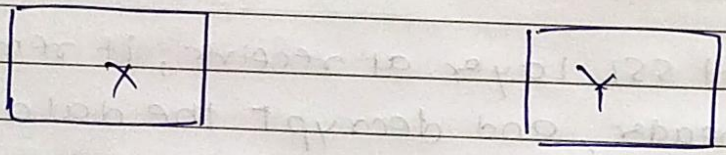
Page No.:
Date:

Unit 6

* Secure Socket Layer (SSL):-

- SSL is internet protocol for a secure exchange of information between web browser and web server.
- It provides secure pipe between web browser and web server.
- SSL considered as additional layer in TCP/IP model. It is located between application layer and transport layer.



L5 data Application L5 data

L5 data | SH | SSL L5 data | SH

L5 data | H4 | Transport L5 data | H4

L4 data | H3 | Internet L4 data | H3

L3 data | H2 | Data link L3 data | H2

0100010001000 Physical. 0100010001000

/ medium

- The application layer prepares data to sent to Y.
- The application layer data passed to SSL layer.
- SSL layer performs encryption and adds it's own header (SH) to encrypted data.
- The data sent via transmission media.
- At receiver, the same process happen.
- At SSL Layer at receiver, it removes SH header, and decrypt the data, gives plain-text back to application layer of Y.

1. Handshake protocol:-

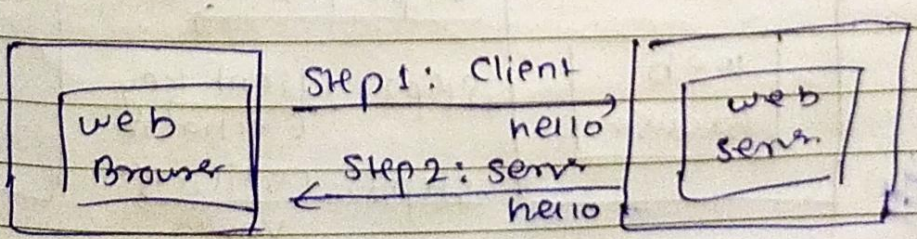
- The handshake protocol of SSL is first sub-protocol used by client and server to communicate using SSL-enabled connection.

- The handshake protocol is actualy made up of four phases:-
  1. Establish security capabilities.
  2. server authentication and key exchange.
  3. Client authentication and key exchange.
  4. Finish.

- Phase 1 :- Establish Security Capabilities:

- The first phase of SSL handshake is used to initiate a logical connection and establish the security capabilities associated with that connection.

- This consist of two messages, the client hello and server hello.

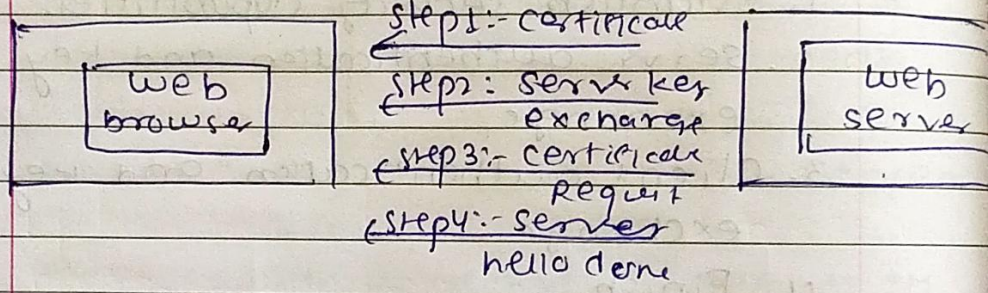


Page No.:
Date:

Phase 2:- Server Authentication and key Exchange

- The server initiates the second phase of SSL handshake, and is sole sender of all messages in this phase.

