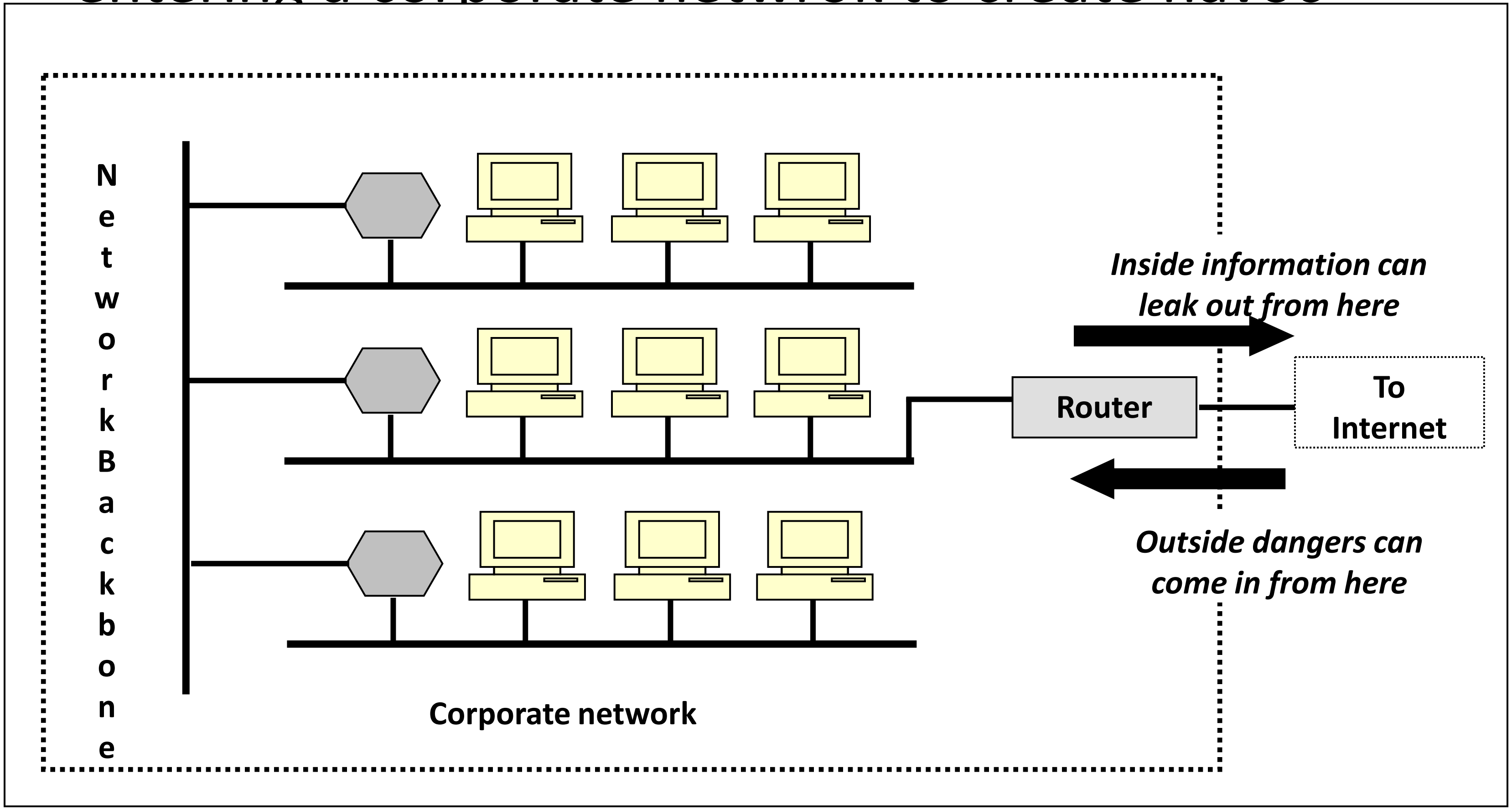
4	**Electronic Mail Security, Web Security, Intrusion, Firewalls, Biometric security**	**15**
	Electronic Mail Security: Pretty Good Privacy, S/MIME, DomainKeys Identified Mail.	3
	IP Security: Overview, Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations, Key Management	3
	Web Security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, HTTPS standard , Secure Socket Shell	3
	Intrusion: Intruders, Intrusion Techniques, Intrusion Detection, Firewalls: Firewall Design Principles, Types of Firewalls	2
	Security in Online transactions	2

Attacks

- Leaking of Valuable and confidential data in the corporate networks
- great danger of outside elements (worms/viruses) entering a corporate netwrok to create havoc


NetworkBackbone
Inside information can leak out from here
Router
To Internet
Outside dangers can come in from here
Corporate network

