Malicious Software

Dr.Gladston Raj S

- Malicious software is often called as malware or malicious code
- It is a software purposely designed to damage the computer system or the data stored in that system.
- Computer viruses, worms, Trojans, spyware are main type of malicious software
- These programs are specially written to spy the traffic flow through the network.
- It is used to record the communication between two parties, execute some unauthorised commands and steal and distribute the information which is private and confidential

- The common type of malware are virus, worms, Trojans, bots, back doors, spyware and adware
- The damage caused by these malwares are not the same
- There may be a damage like causing minor irritation, destroying data from storage devices, capturing confidential data and compromising the system and networks.
- It can’t damage hardware, software and network installed on the computer system

Types of Malware

1. Virus
   - The software which intend to damage the computer system is called virus
   - The damage may be in terms of deletion, modification or corruption of software
   - Previously virus spread through physical devices such as floppy disk, memory stick etc
   - But, nowadays, due to the increase of the use of Internet, spread of virus is faster and it causes more damage as compared to past.
   - Virus have the ability to replicate themselves and thus, spread rapidly

Types of viruses

- Viruses can be classified according to their origin, technique used, damage caused, platforms they used for attack and the types of files they mainly select for damage

1. Parasitic virus
   - This virus is propagated by attach itself to particular program or a file.
   - It is also known as executable.
   - It generally resides at the start or at the end of the file called prepending virus or appending virus respectively
   - The files with extension .com and .exe are easiest to infect because these types of files are directly loaded into their memory and their execution always starts at the first instruction
   - Ex: Jerusalem-slows down the system and deletes the program that the user tries to execute

2. Boot Sector Virus

- This virus spreads when the infected floppy disk or pen drives are used to boot the computers.
- This affects the boot sector of the hard disk
- Ex: Polyboot, Disk killer, Michelangelo and stone virus.

3.Polymorphic Virus

- This type of virus changes itself with each infection and it creates multiple copies.
- This makes it difficult for antivirus software to detect it.
- Ex:- Involuntary, Stimulate, Elkern, Cascade, Phoenix, Marburg, Evil, Satan Bug Proud, Virus 101,Tuareg

4. Memory resident virus

- This virus installs code in the computer memory
- It gets activated when the operating system runs and it damage all the files opened at that time
- Ex:- Randex, CMJ, Meve

5. Stealth Virus

- This type virus hides its path after it infects the computer system
- After infection, the virus modifies itself so it is difficult for the antivirus software to identify it
- It masks the size of the infected file
- Ex:-frodo, Joshi, Whale

6. Macro virus

- This type of virus infects the files that are created using some applications which contain macros
- This virus activated the .docs or .xls files are opened by the user and then infect the normal templates
- This virus attached with the documents; so, it spreads with the infected documents only.
- Ex:- DMV, Melissa, Relax, Nuclear, Word Concept
- Some viruses are activated on a specific date and at specific time.
- This type of virus is called time bomb

- Some are activated by a certain sequence of events and for some specific number of times, it can produce its replicates or the infected program runs automatically for some specific number of times
- This type of virus is called logic bomb

7.Hybrids

- Many times, features of different types of viruses are combined to form a more dangerous virus, called hybrid virus
- Ex: Happy99- it causes email attack
- This virus is sent with the email attachment

8. Email viruses

- This virus is sent with the attachment
- When the attachment is downloaded, immediately the virus program runs and infects the files stored on the computer
- These viruses use the address book of the email holder and send the messages to all the email addresses.
- Ex:-Melissa and Klex
- To protect email virus
  - Use licensed antivirus software
  - Don’t open email attachments directly
  - Use a document viewer
  - Enable virus protection

Working of Antivirus software

- Antivirus is a program which is used to scan files and identify and eliminate the viruses and other malicious software such as Trojan horses or worms
- The antivirus software uses different approaches to detect the viruses.
- Two major approaches are signature or pattern-based approach and behaviour-based approach

1.Signature or pattern based approach

- In this approach, the dictionary has a database containing signature or pattern of viruses
- Then the information from the file is checked with the signature or pattern from the dictionary.
- If there is a match found; then the antivirus program can either delete the file or quarantine it so that the other programs cannot access it.
- This helps in stopping the spread of viruses to other files
- Here database should be updated periodically

2. Behaviour based approach

- The drawback of the first method is that new viruses can’t be detected, as the signature or pattern is not available in the database of the dictionary
- Here, It doesn’t use any database of the known viruses.
- The detection of viruses depends on the suspicious behaviour of the computer programs.
- It monitors the behaviour of all programs

- If some program, tries to modify an executable program, then this behaviour is treated as suspicious and it sends an alert to the user
- So that, new attack can be identified, which is not possible using first approach
- The drawback of this approach is that it creates large number of false positives.
- This limits the use of this approach for the design of antivirus software.

