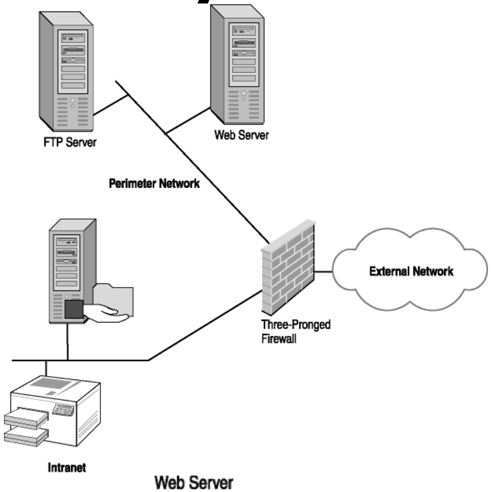
Network Services, Virtualisation, and Cloud Computing

Network Services

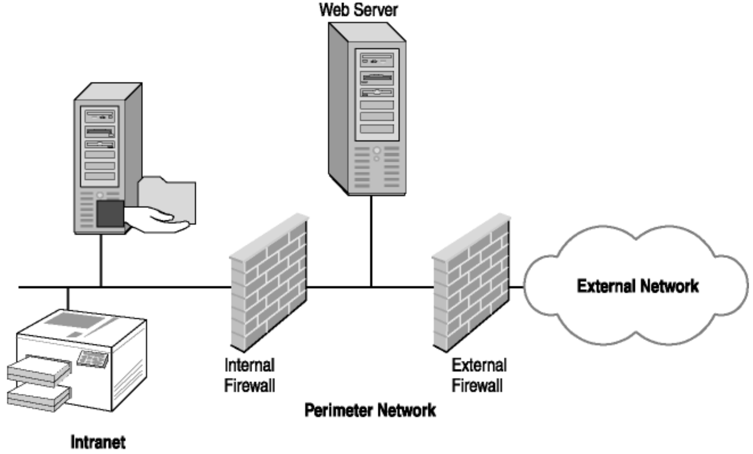
- Client – Server architecture
- Servers often named for the service they provide
- Dedicated Servers
  - Provide a specific service only.
- Non-dedicated Servers
  - Provide several services
- Firewalls can be placed on either type

Screened Subnet (DMZ)

- Three Pronged Firewall
  - Three interfaces



- Two Pronged Firewall
  - 2 firewalls - better protection



Servers

- Web Server
  - In the DMZ
  - Port 80 for HTTP
  - Port 443 for HTTPS
  - Port 20 and 21 for FTP
- File Server
  - Ease of access to files for collaboration
  - Centralised Security
  - Backups are easier
  - NAS (network attached storage) is a dedicated server
  - SAN (storage area network) is a collection of servers to store data

Print Servers

- Allows users to see printers
- Often combined with File servers
- Makes printers available on the network
- Accepts print requests
- Manages print requests using a queue
- Can process and store print jobs

