Web Security

- Prepared by :-Bambhaniya Dipik@ a.

CONTENTS OF WEB SECURITY

- NEED OF SECURITY
- WEB SECURITY REQUIREMENT
- SLL AND TRANSPORT LAYER SECURITY
- SECURE ELECTRONIC TRANSACTIONS
- CONTENTS OF FIREWALL
- TRUSTED SYSTEM
- APPLICATION
- CONCLUSION

Need Of Security

- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primarily by physical and administrative means.

WEB SECURITY :

- Measures to protect data during their transmission over a collection of interconnected networks.
- The World Wide Web is fundamentally a client/server application running over the internet and TCP/IP intranets.

Web security Requirement

- The web is very visible.
- The WWW is widely used by:-
- Business, Government agencies and many individuals.
- These can be described as passive attacks including eavesdropping on network traffic between browser and gaining access to information on a website that is supposed to be restricted.
- Active attacks including impersonating another user, altering information on a website.
- The web needs added security mechanisms to address these threats .

Web Security Threats

- Various approaches are used for providing security web. One of the examples is IP-security.

Parameter	Threats	Consequences	Counter Measures
INTEGRTY	1.Modification of user data, memory, message traffic in transmit.. 2.Trojan horse browser.	1.Loss of information . 2.Compromise of machine. 3.Vulnerability to all other threats.	Cryptographic checksums.
Confidentiality	1. Eavesdropping on the net. 2. Theft of information and data from server and client.	Loss of information and privacy.	Encryption, Web proxies.

(continue……)

Parameter	Threats	Consequences	Counter Measures
Denial of service	1. Killing of user threads. 2. Flooding machine with bogus requests. 3. Filling up disk or memory. 4. Isolating machine by DNS attacks	1. Disupptive 2. Annoying 3. Prevent user from getting work done.	Difficult to prevent.
Authentication	1. Impersonation of legitimate users. 2. Data forgery.	1. Misrepresentation of user. 2. Belief that false information is valid.	Cryptographic techniques.

Web Traffic security Approaches

- A number of approaches to providing web security are possible. figure illustrates this difference.

1. Network level
2. Transport level
3. Application level

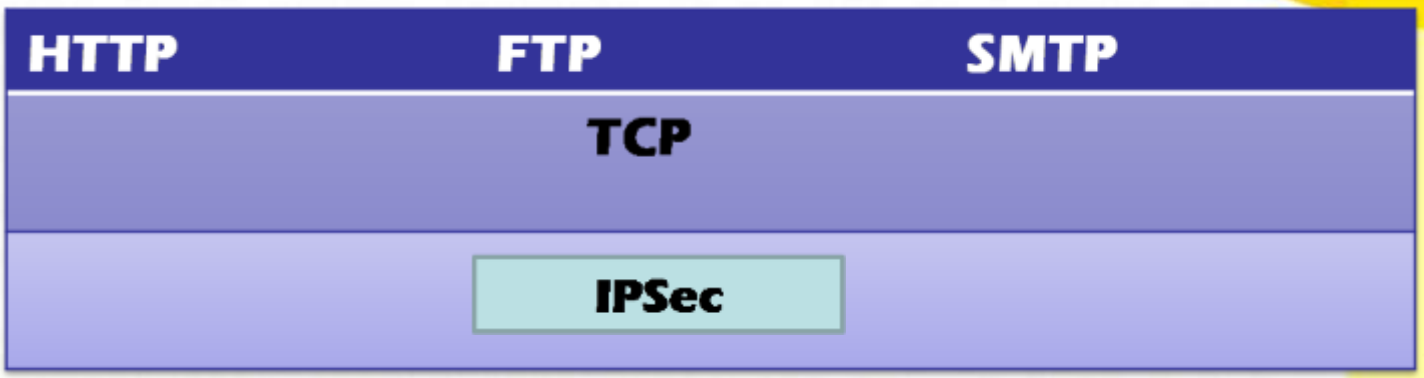


Fig: Network level

(continue……)