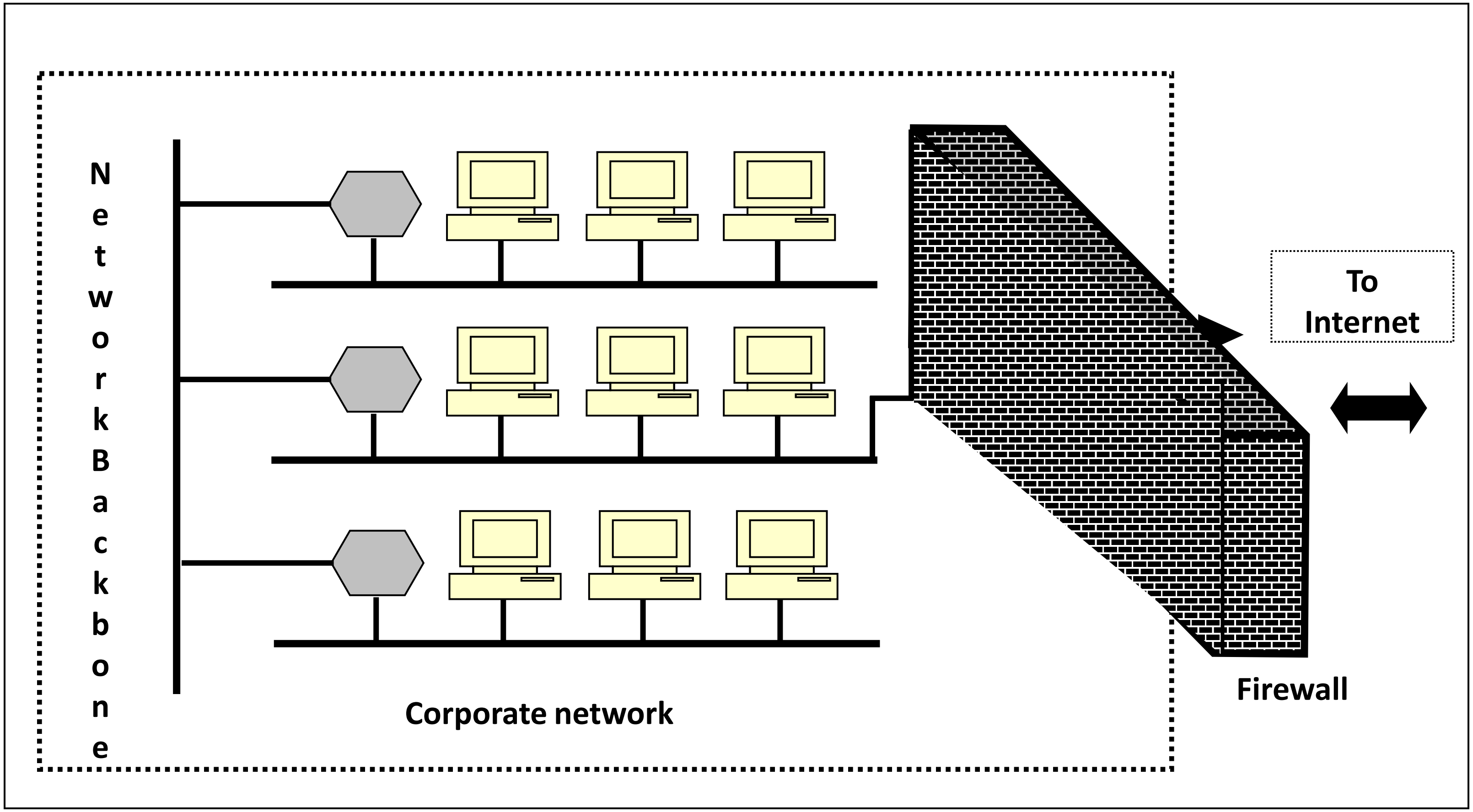
Network Threats

- Mechanisms required to ensure that the inside information remains inside and also prevents the outsider attackers from entering inside a corporate network
- Encryption does not work when outsiders break inside a corporate network
- Better schemes are desired to achieve protection form outsider attacks
- Firewalls

Firewall

- Guards a corporate network by standing between the network and the outside world
- Special type of router
- Controls transmission between internal and external networks
- Decides what to allow/disallow

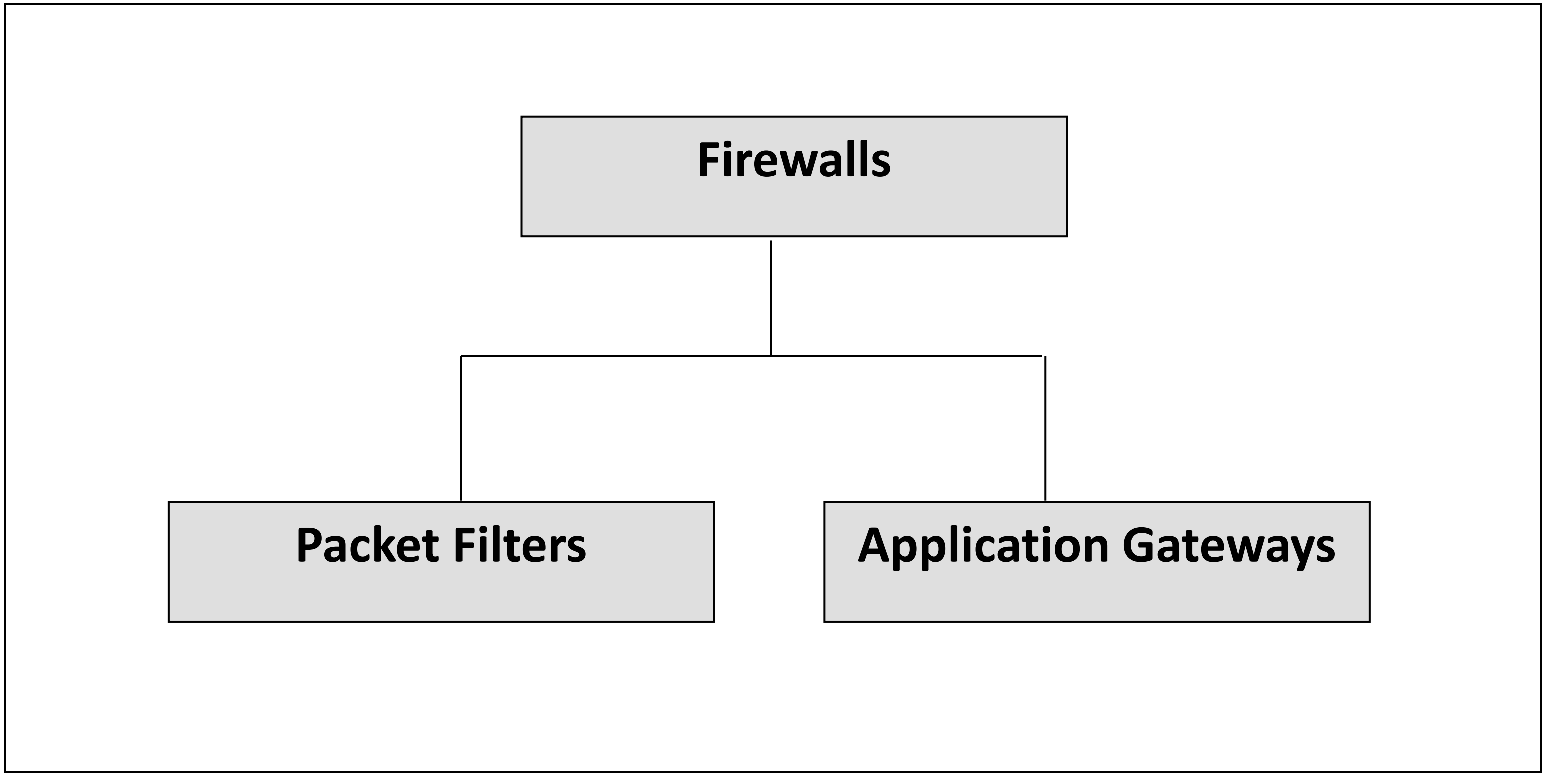
Firewall Concept



Characteristics

- All traffic fro inside to outside and vice versa must pass through the firewall
  - All access to the local network must first be physically blocked and access only via the firewall should be permitted
- Only the traffic authorized as per the local security policy should be allowed to pass through
- The firewall itself must be strong enough so as to render attacks on it useless