Other approaches

- Here, for each new executable program that is being executed, the antivirus software initially tries to emulate the beginning of the code.
- This is done before transferring control to the executable program.
- If it is observed that the program is using self-modifying code or otherwise appears as a virus, then it means that the executable program has been infected with a virus
- The drawback is that false positive rate is large

- Another approach is a sandbox method
- The sandbox emulates the OS and executable runs on this simulation.
- Then, the sandbox is analysed for any changes.
- Then, the conclusion is made about the virus
- The drawback is poor performance
- So, generally, it is used for on demand scans

Prevention

- Install and update antivirus regularly
- Update internet browsers periodically
- Don’t open or download the email attachment sent by unknown person

Detection

- Run the antivirus software to scan the computer system everyday

Eradication

- Use real time antivirus software
- When the virus is detected, the alarm is given and the warning is displayed on the screen, so that the file can be repaired or can be deleted

WORMS

- A small piece of software different from a virus
- It can execute and spread itself, whereas virus needs host program for its execution and spread
- Some modern worms also hide inside a file
- It uses security loop holes within networks to reproduce itself.
- It is self-replicating and it does not make any change in the files or documents.
- It resides in active memory and replicates itself
- It scans the network for another computer, which has security loop hole.
- It copies itself to the new computer system and then replicates itself.
- It expands quickly, affects performance and shut down the computer

- In 1975 John Brunner first used the word ‘WORM’
- John Hupp first time implemented a worm in 1978 at Xerox PARC, to find put the idle Professor so that they can share the load and improve efficiency of the entire network
- The first worm in the worldwide network is Christmas tree, which spread across the IBM’s international network and BITNET

Types of WORMS

1. E-Mail worm:
   - This spread through infected e-mail attachments
   - Distributes itself by attaching to the fake e-mail messages
   - The link to an infected web site is sent in any form of attachment or link in an e-mail
   - When it opens, it activates
   - Can prevent by not opening such attachment

2. Instant messaging worm

- Spread via instant messages
- It spreads by sending links to the infected web sites to each user on the local address list
- These worms infect a user’s account and find out the addresses from the contact list and try to send themselves to all the users in the address list

3. Internet worms

- Spread through network connections
- It scans all the resources using operating system services as well as scans for vulnerable computer systems
- Then, it tries to access these computer systems

4. Internet Relay Chats (IRC) worm

- Spreads via IRC channels.
- It transfers infected files or links to the infected sites

5. File Sharing network worm

- File sharing networks worm places a copy of itself in a shared folder
- It spreads through P2P network

6. Payloads

- It is a code which is designed to do some more such as delete or encrypt files or send the files through e-mail, rather than only spreading the worm
- A very common payload is to install a backdoor in the computer
- This infected computer is then under the control of the attacker
- The network of such computer is Botnet
- They send junk mails, overload router, attack printer, kill other worms

Protecting against worms

- Use the update and license copy of operating system and other softwares
- Do not open the emails sent by unknown sources
- Avoid opening the attachments or using links from unknown sources
- Use license copy of antivirus and firewall

Symptoms of worm

- The performance of the computer becomes slow.
- Computer crash occurs
- Programs automatically open and execute
- Performance of browser comes down
- Some files may be modified and missing
- Shows errors in operating system
- Unknown desktop icons appear
- Emails may be sent automatically

Trojans/Trojan Horses

- It is a program that conceals its purpose
- It claims to do one thing but perform another
- It appears as email attachments
- Using this attacker gets control of the system
- It executes when some specific events occur
- It hides inside some application program and performs some harmful function

Features

- It doesn’t replicate or spread
- It spreads through downloading either an infected file from internet or payload of some other virus
- It is used to steal information from the infected computer system and also download other malicious codes to a computer system

Manual removal

1. Locate the infected file; when a DLL error occur, there is a possibility of Trojan
2. Stop system restore function
3. Restart computer in safe mode
4. Go to control panel and remove the infected file
5. Delete all the files from system folder

Alternative method

- Go in the folder options and display all the hidden folders
- Restart the computer system in the safe mode
- Stop all the processes associated with Trojan

SPYWARE

- Without the knowledge of the owner, it is installed
- It is used to gather the secret and private information
- It changes the configuration
- System performance is affected
- When the user installs some free software from the internet, spyware is installed

BOTS

- Derived from the word **robot**
- It is an automated process which interacts with other network services
- It collects information with instant messaging, IRC chats.
- They can log keystrokes, analyse packets, collect passwords etc
- More versatile

Firewall

- It prevents unauthorised access to and from the network.
- It is an effective tool used to protect the network from the attackers
- It also allows the internal users to access outside network via Internet and WAN
- These are of 2 types- software and hardware or combinations of both.
- Firewall observes each and every packet coming inside and going outside the intranet and allows only authorised packets

- Messages can be protected by encrypting and password
- Firewalls are generally installed between the network and the internet.
- It blocks unauthorised traffic
- It forwards the incoming traffic to more reliable internal computer systems
- It hides the internals of computers and networks, like names of computer system, network topology used, types of network device etc
- It provides strong user authentication
- It can serve as a platform for IPSec

