CyberSecurity Strategy and Firewall:

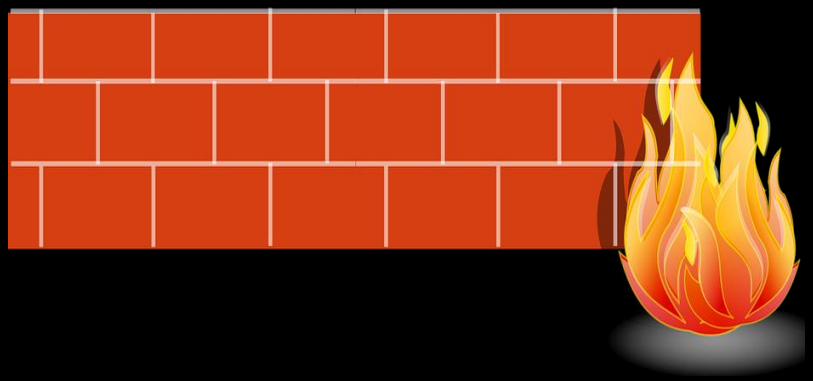
first line of defense against various threats.

د. محمد علاء حسين التميمي
قسم هندسة المعلومات والاتصالات
كلية الهندسة الخوارمي / جامعة بغداد
mohammed. alaa@kecbu.uobaghdad.edu.iq

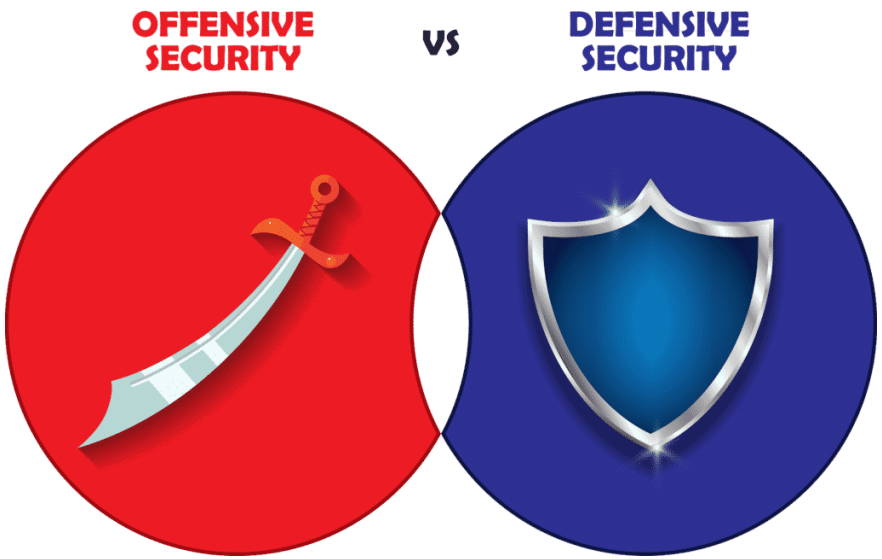
الثلاثاء 2-4-2024

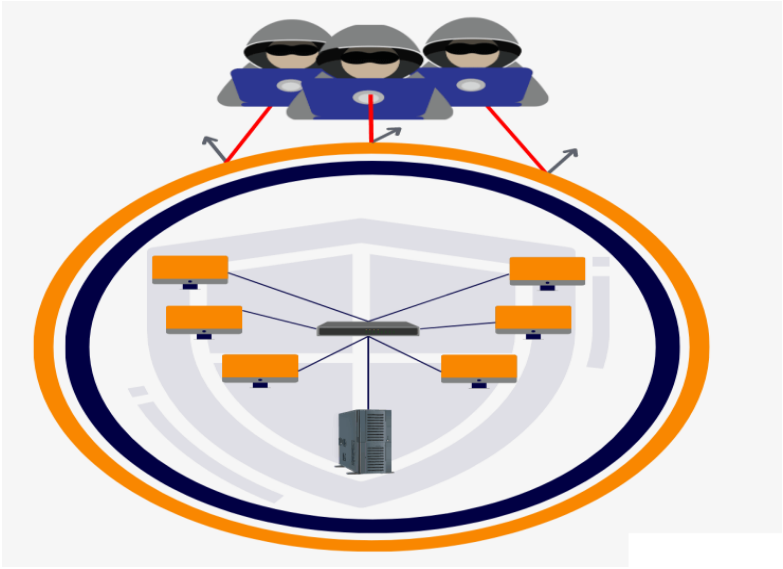
Outline

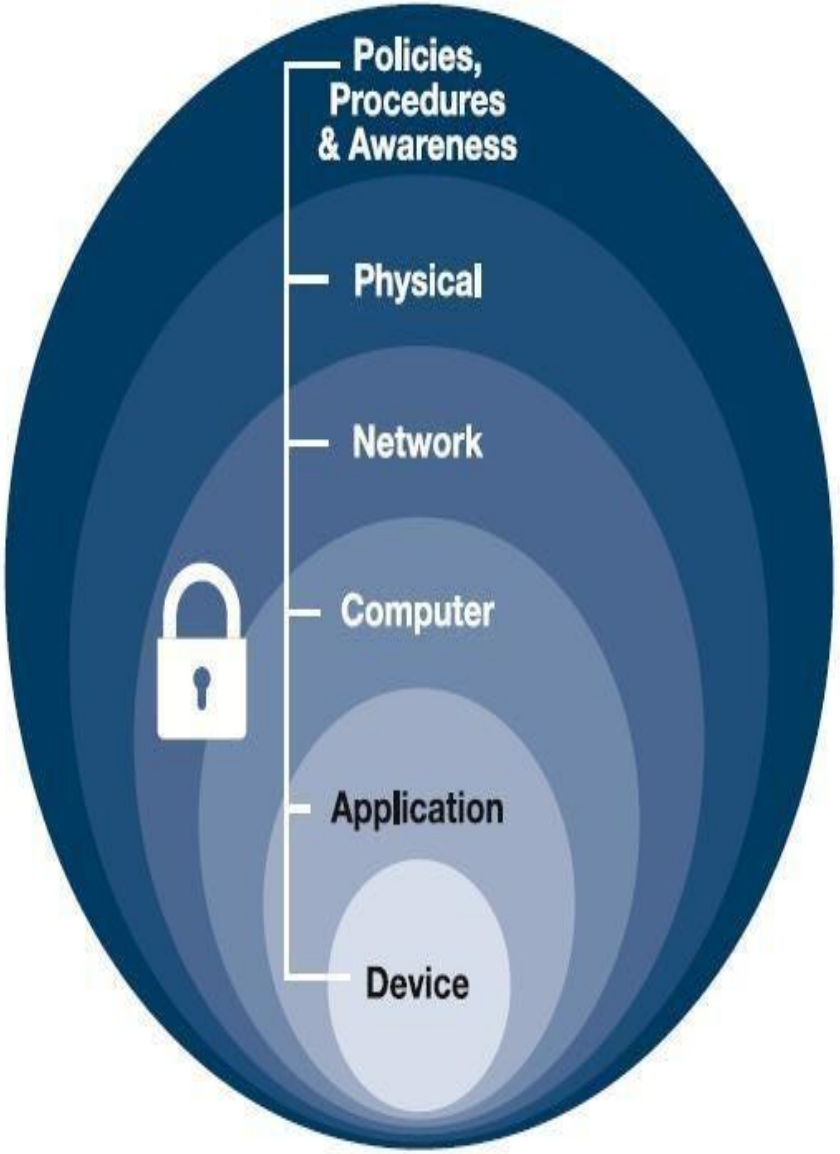
- Overview
- CyberSecurity and Firewall.
- Firewall Layer of Operation.
- Firewall Delivery Modes.
- Firewall Types.
- Advantages / Disadvantages.
- Conclusion.