Firewall Types



Firewalls

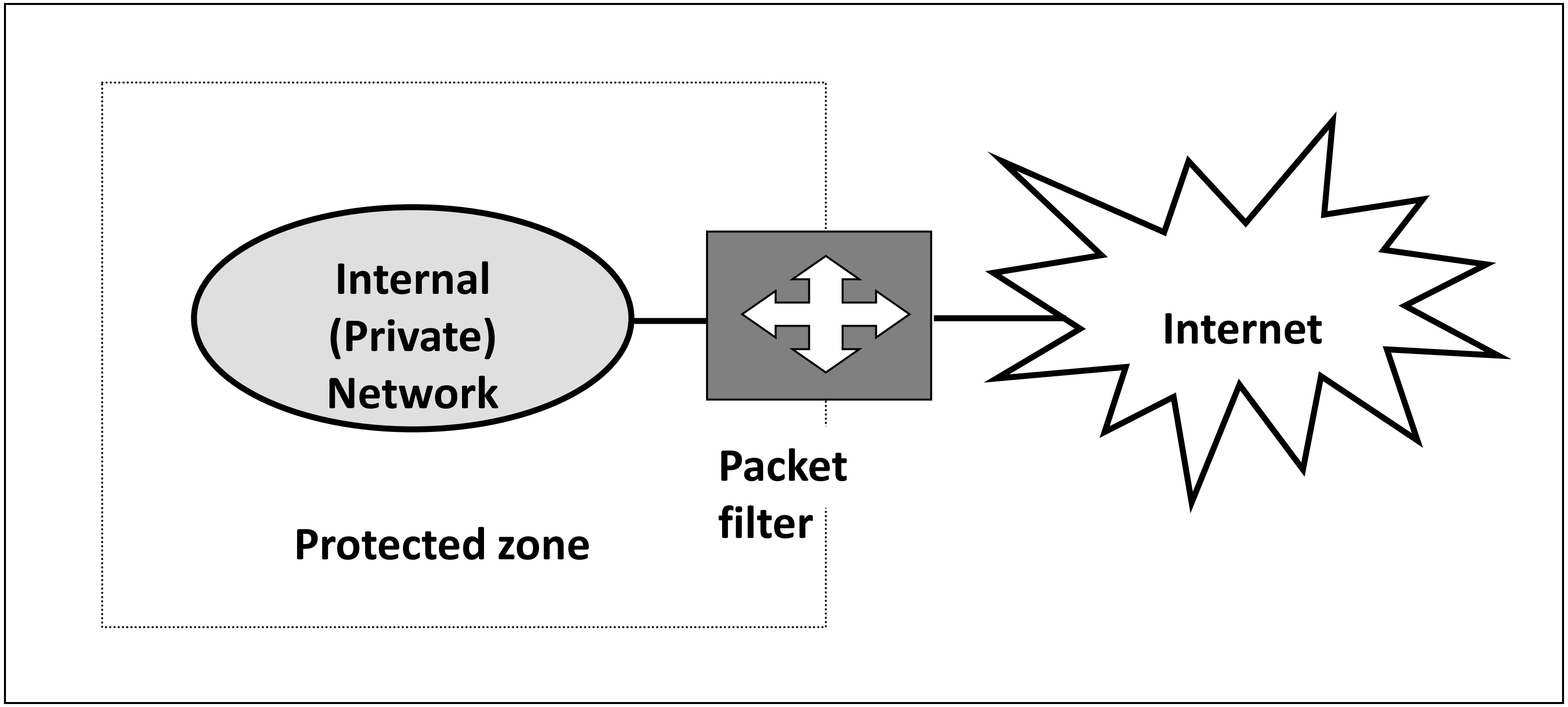
Packet Filters

Application Gateways

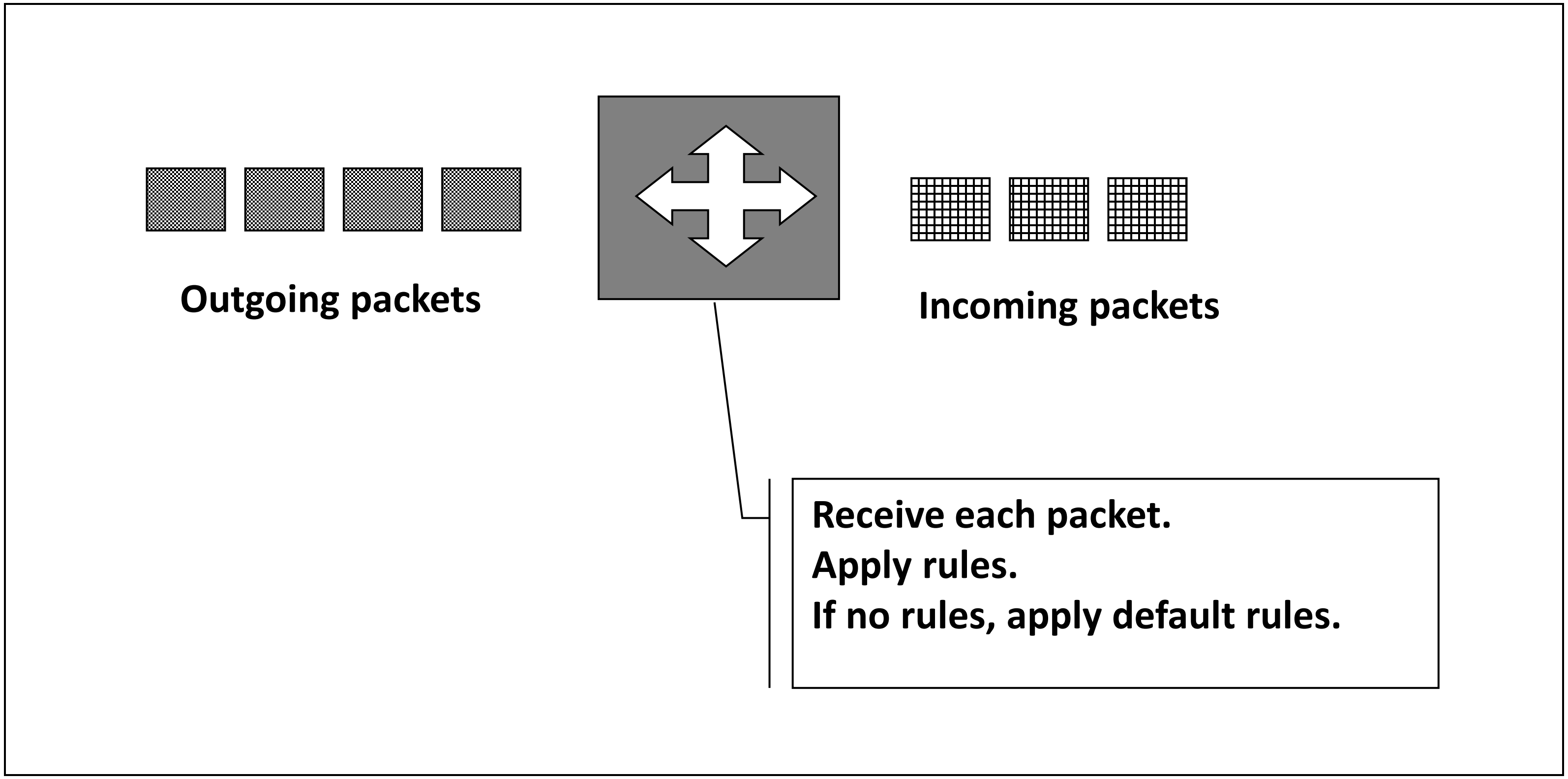
Packet Filters

- Applies a set of rules to each packet and based on the outcome decides to either forward or discard the packet.
- Called the screening router or screening filter
- Implemented using a router
- Configured to filter packets going in either direction
- Filtering rules are based
  - IP/TCP headers
  - Source and destination IP addresses
  - Port numbers