Firewall characteristics

- Must act as gateway for all traffic between two networks
- It allows to pass only authorised traffic that is permitted by local security policy
- The firewall itself is protected from any type of penetration
- It can’t give assurance about protection from attacks coming from outside network
- Risk analysis helps in defining the level of protection for firewall implementation
- Firewall implements different local security policy

- Firewall
  - Defines what type of protection is to be expected from the firewall
  - Specifies the cases when the exceptions are considered
  - Defines the rule for determining authorised and unauthorised traffic
- Firewalls works on simple rules given below
  - All traffic is denied except that which is specifically authorised
  - All traffic is allowed except that which is specifically denied
- Firewall use four techniques to control access and enforce the security policies

1. **Service Control:**
    - The access to any specific types of internet services is controlled by this techniques.
    - It filters the traffic on the basis of port number, protocol or IP address
2. **Direction Control:**
    - It decides from where the particular service requests should be initiated.
    - It decides whether to allow the request to flow through the firewall or not.
3. **User control :**
    - Depending on the user access, it controls the access to a service
4. **Behavioural control :**
    - It control the behaviour of a particular service

Types of firewall

- Firewalls are categorised into three types– packet filtering firewall, application level gateway and circuit level gateways

1. **Packet filtering firewall**
   - It works on the rule and allows the IP packets for incoming and outgoing
   - Using this rule, the packets are forwarded or discarded
   - This firewall works at OSI layers 3 and 4.
   - It is generally designed to filter packets going in both the directions
   - It tracks the source address and destination address of the packets and TCP/UDP port numbers
   - The contents of a packet is not analysed by this firewall

