CSC 402 – Internet Technology

Recap

- Designing of Internet System Network Architecture
- Design Issues
- Web Servers
- Proxy Servers
- RADIUS
- Email Servers
- Cookies
- Load Balancing – Proxy Arrays

Security and System Administration Issues, Firewalls and Content Filtering

- System is secure when nobody can disrupt its operations or use it in a way that is not predefined.
- CIA definition of information security (the most simple one):
  - **Confidentiality** - nobody can read what he is not supposed to.
  - **Integrity** - nobody can change the data without legitimate users knowing.
  - **Availability** - it is not possible to prevent access.
- Typically, computer networks are shared by many applications and services for many different purposes.
- Sometimes data transmitted between application processes is confidential, and the users would prefer others not to be able to read it.
  - E.g., when purchasing a product online, users transmit their credit card numbers over the network.
- Thus, users sometimes want to protect the messages they sent.
- Additional Security Requirements:
  - Authenticity - verifying users & trusted source.
  - Accountability - nonrepudiation, fault isolation, intrusion detection & prevention, and after-action recovery & legal action.

Security and System Administration Issues, Firewalls and Content Filtering

- Firewall
  - Protecting internal network from network-based security threats.
  - Affording access to WAN & the Internet.
- Design goals for a firewall:
  - All traffic from inside to outside, and vice versa, must pass through the firewall.
    - Achieved by physically blocking all access to the local network except via the firewall.
    - Various configurations possible.
  - Only authorized traffic, as defined by the local security policy, will be allowed to pass.
    - Various types of firewalls implementing various types of security policies.
  - The firewall itself is immune to penetration.
    - Use of a hardened system with a secured OS.

Security and System Administration Issues, Firewalls and Content Filtering

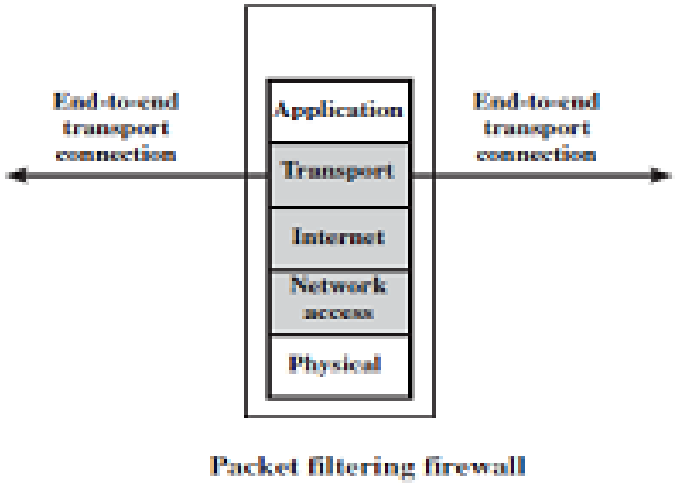
- General techniques that firewalls use to control access & enforce security policy.
- Service control.
  - Determines the Internet services types that can be accessed, inbound or outbound.
  - Filters traffic on the basis of IP address, protocol, or port number.
  - May provide proxy software that receives & interprets each service request before passing it on.
- Direction control.
  - Determines direction of flow of particular service requests initiated.
- User control.
  - Controls access to a service.
  - May be applied to incoming traffic from external users but requires some form of secure authentication as is provided in IPsec.
- Behavior control.
  - Controls how particular services are used. E.g. firewall may filter e-mail to eliminate spam, or enable external access to only a portion of the information on a local Web server.