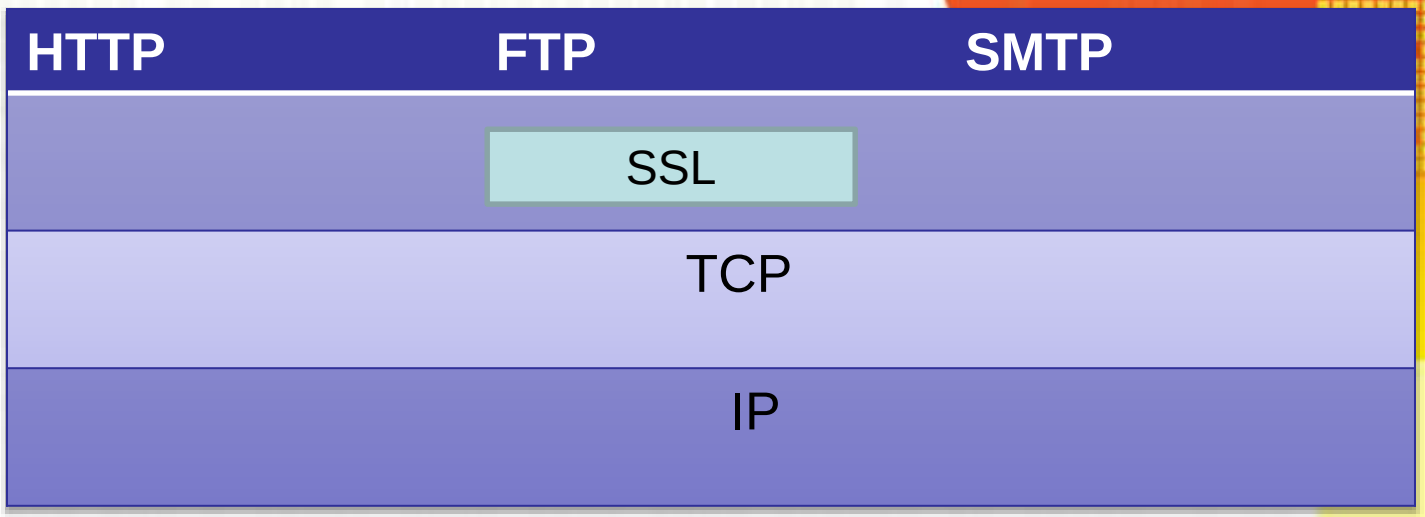


Fig: Transport level

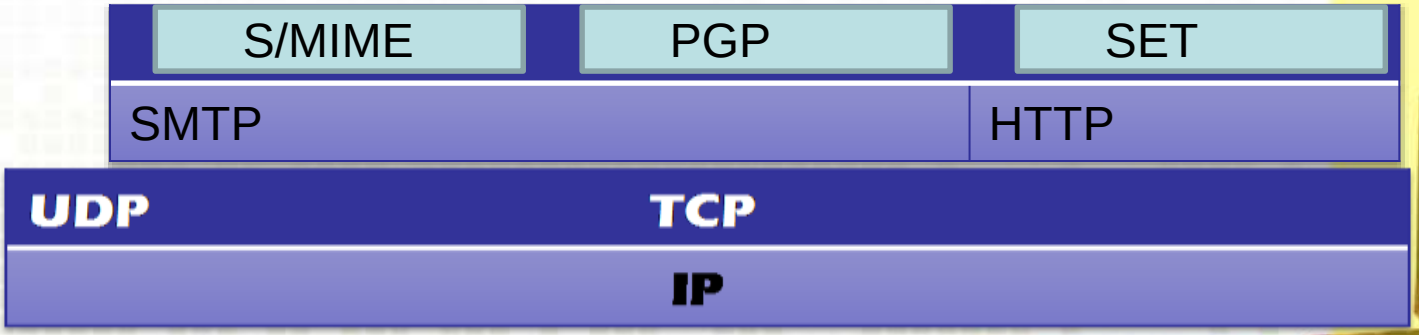


Fig: Application level

Secure Socket Layer[SSL]

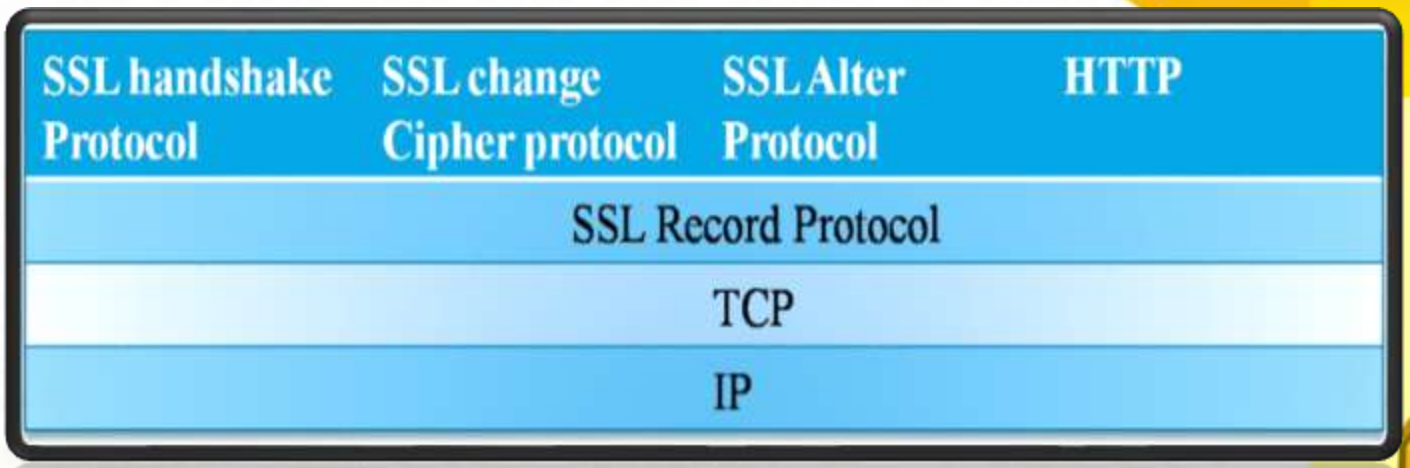
- SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.
- SSL is designed to make user of TCP to provide a reliable end to end secure service.
- SSL provides security services between TCP and application that use TCP.
- The SSL protocol is an internet protocol for secure exchange of information between a web browser and a web server.

Features of SSL

1. SSL server authentication , allowing a user to confirm a server's identity.
2. SSL client authentication , allowing a server to confirm a user's identity.
3. An encrypted SSL session , in which all information sent between browser and server is encrypted by a sending software and decrypted by the receiving software.
4. SSL supports multiple cryptographic algorithms.

SSL Architecture:-

- SSL uses TCP to provide reliable end-to-end secure service.
- SSL consists of two sub protocols , one for establishing a secure connection and other for using it. Figure shows SSL protocol stack.



[Figure : SSL protocol stack]

(continue……)

HTTP:

- Provides the transfer services for web client/server interaction.

SSL Handshake Protocol , SSl change cipher protocol:

- Management of SSL exchanges.SSL Alert Protocol .

SSL Record Protocol:

- It provide basic security services to various higher layer protocols.
- The SSl record protocol provides two services for SSL connections:

Confidentiality:

- The handshake protocol defines a shared secret key that is used for conventional encryption of SSl payloads.

Message Integrity:

- The handshake protocol also defines a shared secret key that is used to from a message authentication code(MAC).

