Firewalls

Evolution of Firewalls

- When organizations first had access to the internet, typically only a small number of people wanted access to the internet.
- Acess to the internet was provided by a internet gateway, a machine with two network cards, one connected to the internet, the other connected to the corporate network (LAN).

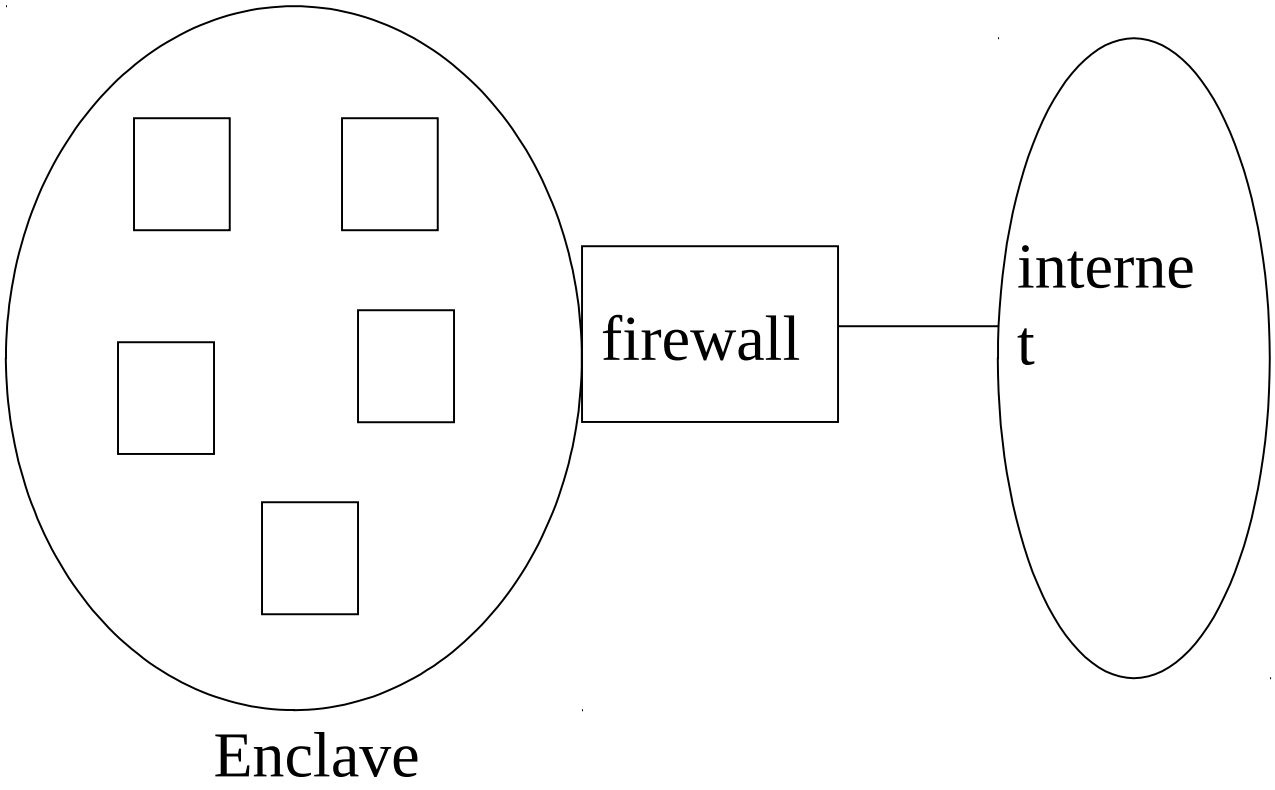
Evolution of Firewalls

- Users would then logon to this host to access the Internet.
- Once logged on, typically the user would use email, telnet and ftp (this was before the Web).

Firewalls - Two Main Types

- The above was replaced by two types of firewall
  - Packet Filtering (IP layer)
  - Proxy Servers (Application Layer)
- Both provide a certain level of security (from the Internet) to an Enclave.

Firewall and Enclave



Packet Filtering Firewalls

- Before Packet Filtering Firewalls were available, routers were used to provide packet filtering.
- The routing tables of routers could be configured to only allow certain packets into the LAN.
- This evolved into Packet Filtering Firewalls.

Packet Filtering Firewalls

- Packet Filtering Firewalls examine TCP/IP packets and filter them based on
  - Source address
  - Destination address
  - Protocol (Source and Destination port number)

Packet Filtering Firewalls (cont.)