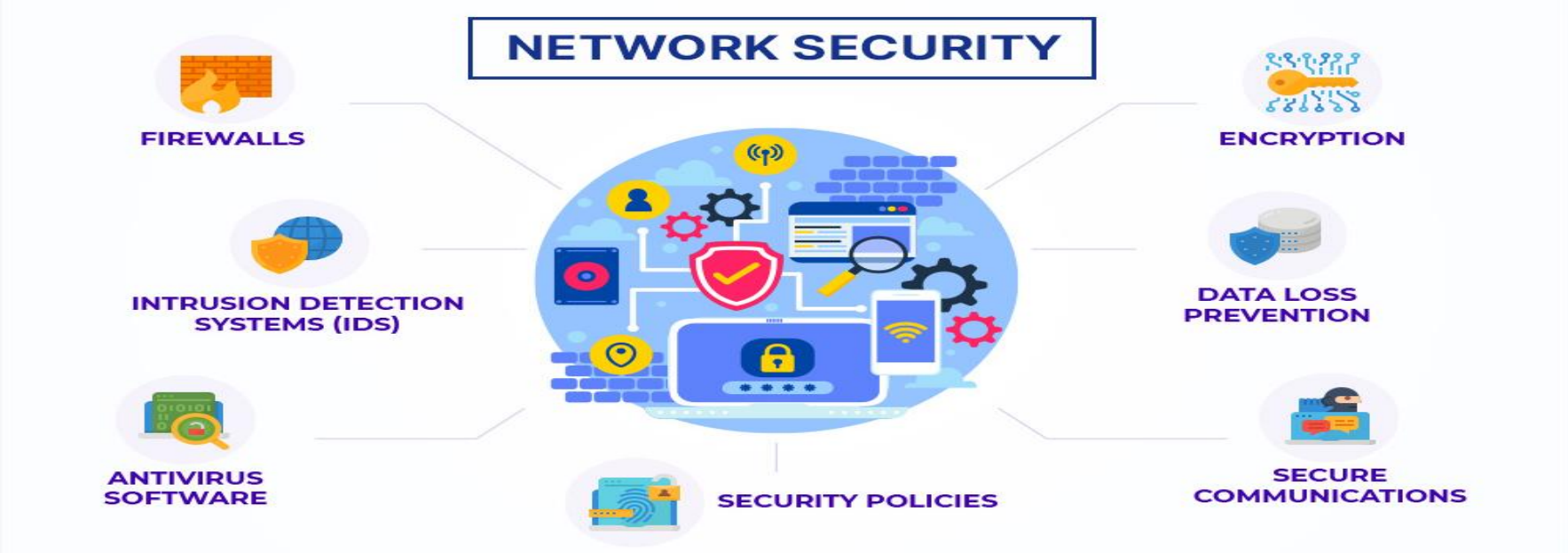
CyberSecurity







CyberSecurity



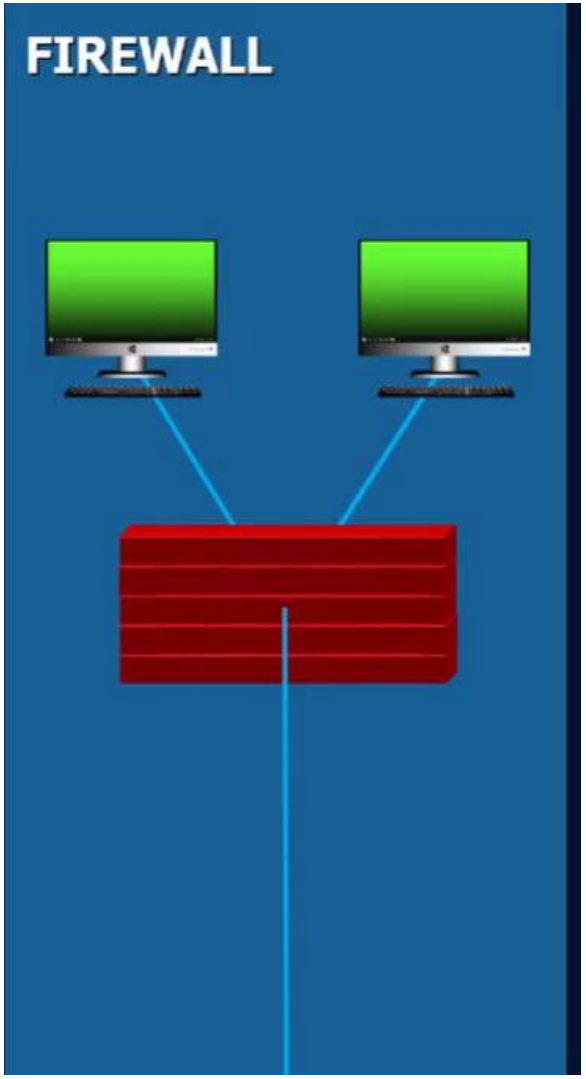
1. Network Segmentation
2. Firewall
3. Next-Generation Firewall
4. Data Loss Prevention
5. Hyperscale Network Security
6. Sandboxing
7. Intrusion Prevention Systems
8. Biometric System
9. Authentication
10. Email Security
11. Remote Access VPN

Overview of firewall

- The Internet has made large amount of information and vast of transfer data over network and internet. Therefore, security of network is the main criteria here and firewalls provide this security.

- Firewalls are a key component of network security and will remain as one of the fundamental areas of cybersecurity.

- Firewalls are an essential part of any cybersecurity strategy. They act as a barrier between your computer network and the internet, filtering incoming and outgoing traffic.



- Firewall technology began to emerge in the late 1980s.
- 1988 by Jeff Mogul from Digital Equipment Corp. which he developed filter systems know as packet filter firewalls. The early firewalls were simple packet filters that analyzed the packets of data that were sent over the network. Packet filtering firewalls are still in use today, although they have evolved significantly. Since then, firewalls have evolved in response to the growing variety of threats:

- **Generation 1 firewalls—antivirus protection**: These consisted of antivirus protections designed to stem the proliferation of viruses invading PCs in the 1980s.
- **Generation 2 firewalls—network protection**: In the mid-1990s, physical firewalls had to be created to protect networks.
- **Generation 3 firewalls—applications**: In the early 2000s, firewalls were developed to address vulnerabilities in applications.
- **Generation 4 firewalls—payload**: These firewalls, developed around 2010, were designed to address evasive and polymorphic attacks.
- **Generation 5 firewalls—large-scale protection**: Around 2017, large-scale attacks using new and more complex methods necessitated advanced threat detection and prevention solutions.

History of Firewalls

1 **Generation 1 firewalls antivirus protection:**

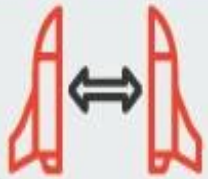
These consisted of antivirus protections designed to stem the proliferation of viruses invading PCs in the 1980s.

2 **Generation 2 firewalls network protection:**

In the mid-1990s, physical firewalls had to be created to protect networks.

3 **Generation 3 firewalls applications:**

In the early 2000s, firewalls were developed to address vulnerabilities in applications.



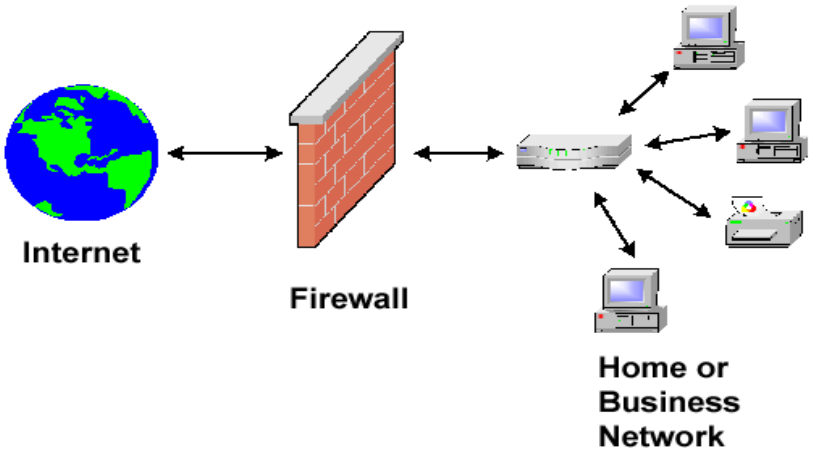
4 **Generation 4 firewalls payload:**

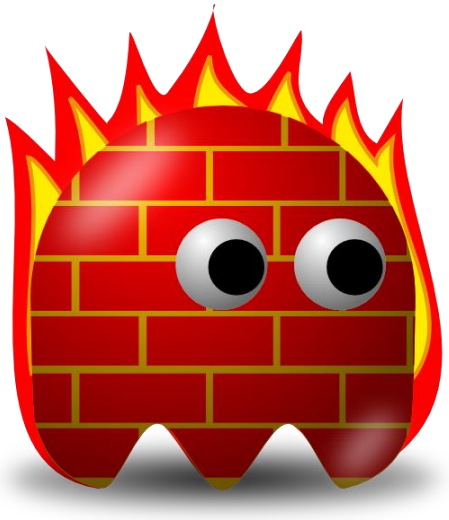
These firewalls, developed around 2010, were designed to address evasive and polymorphic attacks.

5 **Generation 5 firewalls large-scale protection:**

Around 2017, large-scale attacks using new and more complex methods necessitated advanced threat detection and prevention solutions."

- A Firewall is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.





Example Rule

- `allow tcp connection 4.5.5.4:* -> 3.1.1.2:80`
  - Firewall should permit TCP connection that's:
    - Initiated by host with Internet address 4.5.5.4 and
    - Connecting to port 80 of host with IP address 3.1.1.2
  - Firewall should permit any packet associated with this connection
- Thus, firewall keeps a table of active connections. When firewall sees a packet, it checks whether it is part of one of those table. If yes, forward it; if no, drop it / check to see if rule create a new connection.

Port Numbers

- The Well Known Ports are those from 0 through 1023.
- The Registered Ports are those from 1024 through 49151.
- The Dynamic and/or Private Ports are those from 49152 through 65535.

Well-know TCP / UDP ports

TCP Port Number	Description
20	FTP (Data Channel)
21	FTP (Control Channel)
23	Telnet
80	HTTP)used for the World Wide Web
139	NetBIOS session service

UDP Port Number	Description
53	Domain Name System (DNS) Name Queries
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS name service
138	NetBIOS datagram service
161	Simple Network Management Protocol (SNMP)

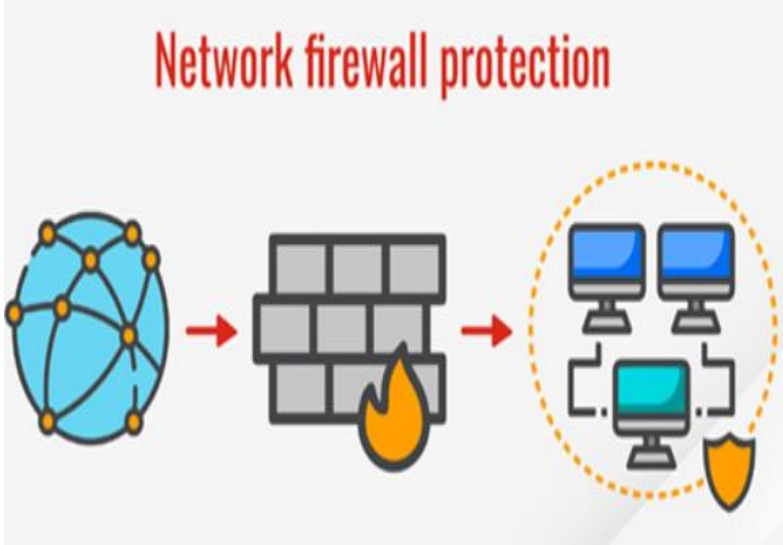
Firewall Layer of Operation

- **A host-based firewall**

is installed on an individual pc to protect it from activity occurring on its network. In other words, hosts running proxy servers which perform logging and auditing of traffic through the network.

- **A network-based firewall**

➢ is a network device protects all computers on the "internal" side from all computers on the "external" side. In other words, Makes decision based on the source, destination addresses, and ports in individual IP packets. Also, Has the ability to perform static and dynamic packet filtering and stateful inspection. Example, Static & Dynamic Filtering or Stateful Inspection.