Security and System Administration Issues, Firewalls and Content Filtering

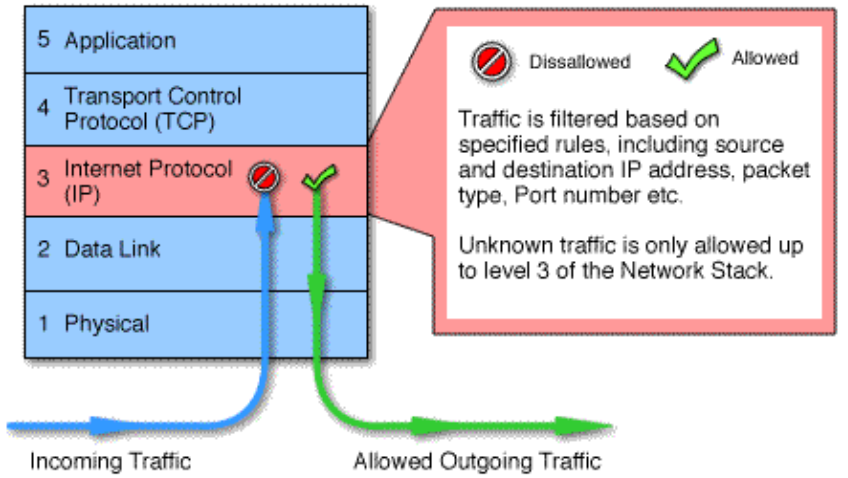
- Firewalls have their limitations, including the following:
  - The firewall cannot protect against attacks that bypass the firewall.
    - Internal systems may have dial-out capability to connect to an ISP.
    - An internal LAN may support a modem pool that provides dial-in capability for traveling employees & telecommuters.
  - The firewall may not protect fully against internal threats.
    - A disgruntled employee who unwittingly cooperates with an external attacker.
  - An improperly secured wireless LAN may be accessed from outside the organization.
  - A laptop, PDA, or portable storage device may be used & infected outside the network, and then attached and used internally.

Security and System Administration Issues, Firewalls and Content Filtering

- Types of Firewall:
- Packet Filtering Firewall.
  - Applies a set of rules to each incoming & outgoing IP packet and then forwards or discards the packet filter packets going in both directions.
  - Based on:
    - Source IP address.
    - Destination IP address.
    - Source and destination transport-level address/ port addresses.
    - IP protocol field.
    - Interface.
- Advantages:
  - Simplicity
  - Transparency to users
  - High speed
- Disadvantages:
  - Difficulty of setting up packet filter rules
  - Lack of Authentication