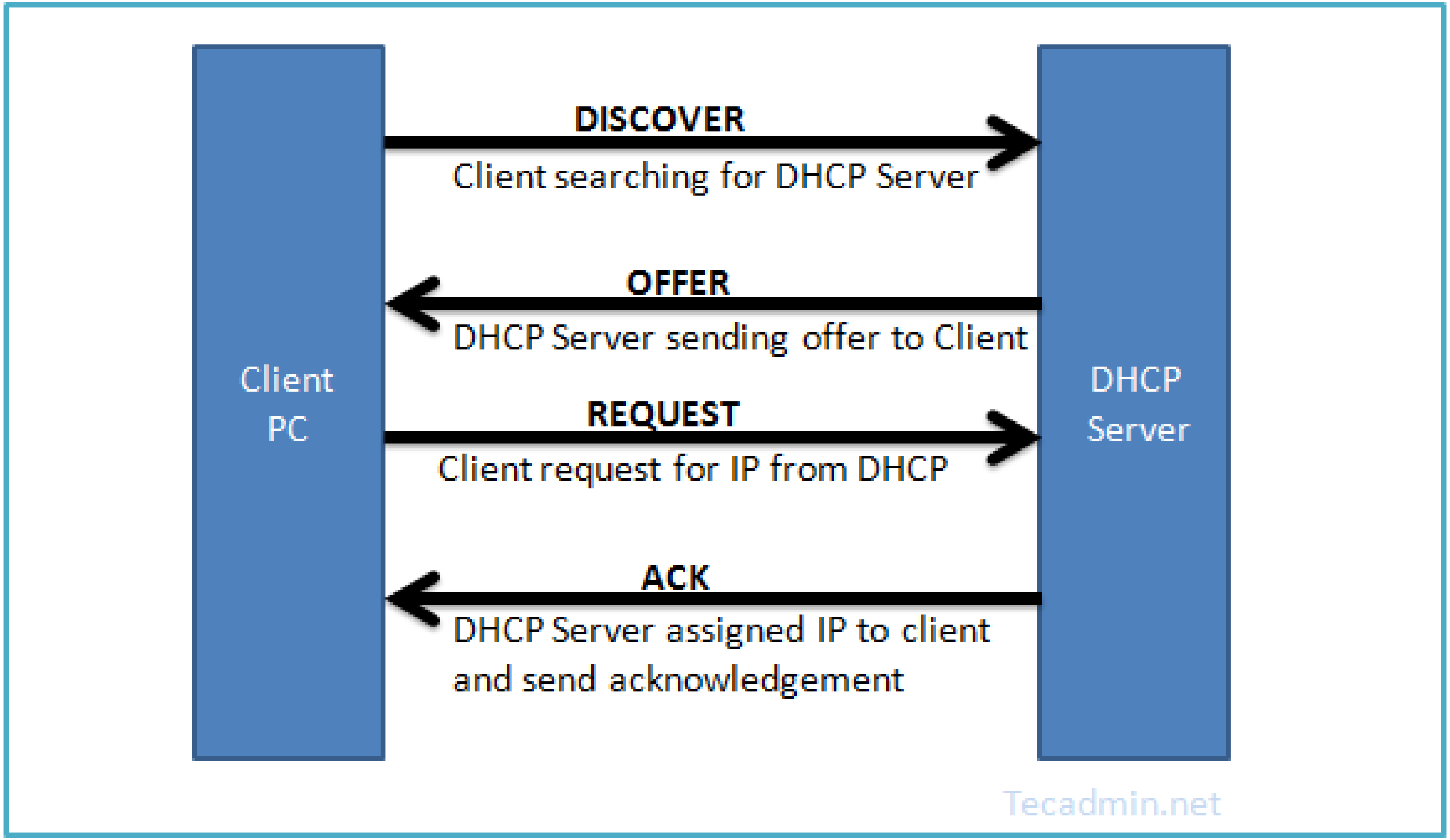
DHCP Server

- DHCP Scope
  - The information the server can provide
  - At least one scope is needed but more than one can be provided
- Address Pool
  - Range of addresses that can be provided to clients
  - If IPv4 then Subnet mask is included
- Lease Duration
  - Addresses to clients have a time limit
  - Clients renegotiate leases before expiry
  - Generates network broadcast traffic

DHCP Server

- Address Reservation
  - Specific clients can have allocated IP addresses – static addresses
  - Servers and printers have Static IP addresses
  - Uses MAC address
- Scope Options
  - Router and DNS server information
  - Time (NTP – Network Time Protocol)

DHCP – DORA process



Client PC

DHCP Server

DISCOVER

Client searching for DHCP Server

OFFER

DHCP Server sending offer to Client

REQUEST

Client request for IP from DHCP

ACK

DHCP Server assigned IP to client and send acknowledgement

DHCP

- Broadcast messages do not go through routers
- Excessive Broadcast messages can slow network
- APIPA
  - 169.254.x.x

DNS – Domain Name Server

- Resolve Hostnames to IP Addresses
- Uses UDP or TCP port 53
- Local DNS should be placed in the DMZ
- Same on Intranet as the Internet
- ISP’s maintain DNS for companies.
  - Two DNS servers needed for redundancy
- DNS Server has a zone file
  - (see https://en.wikipedia.org/wiki/Zone_file)