- Packet Filtering Firewalls can be used to for example
  - prohibit all telnet (port 23) access into a site.
  - only allow Web access to a specified Web server
  - prohibit all TCP/IP connections to certain machines.
  - prohibit all connections on a specific port from outside the site.

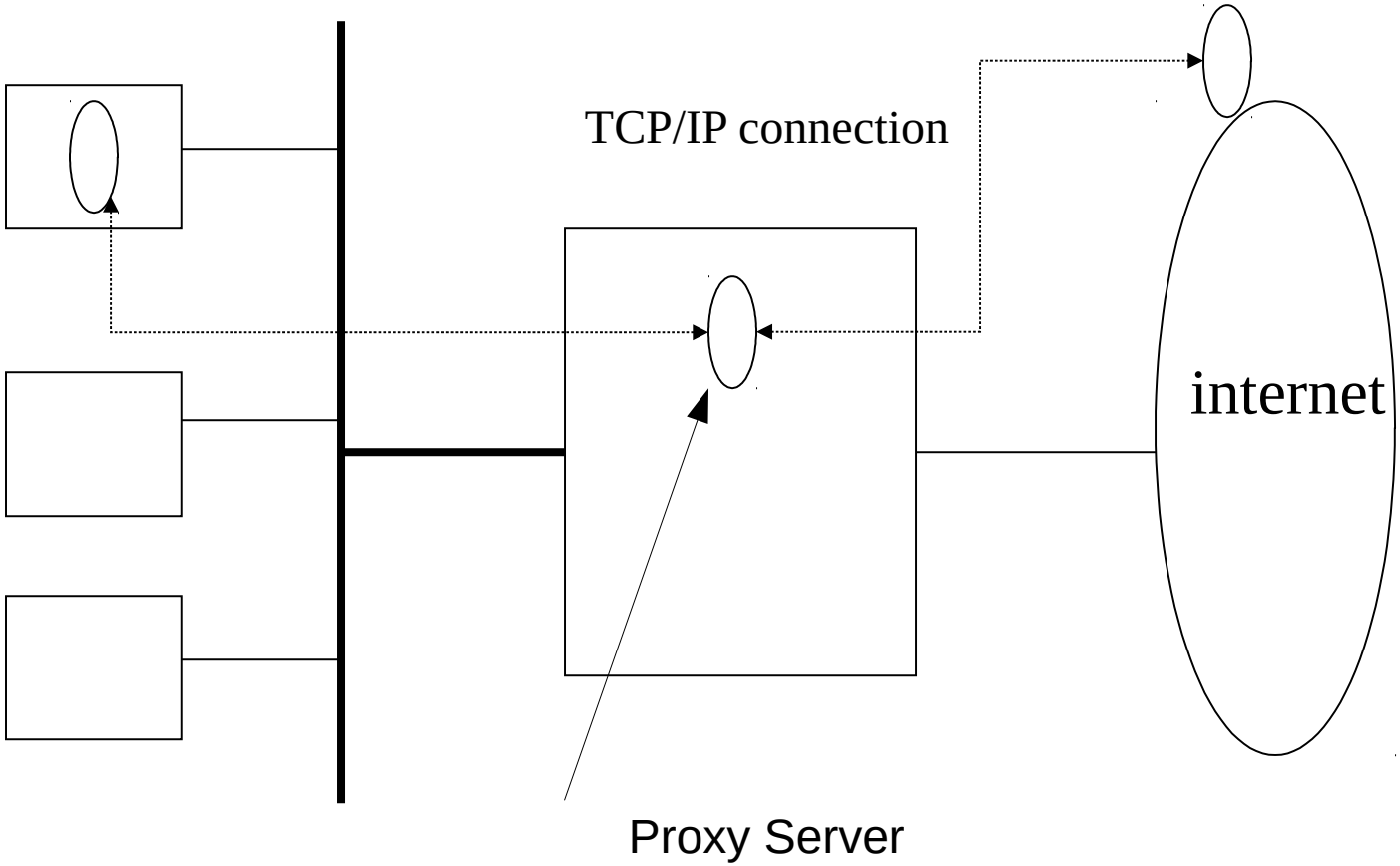
Packet Filtering Firewalls (cont.)

- Packet Filtering Firewalls can be used to for example
  - Allow only HTTP (port 80) traffic
  - only allow ftp'ing of data into a site
- [Filtering decisions based on source IP address are unsafe as source addresses can be forged.]