ts of a
itecture of packet filtering

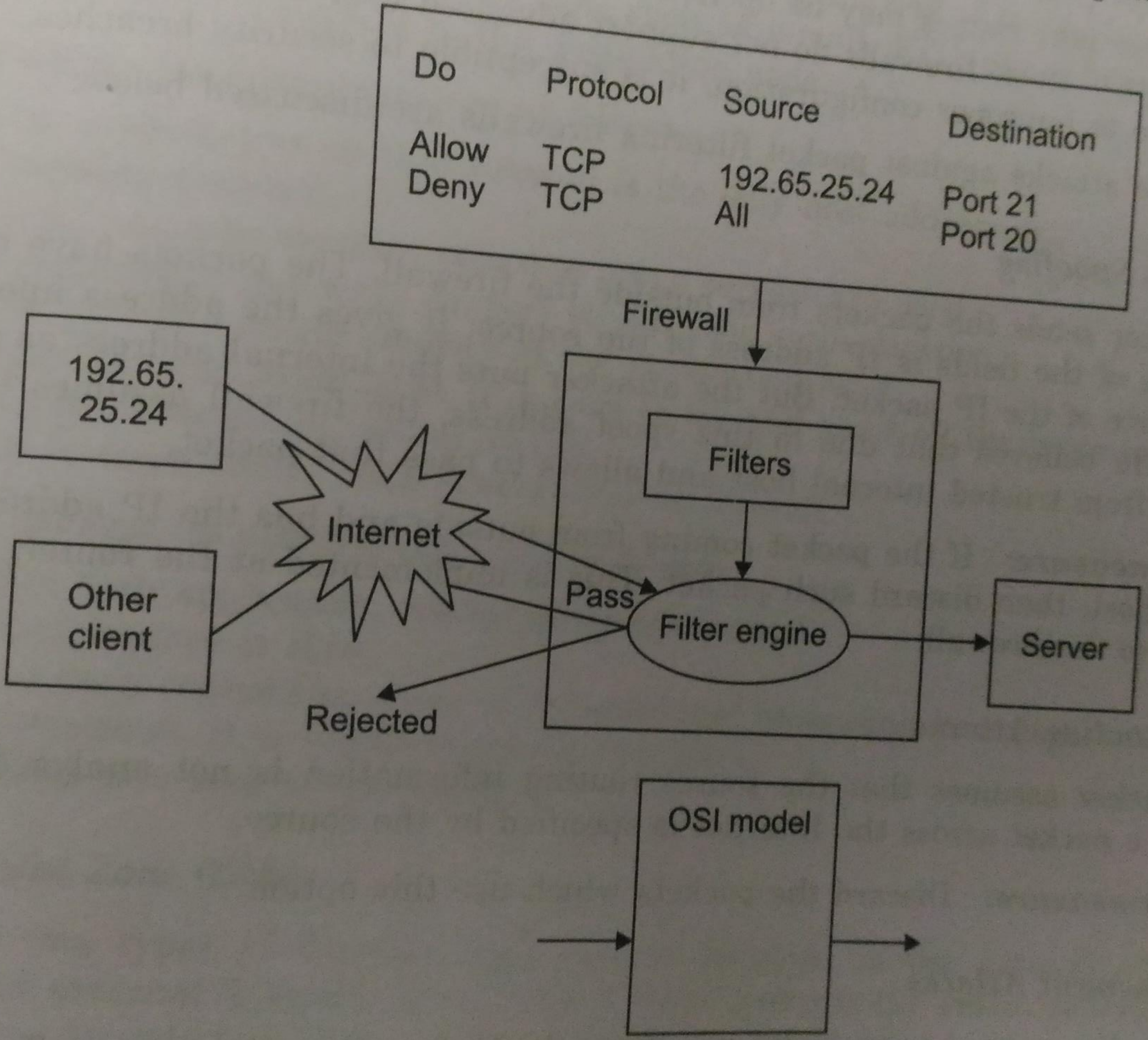


Figure 16.1 Packet filters.

- There are various strategies for implementing packet filters.
- These are based on the information contained in a network packet.
- Some of them are as follows
  - Source IP address
  - Destination IP address
  - Source and destination port number
  - IP protocol field
  - Interface

Advantages

- Performance is good
- It is very fast.
- Packet filters are relatively inexpensive
- It is transparent to users
- The traffic management is good
- simple

Disadvantages

- Direct connections are allowed between untrusted and trusted hosts
- It is vulnerable to spoofing attacks
- Has poor scalability
- Large port ranges may be opened
- Most of these firewalls don’t support advanced user authentication schemes
- Due to improper configuration, it is susceptible to security breaches

- Some of the attacks against packet filtering firewalls are

1. IP address spoofing:
   - The attacker sends the packets from outside the firewall and puts internal address as a source address
   - Firewall assumes that this packet is from trusted internal host and allows to pass that packet

   Countermeasure
   - If the packet coming from outside and has the IP address of internal host, then discard such packet.
   - This is implemented at the router, which is external to the firewall

2. Source routing attacks
   - The attacker assumes that the source routing information is not analysed
   - So, the route of a packet across the internet is specified by the source

   Countermeasure
   - Discard the packets which use this option

3. Tiny fragment attacks

- The attacker creates small fragments using IP fragmentation option
- Separate fragment is used for the TCP header information
- This design helps in avoiding the filtering rules based on TCP header information
- The filtering decision is taken from the first fragment of a packet and on the basic of this first fragment, subsequent fragments, of that packets are allowed or discarded.
- The attacker takes the advantage of this strategy that only the first fragment of the packet is examined for forwarding the complete packet

Countermeasure:

- The preventive measure for this attack is to enforce a rule that the first fragment must hold a predefined minimum amount of the transport header.
- The filter should remember the packet if the first fragment of the packet is rejected.
- Then, discard the remaining fragments of the packet

Application level gateways

- Packet filtering firewalls is based on address information, so it examines the lower layers of the OSI model
- To provide more security, all layers of the OSI model should be examined simultaneously.
- Application level gateway firewall is useful which provides this security
- It uses server-based programs, known as proxy server or bastion host.
- It forwards or rejects the packet by ensuring that the protocol specification is correct

- Proxy accept requests from the external side, examines the request, and then forward the legitimate and trusted requests to the destination host on the other side
- This type of firewall makes decisions at all the seven layers of the OSI model
- It acts as a mediator for different applications such as e-mail, FTP etc
- It doesn’t permit the client to directly connect to the destination node

Advantages

- It is configured so that firewall is the only host address that is visible to an outside network
- For separate services, separate proxy servers are used
- Applications gateways support strong user authentication
- It provides strong security at the application level
- At the application level, it is easy to log and audit all the incoming traffic
- It provides strong access control
- It is more secure than packet filtering firewall

Disadvantages

- For each application, special proxy is required
- Performance is slow
- On each connection, there is an additional processing overhead
- Sometimes, it is inconvenient for the users
- There is a lack of transparency

Demilitarised Zone (DMZ)

- There are two types of firewall based on its locations in the network– internal and external firewall
- An internal firewall protects the entire network of an organization
- An external firewall is installed at the boundary of local or organization network
- It is located inside the boundary router
- The region between the two firewalls is called demilitarized zone or DMZ

- External firewall provides basic security to the entire network
- The internal firewall has strong filter capabilities as compared to external firewall
- This provides strong security to the servers and workstations from the external attacks
- The internal firewall also provides two-way protection.