DNS Zone File

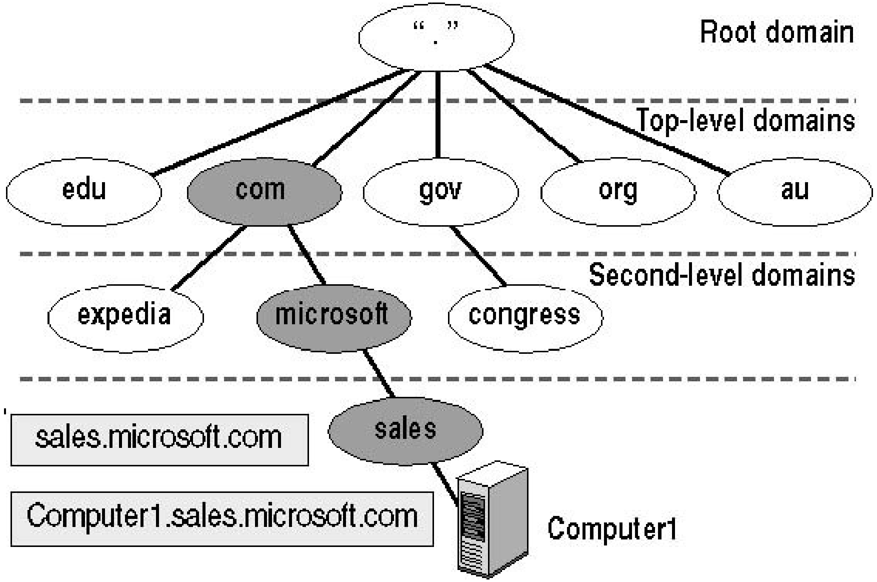
- 5 Columns
  - Name of the server or computer
  - IN – means internet
  - Record Type – See next slide
  - Address of the computer
  - Comments – must have semicolon
- Managed by the DNS administrator
- Zone file breakdown
  - http://www.zytrax.com/books/dns/ch6/mydomain.html

