PDF version download HTML version download

📣 About

The main objectives of this repo

- This is a *'Open Source Study Guide'* for Security+ SY0-501, gathering as many information as possible from many sources on internet to ensure to cover all topics presented on exam.
- The second objective is to help you pass the exam without paying any expensive training courses and also contribute to infosec community <3 .

ℹ️ About the exam

⚠️ **Important Note: The SY0-501 exam is scheduled to be retired in July of 2021** ⚠️

CompTIA Security+ is the first security certification IT professionals should earn. It establishes the core knowledge required of any cybersecurity role and provides a springboard to intermediate-level cybersecurity jobs. Security+ incorporates best practices in hands-on trouble-shooting to ensure security professionals have practical security problem-solving skills. Cybersecurity professionals with Security+ know how to address security incidents – not just identify them.

Security+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. Regulators and government rely on ANSI accreditation, because it provides confidence and trust in the outputs of an accredited program. Over 2.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011. [+]

☑️ Exam Domains

Domain	% of the Exam Content
Threats, Attacks and Vulnerabilities	21%
Technologies and Tools	22%
Architecture and Design	15%
Identity and Access Management	16%

Domain	% of the Exam Content
Risk Management	14%
Cryptography and PKI	12%

✳ Free Resources

1. Practice Questions - Examcompass - I recommend to test your knowledge after study all topics presented on the exam.
2. Practice Questions - Professor Messer
3. Practice Questions - Github
4. Training Course - Professor Messer - 141 YouTube videos (13 hours of content).
5. Lynda Prep Course - 30 day free trial - 21 hours of content

---

- **Index**
    1. Securing Systems
    2. Security Tools
    3. Networks and Infrastructure
    4. Identity and Access Management
    5. Risk Management
    6. Incident Response & Forensics
    7. Testing the Infrastructure
    8. Cryptography

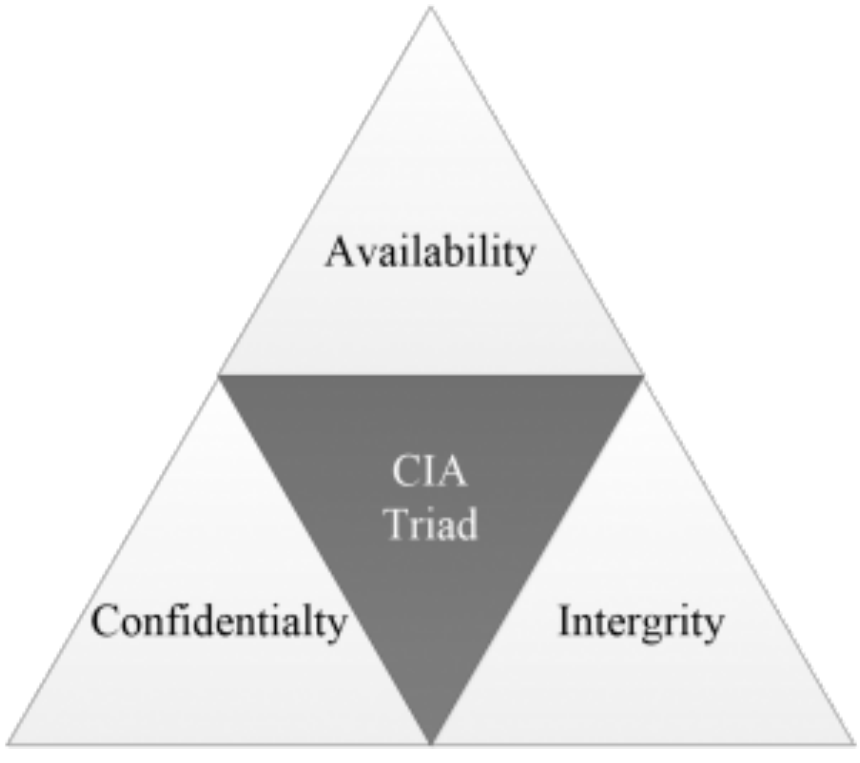
Brief Introduction

Information security, sometimes shortened to infosec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or at least reducing the probability of unauthorized/inappropriate access, use, disclosure, disruption, deletion/destruction, corruption, modification, inspection, recording or devaluation, although it may also involve reducing the adverse impacts of incidents.

Goals of Security

The CIA triad is put into pratice through various security mechanisms and controls. Every security technique, practice, and mechanism put into place to protect systems and data relates in some fashion to ensuring confidentiality, integrity, and availability.

The CIA Triad



Confidentiality

Keeping systems and data from being accessed, seen, read to anyone who is not authorized to do so.

Integrity

Protect the data from modification or deletion by unauthorized parties, and ensuring that when authorized people make changes that shouldn't have been made the damage can be undone.

Availability

Systems, access channels, and authentication mechanisms must all be working properly for the information they provide and protect to be available when needed.

Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO/IEC 27000:2009)

Auditing & Accountability

Basically keep tracking of everthing, like, who's been logging in when are they loggin in whose access this data.

Non-Repudiation

Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

---

1. Securing Systems

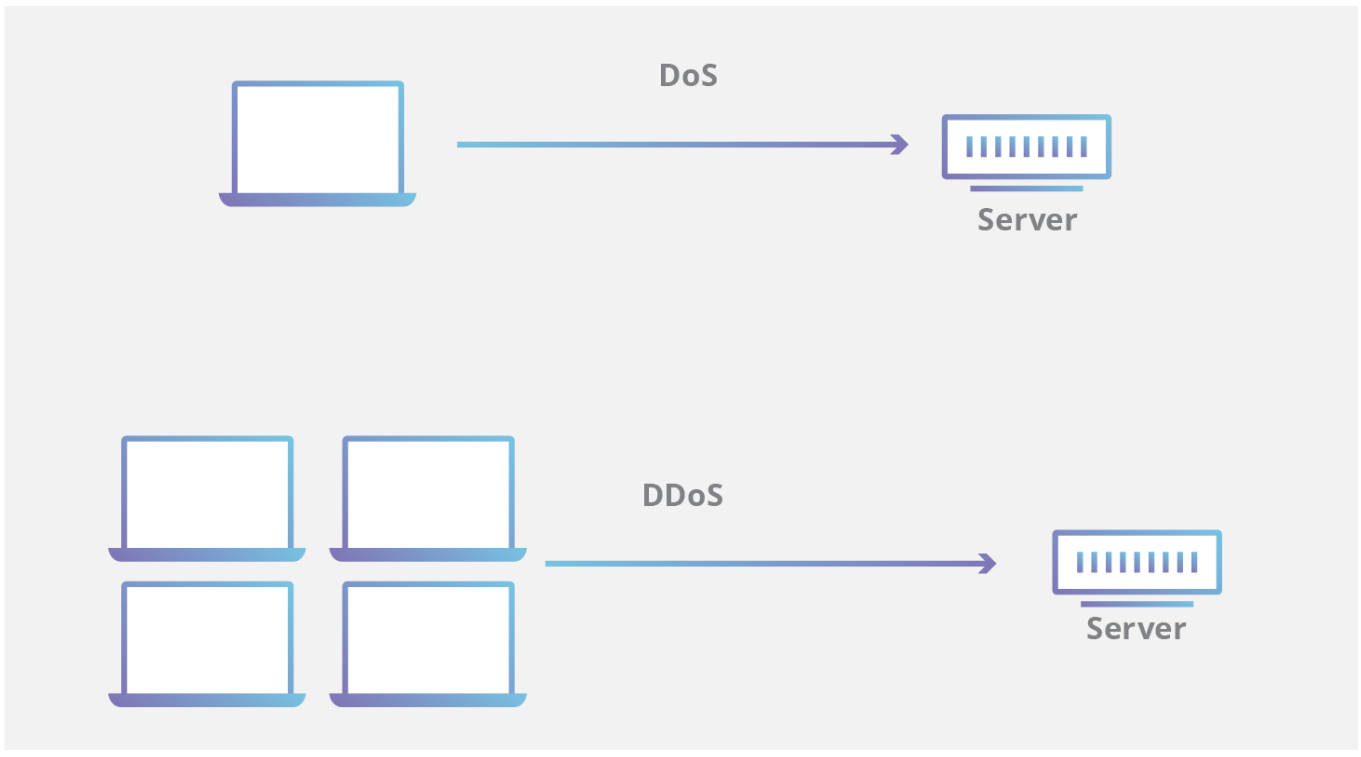
Understanding Attacks

Denial-of-Service (DoS)

- Prevents others from accessing a system / comprimising the availability.

Distributed-Denial-of-Service (DDoS)

- Uses multiple systems to attack a single host - Generally controlled by **BotNets**, which is a type of malware that uses remotely controlled malicious software to control a large range of computers.



- **Volumetric Attack**
  - **Ping Flood**
    - *A ping flood is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP "echo request" packets.*
  - **UDP Flood**
    - *A UDP flood is a form of volumetric Denial-of-Service (DoS) attack where the attacker targets and overwhelms random ports on the host with IP packets containing User Datagram Protocol (UDP) packets.*
- **Protocol Attack**

    - **SYN Flood/TCP SYN Attack**
        - A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic

- **Application Attack**

    - **SlowLoris Attack**
        - *Tries to keep many connections to the target web server open and hold them open as long as possible*

- **Amplification Attack**

    - Generate a high volume of packets to flood the target website without alerting the intermediary, by returning a large reply to a small request. The basic defense against these attacks is blocking spoofed-source packets.

- **Smurf Attack**

    - Flooded with spoofed ping (ICMP) packets.

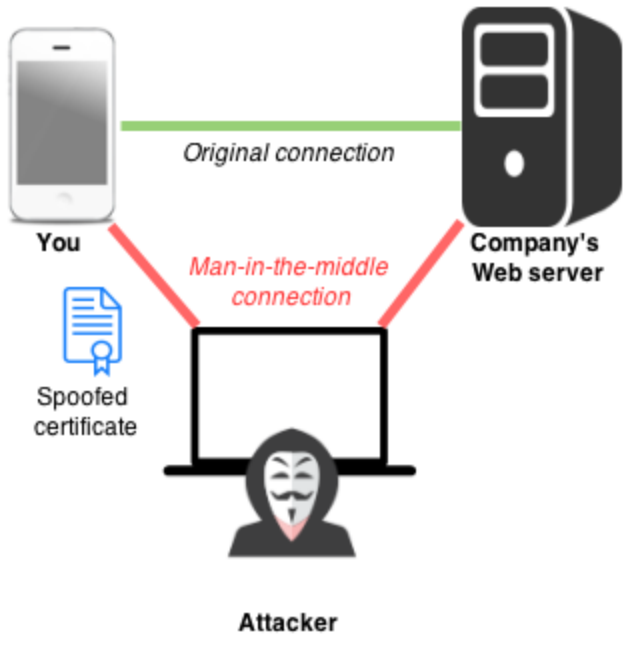
🛑 **ICMP (Internet Control Message Protocol)** is an error-reporting protocol network devices like routers use to generate error messages to the source IP address when network problems prevent delivery of IP packets.

Common Host Threats

- **Spam** - Spam is electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.
- **Phishing & Spear Phishing** - The difference between both is that Spear Phishing is for targeted individuals with some type of information about the victim embeded.
- **Spim** - Phishing through instant messaging
- **Vishing** - Unsolicited use of voice to get sensitive information
- **Click Jacking** - malicious click bait sites that forces you type your PII or download some malicious software.
- **Typo squatting** - Mistype URL's (e.g. - facebook.corn)
- **Domain Hijacking** - the act of changing the registration of a domain name without the permission of its original registrant, or by abuse of privileges on domain hosting and registrar software systems.
- **Privilege Escalation** - is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.

Man-in-the-Middle Attack

- Third-party intercepting between a two-party conversation
- Uses the information to the third party's advantage



- **Wireless MITM**
    - 802.11
    - Bluetooth
- **Wired MITM**
    - Spoof MAC address, IP address, ARP, DNS...
- **Typosquatting** - Type of URL hijacking *(e.g facebook.corn / wikipdia.org)*
- **Domain Hijacking**
- **Replay atack** - when an attacker detects a data transmission and fraudulently has it delayed or repeated. *(e.g The attacker can capture a request sent from victim and replay it to the server).*
- **Downgrade attack** - is a cryptographic attack that makes it change the encrypted connection to the older one *(e.g. cleartext).*
- **Session Hijacking** - Inject information on middle of connection

System Resiliency

Resilient systems don’t eliminate risk. Resilient systems fight off attacks more readily than systems with less resilience. They handle risks better, in other words. The principles here apply to individual systems and to larger systems.

- Generally they handle risks better, adding technologies and processes to enable the system recovery easily.

Scalability

- Adding more resources to take care the demand (manually added)

Elasticity

- The resources grow on demand as they required (e.g. IaaS)

Redundancy - Distributed Allocation

Is a form of distributive allocation.

- Web servers, database servers, middleware, security devices, monitoring systems
- Easier to add security between the segmented areas

- **Mass storage**
- **Redundant systems**
- **Redundant networks**

You can create more than one copy of non-OS critical data so that if one copy dies, another copy is ready to go to keep the systems up and running.

Redundancy and Fault tolerance

- **Maintain uptime**
  - The organization continues to function
- **No hardware failure**
  - Server keep running
- **No software failure**
  - Service always available
- **No system failure**
  - Network performing optimally
- **Redundant hardware components**
  - Multiple devices, load balancing power supplies
- **RAID**
  - Redundant Array of Independent Disks
- **UPS - Uninterruptible power supplies**
  - Prepare for the disconnections
- **Clustering**
  - A logical collective of servers
- **Load balancing**
  - Shared service load across components

Non-persistance

Is data that is collected but will not be saved on restart.

- **Snapshots** - take the current state of something (e.g binary level) and store. A snapshot reverts to known state.
- **Virtualization**
- **Revert/rollbacks tools** - The rollback method bring the system back to a previous state. (e.g. Bad Driver, broken Updated etc).
- **Live boot**

RAID - (Redudant Array of Independent Disks)

Different levels of RAID arrays or combination is for:

- Improve disk access.
- Improve fault tolerance and data integrity.
- Or both

RAID Level	Description	Details
RAID 0	Striping without parity	High performance, no fault tolerance
RAID 1	Mirroring	Duplicates data for fault tolerance, but requires twice the disk space
RAID 5	Striping with parity	Fault tolerant, only requires an additional disk for redundancy
RAID 0+1, RAID 1+0, RAID 5+1, etc.	Multiple RAID types	Combine RAID methods to increase redundancy

RAID 0

- **Has no data integrity.**
- **Improves speed** - data striping(divide the data into pieces in X hard drives); RAID0 speeds up performance but has no integrity, because if one of these hard drives fail, the data is lost.

RAID 1

- **Has data integrity** - but doesn't have performance ; slow process because the data processed in all hard drives.

RAID 5

- **Has disk striping with parity** - parity information is spread across all disks evenly; 1/n of the total disk space available is used for parity. You can only loose one drive and keep the data, the problem is if you loose more than one drive.

RAID 6

- **Disk parity with double distributed parity** - Same as RAID 5 but has one more parity which you can loos two drives and keep your data safe.

RAID 0+1 (01)

- **Disk striping with mirroring** - combines both RAID levels 0 and 1 for performance and redundancy; a mirror of two striped arrays.

RAID 1+0 (10)

- **Disk mirroring with striping** - combines both RAID level 0 and 1 for performance and redundancy; a strip of two mirrored arrays.
  - **The most common RAID styles includes 0, 1, 5 and 10.**
  - **RAID 1 and RAID 0 requires at least 2 drives.**
  - **RAID 5 requires 3 or more drives and RAID 10 requires 4 drives.**

NAS and SAN

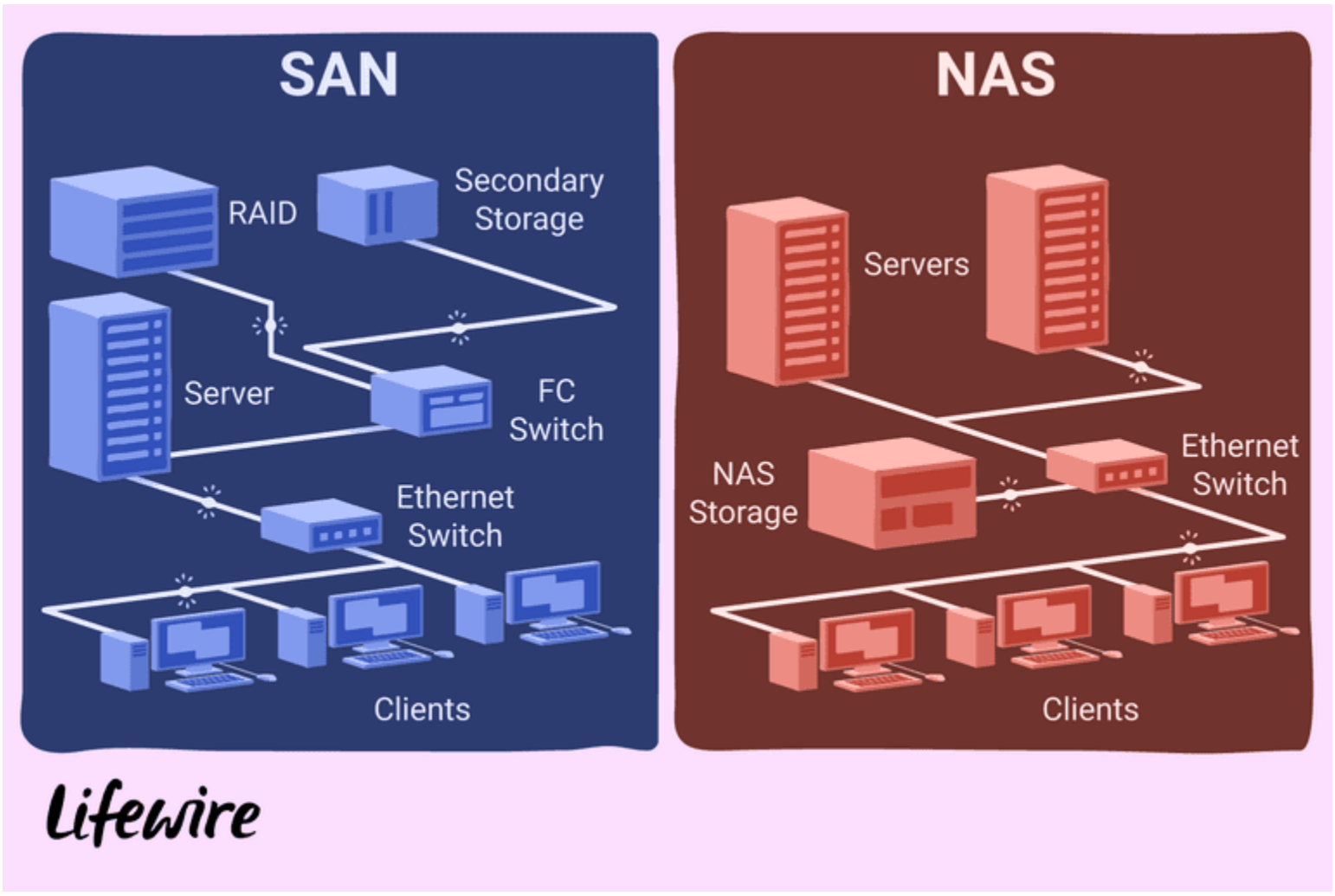
Storage Area Networks and **Network-Attached Storage** both provide networked storage solutions. A NAS is a single storage device that operates on data files, while a SAN is a local network of several devices.

Network Attached Storage (NAS)

- Runs over a standard network
- Shows up as normal shares on network
- Good for small environments
- **File-level**

Storage Area Networks (SAN)

- **SAN runs on block-level storage**
- Fibre Channel (FC) or iSCSI
- Expensive implementation



Physical Hardening

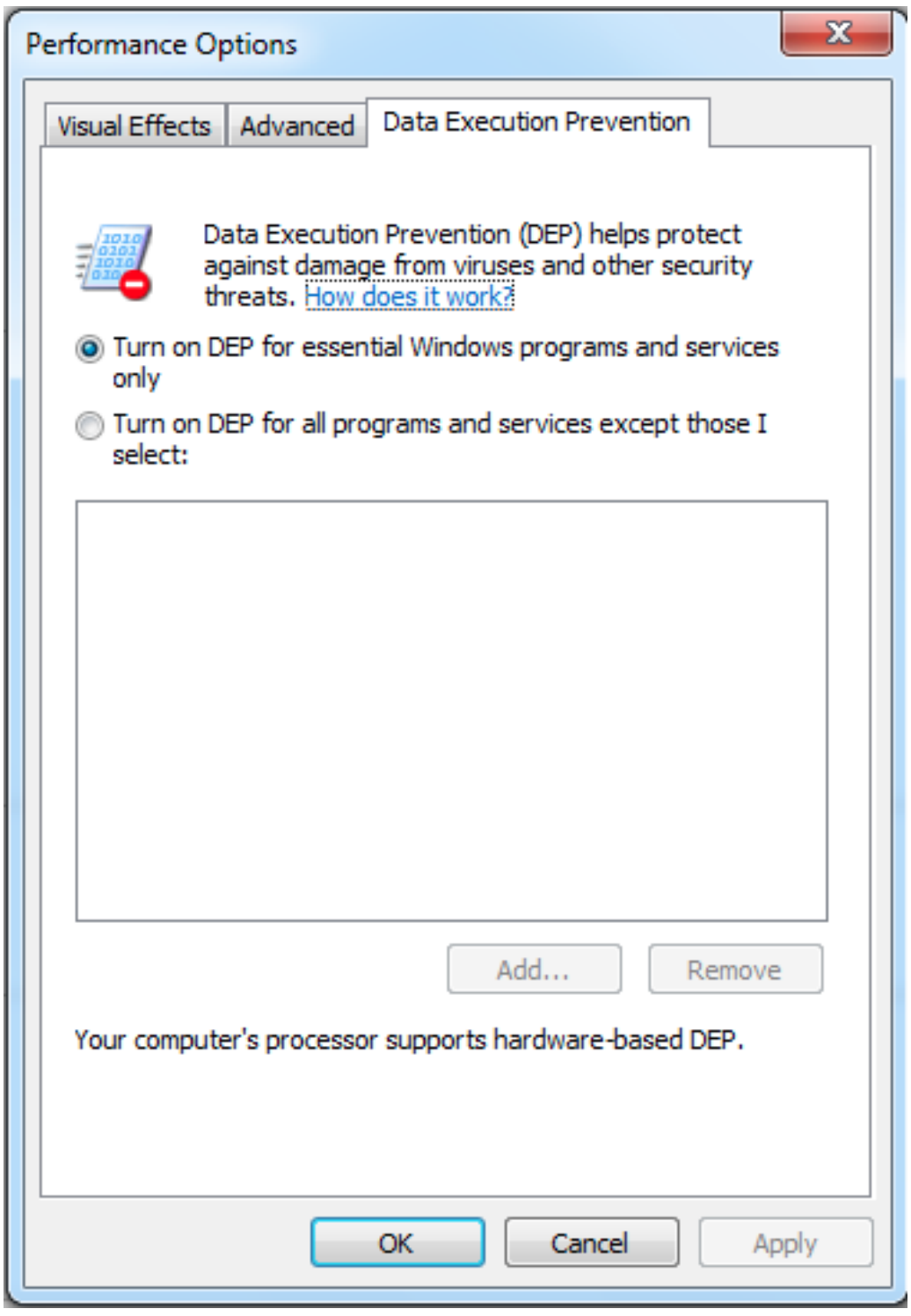
Policies can control how system hardware acts or reacts to an action.

- Removable media controls

Data Execution Prevention (DEP)

DEP is refer to Windows, in generic term is *Executable space protection*; DEP is almost always on by default on Windows.

- Designate sections of memory as executing code or data
  - Code can't run from protected memory locations
  - Prevents malware and viruses from executing



DEP should be always be on, quietly protecting systems from buffer overflows. **The need to turn off DEP is rare**.

- Disabling Ports (can be done in the BIOS); Turn off legacy non-active ports to avoid vulnerable entry point.

RFI and EMI

Electromagnetic Interference (EMI)

Is a disturbance generated by an external source that affects an electrical circuit by electromagnetic induction, electrostatic coupling, or conduction.

- Shielded twisted pair (STP) cable.

- Creating a distance between the device generating the EMI, or shield the emanating device or media.

Security Concerns (without proper shielding)

- Injecting EMI by changing sensor data and other input
- EMI leakage
    - Determine data streams based on EMI emissions; Keyboards, hard drives, network connections

Radio Frequency Interference (RFI)

RFI is EMI that transmits in the **radio frequency** range. (e.g. 802.11, cellular WAN radio bands)...

- Both 802.11 and cellular WANs almost always have automatic channel-hopping features that automatically tune devices to the least congested channel.

Electrostatic discharge (ESD)

Discharge of an electrical current through the air, arcing from a point of a relative positive charge to a point of a relative negative charge.

- Protect equipment by shielding it in protective cases
- Only use properly grounded power supplies
- Anti-ESD wrist strap

Host Hardening

- **Disabling Unecessary Services** - e.g. SSH server, Apache server...
- **Default Passwords** - Simply avoid default passwords and use good password methodologies.
- **Disabling Unecessary Accounts** - e.g. Windows default guest account, Duplicate accounts...
- **Patch Management**
    1. Monitoring patches
        - Might not get reminders
    2. Testing the patches on Sandbox
    3. Evaluating
    4. Deploying the patch
        - Scheduling
    5. Document what is patched

Web server hardening

Make sure that have no data leaks; The server access must be secure.

- Most poupular servers are: Microsoft Internet Information Server, Apache, etc*

- **Security Concerns:**
    - Information leakege, banner information, directory browsing
    - Permissions: Run from a non-privileged account, configure file permissions
    - Configure SSL certificate
    - Log everything - monitor access and error logs

Anti-Malware

- Training for users
- Procedures

        - Best practices
- Monitoring
- IDS
- Third-party anti-malware tools

Host Firewalls

- **Whitelist**
    - Defines all the applications a user is allowed to install
- **Blacklist**
    - Blocked programs

Data & System Security

- Data integrity
- Speed/performance quick access
- High availability

Solutions to secure data:

RAID

- Provides Good integrity
- Provides Good speed
- Affordable

Clustering - Distributive allocation

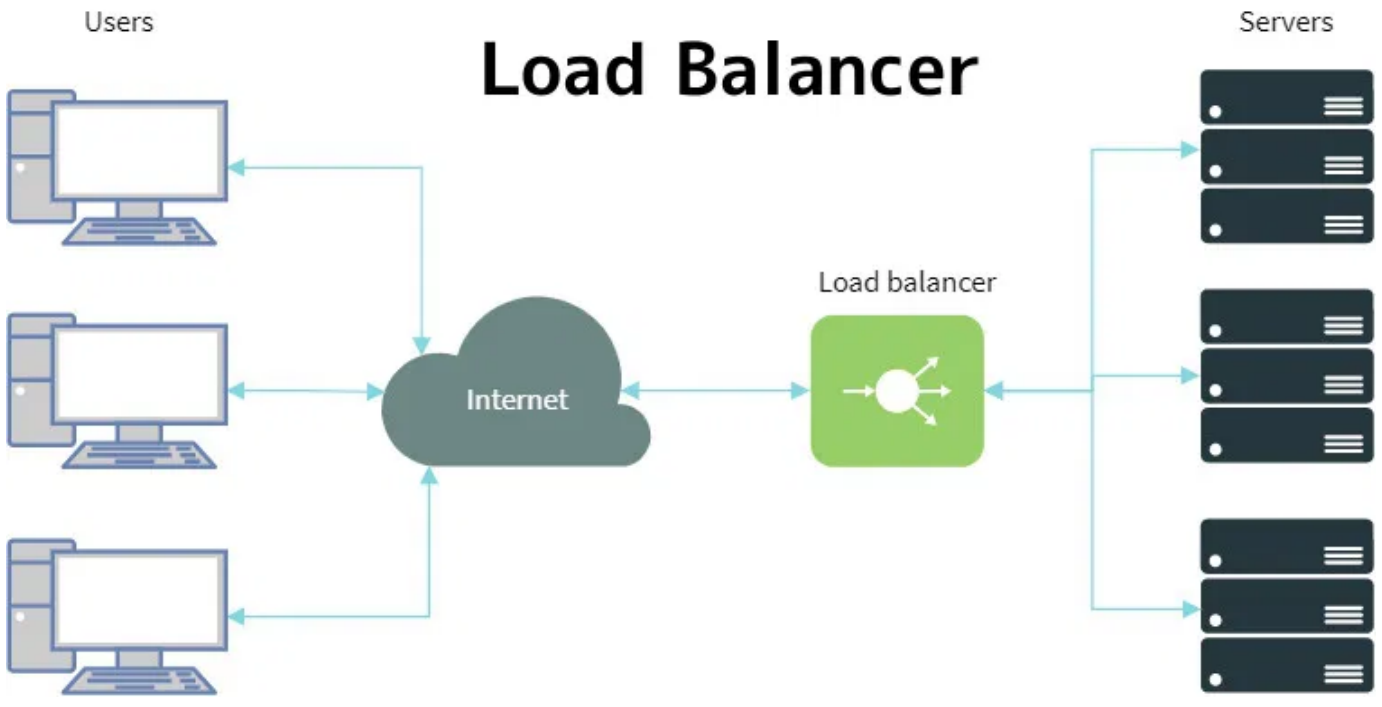
The primary rationale for server clusters is protection against outages and downtime. There are three main reasons for server clustering. They are availability, scalability, and reliability. The key to a protected IT infrastructure lies in redundancy.

- Good method to protect not only Data, but system resources
- Clustering is Expensive

Load Balancing

Refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

- Distributes work loads across multiple machines



- Servers can be added and removed
    - Real-time response to load
- Performs constant health checks
    - If a server disappears, it is removed from the rotation

Virtualize the serves

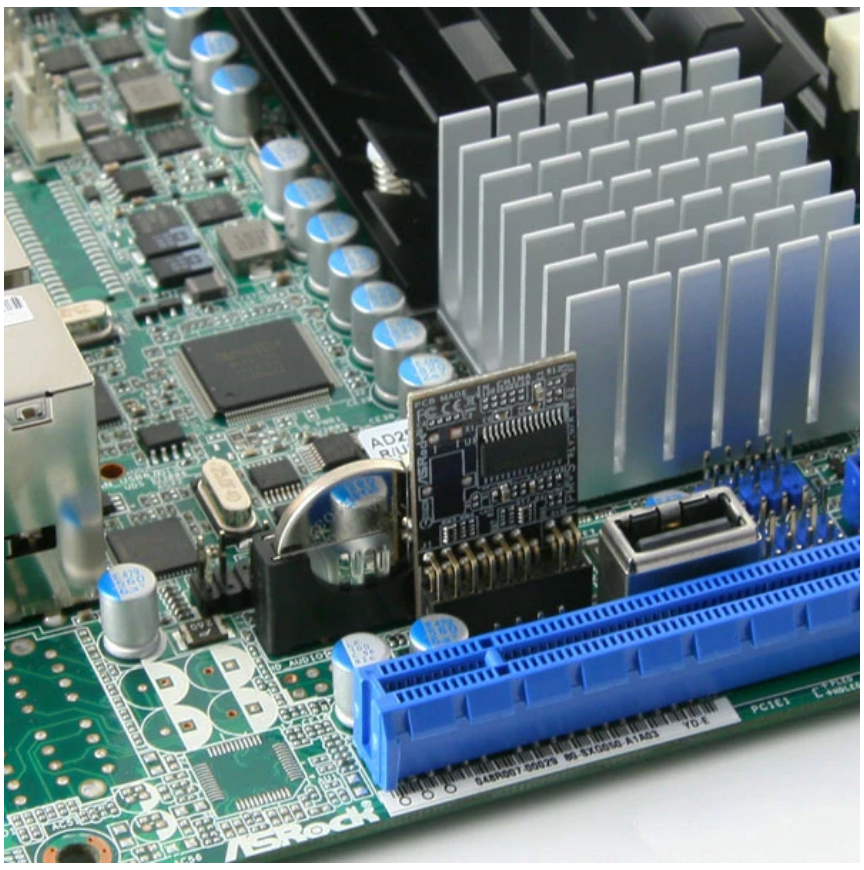
- Scalability
- High-availability comes from elasticity
- Snapshots
- Affordable

Hardware & Firmware Security 💻🔐

Disk Encryption

- **Full Disk Encryption (FDE)**
    - Encrypt an entire drive
    - e.g. Windows - BitLocker
- **Self-encrypting Drive (SED)**

Trusted Platform Module (TPM)



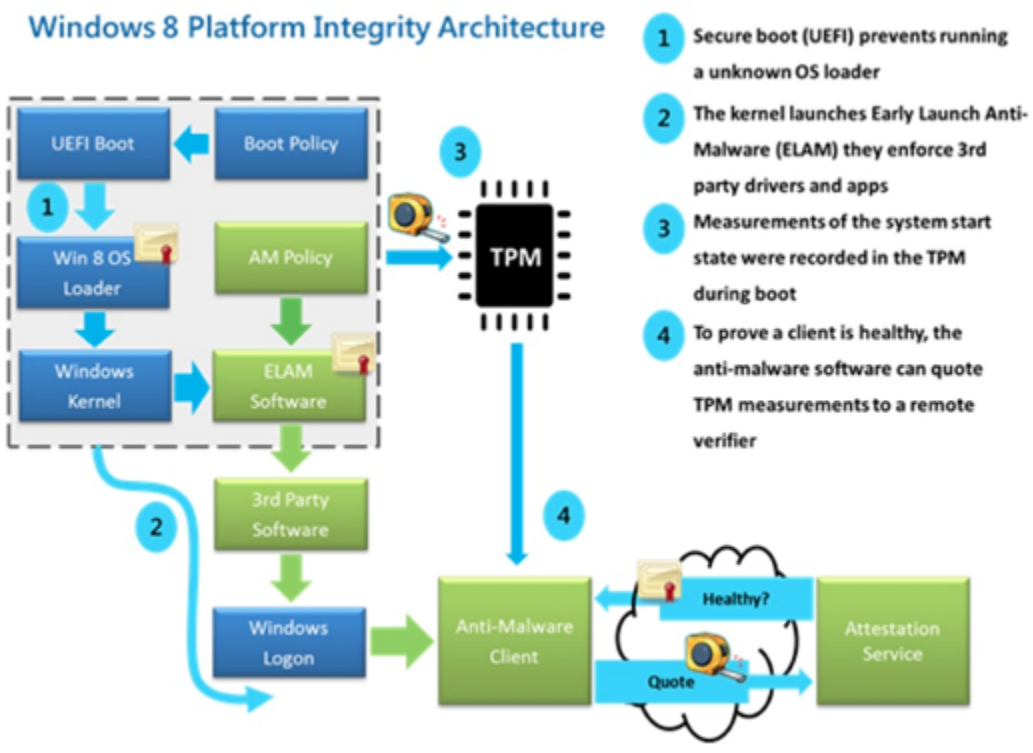
Microchip built into a computer hardware that is used to store cryptographic information(public/private key). *(e.g **BitLocker** 1.2+)*; The OS relies on this **hardware of root trust** to check for low-level changes at boot up.

Examples of disk encryption TPM and non-TPM:

- **BitLocker (for Windows - TPM)**
- **PGP Disk (non-TPM)**
- **TrueCrypt (non-TPM)**
- **FileVault (for macOS - non-TPM)**

  - BitLocker is a built-in Windows Utility Drive Encryption Tool; must have a recovery key to access the data.

Secure Boot - TPM



During the boot process, the TPM and UEFI generate reports about the process and can send those reports to a remote system, like a central authentication server. This process is called **remote authentication** / remote attestation.

- **Secure Boot is built into the UEFI BIOS** specifications. If your system has a UEFI BIOS, it also has the **Secure Boot** functionality.

Remote Attestation

- During the boot, the TPM and UEFI generate reports about the process and can send those reports to a remote system, like a central authentication server. **This process is called remote attestation**.

  - This process is very useful when there are a high number of machines to manage.

- *'Remote Attestation'* and *'Attestation'* is the same thing.

Hardware Security Module (HSM)

Is any type of hardware that's designed to do security work. For ATMs, Web Servers, or other applications that perform an unusually high amount of key handling, it's usually a good idea to offload this work to other hardware.

- Designed for cryptoprocessing
- The gold standard for encryption key security
- **Cryptoprocessors such as HSMs use algorithms to encrypt data to offer an increased level of security. HSMs can encrypt and decrypt information and can manage digital keys.**

Secure OS Types

- **Server OS - RedHat Server, Windows Server etc**
  - Built-in functionality
  - Connections
- **Workstation - Linux Ubuntu, Windows 10 etc**
  - Desktop version
  - Workhorse
- **Embedded Systems - Routers, CCTVs etc**
  - Appliances
  - Their own OS / Usually a minimal OS
- **Kiosk - e.g. Big Touch Screens on Museums, Mall etc**
  - Public device with limited function
  - OS is tightly locked down
- **Mobile OS - Apple iOS and Android OS**
  - Designed for touch screen phones and tablets
  - Optimized for mobile hardware

Picking an OS based on least functionality is a good security practice.

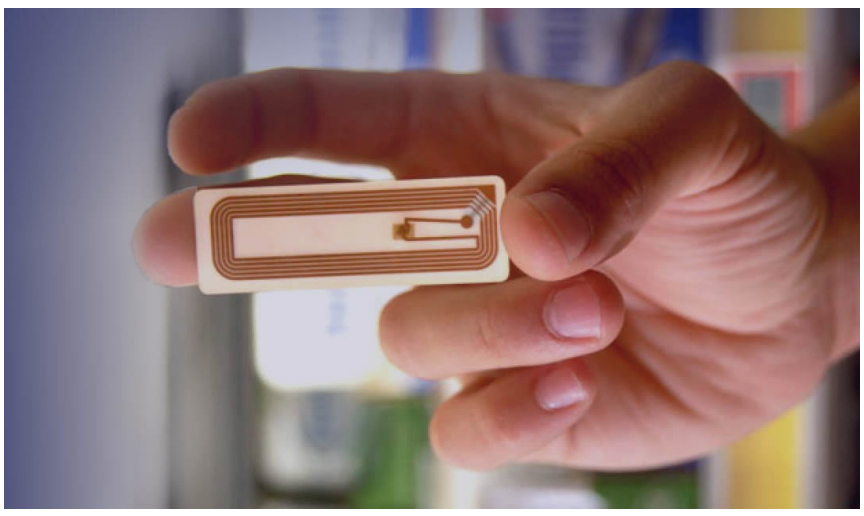
Secure Peripherals ⌨️ 📱 🖨️

1. **Wireless keyboards and mice**
    - Wireless keyboards and mice communicate in the clear
        - Use proprietary wireless communication protocols
        - Over 2.4 GHz frequencies
    - Easy to capture keystrokes with a receiver
        - Inject keystrokes and mouse movements
        - Control the computer remotely
    - Some keyboard manufacturers support AES encryption
2. **Printers/multi-function devices**
    - Printer, scanner, fax
    - Network connectivity
    - Reconnaissance - log files for all activity, address books
    - Unauthorized access - print without authentication
    - Gather information - capture spool files
3. **Displays**
    - Eletromagnetic radiation
    - Firmware hacks
4. **MicroSD cards**
    - Transfering over the 802.11 Wi-Fi (without removing the SD card from the device)
    - SD card authentication vulnerabilities; Predictable access, easy to read files over Wi-Fi
    - API access to the SD card
5. **External storage devices**
6. **Digital cameras**
    - Operates as external storage when plugged into a workstation; Easy to move data around
    - Camera firmware can be compromised

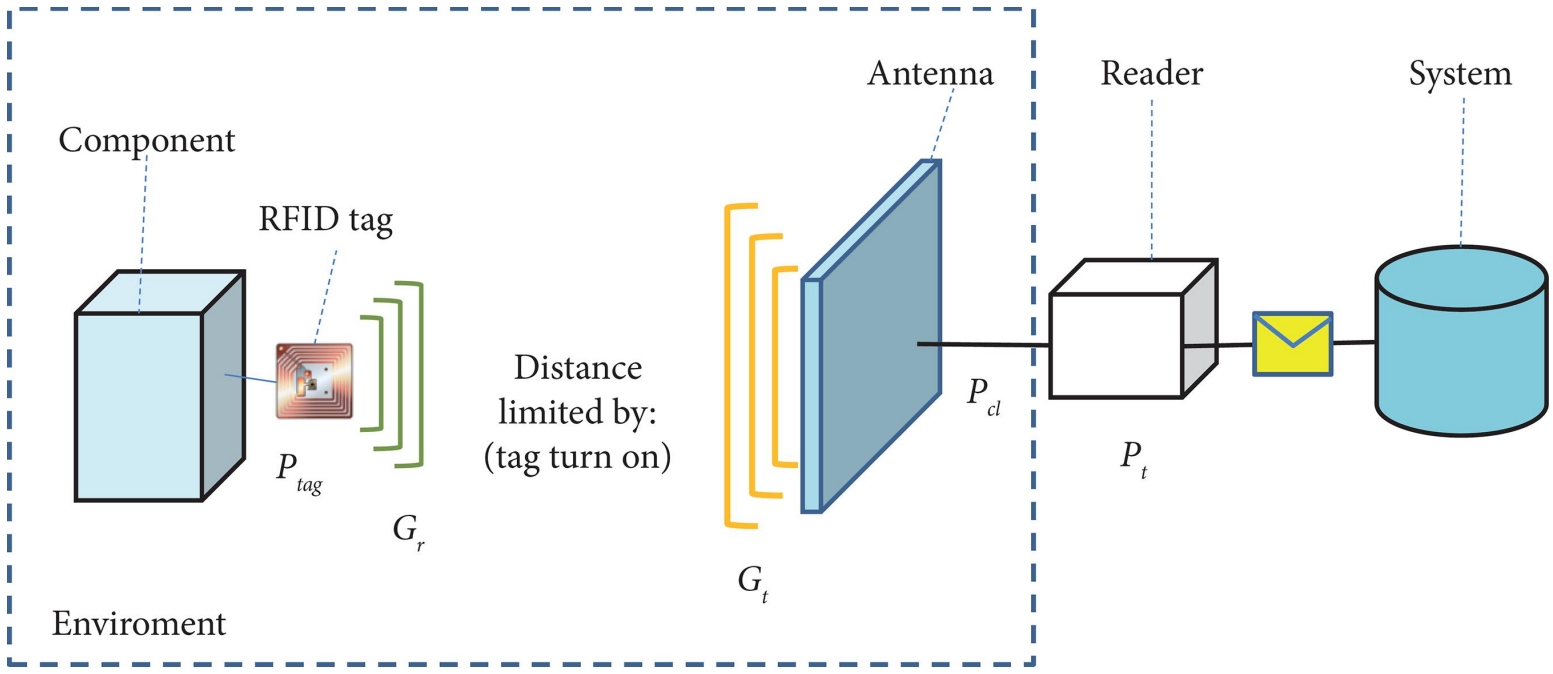
Common security practices:

- Patch!
- Disable unecessary ports
- Avoid backdoors

RFID (Radio Frequency Identification)



- **Access badges**
- **Inventory/assembly line tracking**
- **Pet/animal identification**
- **Anything that needs to be tracked.**



Security Concerns / Attacks

- Data Capture
  - View communication
  - Replay Attack
- Spoof the reader
  - write your own data to the tag
- Denial of Service
  - Signal jamming

NFC - Near Field Communication

Payment systems (Google Wallet, MasterCard partnership etc); Bootstrap for other wireless (helps with Bluetooth pairing); Uses an access token, identity 'card' (short range with encryption support)

Security Concerns

- Remote capture
- Frequency Jamming (DoS)
- Relay/Replay Attack (MITM)
- Loss of RFC device control *(e.g stolen phone)*

Bluetooth Security - Attacks 🔷⚔️

- **Bluejacking** - When **bad actors connects** with any Device that have Bluetooth enable by default.
- **Bluesnarfing** - When the **attacker steals data** from the target device by connecting to an unsuspecting user's device.
- **Bluebugging** - the most serious of the various Bluetooth attacks, involves an attacker attempting to take control of or use a Bluetooth-enabled **cell phone to place calls**.

Types of bluetooth:

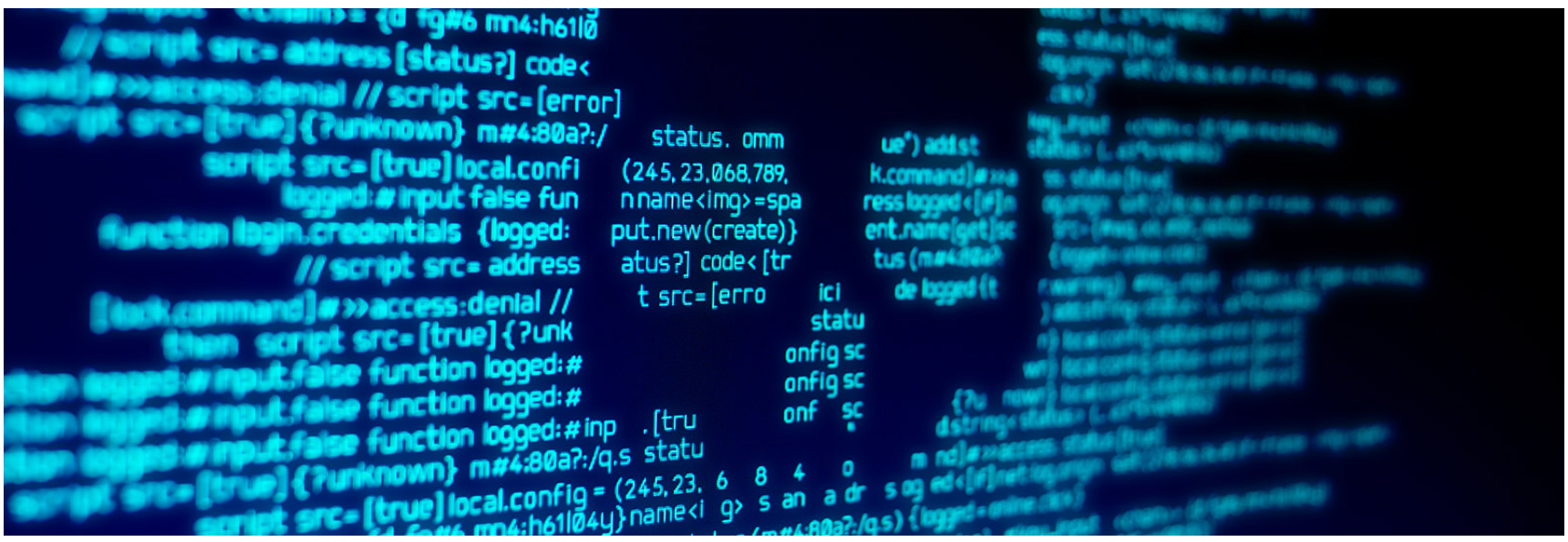
- **Class1** is 328' foot *(100 meters)*
- **Class2** is 33' foot *(10 meters)*
- **Class3** is 3' foot *(1 meter)*

  🛑 **Most Mobile phones and Bluetooth headsets are Class2 (10 meters).**

802.11

- Many peripherals can connect to an 802.11 network as a host. Printers and multifunction devices (MFDs) are very commonly connected with 802.11.

Malwares



Virus

- Piece of malicious software
- Attach to other files
- Propagate
- Spread to other devices
- Active

Adware

- Web-centric
- Programs that pop-up unecessary advertisment

Spyware

- Hide from system
- Tracking your web brownsing
- Stealing cookies

Trojans

- Standalone programs that must be installed **disguised** in programs
- Deliver payload without users knowledge
- Backdoor access
- **How to secure**: Don't run unknown software

RAT - Remote Access Trojan

- Mimic the behavior of legitimate remote control
- Can hide in common 'inofensive' programs like games
- Backdoor access
- **How to secure**: Don't run unknown software

Ransomware - Crypto-Malware

- Uses some form of encryption to lock a user out of a system.
- Usually encrypting the boot drive
- Then forces the user to pay money to get the system decrypted
- Can devastate systems

Logic Bomb

- Are triggered by an event *(e.g. erasing file shares or disk storage at a certain time or date)*
- Can devastate systems

Rootkit

- Piece of software that escalates privileges to execute other things on computer
- Modifies core system files - part of the kernel
- Hard to detect (*e.g cannot see in Task manager*)
- **How to secure**: use secure boot with UEFI (security in BIOS) and to remove you will need a specific rootkit remover.

Backdoor

- Piece of software that work on obfuscating an remote access.

Polymorphic Malware

- Changes his own code to confuse the digital signature of anti-malware programs
- Hard to detect and destroy

Armored Virus

- Design to make harder the detection by anti-malware programs.
- Hard to detect and destroy

Keylogger

- Record keystrokes
- Inject scripts
- **How to secure**: Use anti-virus/malware, keep signatures updated, Firewall rules and keylogging scanner.