Benefits of firewall

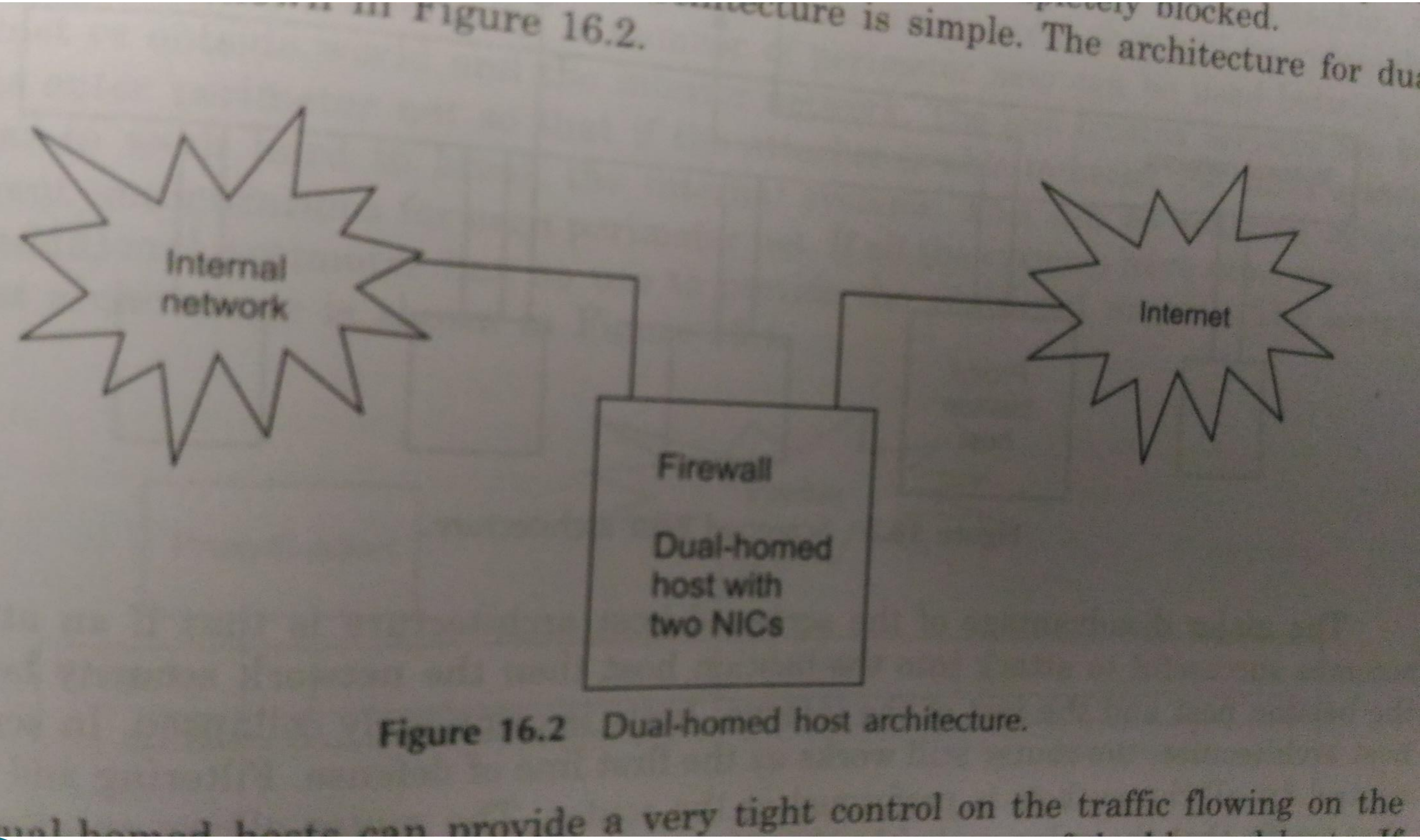
- Increased ability to enforce network security standards/policies
- Centralisation of internetwork audit capability

Limitations of firewall

- It can’t protect those attacks that bypass the firewall
- It can’t protect the network against the internal attacks
- An internal firewall that separates the different parts of a network can’t protect against wireless communications among local computer systems on different sides of the internal firewall
- Different devices such as laptop/portable storage devices may be used and infected outside the network and then used internally

Firewall architectures

1. Dual-homed host architecture
   - It is a computer system which has separate network interfaces for minimum two networks
   - This host computer can act as a router between the networks
   - This routing function should be disabled when it is used in firewall architectures
   - Therefore, the host computer isolates the network from each other, but it can see traffic on all the networks.



pletely blocked.

n in Figure 16.2. ecture is simple. The architecture for du

Internal network
Internet
Firewall
Dual-homed host with two NICs

Figure 16.2 Dual-homed host architecture.

ual homed hosts can provide a very tight control on the traffic flowing on the

- Dual homed hosts can provide a very tight control on the traffic flowing on the network.
- Not a single packet is allowed without the consent of dual-homed hosts
- If the rule is designed that does not allow the packets to flow between the internal and external network, then all the packets are blocked by the dual-homed hosts.
- It provides services by only proxying them.
- Proxying is much less challenging, but it may not be available for all services the users are interested in.