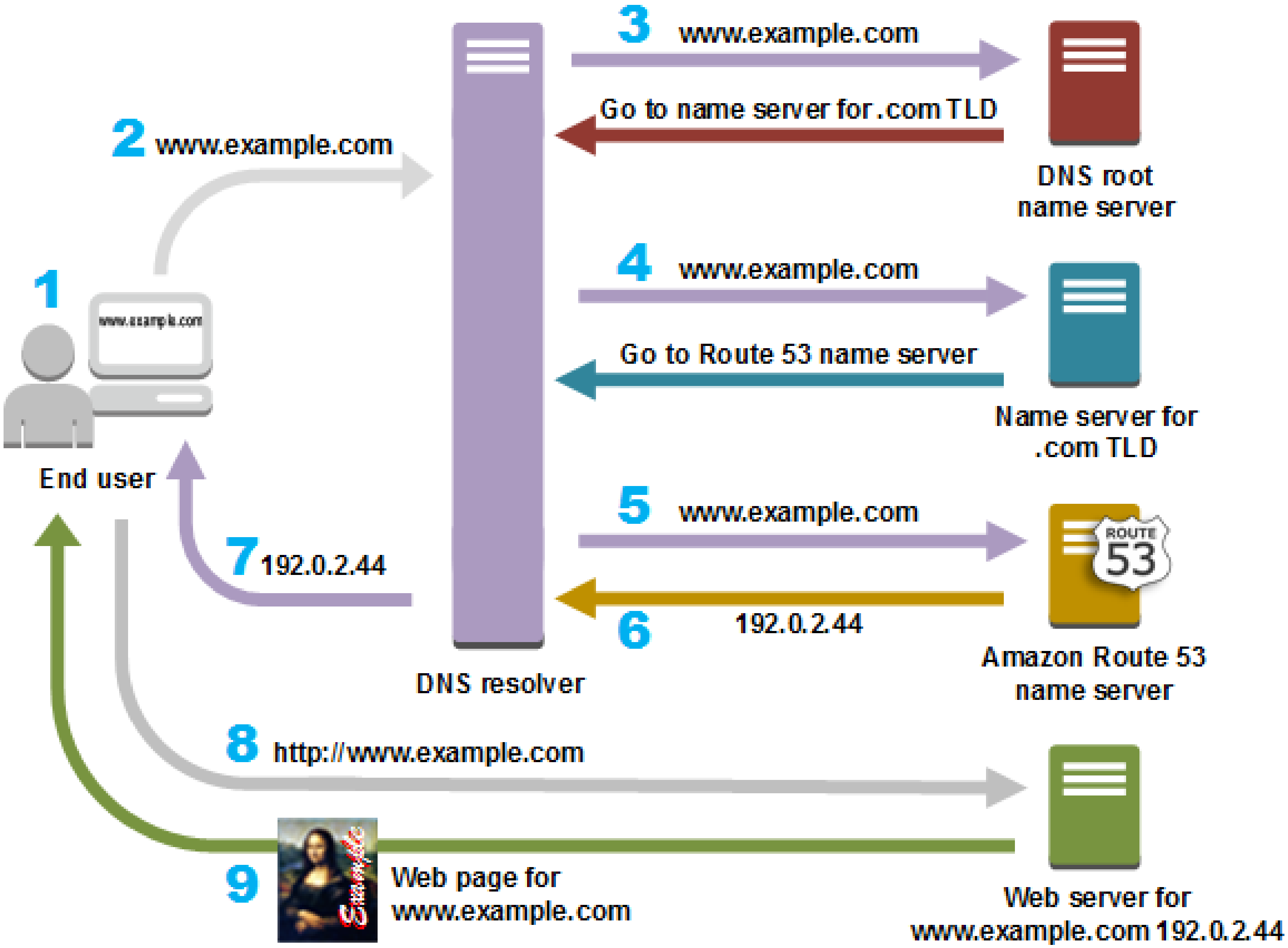
Common DNS Record Types

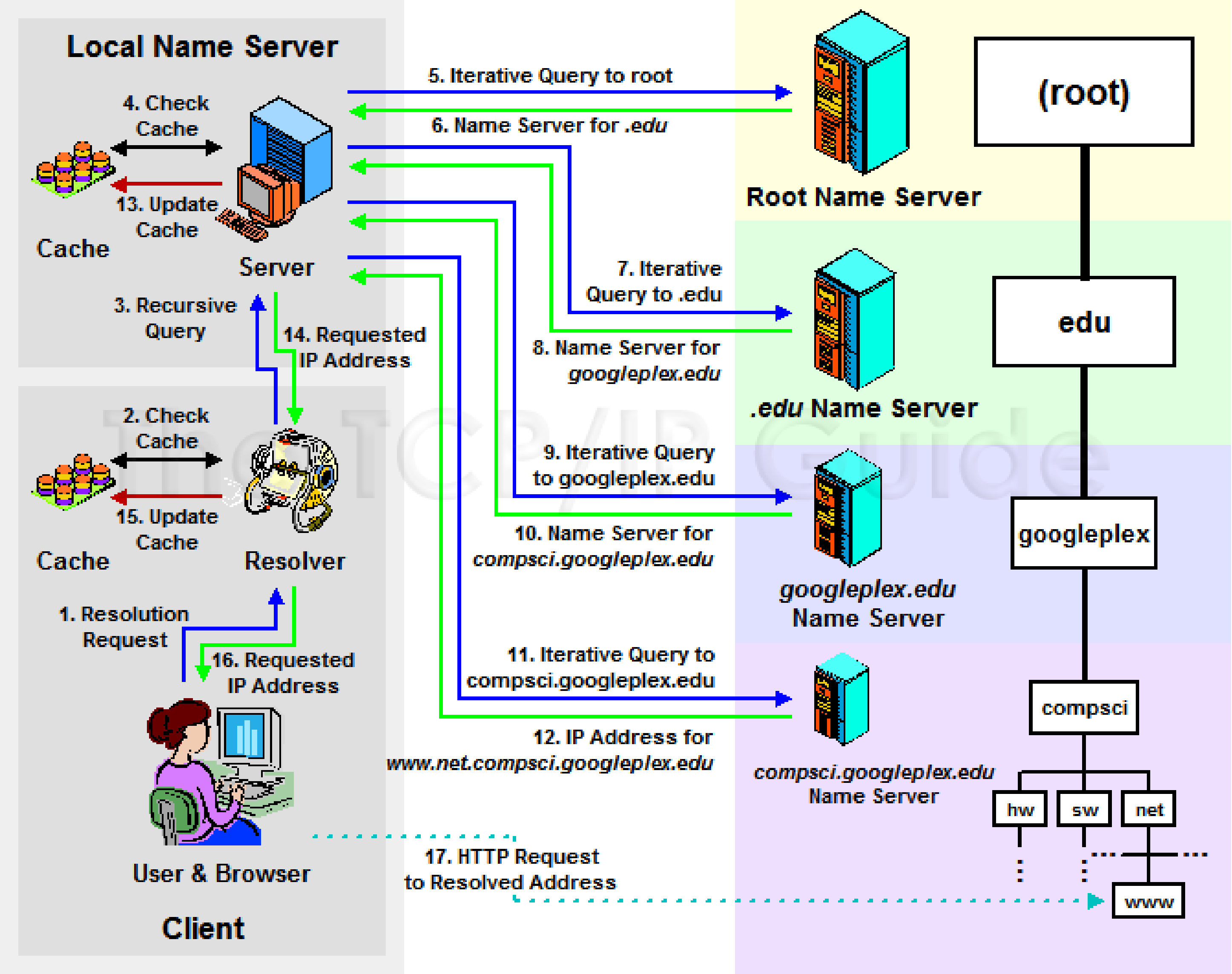
- SOA – Start of Authority
- NS – Name Server (Name or address of the DNS server for the zone)
- MX – Mail Exchanger (Name or address of email server)
- A – IPv4 host record
- AAAA – quad A – Host record for IPv6
- CNAME – Canonical Name. An alias to allow multiple names to be assigned to the same host or address