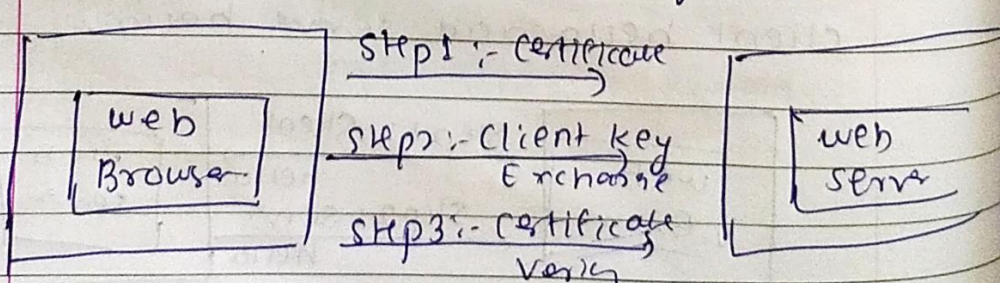
- There steps are certificate, Server key Exchange, Certificate Request and Server hello done.



Phase 3:- Client Authentication and key Exchange

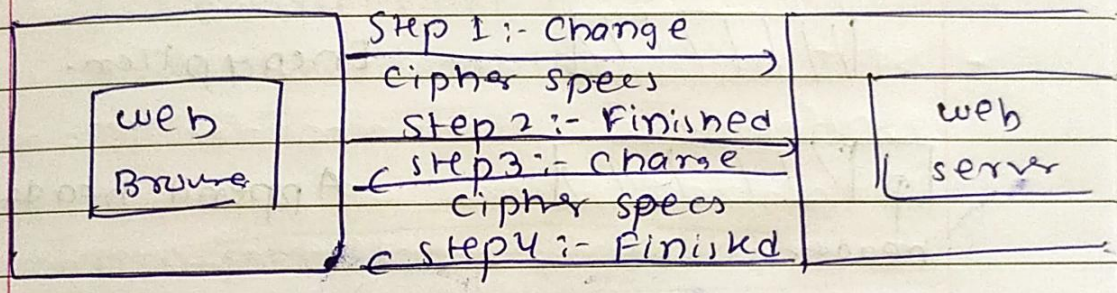
- The client initiates this third phase of SSL handshake, and sole sender of all messages in this phase.

- There steps are certificate, Client key Exchange, certificate verify.



phase 4:- Finish

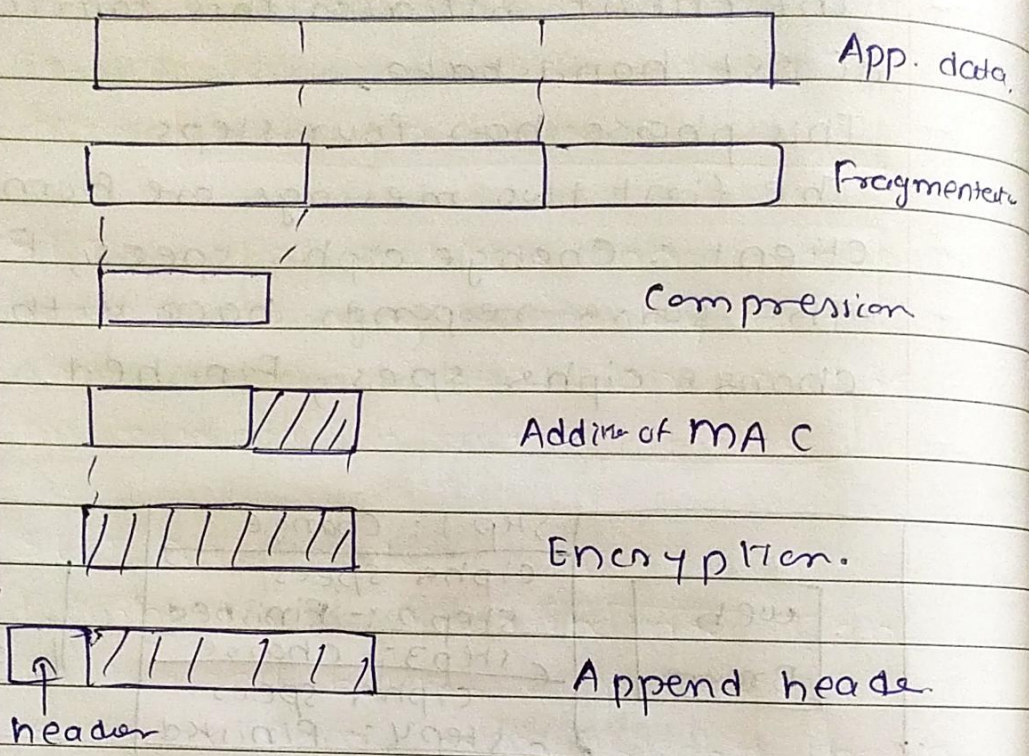
- The client initiates this fourth phase of SSL handshake.
- This phase has four steps.
- The first two messages are from client :- Change cipher specs, Finished
- The server responds back with : change cipher spes, Finished.