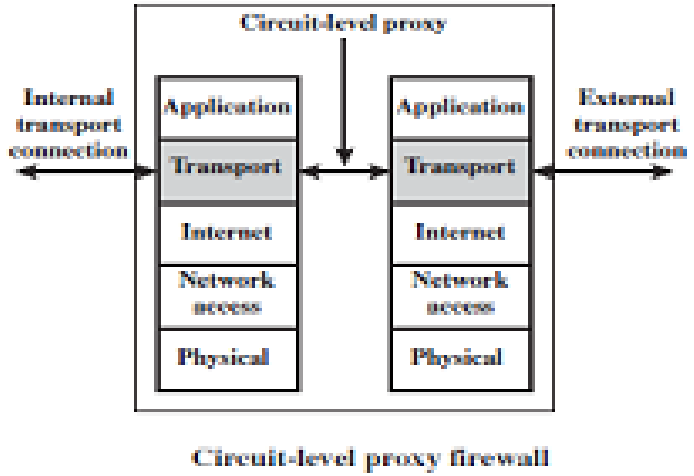


Packet filtering firewall

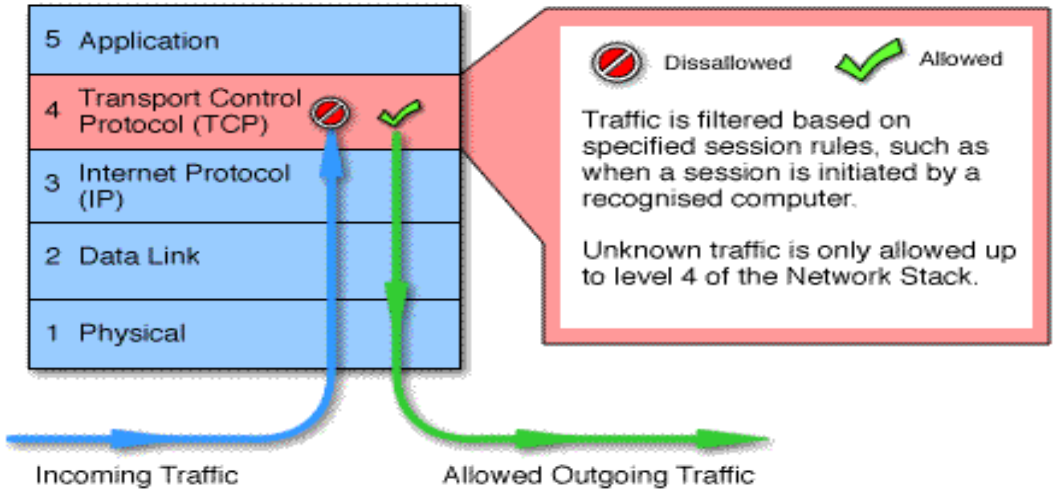


Security and System Administration Issues, Firewalls and Content Filtering

- Circuit-Level Gateway
  - Sets up two TCP connections:
    - between itself & a TCP user on an inner host and one between itself & a TCP user on an outside host.
  - Security function consists of determining which connections will be allowed.

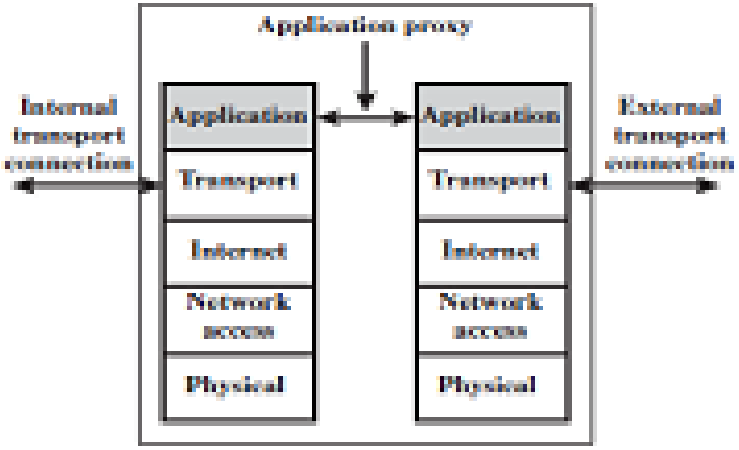


Circuit-level proxy firewall

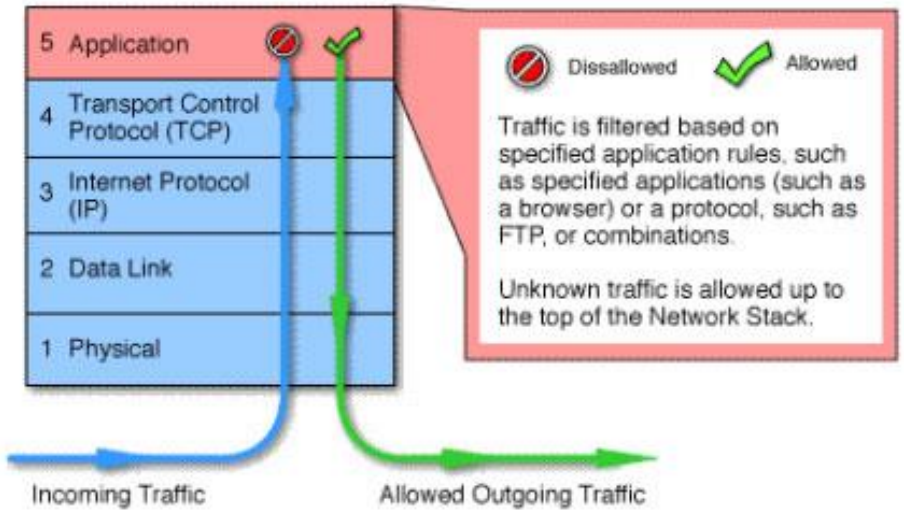


Security and System Administration Issues, Firewalls and Content Filtering

- Application-Level Gateway
  - User contacts gateway using a TCP/IP application , the gateway asks the user for the name of the remote host to be accessed.
  - User provides a valid user ID and authentication information.
  - The gateway contacts the application on the remote host and relays TCP segments containing the application data between the two endpoints.
  - Scrutinize a few allowable applications.
  - Easy to log and audit all incoming traffic at the application level.
  - Additional processing overhead on each connection.
- Advantages:
  - Proxy can log all connections, activity in connections.
  - Proxy can provide caching.
  - Proxy can do intelligent filtering based on content.
  - Proxy can perform user-level authentication.
- Disadvantages:
  - Not all services have proxied versions.
  - May need different proxy server for each service.
  - Requires modification of client.
  - Performance.