Comparison between IPSec and SSL

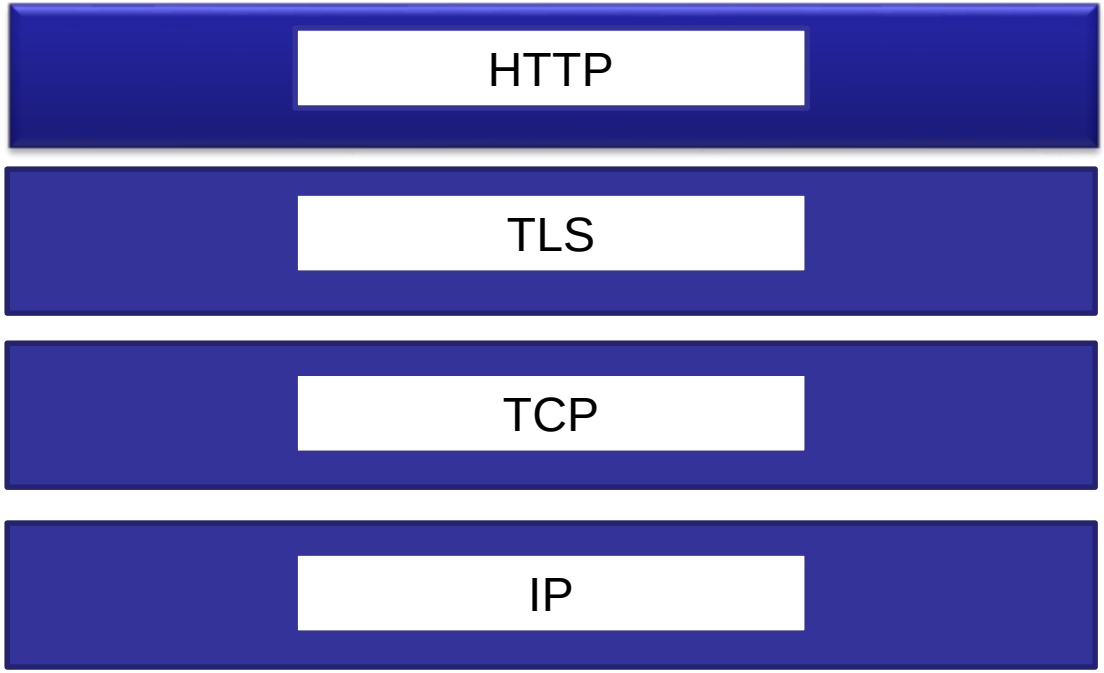
Sr no.	Parameters	IP-Security	SSL
1.	Position in the OSI model	Internet layer	Between the transport and application layers.
2.	Configuration	Complex	Simple
3.	NAT	Problematic	No problem
4.	Software location	Kernel area	User area
5.	Firewall	Not friendly	Friendly
6.	Installation	Vender non-specific	Vender specific
7.	Interoperability	Yes	No
8.	Deploy	More expensive to deploy support and maintain.	Less costly to deploy and maintain.

Transport Layer Security [TLS]

- Transport Layer Security (TLS) is a feature of mail servers deigned to secure the transmission of electronic mail from one server to another using encryption technology.
- TLS can reduce the risk of eavesdropping tampering and message forgery mail communications.
- TLS was designed to provide security at the transport layer.
- TLS is a non-proprietary version of SSL. For transactions on Internet , a browser needs:
  - Make Sure that server belongs to the actual vendor.
  - Contents of message are not modified during transaction.
  - Make sure that the imposter does not interpret sensitive information such as credit card number.

(continue……)

- Figure shows the position of TLS in the protocol.



[Figure: position of TLS in the protocol]

TLS has two protocols :

1. Handshake
2. Data exchange protocol.

(continue……)

1. **Handshake :-**
   - The TLS handshake protocol allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before the application protocol transmits or receives any data.

2. **Data exchange protocol:-**
   - Data exchange protocol uses the secret key to encrypt the data for secrecy and to encrypt the message digest for integrity.
   - The TLS record protocol is designed to protect confidentiality by using symmetric data encryption.

Comparison between IPSec & TLS:

Sr no.	IPSecurity	TLS
1	Type of security is device to device.	Type of security is application to application
2.	It provides network segment protection.	It does not provides network segment protection.
3.	Application modification is required.	Application modification is not required.
4.	Traffic protected with data authentication and encryption is for all protocol.	Traffic protected with data authentication and encryption is only for TCP protocol.
5.	It controlled by using Ipsec policy.	It controlled by using TLS policy.
6.	Scope of protection is for single connection for all traffic protocol.	Scope of protection is for single connection for all TLS protocol.

Secure Electronic Transaction[SET]

- SET is an encryption and security specification develop to protect credit card transactions through Internet SET is not a payment system but a set of security protocols for secured way payment transactions.

SET is a complex specification defined in :-

- Business Description
- Programmer's Guide
- Formal protocol Definition

Services Provided by SET:-

- SET provide a secure communication channel among all parties.
- Provides trust by using X.509V3 digital certificates.
- Ensures privacy.

(continue……)

Requirement for SET:-

- For ensuring payment processing over Internet following are the requirements of SET protocol specifications.
  - Provide confidentiality of payment and ordering information.
  - Ensure the integrity of all transmitted data.
  - Provide authentication about card holder.
  - Provide authentication about merchant.
  - Ensure use of best security practices and system design.
  - Develop a protocol that does not depend on transport security.
  - Facilitate interoperability between software and network.

(continue……)

SET Participants:-

- The sequence of event in SET system is as follows.

1. Customer opens an account
2. Customer receives a certificate
3. Merchant's certificate
4. Customer places an order
5. Verification of merchant
6. Order and payment sent
7. Request for payment authorization by merchant
8. Merchant confirms order
9. Merchant provides goods or services
10. Merchant requests payment.

(continue……)

Key Technology of SET :-

1. **Confidentiality of information** : DES
2. **Integrity of data** : RSA digital signatures with SHA-1 hash codes
3. **Cardholder account authentication** : X.509v3 digital certificates with RSA signatures.
4. **Merchant authentication** : X.509v3 digital certificates with RSA signatures.
5. **Privacy** : Separation of order and payment information using dual signatures.

(continue……)

SET Supported Transactions :-

1. Card holder registration
2. Merchant registration
3. Purchase request
4. Payment authorization
5. Payment capture
6. Certificate query
7. Purchase inquiry
8. Purchase notification
9. Sale transaction
10. Authorization reversal
11. Capture reserval

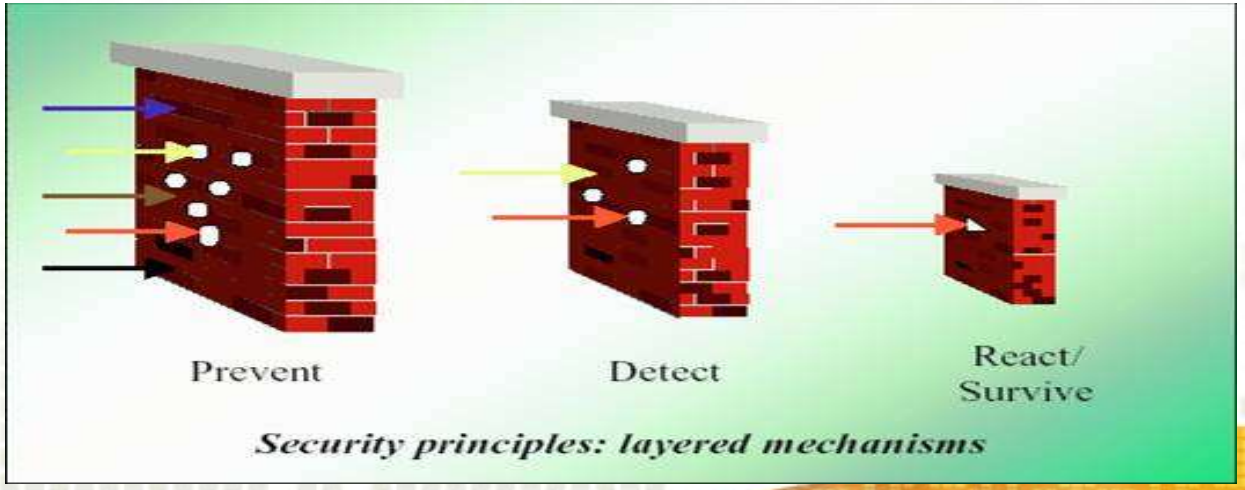
Contents of Firewall

1. Why firewall?
2. What is firewall?
3. Firewall design principles.
4. Capability of firewall.
5. Limitation of firewall.
6. Firewall technology.
7. Design goal of firewall.
8. Types of firewall.
9. Comparison packet filter and proxies
10. Feature of firawall.