Analyzing Output 🔍

Anti-Malware

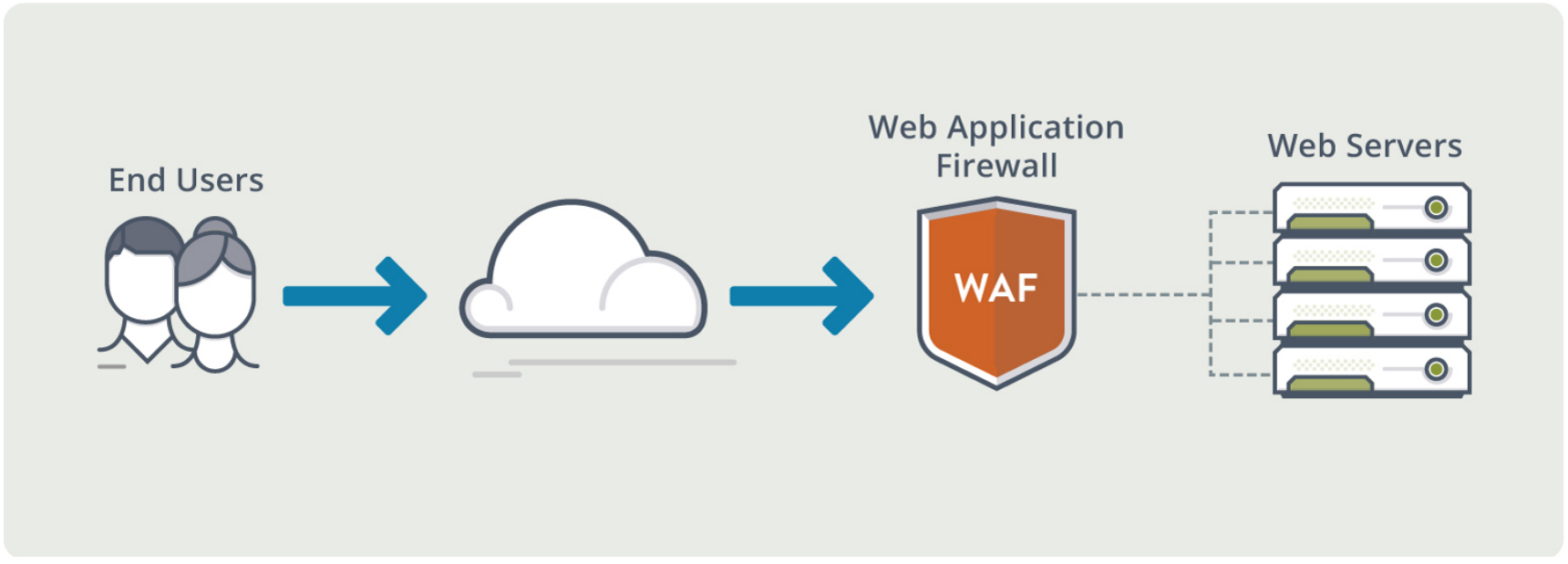
- Almost all anti-malware tools include a point scanner and a mass storage scanner.

Host-based Firewall

- Inbound rules / outbound rules
- All host based firewalls are basically they exclude everybody, so it is called an **implicity deny** *(not programs gets in or out)*
- The output is really an Access Control List
- Use of Least privilege and whitelisting

  🛑 **False positive** - scan results identify a file that may not actually harm a system or is allowed on the system. (e.g. you just downloaded the Cain & Abel to crack some passwords on your assessment, probably Windows Defender will try to block it out).

WAF - Web Application Firewall



- Not like a 'normal' firewall
  - **Applies rules to HTTP/HTTPS conversations**
- Allow or deny based on expected input
  - Unexpected input is a common method of exploiting an application
- SQL injection
  - Add your own commands to an application's SQL query
- A major focus of PCI DSS (Payment Card Industry Data Security Standard)

File Integrity Check

Verify the integrity of file is in good order and ready to run.

Basically to check if the file isn't:

- corrupted
- tampered
- version and date

  🛑 *To create a file integrity check, you can Generate a hash from source code - checksum. If somebody tamper the file or change from source code, the output hash will be different.*

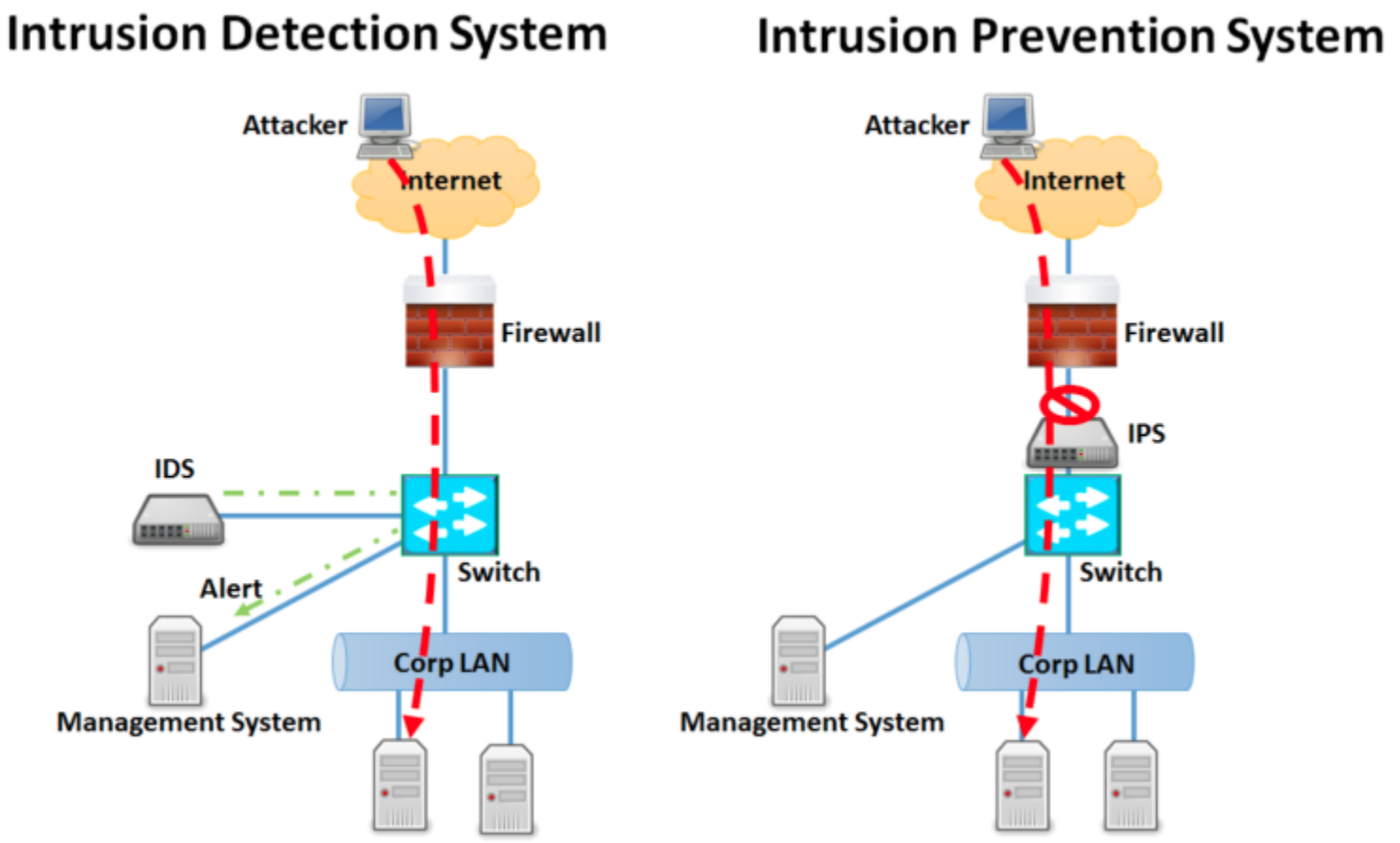
Application Blacklisting | Whitelisting

- Any application can be dangerous
- Security policy can control app execution with Whitelisting & Blacklisting
- ✅ **Whitelisting**:
  - Nothing runs unless it's approved
  - Very restrictive
- ❌ **Blacklisting**:
  - Nothing on the 'bad list' can be executed
  - Anti-virus, anti-malware

*Everything about software management, **application whitelisting**, the main job - it's to make sure that users are running the right applications on each individual systems.*

- Decisions are made in the OS
- **Application hash** - Only allows applications with this unique identifier
- **Certificate** - Allow digitally signed apps from certain publishers
- **Path** - Only run applications inside specific folders
- **Network zone** - The apps can only run from this network zone

IDS and IPS



Intrusion Detection Systems (IDS)

- Lives inside the Network
- Watches within the network traffic
- **Sends alerts** on suspicious activity

Intrusion Prevention System (IPS)

- Active IDS
- IPS is usually close to the edge the network
- **Takes action** to prevent will occur at the IPS device

🛑 **IDS: Notifies** 🛑 **IPS: Acts to stop** 🛑 **Firewall: Filters**

⚠️ IDS and IPS will be explained with more details later below.

Automation Strategies

Automation is often used with various scans and updates based on configurable trigger.

- Repetitive
- Consistent
- Template restoration
- Continuous monitoring network devices (e.g. SNMP)
- Automatic update from OS
- Monitoring host for application whitelists
- Application Development - continuous integration tools like fuzzing, static testing
- Built-in tools vs Shell Scripting to Automate (Powershell(Windows) , Bash(Linux) ..)

Media Sanitization | Data Destruction

Data Sanitization Tools

- **Sanitize entire hard drives:**
  - Darik's Boot and Nuke (DBAN)
- **Sanitize individual files or folders:**
  - Microsoft SDelete

🛑 Cache and temporary files can be tricky to track sometimes.

Purge

Purging will process the device to remove data from the drive, the device might will no longer be usable. Means to use anything other than an internal command to sanitize the data on the media. *(e.g. Degausser: machine with a strong magnetic field that destroys/purge the data from massa storage devices)*

🛑 **Purge also means that the device is basically not useful anymore**

Clearing/Clear

Clear means to tell the device through user commands inherent to the massa storage device to sanitize the data. *(e.g. send commands to a hard drive to erase data)*

- **Can be done with commands such as erase, format and delete (these methods are not final)**
- **Crypto Erase** - In case you lost the keys to encrypted device.

Destroy / Data Destruction

Ruin the media in such a way tha it is no longer functional.

- Mass storage device
- Tape media
- Floppy disks
- Paper

Protect your rubbish

- Secure your garbage (fence and lock)
- Shred your documents (e.g. Governments burn the good stuff)
- Burn documents
- Pulp the paper

Physical destruction

- Shredder / pulverizer
  - Heavy machinery
  - Complete destruction
- Drill / Hammer
  - Quick and easy
  - Platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and the electronics
- Incineration

Certificate of destruction

- Destruction is often done by a 3rd party
- Confirmation that your data is destroyed
- Paper trail of broken data
  - You know exactly what happened

Data Sanitization Tools

- Sanitize entire hard drives
  - Darik's Boot and Nuke (DBAN)
- Sanitize individual files or folders
  - Microsoft SDelete

- Cache and temporary files can be tricky to track sometimes.

---

2. Security Tools

Passive Security

- You're a network ninja
- Watch packets go by
- There's a lot to learn
- Top talkers, servers, clients, applications, OS, services

Active Security

- Send traffic to a device, watch the results
- Query a login page
- Try a known vulnerability
- Check account access

Protocol Analyzers

Protocol Analyzers collect and inventory the network traffic.

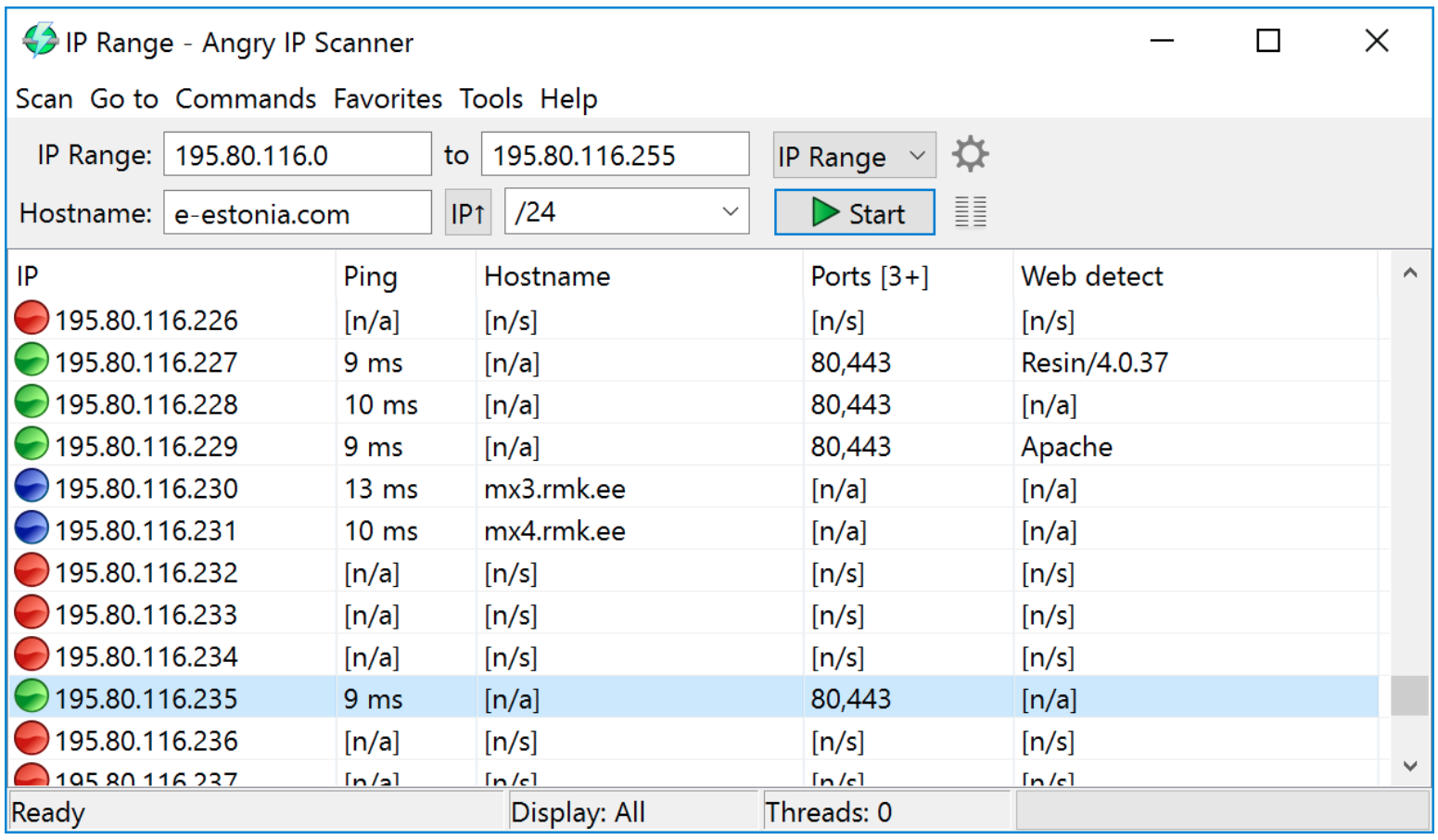
- **Sniffer** - Some type of software that grab all the data that is going in and out of particular interface.

Why Protocol Analyze?

- Count all the packets coming through over a certain time period to get a strong ideas to your network utilization.
- Inspect packets for single protocols to verify they are working properly.
- Monitor communication between client and a server to look for problems.
- Look for servers that aren't authorized on the network.
- Find systems broadcasting bad data.
- Find problems in authentication by watching each step of the process.

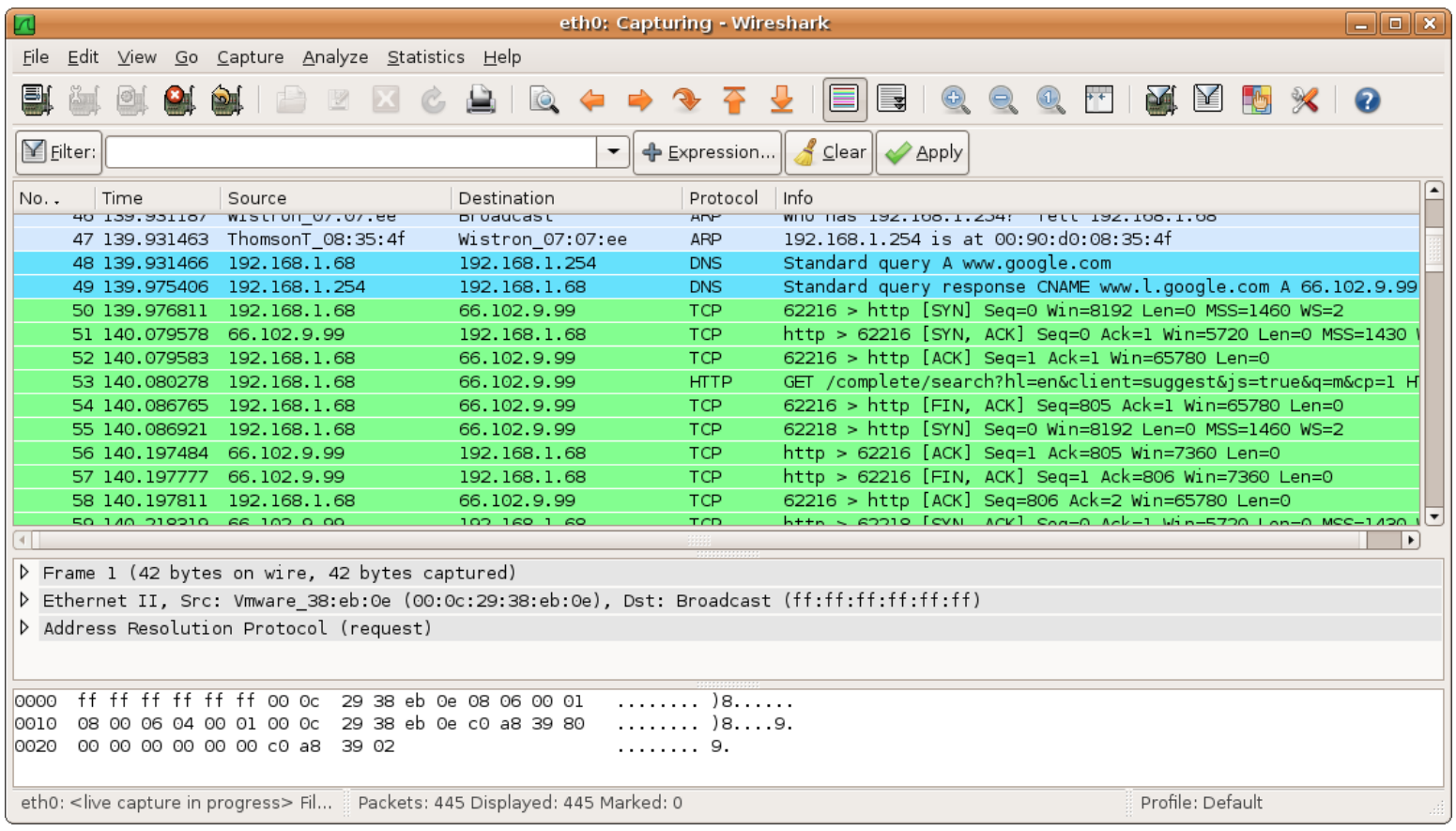
Angry IP Scanner (GUI) - for Windows

Does a good job using simple protocols, mainly ping, to query a single IP address or an address range.



Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level.



- *With Wirehsark you can inspect and detect ARP poisonings, Rogue DHCP servers, Broadcast Storm etc.*

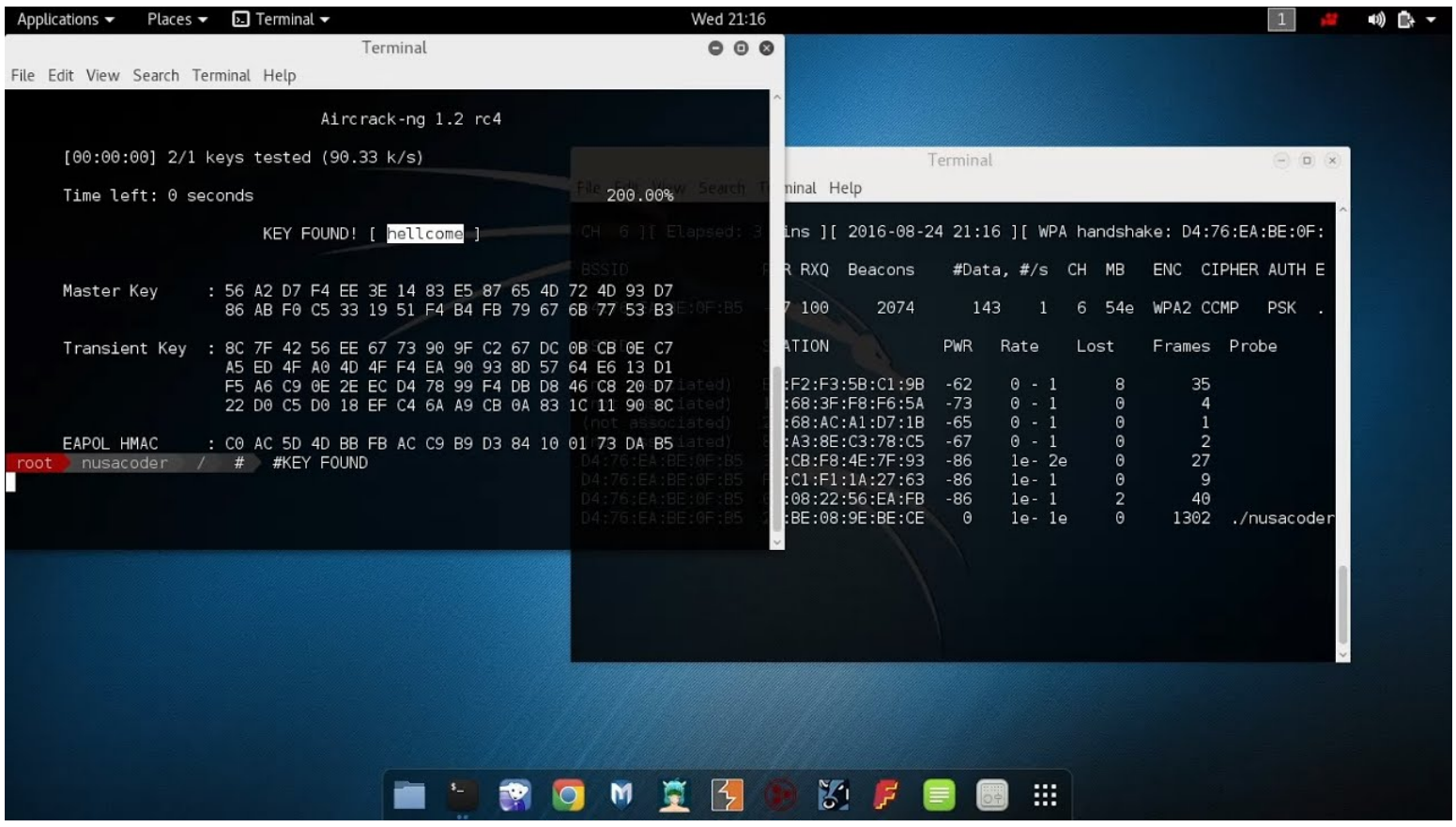
  🛑 Broadcast Storm - when a NIC (or port on a switch) sends large amounts of broadcast traffic, thereby crippling network resources.

Wireless Scanners and Crackers

- **Wireless Monitoring**:
  - Packet capturing
- **Wireless attacks**:
  - Rogue access points
  - Deauthentication attacks
- **Cracking**:
  - Find a wireless netowrk key
  - WEP - Cryptographic vulnerabilities - relatively straightforward

- WPA PSK and WPA2 PSK - Dictionary brute force, rainbow tables

- **Many Open Source projects**:
  - Aircrack-ng Suite, Fern

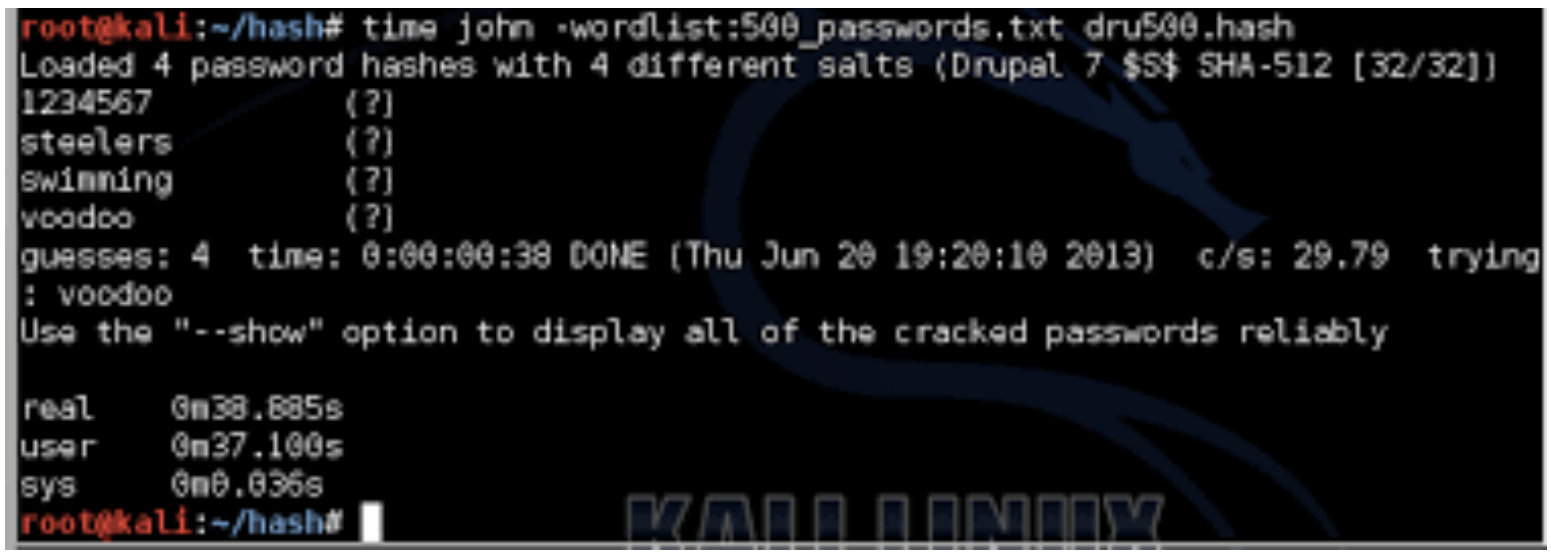


Password Crackers

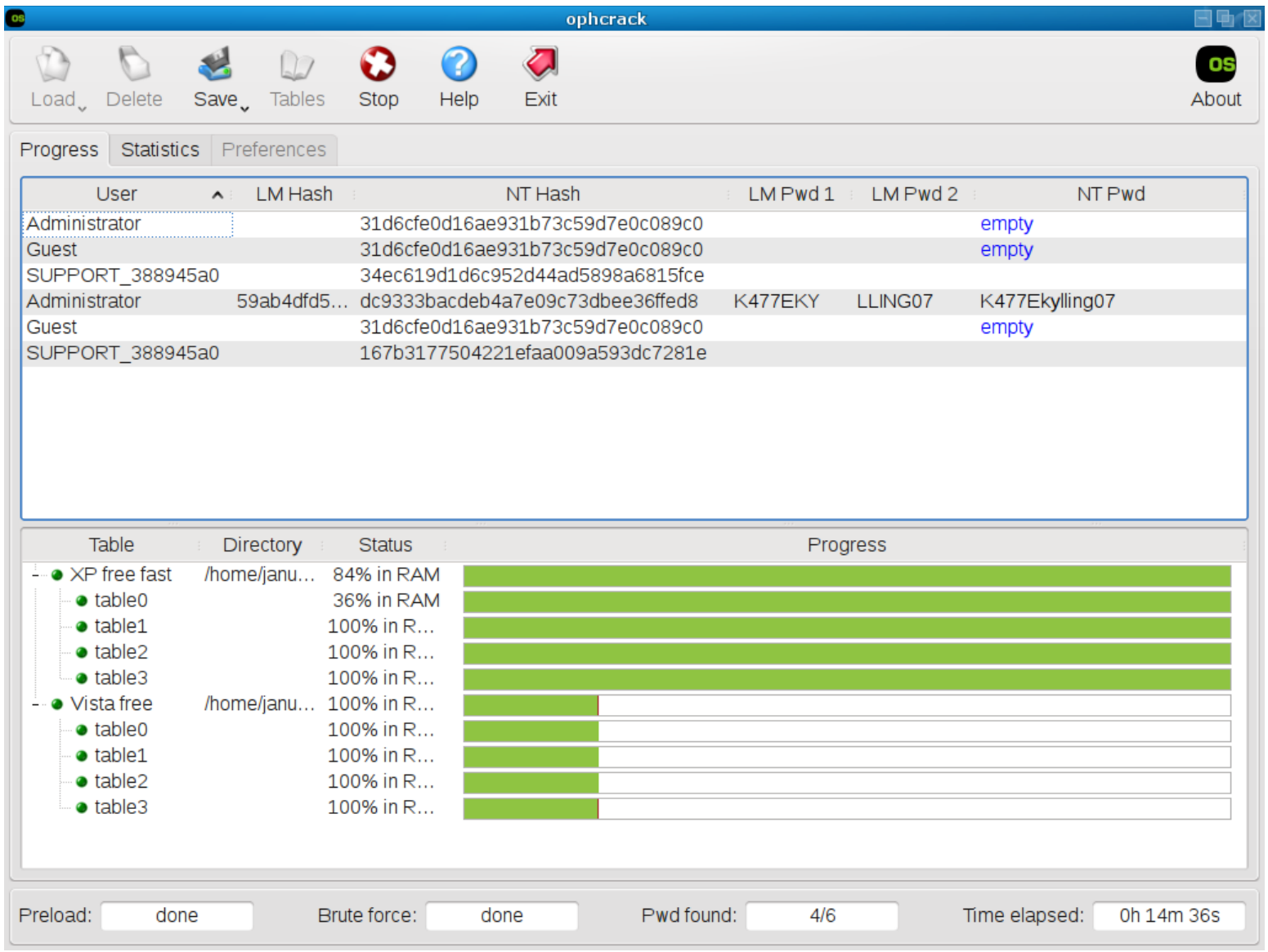
- Passwords are stored as Hashes
- It's a one-way trip (you can't convert hash to plain-text password)
- Some are stored without much complexity - relatively straightforward to brute-force a weak hash
- As an attacker, After get the hashes you can use a good wordlist or rainbow-table to crack them.

Many tools available:

- John the Ripper:



- Ophcrack:



Vulnerability Scanners

- Gather as much information as possible
- Security Patches alert
- **Popular tools**:
  - **MBSA** - Microsoft Baseline Secuirty Analyzer
  - **Nessus** by Tenable
  - **Nikto**

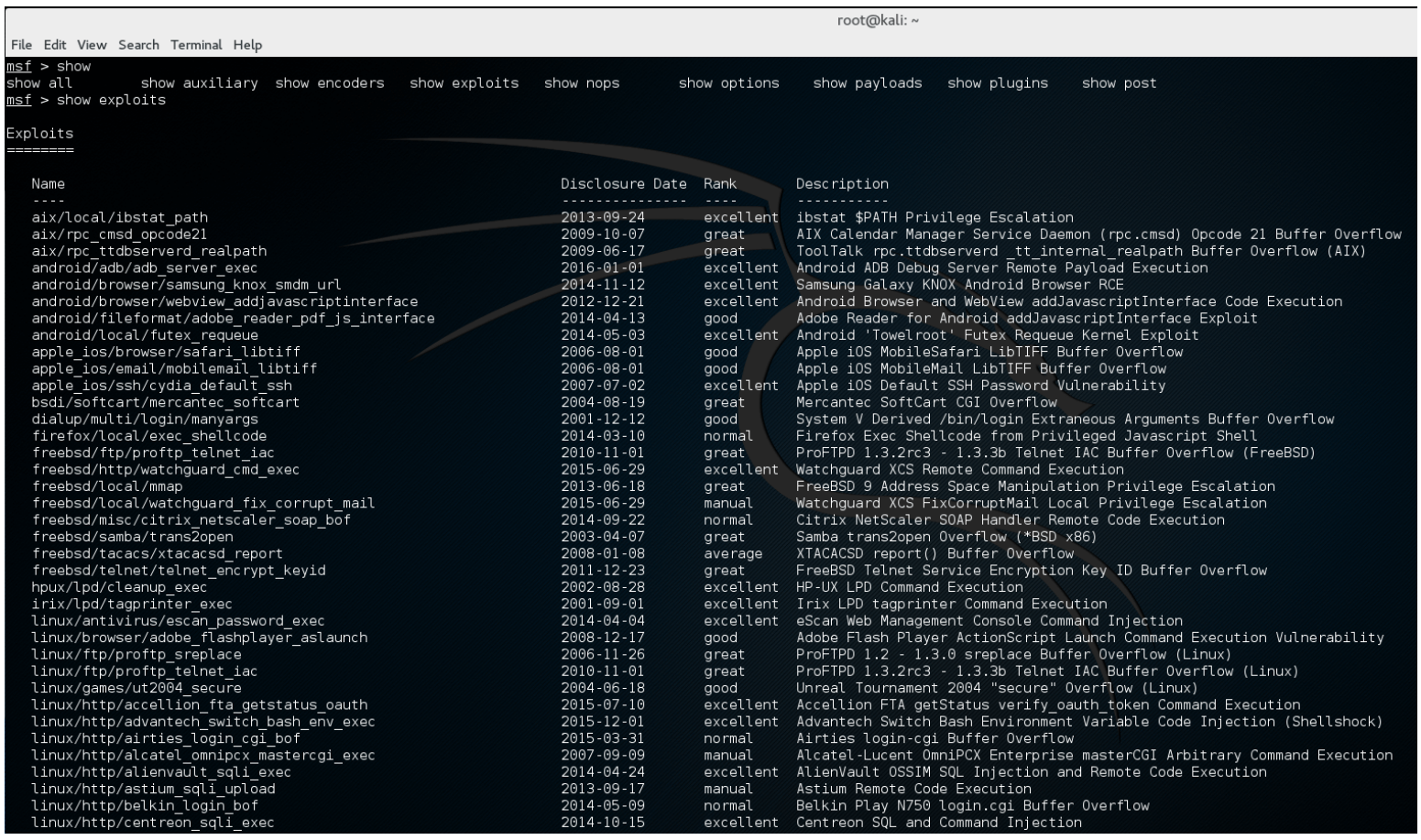
⚠ Vulnerability Scanners will be explained with more details later below at *Chapter 7 - Testing Infrastructure.*

Configuration Compliance Scanner

- **The devices must meet minimum security configurations**
  - Comply with internal requirements or industry regulations
- **Check for varios configurations**
  - OS version
  - Installed applications
  - Network settings
  - Anti-virus / anti-malware settings, versions and signatures
  - Server configurations
- **Auditing may be ongoing**
  - Report on current status, identify changes over time
  - Integrated with login process and/or VPN connection

Exploitation Frameworks

- On the browser, OS, applications, embedded devices, etc.
- Build an exploit using different techniques
- Those frameworks are heavily updated with newest CVEs and most common exploits
- **Tools**:
  - **BeEF** - The browser Exploitation Framework Project
  - **RouterSploit** - Router Exploitation Framework
  - **Metasploit** - Build your own vulnerability tests or use modules in the existing exploit database.



Metasploit Framework - exploits

OS Utilities - Command Line (Linux & Windows)

- Security+ covers simple **Linux** and **Windows commands**.
- *To understand the functionality behind the commands I recommend to test them at your own.*

ping

- Can be handful for DNS checks (up / or down) | is a DNS tool to resolves web addresses to an IP address.
- Test reachability - determine round-trip time, and uses ICMP protocol.

```
~#: ping www.google.com

PING www.google.com (172.217.168.164): 56 data bytes
64 bytes from 172.217.168.164: icmp_seq=0 ttl=55 time=25.981 ms
64 bytes from 172.217.168.164: icmp_seq=1 ttl=55 time=25.236 ms
--- www.google.com ping statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/stddev = 25.236/25.608/25.981/0.373 ms
```

- In **Windows** you need to add a **-t** flag to keep running.

Most useful switches for Ping command - Windows:

Switch	Description
-a	Resolve address to hostnames
-f	Set don't fragment flag in packet (IPv4 only)
-4	Force using IPv4
-6	Force using IPv4

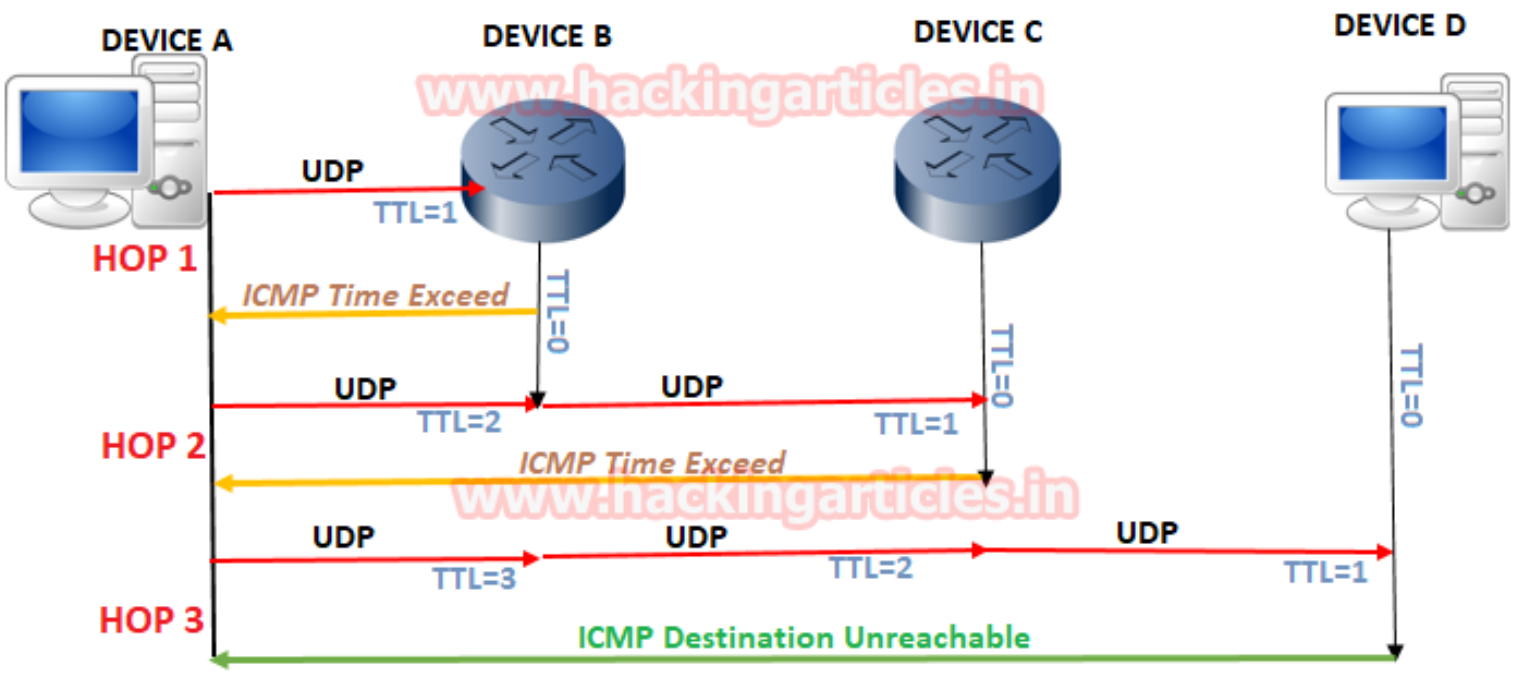
netstat

- Network statistics
- Get info on host system TCP / UDP connections and status of all open and listening ports and routing table.
- Who you talking to?
- Who trying talking to you?

```
netstat -a # (show all active connections) (servers)
netstat -n # (hosts)
netstat -b # (Show binaries Windows)
```

tracert | traceroute

- Traceroute - how packets get from host to another endpoint. Traceroute is helpful to see what routers are being hit, both internal and external.
- tracert - Windows
- traceroute - Linux
- **Take advantage of ICMP Time to Live (TTL) Exceeded error message**
  - The time in TTL refers to hops, not seconds or minutes.
  - TTL=1 is the first router.
  - TTL=2 is the second router, and so on.



- *As shown above, on HOP 2 the TTL exceeded and back to the device A, counting 3 on TTL for the next HOP.*

```
~#: traceroute google.com

traceroute to google.com (172.217.17.14), 64 hops max, 52 byte packets
 1  192.168.1.1 (192.168.1.1)  4.960 ms  3.928 ms  3.724 ms
 2  10.10.124.254 (10.10.127.254)  11.175 ms  14.938 ms  15.257 ms
 3  10.133.200.17 (10.137.201.17)  13.212 ms  12.581 ms  12.742 ms
 4  10.255.44.86 (10.255.45.86)  16.369 ms  15.100 ms  17.488 ms
 5  72.14.201.214 (72.14.201.214)  13.287 ms  29.262 ms  16.591 ms
 6  74.125.235.68 (74.125.242.68)  22.488 ms
    74.125.235.84 (74.125.242.84)  13.833 ms *
 7  74.125.252.202 (74.125.252.202)  24.147 ms
    108.170.252.241 (108.170.25@.241)  26.352 ms
    74.125.252.202 (74.125.252.202)  23.598 ms
 8  108.170.252.247 (108.170.252.247)  31.187 ms
    74.125.252.199 (74.125.252.199)  22.885 ms
```

arp

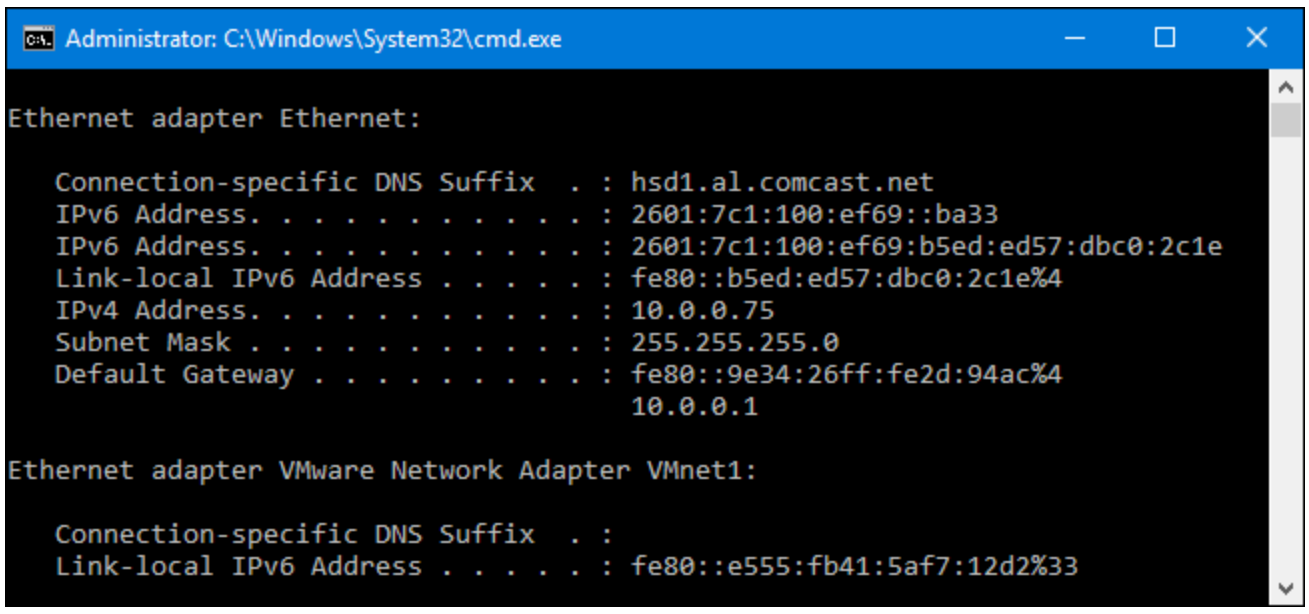
- Address resolution protocol - caches of ip-to-ethernet
- Determine a MAC address based on IP addresses
- Option `-a`: view local ARP table

```
~#: arp -a

? (192.168.1.3) at 00:11:22:33:44:55 [ether] on enp0s10
? (192.168.1.128) at e8:33:b0:70:2c:71 [ether] on enp0s10
? (192.168.1.4) at 2c:33:5c:a4:2e:8a [ether] on enp0s10
_gateway (192.168.1.1) at 00:31:33:8b:2a:da [ether] on enp0s10
```

ipconfig

- Show all IP configuration on **Windows-only** systems.



- **Useful switches:**

Switch	Description
/all	Exhaustive listing of virtually every IP and Ethernet setting (MAC address etc)
/release	Release the DHCP IP address lease
/renew	Renews the DHCP IP address lease
/flushdns	Clears the host's DNS cache
/displaydns	Displays the host's DNS cache

ifconfig

- Equivalent to ipconfig for UNIX/Linux OS.

```
~#: ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:11:22:33:44:55  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.128  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::acf6:2ae2:ab5c:6316  prefixlen 64  scopeid 0x20<link>
        ether aa:bb:cc:dd:ee:ff  txqueuelen 1000  (Ethernet)
        RX packets 156651  bytes 29382856 (28.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 76400  bytes 23111524 (22.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

iwconfig

similar to ifconfig, but is dedicated to the wireless network interface.

```
~#: iwconfig
lo        no wireless extensions.

enp0s10   no wireless extensions.

wlp3s0b1  IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=19 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

docker0   no wireless extensions.
```

ip addr

show / manipulate routing, network devices, interfaces and tunnels.

Show all the ip configuration, mac address, ipv6 etc.

```
~#: ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group d
    link/ether aa:bb:cc:dd:ee:ff brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.111/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s10
       valid_lft 4761sec preferred_lft 4761sec
    inet6 fe80::acf6:2ae2:ab5c:6316 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

nslookup

- Query Internet name servers interactively; check if the DNS server is working

```
nslookup www.certifiedhacker.com

output:
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name:   certifiedhacker.com
Address: 162.241.216.11 inslookup www.certifiedhacker.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.certifiedhacker.com canonical name = certifiedhacker.com.
Name:   certifiedhacker.com
```

```
Address: 162.241.216.11
```

dig

- DNS lookup tool - Functions like nslookup, but allows for further functionality.

```
dig www.certifiedhacker.com

output:
; <<>> DiG 9.11.14-3-Debian <<>> certifiedhacker.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15708
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 2048
; COOKIE: 71bd915b07b3fd08757c9ad65e5d6f3e549d5187359e97cb (good)
;; QUESTION SECTION:
;certifiedhacker.com.           IN      A

;; ANSWER SECTION:
certifiedhacker.com.    14400   IN      A       162.241.216.11

;; Query time: 419 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Mon Mar 02 15:40:29 EST 2020
;; MSG SIZE  rcvd: 92
```

netcat

TCP/IP swiss army knife; you can make any type of connection and see the results from a command line. With nc you can connect to anything on any port number or you can make your system listen on a port number. Can be an agressive tool for recon.

- "Read" or "Write" to the network
  - Open a port and send or receive some traffic
  - Listen on a port number
  - Transfer data
  - Scan ports and send data to be a port
- Become a backdoor
  - Run a shell from a remote device

stat

stat can return the status of an entire file system, the status of the first hard disk and so on.

```
himanshu@ansh:~$ stat test.txt
  File: 'test.txt'
  Size: 22              Blocks: 8          IO Block: 4096   regular file
Device: 807h/2055d      Inode: 3673414     Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/himanshu)   Gid: ( 1000/himanshu)
Access: 2018-02-01 16:49:49.256422217 +0530
Modify: 2018-02-01 16:46:59.628037156 +0530
Change: 2018-02-01 16:46:59.708035450 +0530
 Birth: -
himanshu@ansh:~$
```

- Archive attribute - **Windows** - if something is created or changed

tcpdump

- Tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software

```
anuj@packetflows:~$ sudo tcpdump -i eth0
[sudo] password for anuj:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
23:14:09.691884 IP packetflows.local.47860 > productsearch.ubuntu.com.https: Flags
[S], seq 2046377878, win 29200, options [mss 1460,sackOK,TS val 9320277 ecr 0,nop,w
scale 7], length 0
23:14:09.693521 IP packetflows.local.10745 > cdns01.comcast.net.domain: 47145+ PTR?
 49.33.213.162.in-addr.arpa. (44)
23:14:09.693689 IP packetflows.local.10745 > cdns02.comcast.net.domain: 47145+ PTR?
 49.33.213.162.in-addr.arpa. (44)
23:14:09.727692 IP cdns01.comcast.net.domain > packetflows.local.10745: 47145 1/0/0
 PTR productsearch.ubuntu.com. (82)
23:14:09.728442 IP packetflows.local.12125 > cdns01.comcast.net.domain: 56414+ PTR?
 15.2.0.10.in-addr.arpa. (40)
23:14:09.763628 IP cdns01.comcast.net.domain > packetflows.local.12125: 56414 NXDom
ain 0/0/0 (40)
23:14:09.863208 IP productsearch.ubuntu.com.https > packetflows.local.47860: Flags
[S.], seq 1389760001, ack 2046377879, win 65535, options [mss 1460], length 0
23:14:09.863298 IP packetflows.local.47860 > productsearch.ubuntu.com.https: Flags
[.], ack 1, win 29200, length 0
23:14:09.863432 IP cdns02.comcast.net.domain > packetflows.local.10745: 47145 1/0/0
 PTR productsearch.ubuntu.com. (82)
23:14:09.863465 IP packetflows.local > cdns02.comcast.net: ICMP packetflows.local u
dp port 10745 unreachable, length 118
23:14:09.864415 IP packetflows.local.47860 > productsearch.ubuntu.com.https: Flags
```

Network Scanners

Useful for collect and inventory the hosts on a network, and is useful for reconnaissance of your system.

nmap

The Best way to query a system to check if they have open ports, services, system versions, service versions etc.

```
nmap -v -A -T5 scanme.nmap.org
```

```
...
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|   256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
|_  256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
9929/tcp  open  nping-echo Nping echo
31337/tcp open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
...
```

Zenmap is a GUI version of Nmap.