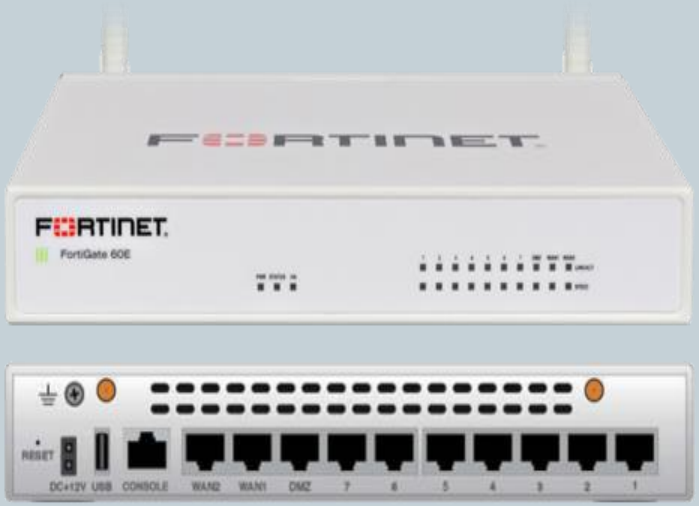


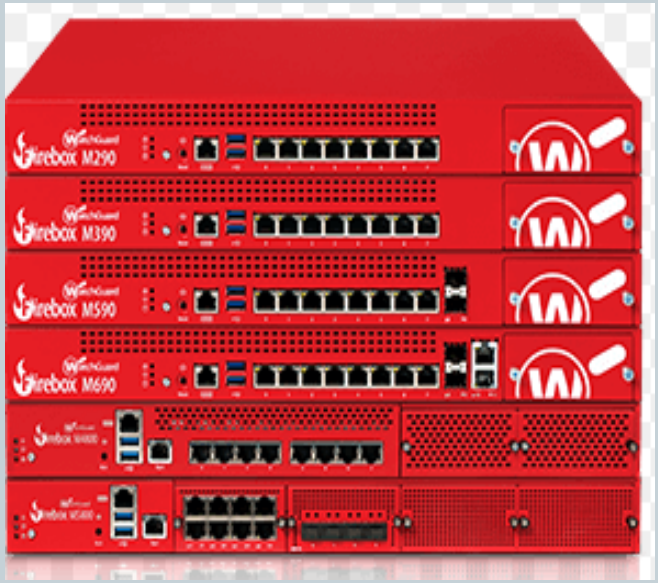
Firewall Delivery Mode

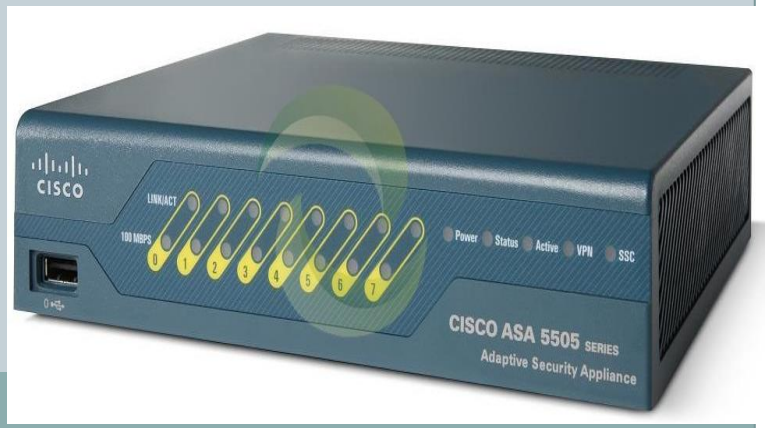
- There are 3 main delivery types: hardware-based, software-based, and cloud-based firewalls (also known as Firewall-as-a-Service or FWaaS).

Fig: Firewall blocking Bad Traffic

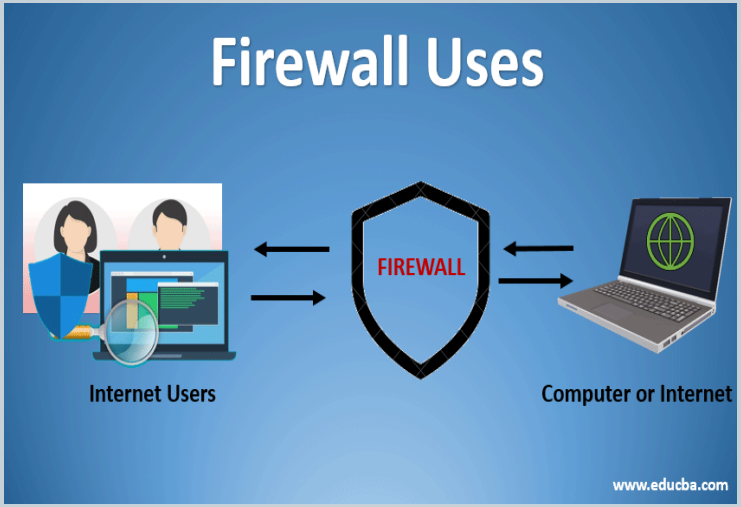
- **Hardware firewalls** is a physical appliance that is deployed to enforce a network boundary.





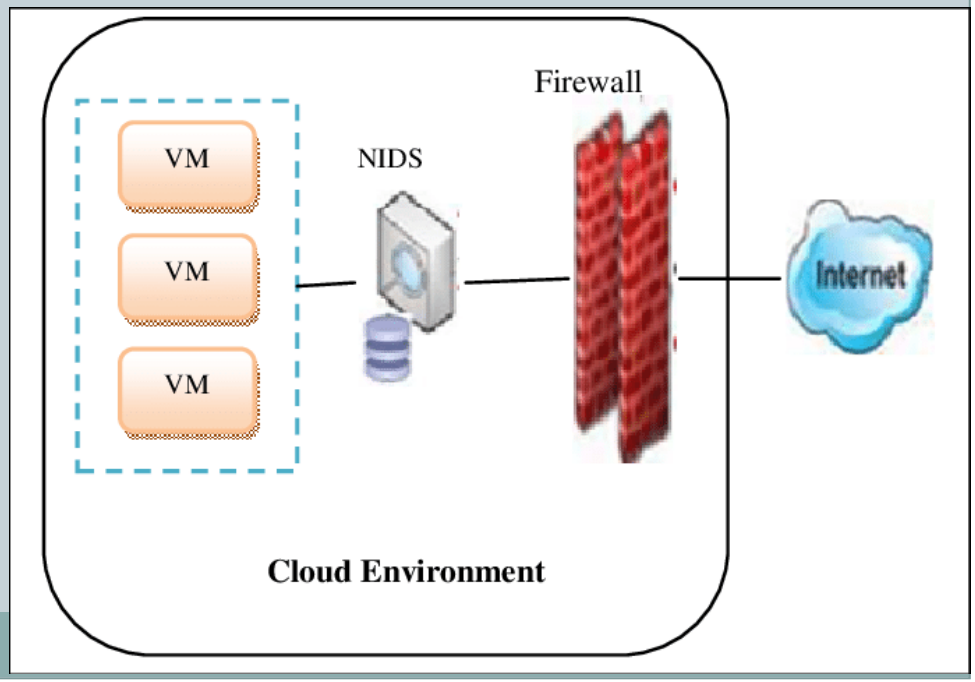


- **Software firewalls** is a program used by a computer to inspect data that goes in and out of the device. It can be customized by the user to meet their needs. It installed on individual pc/servers. They intercept each connection request & then determine whether the request is valid / not.



- **Cloud based firewalls** is cloud firewalls are security products that filter out potentially malicious network traffic.

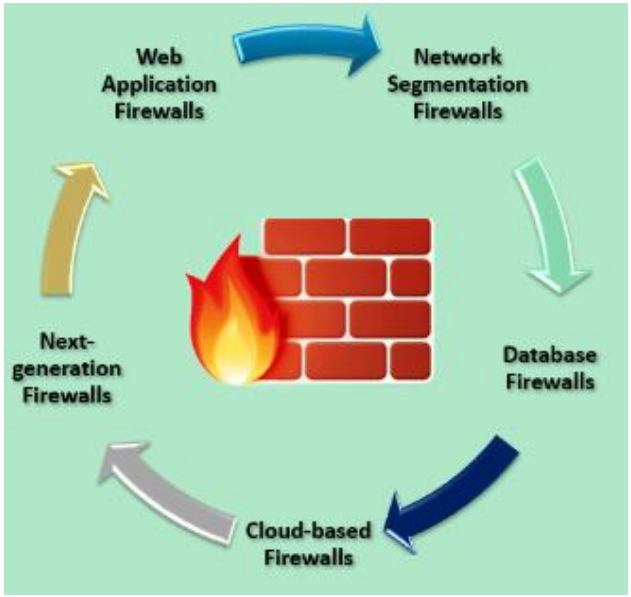
- The difference is that cloud firewalls are hosted in the cloud and provided as a service by security vendors. This cloud-delivered model for firewalls is also called firewall-as-a-service (FWaaS). Cloud-based firewalls can be used to create virtual barriers around cloud platforms, infrastructure, and applications. A cloud firewall can also protect on-premises infrastructure, but this requires routing of traffic between cloud and on-premise environments.



Firewall Types

Firewalls fall into many broad categories

- ❑ Packet Inspection Firewalls
- ❑ Circuit level
- ❑ Application Proxy Server: Filtering Based on Known Services
- ❑ Virtual Private Network (VPN) Firewalls
- ❑ Small Office or Home (SOHO) Firewalls
- ❑ Stateful multilayer
- ❑ Next generation of Firewall