(continue……)

1.Why firewall?

- Internet connectivity has become essential for most organizations.
- The Internet was not designed to be secure
  - It was created for open access to research
- The Internet suffers from major security issues
  - Allows adversaries to attack or gain access to many private networks

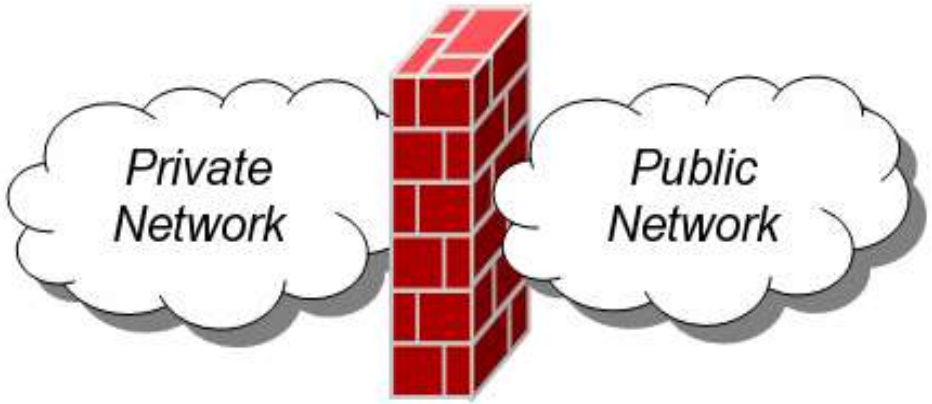


Security principles: layered mechanisms

(continue……)

2.What is firewall?

- The term firewall comes form the fact that by segmenting network into different physical sub network, They limit the damage that could spread from one subnet to other just like fire doors or firewalls.
- A firewall is also called a Border Protection Device (BPD) in certain military contexts where a firewall separates networks by creating perimeter networks in a DMZ “Demilitarized Zone”.



(continue……)

3.Firewall design principals

- A firewall is inserted between the internet and LAN for security purpose. The firewall protects the LAN from internet-based attacks and also provides security audits.
- A firewall may be a hardware or a software program running on a secure host computer.
- A firewall must have at least two network interfaces one for the network it is intended to protect and one for the network and other for the network it is exposed.
- shown in fig.

(continue……)

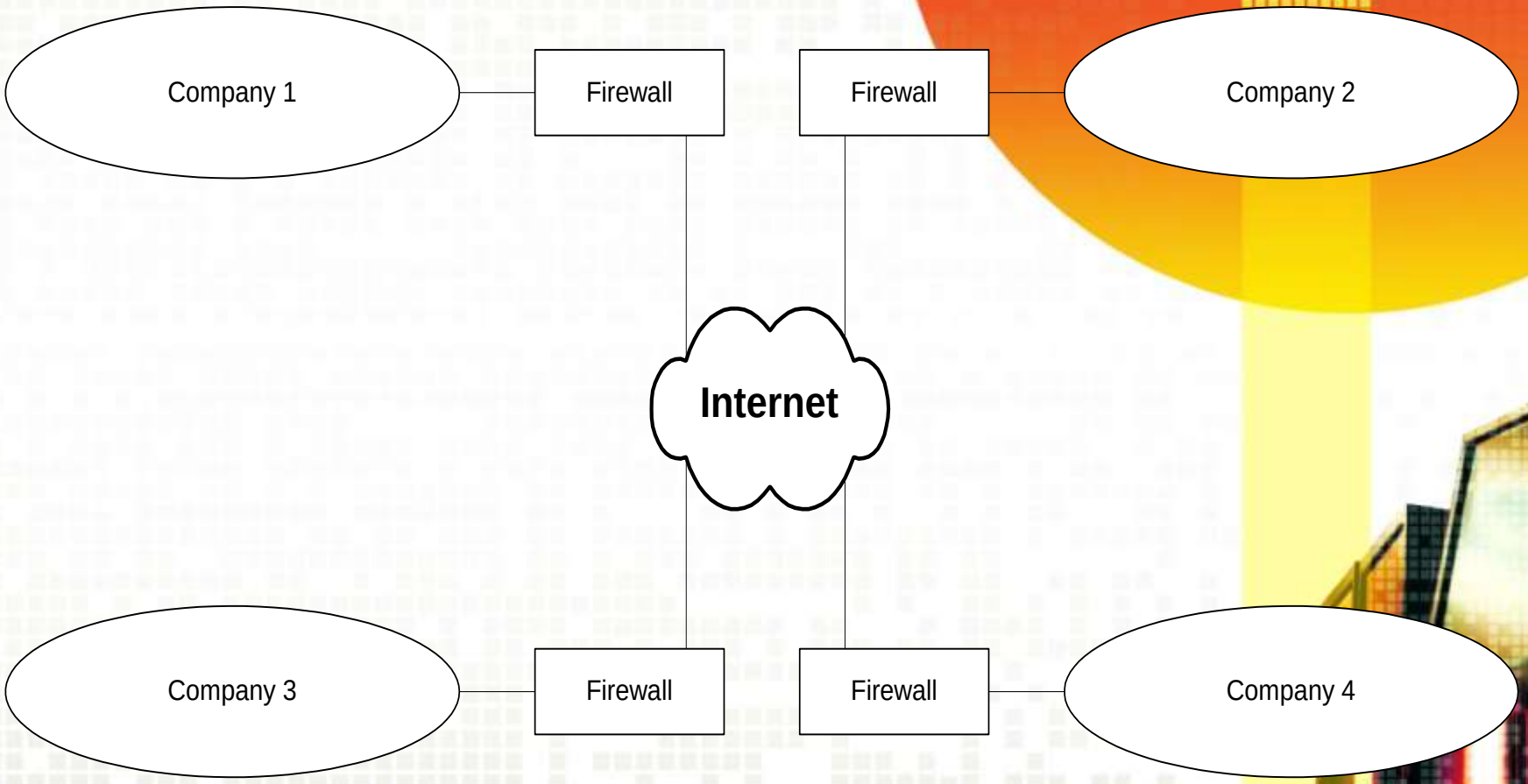


Figure:firewall

(continue……)

4.Capabilites of firewall

- Enhanced privacy
- Concentrated security
- Policy enforcement
- Protect from vulnerable services
- Network logging & statistics
- Limit external access to internal systems

5.Limitation of firewall.