2. The Record Protocol :-

- The Record Protocol in SSL comes into picture after successful handshake is completed between o client and server.
- SSL record protocol takes an application menage as input.
- First, it fragments it into smaller blocks, optionaly compress each block, adds MAC,

encrypts it, adds a header and gives it to transport layer.



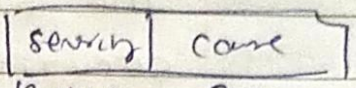
- At receiver's end, the header of each block ~~of~~ is removed, the block is then decrypted, verified, decompressed, and reassembled into application messages.

3. The Alert Protocol :-

- When either the client or server detects an error, the detecting party sends an alert message to the other party.

- Each alert message consists of 2 byte

- First byte signifies the type of error
  warning → 1.
  Error is Fatal → 2



- second byte specifies the actual error.

- If error is fatal, both ports close SSL connection, and also destroy the session identifiers, key, etc.

*. ~~Transport Layer Security (TLS)~~ :

Comparision bet^w SSL and TLS :-

	SSL	TLS
Version	3.0	1.0
Cipher suite	Supports an also called Fortezza	Does not support fortezza
Record protocol	MAC	HMAC
Alert code	Supports 12 alert code	Supports all except no certificate.

* Secure Electronic Transactions (SET):-

- The SET is open encryption and security specification that is designed for protecting credit-card transactions on Internet.

- SET is set of protocals and formats that enable the user to employ the existing credit-card payment infrastructure on Internet, in secure manner.

- SET participants:-

1. Cardholder:- A cardholder is an authorized holder of payment card such as Rupay or mastercard that has been isued by an issuer.

2. merchant:- A merchant is a person or organization that wants to sell goods or services to cardholder. A merchant must have relationship with an acquirer. for accepting payments on Internet.