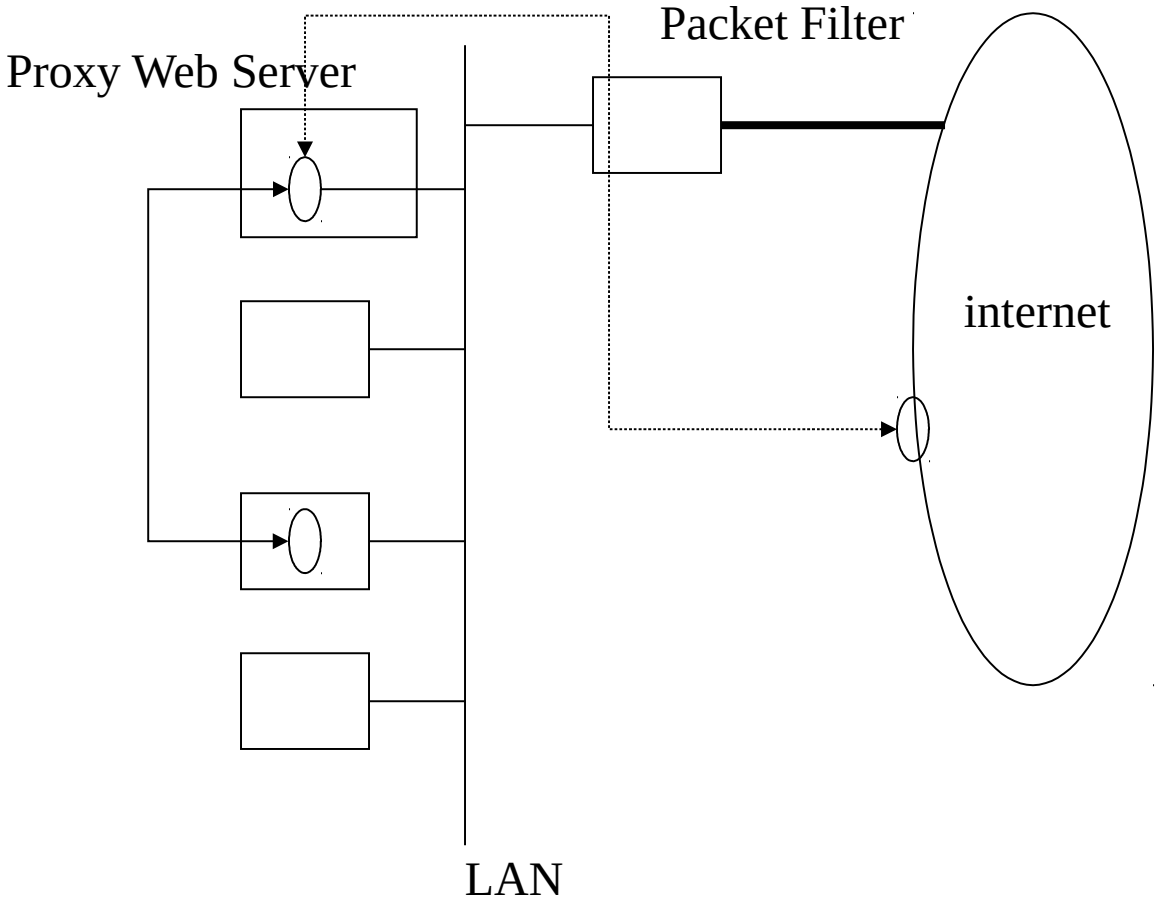
Proxy Server/ Application Gateway

- Two problems with Packet Filters
  - They can not impose restrictions on users of a service
  - The IP address of the client is exposed in a TCP/IP connection.
- Proxy Servers, also known as Application Gateways address both these issues.

Proxy Server



Proxy Web Server plus Packet Filtering Firewall



Proxy Web Server plus Packet Filtering Firewall

- Typically Packet Level Filters and Proxy Server or Application Gateways are used together.
- The Packet Filter blocks all traffic on a specific port except to the Proxy Server.
- The Proxy Server can then filter the service requests.
- A Proxy Server can also boost performance by caching data.

Proxy Web Servers

- Clients (Chrome, Firefox, IE) must be configured to send all requests to the Proxy Server.

Network Address Translation

Network Address Translation

- Allows the use of one set of network addresses internally and another externally.
- Internal address are concealed.
- The router can direct incoming traffic to an internal node based on a NAT table.