- Backdoors may exist
- No protection from insider attacks
- Blocking of required services
- Considered an “all eggs in one basket” approach

(continue……)

6.Firewall technology.

- Firewall technology generally falls into one of the two categories network level and application level.

1. **Network level:**

- Makes decision based on the source, destination addresses, router and ports in individual IP packets.
- Has the ability to perform static and dynamic packet filtering and stateful inspection.

2. **Application level:**

- They are generally, hosts running proxy servers which perform logging and auditing of traffic through the network.

(continue……)

7. Design goal of firewall.

- Firewall are very effective means for network based security threats. The design goals for firewall are as under

  1. All the traffic must pass through firewall both from inside to outside and outside to inside.

  2.Only authorized traffic defined by local security is allowed to pass.

  3.Firewall itself is immune to penetration.

- Generally four techniques are used to control access and enforce the security policy, these techniques are-

  1.Service Control

  2.Direction Control

  3.User Control

  4.Behavior Control

(continue……)

- Insert after the fact security by wrapping or interposing a filter on network traffic

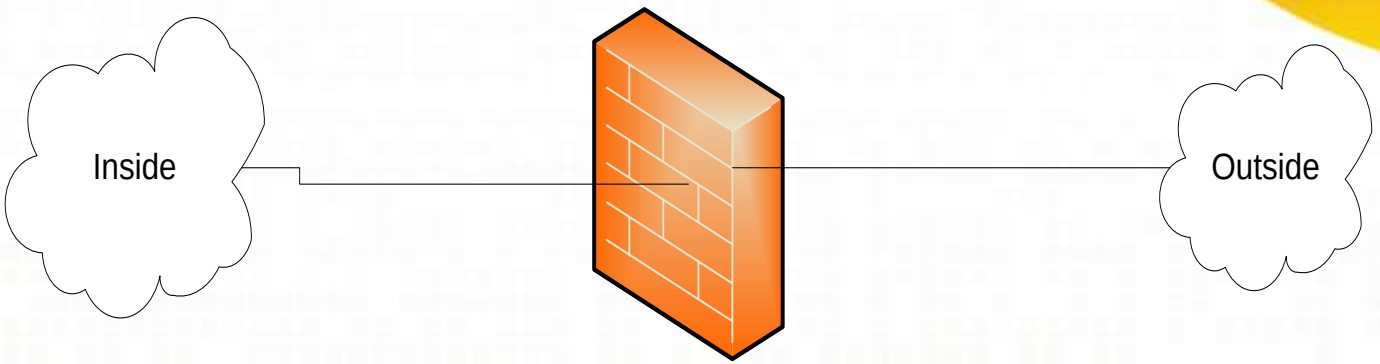


Fig: Cyber Security Spring

(continue……)

Security domain

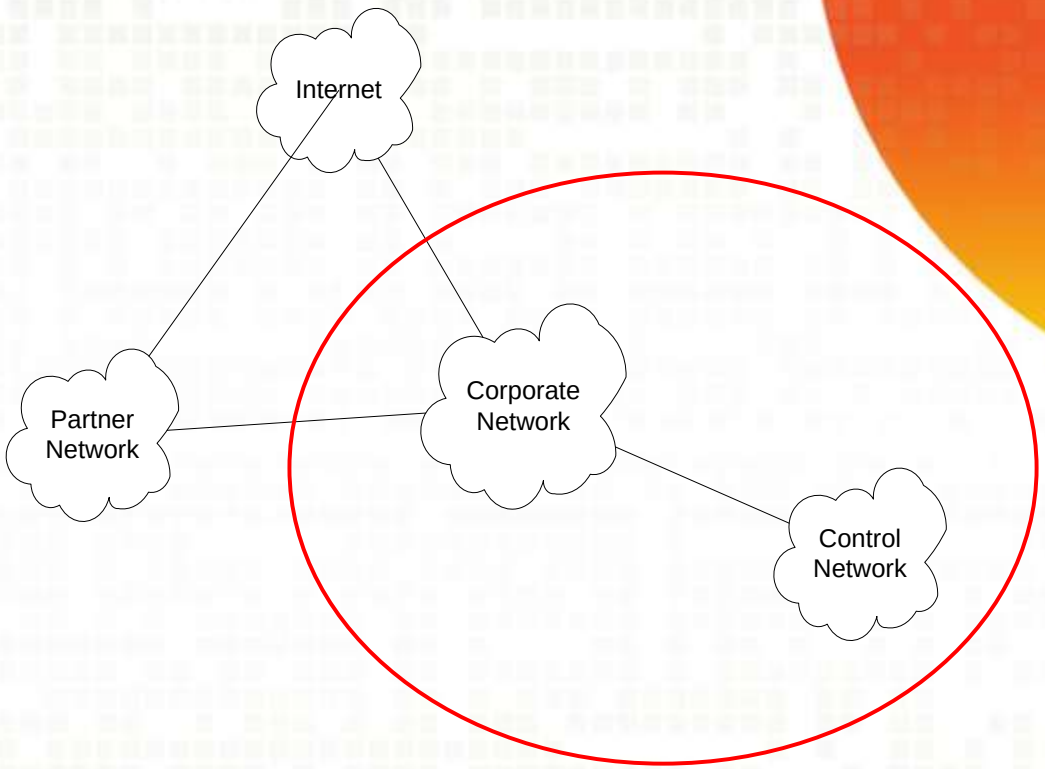


Fig: Cyber Security Spring

(continue……)