3. Issuer:- The issuer is financial institution that provides a payment card to cardholder.

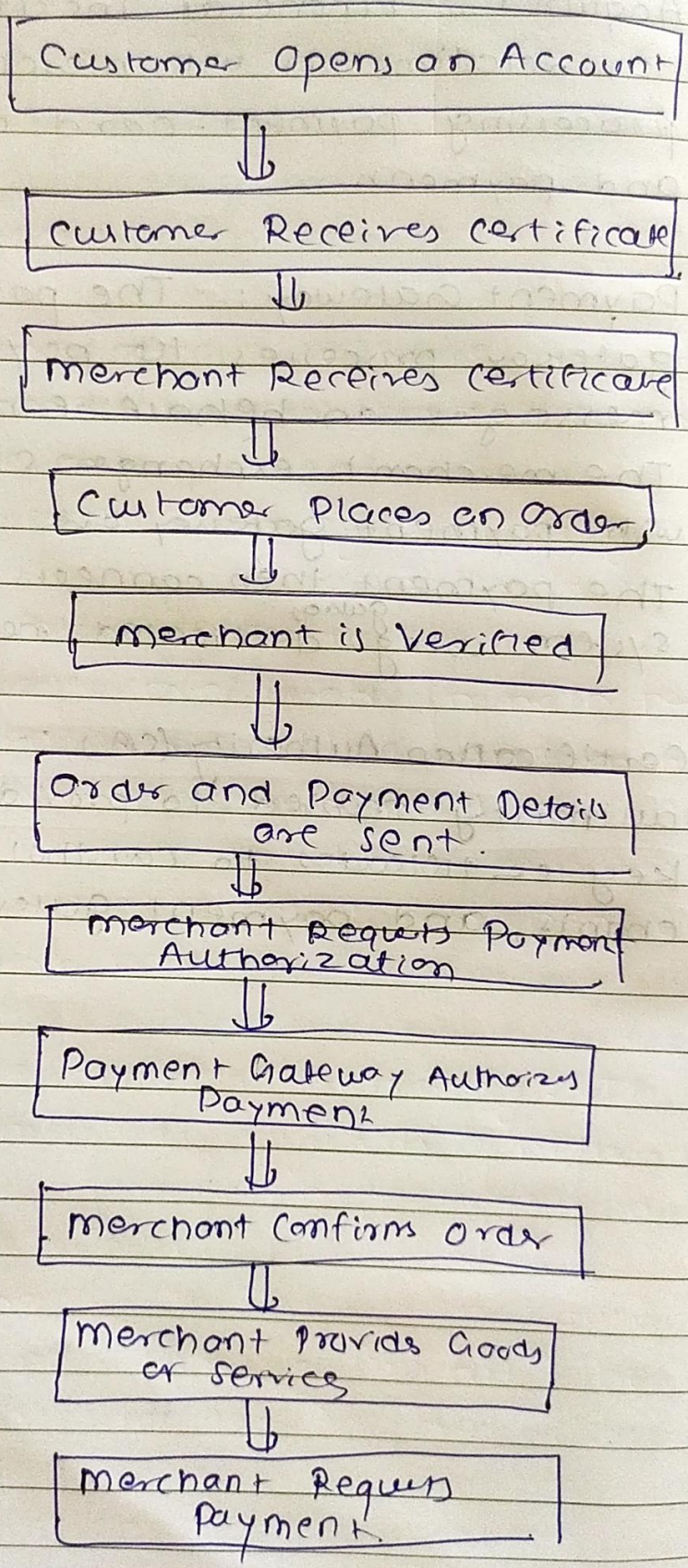
Page No.:
Date:

4. Acquirer :- Financial Institutions that has relationship with merchants for processing payment-card authorizations and payments.

5. Payment Gateway :- The payment gateway processes the payment messages on behalf of merchant. The merchant exchanges SET messages with payment gateway over Internet. The payment gateway then connects to acquirer's system using dedicated network lines.

