Firewall, Types and Implementation

CC Faculty
ALTTC, Ghaziabad

Agenda

- ❑What is Firewall
- ❑Types of Firewall
- ❑Implementation of Firewall

Firewall ?

- A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet.
- The term firewall comes from the fact that by segmenting a network into different physical subnetworks, they limited the damage that could spread from one subnet to another just like firedoors or firewalls.

Firewall?

- A *firewall* puts up a barrier that controls the flow of traffic between networks.
- Strictly controls selected traffic in a secure way

Firewall?

- A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service.
- It may be a hardware device or a software program running on a secure host computer.
- It must have at least two network interfaces, one for the network it is intended to protect, and one for the network it is exposed to.

Who needs a firewall?

- Anyone who is responsible for a private network that is connected to a public network needs firewall protection.
- Anyone who connects so much as a single computer to the Internet via modem should have personal firewall software.

What does a firewall do?

- A firewall **examines all traffic** routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.
- A firewall **filters** both inbound and outbound traffic.
- It can also **manage public access** to private networked resources such as host applications.
- It can be used to **log all attempts** to enter the private network and trigger alarms when hostile or unauthorized entry is attempted.

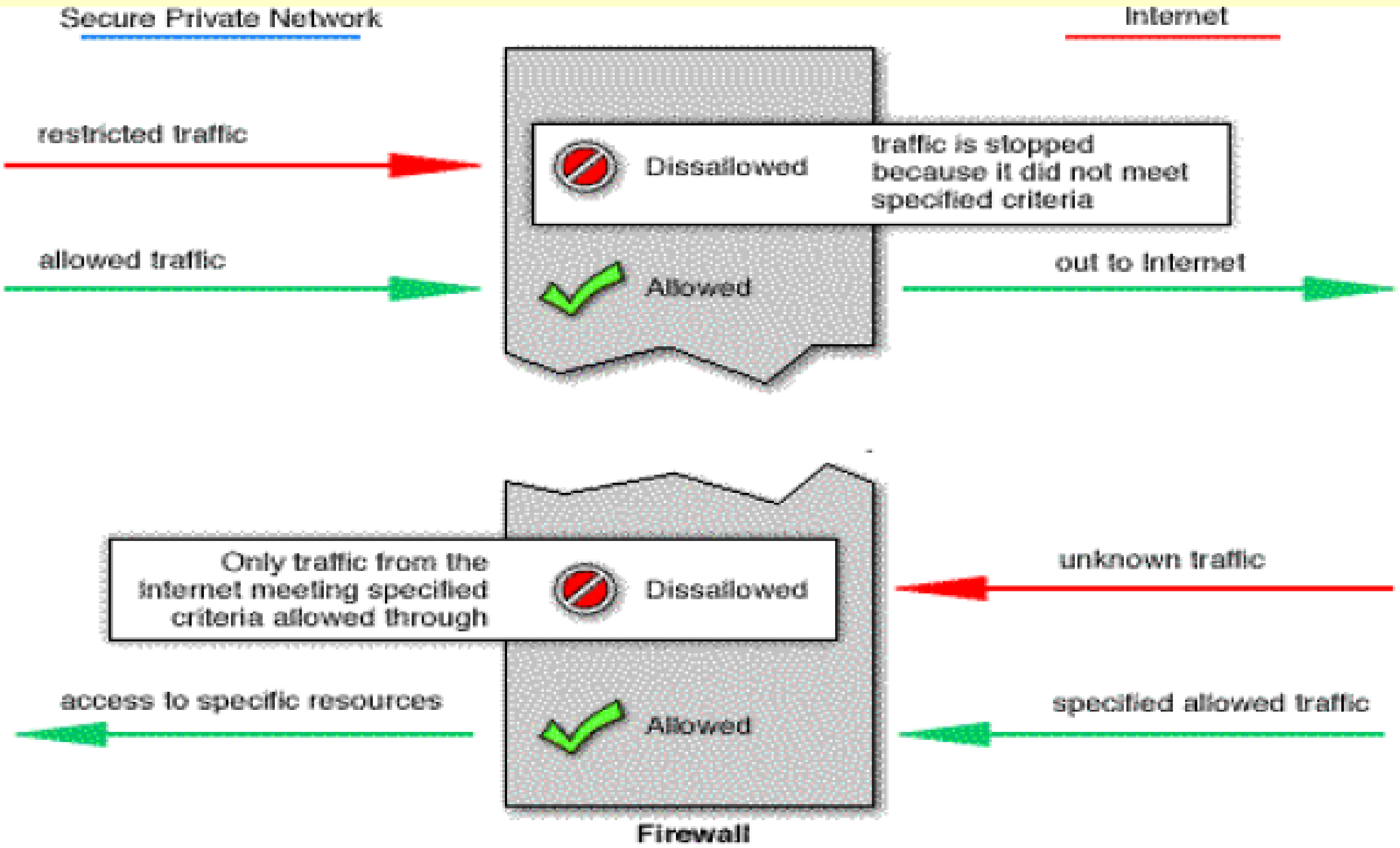
Utility of Firewall

- Implementation of Access Control Policy
- Logging Function
- Auditing Function
- Traffic Monitoring