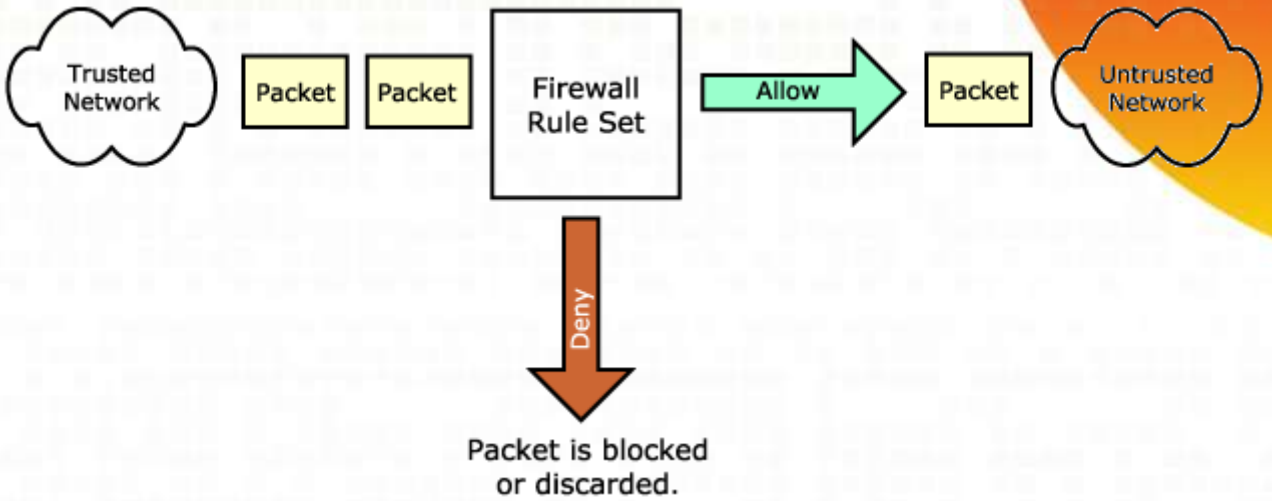
8.Types of firewall.

- Packet-filtering routers
  - Applies a set of rules to individual IP packets as they arrive
- Application gateways / proxy servers
  - Acts as a buffer for services between the internal and external network
- Circuit level gateways
  - Works by never allowing end-to-end TCP connections

(continue……)

1. Packet Filtering Firewall

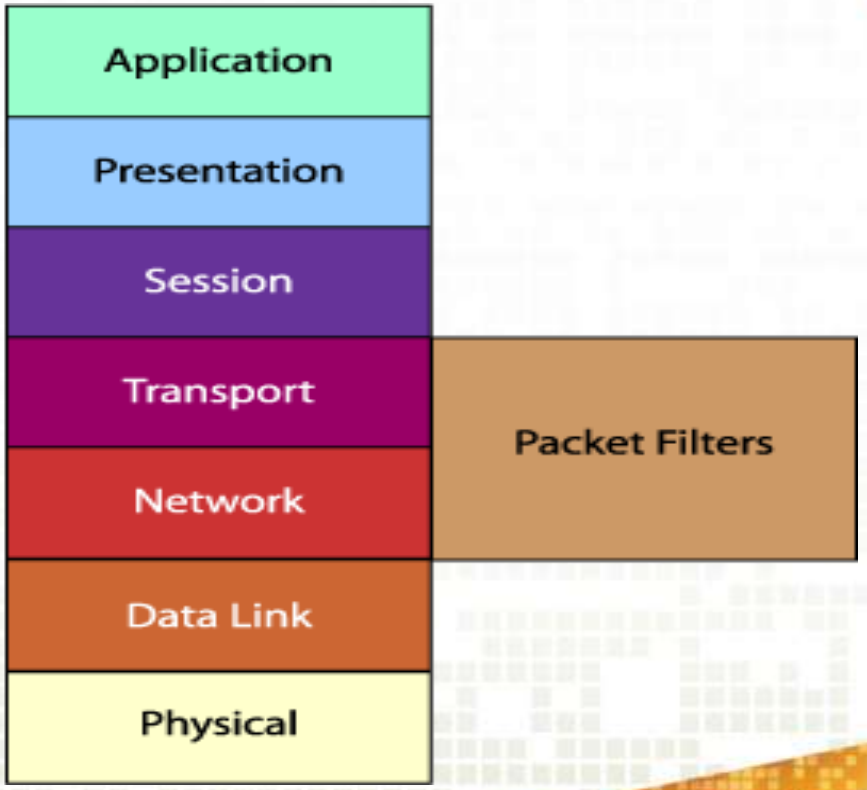
- A packet filtering firewall does exactly what its name implies -- it filters packets.



- As each packet passes through the firewall, it is examined and information contained in the header is compared to a pre-configured set of rules or filters.
- An allow or deny decision is made based on the results of the comparison. Each packet is examined individually without regard to other packets that are part of the same connection.

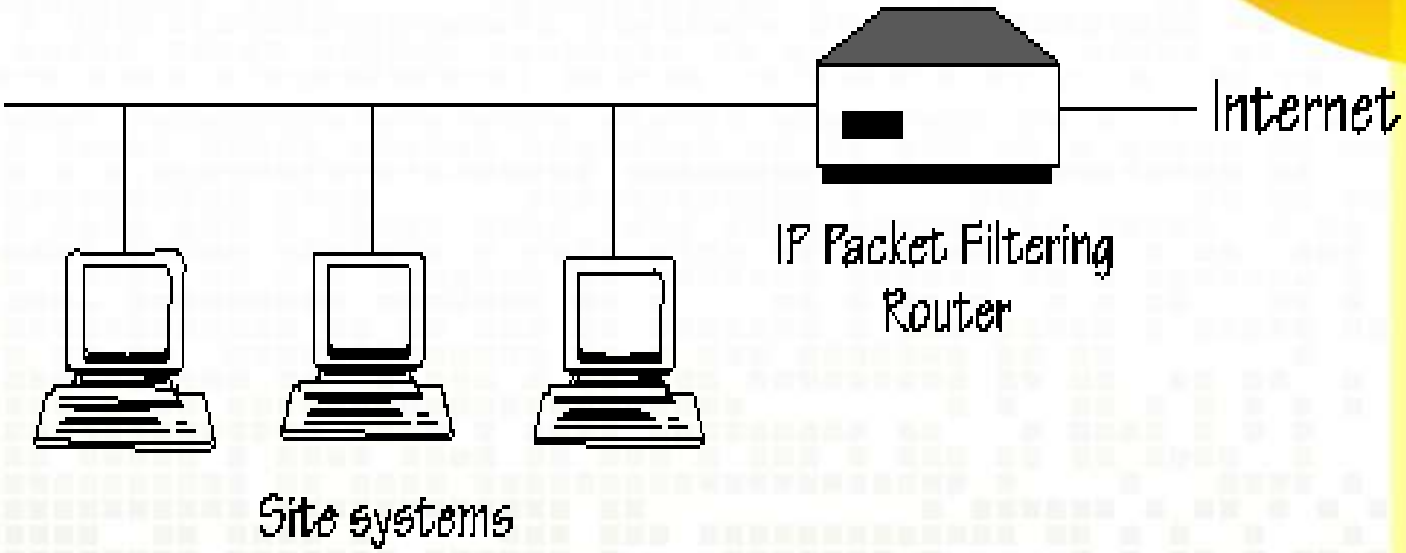
(continue……)

- A packet filtering firewall is often called a network layer firewall because the filtering is primarily done at the network layer (layer three) or the transport layer (layer four) of the OSI reference model.