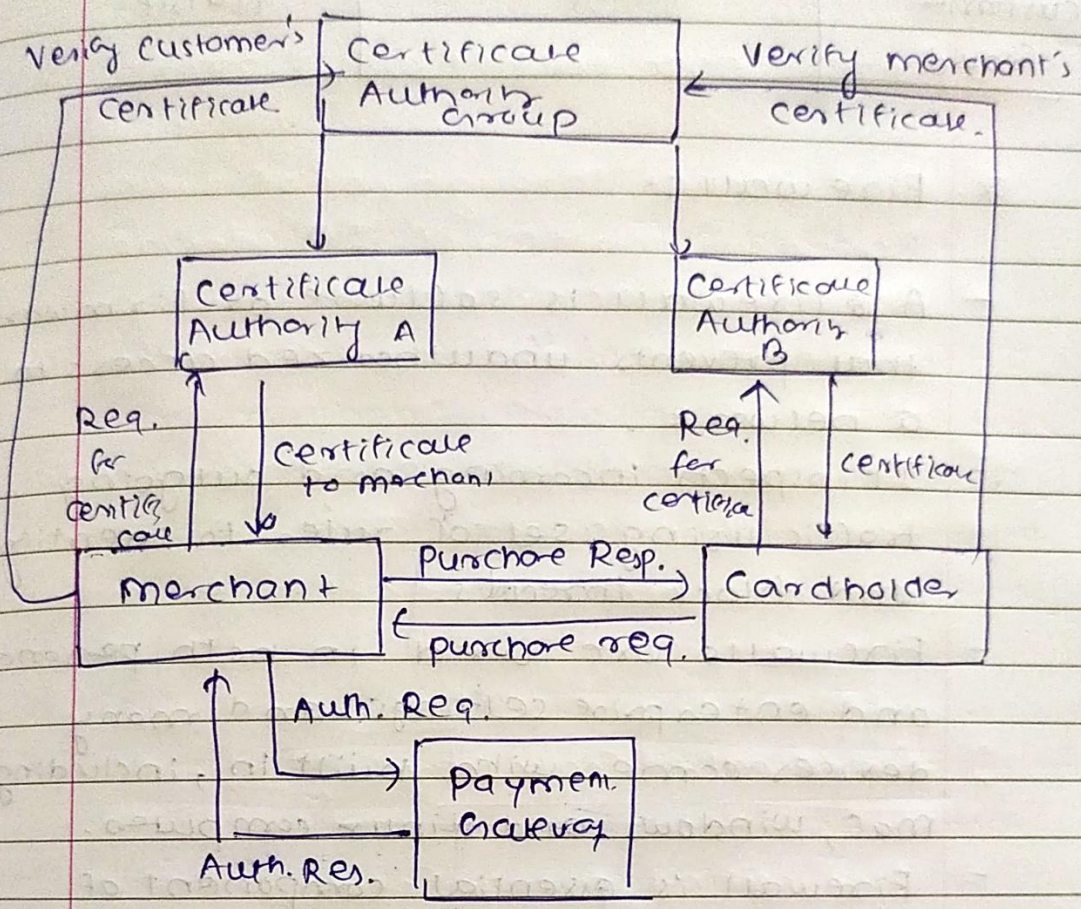
6. Certification Authority (CA) :- This is authority trusted to provide public key certificates to cardholders, merchants, and payment gateway.

* SET Process:


Customer Opens an Account
Customer Receives certificate
Merchant Receives certificate
Customer Places an order
Merchant is Verified
Order and Payment Details are sent.
Merchant Requests Payment Authorization
Payment Gateway Authorizes Payment
Merchant Confirms Order
Merchant Provids Goods or Services
Merchant Requests Payment.

Page No.:
Date:

* SET model:-



* Comp. betw SSL and SET

	SSL	SET
Aim	Exchange of data in encrypted form	E-commerce related payment mechanism
Certification	Two parties exchange certificates	All involved parties must have certificate by trusted third party
Authentication	Not very strong	strong mechanism
Practical Usage	High	High (due to high internet availability) speed

Action in case of customer fraud	merchant is liable	Payment gateway liable

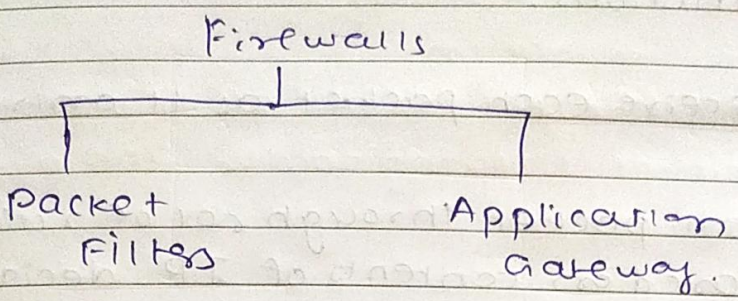
* Firewall :-

- A firewall is software or firmware that prevents unauthorized access to a network.
- It inspects incoming and outgoing traffic using set of rules to identify and block threats.
- Firewalls are used in both personal and enterprise settings and many devices come with built in, including mac, windows and Linux computers.
- Firewall is essential component of network security.

e.g.- A firewall acts like sentry. If implemented, it guards a network by standing between network and outside world.
- All traffic incoming and outgoing must pass through firewall. The firewall decides if traffic can be allowed.