Screened Host Architectures

- Packet filter is used to provide the main security
- The required applications are provided by the bastion host that sits on the internal network
- The packet filtering rules are configured in such a way that the bastion host is the only host on the internal network that is accessible from the internet
- Even then only a certain types of connections are allowed
- If any external computer wants access to the internal computer or wants to use some services, it has to first connect to this host
- Bastion host is responsible to maintain a high level of security for the host

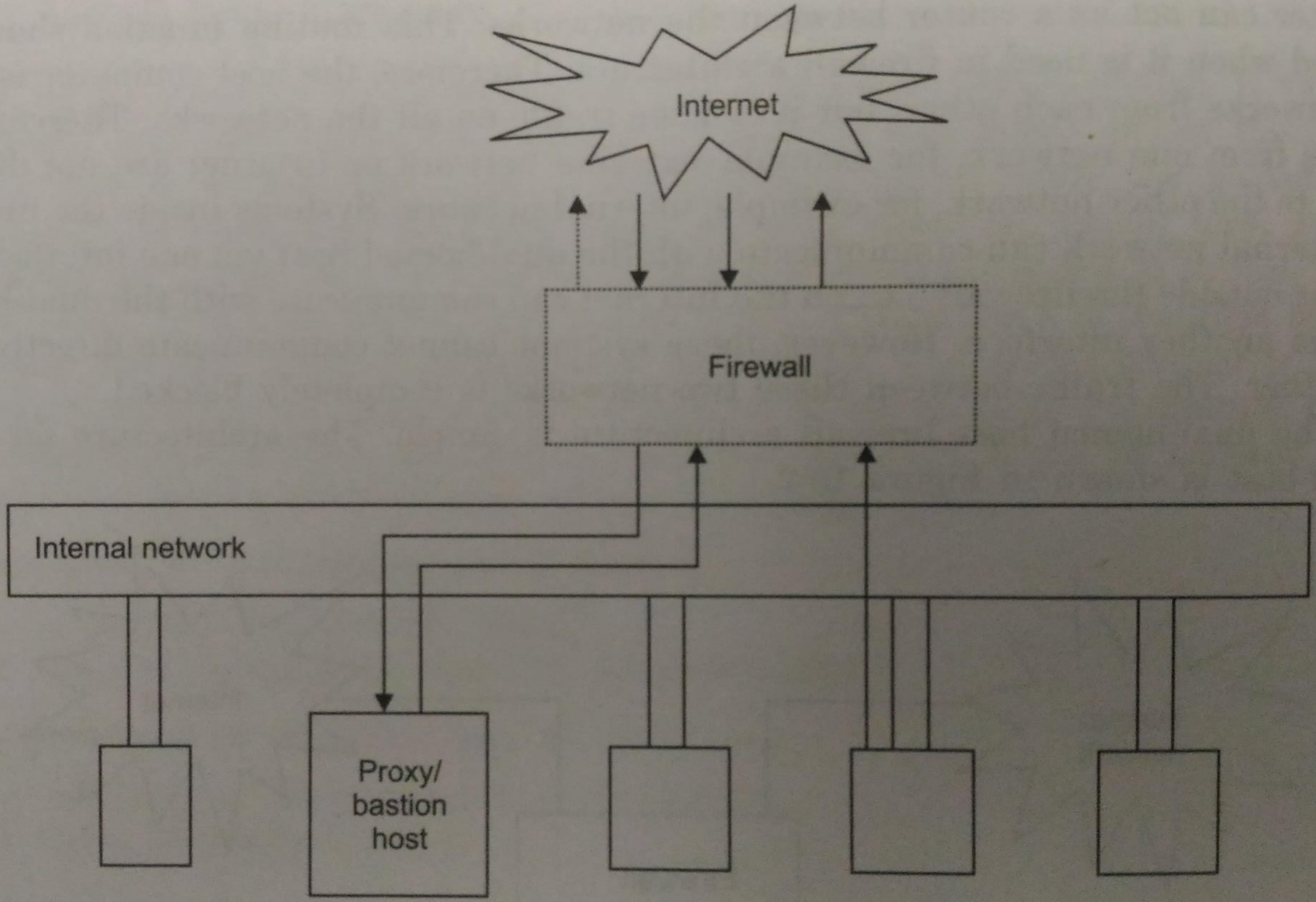


Figure 16.3 Screened host architecture.

- The major disadvantage of the screened host architecture is that if an attacker becomes successful to attack into the bastion host then the network security between the bastion host and the rest of the internal hosts is completely collapsed.
- Here, the router still works as the first line of defence
- Filtering and access control for all the packets is performed at the router.
- The router allows entering only that traffic that the rules explicitly identify.
- It restricts other incoming connections to the host.