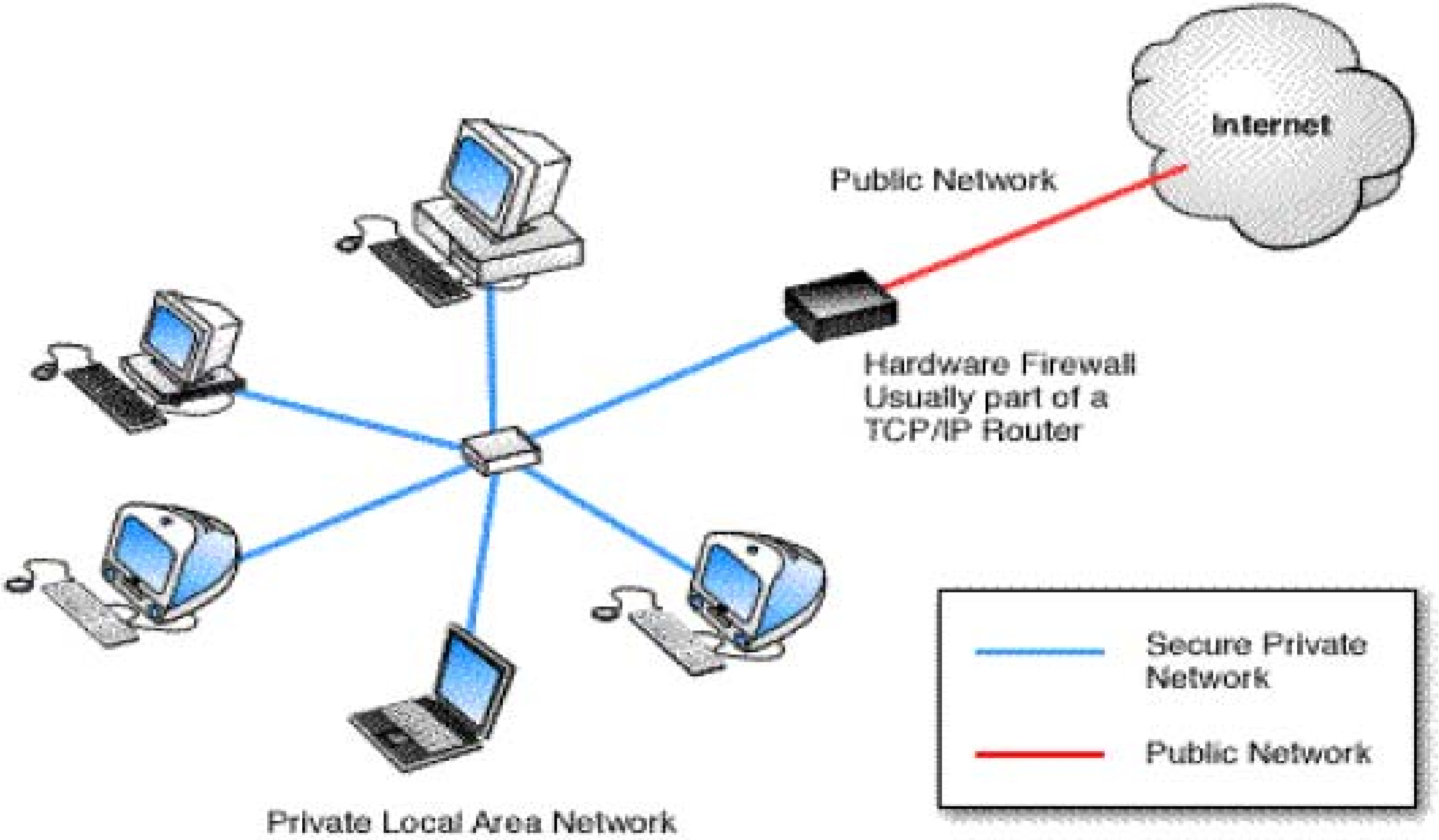
What can't a firewall do?

- A firewall cannot prevent individual users with modems from dialing into or out of the network, bypassing the firewall altogether.
- Employee misconduct or carelessness cannot be controlled by firewalls.
- Policies involving the use and misuse of passwords and user accounts must be strictly enforced.

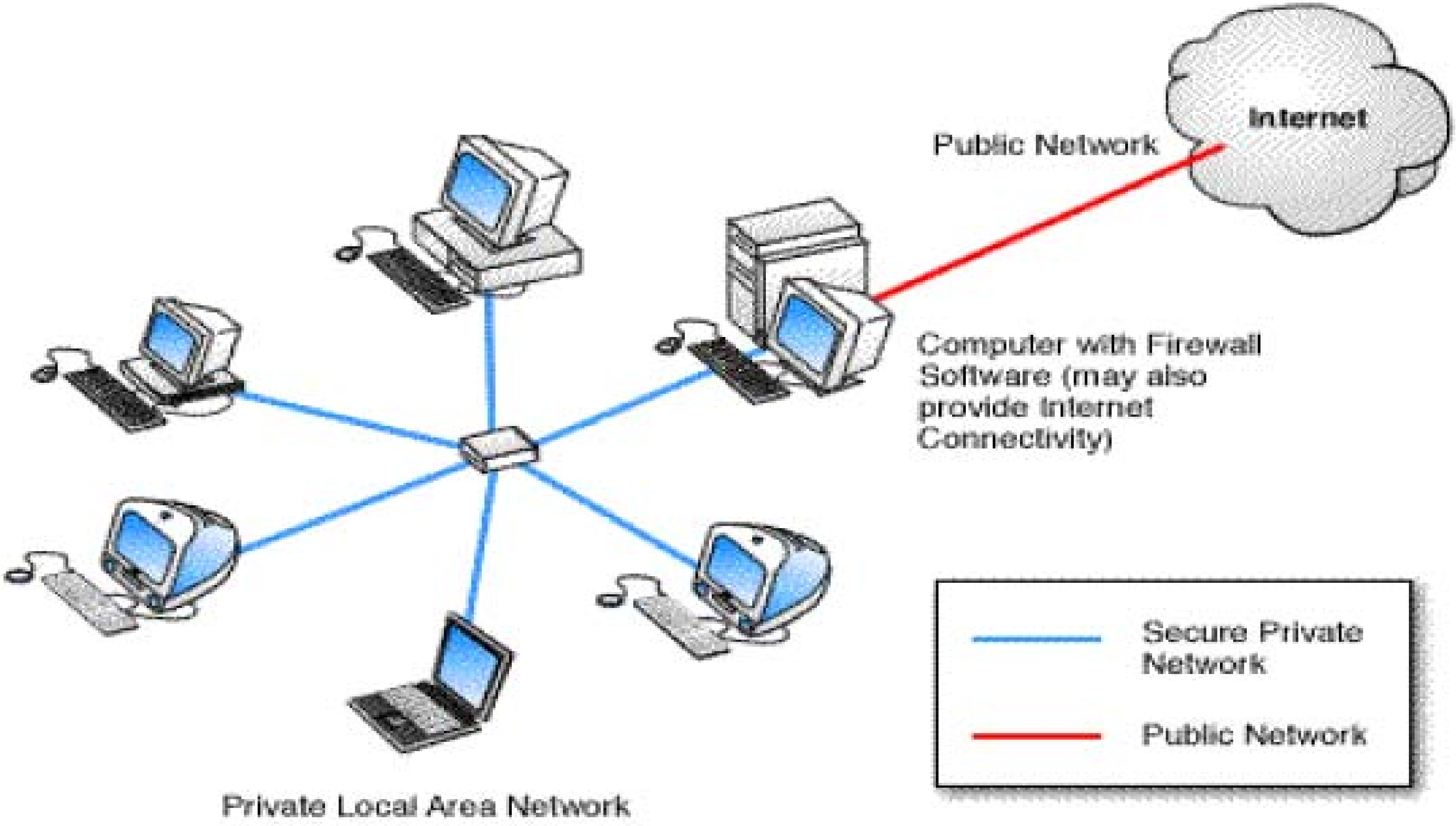
How does a firewall work?