Packet Filter



Packet Filter Operation



Outgoing packets

Incoming packets

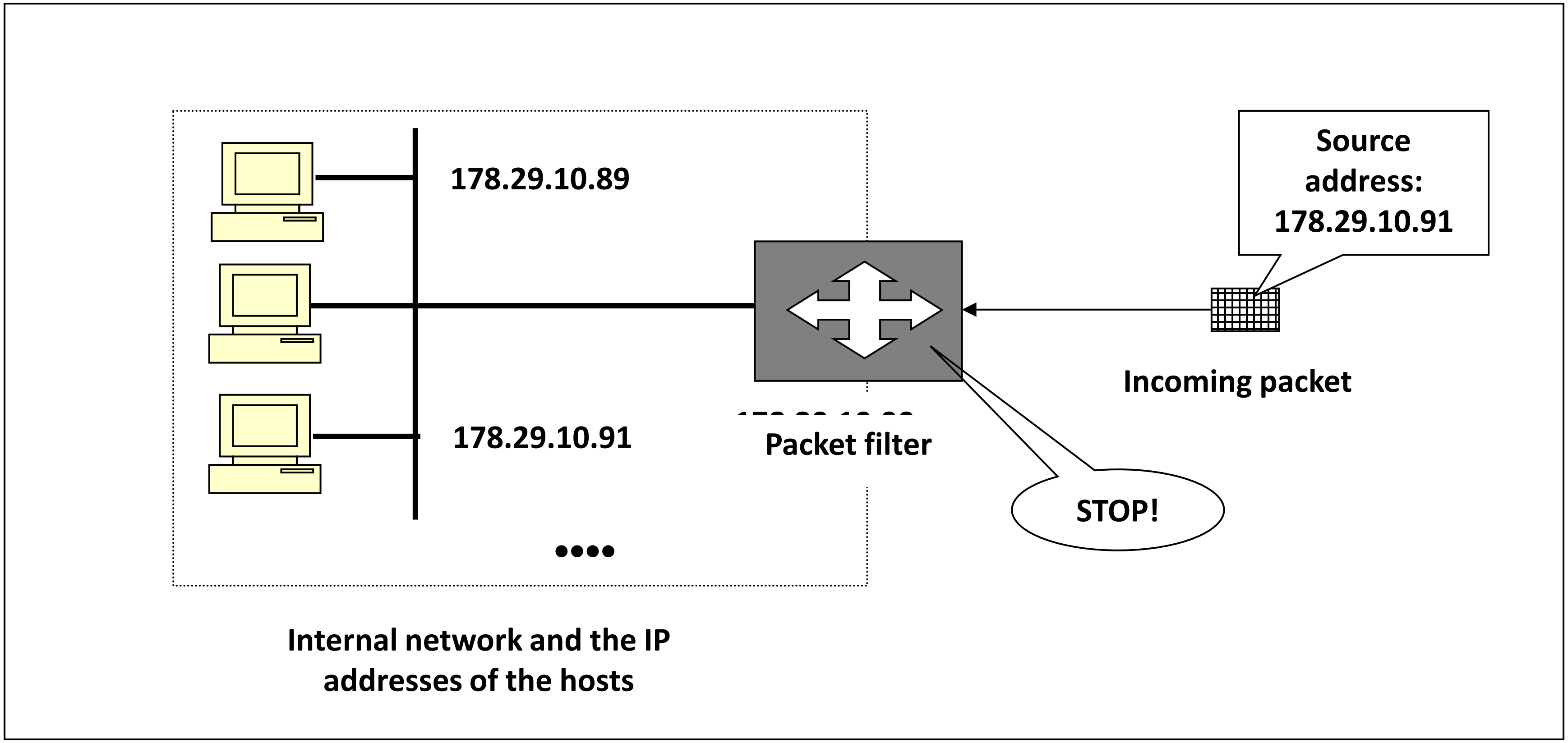
Receive each packet.
Apply rules.
If no rules, apply default rules.

Functions

- Receive each packet as it arrives
- Pass the packet through a set of rules
- Decides whether to accept or discard the packet of the packet.
- If no match with any of the rules take the default action
- Discard all the packets or accept all the packets
- Advantage
  - Simplicity
  - User need not be aware of the packet filter
- Disadvantages
  - Difficulty in setting of the rules
  - Lack of support for authentication

Attacks

- IP address Spoofing
  - Intruder outside the corporate network can attempt to send a packet towards the internal corporate network with the source IP address set to one of the IP addresses of the internal users


178.29.10.89
178.29.10.91
••••
Packet filter
Source address: 178.29.10.91
Incoming packet
STOP!
Internal network and the IP addresses of the hosts

Attacks(Contd)

- Source routing attacks
  - Attacker can specify the route that a packet should take as it moves along the Internet
  - Attacker hopes that by specifying this options, the packet filter can be fooled bypass its normal checks
  - Discarding all the packets can thwart such an attack

Attacks(Contd)

- Fragment attacks
  - IP packets pass through a variety of networks
  - All have a predefined maximum frame size(MTU)
  - this requires fragmentation
  - Attacker attempts to use this characteristic
  - Intentionally creates fragments of the original IP packet and sends them
  - The attacker feels that the packet filter can be fooled, if it only checks the first fragment and does not check the remaining ones
  - Attack can be foiled by discarding all the packets where the upper layer protocol type is TCP and the packet is fragmented

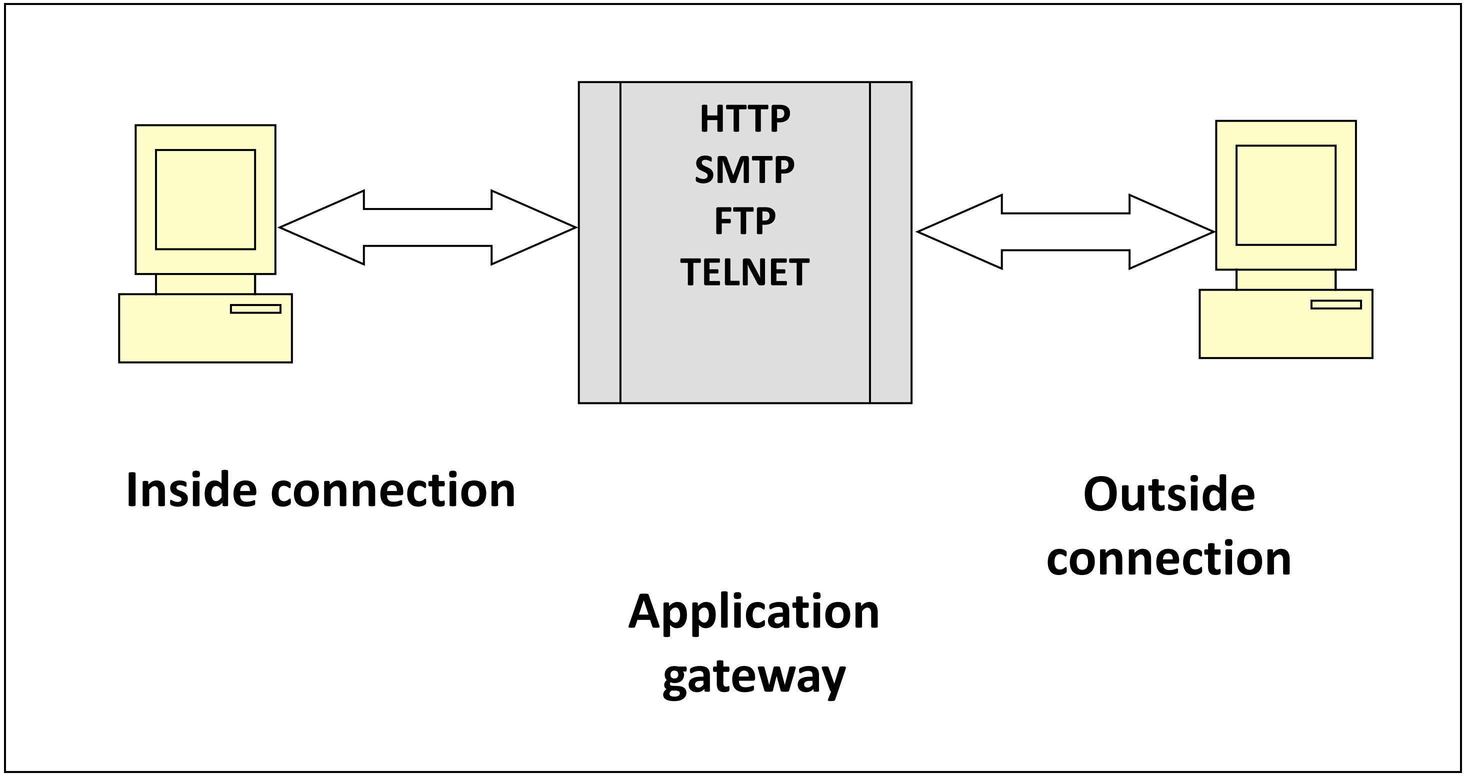
Advancements

- Advanced type is the dynamic packet filter or the stateful packet filter
- Allows the examination of packets based on the current state of the network
- Adapts itself to the current exchange of information
- Can specify a rule as
  - Allow incoming packets only if they are responses to the outgoing TCP packets that have gone through our network
  - Requires to maintain a list of all currently open connections and outgoing packet in order to deal with this rule