Page No.:
Date:

Types of Firewall :-

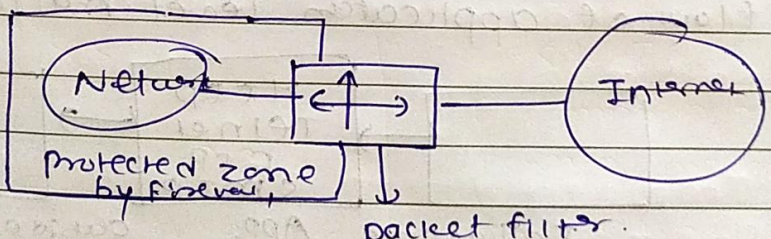


1. Packet Filters :-

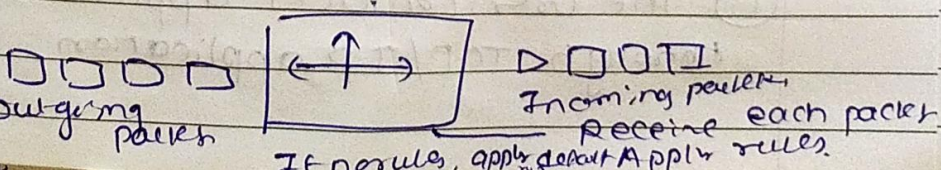
- Packet Filters applies rules to each packet and decides to either forward or discard packet.

- Also known as screening router or screening filter.

- Firewall implementation involves a router, which is configured to filter packets going in either direction.



- A packet filter can be router that performs three main actions.



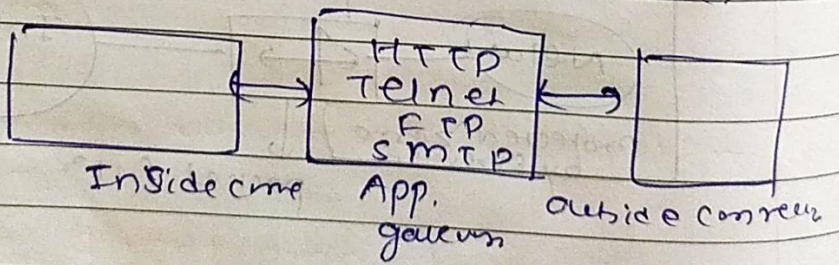
A packet filter performs following functions:-

1. Receive each packet as it arrives.

2. Pass packet through set of rules. Based on contents of IP decide whether to accept or discard packet based rule.

3. If there is no match with any rule, take default action. The default can be discard all packets or accept all packets.

2 Application Gateway:-

- Also called proxy server.
- It acts like proxy and decides about flow of application level traffic.
- 

- It works as follows:-

(1) The user contacts application gateway through TCP/IP application.

(2) The application gateway asks user about the remote host with which user wants to connects. The app. asks for user id and password

(3) User provides information to application gateway.