Secure Private Network
Internet
restricted traffic
Dissallowed
traffic is stopped because it did not meet specified criteria
allowed traffic
Allowed
out to Internet
Only traffic from the Internet meeting specified criteria allowed through
Dissallowed
unknown traffic
access to specific resources
Allowed
specified allowed traffic
Firewall

Hardware Firewall



Software Firewall


Internet
Public Network
Computer with Firewall Software (may also provide Internet Connectivity)
Secure Private Network
Public Network
Private Local Area Network

Perimeter Defense

Firewalls are often described in terms of perimeter defense systems, with a so-called **"choke point"** through which all internal and external traffic is controlled

Types of Filtering

- Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as **address filtering**.
- Firewalls can also filter specific types of network traffic. This is also known as **protocol filtering** because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet.
- Firewalls can also filter traffic by **packet attribute or state.**

Static Packet Filtering

- ❑ It Controls traffic by using information stored within the packet headers.
- ❑ Attributes of the packet are compared with Access Control Policy
- ❑ The information used for filtering
  - ➢ Destination IP address or Subnet
  - ➢ Source IP address or Subnet
  - ➢ Destination Service Port
  - ➢ Source Service Port
  - ➢ Flag(TCP only)

Packet Filtering TCP Traffic

❑ Flag Fields:

- ACK – Reponses to request
- FIN - Termination of session
- PSH –prevents the transmitting system from queuing up before transmission
- RST – resets the state of current session
- SYN – used while initialization of session
- URG – high priority information to be passed

❑ These Flag Fields are used to control traffic

Example of Static Packet Filtering

- ❑ Access Control Policy : internal users can access any service on internet, but all Internet traffic headed towards internal clients should be blocked.
- ❑ Implementation : All Internet Traffic headed to Internal Network with SYN = 1 and all other flags set to 0 should be blocked.
- ❑ It will never allow connection with internal hosts.
- ❑ Port scans will be disallowed.