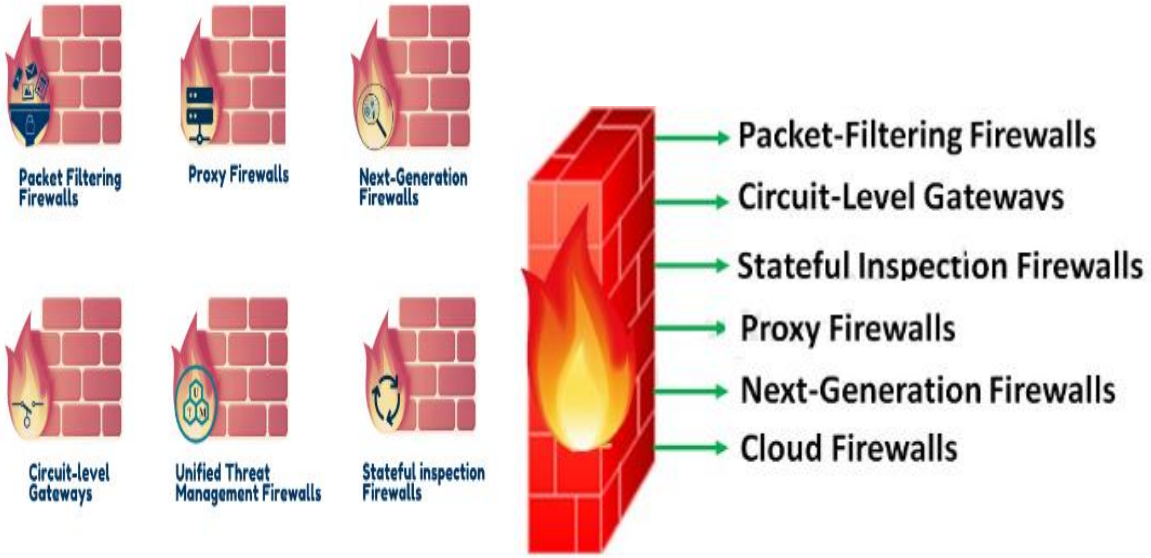
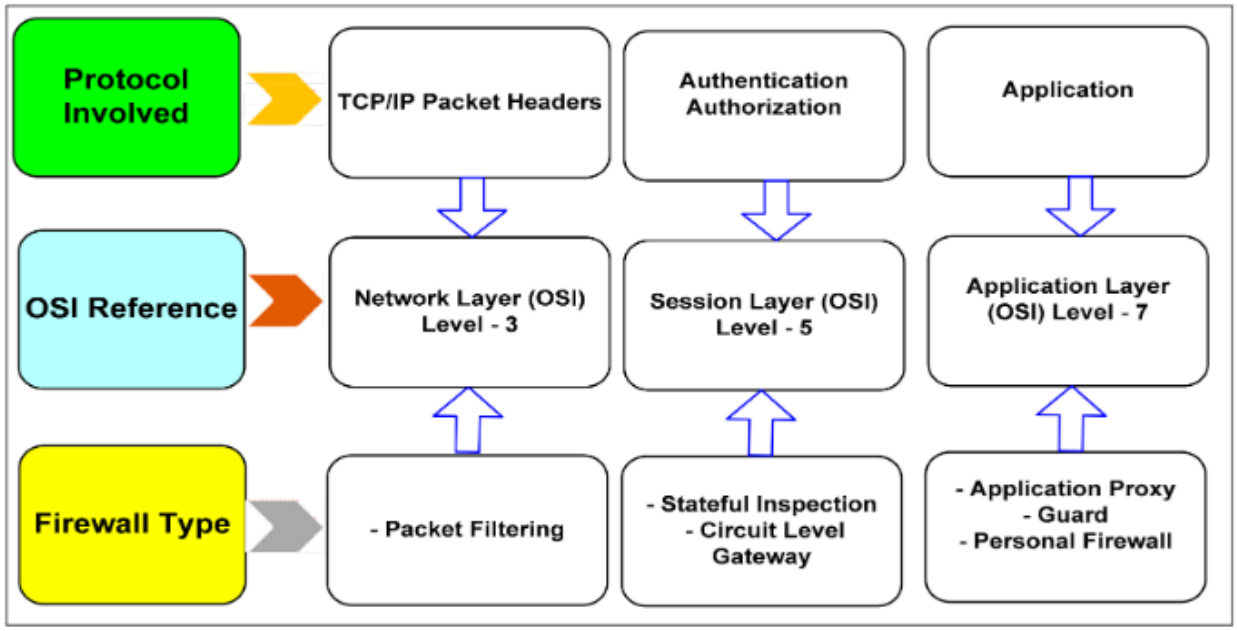
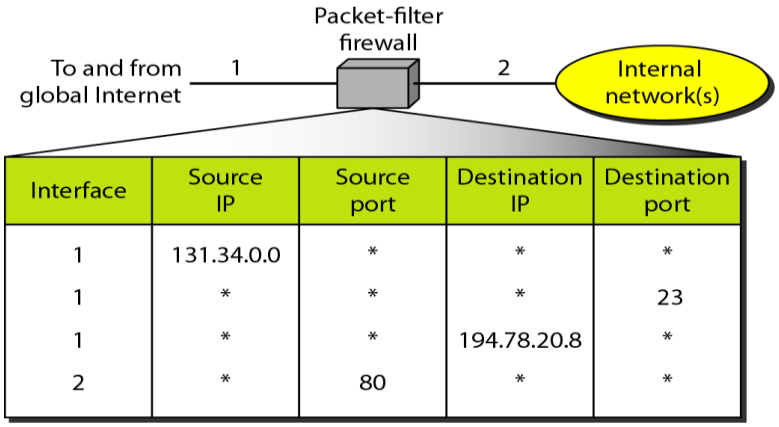


Figure . Firewall practice and level of controls according to the OSI reference model.

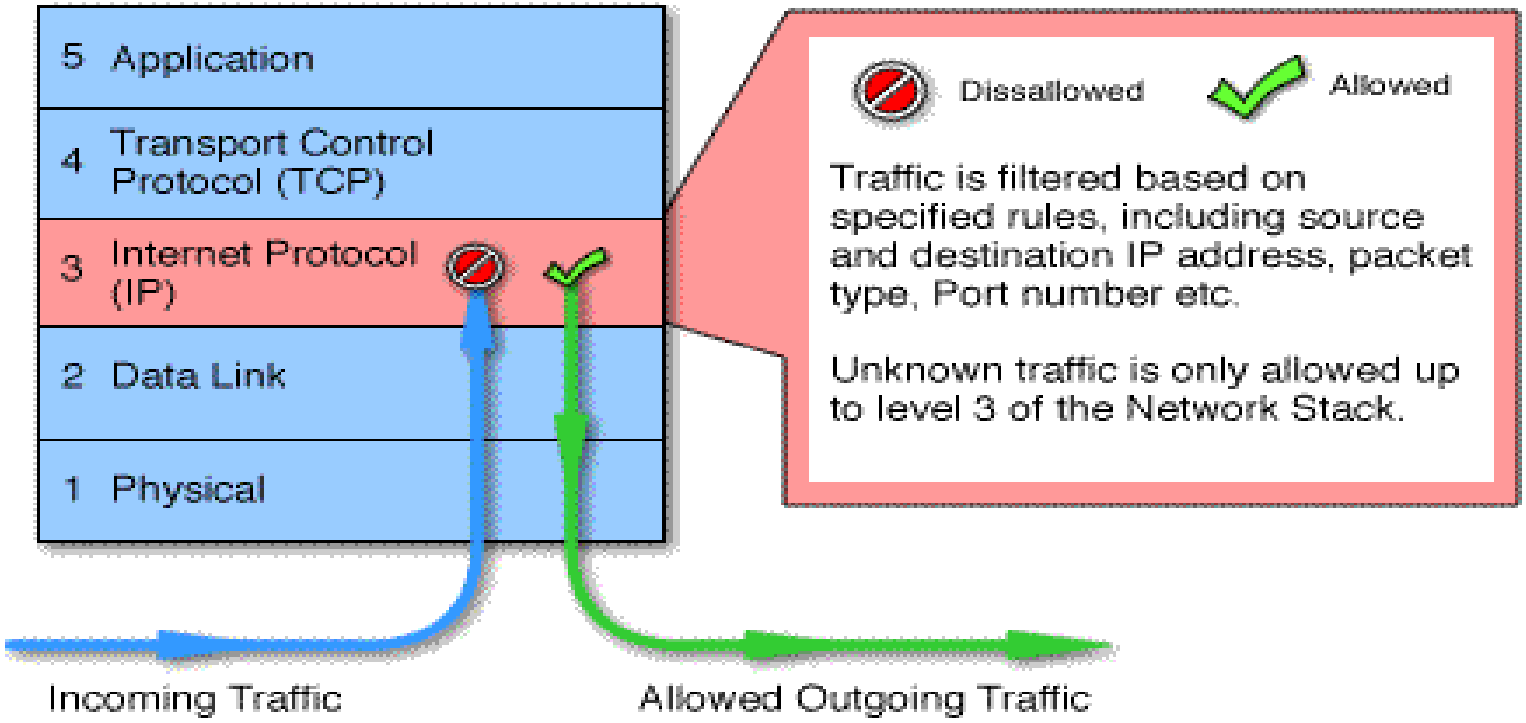


Packet Filtering

- Packet filtering firewalls is low cost and low impact on network performance.
- Work at the network level of the OSI model.



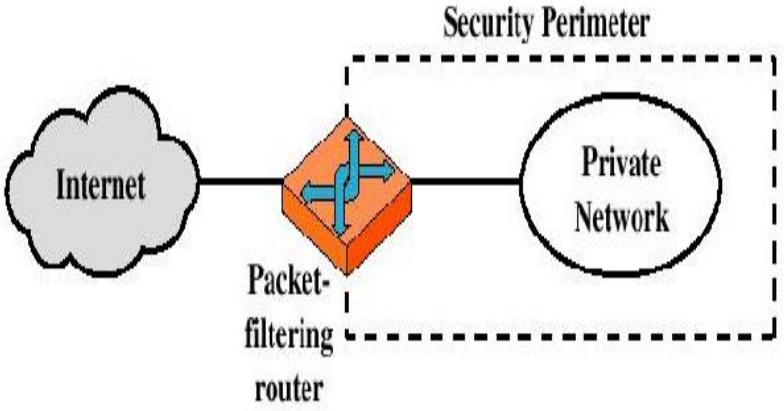
Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*



Two types of packet filtering are used during packet inspection: *static or stateless*

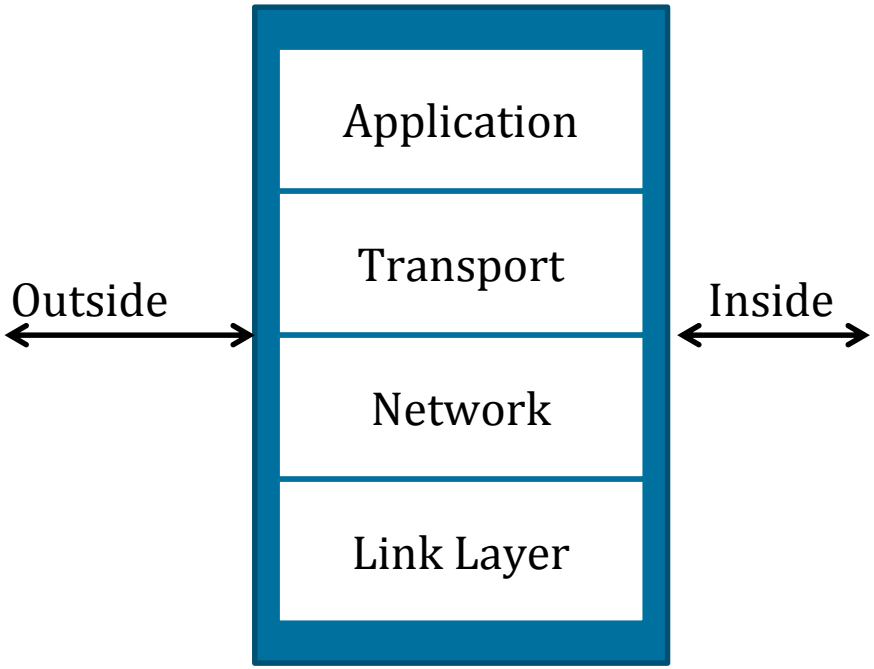
- The static or stateless filtering is a full-duplex communication bastion server allowing two-way communication based on strict filtering rules.
- The static *filtering* in which a packet is filtered in isolation of the context it is in, and stateful filtering in which a packet is filtered actually based on the context the packet is in. The trend now for most inspection firewalls is to use stateful filtering.