NAT Table

- You can associate a port with an internal address.
- All requests on that port are sent to the appropriate internal node.
- Will require a static internal IP address instead of the more usual dynamic address assigned using DHCP.

Personal Firewall

Personal Firewalls

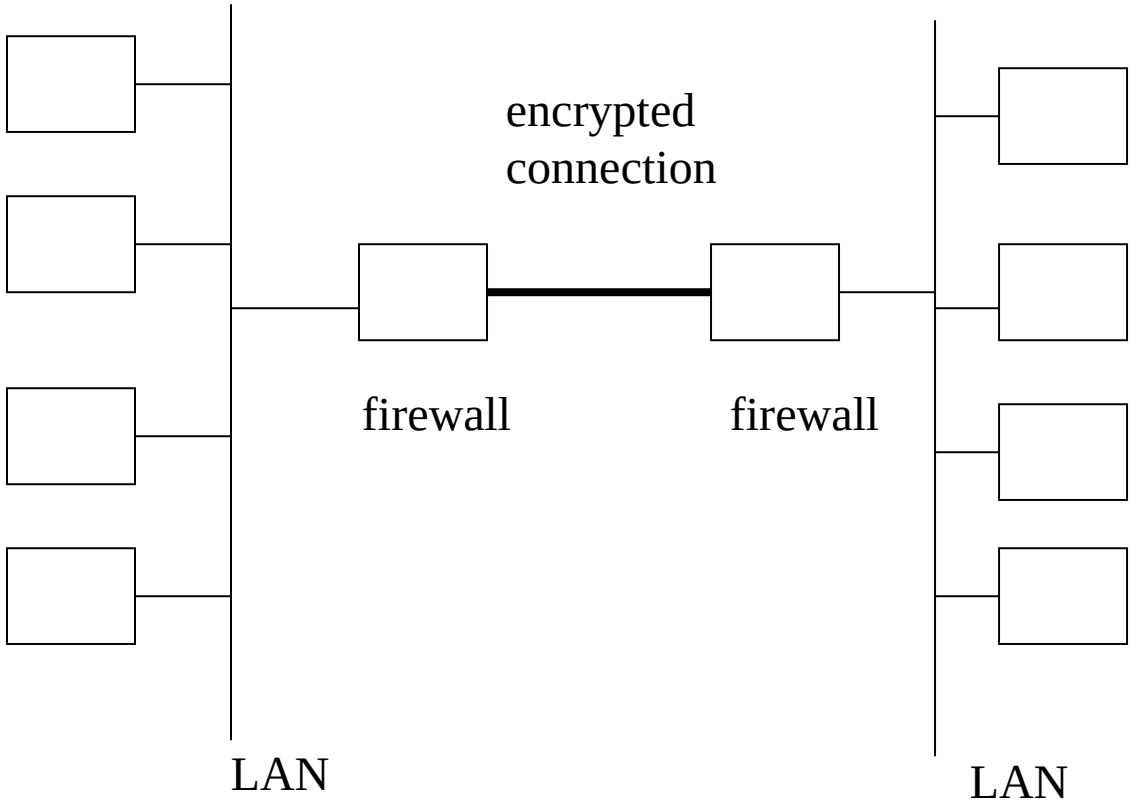
- Controls network traffic to and from a single computer.
- Allows the user to control which programs can access the network.
- Can notify the user when programs access the network.

Virtual Private Networks

Virtual Private Networks

- Most firewalls now support Virtual Private Networks.
- Traffic between firewalls belonging to the same VPN is transparently encrypted.
- Some firewalls support the extension of VPN membership to home users PCs.