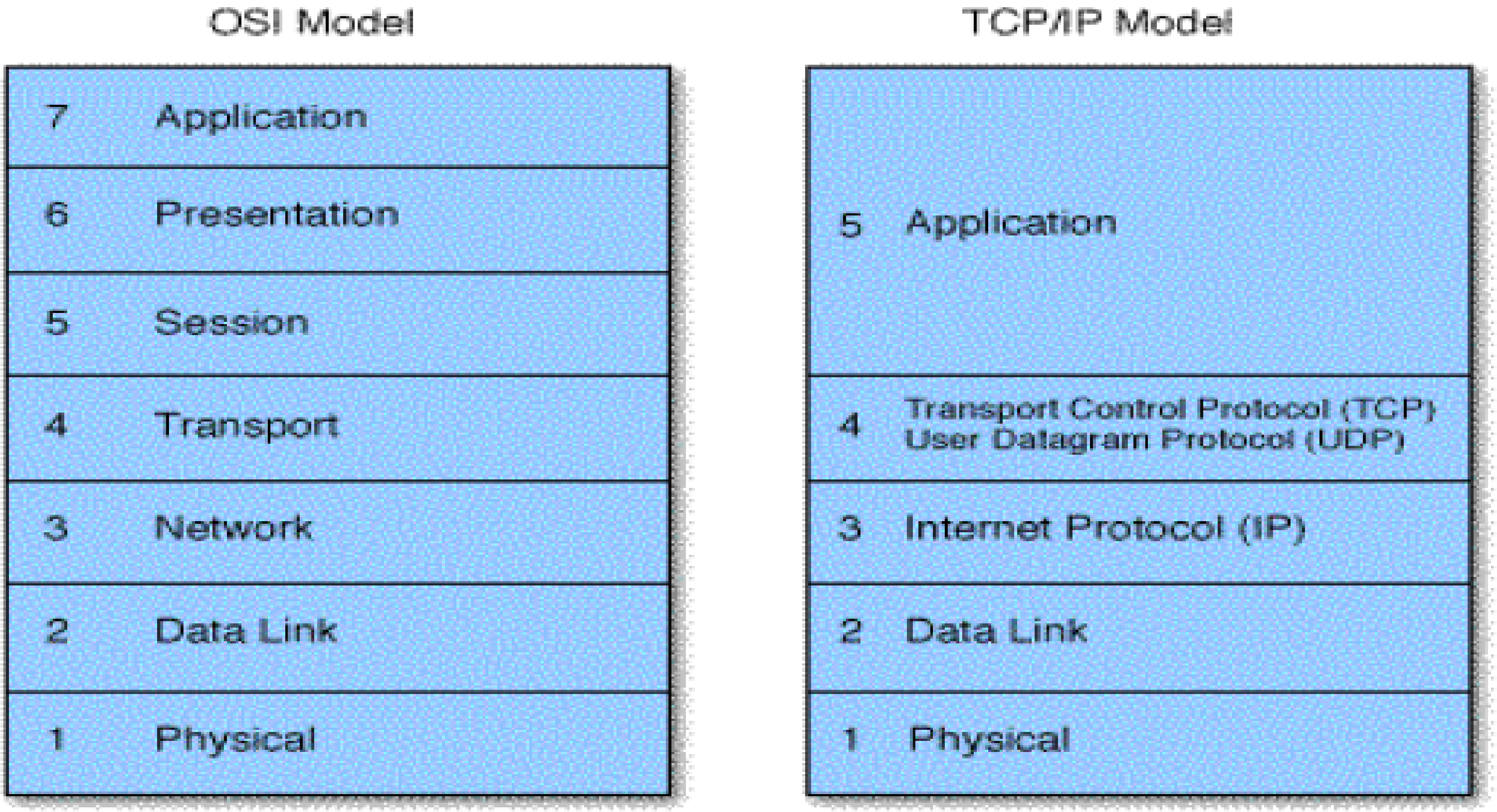
Example of Limitations Packet Filtering

- ❑ **FIN Attack :**
  - ➢ Attacker sends packets with FIN = 1, ACK =1
  - ➢ If service is not running, host sends RST=1, ACK=1
  - ➢ If service is running, host sends ACK=1, FIN=1.
- ❑ **IP Spoofing :**
  - ➢ Attacker can assume the IP address of Outside Server and start session with internal host

Dynamic Packet Filtering

- Besides checking attributes of Filters, It Maintains the connection table in order to monitor the state of communication session

Firewall and OSI Layers



OSI Model		TCP/IP Model	
7	Application	5	Application
6	Presentation		
5	Session		
4	Transport	4	Transport Control Protocol (TCP) User Datagram Protocol (UDP)
3	Network	3	Internet Protocol (IP)
2	Data Link	2	Data Link
1	Physical	1	Physical

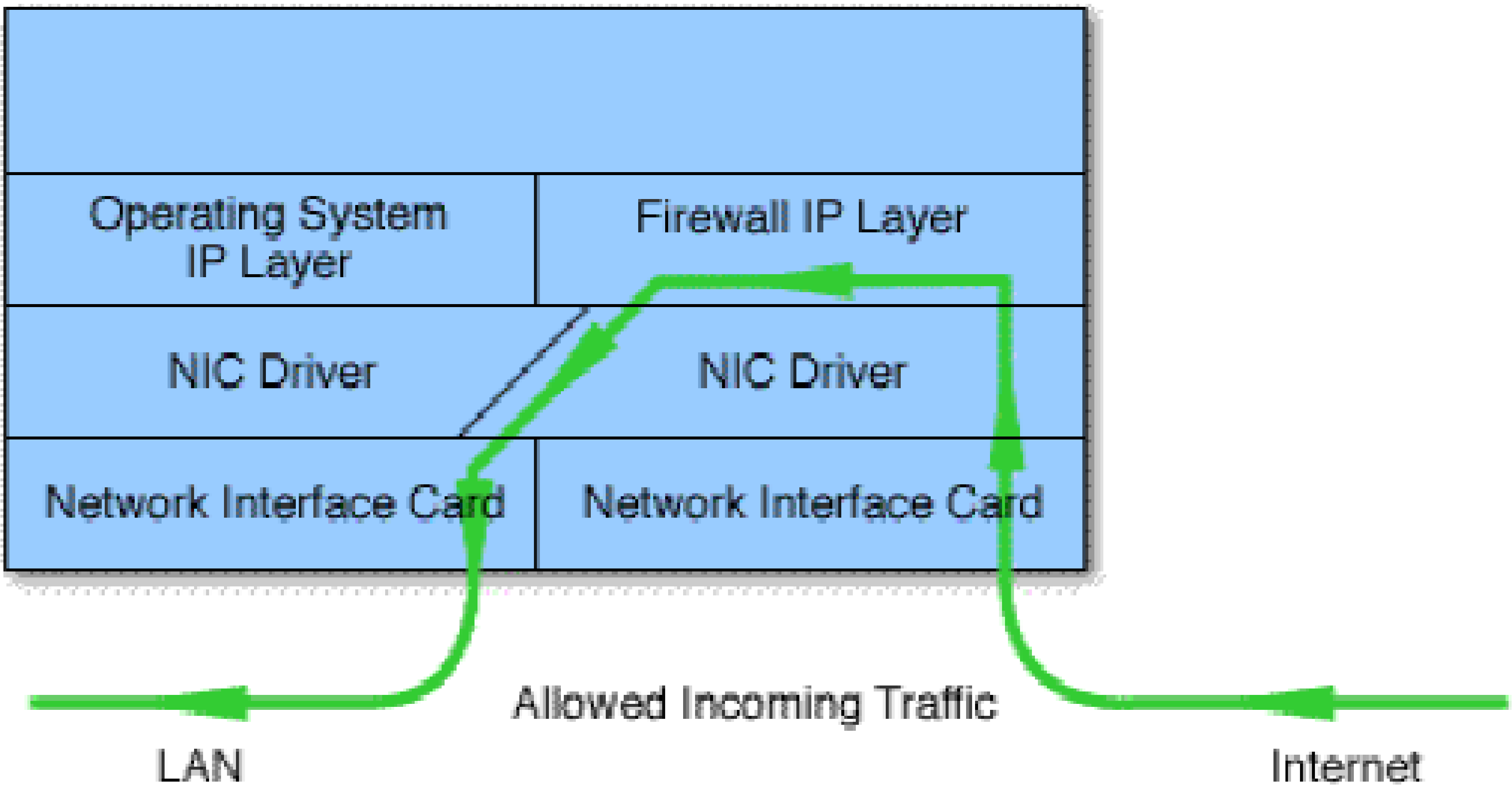
Firewall at Layer 3

- Firewalls operate at different layers to use different criteria to restrict traffic.
- The lowest layer at which a firewall can work is layer three. This layer is concerned with routing packets to their destination.
- At this layer a firewall can determine whether a packet is from a trusted source, but cannot be concerned with what it contains or what other packets it is associated with.