- There fore, the router may also be a single point of failure.
- If the security of the router is compromised, the complete network is available to an attacker.
- This architecture is popular due to the following reasons
  - It allows companies to easily enforce various security policies in different directions
  - It is relatively easy to implement

Screened subnet architecture

- It is similar to previous; but with some extra security
- It gives strength to the security of the firewall by adding a perimeter network, which helps in further isolating the internal network from the internet
- Two screening router are used; to protect network
- Each of these routers are connected to the perimeter net.
- One between internal and perimeter network; other between external and perimeter network
- More perimeter network can be added to offer more security

rules, then

in Figure 16.4. additional security. The screened

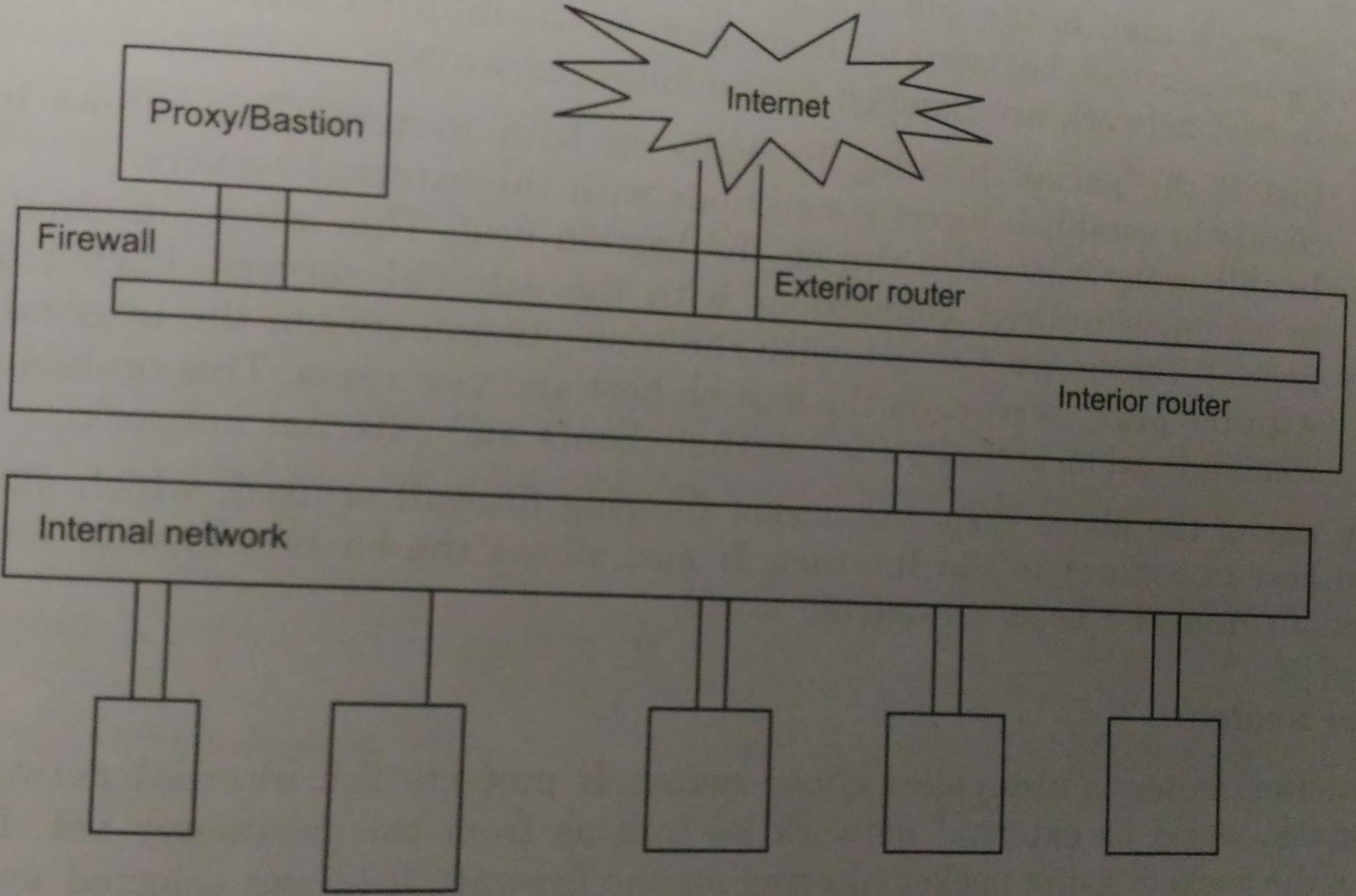
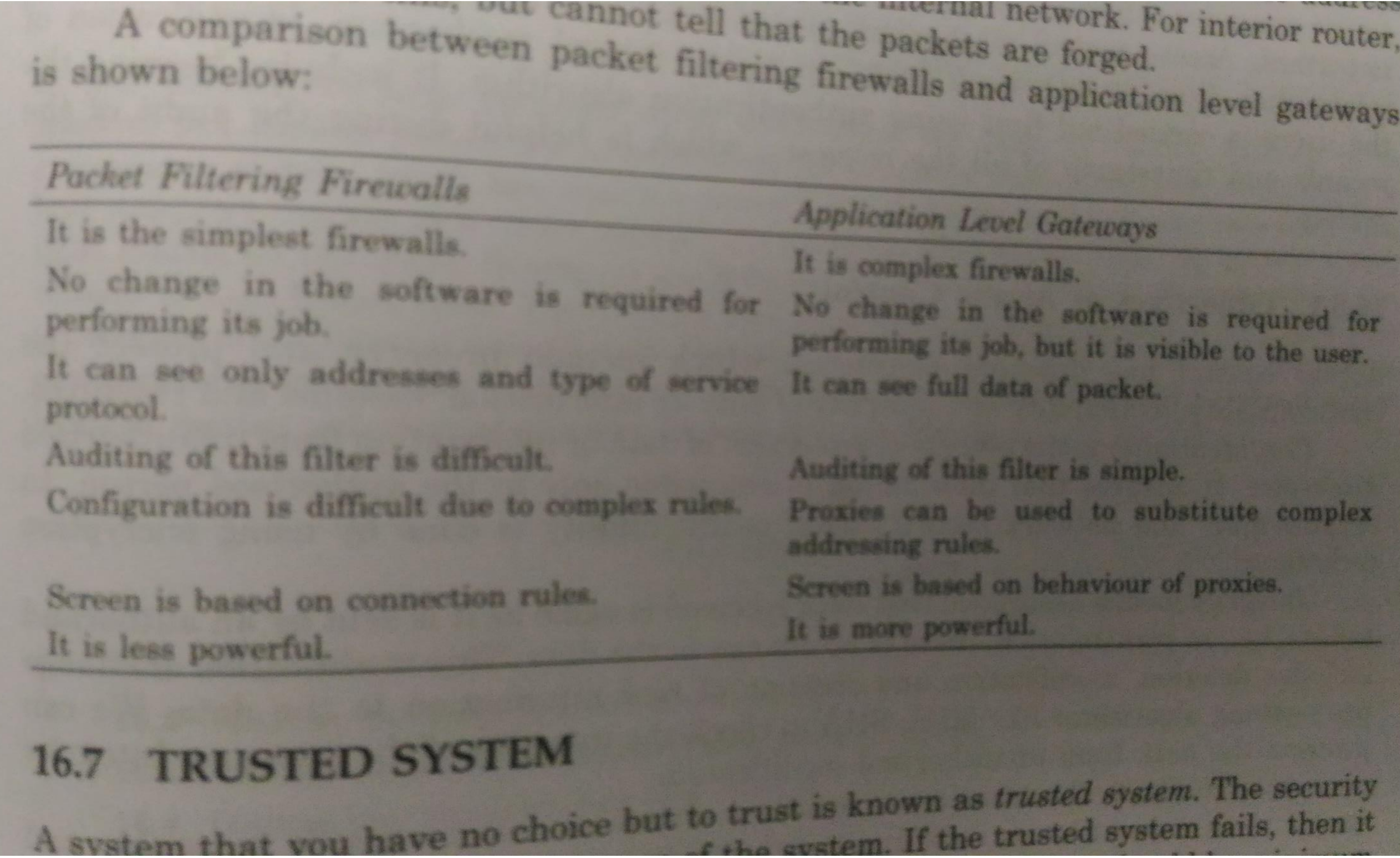