Logging

- **Common Log Format (CLF)** - Standard type of logs that every single type of web server generates.

```
127.0.0.1 - - [28/OCT/2012/13:12:44 - 0500] "GET /CertifiedHacker.png HTTP/1.0" 200 42
    |       |              |                        |                                  |
  HOST    IDENT     DATE & TIME              REQUEST                             STATUS
```

IDENT - If the IdentityCheck directive is enabled and the client machine runs ident, then this is the identity information reported by the client.
GET - Request HTTP method command
STATUS - status, 200 = Everything is ok
BYTES - the number of bytes in the object returned to the client, excluding all HTTP headers.

Remotehost	rfc931	authuser	[date]	"request"	status	bytes
213.240.4.193	-	-	[04/Apr/2005:10:40:52 +0200]	GET /images/nastava%20color.jpg HTTP/1.1	200	13465
213.240.4.193	-	-	[04/Apr/2005:10:40:53+0200]	GET /images/zaglavlje.jpg HTTP/1.1	304	-
213.240.4.193	-	-	[04/Apr/2005:10:40:58+0200]	GET /raspored_ispita.htm HTTP/1.1	304	-
213.240.4.193	-	-	[04/Apr/2005:10:40:59+0200]	GET /images/ispit.jpg HTTP/1.1	304	-
213.240.4.193	-	-	[04/Apr/2005:10:41:02+0200]	GET /obavestenja.htm HTTP/1.1	304	-
213.240.4.193	-	-	[04/Apr/2005:10:41:02+0200]	GET /images/obavestenja.jpg HTTP/1.1	304	-
213.240.4.193	-	-	[04/Apr/2005:10:41:11+0200]	GET /obavestenja/naukaoradu.htm HTTP/1.1	200	18959
212.200.136.5	-	-	[04/Apr/2005:10:41:16+0200]	GET / HTTP/1.0	304	-
212.200.136.5	-	-	[04/Apr/2005:10:41:16+0200]	GET /images/zaglavlje.jpg HTTP/1.0	304	-
212.200.136.5	-	-	[04/Apr/2005:10:41:19+0200]	GET /images/efsuzgrada01.jpg HTTP/1.0	304	-
212.200.136.5	-	-	[04/Apr/2005:10:41:21+0200]	GET / HTTP/1.0	200	7295

There are two types of events: Network and Non-network events.

Non-Network Logs

- Operation System Events
    - Host starting
    - Host shutdown
    - Reboot
    - Service starting, stopping, and failling
    - OS Updates
- Applications Events
    - Application Installation
    - Application starts, stops or crashes
- Security Events
    - Logons
    - Logons successes and failures

Generic Log Structure:

ID	Team_ ID	Student_ ID	Bundle _ID	Task_ID	Role	Page	Event	Arg1	Arg2	Arg3	Timestamp
16474 33	auvarc 0033	auvarc003 3b	12	ICP0903 025	B	1	Request- page	2			22/08/2017 11:55
16474 32	auvarc 0033	auvarc003 3a	12	ICP0903 025	A	1	Request- page	2			22/08/2017 11:55
16474 30	auvarc 0033	auvarc003 3b	12	ICP0903 025	B	1	Select- choice	opB	1		22/08/2017 11:54
16474 31	auvarc 0033	auvarc003 3b	12	ICP0903 025	B	1	Select- choice	result	14		22/08/2017 11:54
16474 29	auvarc 0033	auvarc003 3a	12	ICP0903 025	A	1	Select- choice	opA	1		22/08/2017 11:54
16474 28	auvarc 0033	auvarc003 3a	12	ICP0903 025	A	1	Select- choice	opA	4		22/08/2017 11:54
16474 27	auvarc 0033	auvarc003 3b	12	ICP0903 025	B	0	Request- page	1			22/08/2017 11:54

- Date and Time
- Process/Source/ID
- Account associated/System
- Event Number
- Event Description
- Network Logs

Network Events

- O.S. / System-Level
    - Remote logon fail/not
    - Events on Shared Applicaton/Resources
        - Activity on Web Server (e.g. Apache)
        - Activity on Firewall
- Application-Level

Log Management

Descentralized Log management

In environments such as very small networks and don't have large infrastructure or in isolated network segments, descentralized log management is usually the norm.

Centralized Log management

Means that the log files from different machines are automatically sent to a centralized logging facility or server, such as a syslog server, administrators review logs from a centralized loogging facility on the network. Enterprise correlate them into one unifed management interface, so the administrator can look for trends or events. This can be achieved by using **SIEM tools.**

Centralized features:

- Uses a Central repository
    - Drag on system
- Use SNMP Systems
    - Pulls informaton needed and generates graphs and charts

    🛑 Monitoring-as-a-Services (MaaS)

SIEM - Security Information and Event Management

Collects data points from network, including **log files, traffic captures, SNMP messages, and so on**, from every host on the network. **SIEM can collect all this data into one centralized location and correlate it for analysis to look for security and performance issues, as well negative trends all in real time.**

⚠️ SIEM will be explained with more details later below.

Continuos Monitoring

Is a proactive way of ensuring that the network administrator receives all the different logs and other data points throughout the network from all network devices and all systems, on a constant basis. This data is continually fed into.

Auditing

Important part of ensuring accountability on the network. Examines the logs and other data points of certain events and construct a time frame and event sequence surrounding an incident.

Auditing also consists of other activities, such as:

- Performing Network Sniffing traffic analysis
- Password Cracking
- Vulnerability Assessment
- Penetration Test
- Compliance Audits

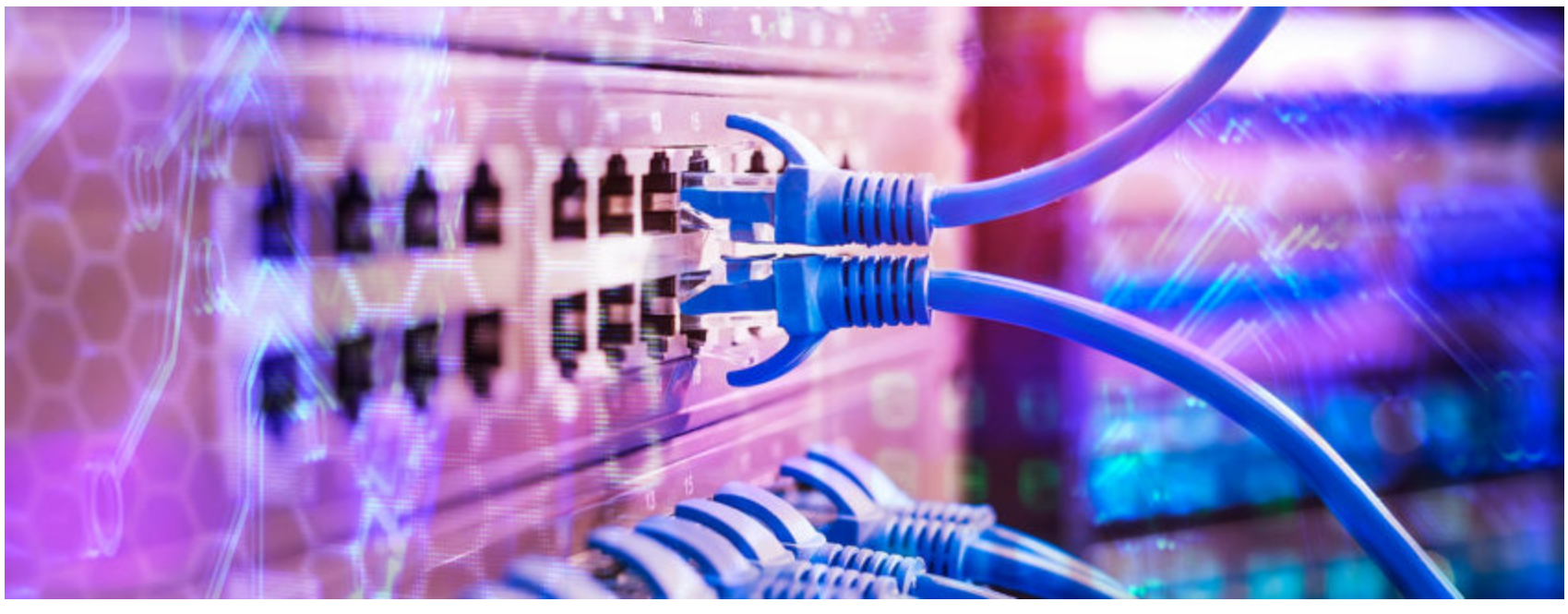
    🛑 **Auditing can reveal weak security configurations**

Trend Analysis

Enables network administrator to correlate different data sources and data points from various places in the network, such as log files, IDS logs, wireless and wired sniffing as well as other event sources, and seek to identify on-going trends in both performance and security. The goal is find patterns that can indicate a emerging issue.

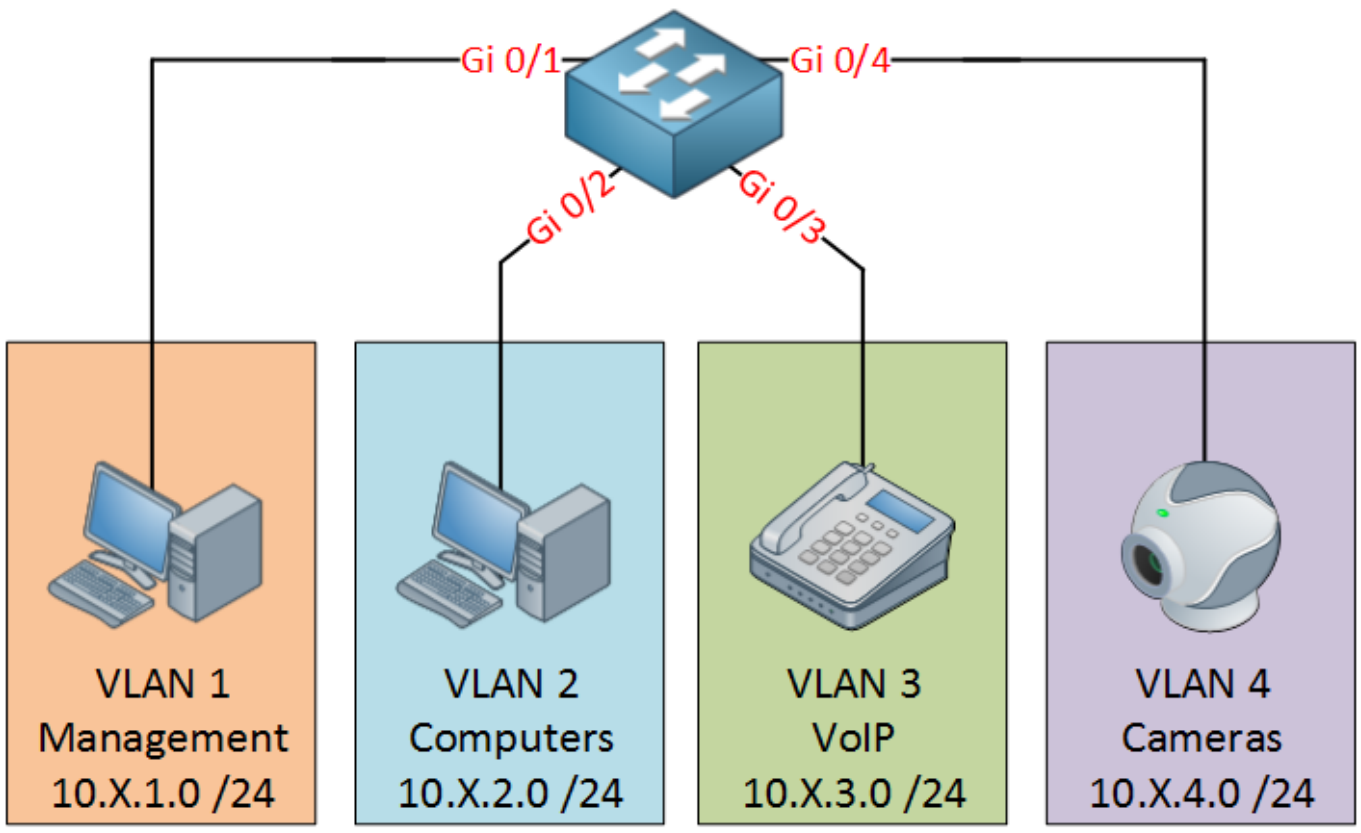
---

3. Networks and Infrastructure



Switches

A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses **MAC addresses** to forward data at the **data link layer of the OSI model.**



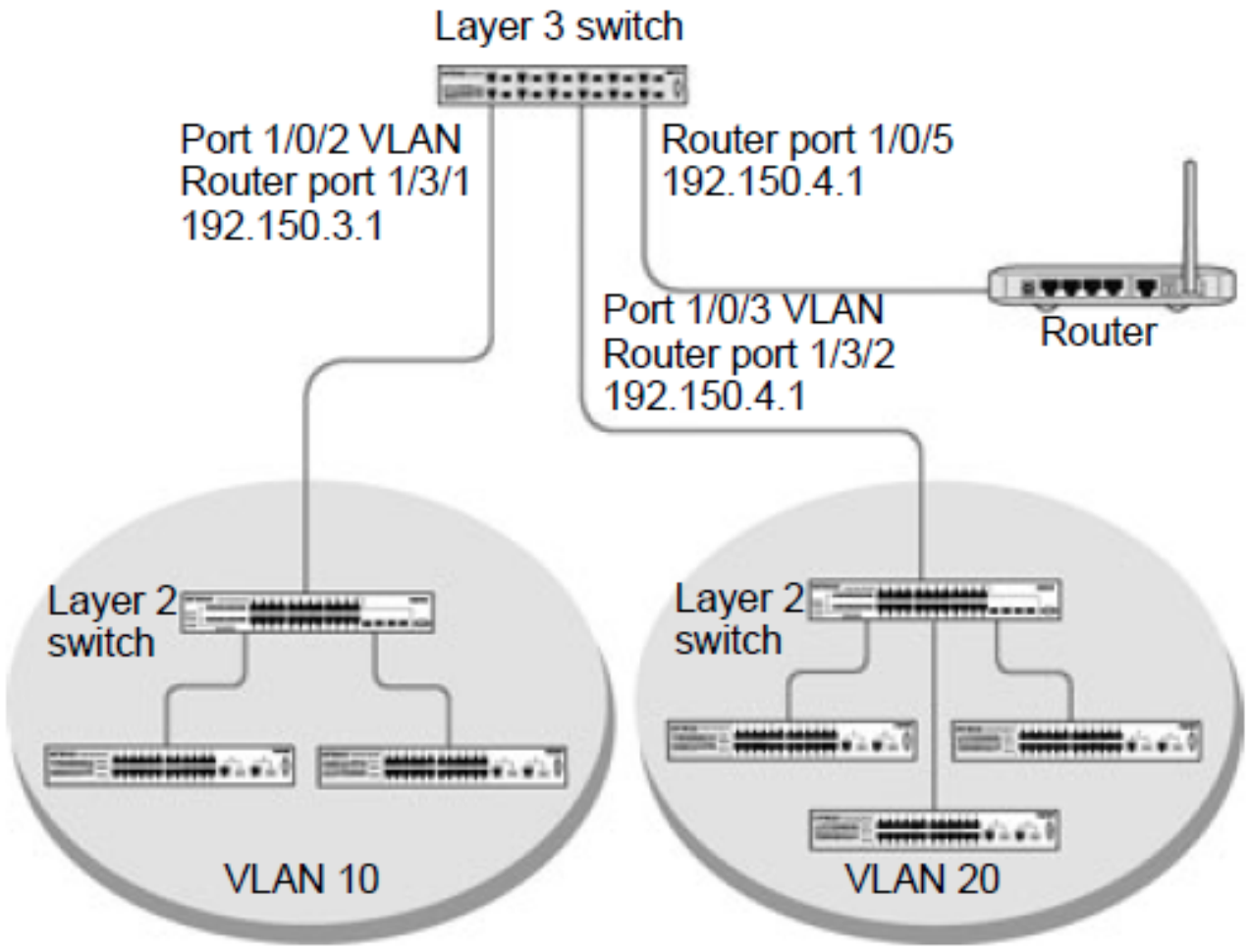
- Filter & forward data based on **MAC address**
- OSI Layer 2 [Data Link]
- Where VLANs are set up
- **STP (Spanning Tree Protocol)** prevents bridge loop / loop floods

  🛑 **Operates in the OSI Layer 2 (Data Link)**

  🛑 **Bridge Loop/Switching Loop** - A switching loop or bridge loop occurs in computer networks when there is more than one Layer 2 path between two endpoints. The loop creates broadcast storms as broadcasts and multicasts are forwarded by switches out every port, the switch or switches will repeatedly rebroadcast the broadcast messages flooding the network.

VLANs

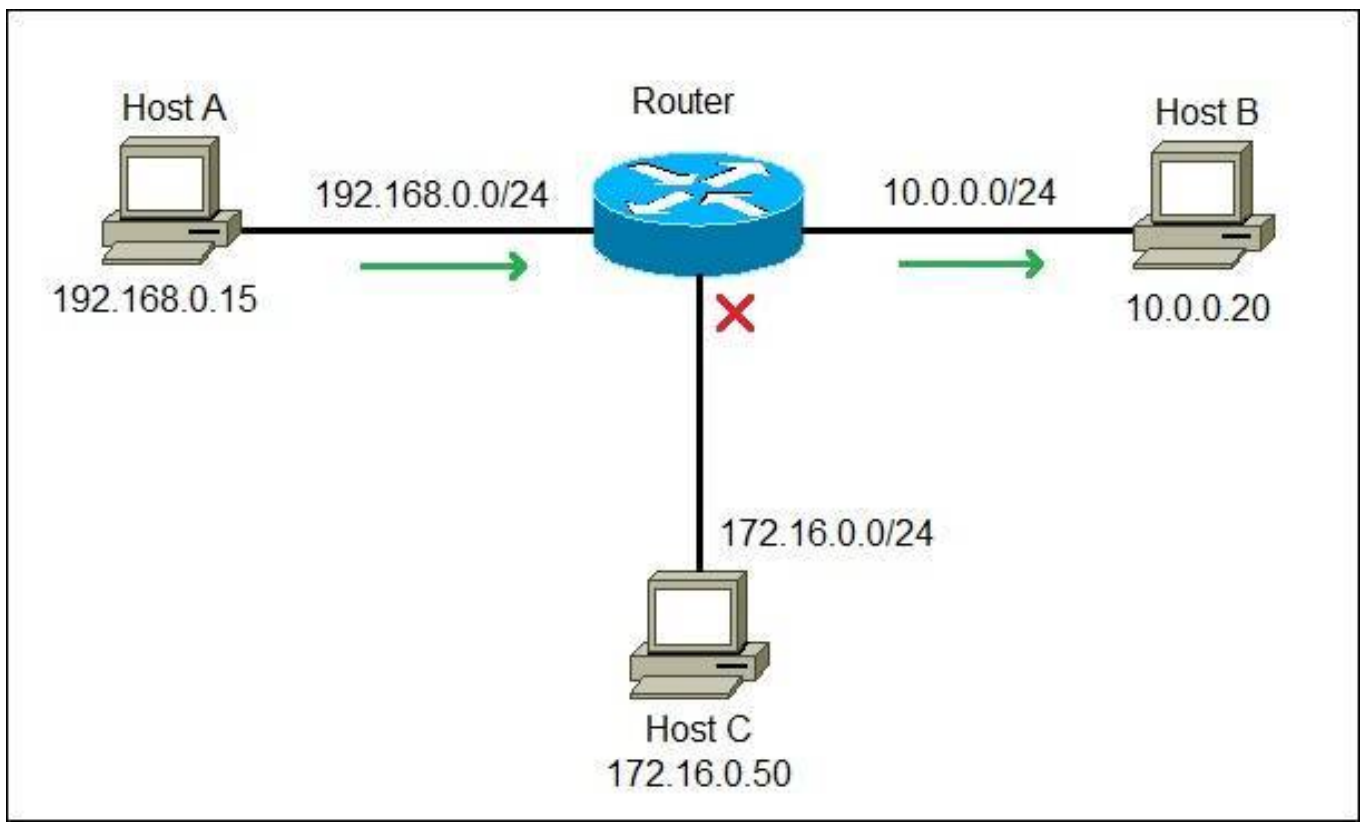
A virtual LAN is any broadcast domain that is partitioned and isolated in a computer network at the data link layer. LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.



- Provides layer 2 separation of networks
- **Flood guarding**
    - **STP (Spanning Tree Protocol) - enable**

Routers

Router is a networking device which helps in routing the data packets between home network & other networks.



- Filter & forward based on **IP address**
- OSI Layer 3 [Network]
- Allocates IP addresses to the devices connected to it using a DHCP server.
- It performs **NAT** (Network Address Translation)

    NAT doesn't provide any security mechanisms. It's simply a way to convert from one IP address to another while the traffic is going through the network.

NAT example:

Origin address	NAT address
Internal Network	External Network
172.17.20.3	10.0.2.5

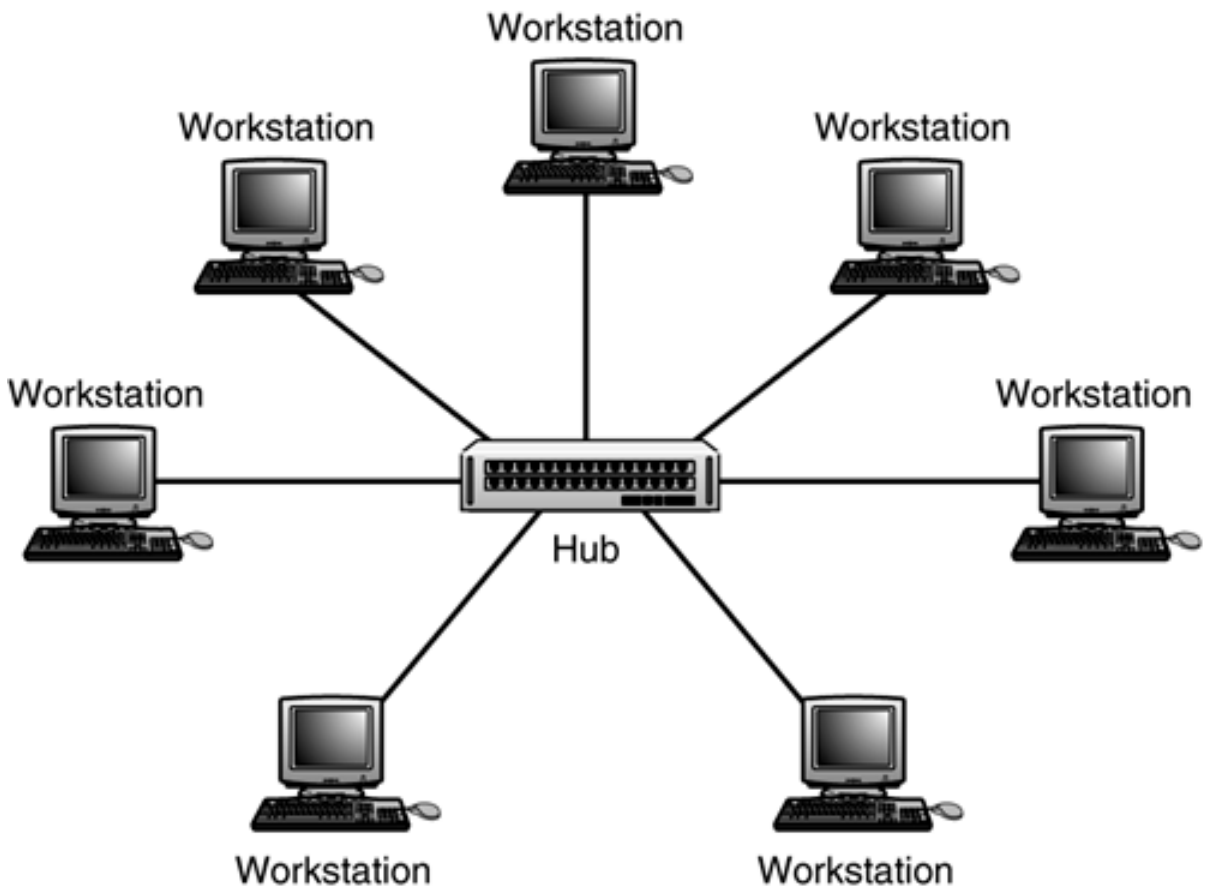
- *Generally operates in the Network layer*
- A firewall is a piece of software that is commonly run on a gateway router which protects us from the evils of the Internet, so it can forward and filter based on port numbers, based on IP addresses, URL's, all kinds of different stuff. **So we would call this a network firewall because the gateway is running the firewall software** and protecting us from the evil of the Internet.

Network Topologies - Basics

The actual organization of a network in terms of how is the data moving around and the best way to do it.

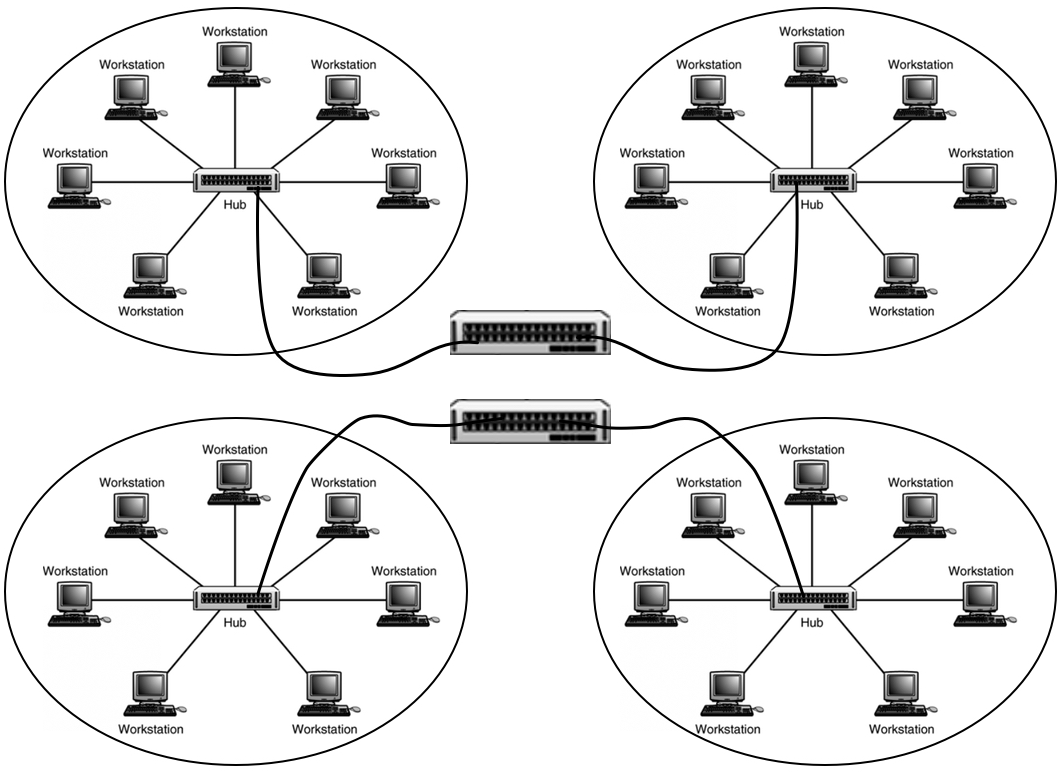
LAN - Local Area Network

- A LAN is a network that has a logical and physical borders that a computer can broadcast

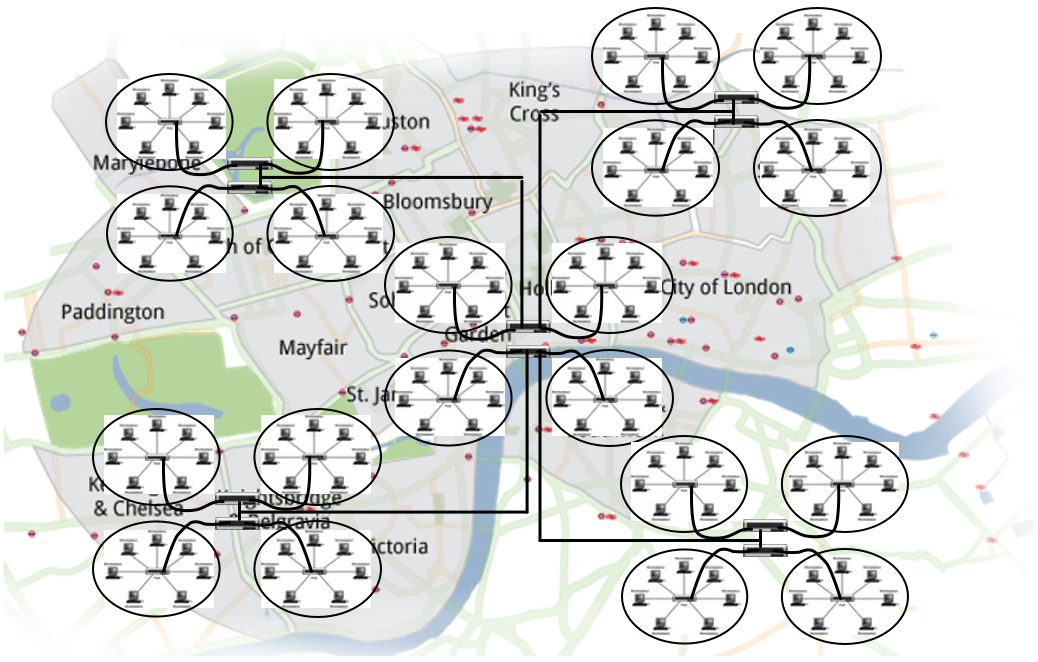


WAN - Wide Area Network

- WAN is a multiple LANs or additional WANs with routing functionality for interconnectivity.



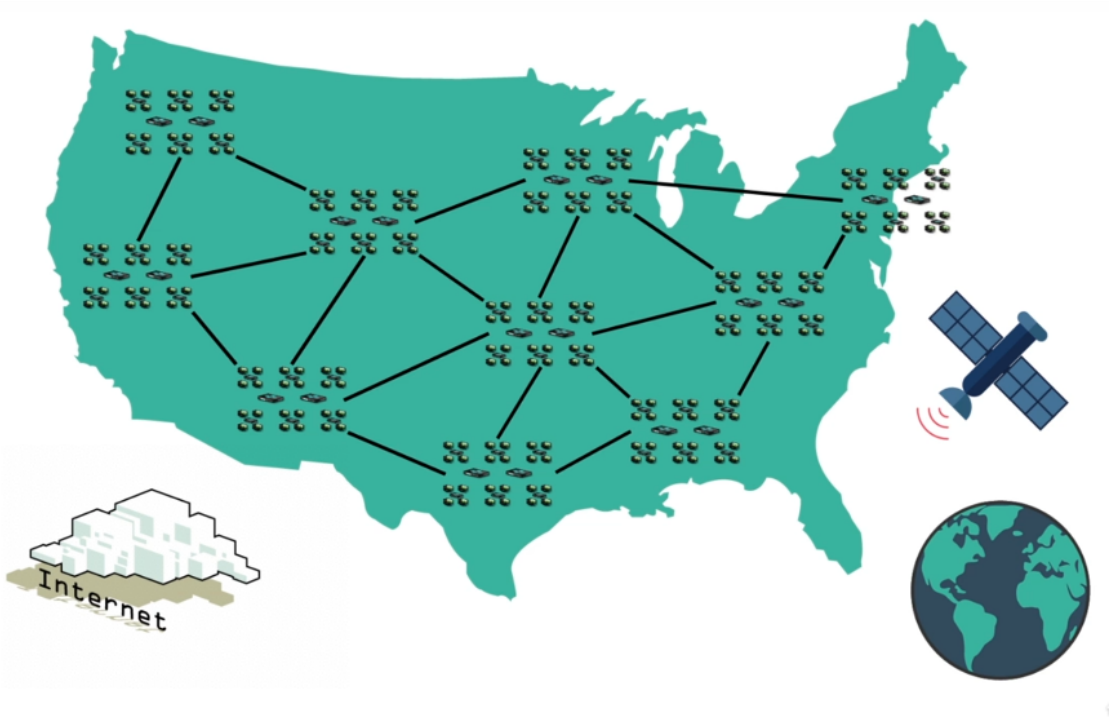
MAN - Metropolitan Area Network



Internet

Connecting WANs through WANs until complete the entire world = Internet.

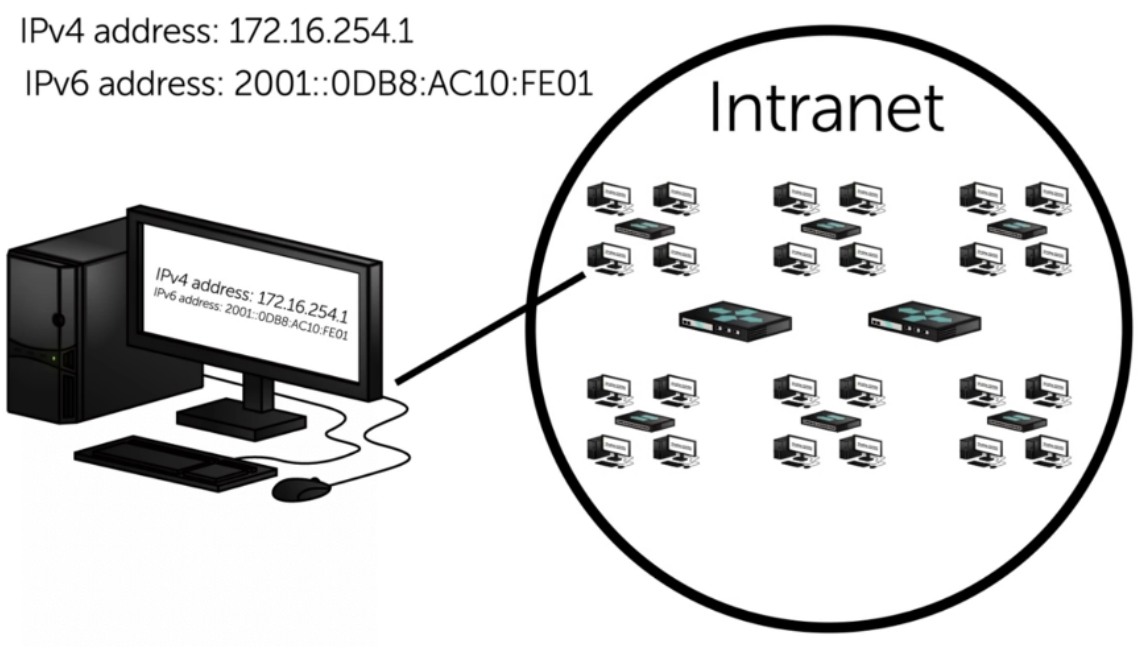
- The protocol which runs the internet is TCP/IP
- As long you're using legitimate IPv4 address or IPv6



Intranet

If you're using the TCP/IP stack and making your own LAN or WAN = Intranet.

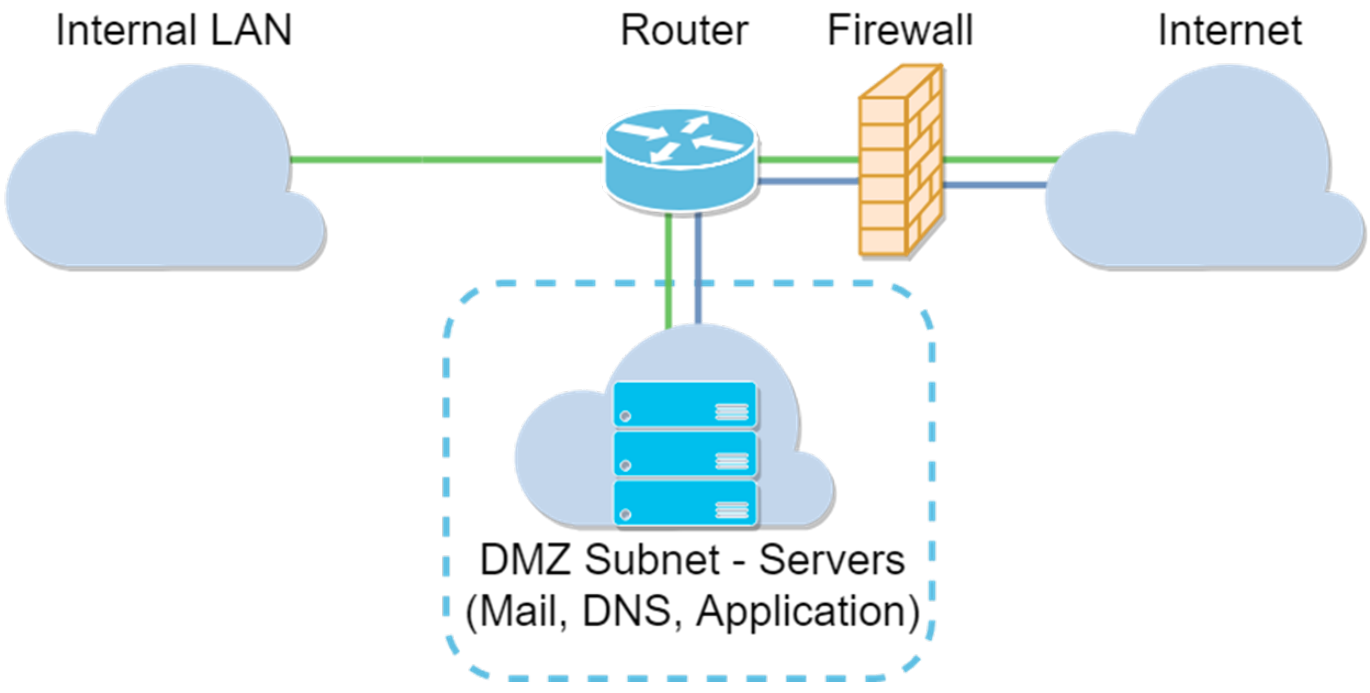
- Intranet is a private network which still runs TCP/IP



🛑 **Extranet**: example of some vendor who need to access the Intranet network. Works like a DMZ but for private access.

Network Zones - Concepts

- **DMZ** - **Demilitarized Zone**: Perimeter network; isolating untrusted network from LAN area. DMZ is a firewall configuration used to secure hosts on a network segment, in most DMZs the hosts on the DMZ are connected behind a Firewall that is connected to a public network(internet).



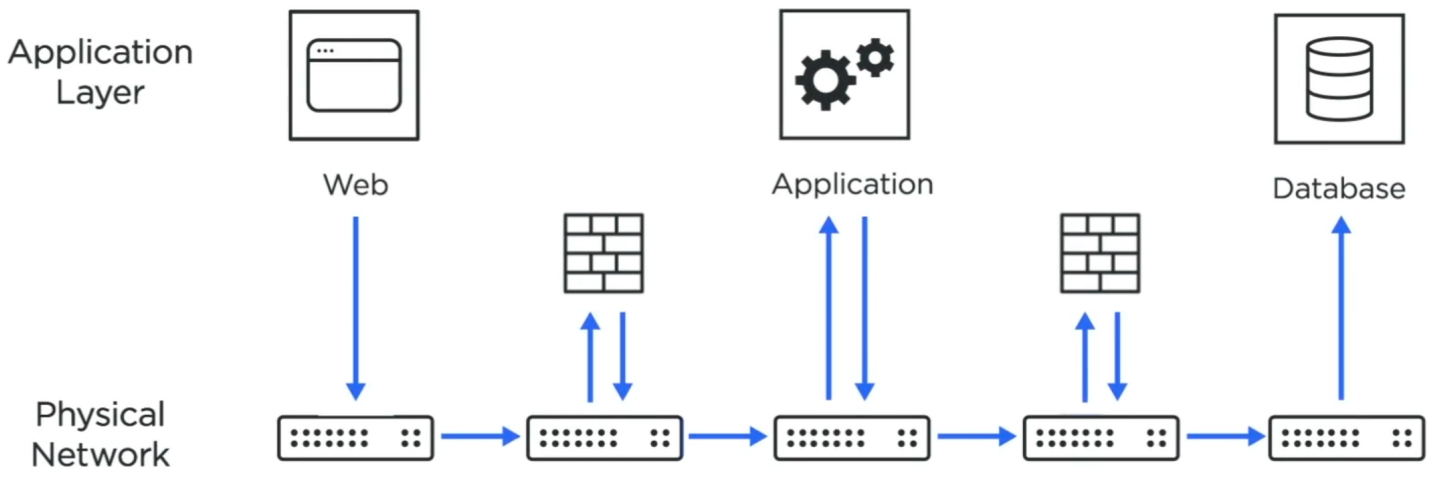
- **LAN** - the core of your network.
- **VLAN** - physical device that designate separate broadcast domains....
- **Wireless Network** - Basically a LAN connected to an Wireless Access Point (WAP).
- **Guest Network** - Optional network for meetings, demos, etc; Have no access to the internal network.
- **Ad hoc** - Wireless without an access point; Point to point communication; *(e.g AirDrop, contact sharing apps, etc)*
- **Airgap** - Simply means a disconnect to provide real isolation and the use of a completely separate internet from the world; Private internet. *(e.g Military/governmental computer network/systems)*
- **Virtualization**

  🛑 **NAT** doesn't provide any security mechanisms. It's simply a way to convert from one IP address to another while the traffic is going through the network.

Network Segmentation

- Physical, logical, or virtual segmentation
  - Devices, VLANs, virtual networks
- Performance
  - High-bandwidth applications
- Security
  - Users should not talk directly to database servers
  - The only applicatons in the core are SQL and SSH

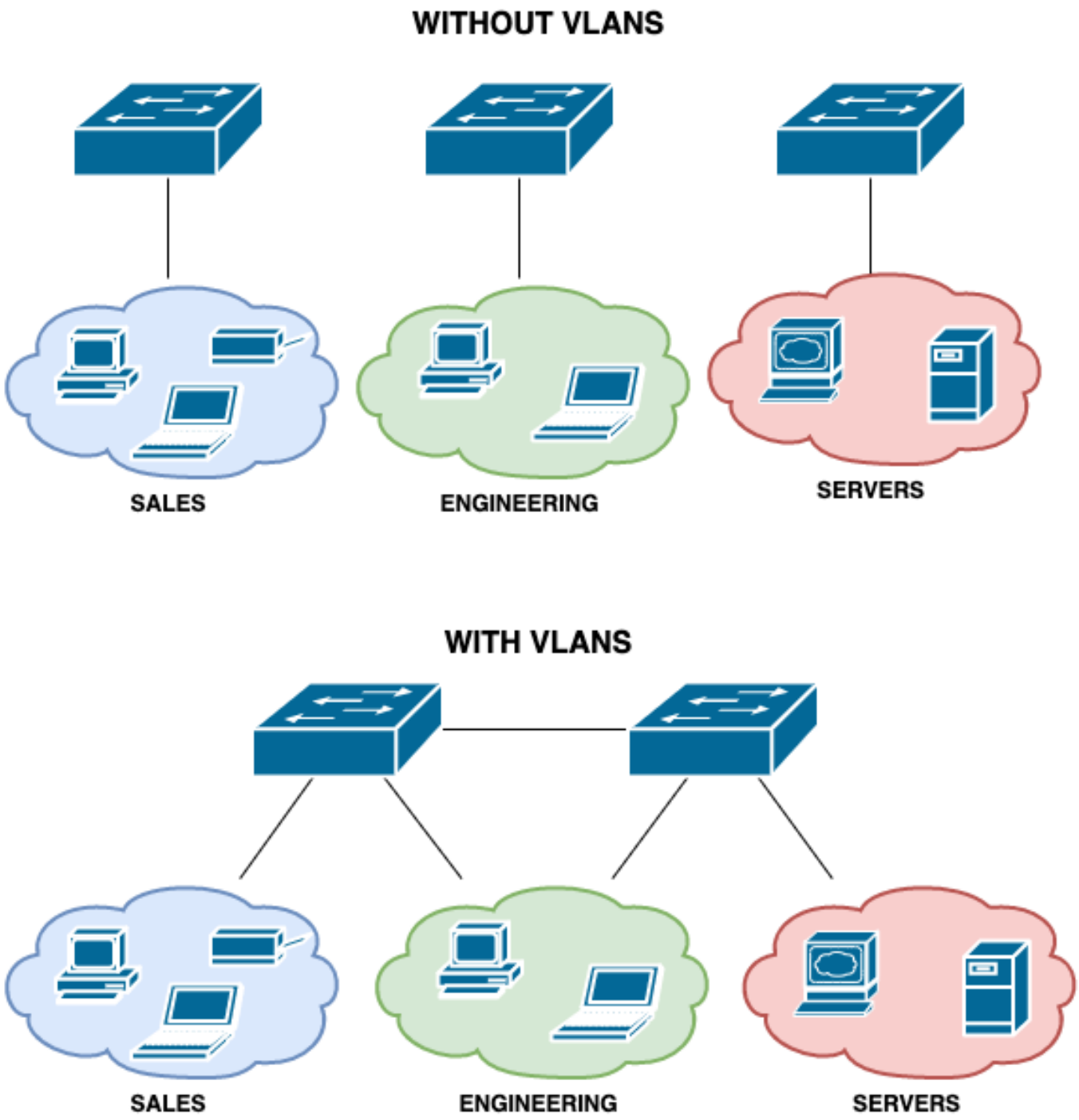
Physical Segmentation - Switches



- **Devices are physically separate**
  - Switch A and Switch B, and so on

- Must be connected to provide communication
    - **Direct connect**, or another switch or router
- **Web servers in one rack, Database servers on another**

Logical Segmentation using VLANs



- Separated logically instead of physically
- Cannot communicate between VLANs without a Layer 3 Device / Router

Virtualizing everything

- When you get rid of physical devices
- Servers, switches, routers, firewalls, load balancers
- Instant and complete control
    - Build a new network
    - Route between IP subnets
    - Drop a firewall between
    - Drag and drop devices between networks

Airgaps

- Remove any connectivity between components
    - No possible way for one device to communicate to another
    - No shared components
- Network separation
    - Secure networks
    - Industrial systems (SCADA, manufacturing)

    - Military/governmental computer network/systems
- 🛑 Removable media can jump the gap

Network Access Control (NAC)

Can be used to prevent hosts from connecting to the network unless they meet certain security requirements

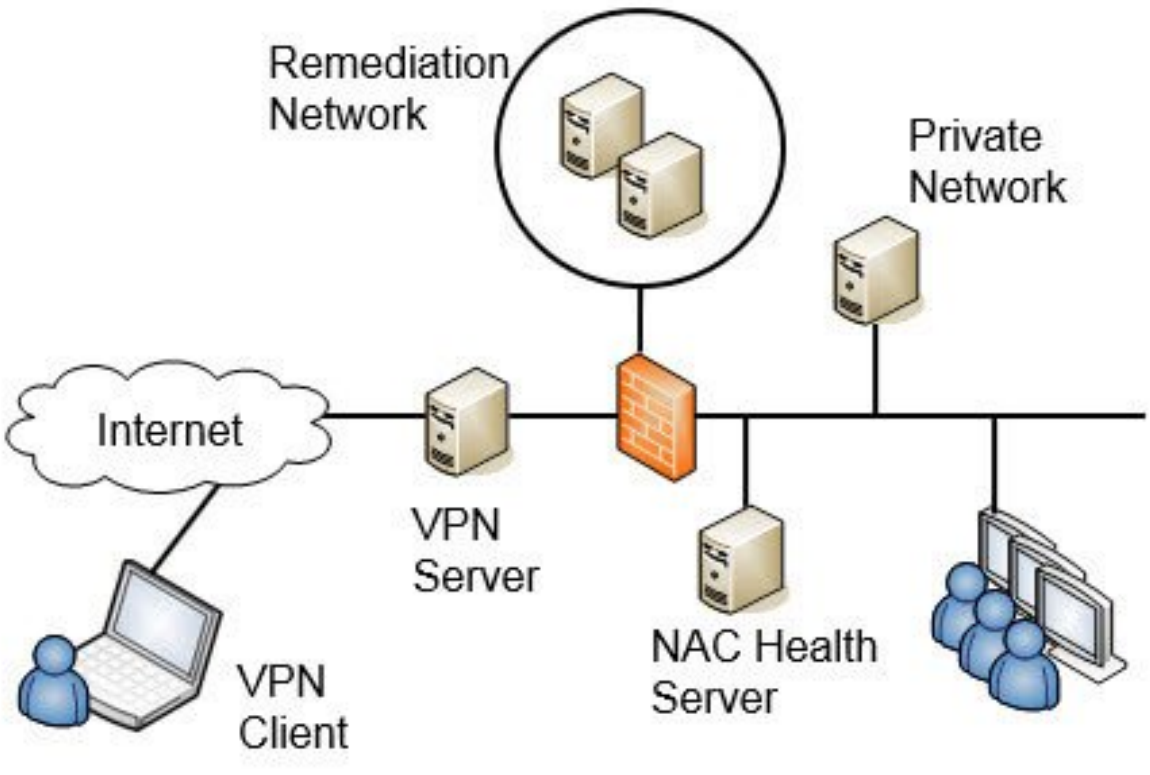
Wireless Network, Remote Access, VPN Access

- Control from wherever you are (inside or outside)
- Access can be based on many rules (by user, group, location, application etc)
- Access can be easily revoked or changed

Posture assessment

BYOD, Malware infections, missing anti-malware, unauthorized applications.