Firewall at Layers 4 and 5

- Firewalls that operate at the transport layer know a little more about a packet, and are able to grant or deny access depending on more sophisticated criteria.
- At the application level, firewalls know a great deal about what is going on and can be very selective in granting access.
- The lower in the stack the packet is intercepted, the more secure the firewall. If the intruder cannot get past level three, it is impossible to gain control of the operating system.

Professional Firewalls have their own IP Layer



Professional Firewalls have their own IP Layer

- Professional firewall products catch each network packet before the OS does, thus, there is no direct path from the Internet to the operating system's TCP/IP stack. It is therefore very difficult for an intruder to gain control of the firewall host computer then "open the doors" from the inside.
- Firewalls have moved down the protocol stack so far that the OS doesn't have to do much more than act as a bootstrap loader, file system and GUI

Types Categories

- Packet Filters
- Circuit level gateways
- Application level gateways
- Stateful Multilayer inspection firewalls

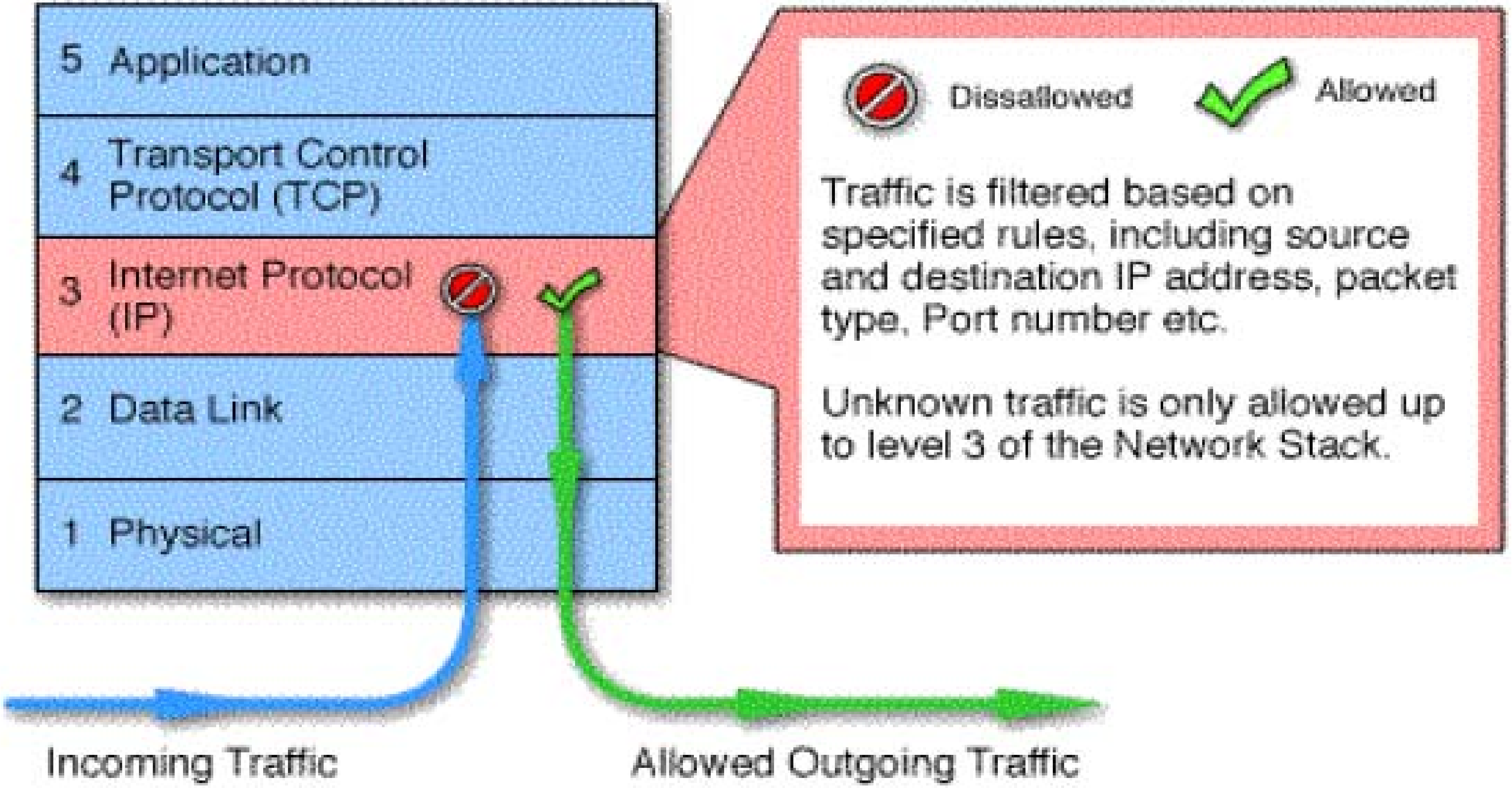
Packet Filter Firewall

- Packet filtering firewalls work at the network level of the OSI model, or the IP layer of TCP/IP.
- In a packet filtering firewall each packet is compared to a set of criteria before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it or send a message to the originator.
- Rules can include source and destination IP address, source and destination port number and protocol used.