Figure 16.4 Screened subnet architecture (using two routers).

Perimeter Network

- It is a firewall installs between a private network and internet
- It controls all the traffic between the private network and the internet
- If the attacker is able to break the outer security of the firewall, then the perimeter net protects the internal network by providing an extra layer of security between the attacker and the internal network.
- There are two types of traffic of the perimeter net
  - To or from the bastion host
  - To or from the internet
- As the traffic from two internal hosts doesn’t pass from the perimeter net, it is safe from the attacker, though the security of bastion is broken.

- **Bastion Host**: The host attached to the perimeter net
- **Interior router**: It protects the internal network from the outside world or external network as well as from the perimeter net
- **Exterior Router**: It protects the perimeter net as well as the internal net from the outside world such as internet.



internal network. For interior router,

, but cannot tell that the packets are forged.

A comparison between packet filtering firewalls and application level gateways is shown below:

Packet Filtering Firewalls	*Application Level Gateways*
It is the simplest firewalls.	It is complex firewalls.
No change in the software is required for performing its job.	No change in the software is required for performing its job, but it is visible to the user.
It can see only addresses and type of service protocol.	It can see full data of packet.
Auditing of this filter is difficult.	Auditing of this filter is simple.
Configuration is difficult due to complex rules.	Proxies can be used to substitute complex addressing rules.
Screen is based on connection rules.	Screen is based on behaviour of proxies.
It is less powerful.	It is more powerful.

16.7 TRUSTED SYSTEM

A system that you have no choice but to trust is known as *trusted system*. The security

of the system. If the trusted system fails, then it

Trusted system

- A system that you have no choice but to trust is known as trusted system.
- The security of the system depends on the success of the system
- If it fails, then it will compromise the security of the entire system
- Therefore, there should be a minimum number of trusted components in a system.
- It provide security, integrity, reliability and privacy

- Many systems are trusted systems if they have the following options:
  1. The probability of threat or risk analysis is calculated, which is used to access the trust for taking the decision before authorisation
  2. To ensure the behaviour within the system, the deviation analysis is used