Virtual Private Network



DMZ

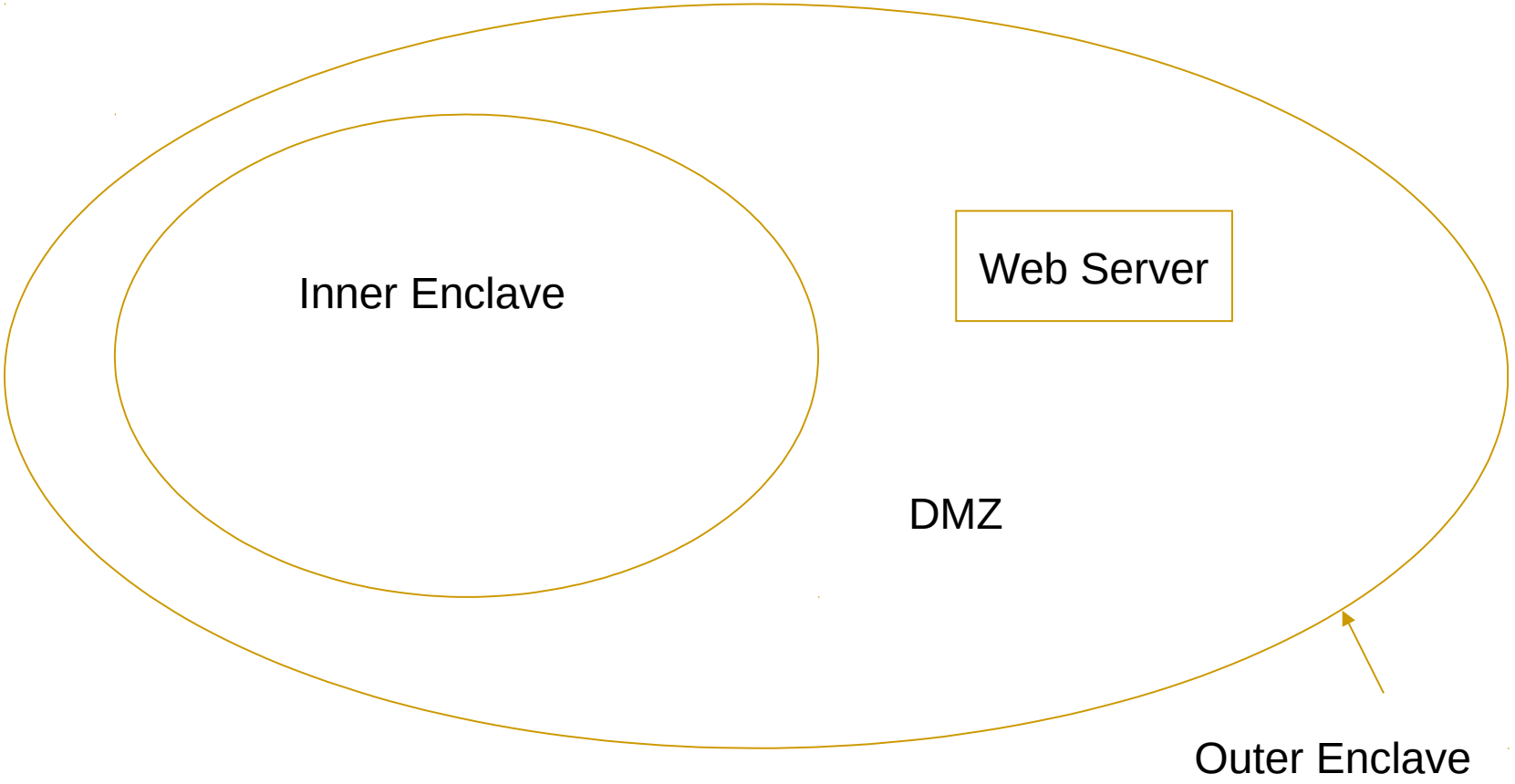
Web Servers behind Firewalls

- Pros:
  - The Web server itself is protected
- Cons:
  - Web Servers often host Web applications which can be a security loophole and can reduce the security of other hosts inside the firewall.

Web Server outside Firewall Enclave

- Pros:
  - Everything else inside the enclave is safer.
- Cons:
  - It is very difficult to protect the Web Server itself.
  - It is difficult to get data (HTTP post) securely into the Firewall Enclave.

DMZ



DMZ

- Web servers put in an outside enclave, protected by a packet-filtering firewall.
- Corporate network inside an (inner) enclave.
- The outer fire either directs traffic to Web Server or inside firewall.
- The middle network sometimes known as a DMZ (Demilitarized Zone).
- Sometimes the DMZ provides a VPN to allow remote administration of Web Server.