Packet Filter Firewall

- The advantage of packet filtering firewalls is their low cost and low impact on network performance.
- Most routers support packet filtering. Even if other firewalls are used, implementing packet filtering at the router level affords an initial degree of security at a low network layer.
- This type of firewall only works at the network layer however and does not support sophisticated rule based models

Packet Filter Firewall



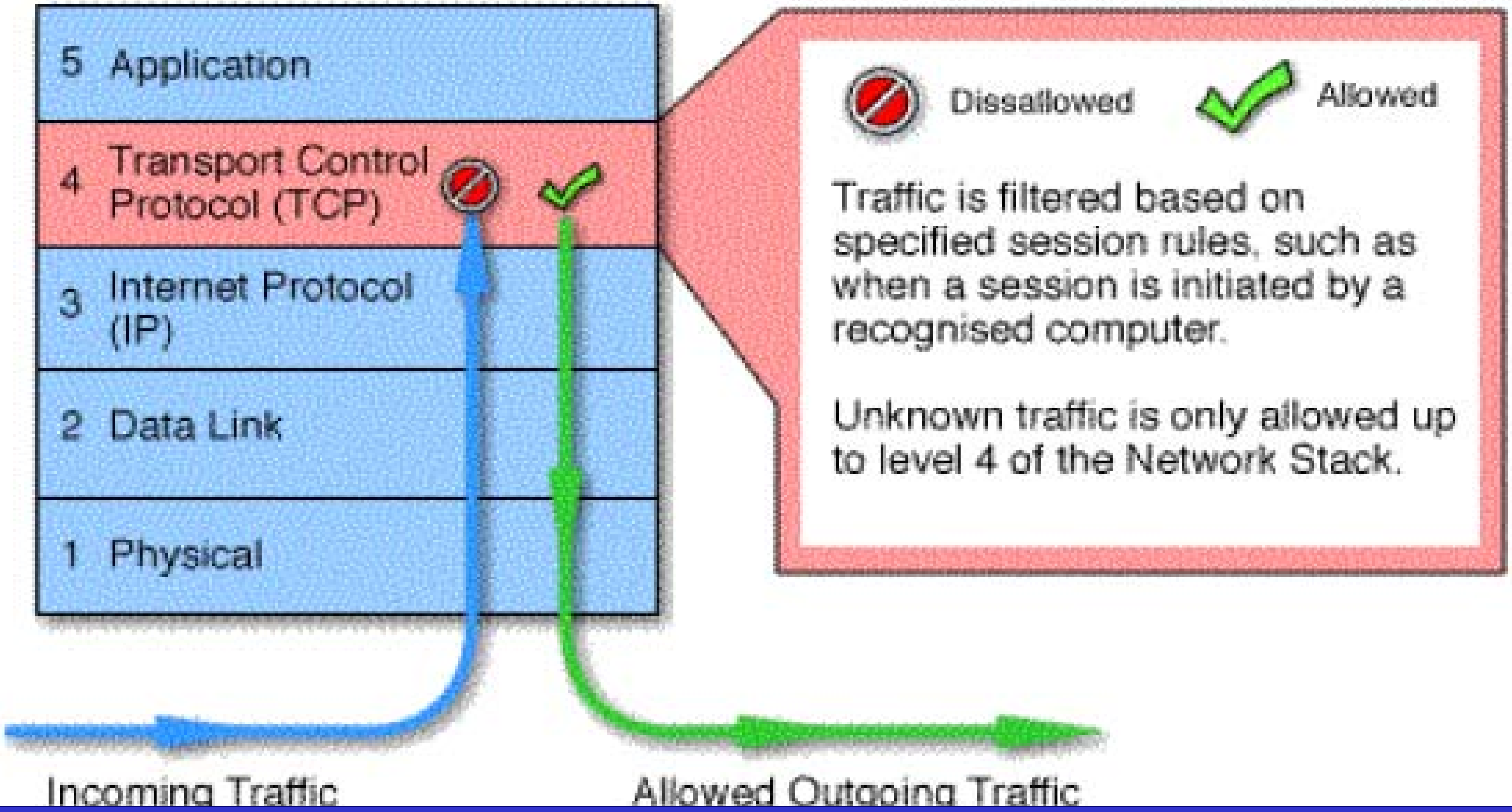
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.

Unknown traffic is only allowed up to level 3 of the Network Stack.

Circuit Level Gateways

- 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.
- 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.

Circuit Level Gateways



Traffic is filtered based on specified session rules, such as when a session is initiated by a recognised computer.

Unknown traffic is only allowed up to level 4 of the Network Stack.