Application Gateways

- Called a proxy server
- Acts like a proxy or substitute
- Decides about the flow of application level traffic
- Working
  - Internal user contacts the application gateway using a TCP/P application(HTTP/TELNET)
  - Application gateway asks the user about the remote host which the user wants to set up a connection for actual communication
  - It also asks for the user id and password required to access the services of the application gateway
  - User provides this information to the application gateway

Application Gateway



HTTP
SMTP
FTP
TELNET

Inside connection

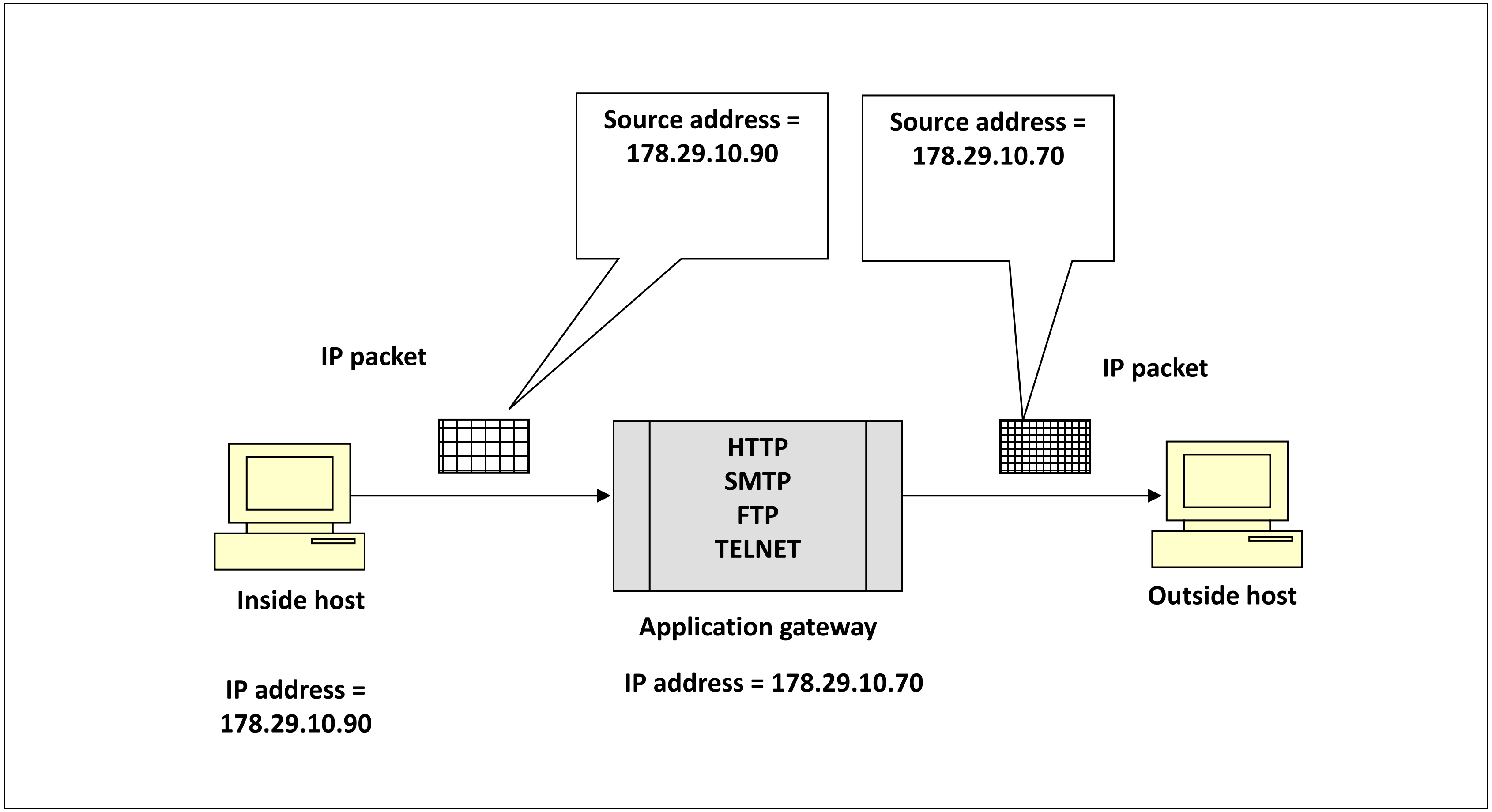
Outside connection

Application gateway

- AG now access the remote host on behalf of the user and passes the packets of the user to the remote host
- Circuit gate way
    - Performs some additional functions as compared to AG
    - Creates a new connection between itself and the remote host
    - User is not aware of this and thinks that there is a direct connection between itself the remote host
    - CG changes the source IP address in the packets form the end user's IP address to its own
    - IP addresses of the computers of the internal users are hidden form the outside worlds

– From here onwards the application gateway acts like a proxy of the actual end user and delivers packets from the user to the remote host and vice versa

Circuit Gateway

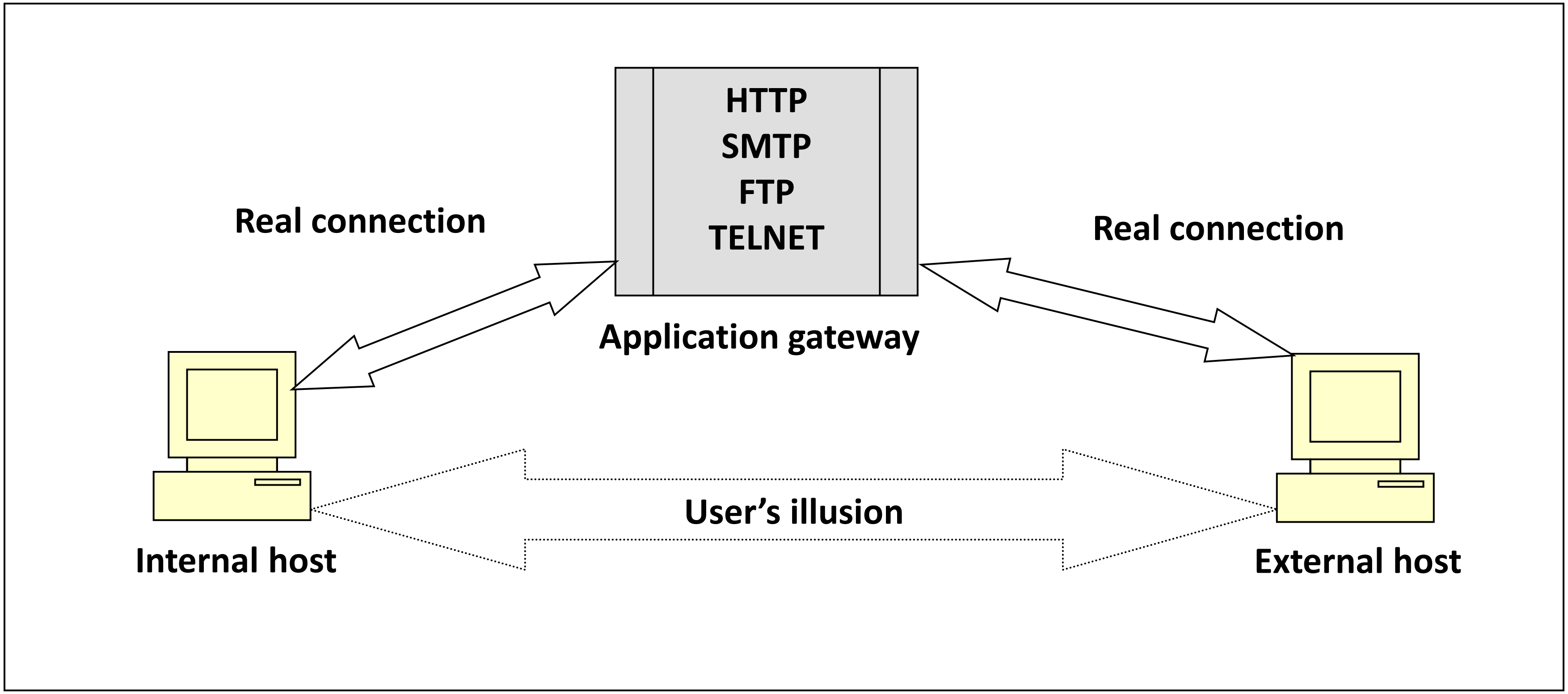


Source address = 178.29.10.90
Source address = 178.29.10.70
IP packet
IP packet
HTTP
SMTP
FTP
TELNET
Inside host
Outside host
Application gateway
IP address = 178.29.10.90
IP address = 178.29.10.70