- Before connecting to the network, perform a **health check**:
    - Is it a trusted device?
    - Is it a running anti-virus? Which one? Is it updated?
    - Are the corporate applications installed?
    - Is the disk encrypted?



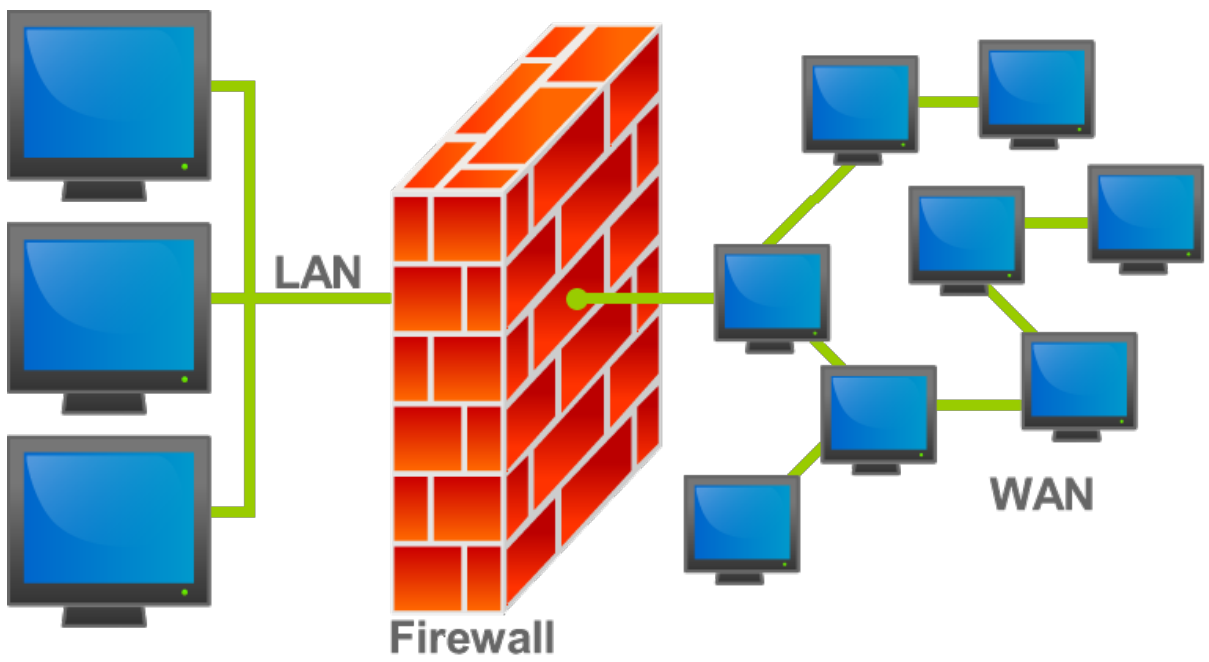
Health checks from Posture Assessment

- Persistent agents
    - Permanently installed onto a system
- Dissolvable agents
    - No installation is required
    - Runs during the posture assessment
    - Terminates when no longer required
- Agentless NAC
    - Integrated with Active Directory
    - Checks are made during login and logoff
    - Can't be scheduled

🛑 **If Posture Assessment fails**, the quarantine network notify administrators, just enough network access to fix the issue.

Network Firewalls - Concepts

- Control the flow of network traffic
- Standard issue - home, office, and in your operating system



- Corporate **control of outbound and inbound** area (sensitive data)
- Control of inappropriate content
- Protection adware, spyware etc
- **Firewall Rules**
  - **ACL - Access Control Lists**
    - Allow or disallow traffic based on tuples
    - Grouping of categories (Source IP, Destination IP, port number, time of day, application, etc)
  - Can be very general or very specific
  - **Implicit deny** - prevents access unless specifically permitted.
- Filters traffic by port number
  - OSI layer 4 (TCP/UDP) - **some firewalls can filter through OSI layer 7**
- Can encrypt traffic into/out of the network
- Can proxy traffic
- Most firewalls can be **layer 3 devices (routers)**

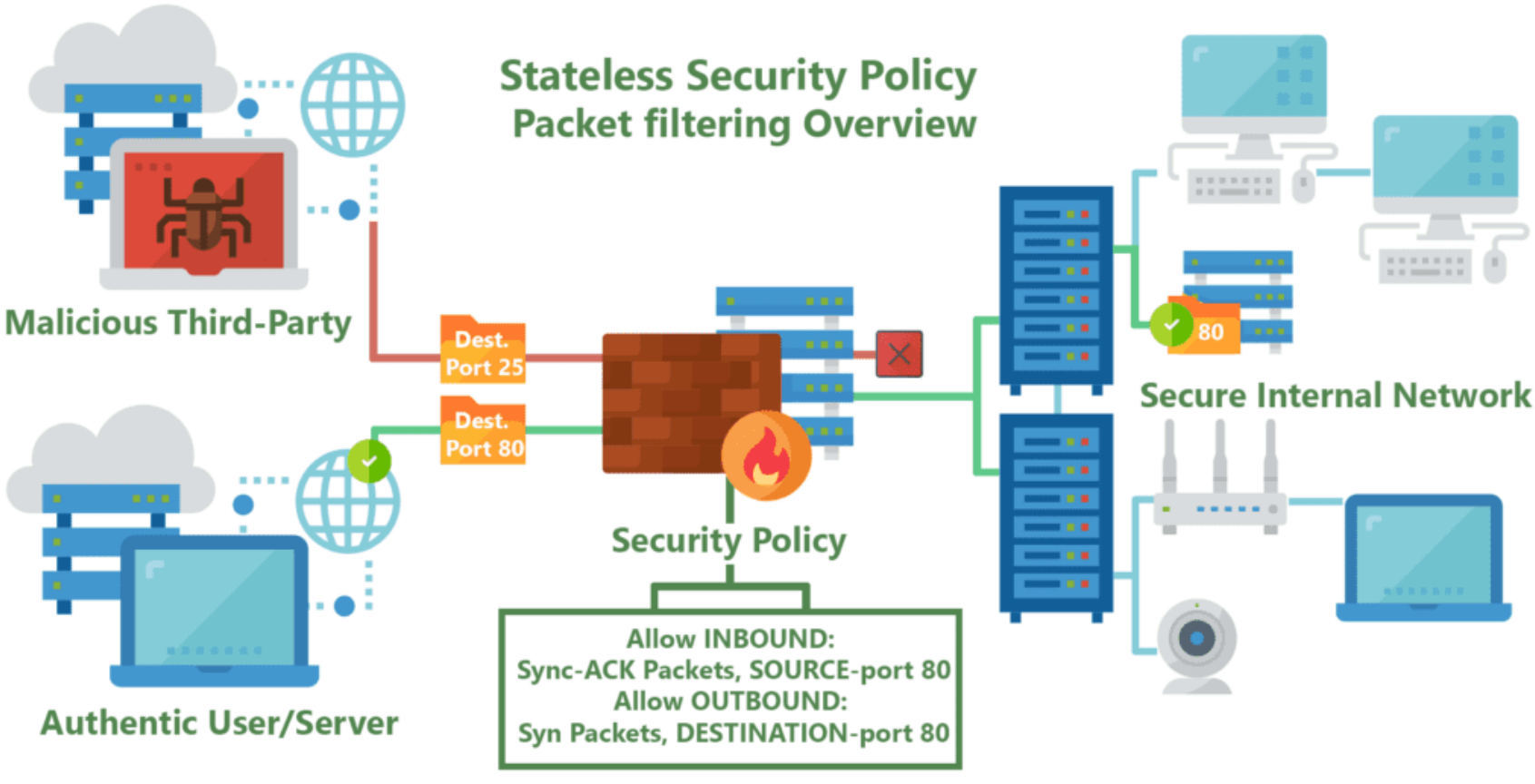
🛑 A "deny any-any" rule denies all traffic from all sources, so it should be the last rule in the ruleset.

Stateless Firewall

- **Typically faster and perform better under havier traffic loads.**

They watch network traffic and restrict / block packets based on source and destination address or static values **(ACL Rules)** as shown below.

Rule #	Source IP	Destination IP	Dest Protocol (TCP/UDP)	Dest Port #	Allow/ Block
1	10.1.1.1	10.10.10.10	tcp	80	Allow
2	10.10.10.10	10.1.1.1	tcp	any	Allow



Stateful Firewall

- **Are better at identifying unauthorized and forged communications.**

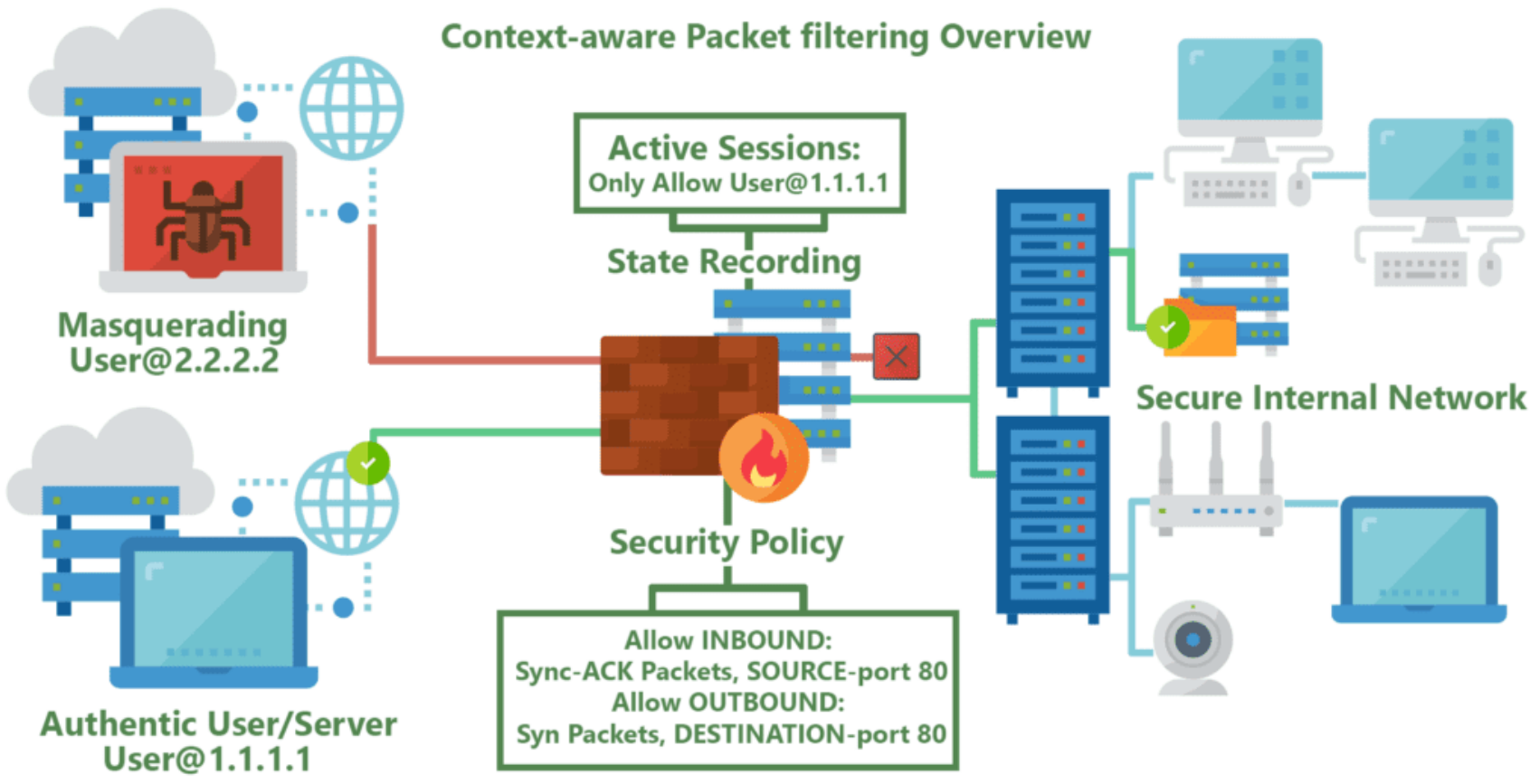
Can watch traffic streams from end to end. They are aware of communications paths; Can implement varios **IPSec** functions (tunnels and encryption); **Can tell what stage a TCP connection is in (open, open sent, synchronized SYN ACK or established).**

ACLs

Rule #	Source IP	Destination IP	Dest Protocol (TCP/UDP)	Dest Port #	Allow/ Block
1	10.1.1.1	10.10.10.10	tcp	80	Allow

Session Table

Session#	Protocol	Source IP	Source Port	Destination IP	Destination Port
1	tcp	10.1.1.1	15442	10.10.10.10	80



Packet-filtering

- Inspect data packets (drop or forward), such as the destination and originiation IP address, packet type, port number and other surface-level information.

Circuit-level firewall

- Quickly approve or deny traffic; verify transmission protocol (TCP) handshake (session).

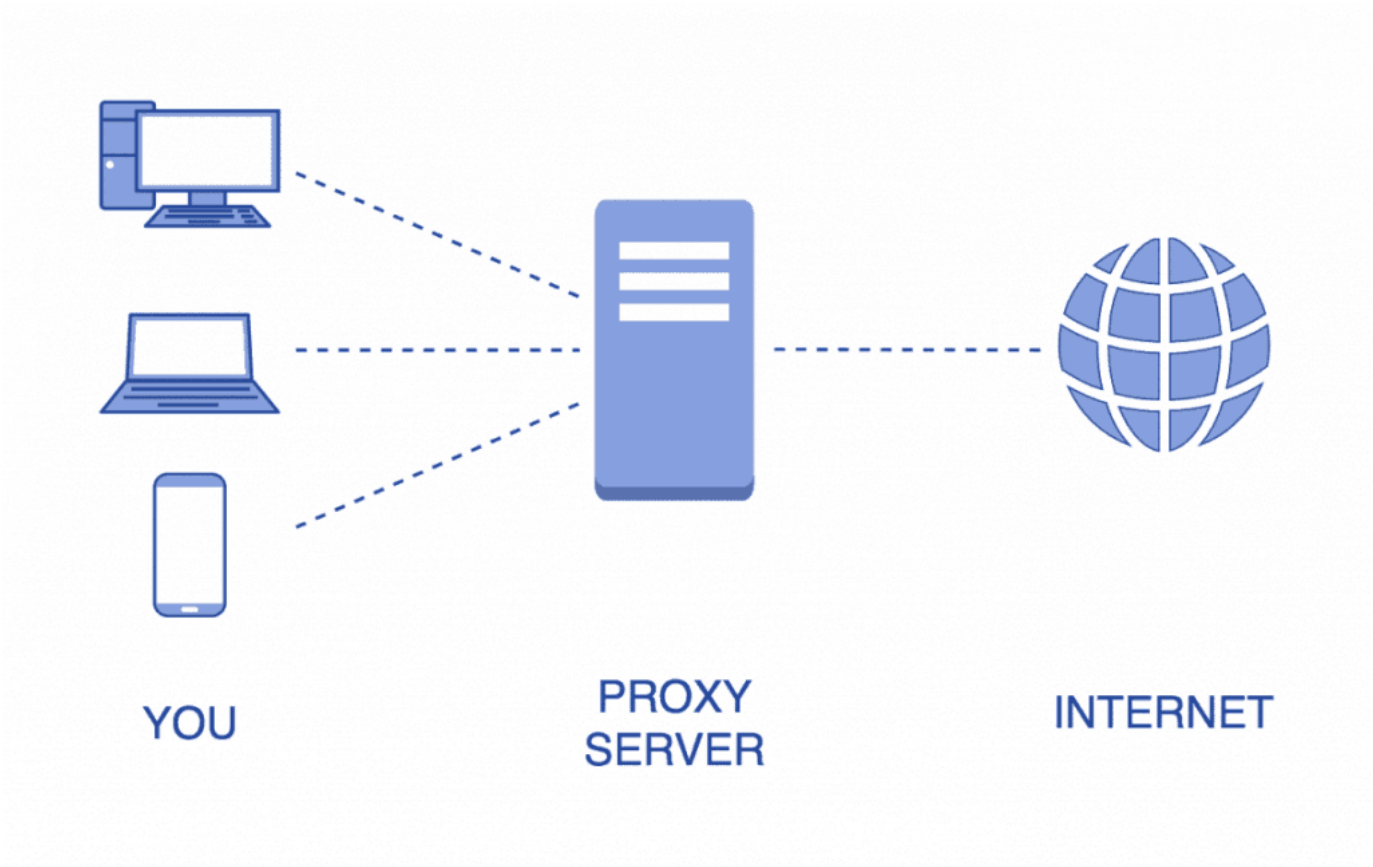
Application-level Firewall

- Filter traffic based on user group, group membership, application or services (works at **layer 7 OSI [Application Layer]** - also called proxy firewall as well).
- Every packet must be analyzed and categorized before a security decision is determined.

Proxy Servers

A box/piece of software running on a computer acts an intermediary between two different devices having a session.

- Useful for caching information, access control, URL filtering, content scanning.



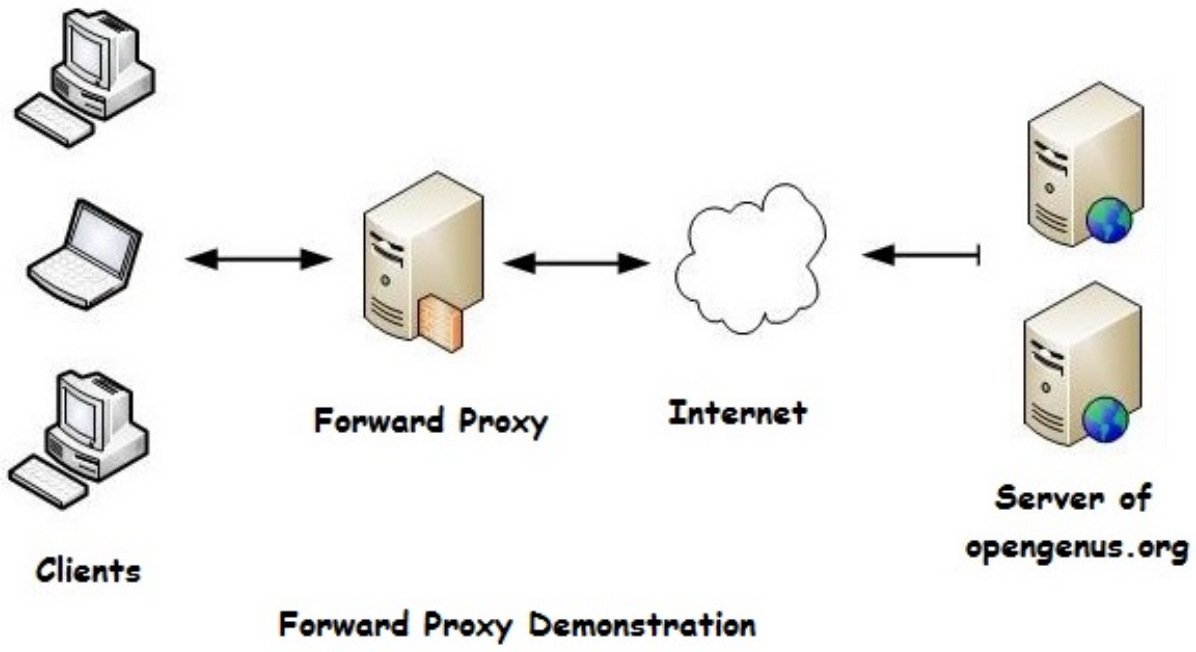
Most proxies in use are application proxies; Many proxies are multipurpose proxies (HTTP, HTTPS, FTP, etc)

- Application-specific
  - Web proxy
  - FTP proxy
  - VOIP proxy

- One of the simplest 'proxies' is NAT (Network Address Translation) - a Network-level proxy.

Forward Proxy - Client

The proxy simply forward the requests of respective client and retrieve the response back to the client.

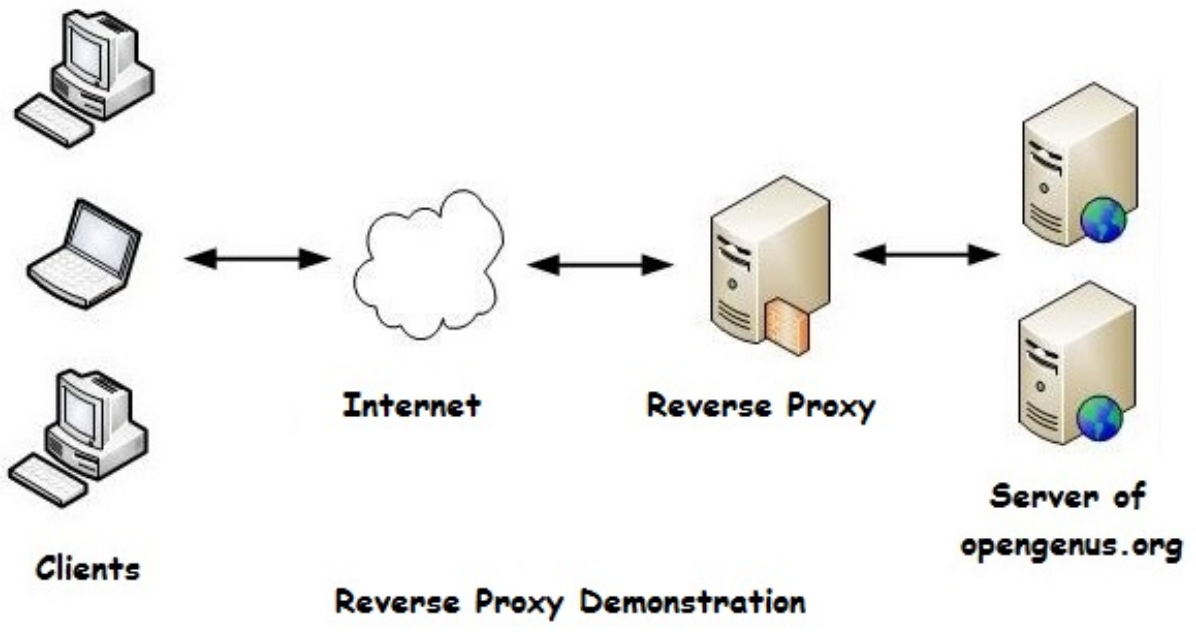


Forward Proxy Demonstration

- Hides the **client**
- Provides:
    - Caching
    - Content filtering
    - Acts similar to firewall (block based on URL, content filtering and so on).

Reverse Proxy - Server

Like a forward proxy but complete reverse.

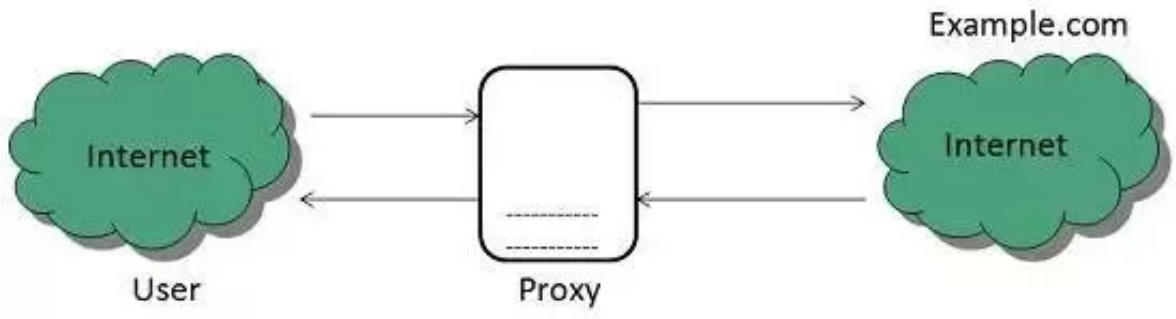


Reverse Proxy Demonstration

- Hides the **servers**
- Provides
    - High security
    - Protect the servers
    - Handle DoS attacks
    - Load balancing
    - Caching
    - Encryption acceleration

Open Proxy

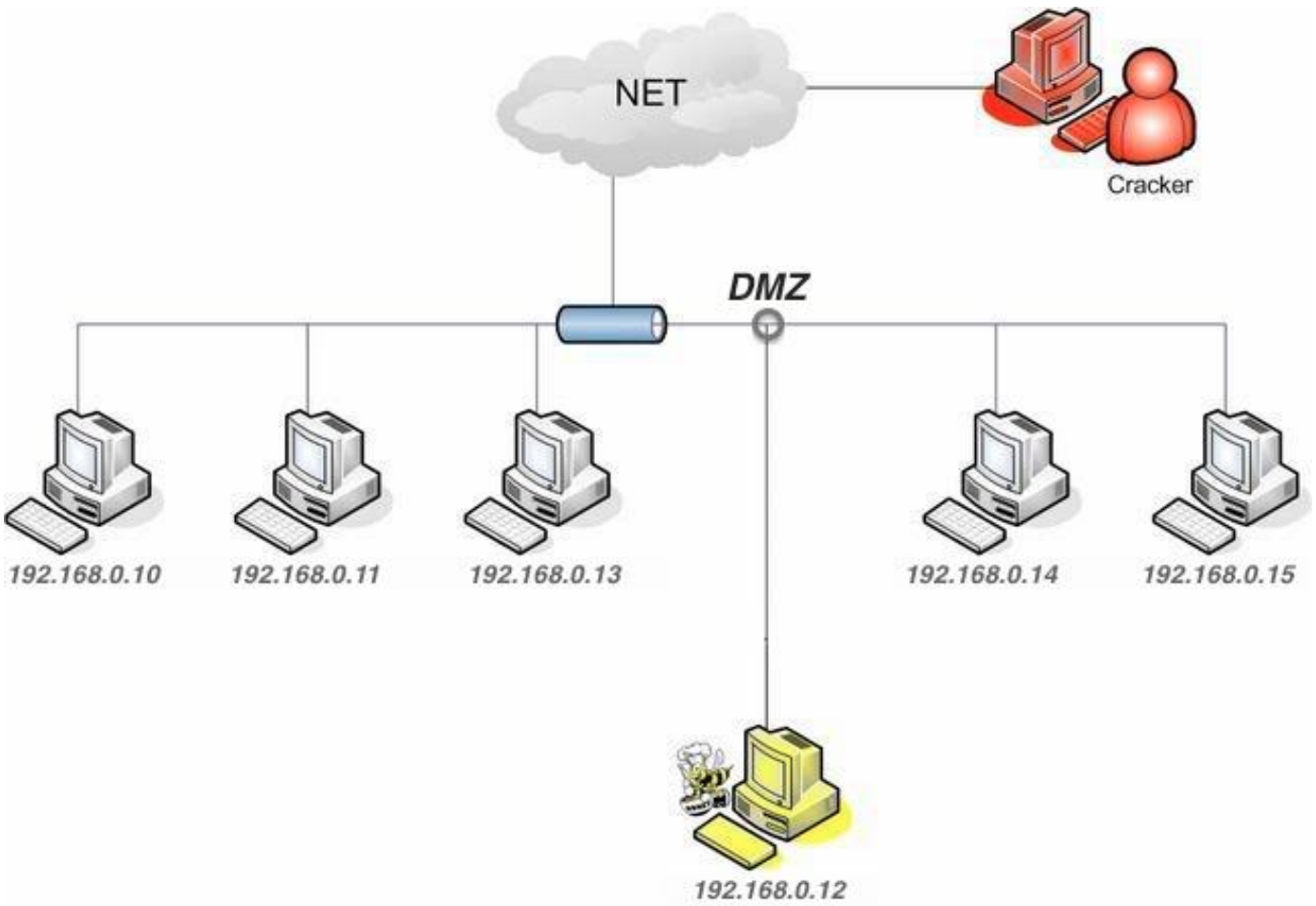
- A third-party, uncrontrolled proxy
    - Can be a significant security concern
    - Often used to circumvent existing security controls
- **A significant security concern** about open proxies, is that the owner of the proxy can add whatever they'd like into the network communication. They can send URL request and response with malicious code or redirection to another malicious website.



Honeypots

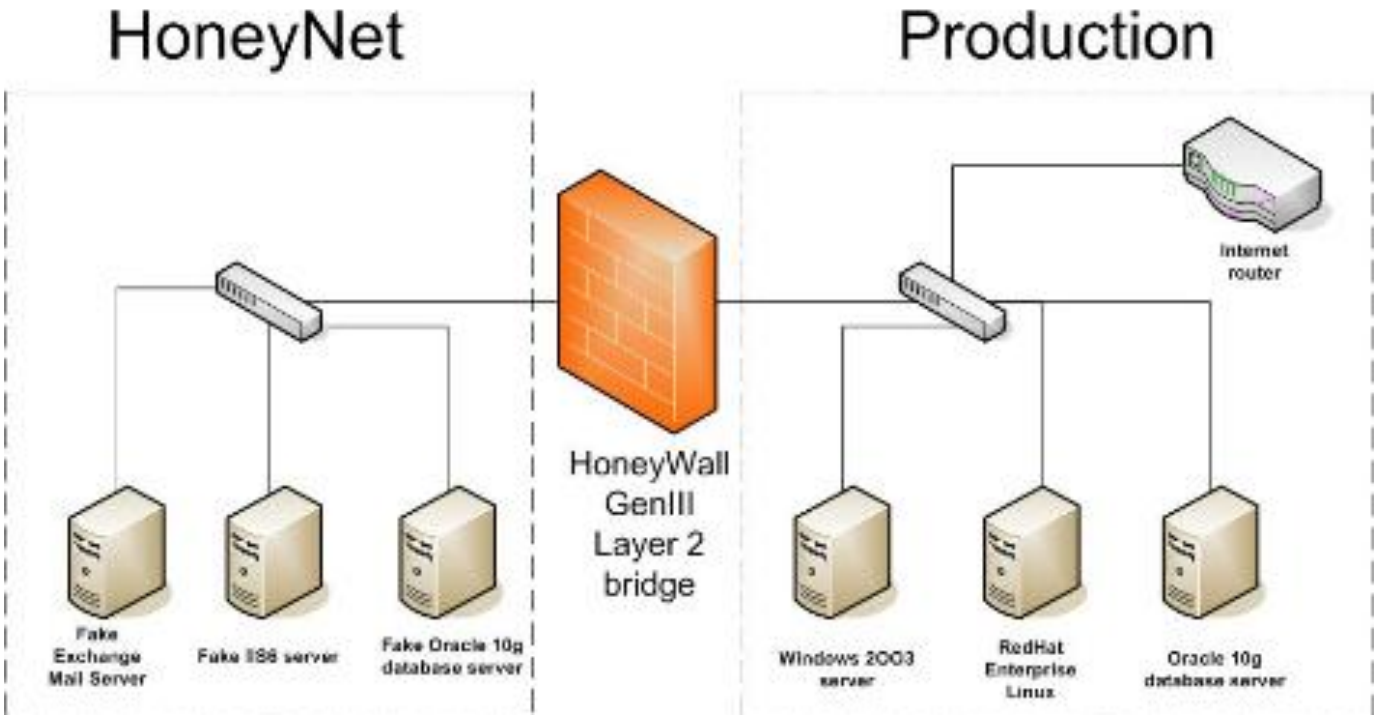
Emulate a web server, vulnerable machine purposely to attack; Inviting target to keep away from targets.

- Benefit to see how threat actors, what techniques they're using, what vulnerabilities are they look for, what ports, and so on.
- Log all information (port information and the origin IP address)
- **Usually located in the DMZ to get close to the source but still isolated to capture the traffic.**
- **Tools**:
  - Project Honeypot
  - Honeyd



Honeynet

A honeynet is a vulnerable and **simulated computer network** using a decoy server. **By design, honeynets are not authorized for any authentic uses. If a honeynet is accessed, a fair assumption is that the person accessing it is a bad actor.**



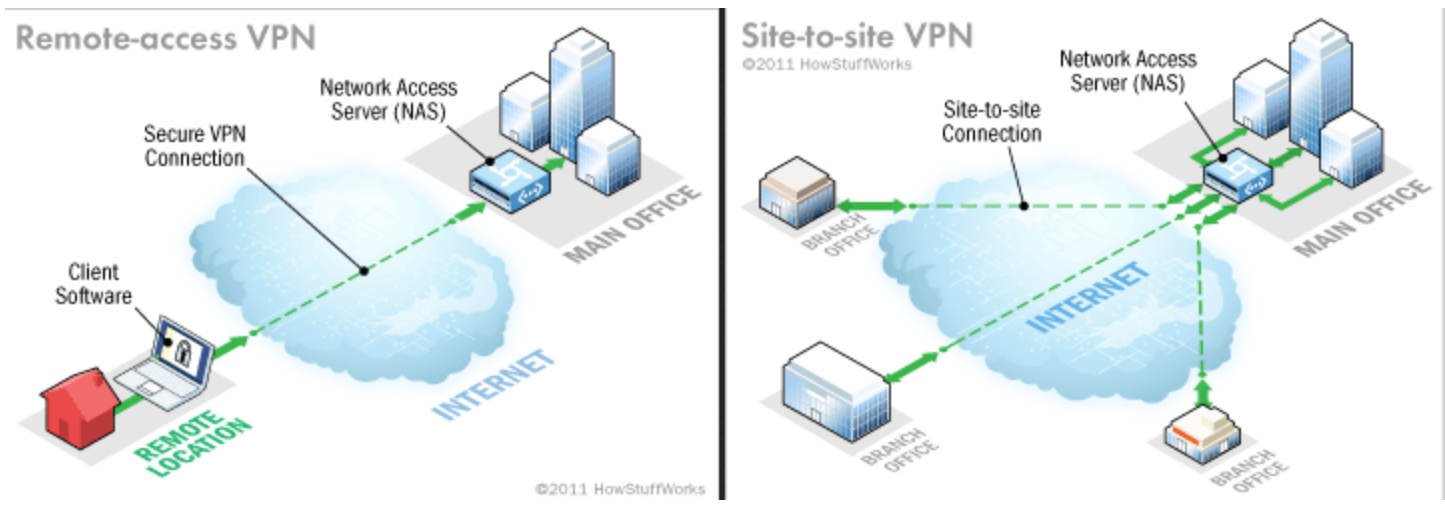
UTM - Unified Threat Management

- **All-in-one security appliance**
- Combine a lot of security technologies in one device:
  - URL Filter / content inspection
  - Malware inspection
  - Spam filter
  - CSU/DSU
  - Router, Switch
  - Firewall
  - IDS/IPS
  - Bandwidth shaper
  - VPN endpoint

VPN - Virtual Private Networks

Organizations use virtual private networks (VPNs) to create an end-to-end private network connection (tunnel) over third-party networks such as the Internet or extranets. The tunnel eliminates the distance barrier and enables remote users to access central site network resources. The **IP Security (IPsec) protocol** provides a framework for configuring secure VPNs and is commonly deployed over the Internet to connect branch offices, remote employees, and business partners. Secure site-to-site VPNs, between central and remote sites, can be implemented using the IPsec protocol. IPsec can also be used in remote-access tunnels for telecommuter access.

The two types of VPN - Remote Access and Site-to-Site



Remote-access VPN

is created when VPN information is not statically set up, but instead allows for dynamically changing information and can be enabled and disabled. Consider a telecommuter who needs VPN access to corporate data over the Internet. The telecommuter does not necessarily have the VPN connection set up at all times. The telecommuter's PC is responsible for establishing the VPN, each host typically has Cisco VPN client software.

Site-to-Site VPN

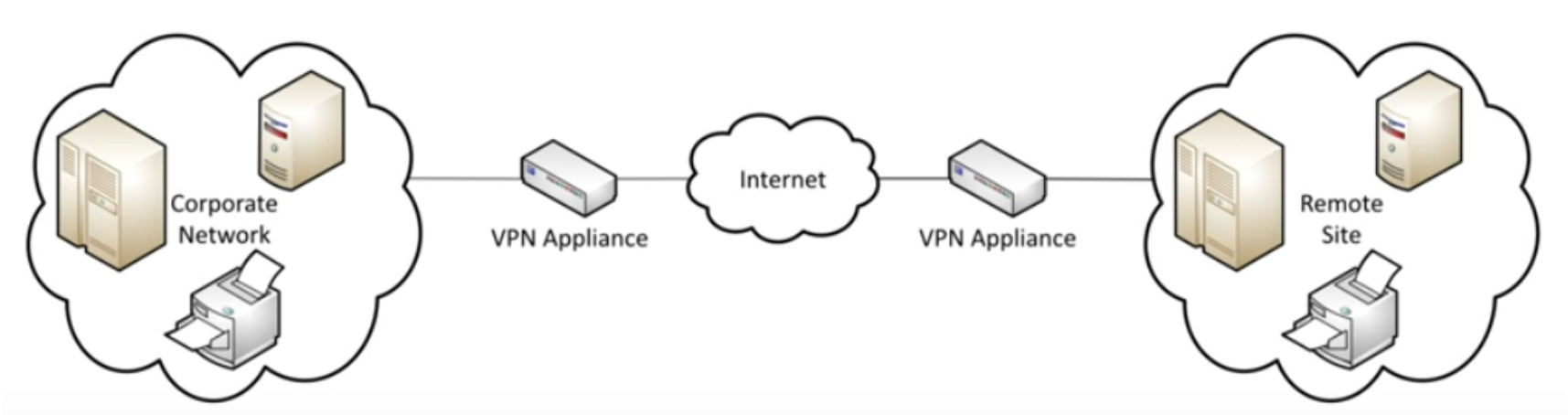
is created when connection devices on both sides of the VPN connection are aware of the VPN configuration in advance.

VPN Setup Steps

1. Protocol to set up tunnel
2. Protocol to handle authentication and encryption

VPN Concentrators

- VPN appliances are usually located on the edge of the network
    - Internet-facing
- Sites connect from one site to another across the Internet



- The Appliances can be a standalone VPN devices or it may be integrated into another technology, such as Firewall.

Early VPNs Protocols

- **PPTP** - Point-to-Point tunneling Protocol
    - Oldest VPN protocol
    - Uses PPP for tunnel
    - Password only

    - **TCP port 1723**
    - Weak encryption

- **L2TP** - Layer 2 Tunneling Protocol
    - Cisco proprietary
    - SImilar to PPTP
    - L2TP tunnel
    - IPsec encryption
    - **UDP ports 500, 1701, 4500**
    -

- 'Pure' **IPsec**
    - uses IPsec for tunneling and encryption
    - Great for IPv6
    - **UDP ports 500, 4500**

- **SSL** and **TLS**
    - **TCP port 443**
    - Often works within a web browser
    - TUN/TAP (virtual network driver) tunnel
    - TLS encryption

- **OpenVPN**
    - Unique tunnel
    - Encryption based on SSL/TLS protocol
    - **TCP port 1194**, but can be changed

IPSec - Internet Protocol Security

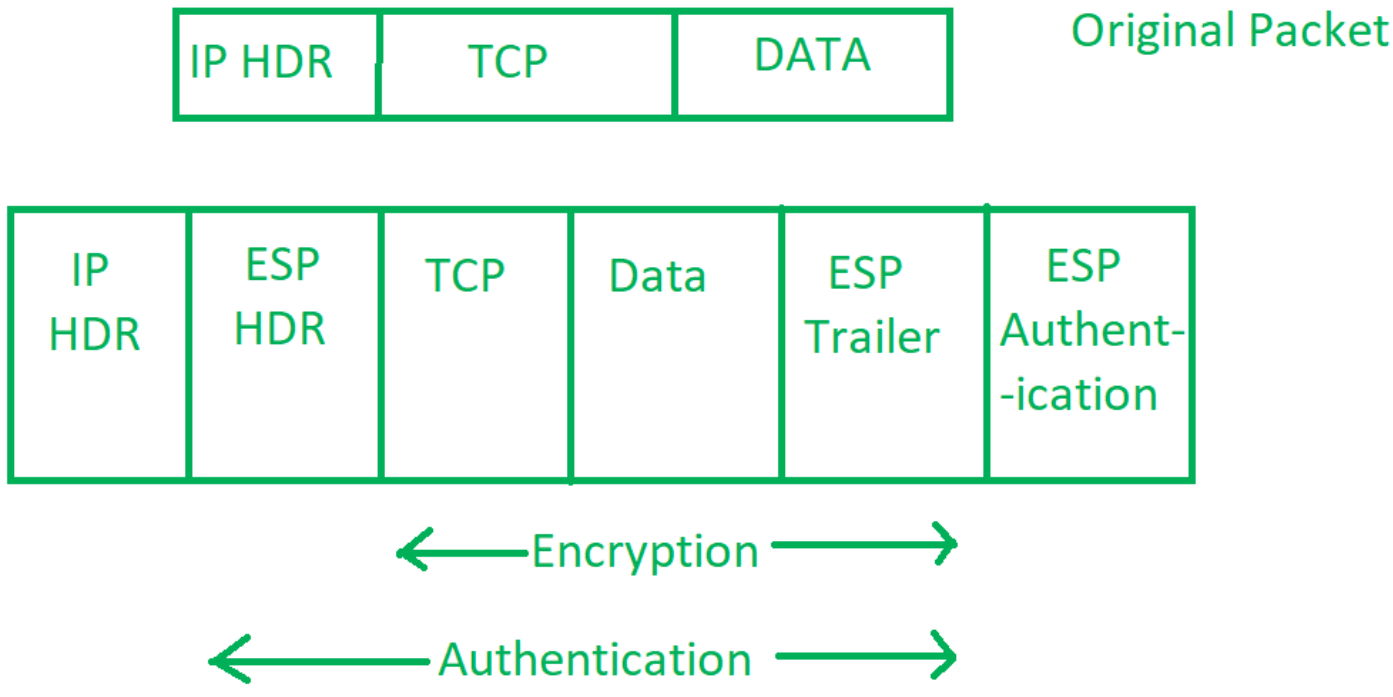
Is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over an IP network.

- 🛑 IPSec works at the Layer 3 - Network (IPv4)

IPSec Components

1. **Encapsulating Security Payload (ESP)** – It provides data integrity, encryption, authentication and anti replay. It also provides authentication for payload.
2. **Authentication Header (AH)** – It also provides data integrity, authentication and anti replay and it does not provide encryption. The anti replay protection, protects against unauthorized transmission of packets. It does not protect data's confidentiality.

3. **Internet Key Exchange (IKE)** – It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication. **The Key Management Protocol (ISAKMP) and Internet Security Association which provides a framework for authentication and key exchange.** ISAKMP tells how the set up of the Security Associations (SAs) and how direct connections between two hosts that are using IPsec.



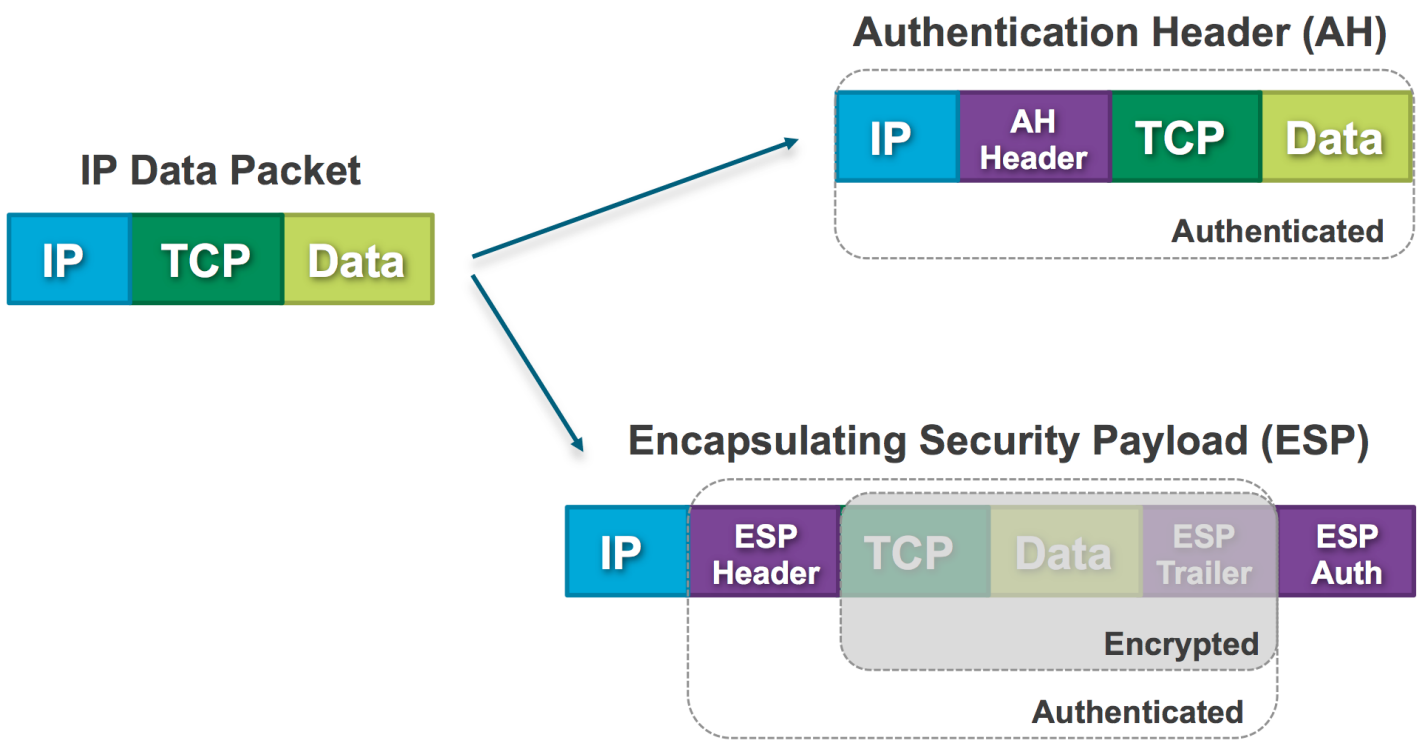
IPSec Transport Mode and Tunnel Mode

When IPsec protects traffic, it has a couple of services and modes to choose from.