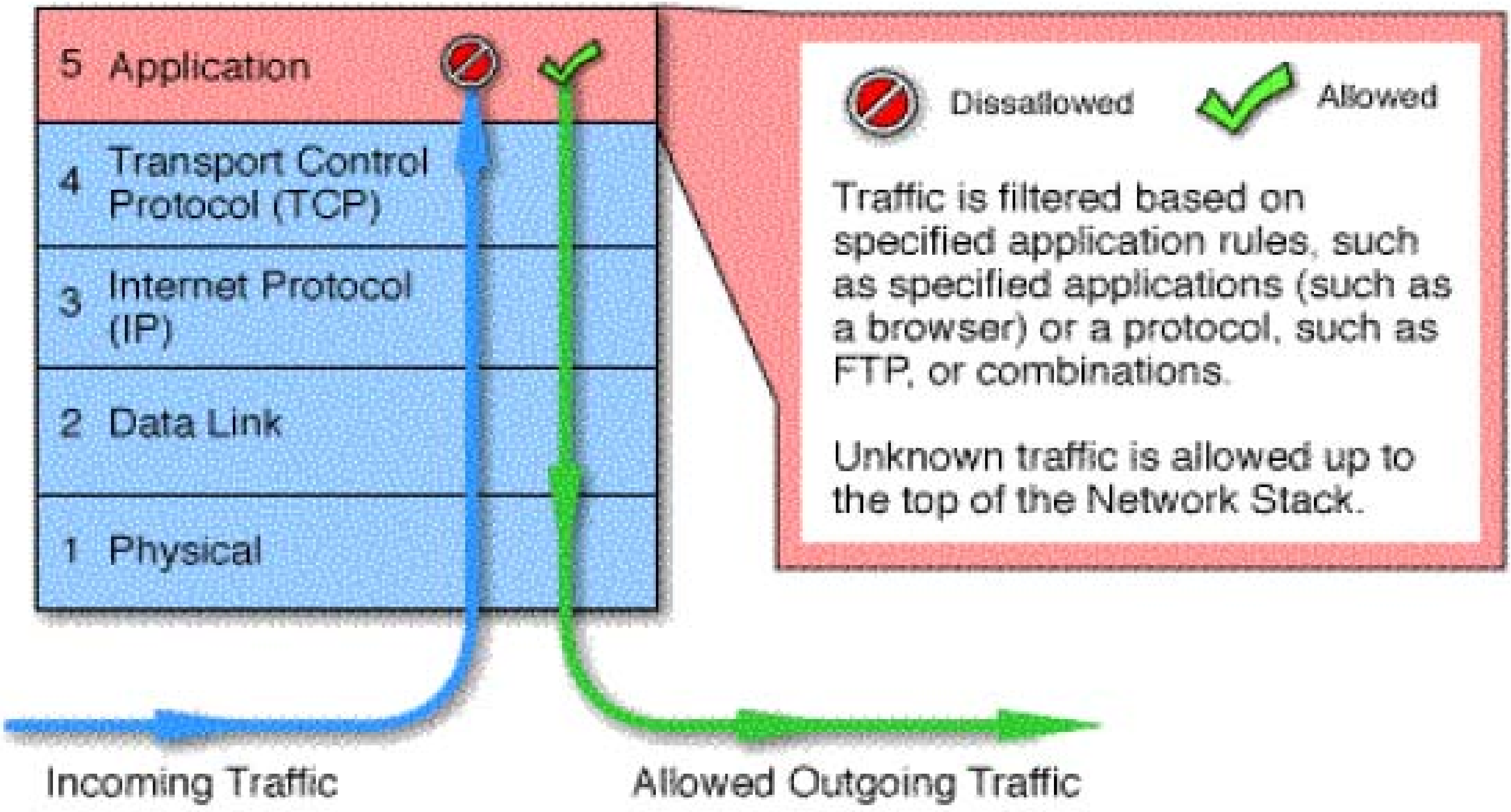
Application Level Gateways

- They can filter packets at the application layer of the OSI model and are also called Proxies.
- Incoming or outgoing packets cannot access services for which there is no proxy.
- In plain terms, an application level gateway that is configured to be a web proxy will not allow any ftp, gopher, telnet or other traffic through.
- Because they examine packets at application layer, they can filter application specific commands such as http:post and get, etc.

Application Level Gateways

- Application level gateways can also be used to log user activity and logins. They offer a high level of security,
- They have a significant impact on network performance. This is because of context switches that slow down network access dramatically.

Application Level Gateways



Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.

Unknown traffic is allowed up to the top of the Network Stack.

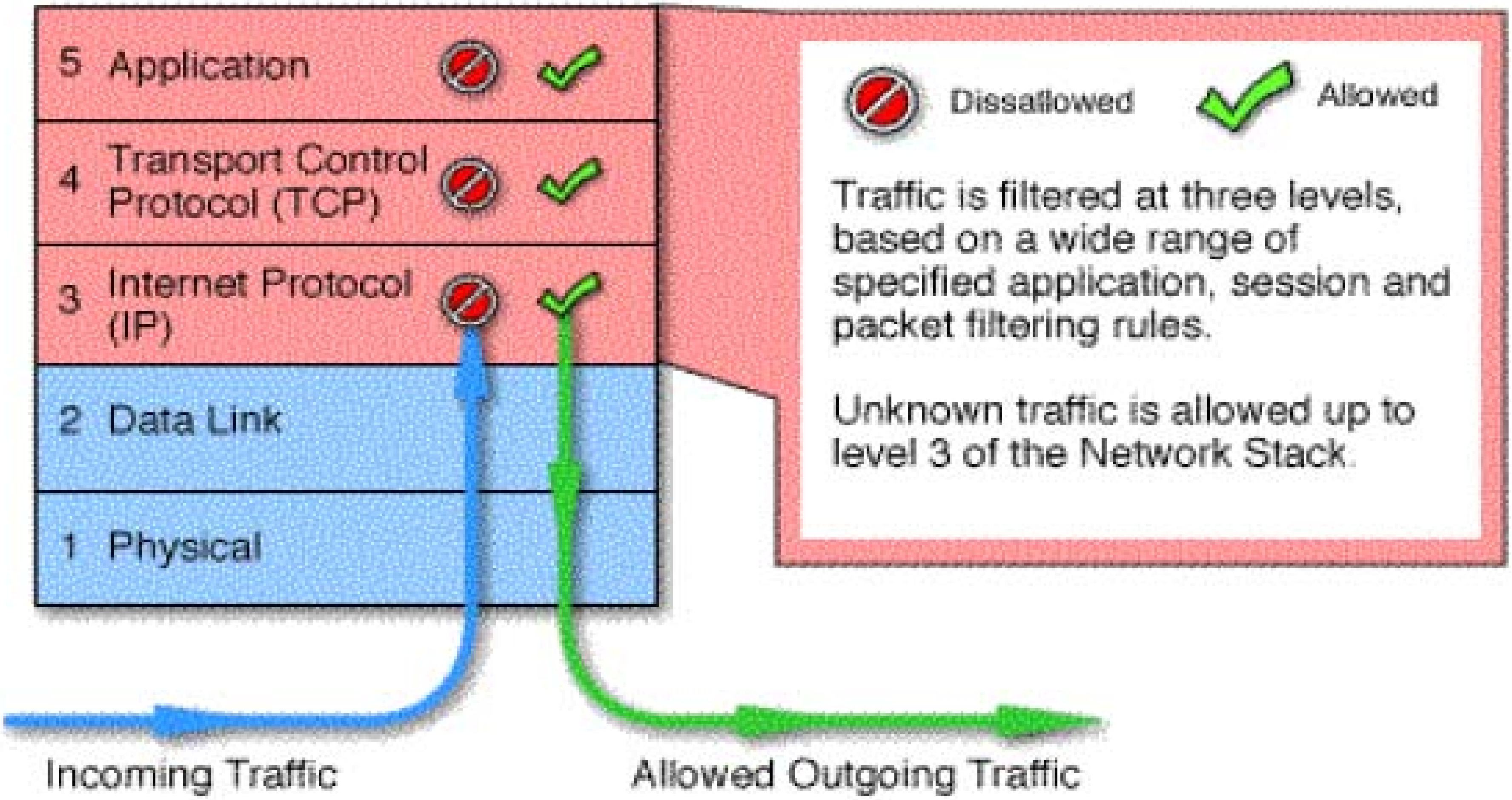
Stateful Multilayer Inspection Firewalls

