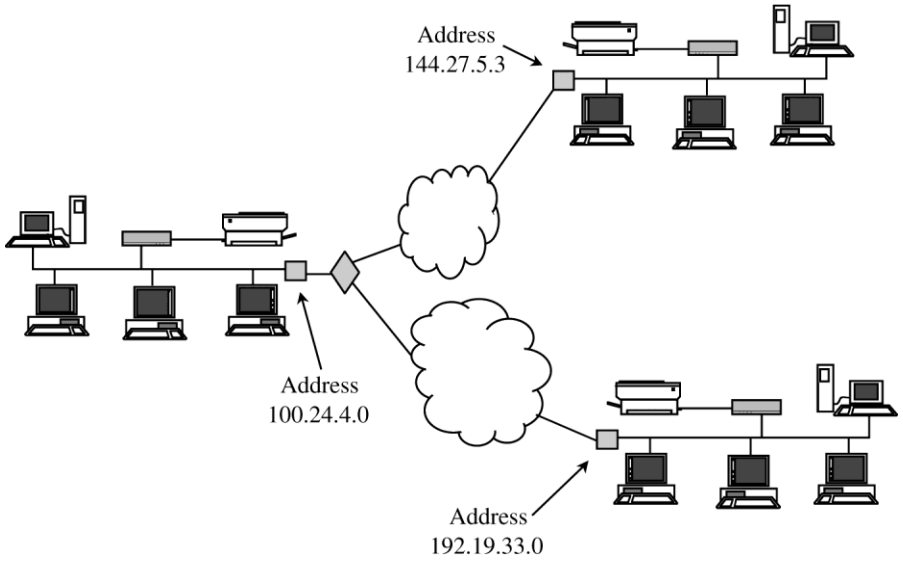
Layered Network Protection.



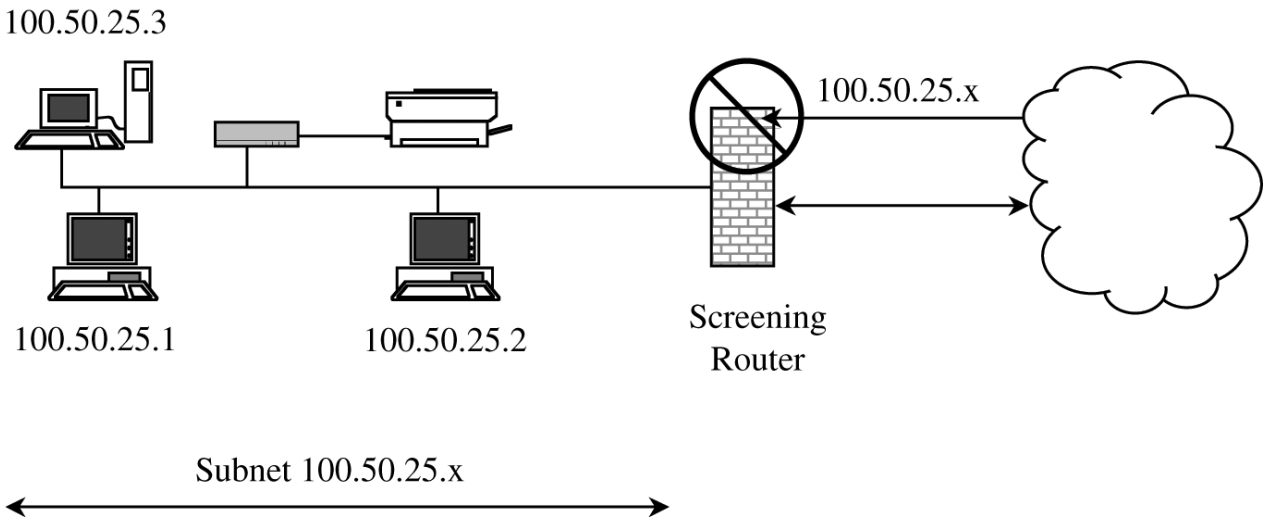
Onion Routing.