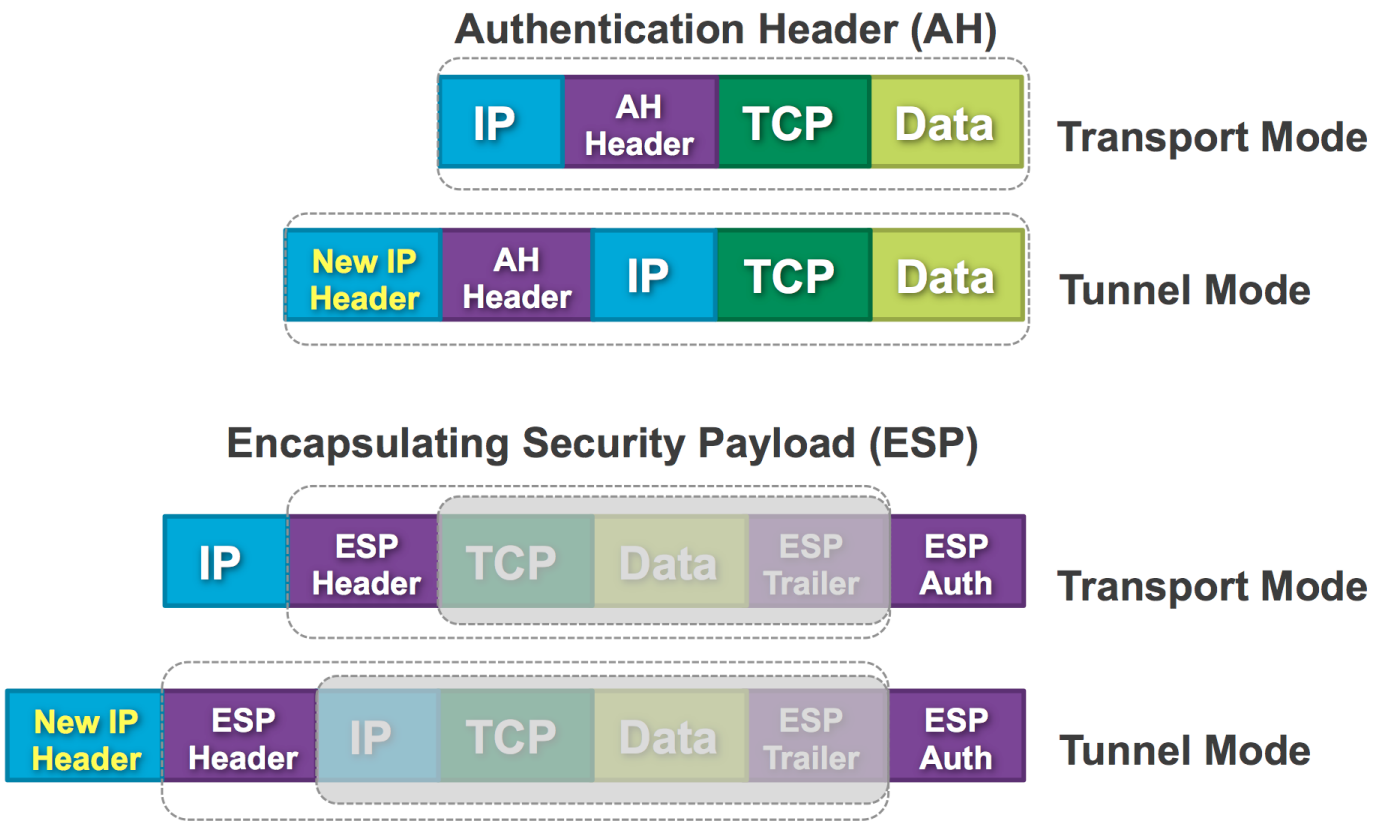
Transport mode - preserving original IP header. Typically used in combination with GRE or other encapsulating protocols. (Host-to-Host)

Tunnel mode - encapsulating entire IP datagram within a new header, essentially tunneling the packet. (The gateway creates the tunnel)

1. *Some TCP data will be sent over:*



2. *And now about how those IP protocols fit in the two modes.*



The last mode is what is typically used with crypto map based IPsec VPNs.

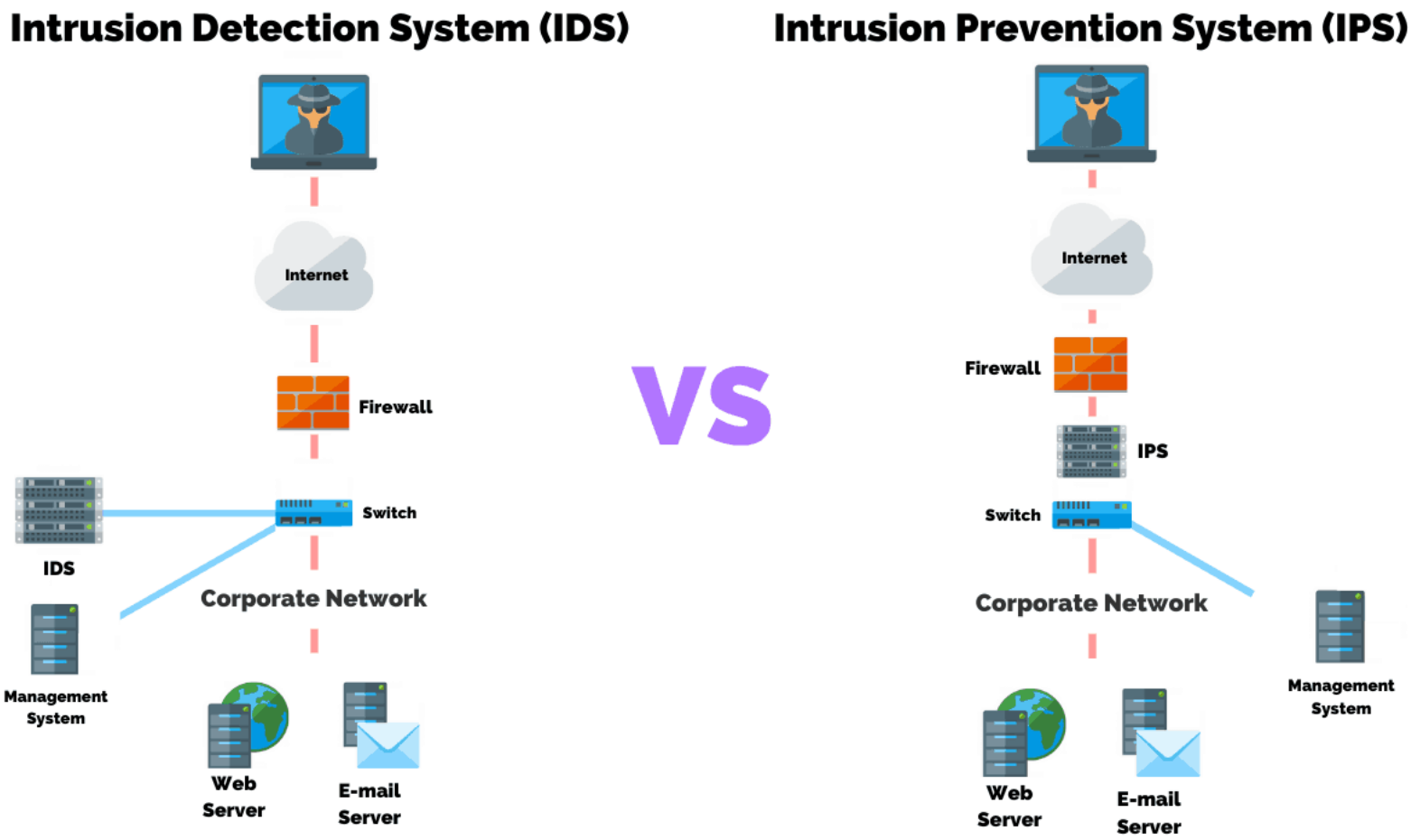
Use of IPSec

- **VPNs**
    - Pure IPsec (using tunneling mode)
    - IPSec with L2TP (add a tunnel layer)
- **RADIUS and TACACS+**
- **IPSec with IPv6**
- **Using IPSec with Non-security protocols / Encrypting Unsecured Protocols**
    - e.g. IPsec over Telnet

NIDS and NIPS

Both technologies watch network traffic to detect exploits against OS, applications, etc.

- **Network Intrusion Detection Systems (NIDS)**
    - Passive device that detect anomalies.
- **Network Intrusion Prevention Systems (NIPS)**
    - Active device that detect and prevents when something on the network traffic is suspicious by blocking it.



- Attacks could be in the form of malformed network traffic or excessive amounts of traffic.

Prevention vs. Detection

Detection

- **NIDS** is a **passive** device and focuses on detection alone, making it a **detection control**. It detects network traffic issues and **alerts and administrator** to these issues, also logging the events in the process.

Prevention

- **NIPS** is /**inline**(Active) device and focuses not only on detecting network attacks, but **preventing them. (e.g block things from router)**

Identification technologies

NIDS/NIPS solutions act very much like firewalls in that they inspect packets.

There's 4 types of detection methods:

1. **Behavioral/Anomaly** - Comparing traffic with a baseline of patterns considered normal for the network
2. **Signature** - Preconfigured Signature-based
3. **Rule** - Preconfigured rules in a ruleset - like firewall
4. **Heuristic** - Use AI to identify (Anomaly and Signature)

   - *Anomaly-based NIPS/NIDS detect new patterns and are much more efficient than signature-based, which can only work with known variants.*

   - Remember all these technologies can report **False positives** or **False negatives**.

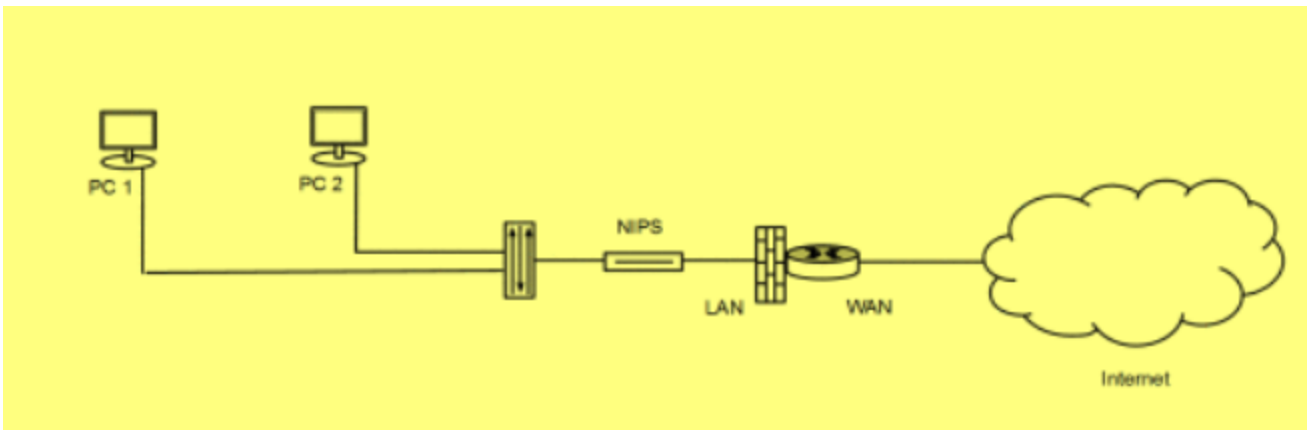
   - **In simple words:**

     - **IDS: Notifies**
     - **IPS: Acts to stop**
     - **Firewall: Filters**

Sensors

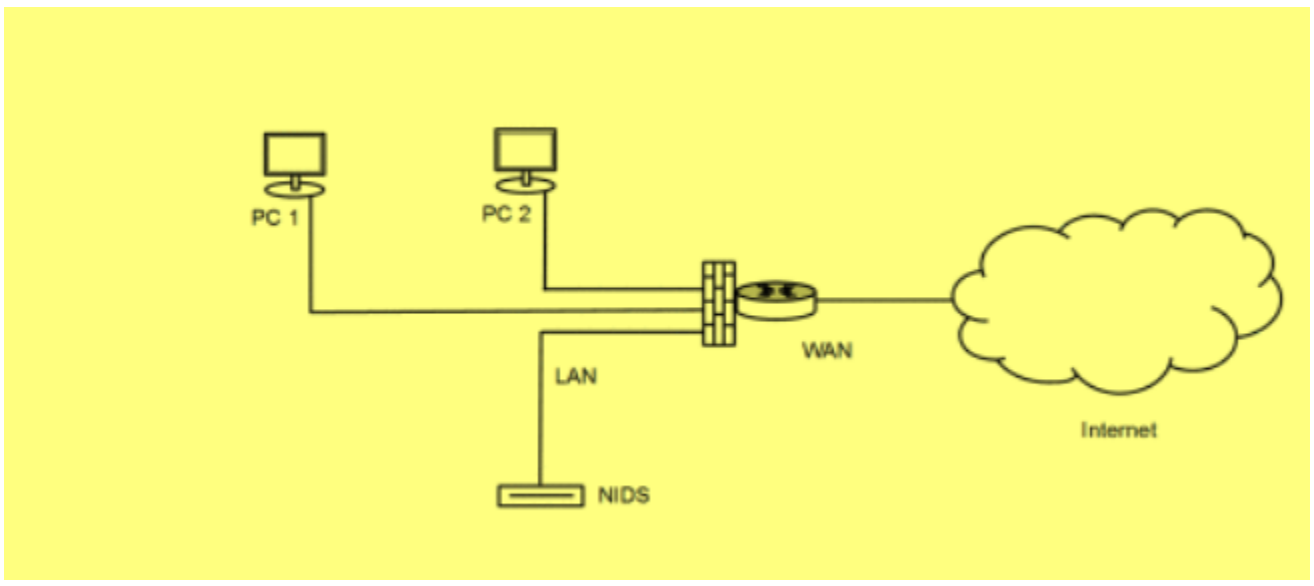
NIPS uses In-band sensor

- NIPS sensor must be installed **in-band** to your network traffic. All packets must go through in-band sensor devices/



NIDS uses Out-of-band sensor

- NIDS sensor, being **passive**, is normally installed **out-of-band** of the communication. Just plugging it into a switch only allows the sensor to see traffic to and from the switch plus broadcast traffic. The common out-of-band devices is a **network tap** or a **port mirror.**



Network Tap

- Is a device that you can insert anywhere along a run to grab packets / intercepting network traffic
- Physical taps
  - Disconnect the link, the tap goes in the middle
  - Can be an active or passive tap

Port Mirror

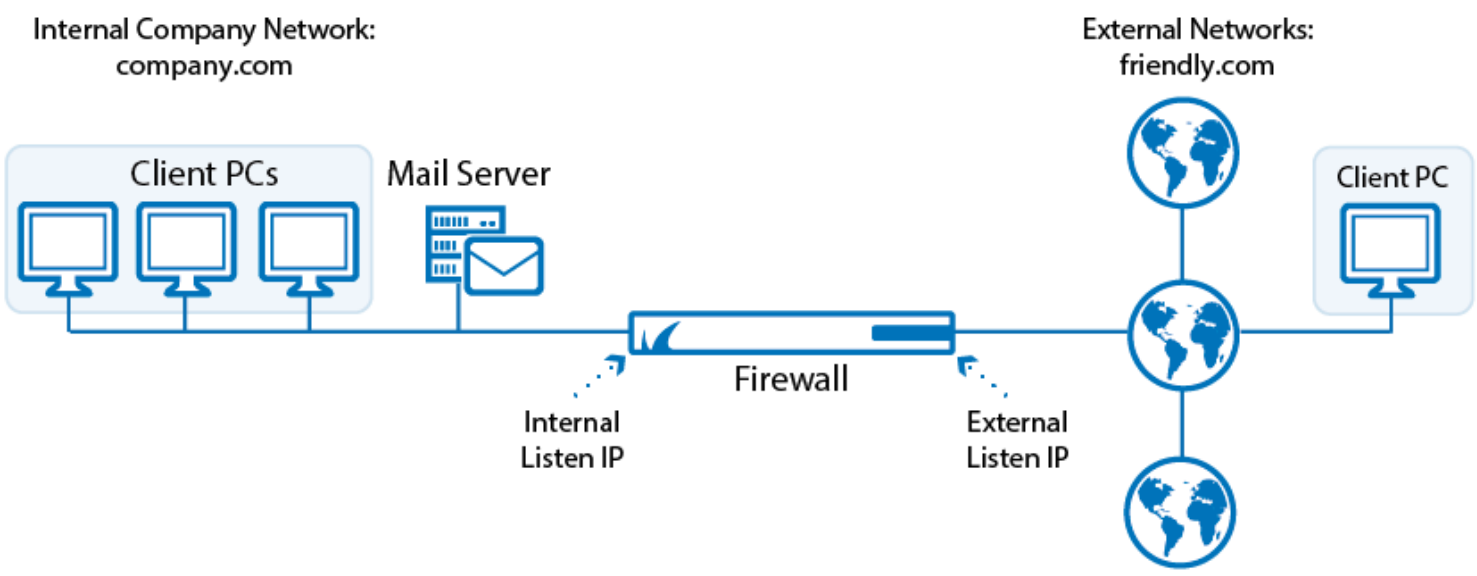
Port Mirror is a software-based tap, also called a Switch Port Analyzer, or SPAN in Cisco devices, is a special port on a managed switch configured to listen for all data going in and out of the switch. Unlike a network tap, port mirroing is convenient and easily changed to reflect any changes in your NIDS/NIPS monitoring stragegy.

Other types of Sensors and Collectors

- **Gather information from network devices**
  - Built-in sensors, separate devices
  - Integrated into switches, routers, servers, firewalls, etc
- **Sensors**
  - IPS
  - Firewall logs
  - Authentication logs,
  - Web server access logs, database transaction logs, email logs
- **Collectors**
  - Proprietary consoles IPS, Firewall, SIEM consoles, syslo servers
  - Many SIEMs include a correlation engine to compare diverse sensor data

Mail Gateways

- **Unsolicited email - stop it at the gateway before it reaches the user**
- Can be on-site or cloud-based

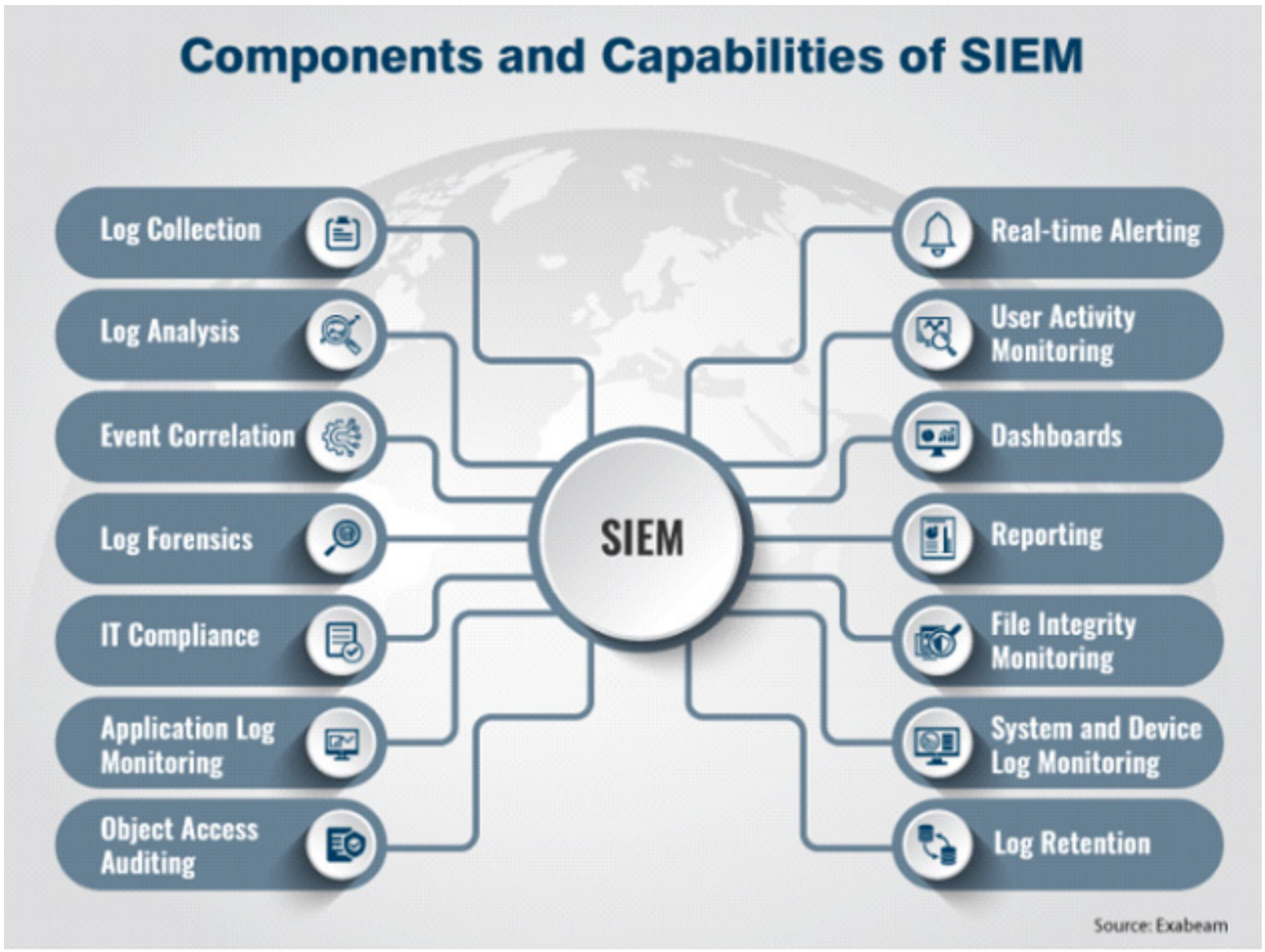


- **Email filtering - Inbound and outbound**
  - Unsolicited email advertisments
  - Control of phishing attempts
  - Anti-virus - blocking bad attachments
  - DLP - Data Loss Prevention - Block confidential information in emails
- **Another Features**:
  - Whitelisting (only receive email from trusted users)
  - SMTP standards cheking - Block anything doesn't follow RFC standards
  - rDNS - Reverse DNS - Block email where the sender's domain doesn't match the IP Address
  - Tarpitting - Intentionally slow down the server conversation
  - Encryption - can be required on the gateway based on policy; force encryptionS

SIEM - Security Information and Event

Management

SIEM tools aggregate and correlate data, allowing you to organize it into valuable information. You can get to the time sequence of an event in all the logs quickly, have alerts and the ability to notify you based on a configurable trigger.



- **Aggregation**: Collecting data from disparate sources and organizing the data into a single format. Any device within a SIEM system that collects data is called collector or an aggregator.
- **Correlation**: Is the logic that looks at data from disparate sources and can make determinations about events taking place on your network. (Could be in-band or out-of-band, depending on the placement of the NIDS/NIPS).
    - **Alerts** - For notification if something goes bad.
    - **Triggering** - Exceeding thresholds.
- **Normalization**: Will actually create multiple tables / organize in such a way that the data can become more efficient and allows our analysis and reports tools to work better.
- **WORM - Write Once Read Many**: The concept being is that log files are precious, and a lot of times you might want to look at them in an archival way, so that we can use optical media like WORM drives to store them.

Another SIEM features

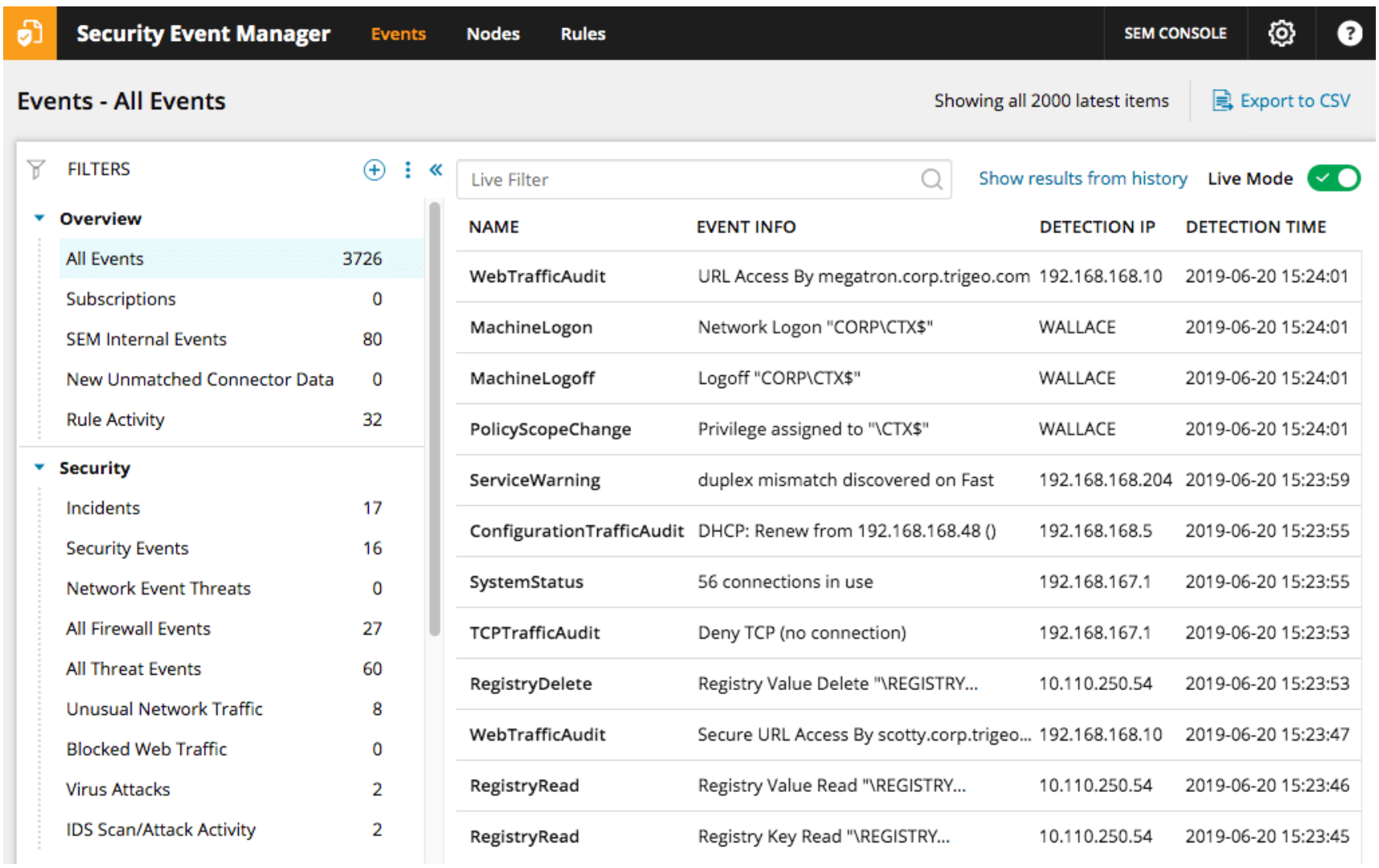
- **Time synchronization**:
    - Switches, routers, firewalls, servers, workstation has its own clock.
    - **Synchronizing the clocks becomes critical for Log Files, authentication information, outage details**.
    - Automatic update with **NTP (Network Time Protocol)**.
- **SYSLOG**:
    - Standard for message logging: Diverse systems, consolidated log
    - Usually a central loggin receiver: Integrated into the SIEM
    - Require a lot disk space
    - WORM drive technology
- **Event de-duplication**:

    - Preventing Event storms
    - Filter out the noise - focus on the real problems
    - Flapping (down / up / down)

- **Automated alerting and triggers**:
    - Constant information flow (important metrics in the incoming logs)
    - Track important statistics
    - Send alerts when problems are found *(email, text etc)*
    - Create triggers to automate responses *(e.g open a ticket, reboot a server)*

🛑 **SYSLOG stands for System Logging Protocol** and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review.

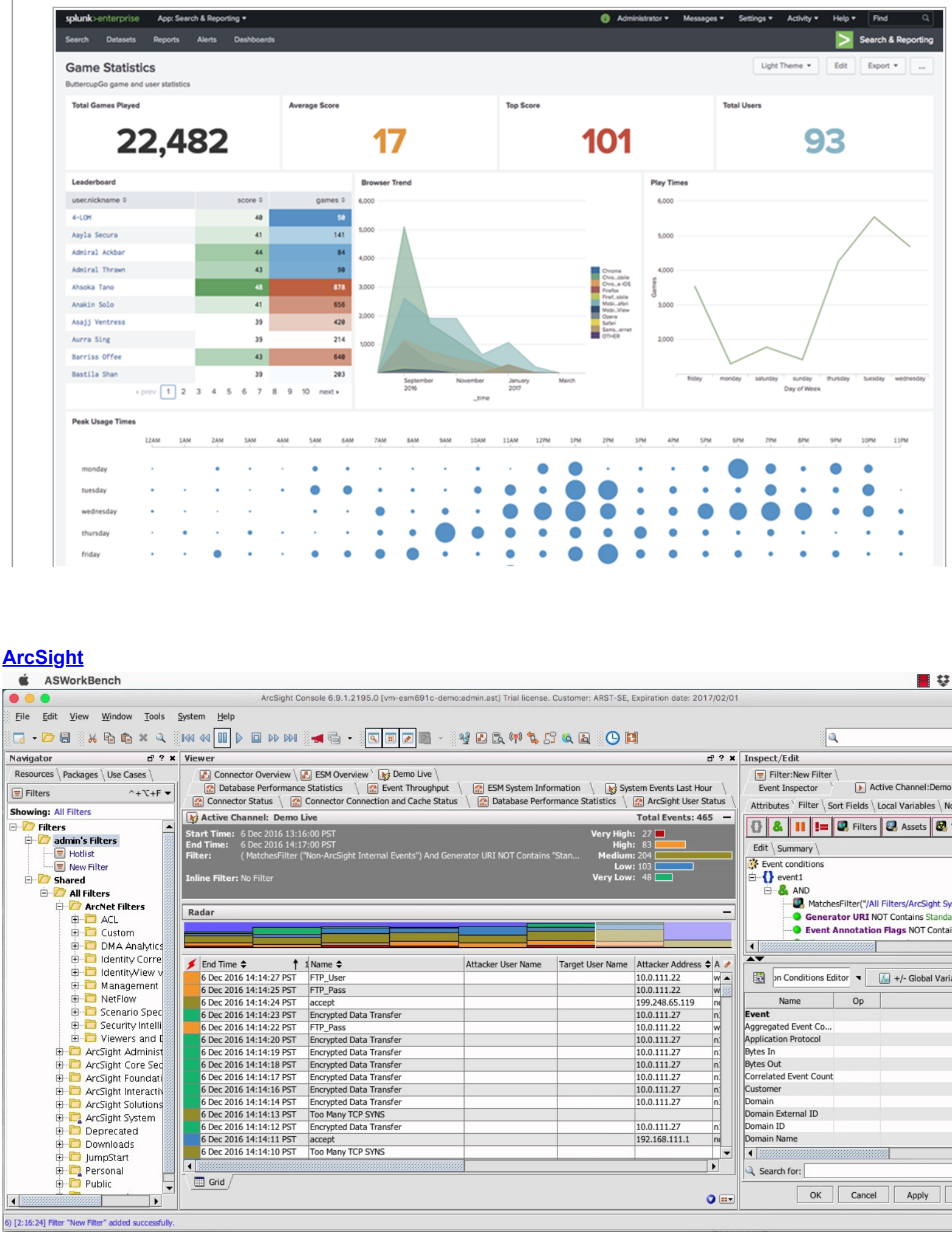
SIEM Logs Example



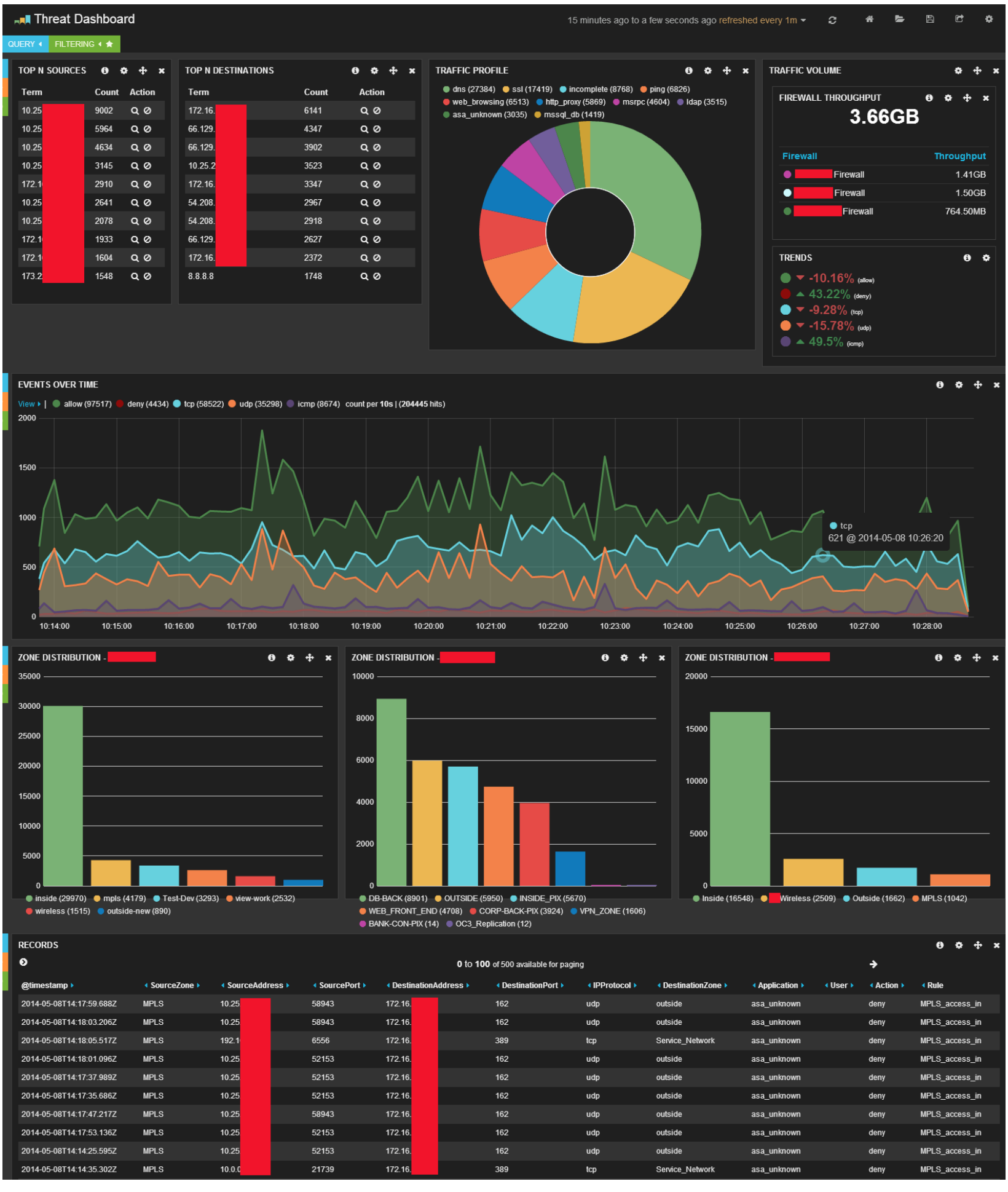
Most Popular SIEM Tools:

- **Splunk**

- [ArcSight]



- [ELK - Elastic Search, Log Stash and Kibana] **(Open Source)**



3. Networks and Infrastructure part 2 - Beyond the Basics

802.11

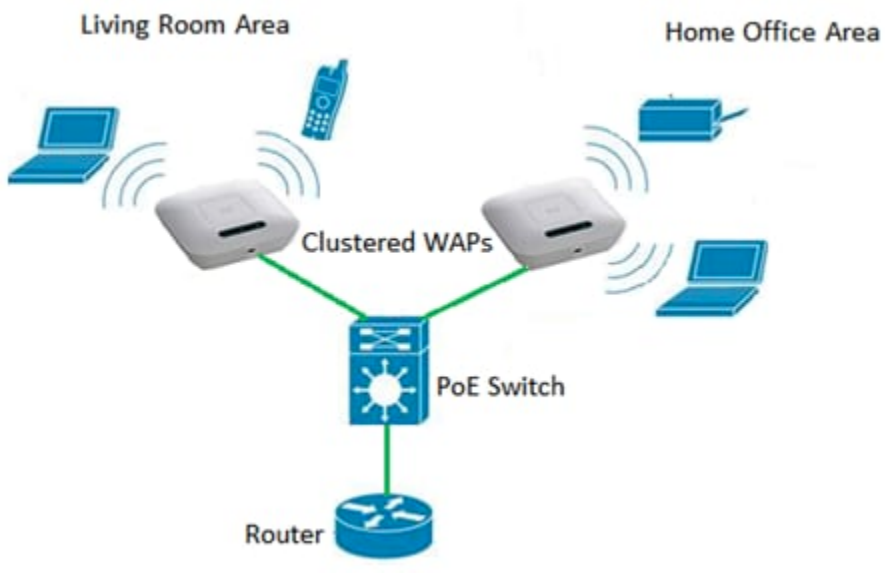
IEEE 802.11 is part of the IEEE 802 set of LAN protocols, and speci fies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) Wi-Fi computer communication in various frequencies, including but not limited to 2.4 GHz, 5 GHz, and 60 GHz frequency bands.

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

Wireless Access Point (WAP)

- Wireless Access Point is a Bridge between **802.11** and **Ethernet**.
- Every WAP have MAC address.
- **SSID (Service Set identifier)** associated to the MAC address on a WAP is known as **BSSID - (Basic Service Set Identifier)**
- When a large network is connected multiple WAP's through a **Common Ethernet Broadcast Domain** - turns out **ESSID - (Extended Service Set Identifier)**
- MAC Filtering - limit access through the physical hardware address.



🛑 **WAP is a bridge** - extends the wired network on the wireless network (operates on OSI Layer 2 - data link)

🛑 **Not a wireless router!** A wireless router is a router and a WAP in a single device.

🛑 Security Through Obscurity:

- **Enabling MAC Filtering don't provide security** - the addresses can easily spoofed.
- **Disabling SSID broadcasting don't provide security** - is easily determined through wireless network analysis.

Wireless LAN (WLAN) Controllers

- **Controlling Multiple Access Points**
- Centralized management

- Deploy new access points
- Performance and security monitoring
- Configure and deploy changes to all sites
- Report on access point use
- Usually a proprietary system
    - The wireless controlled is paired with the access points
- **LWAPP**
    - **Lightweight Access Point Protocol** - is a protocol that can control multiple Wi-Fi wireless access points at once.
    - Cisco proprietary - CAPWAP, based on LWAPP
    - Manage multiple access points simultaneously

Fat/Thick Access Point

- Thick/Fat access points
    - The access point handles most wireless tasks
    - The switch is not wireless-aware
- **Good for small environments**
- Management console to configure security controls
- ACLs
- White/black listing
- Encryption
- Manage individually
- Also called controller-based AP

Thin Access Point

- Just enough to be 802.11 wireless
- The intelligence is in the switch
- Less expensive

- **Good for big environments.** *(e.g A building with multiple floors and hundreds of users might rely on one good switch (with a redundant backup) to control dozens of thin access points)*
- **Act as a repeater** taking the wireless signal and pushing it ot a managed access control (AC) switch that handles encryption and other security. Also called **Standalone AP**

Vulnerabilities with Wireless Access Points

Rogue Access Point

- **Unauthorized** access point plugged into a wired one. *(Can be accidental)*

Evil Twin Attack

- Is a Rogue AP tha is broadcasting **the same (or very similar) SSID**.

802.11 Jammer

- **Jamming is a form of intentional interference on wireless networks, designed as a DoS attack**. This type of attack by overpowering the signals of a legitimate wireless AP, typically using a rogue AP with its transmit power set to very high levels.

Deauthentication / Disassociation Attack

- Deauth Attack Is a type of denial-of-service attack that targets communication between a **user** and a **Wi-Fi wireless access point**.

Technical details: The IEEE 802.11 (Wi-Fi) protocol contains the provision for a deauthentication frame. Sending the frame from the access point to a station is called a "sanctioned technique to inform a rogue station that they have been disconnected from the network".

Cracking WEP, WPA, WPA2 and WPS ⚔️

WEP

- **IV Attack** - Initialization Vector is vulnerable to cracking.
    - Aircrack can grab WEP keys and crack them.
- WEP is the **oldest security standard 802.11**

WPA/WPA2

- WPA/WPA2 uses 4-way handshake
- WPA is vulnerable to a dictionary attack
- Can be cracked at the initial connection between the WPA/WPA2 client and the access point during the 4-way handshake
- Aircrack can grab WPA handshakes on authentication time and crack the PSK's (if they are common/weak).

WPS

Wi-Fi Protected Setup (WPS) - is a push button configuration, which enables the router WPS enable to another WPS device (wireless printers are the most common).

- 8 digit key is actually only 7 digits, 2^7
- Key exchange is the first processed in 4-bit and 3-bit
- Can be cracked using Reaver or Brute forcing
    - The WPS validates each half of the PIN
    - First half, 4 digits. Second half, 3 digits.
    - First half, 10,000 possibilities. Second half, 1,000 possibilities
    - It takes about for hours to go through all of them
- *The new generation of WPS enabled device can detect an attack and shut off.*
- **WPS Attack Prevention**:
    - Get rid of older routers
    - Firmware updates
    - Upgrade to newer wireless routers

Hardening 802.11 Networks

- Survey installation issues
- Maintaining existing wireless networks
- Monitoring
- Define how to defend wireless clients

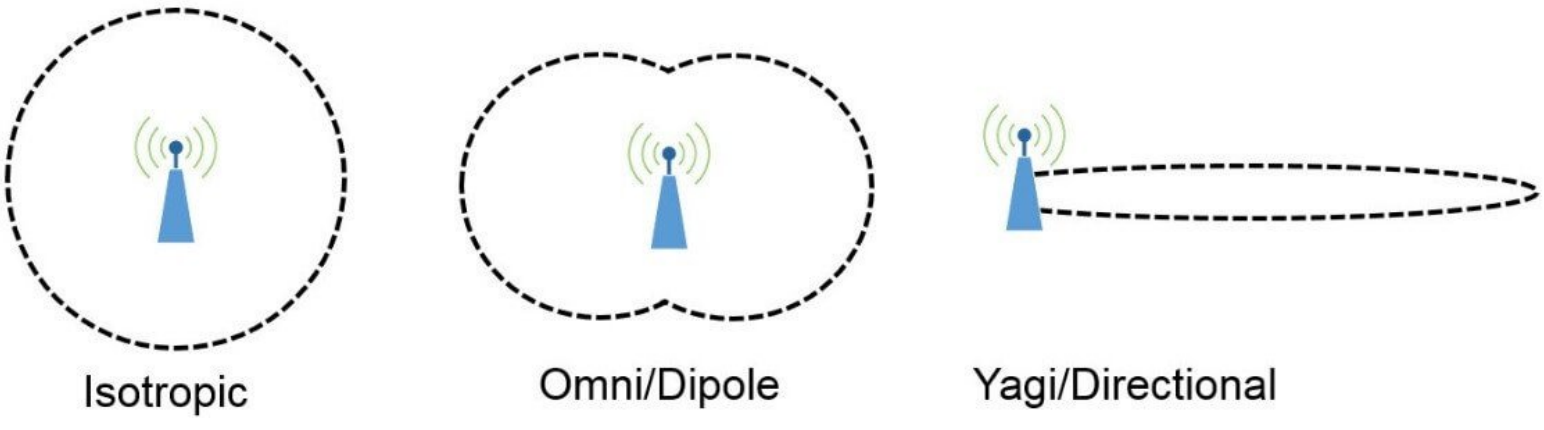
Site Survey & Installation

- **Survey Tools**
    - Find SSIDs
    - Find MAC addresses
    - Band, channels, and signals
    - Document everything around 802.11 device
- **Maintanance Wireless Networks**
    - Good Documentation
        - SSIDs
        - MAC addresses associated to
            - WAPS
            - AP locations
            - Heatmaps
    - **Scanning**
- **WIDS** - Wireless Intrusion Detection System - *listen to what is going on inside the wireless network and help detect potential threats, or any abnormality.*
    - Monitors wireless radios
    - Watches for rogue access points
    - Knows MAC address of authorized equipment
    - Watches working protocols
- *Good Practice:*
    - AP isolation enabled
    - 802.1X is more robust

Antenna Types

The most commonly used wireless antenna on both WAPs and wireless devices is an omnidirectional (or omni) antenna. Omnidirectional antennas transmit and receive signals in all directions at the same time. This allows wireless devices to connect to a WAP from any direction.

Another type of antenna is a directional antenna. A directional antenna transmits in a single direction and receives signals back from the same direction. Because the power of the antenna is focused in a single direction, the directional antenna has greater gain than an omni antenna, and it can transmit and receive signals over greater distances.



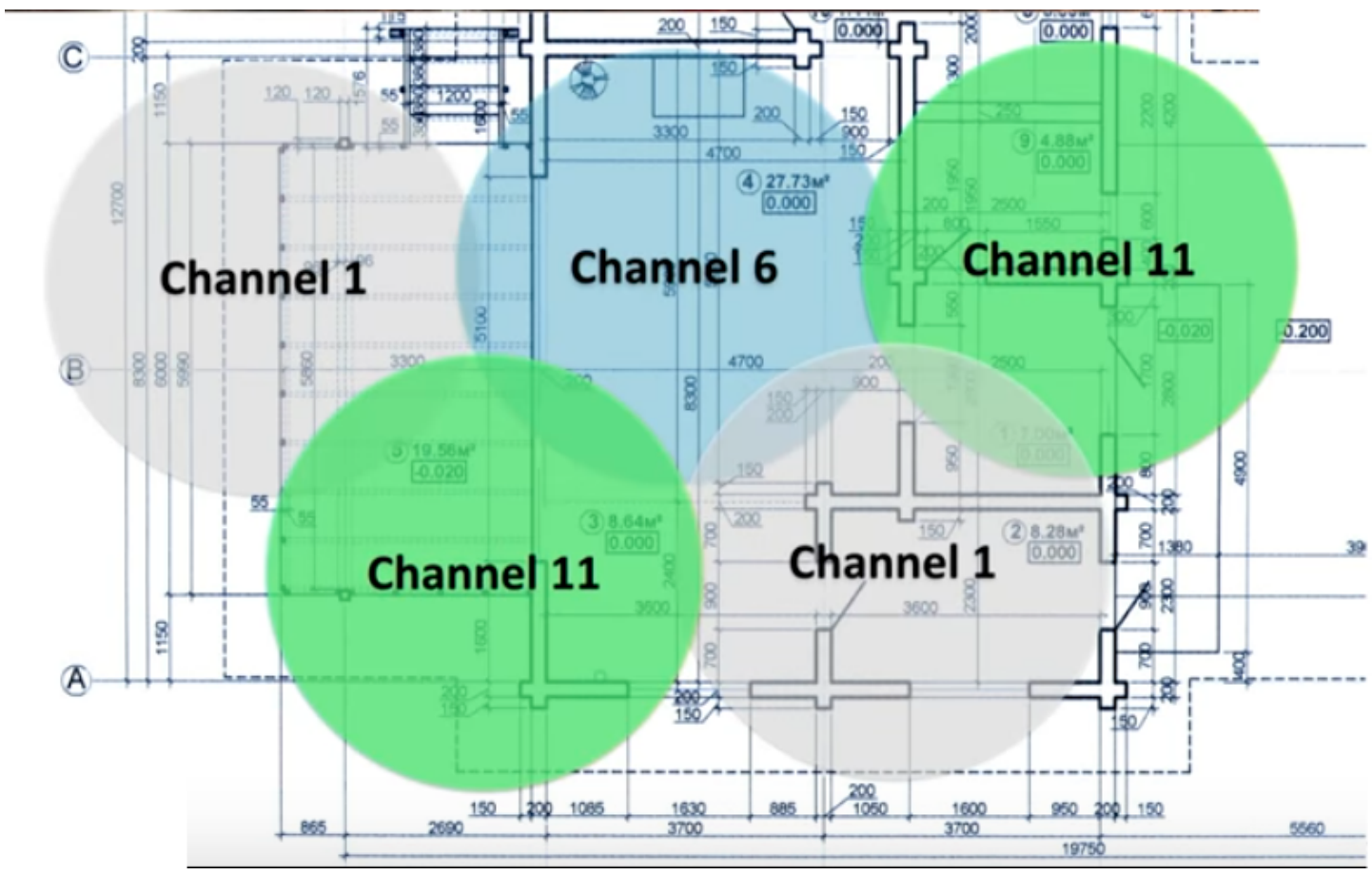
- **Omnidirectional**
  - Signals goes on every direction.
- **Dipole**
- **Directional**
  - Long individual beam, increased distances.
  - **Yagi antenna**
    - Very directional and high gain.
  - **Parabolic antenna**
    - Focus the signal to a single point.
- **Patch Graphic**
  - Half Omni (e.g stick to the wall the get one side signals).

Antenna Placement Examples

Antennas should be centrally located throughout different areas of the facility so that hey can adequately span all areas of coverage within a facility, without being too close to exterior walls or the roof whenever possible.