- 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.
- They allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways.
- They rely on algorithms to recognize and process application layer data instead of running application specific proxies.

Stateful Multilayer Inspection Firewalls

- Stateful Multilayer inspection firewalls offer a high level of security, good performance and transparency to end users.
- They are expensive however, and due to their complexity are potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

Stateful Multilayer Inspection Firewalls



Traffic is filtered at three levels, based on a wide range of specified application, session and packet filtering rules.

Unknown traffic is allowed up to level 3 of the Network Stack.

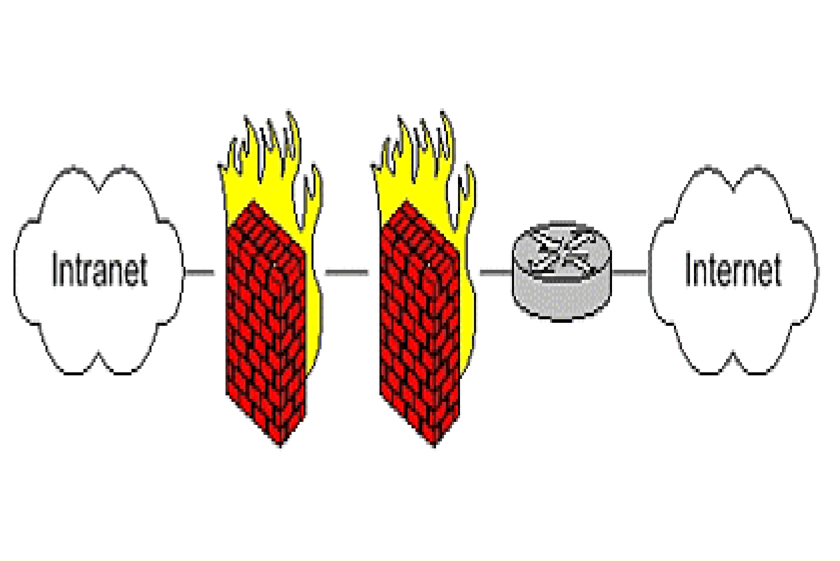
Implementation of Firewall

- ❑ Determine the access denial methodology to use
- ❑ Determine inbound access policy.
- ❑ Determine outbound access policy
- ❑ Determine if dial-in or dial-out access is required.

Firewall redundancy: Deployment Scenarios

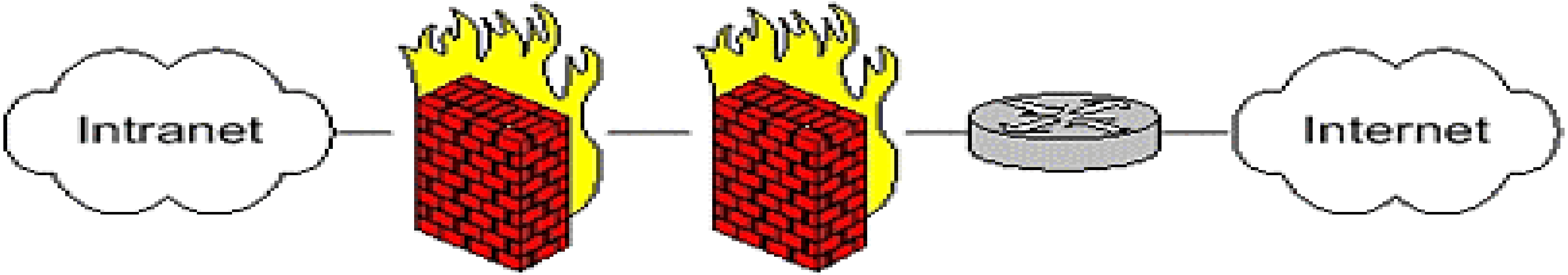
- ❑Fault Tolerance and Load Balancing
- ❑Enhanced Perimeter protection

Deployment Scenarios - I



- ❑ Added benefits of fault tolerance and load balancing
- ❑ Both firewalls should be configured to "fail-safe," that is, in the event of a failure, they should automatically block all traffic
- ❑ The router may be configured to divide traffic between the two firewalls, either on a priority basis or on a fair-share basis

Deployment Scenarios - II



- ❑ Deployed in high-security environments
- ❑ the two firewalls are from different vendors and may even run on different operating systems

Thanks!