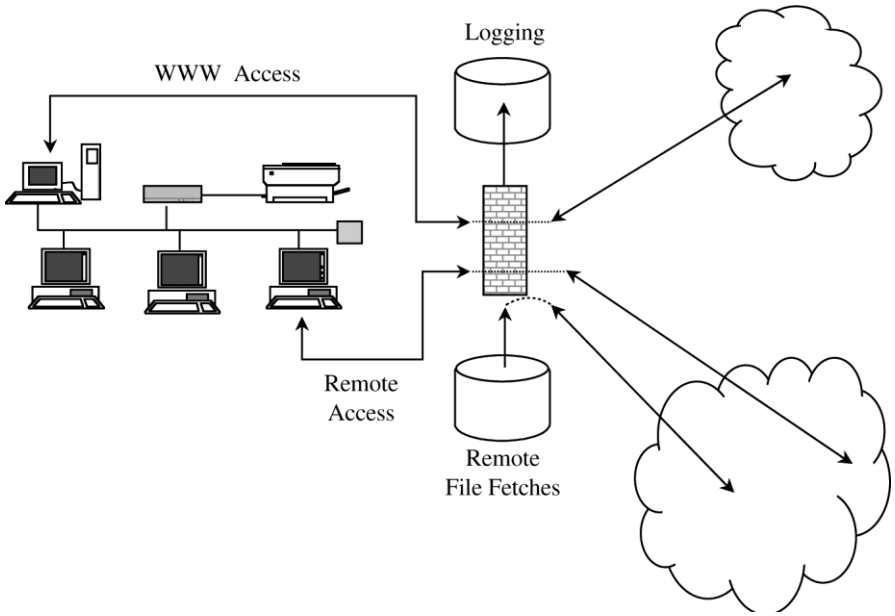
Packet Filter Blocking Addresses and Protocols.



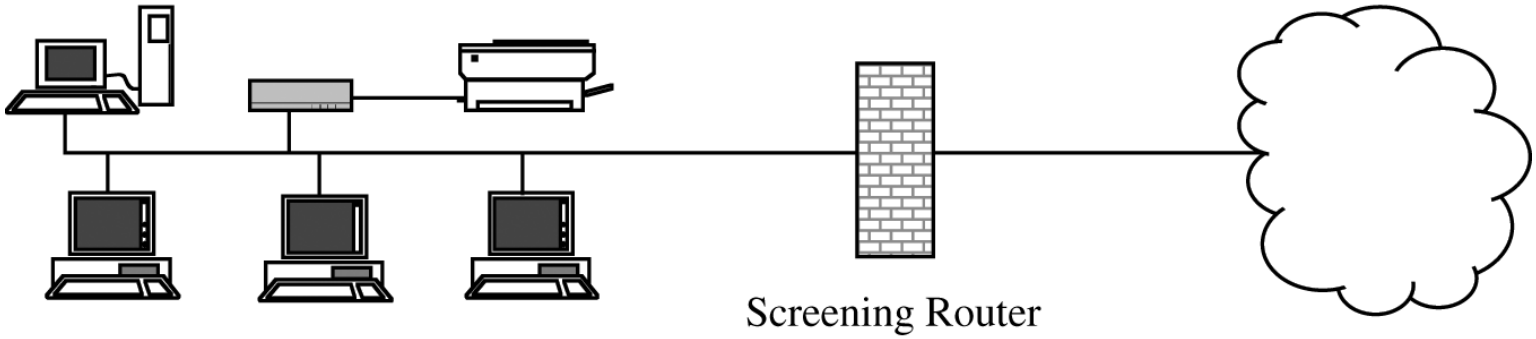
Three Connected LANs.