- Stadium like = **Omnidirectional Antenna**
- Outdoors = **Dipole Antenna**
- Shooting long distances *(one building to another)* = **Directional Antenna**

Example on 2.4 GHz Frequency Ranges

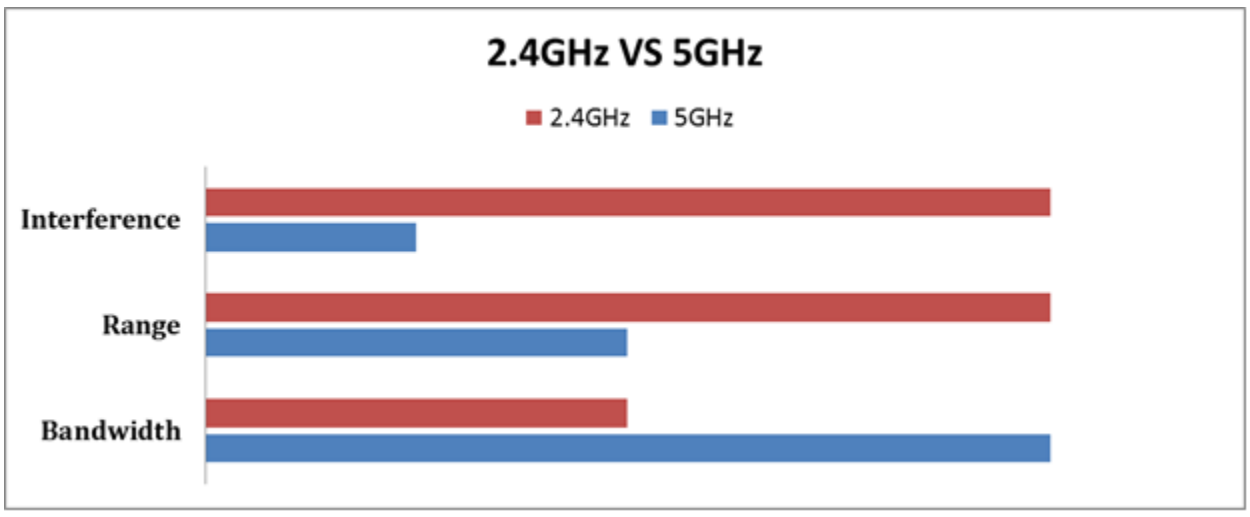


- Make sure to have multiple access points that were not overlapping any of the frequencies
- **On 2.4 GHz frquency ranges to avoid one overlaps each other.**
  - Channel 1

- Channel 6
- Channel 11

Band Selection - 2.4 vs 5 GHz

The higher the frequency of a wireless signal, the shorter its range. **2.4 GHz wireless networks, therefore, cover a larger range than 5 GHz networks. In particular, signals of 5 GHz frequencies do not penetrate solid objects as well as 2.4 GHz signals, and this limits the reach of 5 GHz frequencies inside homes.**



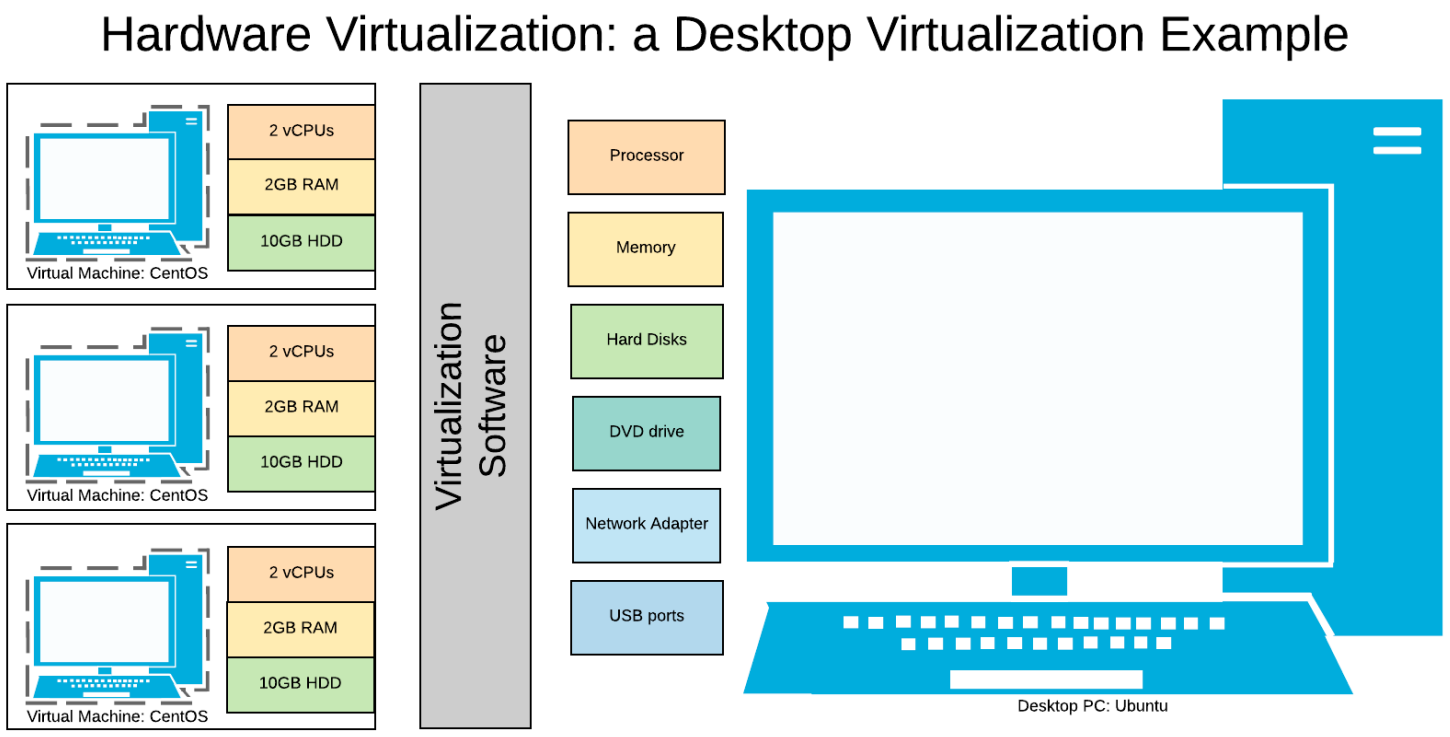
2.4 GHz

- Longer range
- Penetrate walls easily

5 GHz

- Faster choice
- Automated channels
- Wider Channels = better

Virtualization



- Virtual version of host hardware
- Separate OS, independent CPU, memory, network, etc

- Multiple virtual servers on one box/physical device
- Hardware consolidation and reduced energy consumption
- System Recovery

Hypervisor

- Virtual Machine Manager
  - Manages the virtual platform and guest OS
- Hardware management (CPU, Networking, Security etc)

Types of Hypervisors

- **Type II**
  - Runs on top of host OS (Windows, Linux, Mac, etc)
- **Type I**
  - Runs directly on top of hardware, independent of host OS. *(e.g bootable Linux thumbdrive)*
  - Bare metal, embedded, native
- **Application containerization**
  - Run an application without launching an entire VM
  - Uses just the right resources for the application
  - Everything you need to run the app is in the image (container/cell)
- **Cloud-based Virtualization**
  - IaaS (e.g. AWS, MS Azure)

Virtualization Benefits

- Security Feature
- Patch management
- Centralized hardware maintenance
- Resilient and high availability
- Great for testing everything and sandboxing environment
- Snapshots and backups
- Network Separation

Virtual Threats

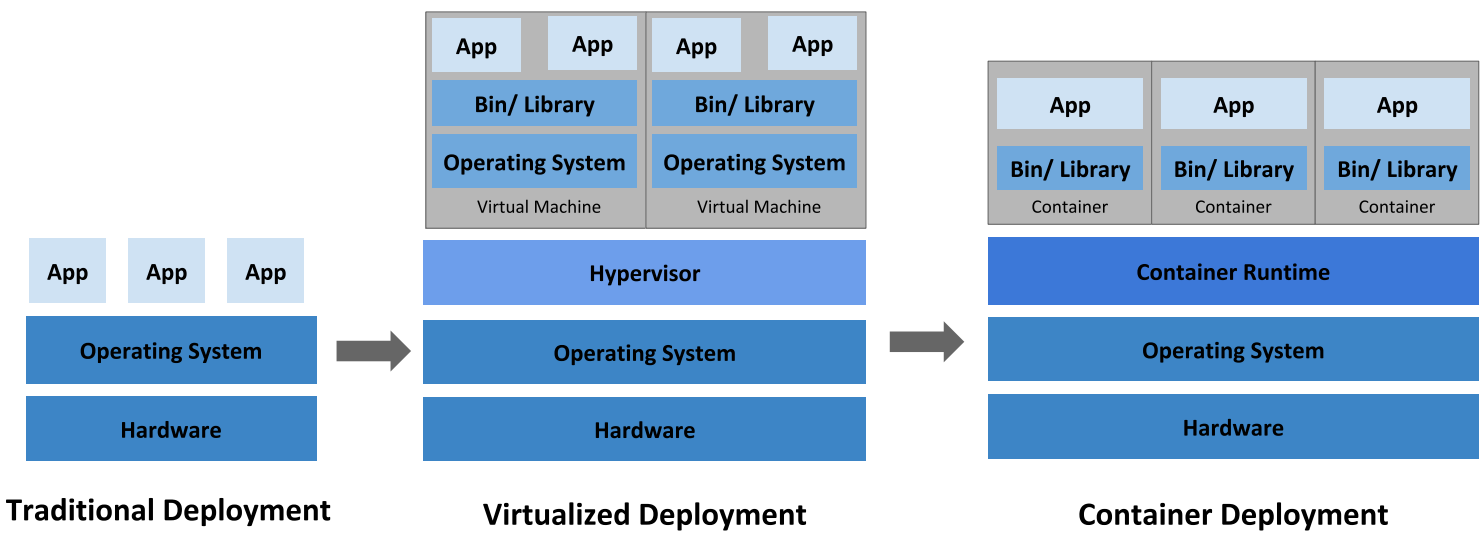
- **VM sprawl** - the out-of-control creation of VMs outside of security controls.
  - It becomes almost too easy to build instances
  - The virtual machines are sprawled everywhere in which become extremely difficult to deprovision
  - The correct way to deploy many instances is through a formal process and detailed documentation
    - You should have information on every virtual object
- **VM escape** - when a user inside a VM finds a way to break out the VM and get into the underlying hypervisor/host OS.

Virtualization Hardening

- Remove remnant data
- Make good policies
- Define user privileges
- Patch everything!
- **CASB - Cloud Access Security Brokers:** Intermediary between your infrastructure(in-house stuff) and the cloud; Make sure policies are controlled; watches for malware;
  - Visibility - determine what apps are in use; are they authorized to use the apps?
  - Compliance - are users complying with HIPAA, PCI?

- Threat prevention - allow access by authorized users, prevent attacks
- Data security - ensure that all data transfers are encrypted; Protect the transfer of PII with DLP

Containers



- Containers are self-contained applications that can communicate with network resources that have been explicity allowed
- Runs isolated instances of programs and services
- Can depend on each other, and can be configured to communicate with each other on a single host
- Runs a single program and all its dependencies, when the programs exists

IaaS - Infrastructure-as-a-Service

- Basically virtual machines hosted by a cloud provider's infrastructure; Users simply connect to them via RDP (remote desktop protocol) or another secure remote connection protocol and use the as they would any other computer.
  - **e.g: AWS, Microsoft Azure, Digital Ocean, Google Cloud.**

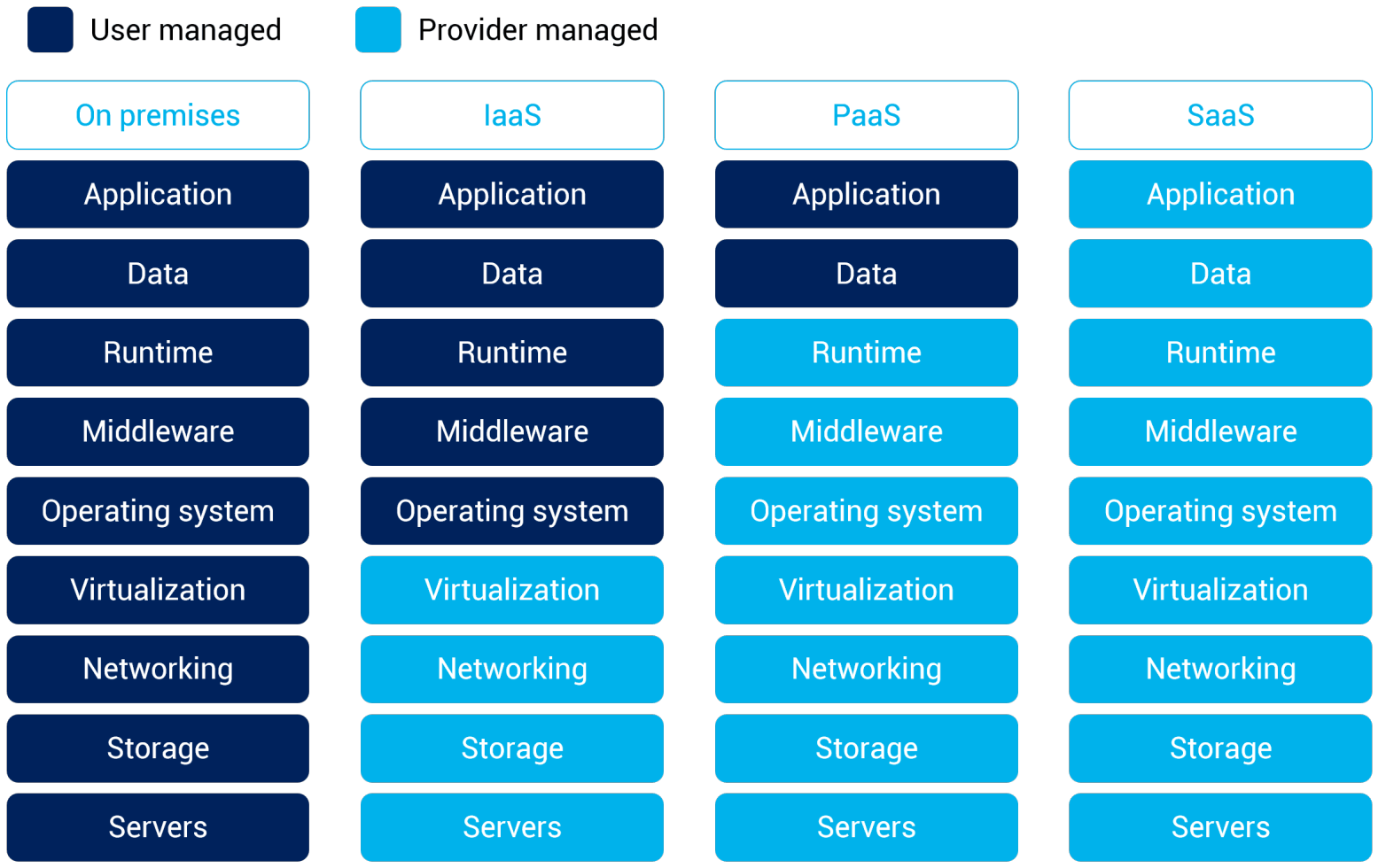
PaaS - Platform-as-a-Service

- Offers a computing platform, such as Web application server or database server with easy setup focusing on quick deployment; Enables you to access a software development platform without the need to host it yourself.
  - **e.g: Heroku, SalesForce**.

SaaS - Software-as-a-Service

- SaaS is a subscription based license; Access applications via subscription;
  - **e.g: Microsoft Office 365, Dropbox storage, Google Docs**.

IaaS | PaaS | SaaS



- **On-premise**: Your application are on local hardware; Your servers are in your data center in your building

Cloud Deployment Models

- **Private Cloud**
  - A group of virtual machines that only the organization can access.
- **Public Cloud**
  - Amazon S3, Microsoft Azure - Open for business
- **Community Cloud**
  - Is make up of infrastructure from several different entitites wich may be cloud providers, business partners, and so on. (members only type of thing)
- **Hybrid Cloud**
  - Any combination of the cloud models described above
- **Virtual Desktop Environment (VDE)**
  - Remote Access to a Remote System that **is not virtualised**

Security in the Cloud

- **Virtual Desktop Integration (VDI)**
  - The actual virtualized environment in the cloud
  - Enhanced security
    - Centralized and easier to manage
    - Changes can be easily controlled
    - The data never leaves the data center

Security as a Service (SECaaS)

- Instead of managing your own security solution, move it to the cloud
  - Pay of what you use
  - Scale up and down as needed
- Continuously monitoring
  - Uniformly applies to all traffic
- Anti-virus/anti-malware signatures are constantly udpated
  - Block emerging threats without deploying updates

Embedded Systems - Static Hosts

IoT (Internet of Things):

- **Wearable technology**
  - Watches, health monitors, glasses
  - Track our location
  - Where is that data and how is it stored?

- **Home automation**
    - Video doorbells (e.g Ring-Bot device)
    - Internet-connected garage door openers
    - It knows when you are home (and when you aren't)

HVAC - Heating, Ventilating, and Air Conditioning

- Thermodynamics, fluid mechanics, and heat transfer
- Very complex system
    - Must be integrated into the fire system
- Workstation manages equipment
    - Makes cooling and heating decisions for workspaces and data centers
- Traditionally not built with security in mind
    - Very hard to recover from a infrastructure DoS

SCADA | ICS:

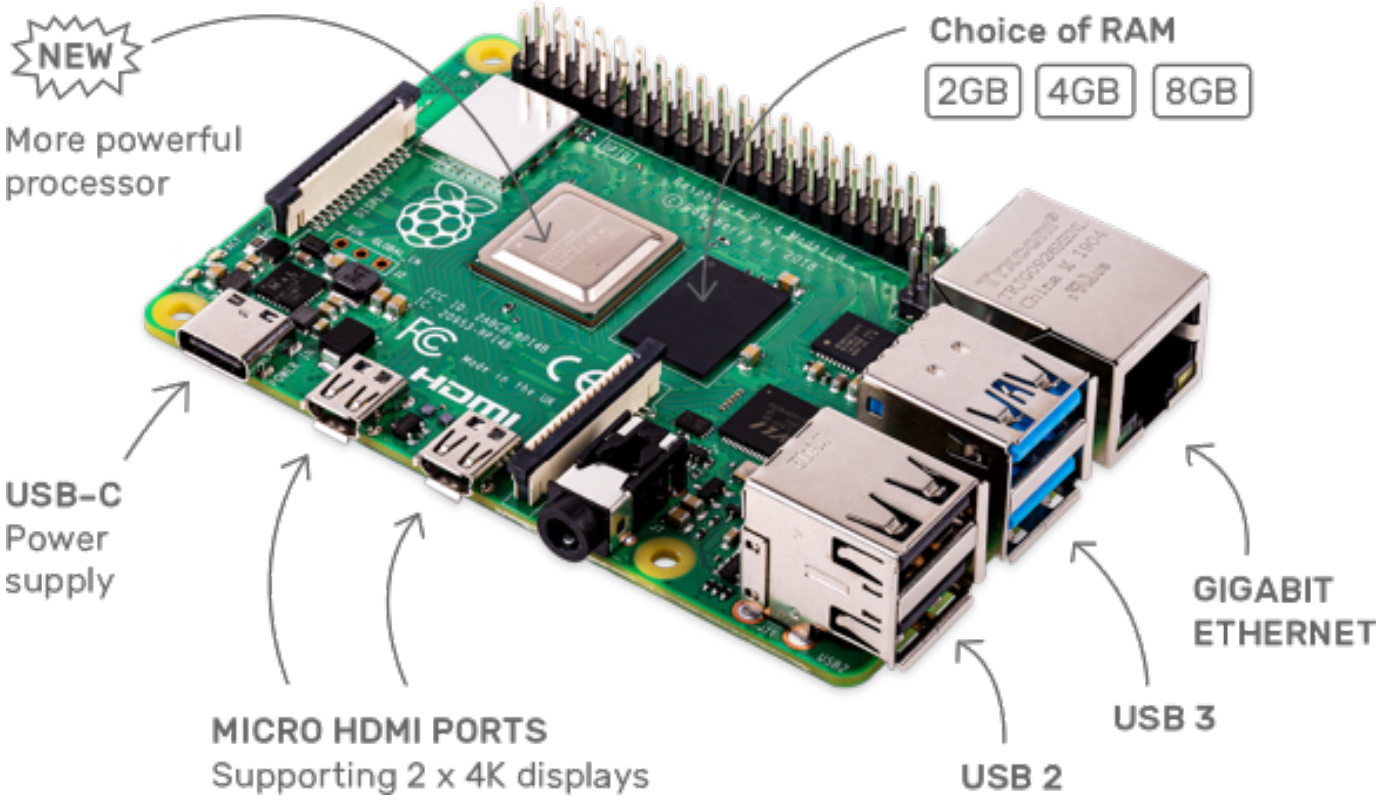
- **SCADA** - Supervisory Control and Data Acquisition
    - Pretty much ICS with more funcionality
- **ICS** - Industrial Control Systems
    - HVAC - Heating Ventilation, and Air Conditioning

- Distributed control systems
    - Real-time information
    - System control
- Requires extensive segmentation
    - No access from the outside

SoC - System on a Chip

- Multiple components running on a single chip
    - Common with embedded systems
- Small form-factor

- External interface support
- Cache memory, flash memory
- Usually lower power consumption



As shown above, you can see the Raspberry Pi 4 and the chip (Broadcom processor) controlling every interface on the device (HDMI ports, Ethernet, etc)

- Security considerations are important
  - Difficult to upgrade hardware
  - Limited off-the-shelf security options

Printers, Scanners and Fax machines

- All-in-one or multifunction devices (MFD)
  - Everything you need in one single device
- Printers have a very sophisticated firmware
- Some images are stored locally on the device
  - Can be retrieved externally
- Logs are stored on the device
  - Contain communication and fax details

Camera systems

- Video monitoring for home or office
- Video recorders and Cameras are IP devices
  - Authenticate using a specialized application
- Privacy concerns

Another Devices (Special purpose)

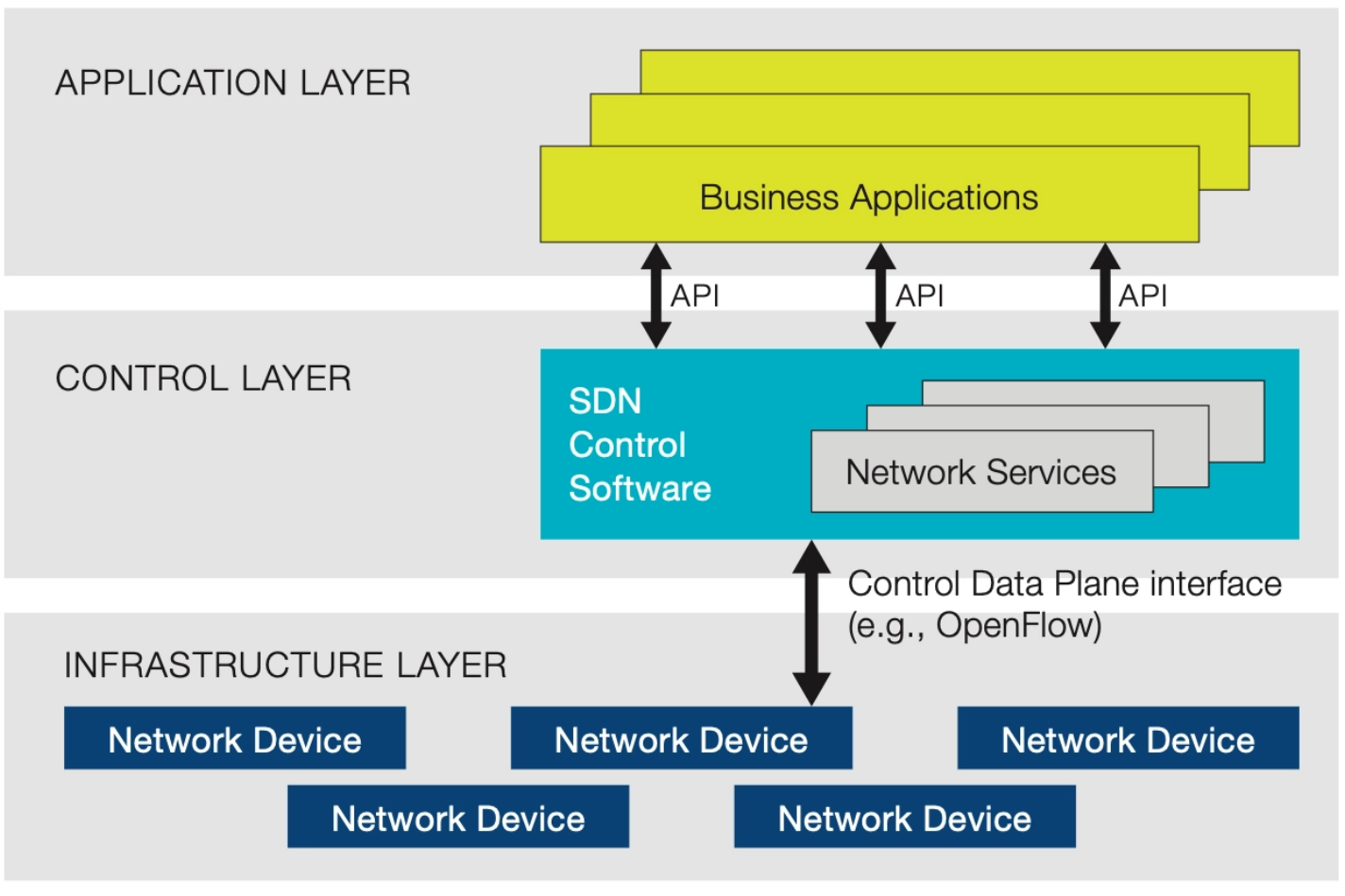
- Medical devices
  - Heart monitors, insulin pumps
  - Often use older OS
- Vehicles
  - Internal network is often accessible from mobile networks
  - Control internal electronics
  - Disable the engine
- Aircraft / UAV (Unmanned aerial vehicle)
  - DoS could damage the aircraft and other on the ground

Securing Static Hosts

- Change default passwords
- Turn off unnecessary services
- Monitoring security and firmware updates
- **Defense in depth**
    - Network Segmentation - VLANs with Firewalls; VPN to connect a pipeline securely.

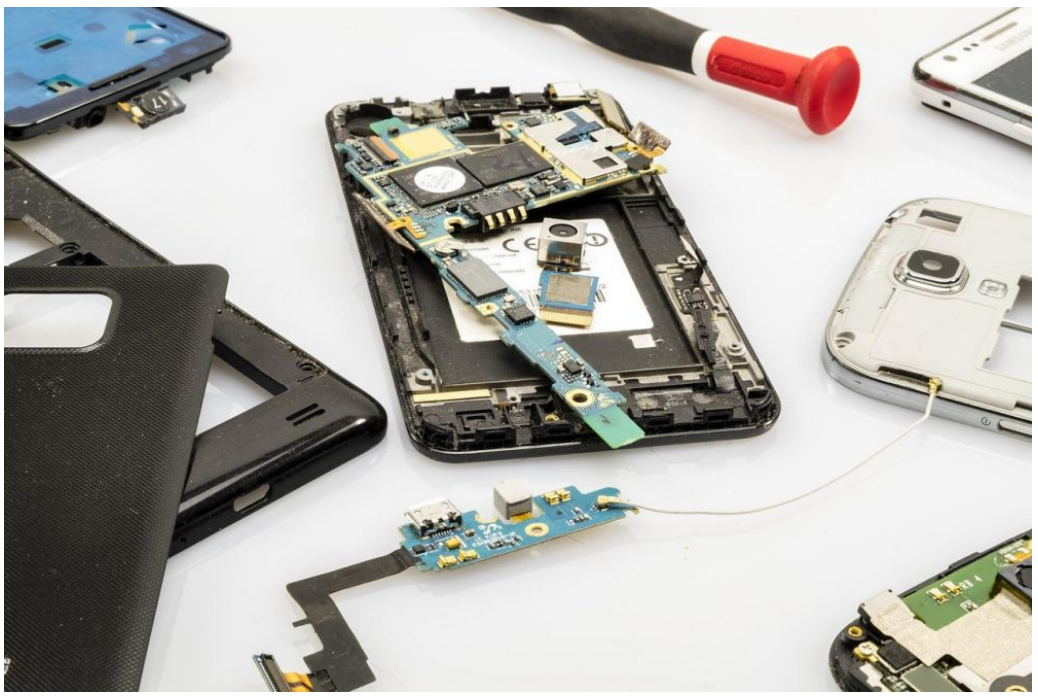
SDN - Software Defined Networking

Technology that separates the **control plane** management of network devices from the underlying **data plane** that forwards network traffic.



- Directly programmable
    - Configuration is different than forwarding
- Agile
    - Changes can be made dynamically
- Centrally managed
    - Global view, single pane of glass
- Programmatically configured
    - Orchestration without human intervention
- Open standards / vendor neutral
    - Standard interface to the network

Mobile Connectivity



- **SATCOM** - Sattelite communication phone
- **Bluetooth**
- **Wi-Fi** and **Tethering**
    - ADHOC, Wi-Fi Direct (Easy connection)
    - Tethering - Wired and Wireless Tethering: acts like a router
- **NFC** - Near Field Communication: Almost/Physical contact with another device *(there's no security envolved when activated)* - Easy connection
- **ANT/ANT+** - Very simple form of wireless communication; slow and protected; (e.g Odometers, Heart Rate Monitors, Bikes)
- **Infrared (IR)** - Most Androids, communication Transmitter.
- **USB**, USB OTG (On-the-Go)

Mobile Enforcement

Set of policies to make sure what people are able to do on mobile devices.

Sideloading

- Installation of third-party applications that is different from original Application Store (Google Play, Apple Store)

Carrier Unlocking

- Security revolves around connectivity - Moving to another carrier can circumvent the MDM

Rooting/Jailbreaking

- Root Access
    - Install custom firmware
- Root Access Issues
    - Auto updates disabled
    - Trouble accessing the store
    - Exposure to malware

Things to AVOID on Mobile 🚫

*To achieve this topics you will need a **good policy**.*

- **Firmware OTA updates** *(over-the-air) - turn off*
    - Significant changes without connecting the device
    - This may not be a good thing - the MDM can manage what OTA updated are allowed
- **Camera use**
    - Can be use to take pictures of confidential information etc.
- **SMS/MMS** - *Control of data can be a concern*
    - Outbound data leaks, financial disclosures
    - Inbound notifications, phising and smishing attempts
- **External Media**
    - Limit data written to removable drives or prevent the use of them from the MDM
- **USB OTG** - *USB On-The-Go*
- **Recording Microphone** - *Audio recordings*
    - A legal liability - every state and country has different laws.
    - Disable or geo-fence - manage from the MDM
- **GPS tagging** - *Location services*
    - Every document may contain geotagged information on metadata (Longitutde, latitude embed on photos, videos, etc)
    - This may cause security concerns
- **Payment Methods** - *Sends small amounts of data wirelessly over a limited area (NFC); Apple Pay, Android Pay, Samsung Pay etc*
    - Bypassing primary authetication would allow payment
- **Wi-Fi Direct / AD HOC** - *Connect wireless devices directly without an access point*
    - Simplicity can aid vulnerabilities - Invisible access to important devices
- **Hotspot / tethering** - *Turn your phone into a WiFi Hotspot*
    - May provide inadvertent access to an internal network

Mobile Device Management - MDM

- **Content Management**
    - Applications Management
    - Databases
    - Documents
- **Geolocation**
    - Knows the location of that device
- **Geofencing**
    - Geolocation with geographic trigger
        - Restrict or allow features when the device is in a particular area
        - e.g - Camera might only work when outside the office
        - e.g - Only allow logins when the device is located in a particular area
- **Push notification services**
    - Applications will push notifications if you want
- **Passwords and PINs**
    - Require use of passwords and PINs
    - Can recover passwords
- **Biometrics**
    - Fingerprints
    - Facial Recognition
    - Vocal Recongnition
    - Can lock and unlock devices
    - Use to configure applications
- **Screen Locks**
    - Make sure your screen is locked
- **Remote Wipe**
    - Great when the device is lost

Mobile Application Management - MAM

- Versioning
- Updates
- Patches
- Context-aware authentication
    - Where are they right know?
    - What OS are they using?
    - What time/day are they trying to authenticate?
- Storage segmentation
    - Dedicating a storage space for our applications
- Full Device Encryption
    - Encrypt the entire storage of the device

🛑 *Some companies provides **MDM solutions** (e.g Google - Android: What applications people can install, security policies and so on)*

Mobile Device Deployment Models

Any device connected to an organization's network represents a potential risk. As a simple example, if someone connects an infected device to a network, it might be able to infect other devices on the network. To limit this risk, organizations take steps to monitor and manage mobile devices.

	COPE	CYO	BYO
Cost	Company	Company/Employee	Company/Employee
Admin	Company	Company/Employee	Employee
Support	Company	Company/Employee	Employee
Security	Company	Company	Employee
Software	Company	Company/Employee	Company/Employee
Replacement (warranty)	Company	Company	Employee
Device compatibility	Company	Company	Employee
Management/Maintenance	Company	Company/Employee	Employee
Standards	Company	Company	Employee
Application	Company	Employee	Employee

1. COBO

Corporate Owned, Business Only

- Company owned
- Company devices what to do with that device
- What applications are on that device
- Very specific security requirements
- The device is not for personal use
- What encryption is used?
- What wireless is connected?

2. COPE

Corporate Owned, Personally Enabled

- Company buys the device
- Used as both a Corporate device and Personal Device

- Everyone has the same device
- Great control because everyone has same device on environment
- People will still want to use their own devices
- Learning curve

3. CYOD

Choose Your Own Device

- Similar to COPE, but with the user's choice of device
- Users get to choose from a list af approved devices
- Less of learning curve

4. BYOD

Bring Your Own Device

- User get to choose to bring their own devices, based on their experiences
- Difficult to secure
- Learning curve is decreased
- Very heavy device management
- Mobile application management

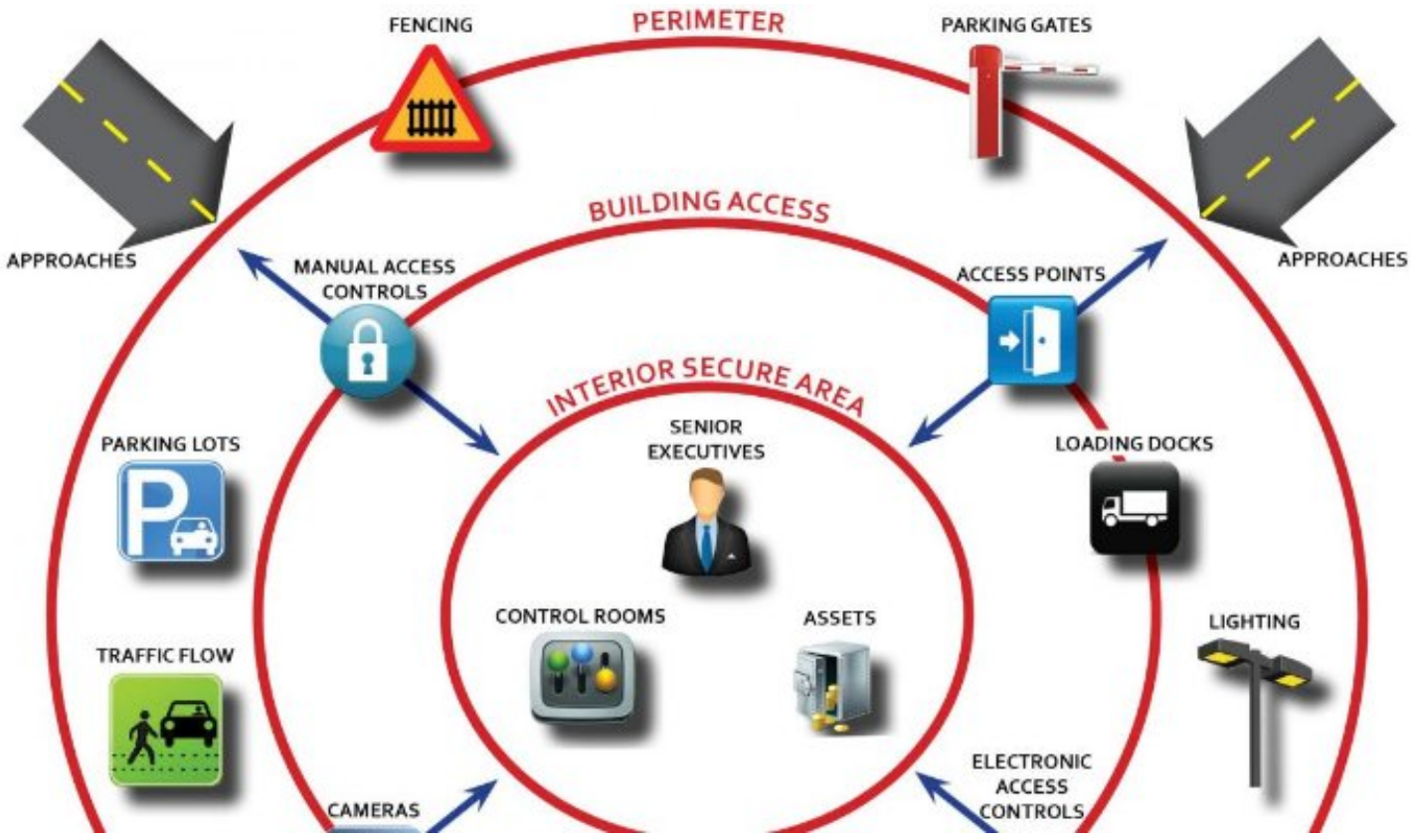
5. VDI / VMI

Virtual Desktop Infrastructure / Virtual Mobile Infrastructure

VDIs host a user's desktop operating system on a server; it's also possible to deploy a VDI that users can access with their mobile device. This allows users to access any applications installed on their desktop. When the organization hosts a remote access solution such as a virtual private network (VPN), users can access the mobile VDI from anywhere if they have Internet access.

- The apps are separated from the mobile device
- The data is separated from the mobile device
- Data is stored securely, centralized
- Physical device loss - Risk is minimized
- Centralized app development
  - Write for a single VMI platform

Physical Controls



Deterrent Physical Controls

- Outside light, Parking Lot Lighting
- Signage (e.g Restricted Area)
- Security Guards

Preventive Physical Controls

- **External**
    - Fences, Gates, Barricades, K ratings(designed to stop vehicles)
    - Mantraps (some type of entry system, consisting of 2 doors)
    - Cabling systems
        - Airgap
            - Physical separation between networks
        - Protected Distribution System (PDS)
            - Protect your cables and fibers to prevent direct and inductive taps
- **Internal**
    - Safe - for important documents
    - Locked cabinets
    - Faraday cages - block eletromagnetic fields to protect sensitive electronic equipment
    - Locks
        - Key management system (where the keys are stored? who is in possession of those keys?...)
- Individual Workstation
    - Cable Locks
    - Screen filters

Detective Physical Controls

- Alarms
- Cameras
- Motion detectors
- Infrared detectors
- Log Files - can be important in terms of tracking
    - Caben be physical or digital
    - e.g - *Entering the parking area; Identification upon entering the building; Badge assignment tracks door*

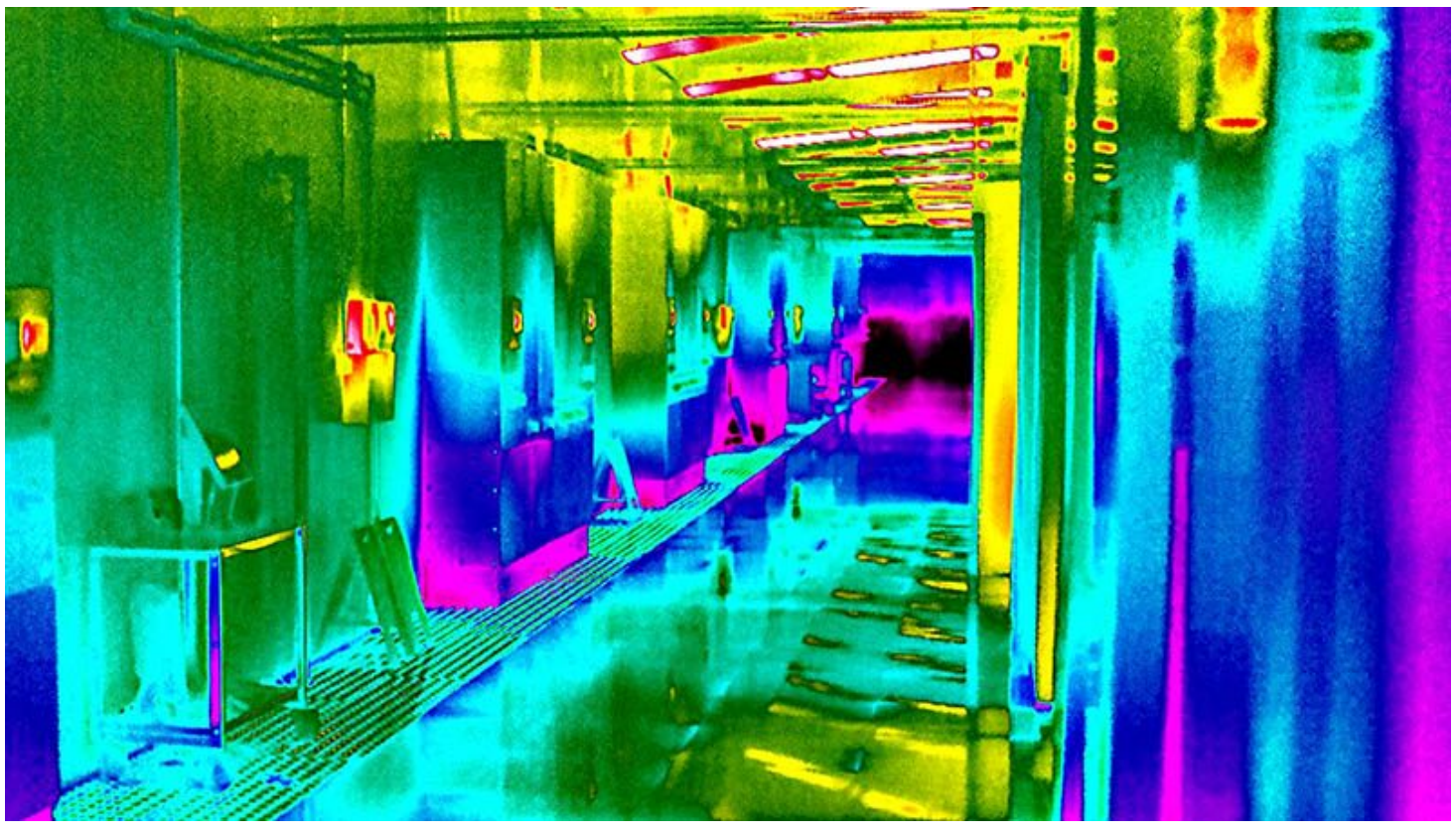
operation

Compensating & Corrective Physical Control

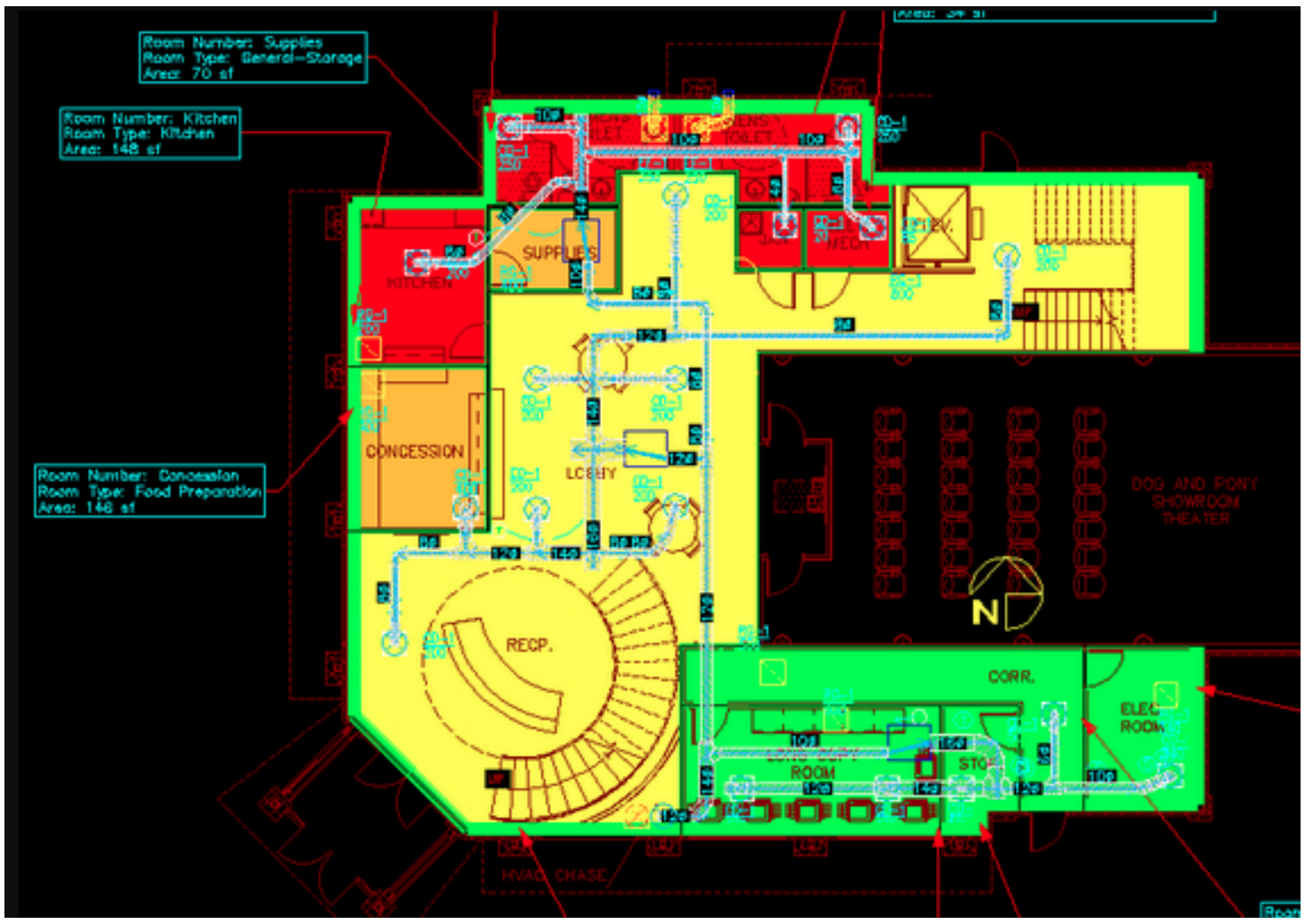
Temporary fixes when these controls are weakened.
e.g - If the outside fence in some way got a big hole, you need to place a security guard on that location until the fences got fixed.

HVAC - Heating, Ventilation, and Air Conditioning

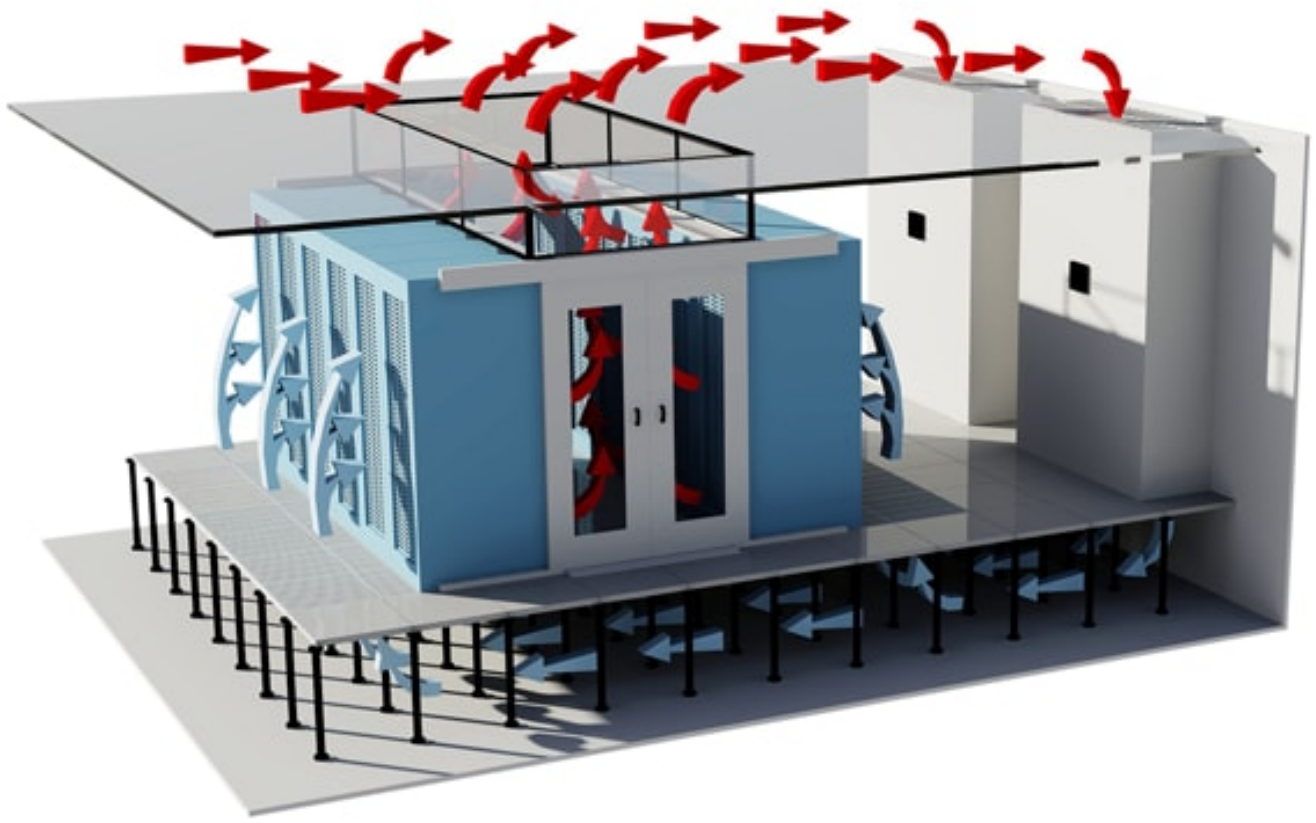
- Office Environment - room temperature, humidity
- Server Rooms - Super sophisticated HVAC's systems; Make sure keep cool and dry
- **Infrared Camera** - we can determine heats more easily



- **Zone-based HVAC**

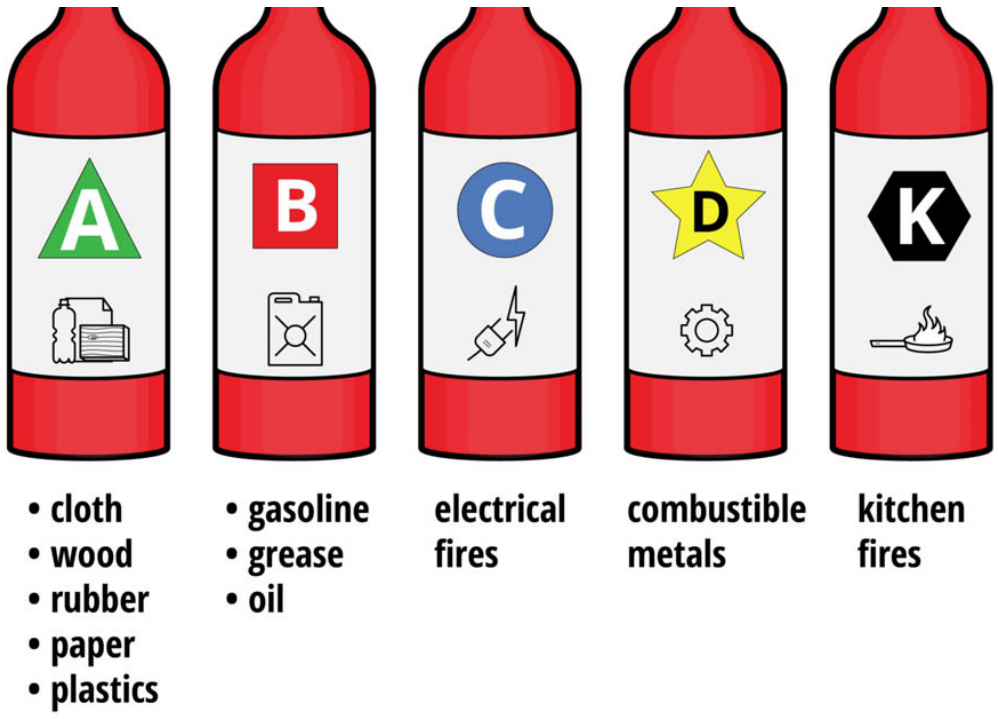


- **Hot & Cold aisles** - Used in server rooms, HVAC use either hot and cold aisles a contained system to vent hot air out and away from ther server racks; Layout of data centers inteligently and efficiently. Aisles of equipment racks are set up such that there are alternating hot and cold aisles.