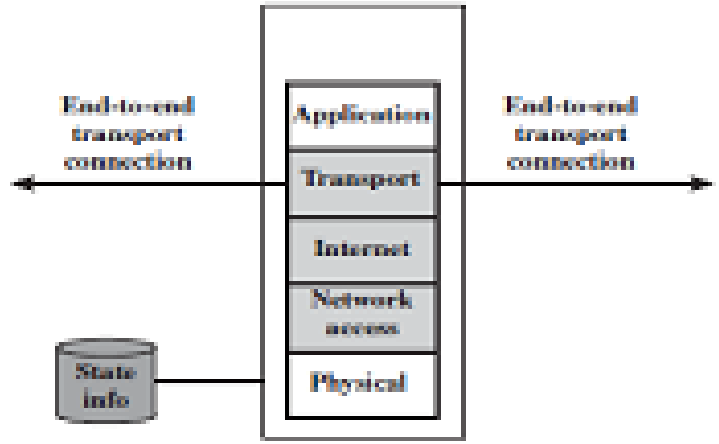


Application proxy firewall

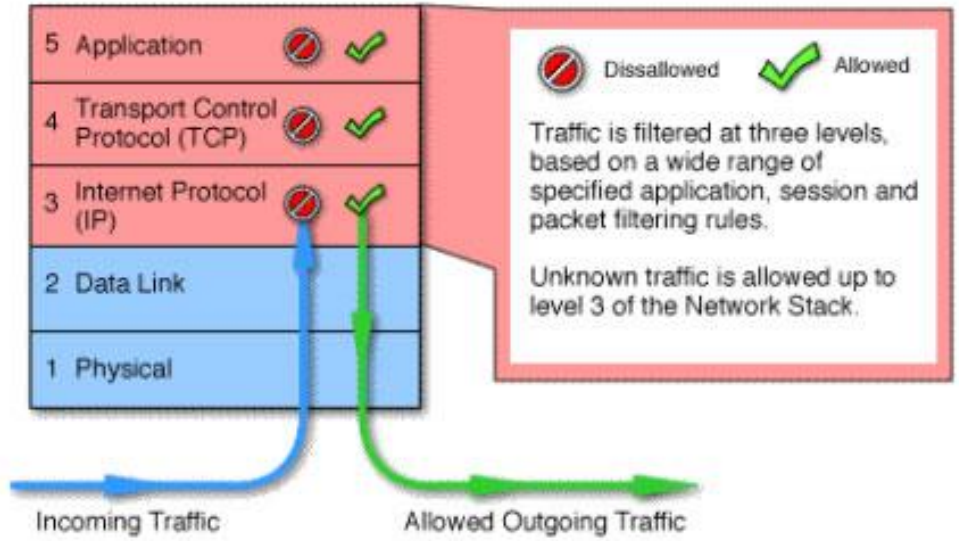


Security and System Administration Issues, Firewalls and Content Filtering

- Stateful (Multilayer) Inspection Firewalls:
  - Rules for TCP traffic by creating a directory of outbound TCP connections allow incoming traffic to high-numbered ports only for those packets that fit the profile of one of the entries in the directory.
  - Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number, such as session hijacking.
- You can also refer: http://ciscodocuments.blogspot.com/2011/05/chapter-03-network-security-using-cisco_24.html



Stateful inspection firewall



Content Filtering

- A.k.a “Web Filtering” or “Information Filtering”.
- Technique that allows content to be blocked or allowed based on analysis of its content, rather than its source or other criteria.
- It is most widely used on the internet to filter email and web access.
- Used by organizations such as offices and schools to prevent users from viewing inappropriate web sites or content, or as a pre-emptive security measure to prevent access of known malware hosts.
- **Browser based filters**: Implemented via a third party browser extension.
- **Client-side filters**: Software managed, disabled, or uninstalled by network admin.
- **Content-limited (or filtered) ISPs**: ISP offers access to only a set portion of Internet content.
- **Search-engine filters**: Many search engines, such as Google and Alta Vista offer users the option of turning on a safety filter that filters out the inappropriate links from all of the search results.