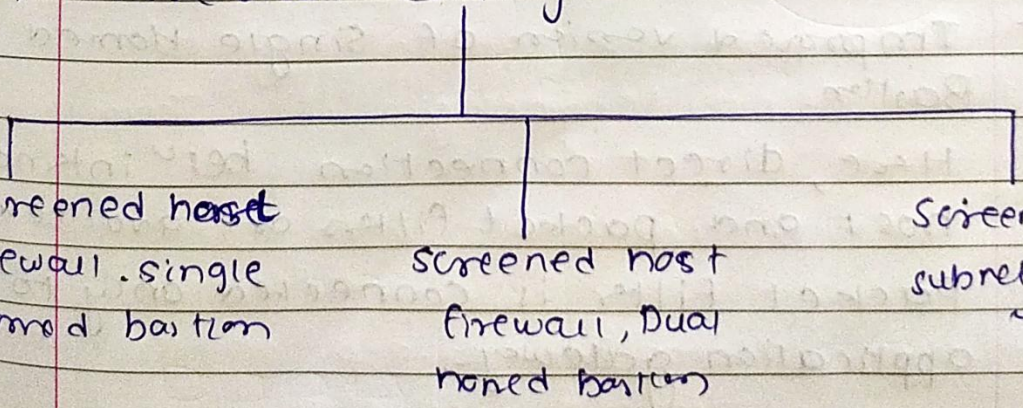
(4) The application gateway now accesses the remote host on behalf of user and passes packets of user to remote host.

(5) From here, application gateway acts like proxy and delivers packets from user to remote host and vice versa.

- It is more secure that packet filters.

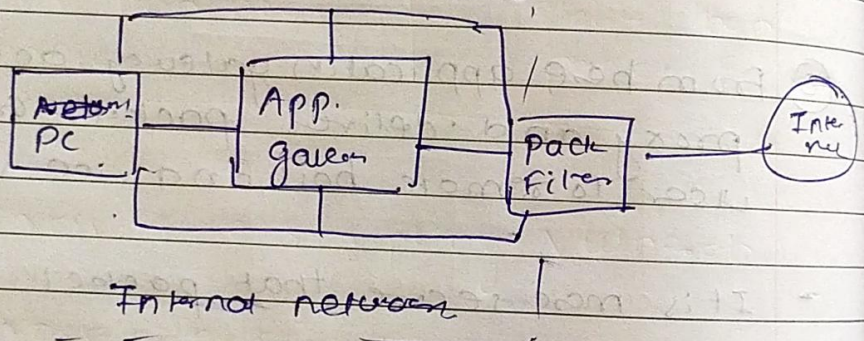
- Disadvantage : overhead in terms of connection.

* Firewall Configuration :-



1. Screened Host Bastion, Single-Homed Bastion :-

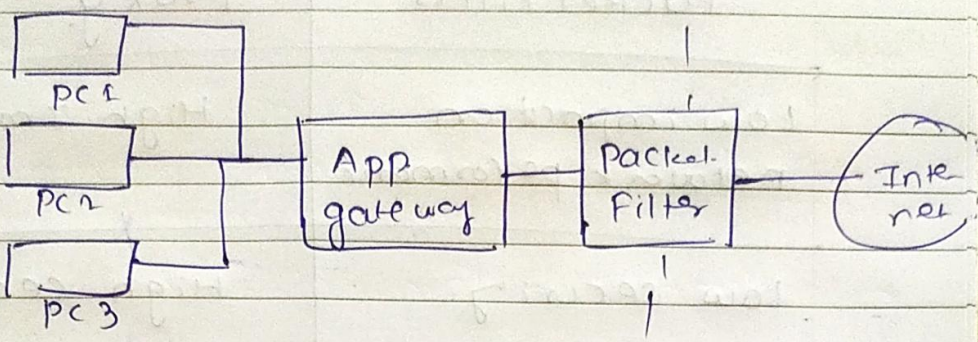
- This firewall consist of two ports: a packet-filtering router and application gateway.
- Packet filter ensures :-
  1. incoming traffic allowed only if it is destined for application gateway
  2. outgoing traffic allowed only if it is originating from application gateway.



- App. gateway perform auth. and proxy funct.