(continue……)

- You use packet filters to instruct a firewall to drop traffic that meets certain criteria.
- For example, you could create a filter that would drop all ping requests. You can also configure filters with more complex exceptions to a rule.



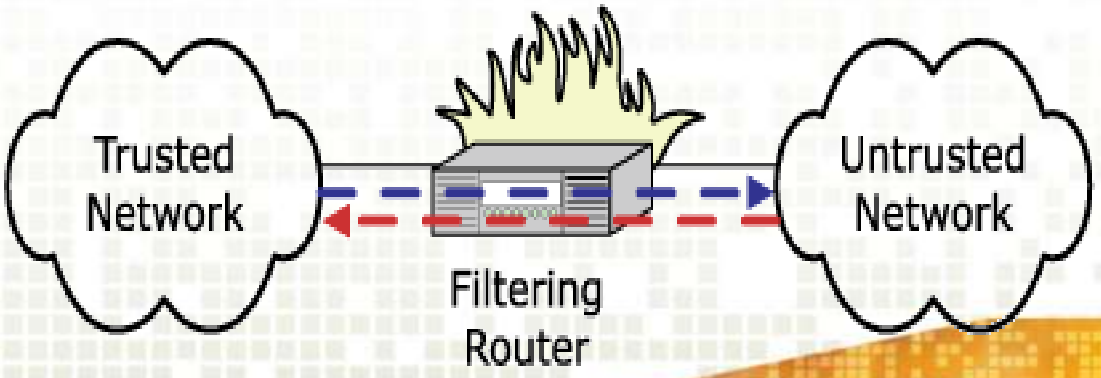
[**Figure**: **Example of a Packet-Filtering Firewall.]**

(continue……)

- Packet filtering rules or filters can be configured to allow or deny traffic based on one or more of the following variables:

Field of packet filtering firewall

- Source IP address
- Destination IP address
- Protocol type (TCP/UDP)
- Source port
- Destination port



(continue……)

Advantages of packet filters

1. Packet filtering is typically faster than other packet screening methods.
2. Packet filtering firewalls can be implemented transparently.
3. Packet filtering firewalls are typically less expensive.

Disadvantages of packet filters

1. Packet filtering firewalls allow a direct connection to be made between the two endpoints..
2. Packet filtering firewalls are fast and typically have no impact on network performance.
3. Defining rules and filters on a packet filtering firewall can be a complex task.

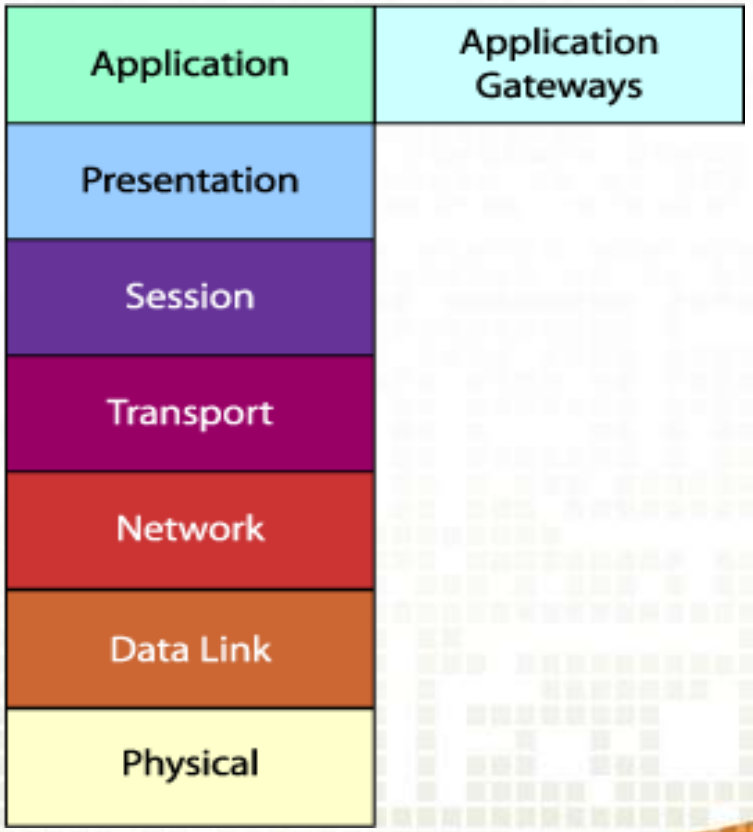
(continue……)

2.Application gateways / proxy servers

- The proxy plays middleman in all connection attempts.
- The application gateway/proxy acts as an intermediary between the two endpoints.
- This packet screening method actually breaks the client/server model in that two connections are required: one from the source to the gateway/proxy and one from the gateway/proxy to the destination.
- Each endpoint can only communicate with the other by going through the gateway/proxy.

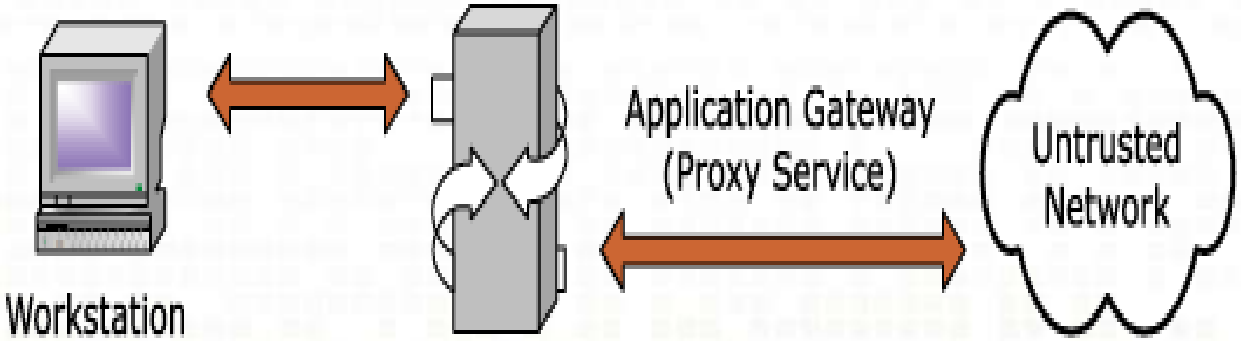
(continue……)

- The gateways/proxies are carefully designed to be reliable and secure because they are the only connection point between the two networks.