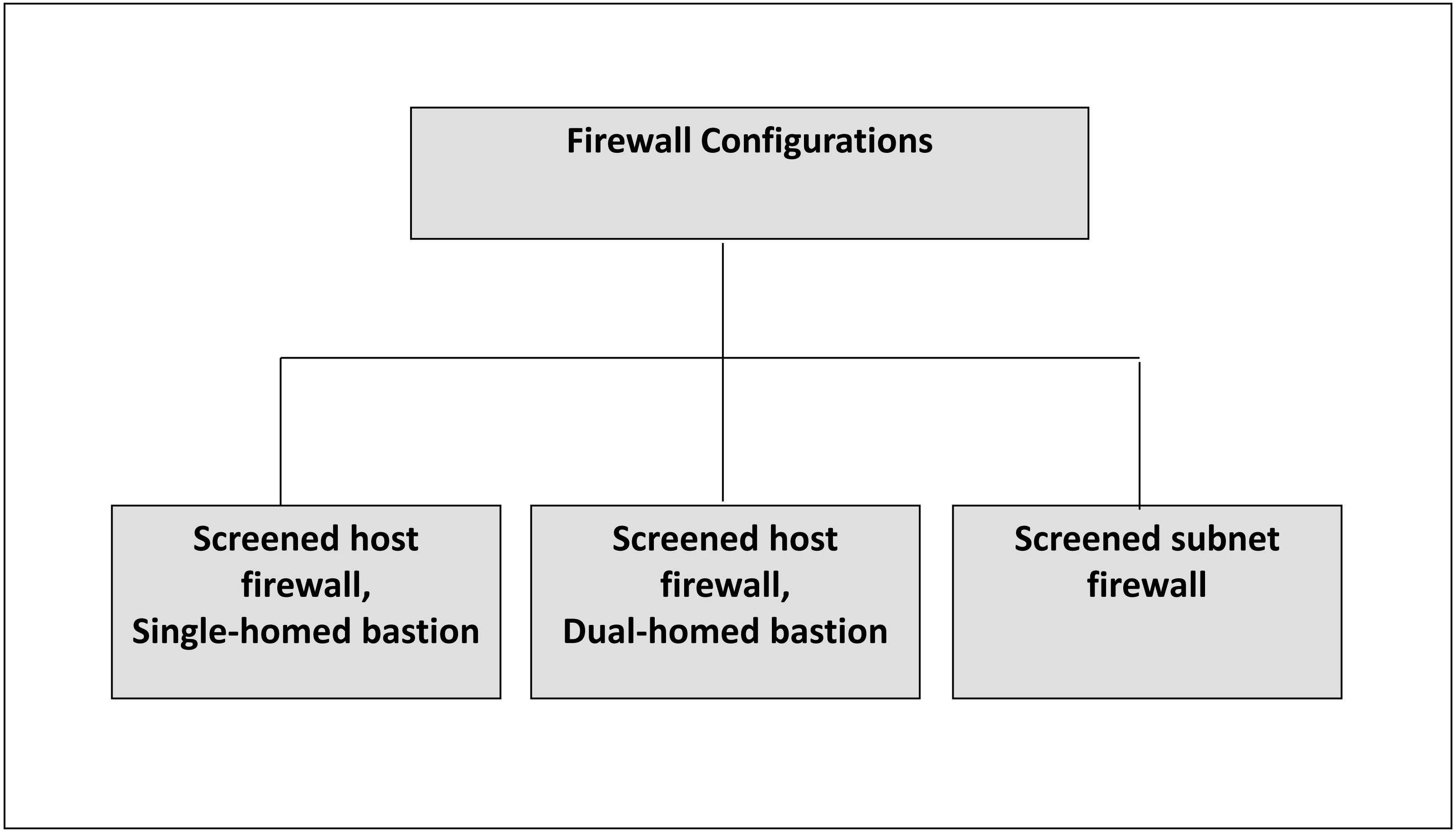
Advantages

- AG ‘s are more secure than packets filters
- Rather than examining every packet against a number of rules we simply detect whether a user is allowed to work with TCP/IP application or not
- Disadvantage
  - Overhead in terms of connections
  - There are actually two sets of connections
    - Between the end user and the application gateway
    - Between AG and the remote host
    - AG has to manage these two sets of connection and the traffic goin between then
  - AG is also called bastion host
  - Is a key point in the security of the network