- Whether static or stateful, the rules a filtering server follows are defined based on the organization's network security policy, and they are based on the following information in the packet:
  - Source address
  - Destination address
  - Address internal to the network.
  - ICMP message type.
  - Payload data type.
  - TCP or UDP source and destination port number.
  - Connection initialization and datagram using TCP ACK bit.



Stateless Firewall

e.g., ipchains in Linux 2.2



Firewall

Filter by packet header fields

1. IP Field
   (e.g., src, dst)
2. Protocol
   (e.g., TCP, UDP, ...)
3. Flags
   (e.g., SYN, ACK)

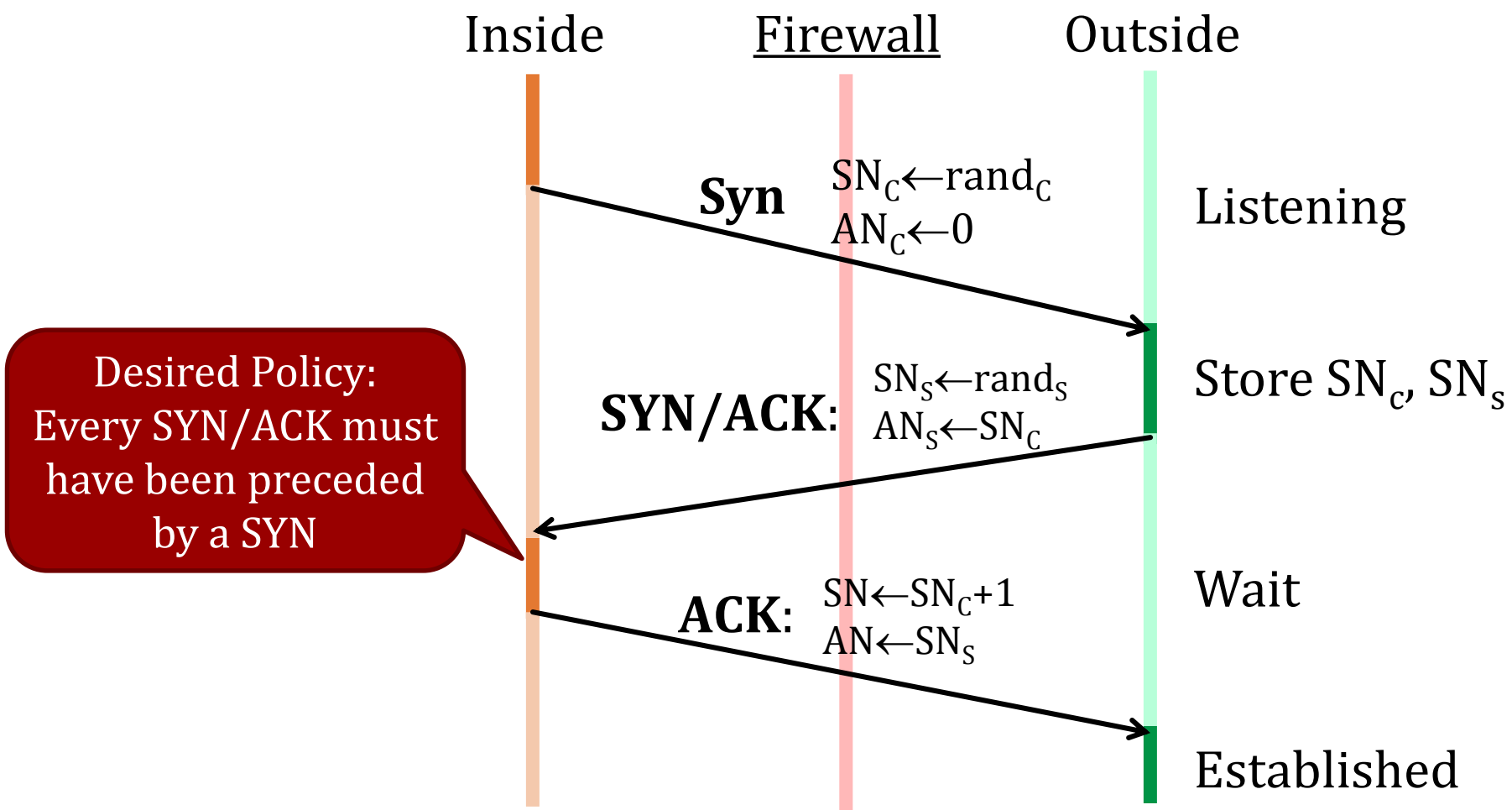
Example: only allow incoming DNS packets to nameserver A.A.A.A.