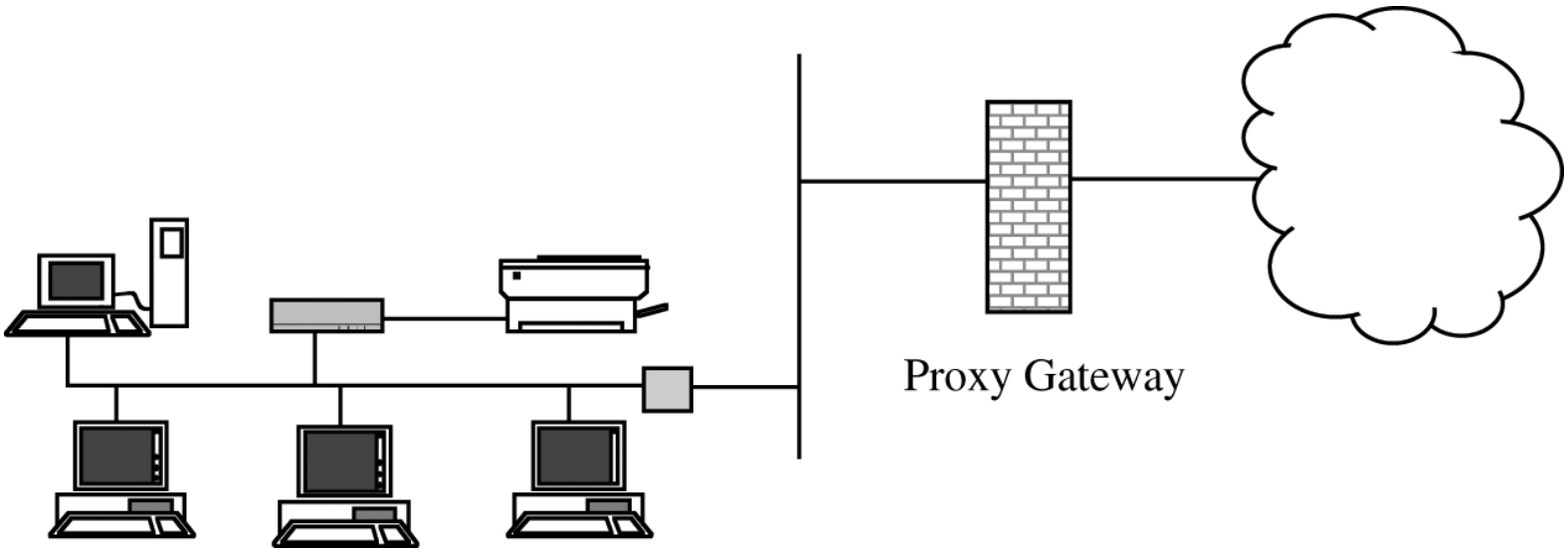
Filter Screening Outside Addresses.



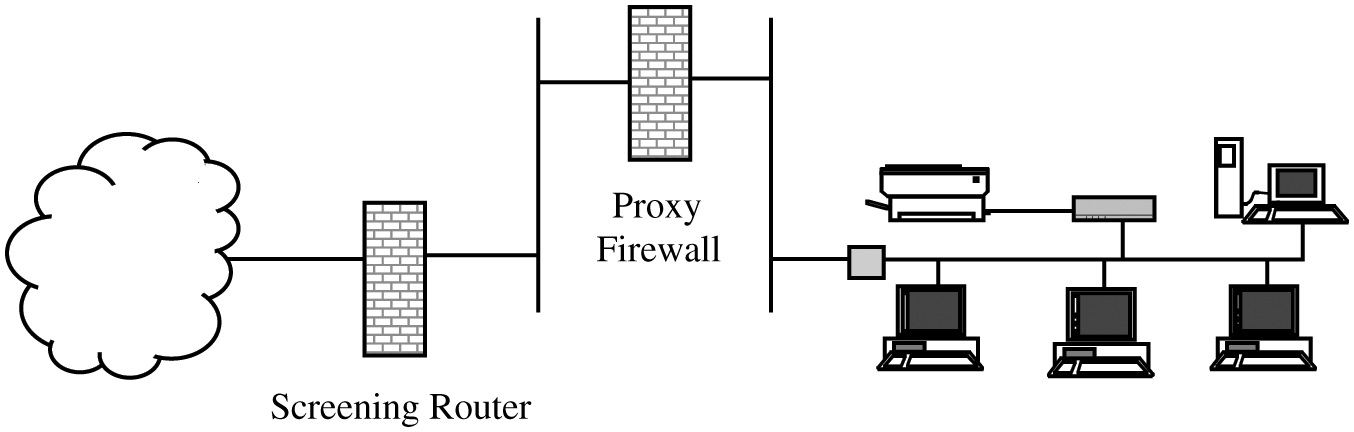
Actions of Firewall Proxies.



Firewall with Screening Router.



Firewall on Separate LAN.



Firewall with Proxy and Screening Router.