2. Screened Host Bastion Dual Homed Bastion :-

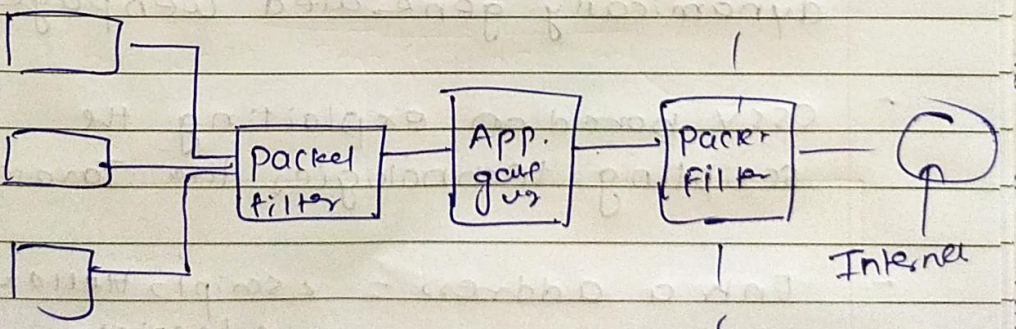
- Improved version of Single Homed Bastion.
- Here, direct connection bet^n internal host and packet filters are avoided.
- Packet Filter is connected only to application gateway.



- If Packet filter is successfully attacked, the internal hosts are protected.

3. Screened subnet Firewall:-

- offers highest security.
- Here, two packet filters are used, one between Internet and application gateway and one between internal network and application gateway.



Packet Filter	Proxy
Low impact on network performance	High Impact
low security	High security.
Transparent to user	Not transparent
Difficult to configure	Easy to configure
Faster than proxy. firewall	Slower than packet Filtering

× Cross-site Scripting Vulnerability:

- Cross-site scripting happen when malicious tags or scripts attack a web browser via another site's dynamically generated webpage.
- CSSV based on exploiting the scripting technologies like Javascript.
- Enter address = <script> Hello world </script>
- www.test.com/address.asp?address = <script> Helloworld </script>

- The serve side program does not validate and sends the value of field address to next web page.

- It user would see Hello world in next web page.

Intruders :-

- No matter how much secure a system is, the attackers who would constantly try to find their way. This attackers are called intruders because they try to intrude into privacy of our network.

- Three types :-

1. Masquerader :- A user does not have authority to use a computer, but penetrates into system to access legitimate user's account is called as masquerader, external user

2. Misfeasor :- A user can be misfeasor if :-
   1. A user, who does not have access to some applications accesses them.
   2. A user, who have access to some applications but misuses them.

3. Clandestine :- An internal or external user who tries to work with the privileges of supervisor user to avoid auditing info being captured and recorded is called clandestine users.

- Intruders try to attack by obtain password of legitimate users.

- Intrusion Detection :- 1. statistical Anomaly detection
  2. Rule-based detection

1. statistical Anomaly detection :- Behaviour of users are captured as statistical data and processed. Rules are applied to test whether user behaviour was legitimate or not.

(i) Threshold Detection :- Thresholds are defined for all users as group and frequency of various events are measured against these threshold.

(ii) Profile based Detection :- Profiles are individual are created and they are matched against to collected statistics to see behaviour

Virtual Elections:-

- Cryptography can be useful in virtual elections.
- Computerized voting would be come quite common in next few decades.
- Implementation can be as follows:-
  1. Each voter cast the vote and signs it with his private key.
  2. Each voter encrypts the signed vote with public key of Election Authority (EA)
  3. Each voter sends vote to EA.
  4. EA decrypts the voter with its private key and verifies the signature of voter with help of voter's public key.
  5. EA then tabulates all votes and announces the result of elections.
- This procedure would ensure duplicate voting is disallowed as voter has signed and no one can change another voter's vote as it is digitally signed.
- But EA can know who voted for whom, leading to privacy concerns.

(b) Rule-based Detection:- Set of rules are applied to see if given behaviour is suspicious. Two types:-

1. Anomaly Detection:- Usage patterns are collected to find deviation in user pattern, with helps of rule.
2. Penetration Identification:- Expert system that looks for illegitimate behaviour.