Allow UDP port 53 to A.A.A.A
Deny UDP port 53 all

Fail-safe good practice

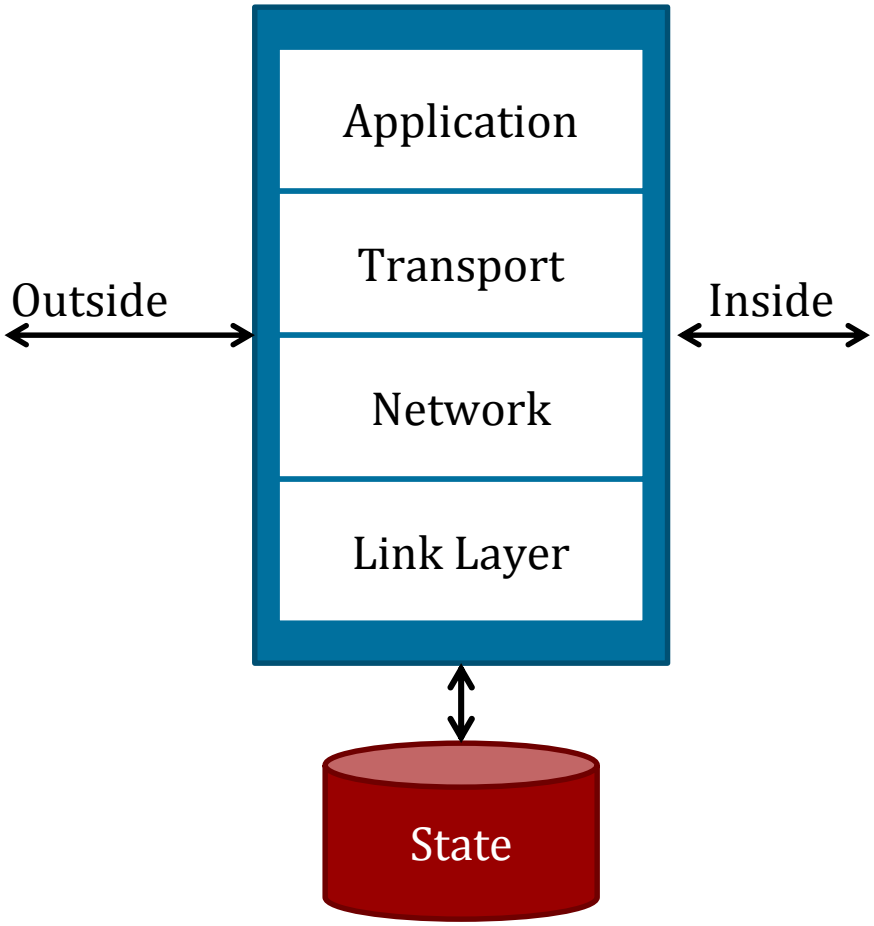
Need to keep state

Example: TCP Handshake



Stateful Inspection Firewall

e.g., iptables in Linux 2.4

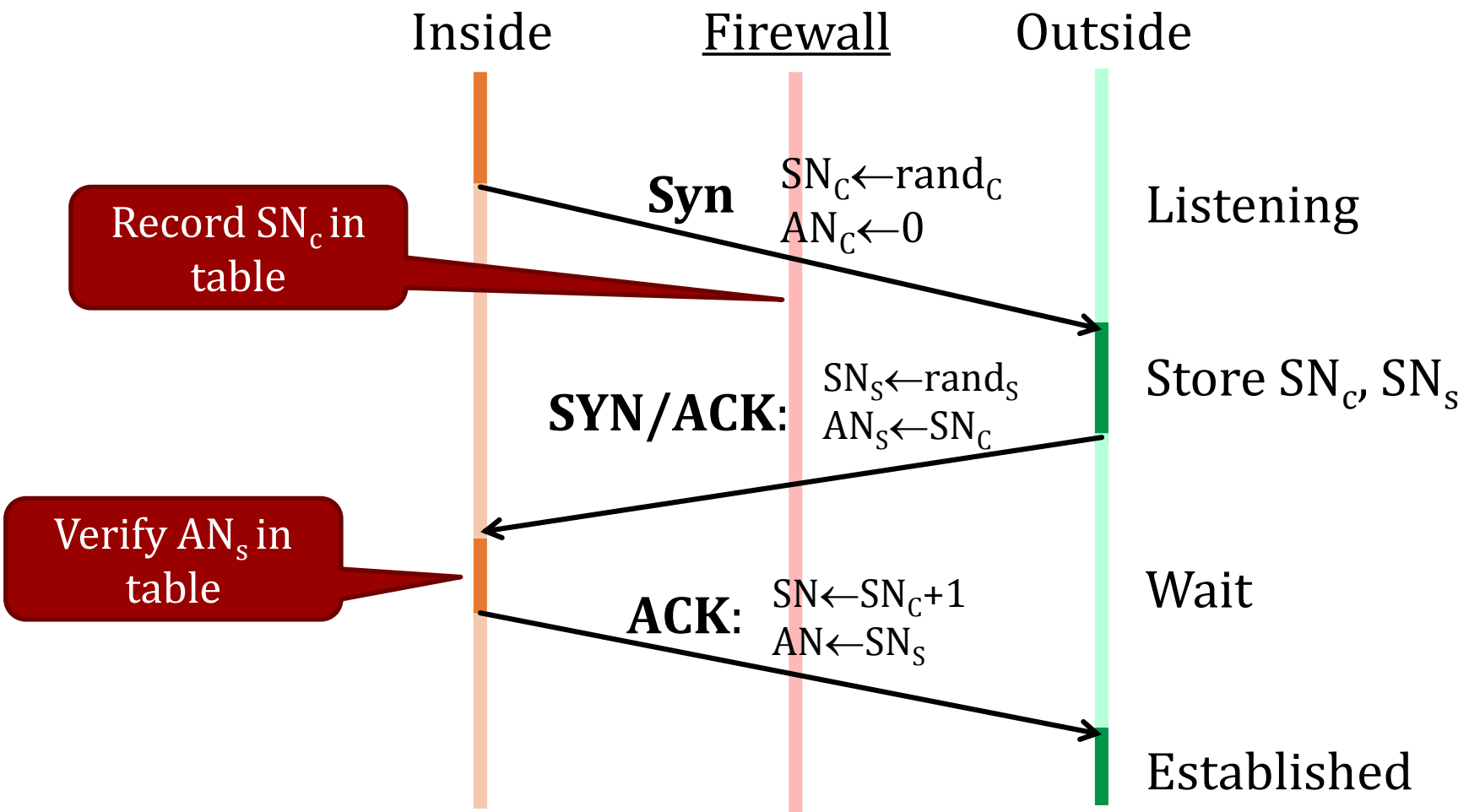


Added state
(plus *obligation* to manage)