(continue……)

- When a client issues a request from the untrusted network, a connection is established with the application gateway/proxy.
- The proxy determines if the request is valid (by comparing it to any rules or filters) and then sends a new request on behalf of the client to the destination.



- By using this method, a direct connection is never made from the trusted network to the entrusted network and the request appears to have originated from the application gateway/proxy.

(continue……)

- **Advantages of Application gateways / proxy servers**

1. Application gateways/proxies do not allow a direct connection to be made between endpoints.
2. Typically have the best content filtering capabilities.
3. Allow the network administrator to have more control over traffic passing through the firewall.

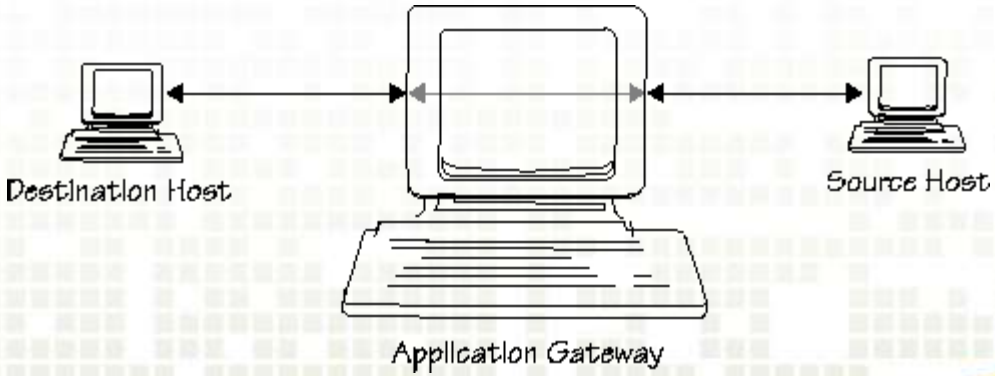
- **Disadvantages of Application gateways / proxy servers:**

1. The most significant weakness is the impact they can have on performance.
2. it requires more processing power and has the potential to become a bottleneck for the network.
3. Typically require additional client configuration.

(continue……)

3.Circuit level gateways

- Unlike a packet filtering firewall, a circuit-level gateway does not examine individual packets. Instead, circuit-level gateways monitor TCP or UDP sessions.
- Once a session has been established, it leaves the port open to allow all other packets belonging to that session to pass. The port is closed when the session is terminated.
- circuit-level gateways operate at the transport layer (layer 4) of the OSI model.



(continue……)

Advantages of Circuit level gateways

- Circuit level gateways are relatively inexpensive and have the advantage of hiding information about the private network they protect. On the other hand, they do not filter individual packets.

Disadvantages of Circuit level gateways

- The circuit level gateway does not permit end-to-end TCP connection but two TCP connections are set-up.
- A typical use of circuit level gateway is in situation when system administrator trusts the internal users.

9.Comparison packet filter and proxies

Sr no.	Packet filter	Proxy (application level)
1.	Works at network layer of OSI and IP layer of TCP.	Works at application layer of OSI , TCP of TCP.
2.	Low impact on network performance.	High impact on network performance.
3.	Low level security as compare to proxy.	High level of security
4.	Packet filtering is not effective with the FTP protocol.	FTP and Telnet are allowed into the protected subnet.
5.	Simple level of security and faster than proxy firewall.	Capability to examine the traffic in detail, so slower then packet filtering.
6.	Normally transparent to the users.	Not transparent to the users.
7.	Difficult to configure as compare to proxy.	Easier to configure as compare to packet filtering.
8.	They can not hide the private network topology.	They can hide the private network topology.

(continue……)

10.Features of firewall

- Firewall technology will continue to change
  - Increased operational change
  - More user aware
  - Increased role of endpoint machines, but centralized firewalls provide layered security
  - IPv6 roll out may leverage firewalls as quick fix points
- Integration with other technologies
  - Intrusion detection
  - Other scouring technologies
  - Encryption/authentication
- Obsolete by some technologies
  - End-to-end encryption – only basic filtering can be done

Trusted Systems

- The ability of the system can be enhanced to defend against intruders and malicious by implementing trusted system technology.
- A trusted system is a computer and operating system that can be verified to implement a given security policy.

Security policy:

- A "*security policy*" defines the security rules of a system.
- Without a defined security policy, there is no way to know what access is allowed or disallowed
- **An example policy: (simple)**
  - Allow all connections to the web server
  - Deny all other access

Application of web security

- Web application security is a branch of Information Security that deals specifically with security of websites, web applications and web services.
- At a high level, Web application security draws on the principles of application security but applies them specifically to Internet and Web systems.
- Typically web applications are developed using programming languages such as PHP, Java EE, Java, Python, Ruby, ASP.NET, C#, VB.NET or Classic ASP.

1.Security threats

2.Security standard

3.Security technology

Black Box

White Box

Password cracking

Conclusion

- The web is very visible. The WWW is widely used by:-
- Business, Government agencies and many individuals.
- The world wide web is fundamentally a client/server application running over the internet and TCP/IP intranets.
- The web is increasingly serving as a highly visible outlet for corporate and product information and as the platform for the business transactions.
- Reputations can be damaged and money can be lost if the web servers are subverted.
- A web server can be exploited as a launching pad into the corporation's or agency's entire computer complex.

Reference

http:// www.howstuffworks.com
http://www.microsoft.com
http://www.securityfocus.com
http://www.wikipediya.com
http://www.
http://www.kerio.com/us/supp_kpf_manual.html
http://www.broadbandreports.com/faq/security/2.5.1.
http://www.firewall-software.com

Stallings, W. (2003). Transport-level security, Firewalls In Cryptography & Network Security: Principles & Practices (pp. 616-635).

Any Queries ?

THANK YOU