Internet DNS

- First check zone file
- Then cache – a temporary store of recent resolved names and IP addresses
  - Improves subsequent resolutions
- Trailing dot (in first few rows) – signifies the root
  - 13 global root servers
  - TLD – top level domain
  - SLD – Second Level Domain
  - Subdomains (optional)
  - Host
- www.yahoo.com is actually www.yahoo.com.
  - Did you notice the trailing dot in Zone file?



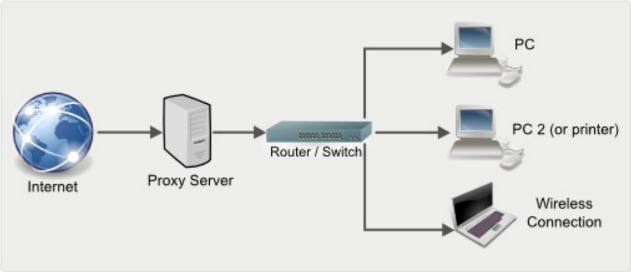

3 www.example.com
Go to name server for .com TLD
2 www.example.com
DNS root name server
4 www.example.com
1
www.example.com
Go to Route 53 name server
Name server for .com TLD
End user
5 www.example.com
ROUTE 53
7 192.0.2.44
6 192.0.2.44
DNS resolver
Amazon Route 53 name server
8 http://www.example.com
Example
9 Web page for www.example.com
Web server for www.example.com 192.0.2.44



Local Name Server
4. Check Cache
13. Update Cache
Cache
Server
3. Recursive Query
14. Requested IP Address
2. Check Cache
15. Update Cache
Cache
Resolver
1. Resolution Request
16. Requested IP Address
User & Browser
Client
5. Iterative Query to root
6. Name Server for .edu
7. Iterative Query to .edu
8. Name Server for googleplex.edu
9. Iterative Query to googleplex.edu
10. Name Server for compsci.googleplex.edu
11. Iterative Query to compsci.googleplex.edu
12. IP Address for www.net.compsci.googleplex.edu
17. HTTP Request to Resolved Address
Root Name Server
.edu Name Server
googleplex.edu Name Server
compsci.googleplex.edu Name Server
(root)
edu
googleplex
compsci
hw
sw
net
www

Proxy Server

- Makes requests for resources on behalf of a client
- Slows Internet Browsing
- But speeds up subsequent searches
- Filters requests – blocking prohibited websites
- Can modify the requesting PCs information (e.g. blocking senders identity – provides a level of security)
- All requests to internet go through the proxy server, so it needs to have adequate resources to handle traffic



Mail Server

- anti-spam
- Encryption/Decryption
- Located in DMZ
- Protocols
  - SMTP – Port 25 – Sends emails between mail servers. Push Protocol.
  - POP3 – Port 110 – Receiving Emails. Pull Protocol.
  - IMAP4 – Port 143 – Receiving email. Newer and is superior to POP3. Pull Protocol.