- Timeouts
- Size of table

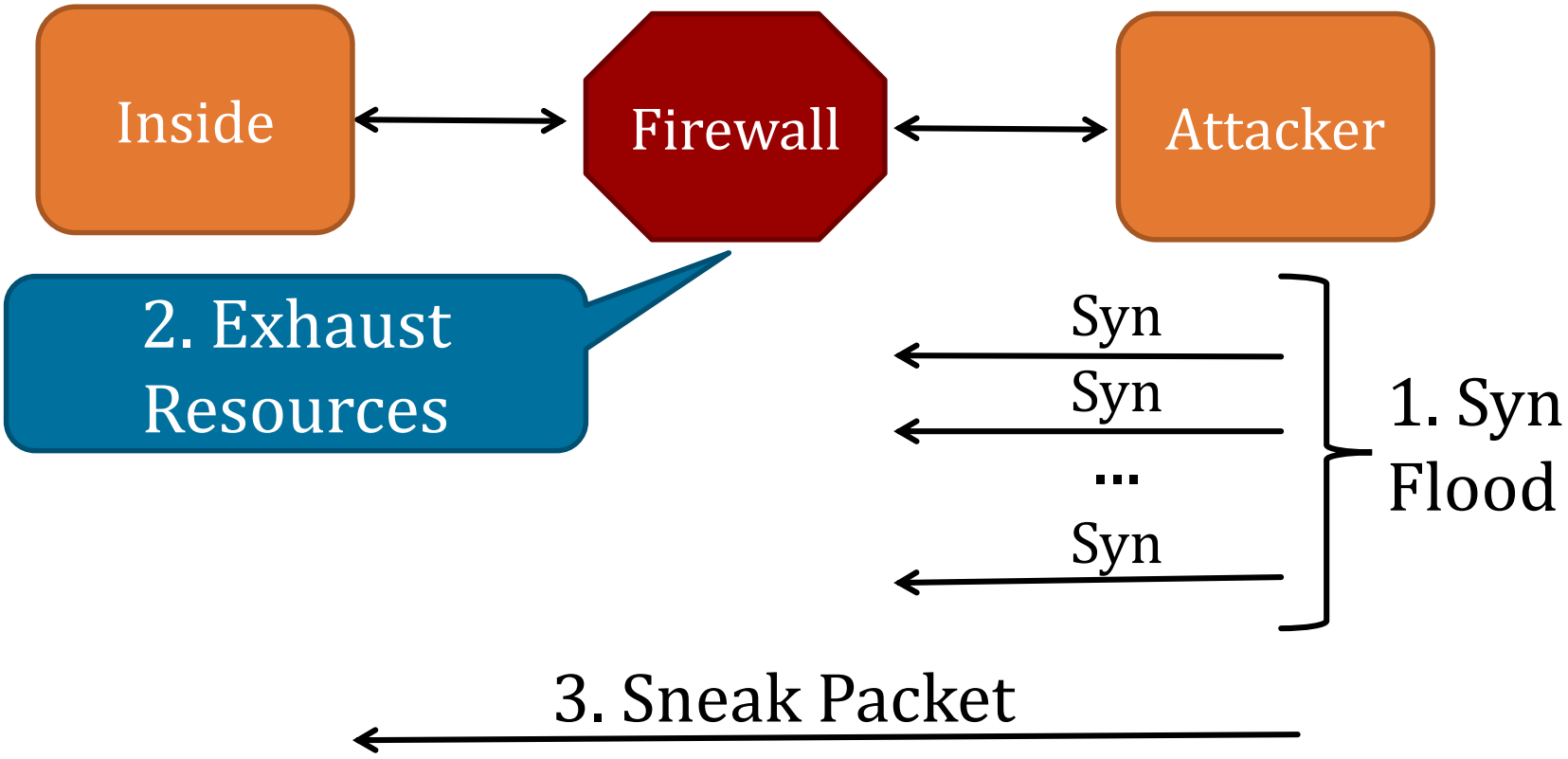
Stateful More Expressive

Example: TCP Handshake



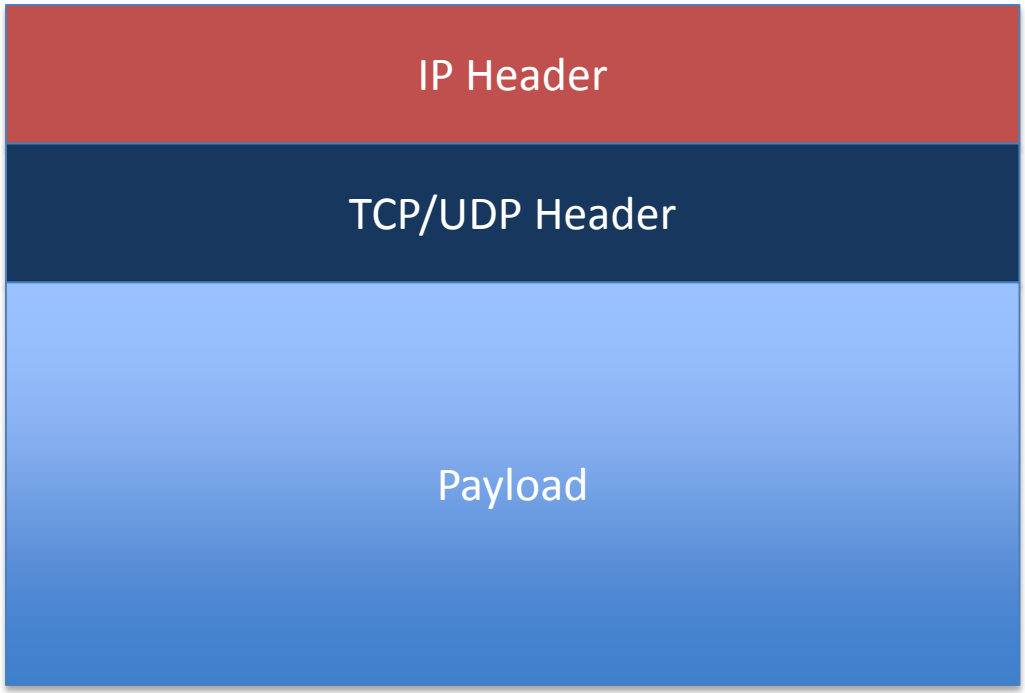
State Holding Attack

Assume stateful TCP policy



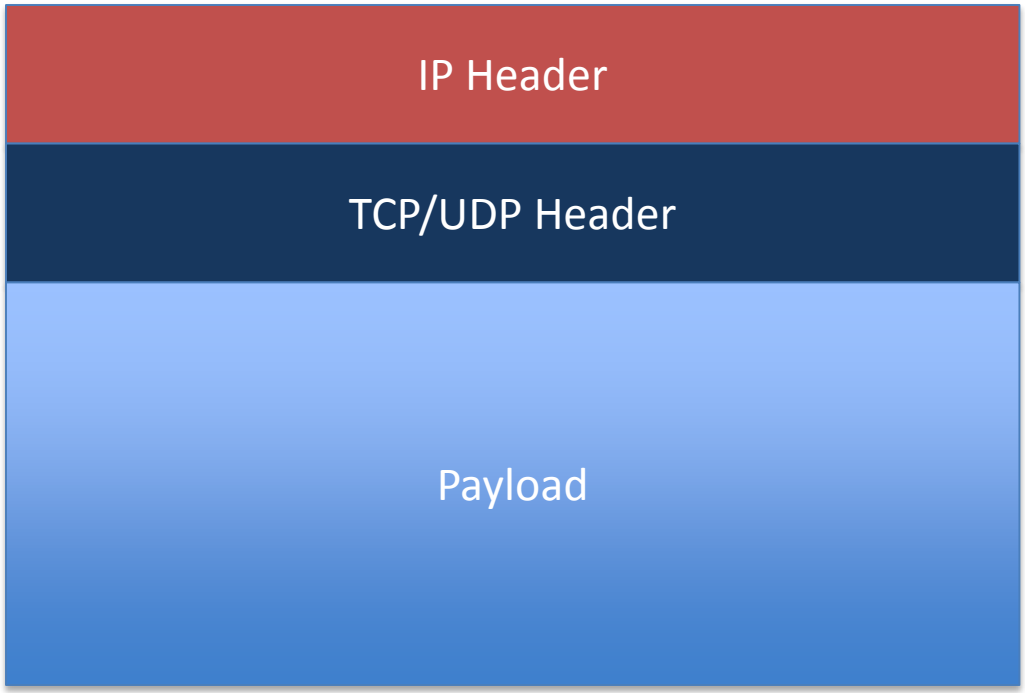
Deep Packet Inspection

- Examine payload (data) portion of packet as well as headers

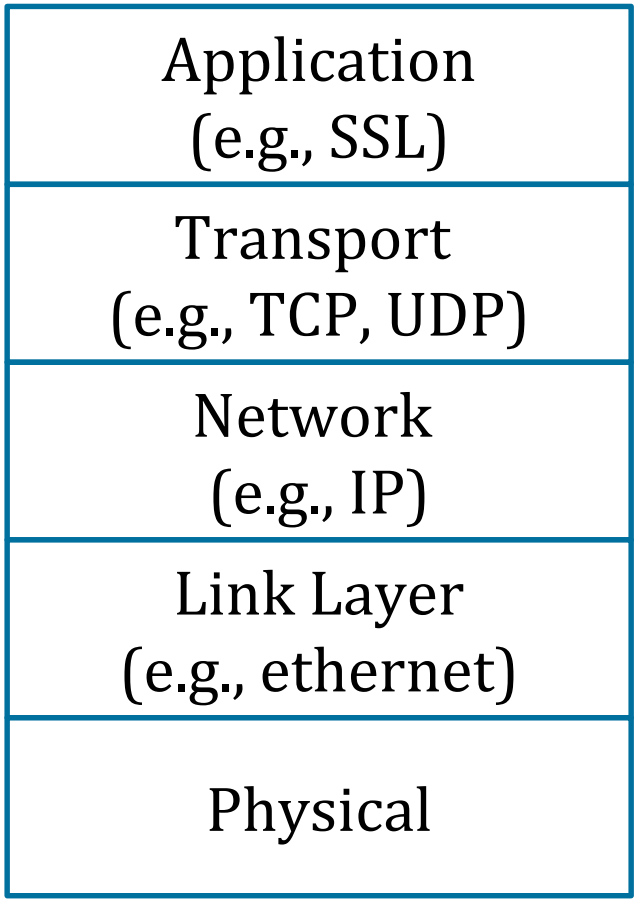


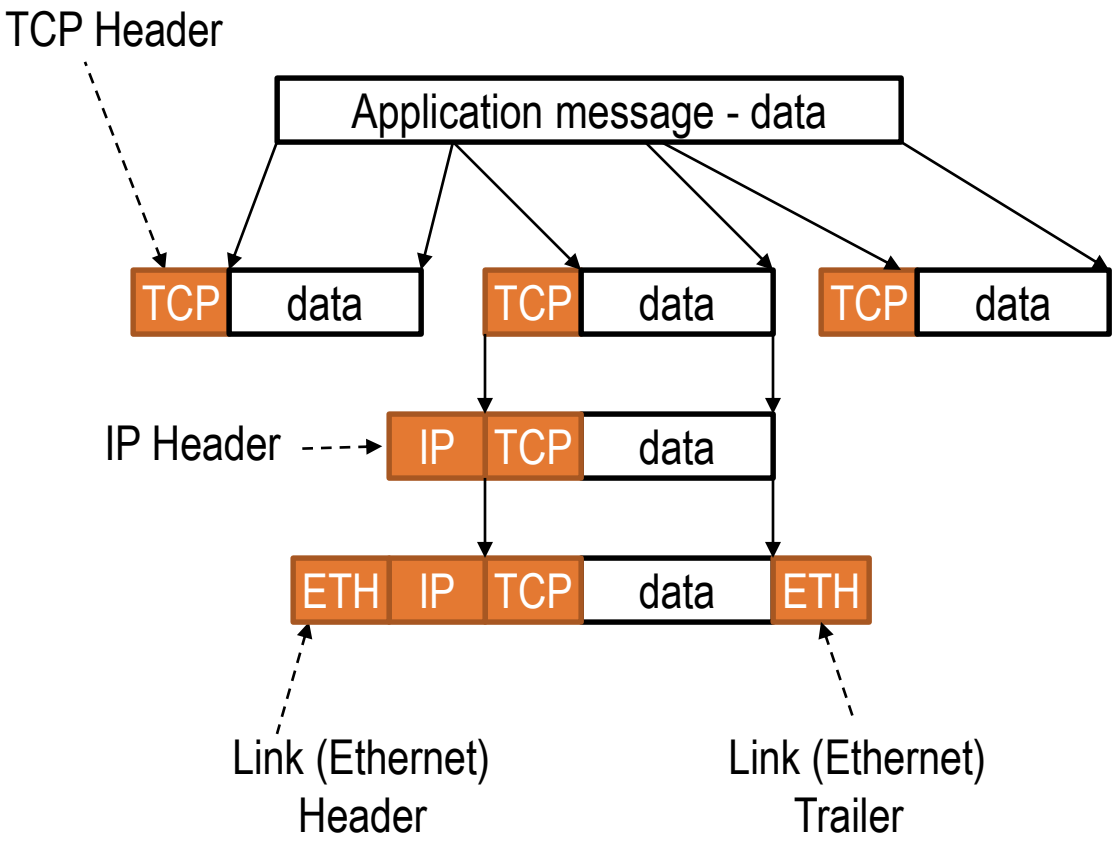
Deep Packet Inspection

- Examine payload (data) portion of packet as well as headers



Recall: Protocol Stack





- **IP Address Filtering**

Table Destination IP filtering

Application protocol	Source IP	Destination IP	Action
HTTP	Any	198.124.1.0	Allow
Telnet	Any	198.213.1.1	Deny
FTP	Any	198.142.0.2	Allow

- **TCP and UDP Port Filtering**

Table Filtering rules based on TCP and UDP destination port numbers

Application	Protocol	Destination port number	Action
HTTP	TCP	80	Allow
SSL	UDP	443	Deny
Telnet	TCP	23	Allow

- **Packet Filtering Based on Initial Sequence Numbers (ISNs) & Acknowledgment (ACK) Bits**

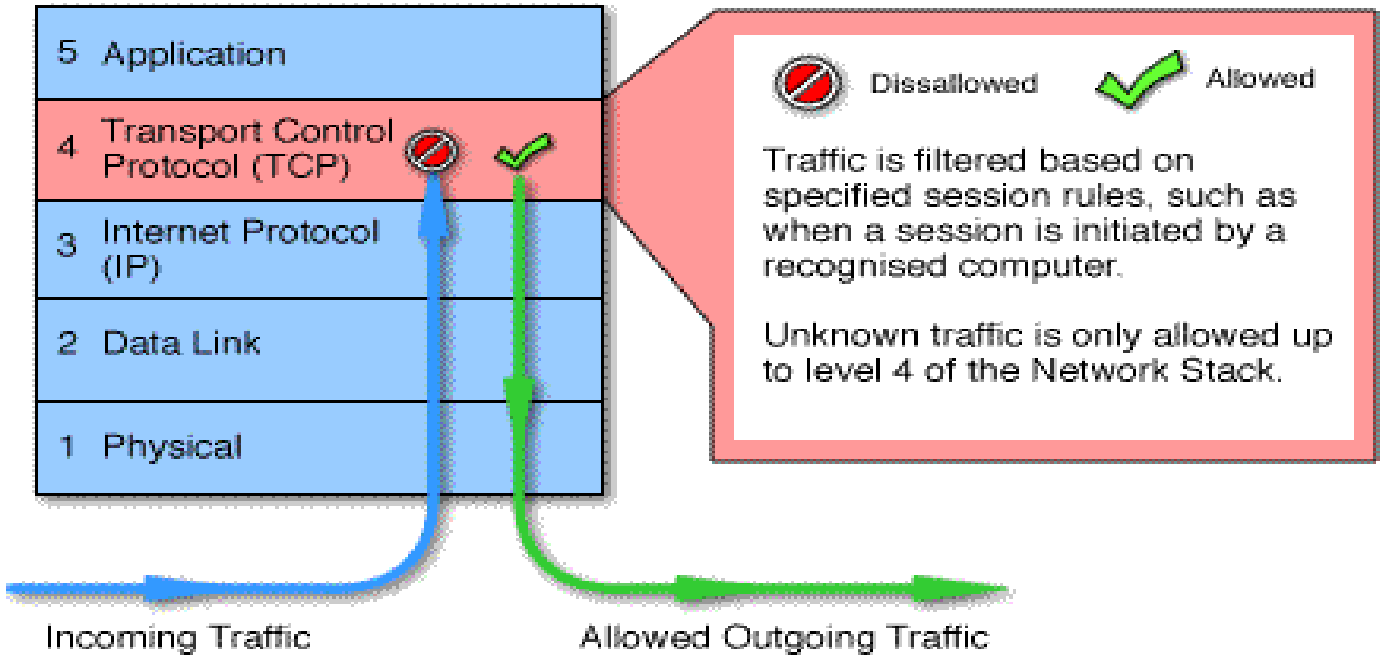
Table Rules for filtering based on ACK field bit

Sequence number	IP Destination address	Port number	ACK	Action
15	198.123.0.1	80	0	Deny
16	198.024.1.1	80	1	Allow

A packet-filter firewall filters at the network or transport layer.