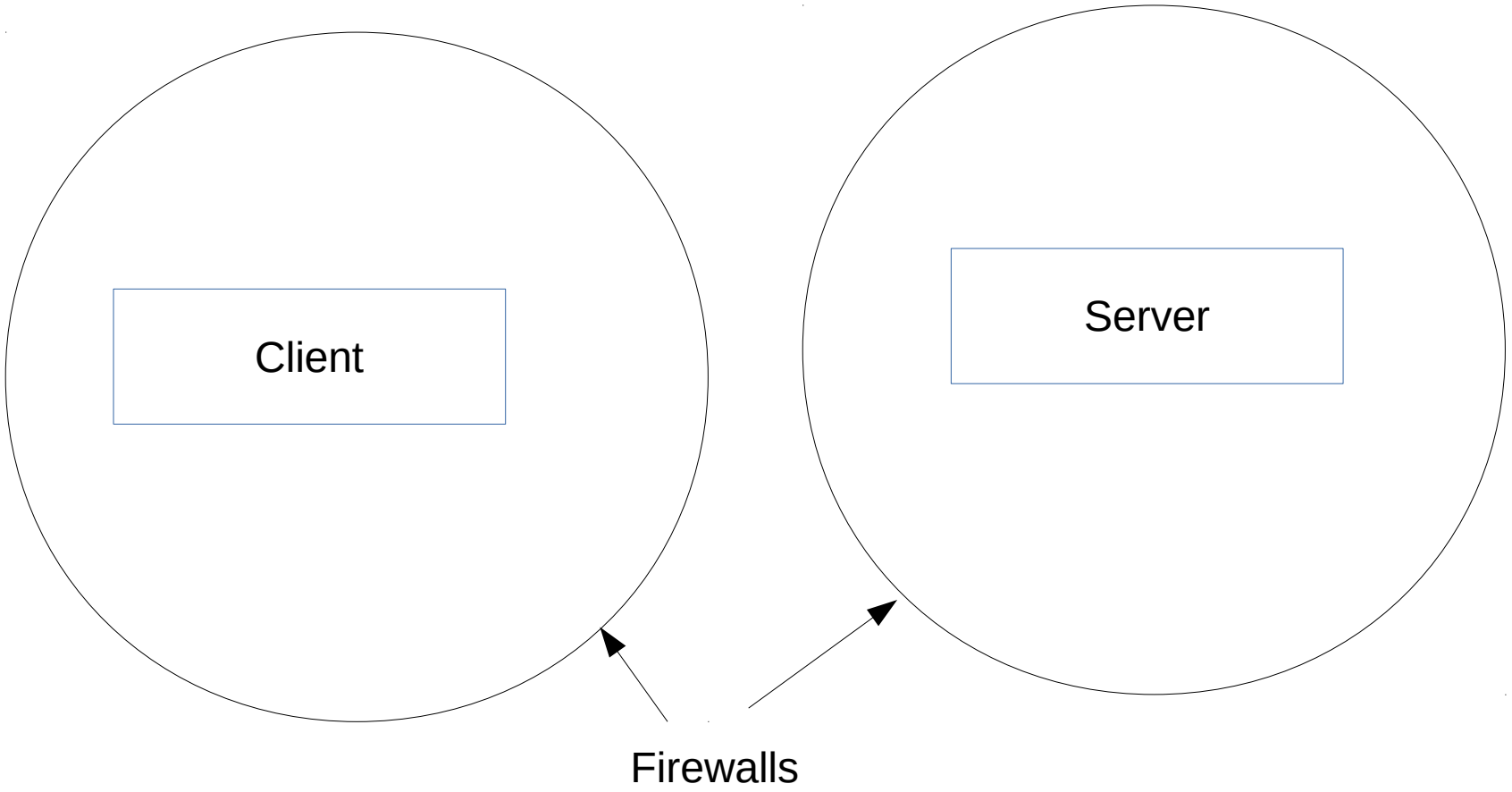
Problems with Firewalls

- Firewalls can be a problem for users (not allowed to do what they want to do, for example downloading ZIP files).
- Maven – needs to be configured for proxy server. (Plugins downloaded as JAR files).
- Grails – plugins downloaded as zip files.
- [Dan's Guardian (&Squid) configured with grails.org added to a whitelist of sites.]
- This requires communication with the firewall administrator.

Firewalls and RMI

- Firewalls are a problem for developers of distributed applications using RMI.
- Firewalls on the client side are normally not under the control of the distributed application developer.
- They often (always?) forbid the client server interaction over JRMP (Java Remote Method Protocol).
- (Port number 1099.)
- This is a problem for internet application but not intranet applications.

Firewalls and RMI



Web Services

- JRMP (or IIOP) are binary protocols.
- They were never designed to run over HTTP.
- Hence the evolution of Web Services.
  - Run over HTTP
  - Text messages (XML or JSON)
- No problem with client side firewalls.
-