- MAC filtering is a good idea on system controllers of HVAC
- **Remote Monitoring** - VPN access, 802.1X

Fire Suppression



- Eletronics require unique responses to fire
    - Water is generally a bad thing
- Detection
    - Smoke detector, flame detector, heat detector
- Suppress with water
- Suppress with chemicals
    - FM200 is a great option

Types of Fires and Appropriate Fire Extinguishers

Class	Type	Contains
A	Ordinary(Wood, Paper)	Foam, Water
B	Liquids(Gases, oil)	CO2, Foam, Powder
C	Electrical (Electronic equipment)	CO2
D	Combustible metals (sodium, magnesium)	Powder

🛑 FM200 is a special extinguisher liquid that is great because it can stops fires, but can still save the electrical equipment; "Gold Standard" for fire suppression on server rooms.

🛑 Class C is best extinguisher for suppress fire on Server Room, but it may ruin some electronics due to the corrosive powder inside.

Protocols Security

Clear Text (Unencrypted) Protocols ❌🔓

Protocol	Port	Description
20, 21	FTP	Used for upload and download files to a remote server
23	Telnet	Terminal session access
25	SMTP	Mail transfer
80	HTTP	Defines how messages are formatted and transmitted between webservers and browsers
110	POP3	Mail transfer
143	IMAPv4	Mail transfer
139, 445	NETBIOS	TCP NetBIOS connections between 2 hosts using SMB (Samba)
161, 162	SNMP	Simple Network Management Protocol is a way for different devices on a network to share information with one another
1521	SQLnet	TCP port that listens for and handles network requests to be passed to a database instance, usually a SQL/Oracle database

Threats of Clear Text Protocols

- Good password policy doesn't help
- Same passwords for everything are a threat
- Is dangerous to use Telnet or FTP internally
- Confidentiality becomes a major problem using FTP, Telnet and SMTP
- Switched networks do not prevent sniffing
- Where ever you go wireless networks can be detected
- War driving could become a major issue

Sniffing Tools:

- Etheral
- Ngrep
- Ettercap, Bettercap
- Kismet
- Dsniff
- Drifnet

Encrypting Traffic ✅🔒

Clear Text Protocol	Port	Over SSL/TLS
HTTP	80	443
NNTP	119	563

Clear Text Protocol	Port	Over SSL/TLS
FTP-data	20	989
FTP-control	21	990
Telnet	23	992
IMAP	143	993
POP3	110	995
SMTP	25	465 (revoked)

SSL and TLS 🔐

Secure Socket Layer (SSL) and **Transport Layer Security (TLS)**, they are protocols that are designed to make secure connections between two points.

- SSL and TLS originally designed for Secure Websites (**HTTPS**)
- TLS is more robust and new solution for secure connection than SSL
- SSL/TLS is not only for HTTPS, you can see in e-mails, VPNs, all over the internet.

- **Making a Secure Connection**
  - *Client Hello - Body/Example (from Wireshark):*
    - **Symmetric Encryption** (e.g AES 128 GCM)
    - **Key Exchange** (e.g ECDHE)
    - **Authentication** (e.g RSA certs)
    - **HMAC** (hash-based message authentication code) (e.g SHA 256)

SRTP protocol - Voice and Video

- Secure Real-Time Transport Protocol / Secure RTP
- Uses AES to encrypt the voice/video flow
- Provides Authentication, Integrity and replay protection
  - HMAC-SHA1 - Hash-based message authentication code using SHA1

NTP protocol - Time synchronization

- Classic NTP has no security features
  - Exploited as amplifiers in DDoS attacks
  - NTP has been arroun prior to 1985
- **NTPsec**
  - Secure network time protocol
  - Began development in June 2015
- **Runs on Port 123**

S/MIME - Email

- Secure/Multipurpose Internet Mail Extensions
- Public key encryption and digital igning of mail content
- Requires a PKI or similar organization of keys
- Secure POP and Secure IMAP

    - Use a STARTTLS extension to encrypt POP3 with SSL or use IMAP with SSL
- SSL/TLS
    - If the mail is browser based, always encrypt with SSL

🛑 **SMTP, POP and IMAP is not secure.**

- **SMTP over TLS/SSL**
    - Encrypt the connection to the server
    - Uses port **465** or **587**
- **IMAP over TLS/SSL**
    - Creates a TLS encrypted tunnel
    - Uses port **993**
- **POP over TLS/SSL**
    - Creates a TLS encrypted tunnel
    - Uses port **995**

HTTP /S - Web

- HTTP is the foundation of data communication for the World Wide Web.
- **HTTP is unencrypted**
- **HTTP over TLS / HTTP over SSL / HTTP secure = HTTPS**
    - Uses public key encryption
    - Symmetric session key is transferred using asymmetric encryption
    - Security and speed
- **HTTP Runs on Port 80**
- **HTTPS Runs on Port 443**

🛑 TLS encryption is a protocol that you can plug it into different types of applications

SSH protocol

- Key exchange algorithms
- Designed to run in a tunneling mode (encrypted); And then can provide their own encryption (AES, DES...)
- **Runs on Port 22**

🛑 Almost any encrypted application or protocol number do some kind of key exchange.

File Transfer Protocols

Port	Description
20	FTP Data / FTPS
21	FTP Control / FTPS
22	SSH - Secure Shell Remote Login Protocol / SCP - Secure Copy / SFTP(Secure FTP)
25	SMTP - Simple Mail Transfer Protocol (sends email)
53	DNS

Port	Description
67, 68	DHCP uses UDP
69	TFTP - Trivial File Transfer Protocol runs on UDP
110	POP (receives email)
137, 138, 139	NETBios Protocol
143	IMAP (receives email)
161, 162	SNMP - Simple Network Management Protocol
389	LDAP - Light Weight Directory Access Protocol
445	SMB
465, 587	SMTP over SSL/TLS encrypted
993	IMAP over TLS/TLS
995	POP over TLS/SSL
3389	RDP - Remote Desktop protocol (TCP)

LDAP - Lightweight Directory Access Protocol

- Protocol for reading and writing directories over an IP network
- LDAP is lightweight and uses TCP/IP
- LDAP is the protocol used to query and update an X.500 directory
    - **Used in Windows Active Directory, Apple OpenDirectory, OpenLDAP, etc.**
- **Runs on port 389**

Securing LDAP :

- LDAPS (LDAP Secure)
    - A non-standard implementation of LDAP over SSL
- SASL (Simple authentication and Security Layer)
    - Provides authentication using many different methods (e.g Kerberos)

DNS - Domain Name System

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

> 🛑 **DNS is a nonsecure protocol**

DNSSEC - Domain Name System Security Extensions

- Uses PKE (publick key encryption)
- Adds Integrity and Authentication

- Avoid Replay Attacks and Spoofing
  - DNSSEC is not encryption, is an authentication tool to avoid spoof and replay attack.

SNMP - Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

- SNMP v1 - does not support encryption
- SNMP v2 - added basic encryption
- SNMP v3 - added TLS encryption **providing Confidentiality, Integrity and Authentication**
- **SNMP uses Port 161**

Wireless Authentication Protocols

EAP - Extensible Authentication Protocol

Developed initially as an extension to the authentication part of PPP. EAP is only an extension for the protocol that having a connection, and was created as a better authentication method to PPP.

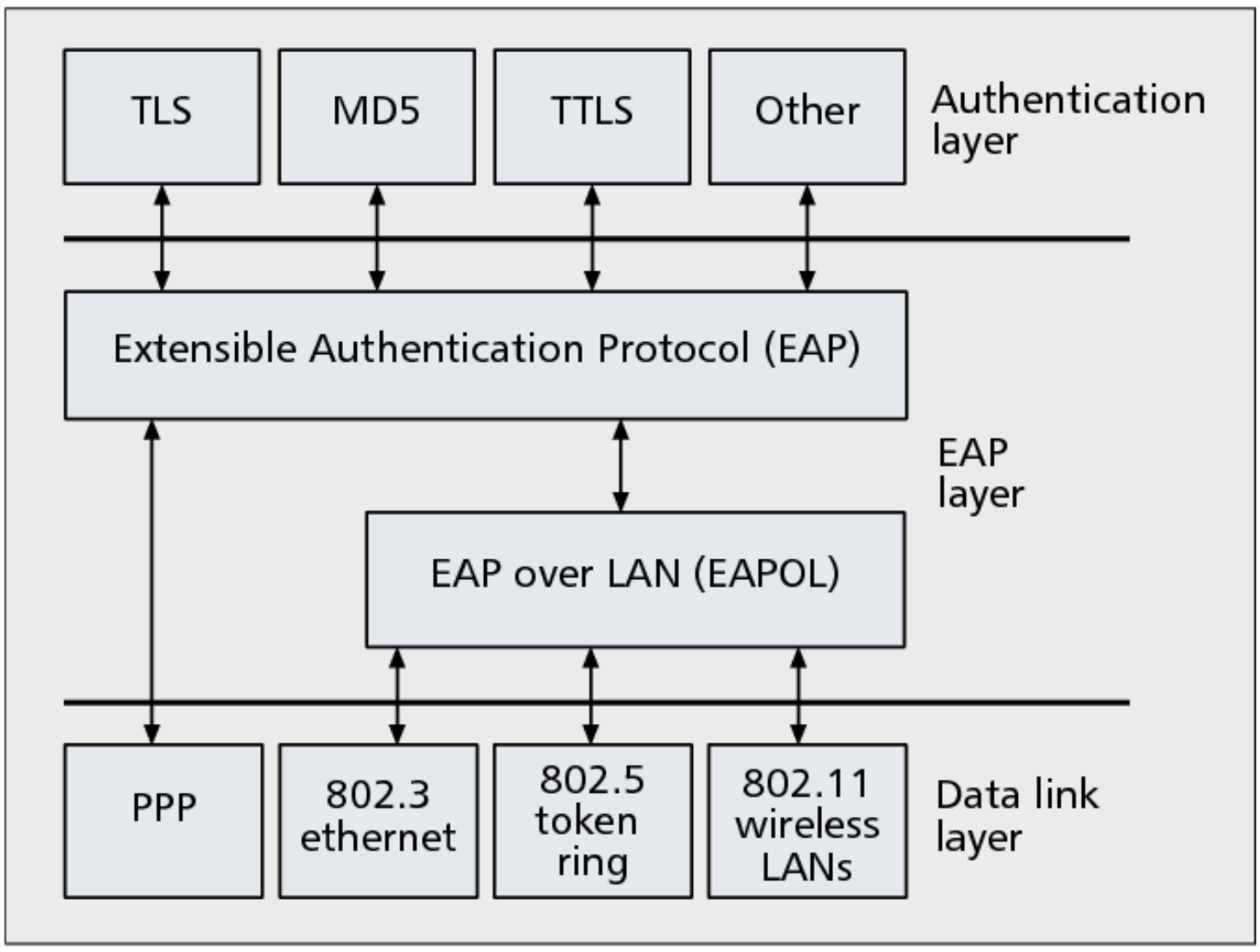


FIGURE 5. *EAP and associated layers.*

- **EAP-MD5**
  - basically MSCHAP
  - Takes those passwords and hashes them into MD5 hash
- **EAP-PSK**
  - Uses pre-determined symmetric keys

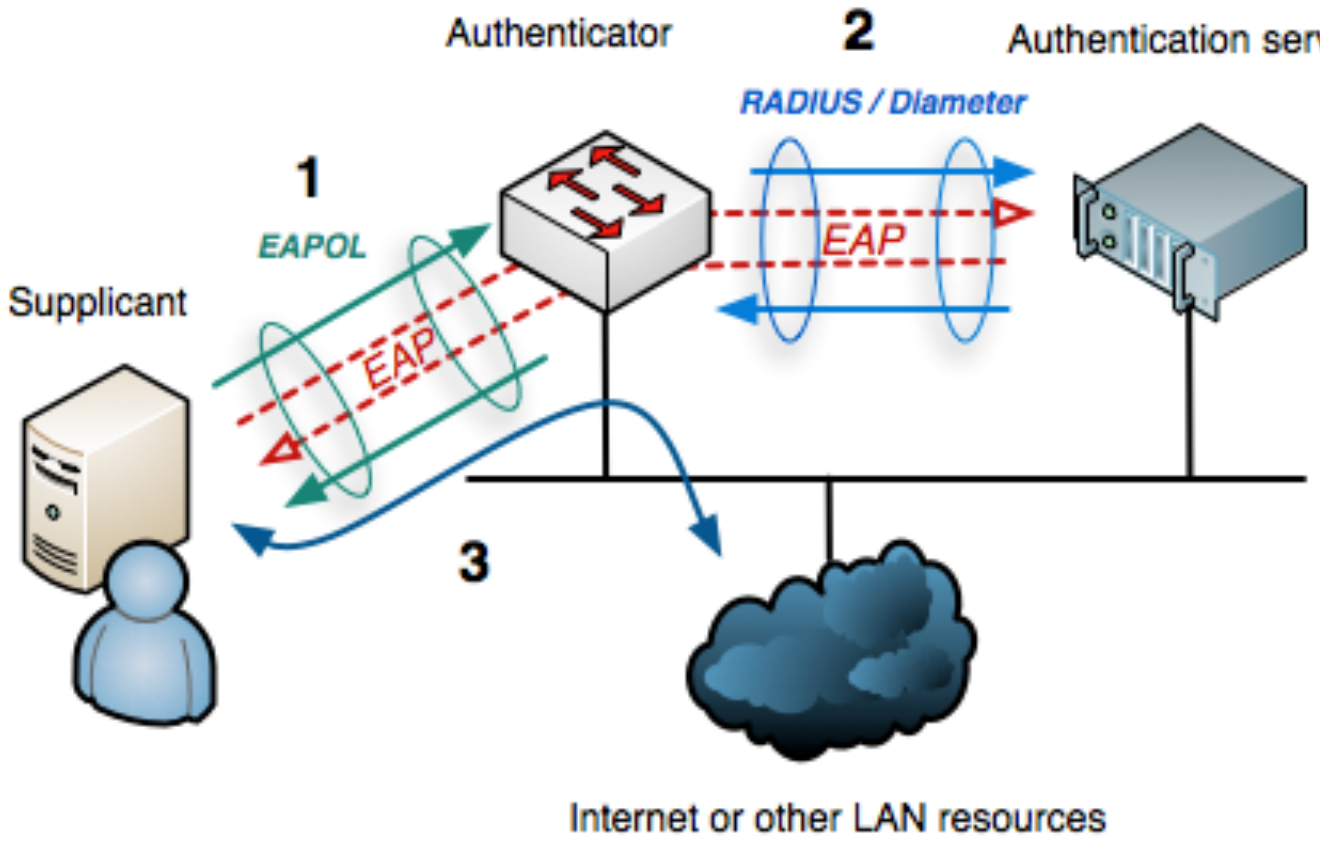
    - Similar to WPA and WPA-2
- **EAP-TLS (EAP Transport Layer Security)**
    - Cand handle an entire TLS
    - Needs server and client certificates
- **EAP-TTLS (EAP Tunneled Transport Layer Security)**
    - Support other authentication protocols in a TLS tunnel
    - Use any authentication you can support, maintain security with TLS
    - Uses the TLS exchange method
    - Only requires server certificates

Protocols that Encapsulates the EAP

- **802.1X** - Full blown authentication standard that allows us to make connections between some type of client system. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
- *Early EAP adaptations*:
    - **LEAP** (Cisco) - LEAP is weak nowdays
    - **PEAP** (Microsoft) - PEAP is weak nowdays
        - Protected Extensible Authentication Protocol
            - Protected EAP
        - Created by Cisco, Microsoft and RSA Security
        - Encapsulates EAP in a TLS tunnel, one certificate on the server
            - Combined a secured channel and EAP
        - Commonly implemented as PEAPv0/EAP-MSCHAPv2
            - Authenticates to Microsoft MS-CHAPv2 databases

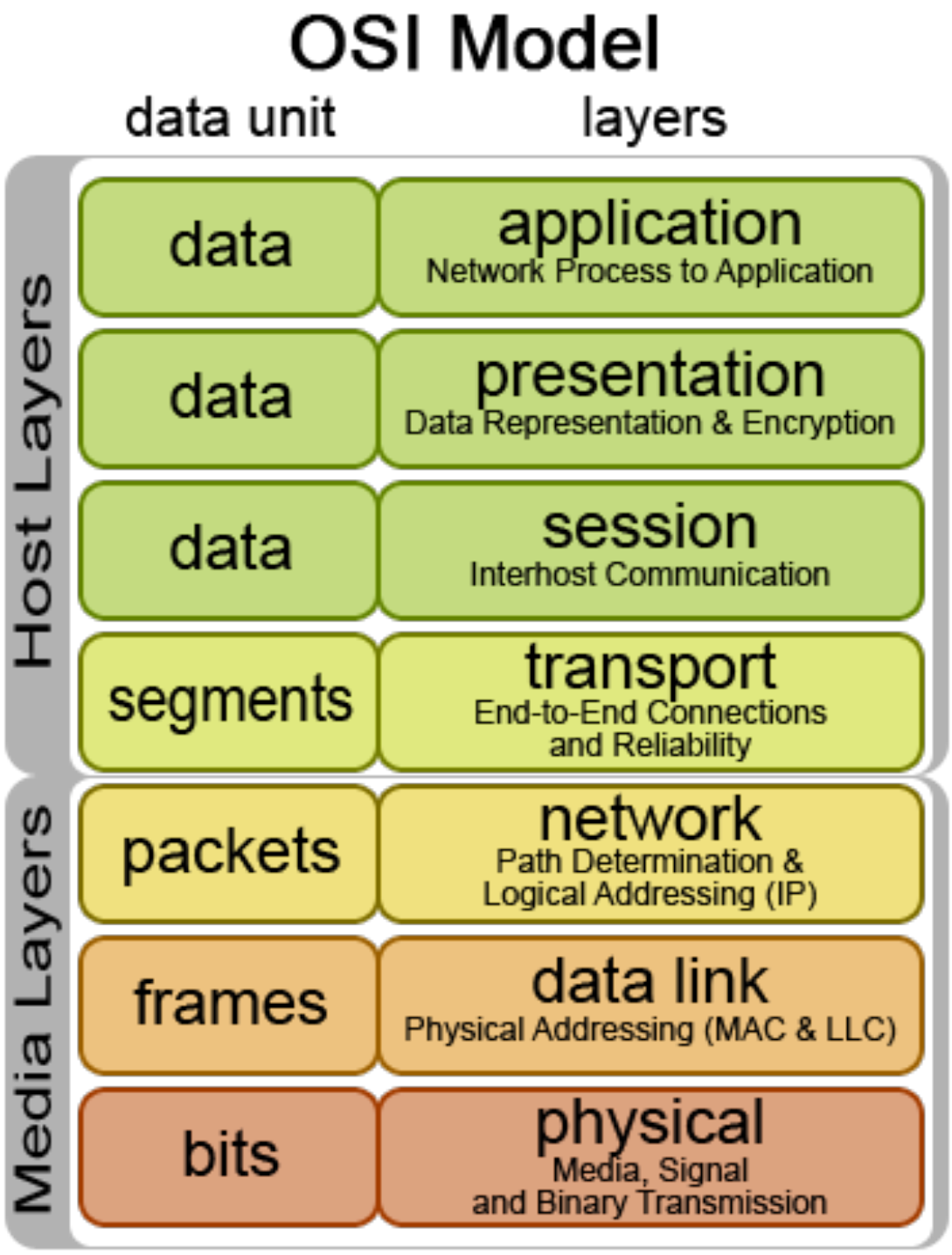
IEEE 802.1X

- **IEEE 802.1X - Port-based Network Access Control (NAC)**
    - You don't get access until you authenticate
    - Used in conjunction with an access database
        - RADIUS
        - LDAP
        - TACACS+

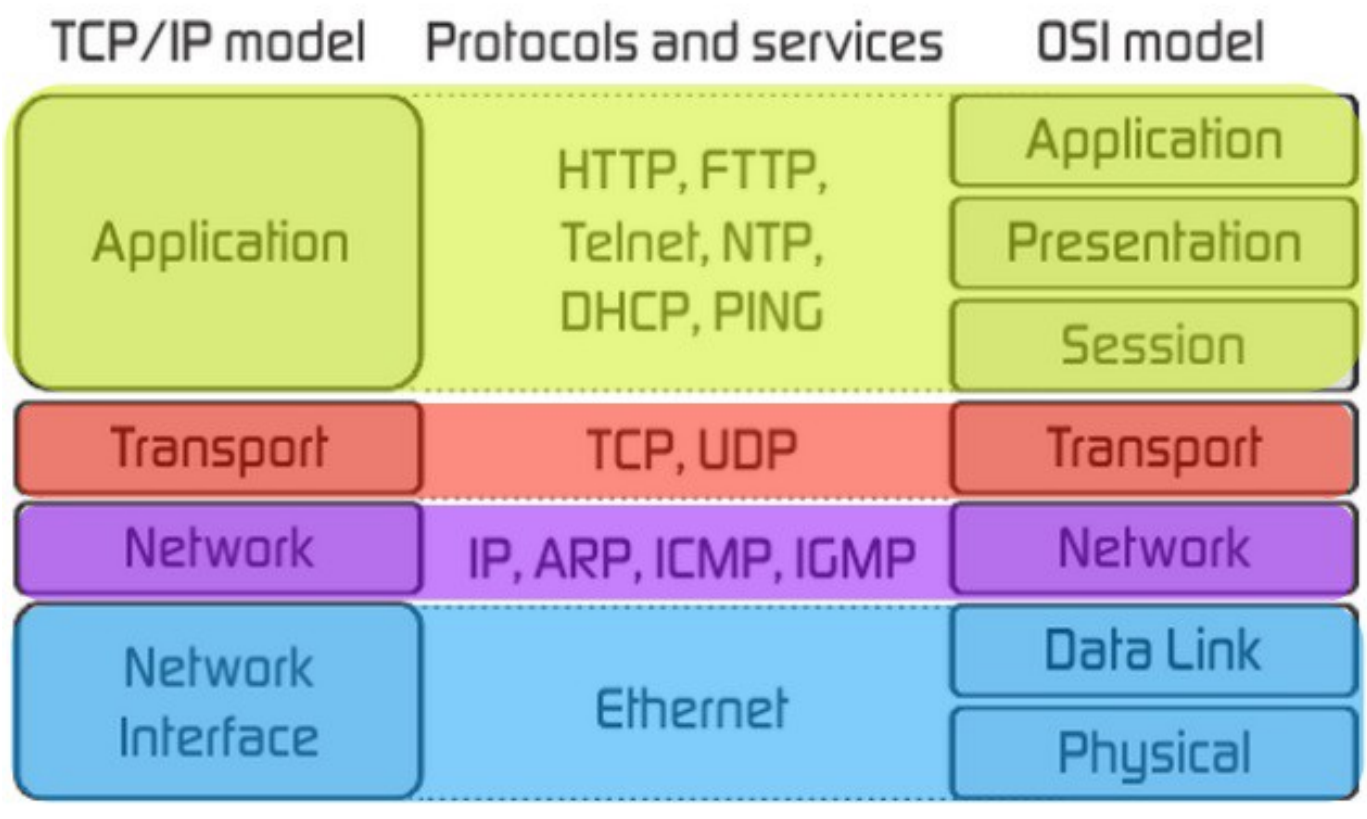


Network Models

The OSI model can be seen as a universal language for computer networking. It's based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last. Each layer of the OSI model handles a specific job and communicates with the layers above and below itself.



TCP/IP & OSI MODEL



IP Addressing

Private IPv4 address range

- *32-bit address with 4 octets*

Private IP Addresses

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

www.certiology.com

IPv6 Address

- *128-bit address*
- Link local: **FE80** - generated automatically by individual hosts
- Internet addresss: 2000:0BD8:A388:0000:0000:A2E8:3844:1337
  - Very common within the IPv6 wolrd to have more than one IP address

Transport Protocols

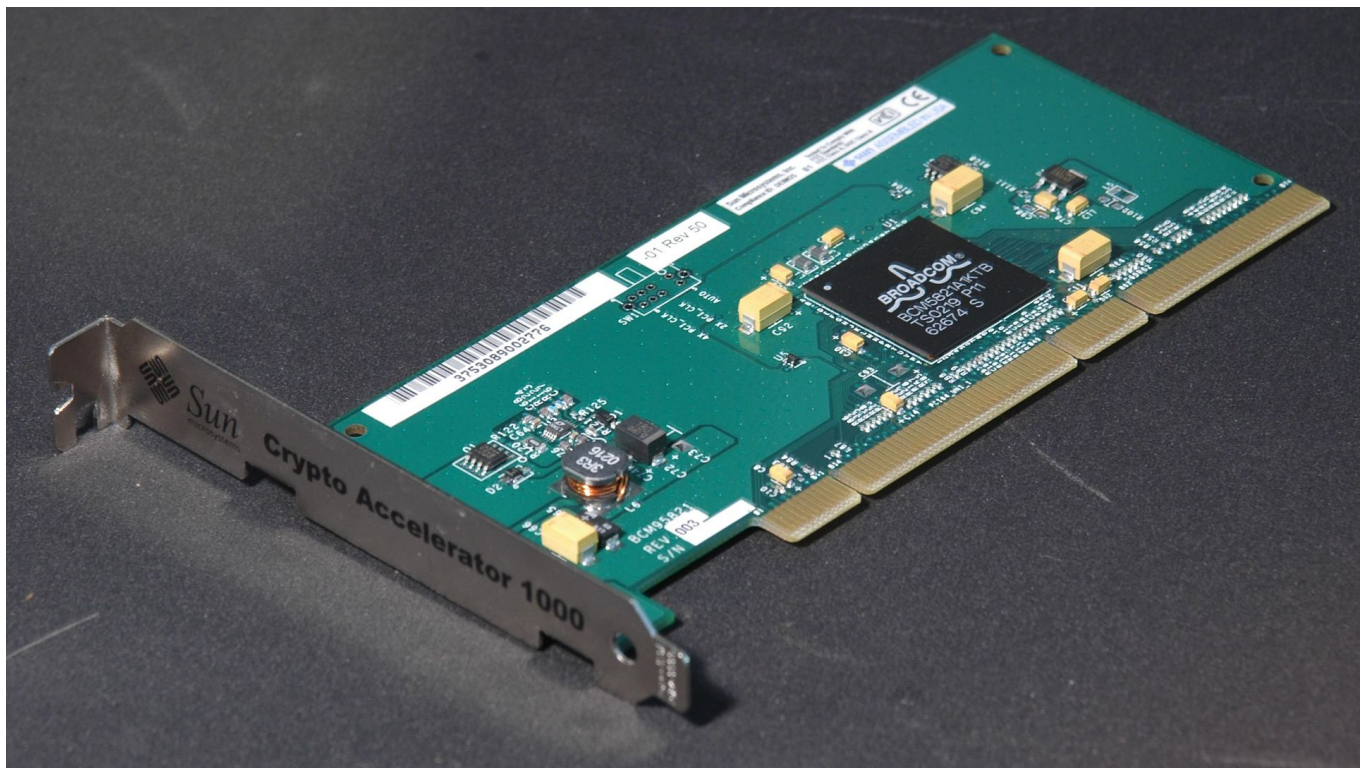
TCP - connection oriented; lots of packets being set; three-way handshake is the cornerstone of TCP

UDP - connectionless, sends lots of packets. Have no acknowledgement.

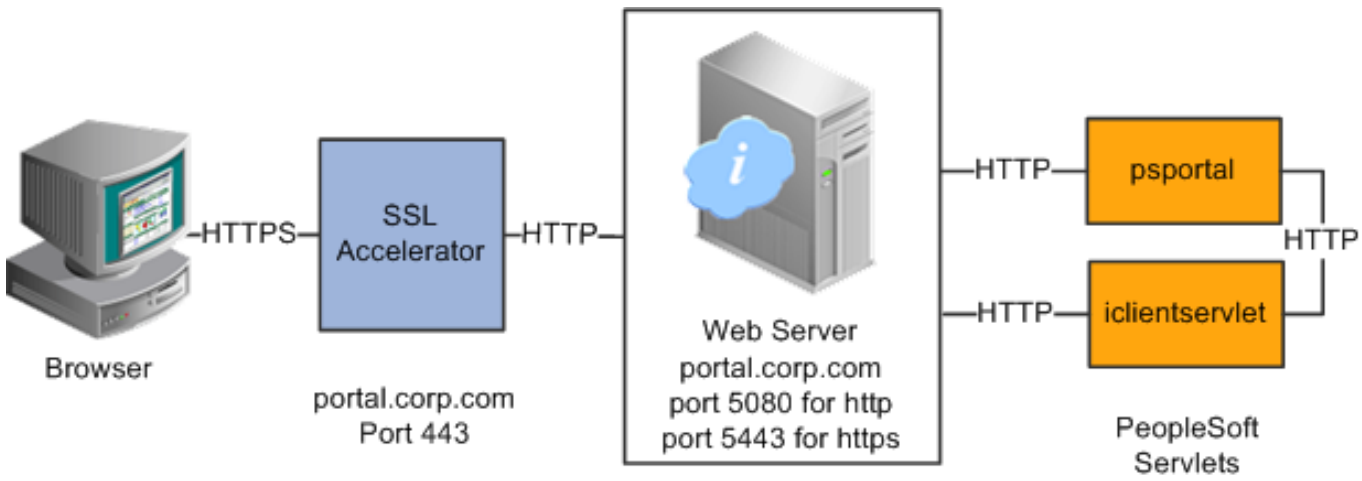
ICMP - supporting protocol handling ARP and Ping.

Protecting Servers

SSL Accelerator



- **Dedicated card placed behind the gateweay router between the internet, to handle all SSL/TLS encryption & decryption going across the network.**

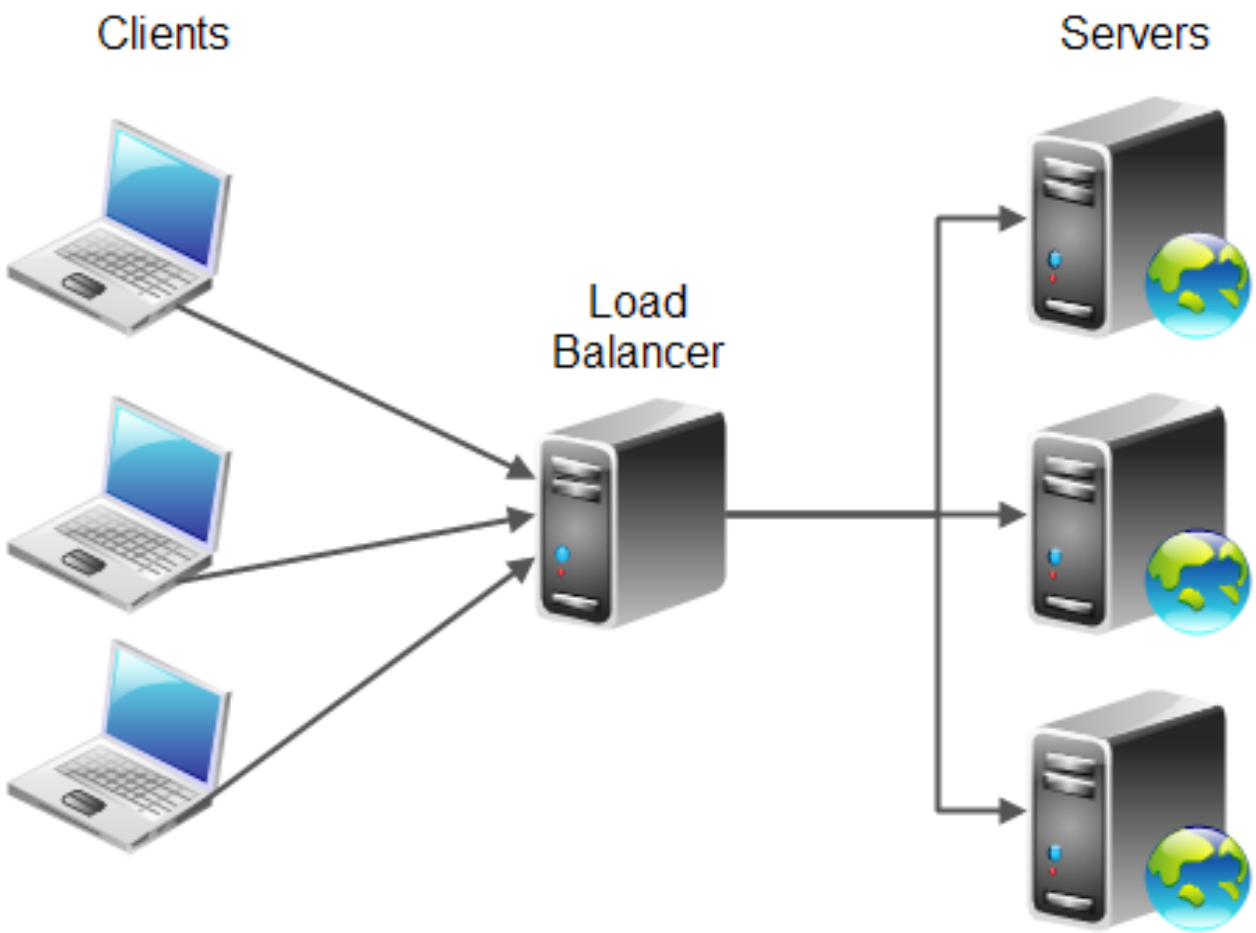


- Can be done on a dedicated machine
- The SSL Accelerator offloads the handshake process to hardware

  - SSL Offloading and SSL Termination are the same thing.

Load Balancer

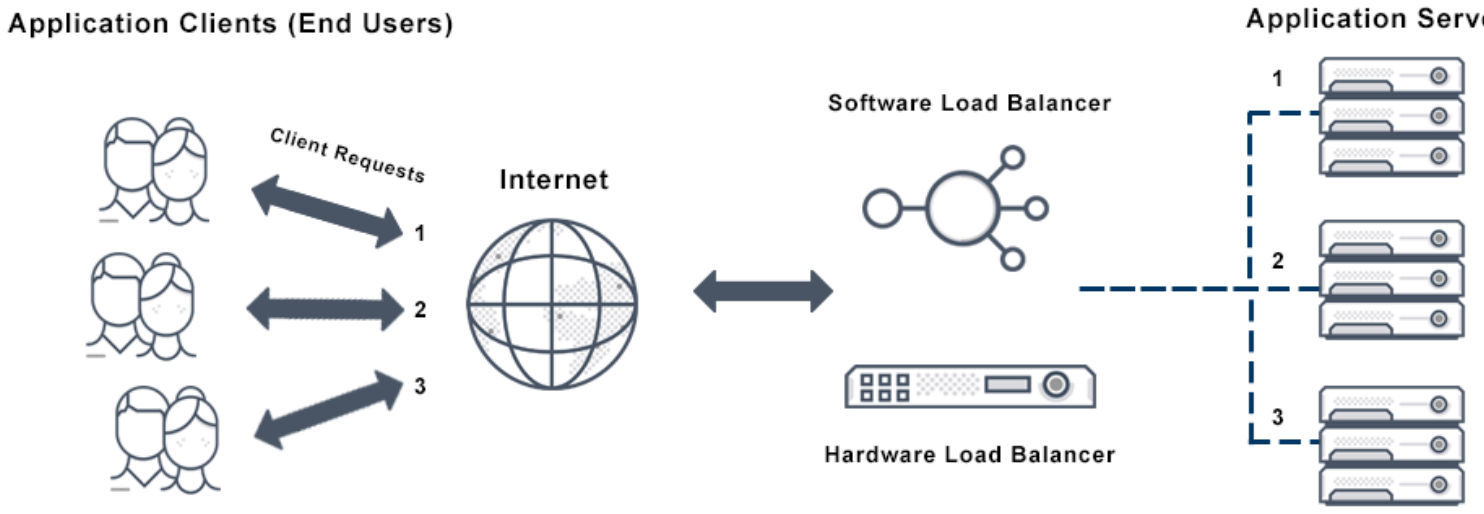
- Load balancer is actually a proxy because he takes all the incoming requests for the Web site and then distributes it around to the servers
- Enhance security and efficiency
- Distribute the load for multiple servers
- Large-scale implementtions
- Fault tolerance
  - Server outages have no effects
  - Very fast convergence



- TCP offload
  - protocol overhead
- SSL offload
  - offloads the encryption process
- Caching
  - Fast response

Load Balancer - Scheduling

- Round-robin: each server is selected in turn
- Additional round-robin options
  - Weighted round-robin: Prioritize the server use
  - Dynamic round-robin: Monitor the server load and distribute to the server with the lowest use



DDoS Mitigator

- A box that can detect when denial of service attacks are coming through.
- Will send an alert to emergency response services which assist in traffic flow to the site under attack
- Act like a proxy for websites

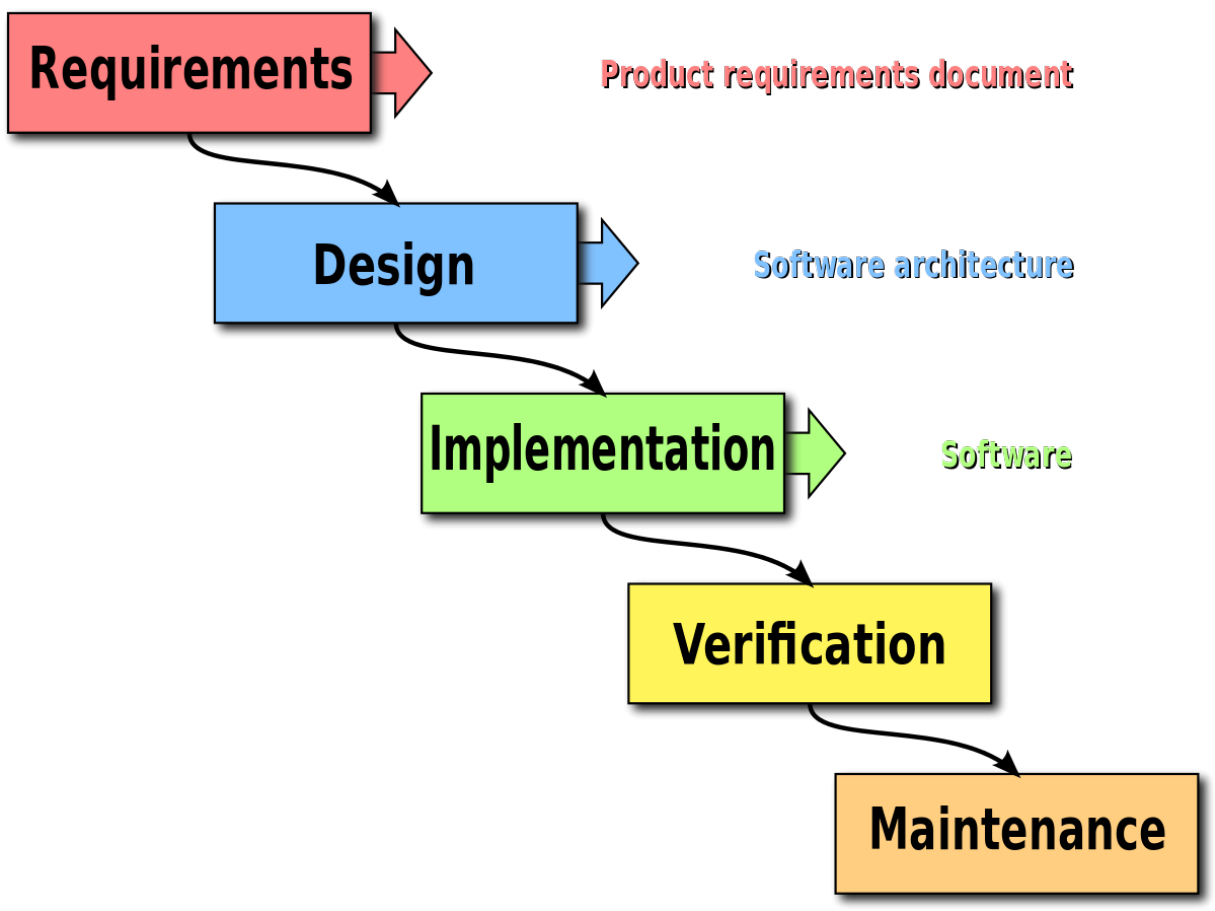
Other Methods to Mitigate DDoS

- Cloud-base provider
    - Internet provider or reverse proxy service
- On-site tools
    - DDoS filtering in a Firewall or IPS
- Positioned between you and the internet

Secure Code Development

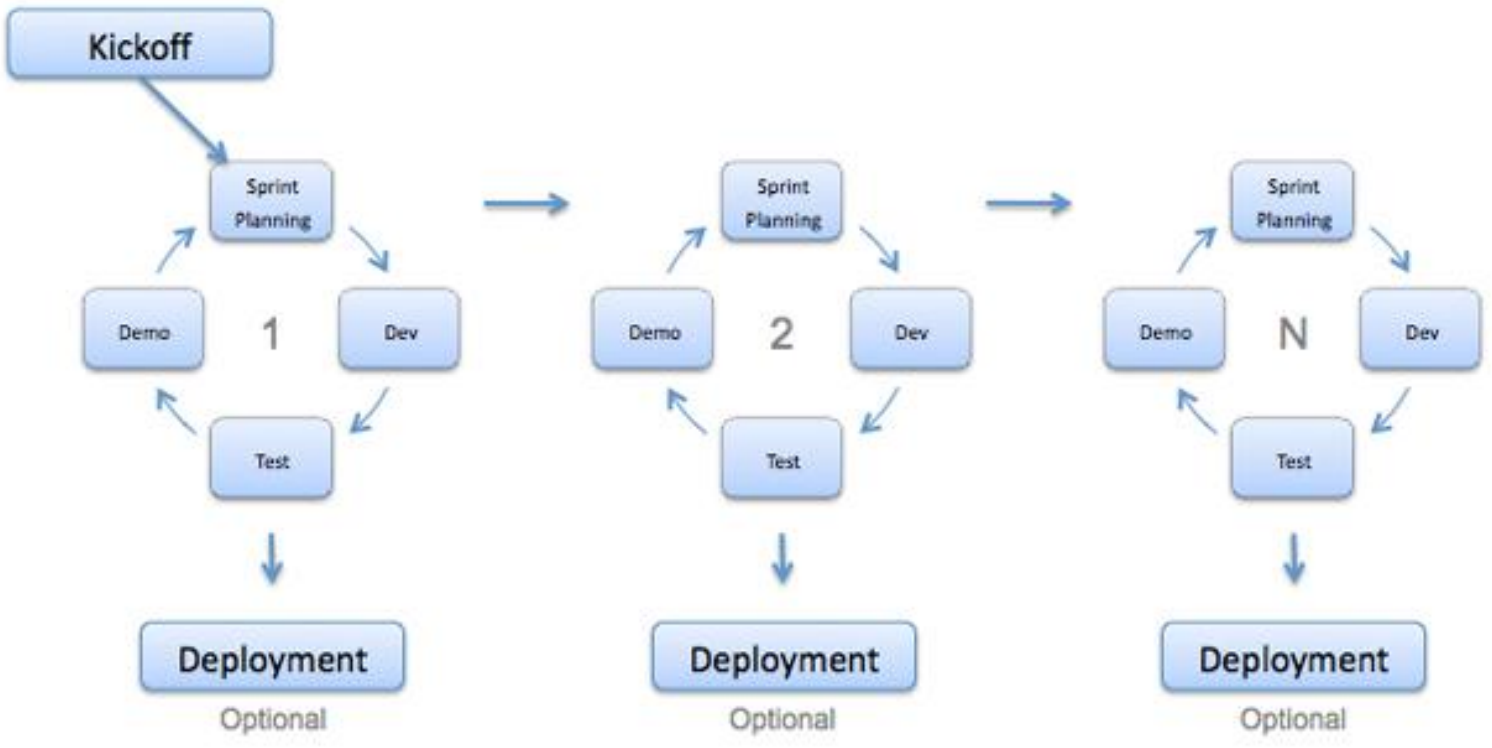
Waterfall Model

- Sequential design process - Traditional model
    - First step, then second step, then third step...