Application Gateway - Illusion



Firewall Configurations



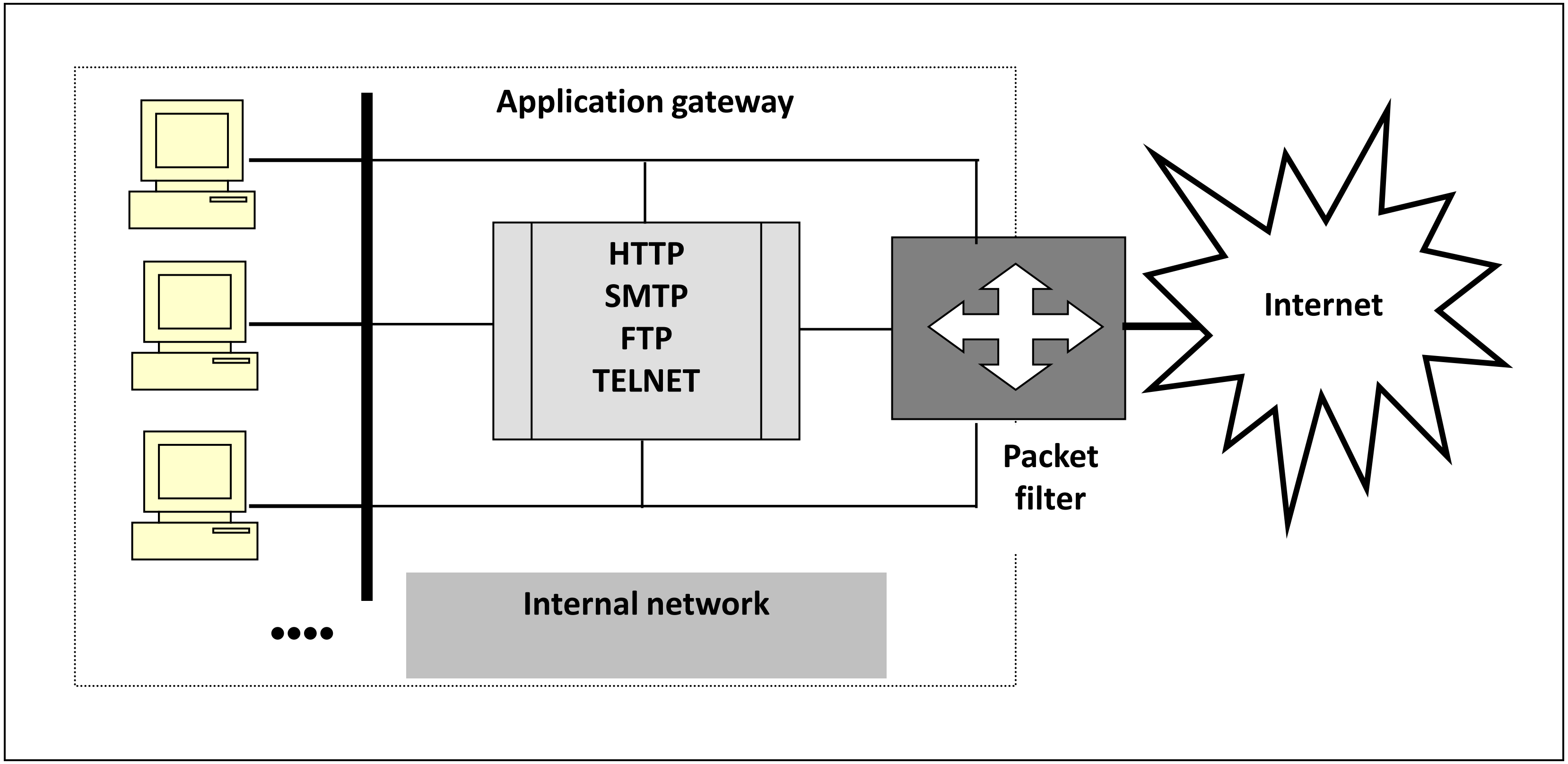
Firewall Configurations

Screened host firewall, Single-homed bastion

Screened host firewall, Dual-homed bastion

Screened subnet firewall

Screened Host Firewall, Single-homed Bastion

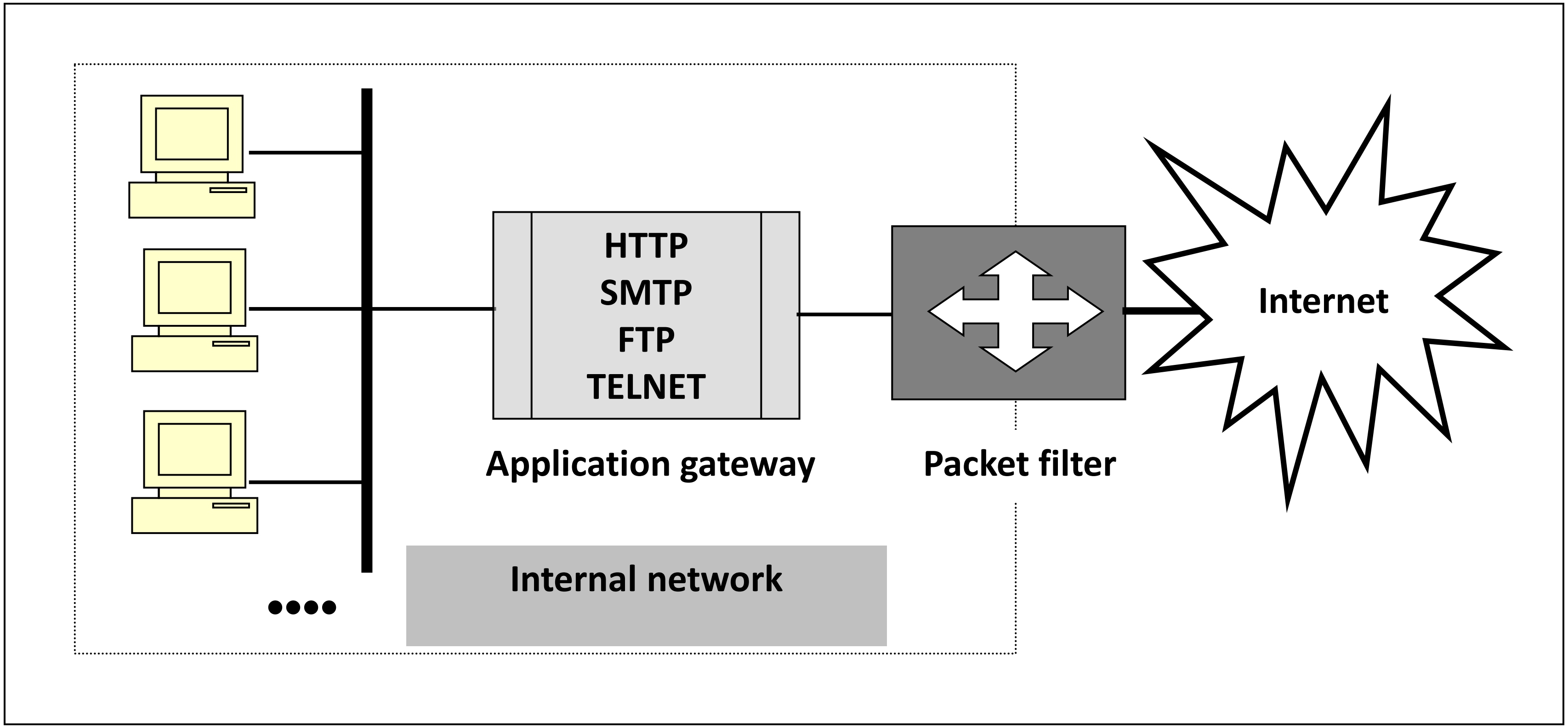


Screened Host Firewall, Single-homed Bastion

- Firewall is set up consists of two parts
  - a packet filtering router and an application gateway
- Purposes
  - Packet filter assures that the incoming traffic is allowed only if it is destined for the application gateway
  - Examines the destination address field of every incoming IP packet
  - It also ensures that the outgoing traffic is allowed only if it is originating from the application gateway by examining the source address field of every outgoing IP packet

- Configuration increases the security of the network by performing checks at both packet and application levels
- Giver more flexibility to network administrators to define more granular security policies
- Disadvantage
  - Internal users are connected to the application gateway and the packet filter
  - Is the packet filter is attacked then the whole internal network is exposed to the attacker