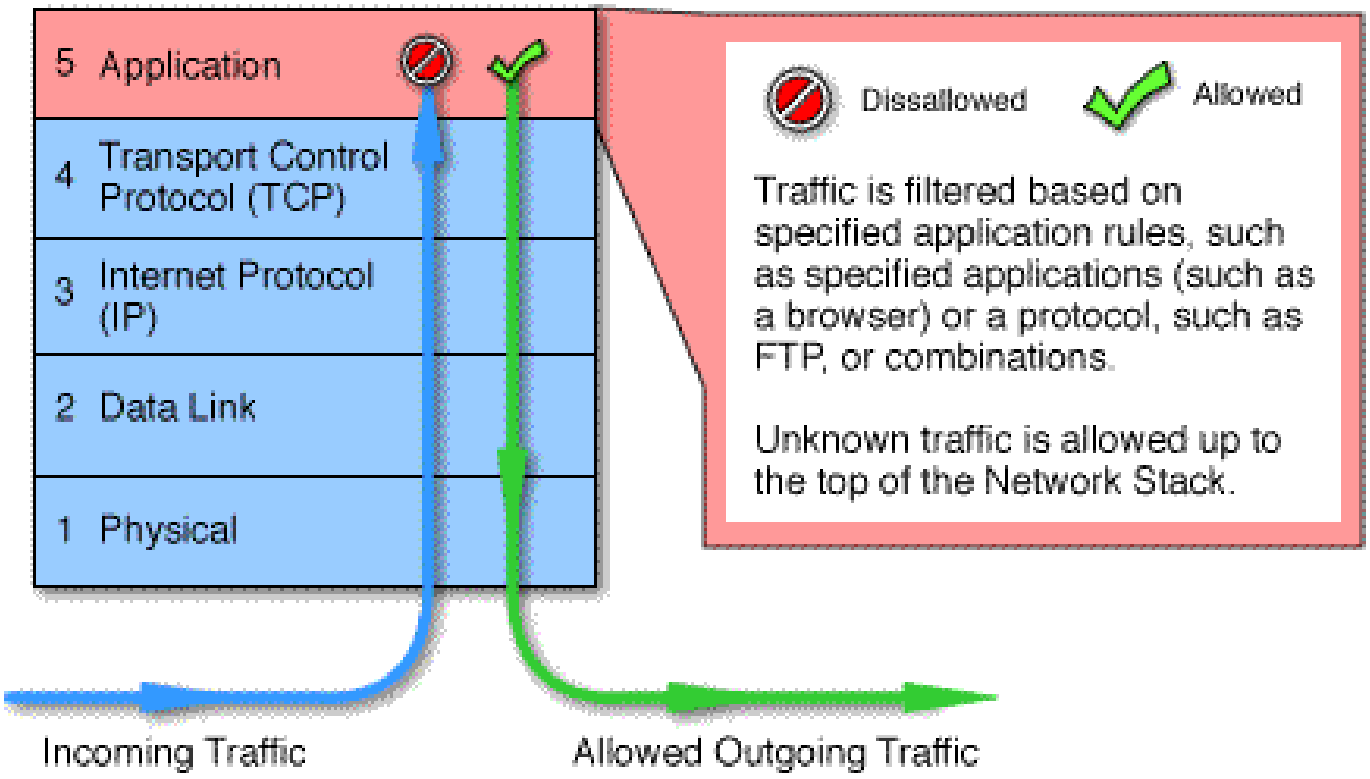
Circuit Level

- Circuit level gateways is Stand-alone system or Specialized function performed by an Application-level Gateway. Its work at the session layer of the OSI model, or the TCP layer of TCP/IP
- Monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- The security function consists of determining which connections will be allowed



Application Level

- Application level gateways, also called proxies, are similar to circuit-level gateways except that they are application specific
- Gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through.



- An example of a proxy server is a Web application firewall server.
- A **WAF** or **web application firewall** helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

- applications are filtered based on their port numbers as below:
  - HTTP (port 80)
  - FTP (port 20 and 21)
  - SSL (port 443)
  - Gopher (port 70)
  - Telnet (port 23)
  - Mail (port 25)

- For newer application firewall, the following proxies are also included: HTTP/ Secure HTTP, FTP, SSL, Gopher, email, telnet, and others. This works for both incoming and outgoing requests.

A proxy firewall filters at the application layer.

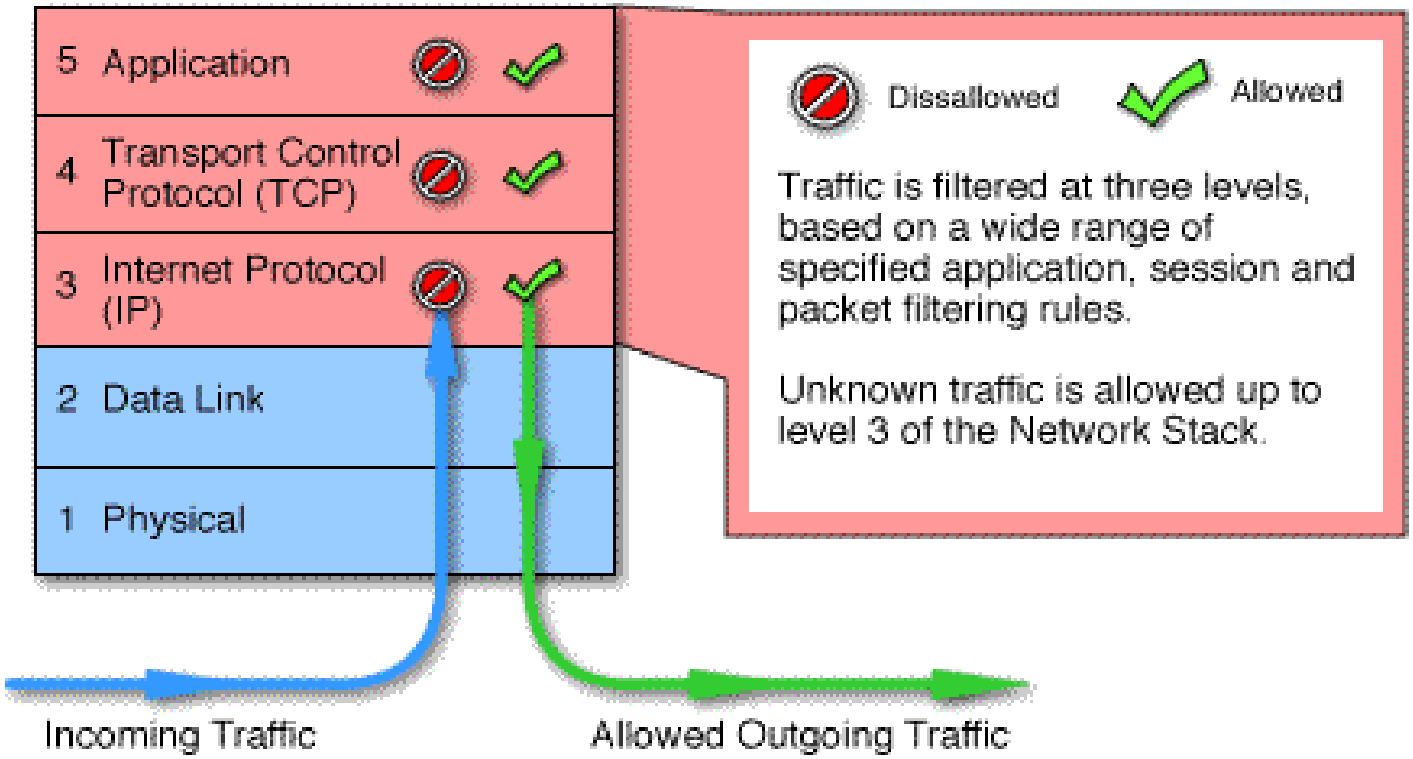
VPN Firewall

- **VPN firewall** is a type of firewall device used to prevent harmful or unauthorized users from accessing or exploiting VPN connections.

- VPN firewall is a cryptographic system including Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and IPSec that carry Point-to-Point Protocol (PPP) frames across an Internet with multiple data links with added security.

Stateful Multilayer

- Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls.
- They filter packets at the network layer, determine whether session packets are legitimate and evaluate contents of packets at the application layer



Next-generation of firewalls

- A next-generation firewall (NGFW) is the only type of firewall that provides the capabilities to protect modern businesses against emerging cyberthreats. As malware and threats have become more difficult to detect at the access point, NGFW security has evolved to span the network and monitor behavior and intent.

- NGFWs provide functions like deep-packet inspection, intrusion prevention (IPS), advanced malware detection, application control, and provide overall network visibility through inspection of encrypted traffic. They can be found anywhere from an on-premises network edge to its internal boundaries, and can also be employed on public or private cloud networks.

- NGFWs CPU-intensive capabilities include decryption at a very high-performance level, deep-packet inspection post decryption, detection of malicious URLs, identification of command-and-control activities, and download of malware and threat correlation.

- Firewall is changing. Even with the developments in next-generation firewalls, the trend is moving towards higher autonomy and remote delivery methods.

- It's expected that firewalls will be even more active in the future and better communicate with various other cybersecurity components, creating a more holistic security mechanism.

- The next logical step would be integration into Security Information and Event Management solutions.

Advantages of firewall

- Port Control
- Network Address Translation
- Application Monitoring (Program Control)
- Packet Filtering
- Data encryption
- Hiding presence
- Reporting/logging
- e-mail virus protection
- Pop-up ad blocking
- Cookie digestion
- Spy ware protection etc.
- **Content Screening**
- **Logging and Monitoring**
- Protocol filtering
- Application gateways

- Centralized Management & Reporting: This allows you to easily manage your firewall from a central location and view reports on security activity.
- Antivirus & AntiSpam: This protects your devices from viruses, spyware, and spam emails.
- DDoS Protection: This protects your network from distributed denial-of-service (DDoS) attacks, which can overwhelm your network with traffic and make it unavailable to legitimate users.
- Web Filtering: This allows you to block access to certain websites, such as malicious websites or those that are not work-appropriate.
- Intrusion Prevention System (IPS): This helps to prevent unauthorized access to your network by detecting and blocking suspicious activity.
- Deep Packet Inspection: This allows you to inspect the contents of data packets that are traveling across your network. This can be helpful for identifying malware and other threats.
- Application Control: This allows you to control which applications are allowed to access the internet. This can be helpful for preventing unauthorized applications from communicating with the internet.
- VPN: A virtual private network (VPN) encrypts your internet traffic and tunnels it through a secure server. This can help to protect your privacy and security when you are using public Wi-Fi.

Disadvantages of firewall

- slow down network access dramatically
- more susceptible to distributed denial of service (DDOS) attacks.
- not transparent to end users
- require manual configuration of each client computer.
- The most obvious being that certain types of network access may be hampered or even blocked for some hosts, including telnet, ftp, X Windows, NFS, NIS, etc.
- A second disadvantage with a firewall system is that it concentrates security in one spot as opposed to distributing it among systems, thus a compromise of the firewall could be disastrous to other less-protected systems on the subnet.

Thanks..!!!