Authentication, Authorisation, and Accounting (AAA)

- Security required to protect resources
  - Open access is not an option
  - Completely closed access not an option
- Triple A server
  - Quad A if auditing added
- AAA servers check credentials

Authentication Server

- Examines credentials of user to access the network. Gatekeepers
- Dedicated machines / routers / switches / RAS – Remote Access Server
  - Domain Controller – Centralized Authentication Server
  - RADIUS – Remote Access Dial in User Service
  - TACACS+ - Terminal Access Controller Access-Control System Plus
  - Kerberos
- Some need security token
- Single Factor Authentication
  - Normally just a password and username
- Multi Factor authentication – normally two of these three
  - Something user knows (password or pin)
  - Something the user has e.g. smart card, Pin from security token
  - Something they are. Biometrics.
- Authentication Servers in DMZ if external users login

Authorisation

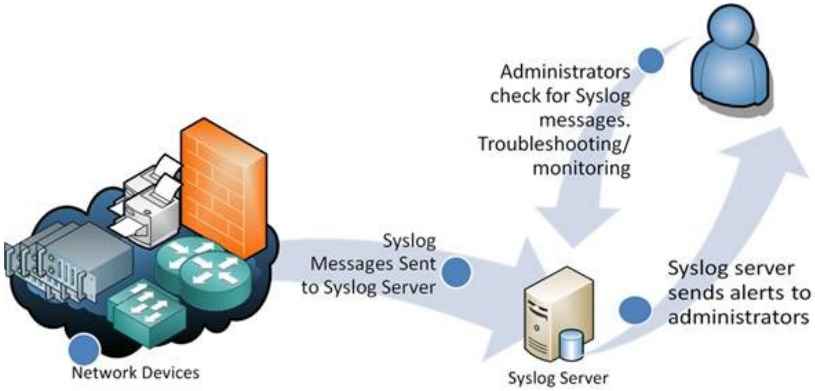
- Next step in access control is called authorisation
- Only allow user access to what is needed
- Principle of least privilege
  - Only give users what they need to do their job

Accounting

- Final step after authentication and authorisation
- Tracking what the users do
  - What they access and when
  - Actions performed
- Normally done through logs
  - Event Viewer is MS basic logging

Syslog Server

- Allows administrators to monitor network/server status
- Event Messages
- Listeners
  - listen on Port 514
  - Database storage
  - Management and filtering facilities
- https://www.networkmanagementsoftware.com/what-is-syslog/



Administrators check for Syslog messages. Troubleshooting/ monitoring
Syslog Messages Sent to Syslog Server
Syslog server sends alerts to administrators
Network Devices
Syslog Server

Internet Appliances

- A Device that makes internet access easy
- Intrusion Detection Systems (IDS)
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM)
- IDS and IPS – look for activity that could be harmful
- IDS – Passive and sends emails to administrators
- IPS – Active and will try and stop an attack

Unified Threat Management

- Centralises security management to manage through an interface.
  - Firewall
  - Anti-malware
  - Anti-spam
  - Content filtering
  - IPS
- Single device
- Single Point of Failure (SPoF)
- Replaces firewall – next generation of Firewall?

Internet Appliances – Spam Gateways

- Every users problem!
- An appliance that specifically blocks emails from entering the network
- Located in cloud or on internal network
- Emails go through the gateway before being passed to email server
  - The spam folder will need to be checked for false positives

Internet Appliances – Load Balancing

- Large companies (e.g. Amazon) have more than one server, possibly 100’s
- Load Balancing ensures that one server is not overloaded
- In cloud or local hardware
- Cross Region Load Balancing
  - Amazon.com / Amazon.co.uk / Amozon.fr etc.
- Content based Load Balancing
  - Switches requests based on content request
    - e.g. Web, Video Streaming, Downloads, etc.

Load Balancing Benefits

- Performance
  - Servers can be configured to provide specialised services
- Scalability
  - Demand spikes can be handled by providing more servers. For example - Black Friday offers
- Reliability
  - Business Critical applications
  - Traffic can be redirected in the event of a server outage

Legacy and Embedded Systems

- Hardware, Software or Network Protocol
- Embedded System – Critical in a systems process
- Replacing Expensive
- If its not broken, don’t fix it
- Repair expensive
- Spare parts scarce
- Specialised skills to maintain
- Move to Virtualisation!