Screened Host Firewall, Dual-homed Bastion



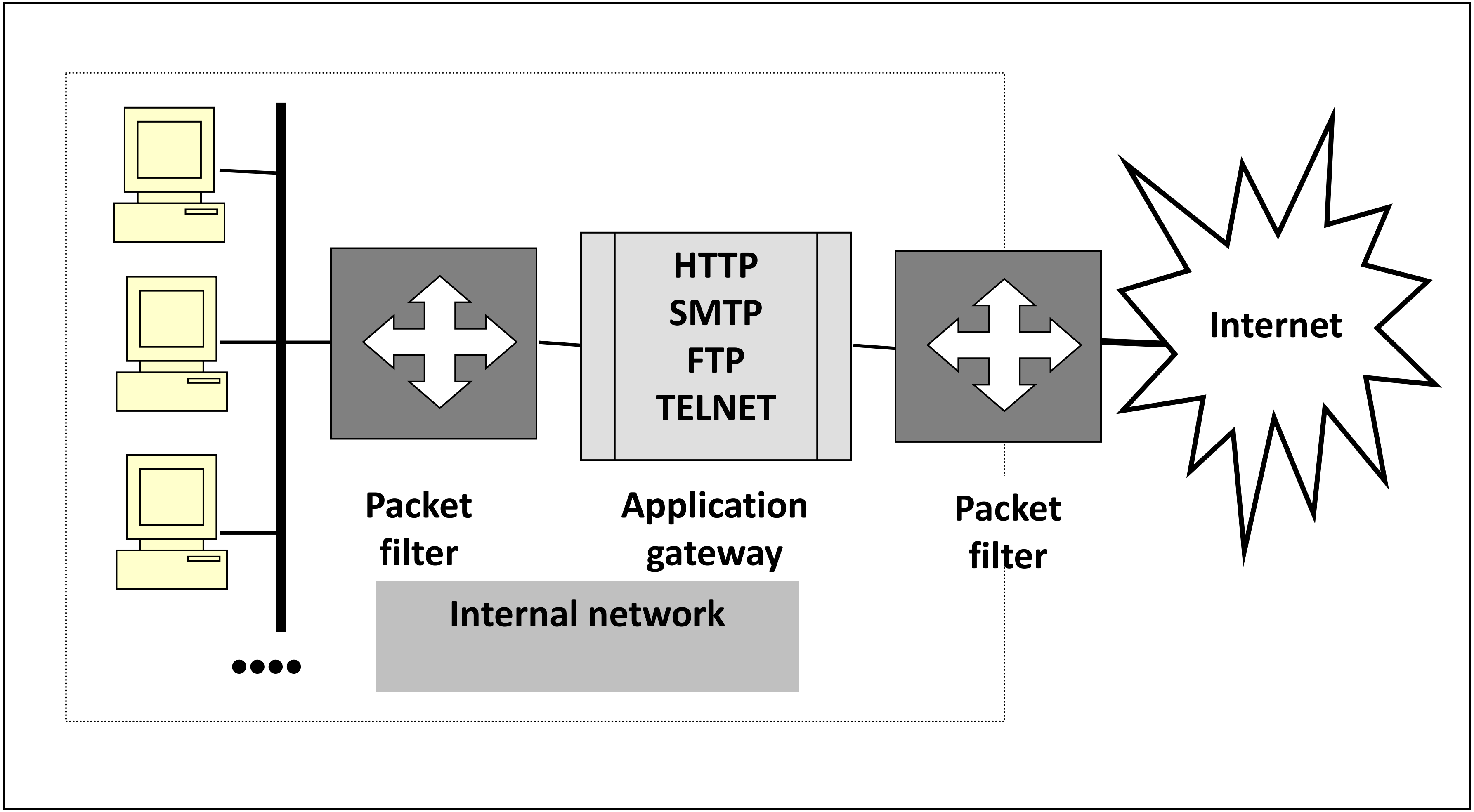
Screened Host Firewall, Dual-homed Bastion

- Configuration is an improvement over the earlier scheme
- Direct connections between the internal hosts and the packet filter are avoided
- The packet filter connects only to the application gateway, which in turn has a separate connection with the internal hosts
- Even if the packet filter is successfully attacked only the application gateway is visible to the attacker
- Internal hosts are protected

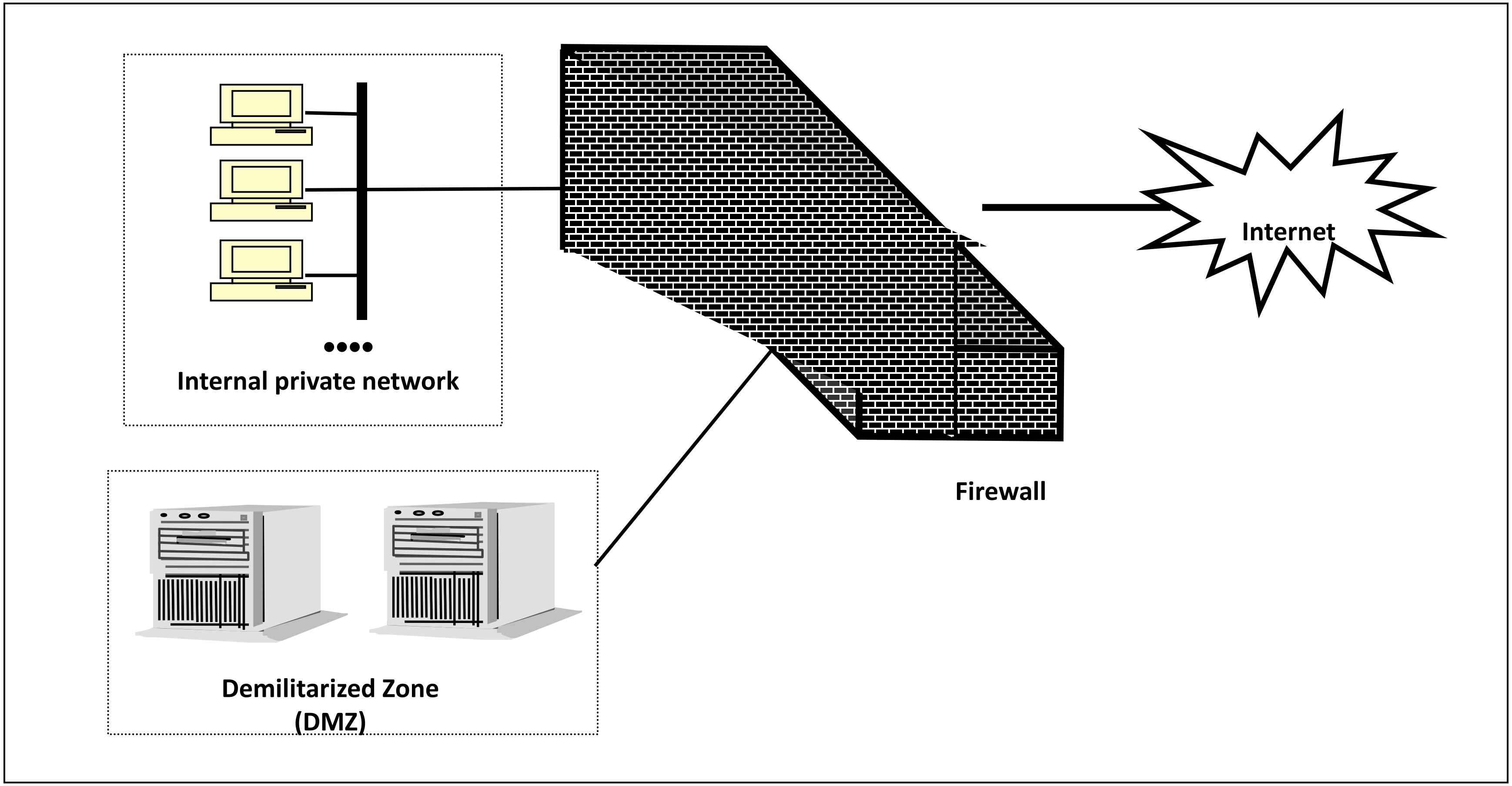
Screened Subnet Firewall

- Offers highest security
- Improvement over the previous scheme of
- Two packet filters are used
  - One between internet and the application gateway,
  - Other between the application gateway and the internal network
- Three levels of security

Screened Subnet Firewall



Demilitarized Zone (DMZ)



Demilitarized Zone (DMZ)

- Popular in firewall architecture
- Firewalls are arranged to form a DMZ
- DMZ required only if an organization has servers that it needs to make available to the outside world
- There are at least three network interfaces
  - One connects to the internal private network
  - Second connects to the external public network (Internet)
  - Third connects to the public servers (forms the DMZ)

Advantage

- The access to any service on the DMZ can be restricted
- We can limit the traffic in/out of the DMZ network to the HTTP and HTTPS protocols
- All other traffic can be filtered
- Internal private network is no way directly connected to the DMZ
- Even f the attacker can somehow manage to hack into the DMZ the internal private network is sfe and out of the reach of the attacker