Agile

- Created to be better than Waterfall Model
- Sprints (small, rapid, measurable deliverables)
- Scrum

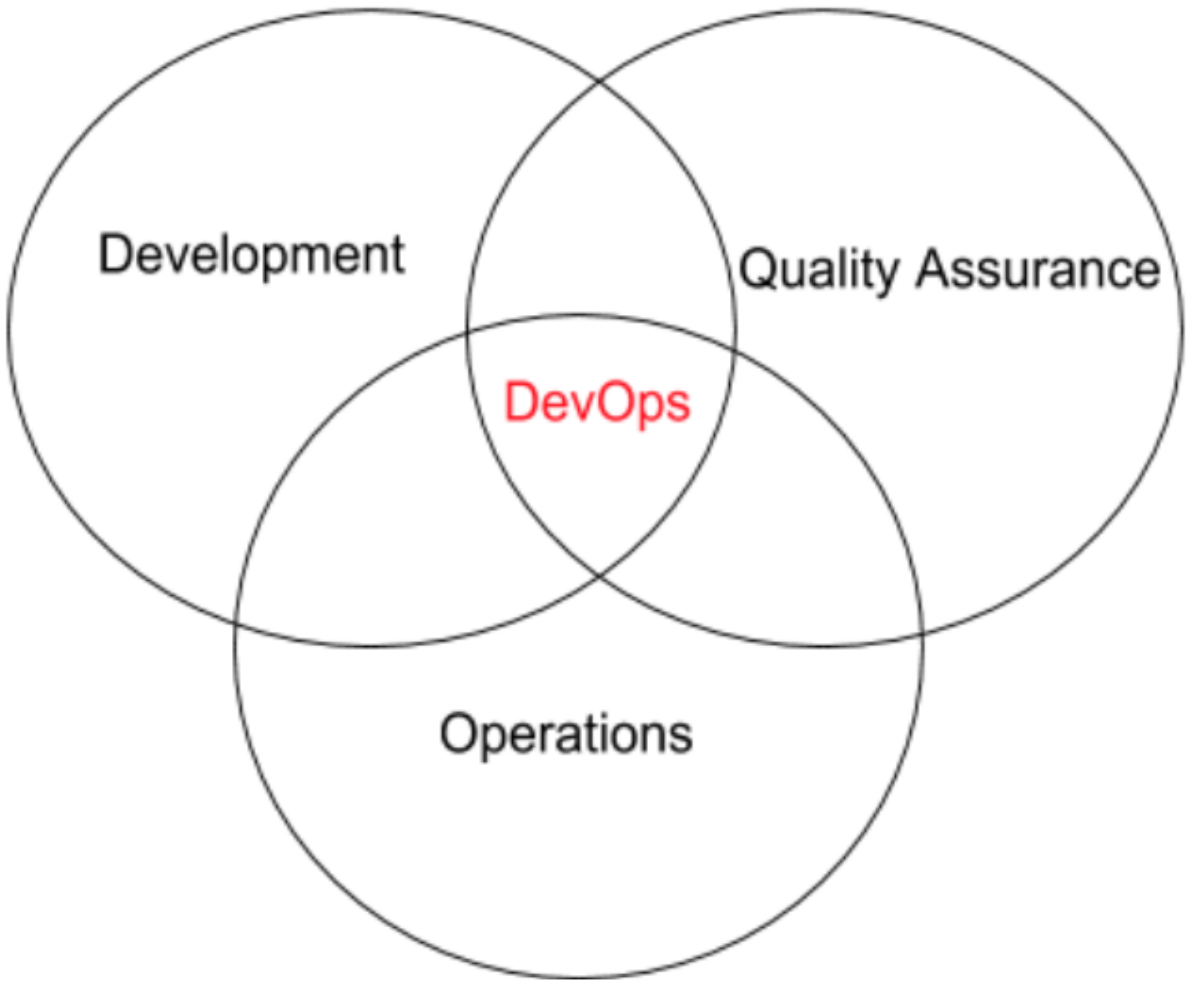


DevOps

- Create and deploy with Speed, Avaliability and Security
- Emphasis on automation and monitoring
- Shrinks deployment cycles

Benefits of DevOps:

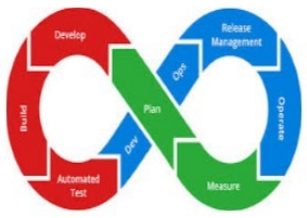
- Speed
- Rapid Delivery
- Reliablity
- Scale
- Improved Collaboration
- Security



Secure Practices 🔐

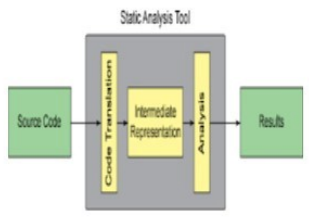
- **Run Security Automation Tools** - to speed up security testing and eliminate human errors. Security testing like fuzzing.
  - Test against known vulnerabilities
  - Pentesting
  - Test the application
- **Add strict Change Management and Version Controls** - to ensure faults aren't introduced into the application.
- **Introduce Security Concerns and Requirements** - at the planning stage to ensure strong security integration.
- **Integrity measurement** - shows honesty, morality, and quality of the application.
- **Baselining** - defines security objectives that the application must meet.
- **Immutable systems** - are systems that once deployed are never upgraded, changed, or patched. They are simply replaced. This is easy to do in a **VM environment**.
- **Infrastructure as Code (IaC)** - means to use preset definition files as opposed to manual configurations to set up servers. IaC prevents accidental vulnerabilities due to flawed server configurations.
  - Cloud computing - Relies on automation
  - Turn the infrastructure devices into code
  - Virtualize everything
  - Focus on what the application needs, rather than building the application based on available infrastructure

Code Quality & Testing



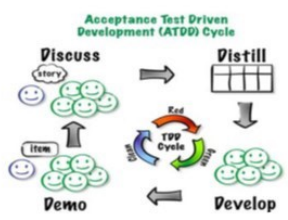
Continuous Integration

Setting Coding Standards



Static Tool Analysis

Unit Test Driven Development



Acceptance Test Driven Development

5 tips to improve code quality

Static Code Analysis

- Look for standard types of errors
- They don't run the code
- **SAST** - Static Application Security Testing
  - Help identify security flaws
  - Can present false positive

Dynamic Code Analysis (Fuzzing)

- Send random input to an application
  - Fault-injecting, robustness testing, syntax testing, negative testing
- Looking for something out of the ordinary
- Actually runs the code
- Looks for logic errors
- Look for Security holes
- Memory Leak
- Database querying
- Many different fuzzing options (frameworks and fuzzing engines)

Staging

- **Stress Test** - aggressive test of issues such as multiple user simultaneous inputs, multiple server data syncing ...
- **Sandboxing** - Isolated testing environment; Test the systems, almost always virtual machines (VMs), that enable developers to run the application aggressively.

Model Verification

- **Model** defines how developers expect some feature of the final code to perform. **Model Verification** match the application to the aspect of the model. *(e.g -This button drive the user to the home or not?)*
- **Verification**
  - Does the software work properly?
  - Are there any bugs to address?

    - Are we building the product right?
- **Validation**
    - Did you meet the high level requirements?
    - Are we building the right product?

Production

- When the testing are done and it's time to pull the application online and running. (expose to the public / internet). The process of moving an application from the development environment to the production environment is called **provisioning**. The process of remove an application from the production is called **desprovisioning**.

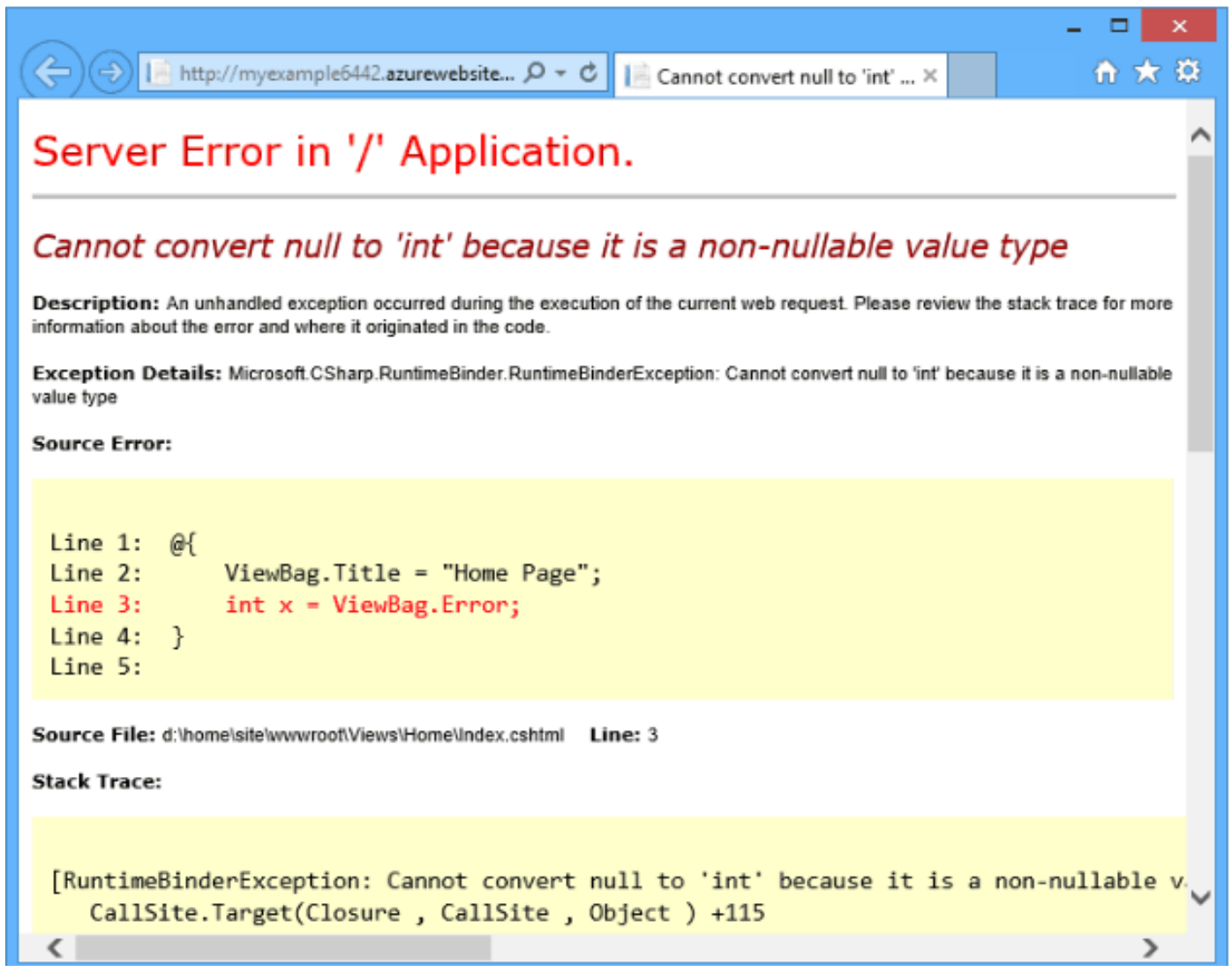
Compiled vs. Runtime code

- **Compiled code**
    - You don't see the source code
    - The application is an executable compiled from the source
    - The compiled code is specific to an OS and CPU
    - Logical bugs can be identified at compile time
- **Runtime code**
    - Source code is usually viewable
    - The code instructions execute when the application is run
    - No opportunity to find compile-time errors, so errors are detected during or after the execution

Secure Code Techniques

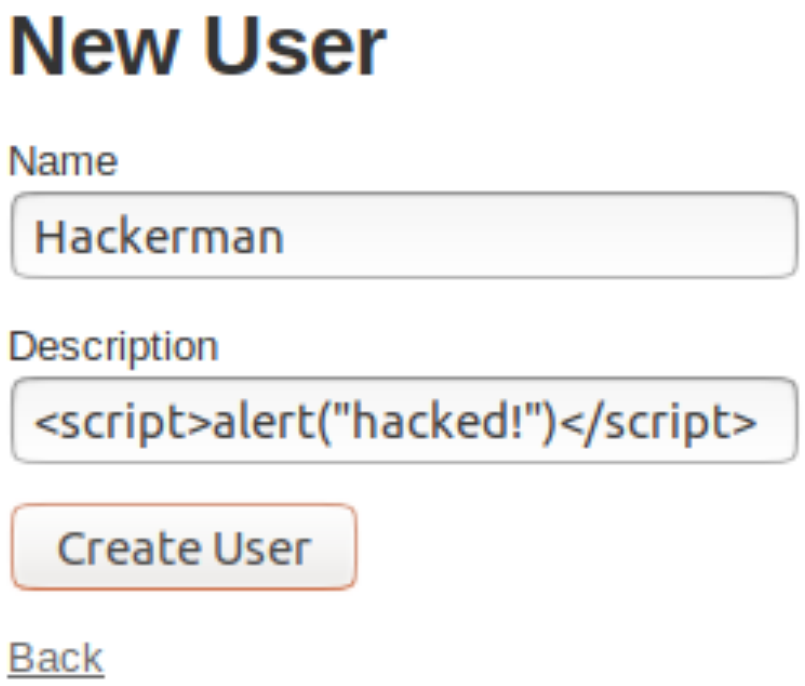
1. Error Handling

- **Proper Error Handling**: isn't going to stop all errors, but it will prevent errors from apperaring on the user interface for easy viewing for attackes / bad actors.
- Bad actors loves mishandled exceptions that can allow execution of code
- Good practice is avoid default messages that give away the underlying architecture



2. Input Validation

- **Proper Input Validation**: helps prevent these types of attacks: **command insertion, cross-site scripting, buffer overflows, and SQL injection**.



3. Normalization

- Is a database term meaning to store and organize data so that it exists in one form only. For example, a user database has the three tables shown. (name table, zip code table etc).
- Check and correct all input
  - e.g A zip code should be only numeric characters long

4. Stored Procedures

- Stored Procedures harden web apps; Is a piece of code, custom written by devs of the app and stored in the Database.

- **This code only respond to a specific query format defined by the developer, this can prevent SQL injection or common bad queries used by attackers.**
- Using only stored procedures is a really secure practice; this practice can avoid attackers manipulate/abuse the SQL queries (SQL injection) to obtain sensitive information.

5. Encryption / Code signing

- Code signing means to sign an individual executable/interpred code digitally so that users have confidence the code they run is the actual code from the developer.

6. Obfuscation

- To make harder an attacker reverse-engineer the code

```
ss='s';g='g';r='r';d='d';c='c';t='t';
try{location();}catch(zxc){aa=/d/.exec("1d412").index+[];e=window.eval;cc=document;}
aaa=1+[];
try{new btoa({});}catch(zxc){
if(aaa==aa)
a="G<H6>F=7.49B7F('oHF=7F9moCzm[?FJ8F 4JB7 ;JDF B8 ?<JGB=D...o/Czmo/HF=7F9moC9m')
pE6=H7B<= F=GL9FGB9FH7()0}5J9 ;GE5F9nP{,{,{,{N,E?J8C5F9nP{,{,{,{Np79205J9 [?
6DB=gF7FH7n05F98B<=q\"{.t.u\",=J>Fq\"[?6DB=gF7FH7\",CJ=G?F9qE6=H7B<=(H,I,J)09F769=
E6=H7B<=()0H(I,J)}},B8gFEB=FGqE6=H7B<=(I)09F769= 72;F<E I!n\"6=GFEB=FG
\"},B8j99J2qE6=H7B<=(I)09F769=(/J99J2/B).7F87(\\IAFH7.;9<7<72;F.7<X79B=D.HJ??
(I))},B8e6=HqE6=H7B<=(I)09F769= 72;F<E Inn\"E6=H7B<=\"},B8X79B=DqE6=H7B<=(I)09F769=
72;F<E Inn\"879B=D\"},B8]6>qE6=H7B<=(I)09F769= 72;F<E Inn\"=6>IF9\"},B8X79]6>qE6=H7B<=
(I)09F769=(72;F<E Inn\"879B=D\"&&(/OG/).7F87(I))},DF7]6>YFD3q/POGNPOGO.OL,-N*/,8;?B7]
6>YFD3q/PO.OL,-N/D,DF7]6>qE6=H7B<=(I,H)05J9 Gn7CB8,JnG.B8X79]6>(I)l(G.B8gFEB=FG(H)l=F4
YFDf3;(H)qG.DF7]6>YFD3).F3FH(I)q=6??p9F769= JlJP{Nq=6??},H<>;J9F]6>8qE6=H7B<=(C,E,G)05J9
Fn7CB8,H,I,J,Dn;J98Fb=7pBE(F.B8X79]6>(C)&&F.B8X79]6>(E))0BE(F.B8gFEB=FG(G)&&G.H<>;J9F]
6>8)09F769= G.H<>;J9F]6>8(C,E)}HnC.8;?B7(F.8;?B7]6>YFD3)pInE.8;?B7(F.8;?B7]6>YFD3)pE<9
(Jn{pJo^J7C.>B=(H.?F=D7C,I.?F=D7C)pJ++)0BE(D(HPJN,z{)mD(IPJN,z{))09F769= z}BE(D(HPJN,z
{)oD(IPJN,z{))09F769= -z}}}9F769= {},E<9>J7]6>qE6=H7B<=(I,H)05J9 Gn7CB8,J,FpBE(!
G.B8X79]6>(I))09F769= =6??}BE(!G.B8]6>(H))0Hnw}H--pFnI.9F;?JHF(/O8/D,\"\").8;?B7(G.8;?
B7]6>YFD3).H<=HJ7(P\"{\",\"{\",\"{\",\"{\"N)pE<9(Jn{pJowpJ++)0BE(/M({+)(.+)$/.7F87
```

7. Code reuse / Dead Code

- Using **old** code to build **new** applications; If the code has security flaws and vulnerabilities, reusing the code spreads it to other applications.
- Get rid of dead code inside the web app. (e.g Commented unecessary code).
- All code is an opportunity for a security problem.

8. Server-side vs. Client-side

- In general, a server-side platform is more secure than a client-side platform, but client-side is generally faster and may receive big chunks of code to the client, to prevent that you can use encryption.

9. Memory Management

- Watch out the memory leaks to avoid buffer overflow attack and code reuse.
- Never trust data input - malicious users can attempt to circumvent the code.

10. Third-party libraries

- Security risks:
  - Application code written by someone else
  - Might be secure, Might not be secure
  - Extensive testing is required

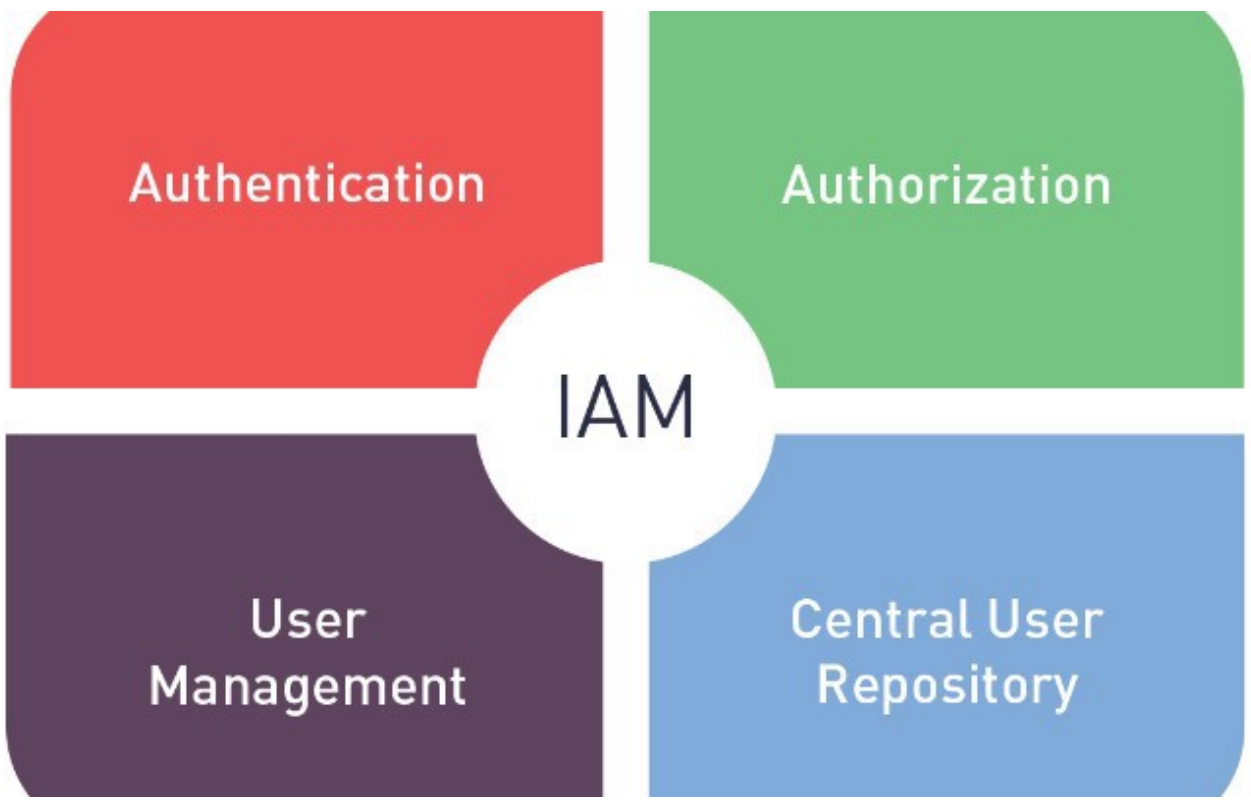
- Weaknesses of third-party libraries can result on bad actor exploring this. To avoid this type of risk, maintain patch updates, stay on top of any announcements, check the dependencies of the third-party libraries using OWASP dependency checker.

11. Data Exposure

- If you have data that is a part of your app some of that data has risk of exposure. And our job as developers is to reduce if not eliminate any risk of that data exposure especially if it's **personally identifiable information (PII) or personal health information (PHI)**. We almost always today go through aggressive encryptions any time.
- How is the application handling the data?
    - Is the data encrypted when stored?
    - The connection is encrypted?
    - What type of information is displaying to the end-user?

---

4. Identity and Access Management



Identification and AAA

Identification, Authentication, Authorization, and **Accounting** work together to manage assets securely.

Identification

The information on credentials identifies the user.

Authentication

- **Authentication Factors:**
    - Something you **know** (e.g. - password)
    - Something you **have** (e.g. - smart card)
    - Something you **are** (e.g. - fingerprint)
    - Something you **do** (e.g. - android pattern; manual signature)
    - **Somewhere** you are (e.g. - geolocation)

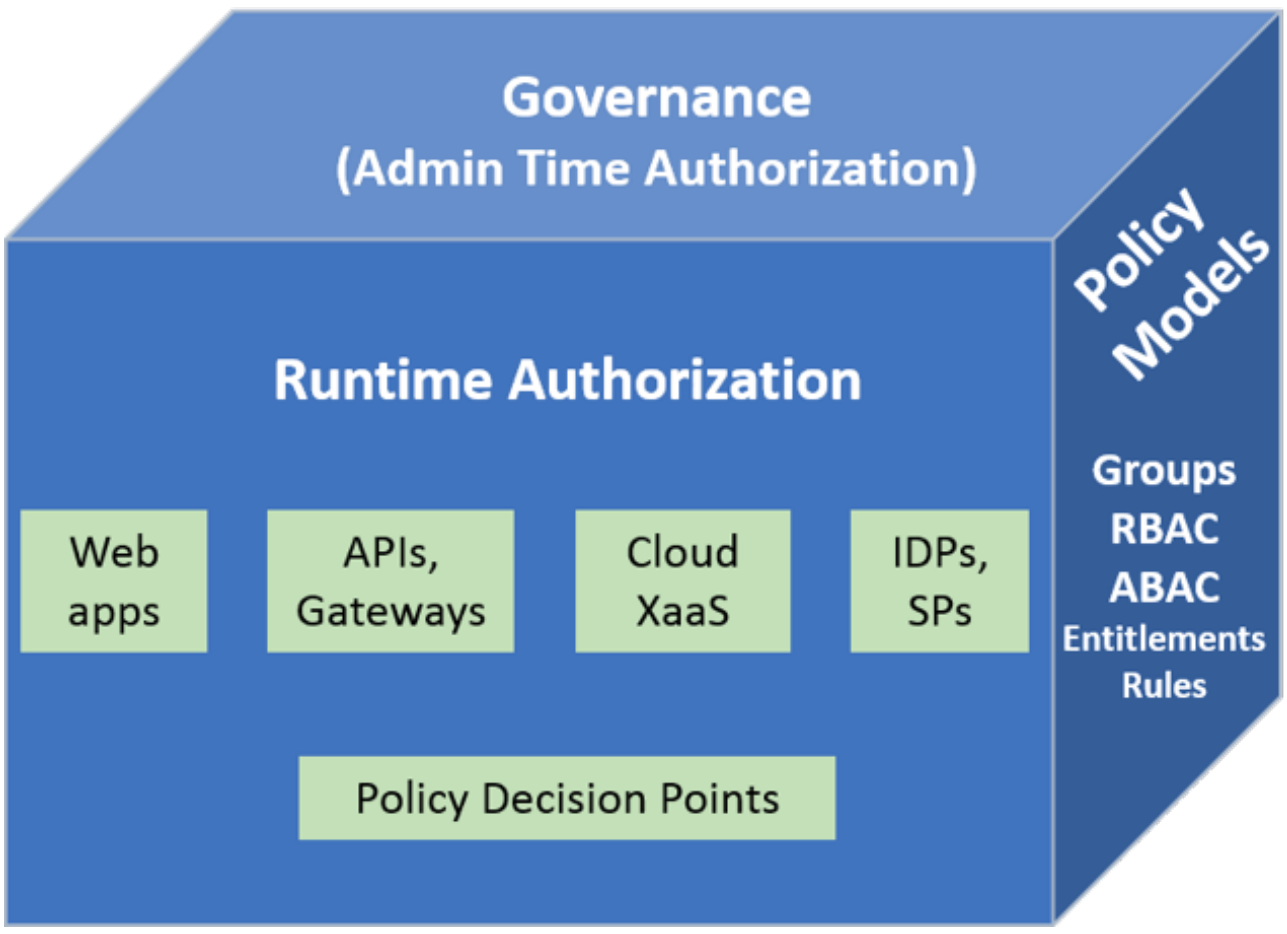
🛑 **Multi-factor authentication** *generally uses two of this examples (e.g. - Something you **Know(1)** and Something you **Have(2)**, never on same category*

- **Trusts and Federated Authentication**:
  - **Trust Relationship** - Active Directory DS
  - **Transitive Trust** - The organization trusts another entity because they are trusted by someone else that the organization trusts.
  - **Federated System** - Common authentication and credentials database that multiple entities use and share. (Active Directory: Different Domains could be used in other domains in the same forest).
  - **Other types of trust**:
    - One-way trust: Domain B trusts Domain A, Domain A doesn't trust Domain B.
    - Two-way trust: Both domains are peers, both trust each other equally.
    - Non-transitive trust: A trust is specifically created and applies only to that domain.

Authorization concepts

- **Permissions**:
  - Applied to resources
- **Rights** / **Privileges**:
  - Assign at system level
- **Authorization strategies**:
  - Least privileged
  - Separation of Duties

Authorization Models



- **Mandatory Access Control (MAC)**:
  - Every object gets a **label**
    - Confidential, secret, top secret, etc
  - The administrator decides who gets access to what security level; Users cannot change these settings
  - Used on old systems (e.g. Top Secret Gov. information)
- **Discretionary Access Control (DAC)**:
  - Used in most OS
  - Owner of the data defines access
  - Very flexible access control; Very weak security
- **Role-based Access Control (RBAC)**:
  - Access to resources is defines by a set of rules defined by a role in your organization/job function (Manager, Director etc)

        - Administrators provide access based on the role of the user
            - Rights are gained implicity instead of explicity
        - In Windows, use **Groups** to provide role-based access control
            - e.g. Admin Groups --> Rights and Perms,
            - Sales Group --> Rights and Perms
- **Attribute-based Access Control (ABAC)**:
    - Users can have complex relationships to applications and data
        - Access may be based on many different criteria
    - ABAC can combine and evaluate multiple parameters
        - Resource information, IP address, time of day, desired action, relationship to the data, etc
- **Rule-based Access Control**:
    - Generic term for **Following Rules**
        - Conditions other than who you are
    - Access is determined through system-enforced rules
        - System administrators, not users
    - The rule is associated with the object
        - System checks the ACLs for that object
    - Rule examples
        - Permitting access for an account or group to a network connection at certain hours of the day or days of the week
        - Only Chrome browsers may complete this web form

🛑 Rule Based Access Control (RBAC) introduces acronym ambiguity by using the same four letter abbreviation (RBAC) as Role Based Access Control. Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator.

🛑 **Access is defined by ACL, Access Control List**. 🛑 **Implicity deny** prevents access unless specifically permitted.

File system security

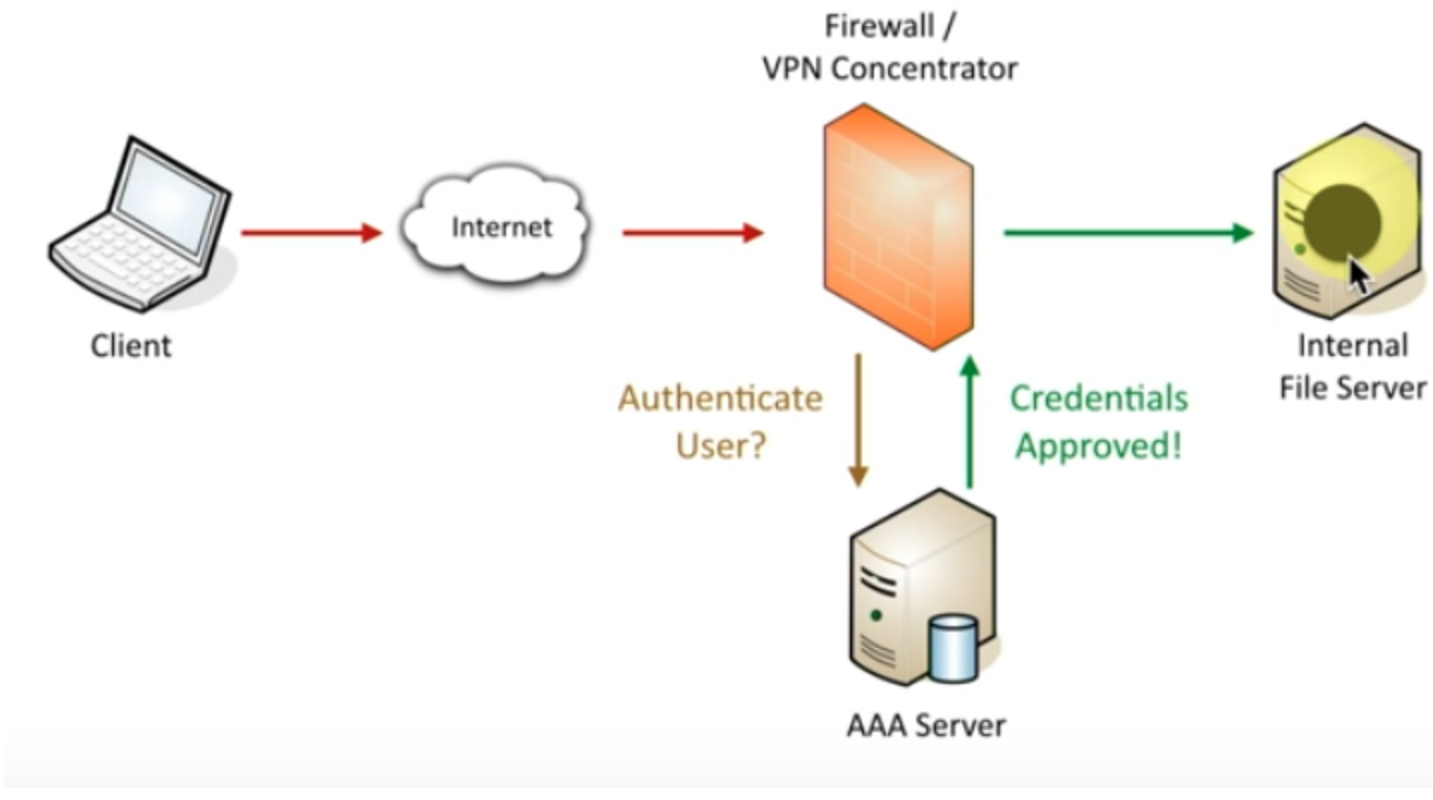
- Store files and access them
    - Hard drives, SSDs, flash drives, DVDs
    - Part of most OS's
- Accessing information
    - ACL - Access Control List
    - Group/User rights and permissions
    - Can be centrally administred and/or users can manage files they own
- Encryption can be built-in
    - The file system handles encryption and decryption

Database security

- Databases have their own Access Control
    - Username, password, permissions
- Encryption may be an option
    - Most databases support data encryption
- Data integrity is usually an option
    - No data is lost because of a fault
    - Part of the database server operation
- Applications can provide a secure front-end
    - Prevent SQL injections and inappropriate access to data

Triple AAA

Authentication, Authorization and Accounting



Two most popular protocols of triple AAA is RADIUS and TACACS+, providing centralized **Authentication**, **Authorization** and **Account management and registry logging** for computers to connect and use a **network service** securely.

RADIUS or TACACS+ server resides on a remote system and responds to queries from clientes such as VPN clients, wireless access points, routers and switches.

How RADIUS and TACACS+ works:

1. **[Authentication]** -> The server authenticates **username and password**
2. **[Authorization]** -> Determine if a user is **allowed to connect** to the client
3. **[Accounting]** -> **Log** the connection

RADIUS - Remote Authentication Dial-In User Service

Used for network access

1. **Radius Server**: Get the stack of usernames and passwords (can be MySQL, AD/DS, etc.)
2. **Radius Client**: The Gateway between users and servers
3. **Radius Supplicant**: The person that want to authenticate

RADIUS can use up to 4 different ports: Ports used by RADIUS | :-:|- **1812** | **1813** | **1645** | **1646** |

TACACS+ - Terminal Access Controller Access-Control System Plus

Is really good to manage a big number of network devices.

Provide the same as RADIUS but the service decouple the authorization from the authentication. Manages the authorization better than RADIUS.

- **Uses TCP Port 49**
- **TACACS encrypts all information** between the client and server.
- **RADIUS only encrypts the passwords**

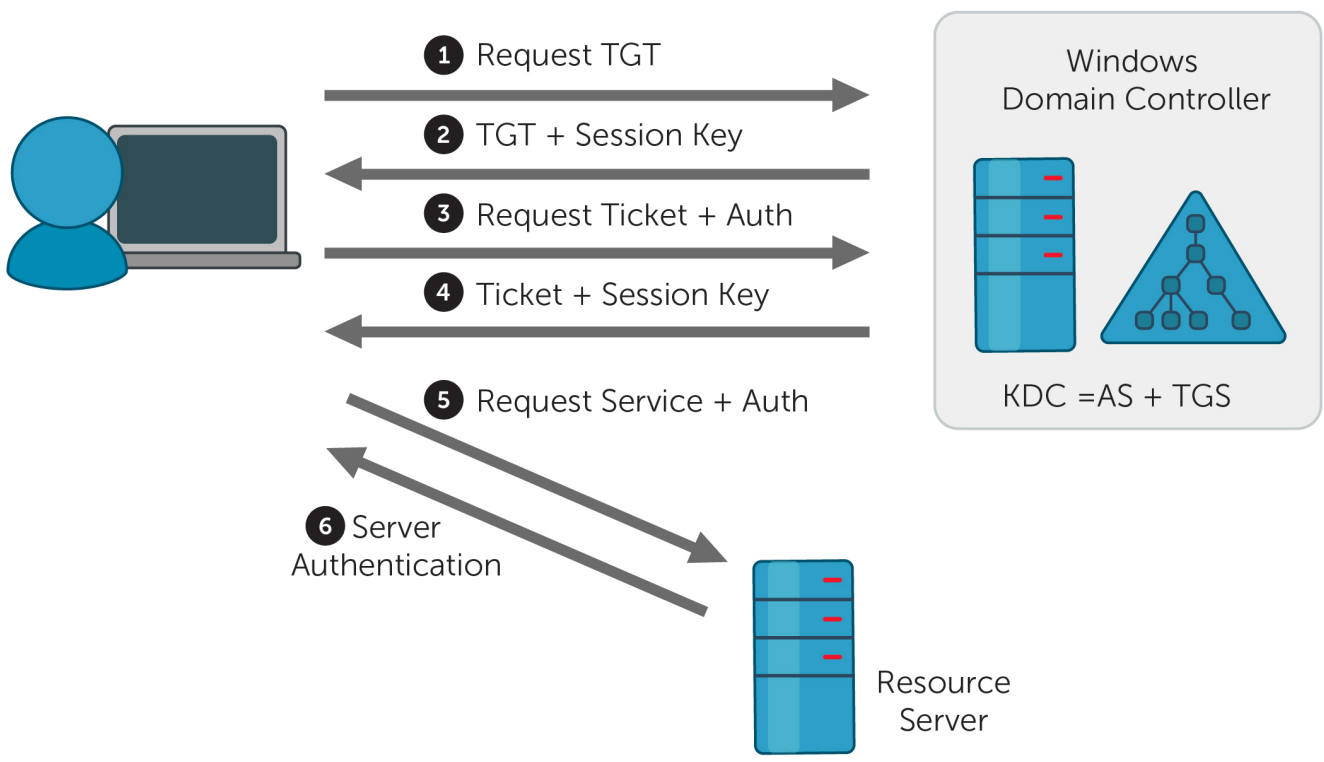
Authentication Methods

- **PAP** - *Password Authentication Protocol*
  - Is the oldest authentication method. PAP sends username and password **in the clear / plaintext**
- **CHAP** - *Challenge Handshake Authentication Protocol*
  - Uses a hash value of challenge message to authenticate
- **NTLM** - *NT LAN Manager* for Windows
  - Similar to the CHAP; uses a challenge hashed message with a different process than CHAP
  - 🛑 NTLM is vulnerable to a credentials forwarding attack (use credentials of one computer to gain access to another) -> Most secure systems migrate to Kerberos

Kerberos for Active Directory Domain Services (AD DS)

1. Authenticator (Encrypted with user's password)
2. TGT (Encrypted with KDC's key) [ticket-grant-ticket]
3. Resource Ticket (Encrypted with Resource's key by the KDC and issued to the user)
4. Resource Ticket used by Client to access the resources

🛑 **Uses Port 88**



SAML - Security Assertion Markup Language

Used exclusive for **Web Application**

LDAP - Lightweight Directory Access Protocol

Query Directories: Structured language that allows one computer to go into somebody's directory and query, update...

🛑 **Uses TCP/UDP Port 389**

Single Sign-On

Authenticate one time - gain access to everything

- **LAN**: Windows Active Directory is dominant for **security SSO**
- **SAML**: SSO for **Web Application** / used to manage multiple apps using a single account

PPP - Point-to-Point Protocol

In computer networking, Point-to-Point Protocol (PPP) is a data link layer (layer 2) communications protocol between two routers directly without any host or any other networking in between. It can provide connection authentication, transmission encryption, and compression.

- Transport layer protocol
    - Initiate connection
    - Get address information
    - Make connection
- Poor authentication mechanisms:
    - PAP - password authentical protocol (passwords in the clear)
    - CHAP - Challenge handshake authentication protocol - (use of hashing)
    - MS-CHAP (Microsoft CHAP)

Accounts Types 👤

User accounts

- This is the account type most people will use
- Storage and files can be private to that user
- No privileged access to the OS

Shared accounts

- Used by more than one person/guest login, anonymous login
- Very difficult to create an audit trail
- Password management becomes harder
- Best practice is simply DON'T use these dumb type of accounts

Service accounts

- Used exclusively by services running on a computer
    - No interactive/user access(ideally)
    - Web server, database server, etc
- Access can be defined for a specific server
    - Web server rights and permissions will be different than a database server
- Commonly use usernames and passwords using policy to determine best passwords practices

Privileged accounts

- Administrator, Root
- Complete access to the system
- This account should NOT be used for normal administration
- Needs to be HIGHLY secured - Strong passwords, 2FA, scheduled password changes

User Account Management

Least privilege

- Rights and permissions should be set to the bare minimum
  - You only get exactly what's needed to complete your objective
- This is apply to all users in the organization
- All users accounts must be limited
  - **Applications should run with minimal privileges**
- **Don't allow users to run with administrative privileges**
  - Limits the scope of malicious behavior

🛑 **Privilege creep** - when someone get a bunch of new privileges unecessarily; gradual accumulation of access rights beyond what an individual needs to do his or her job.

Continuous Access Monitoring

Monitoring all users account activity

- Track Log on and Log off activity
- Track file access

🛑 **Shared Accounts = BAD!!!**

🛑 **Multiple Accounts = Use different user/pass**

🛑 **Use least privilege - enough necessary to accomplish task**

🛑 **Monitor and log activity of users with multiple accounts (LOG EVERYTHING)**

🛑 **Avoid default usernames on user accounts**

Access Control Technologies

Proximity Cards

- Close range card - contactless smart card
- Passive deivce
  - No power in the card - powered from the reader
- Not a large data storage device
  - Often used as an identifier
  - Keycard door access, library cards, payment systems
  - The identifier is linked to data stored elsewhere

Smart cards

- Integrated circuit card - contact or contactless
- Common on credit cards - Also used for access control
- Must have physical card to provide digital access - a digital certificate
- Multiple factors - use the card with a PIN or fingerprint

Biometrics

- Fingerprints
- Facial Recognition
- Vocal Recongnition
- Can lock and unlock devices
- Use to configure applications
- **Biometric acceptance rates**:
  - **False acceptance rate (FAR) - Type II**
    - Likelihood that an unauthorized user will be **accepted** (This would be bad)
  - **False injection rate (FRR) - Type I**
    - Likelihood that an authorized user will be **rejected**
  - **Crossover error rate (CER)**
    - The rate at which FAR and FRR are equal
    - Adjust sensitivity to equalize both values
    - Used to quantitatively compare biometric systems

🛑 **Type II and Type I errors** - In statistical hypothesis testing, a type I error is the rejection of a true null hypothesis (also known as a "false positive" finding or conclusion), while a type II error is the non-rejection of a false null hypothesis (also known as a "false negative" finding or conclusion). 🛑 **FAR and FRR** can apply to many softwares that uses authentication and authorization methods.

Token generators

- Pseudo-random token generators - useful authentication factor
- Carry around a physical hardware token generator
- Use software-based token generator on your phone

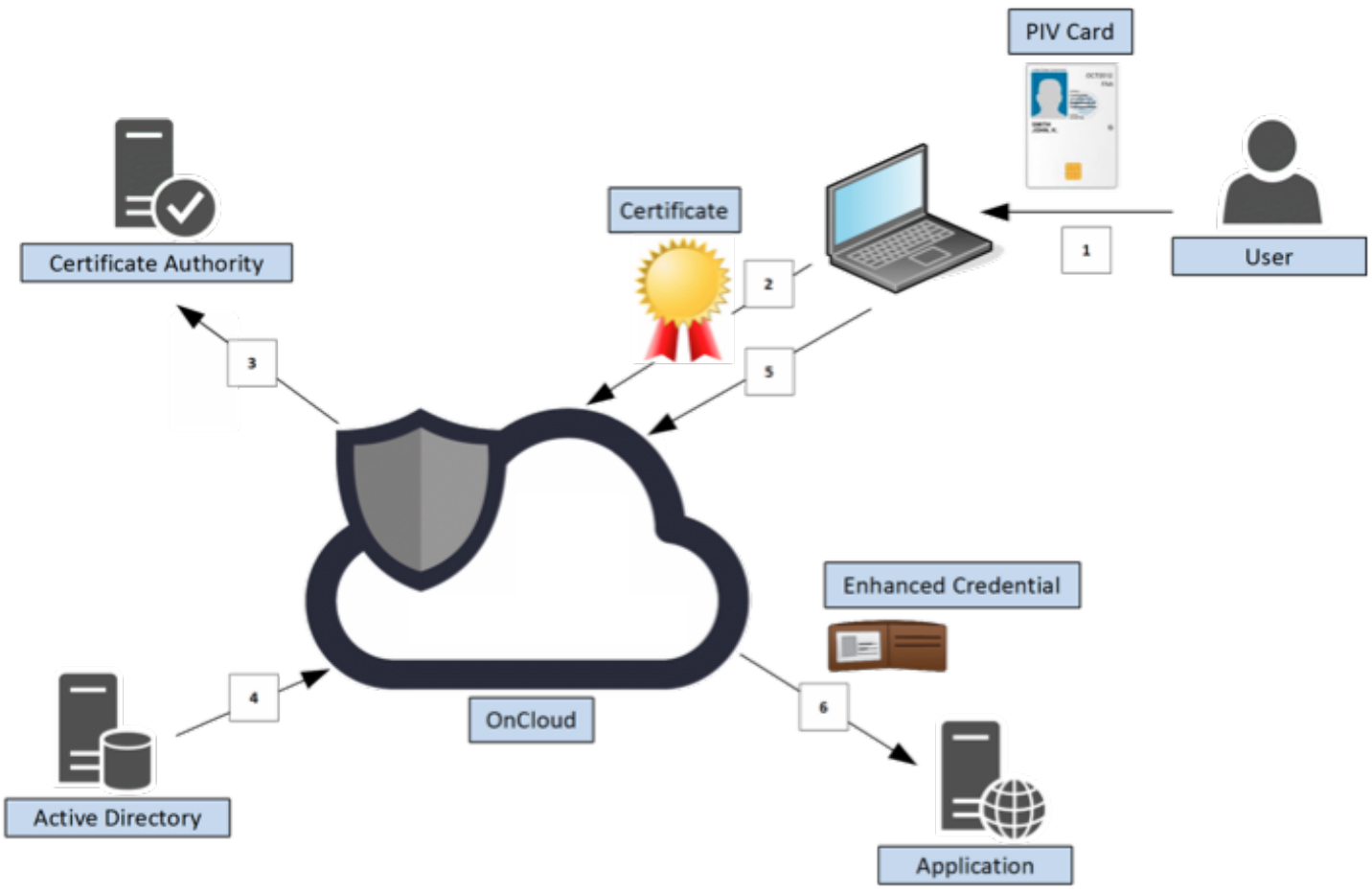
HOTP - HMAC-based One-time Password algorithm

- One-time passwords
  - Use them once, and never again
  - Once a session, once each authentication attempt
  - Keyed-hash message authentication code (HMAC)
  - The keys are based on a secrete key and a counter
- Token-based authentication
  - The hash is different every time
- Hardware and software tokens available

TOTP - Time-based One-Time Password algorithm

- Use a secret key and the time of day
- No incremental counter
- Secret key is configured ahead of time
  - Timestamps are synchronized via NTP
- Timestamp usually increments every 30 seconds
  - Put in your username, password, and TOPT code
- One of the more common OTP methods used by Google, Facebook, Microsoft, etc

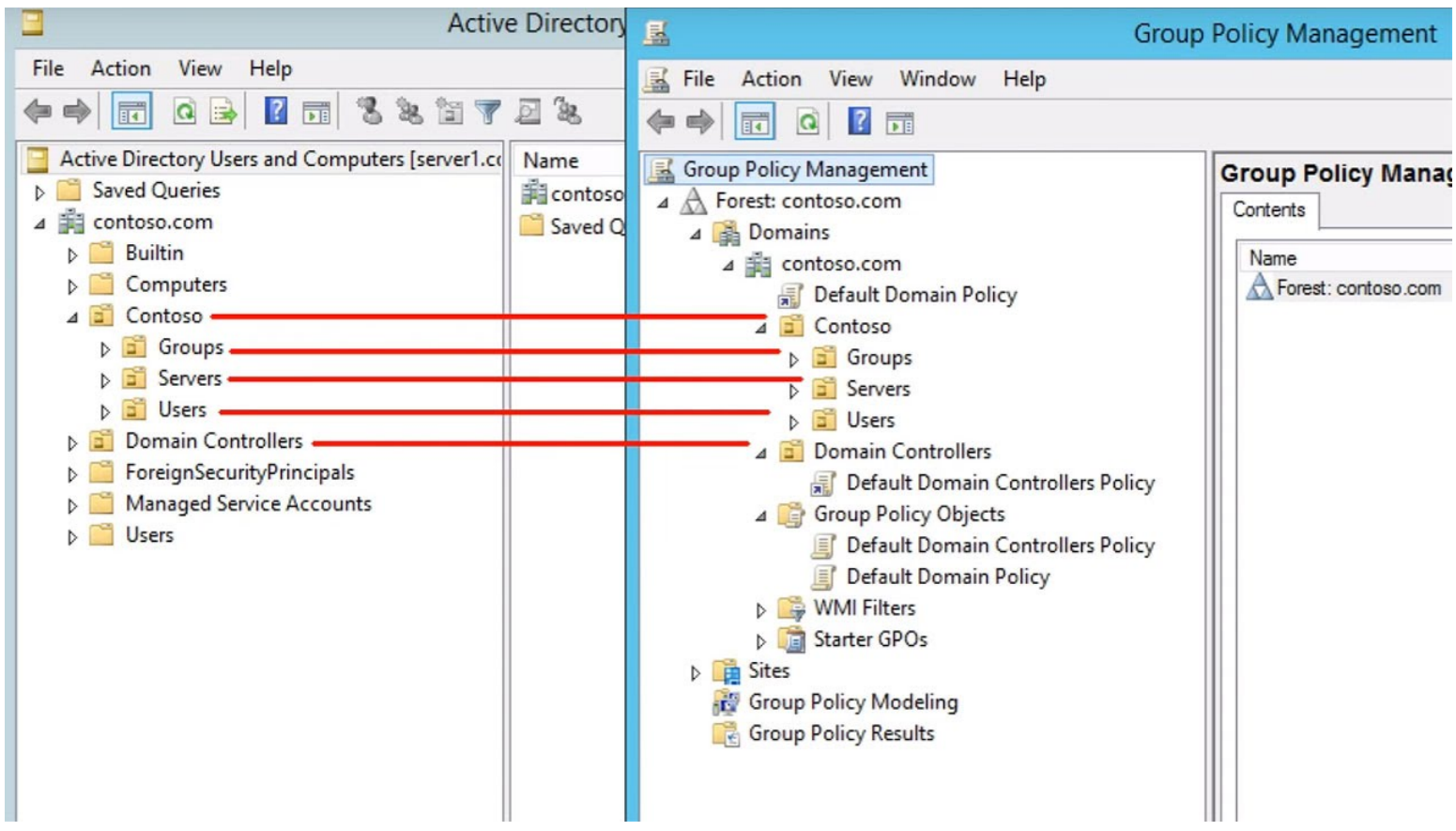
Certificate-based authentication



- Smart card
- **PIV** (Personal Identity Verification) card
  - US Federal Government smart card
  - Picture and identification information
- **CAC** (Common Access Card)
  - US DoD smart card
  - Picture and ID
- IEEE 802.1X
  - Gain access to the network using a certificate on device storage or separate physical device

Account Policy Enforcement

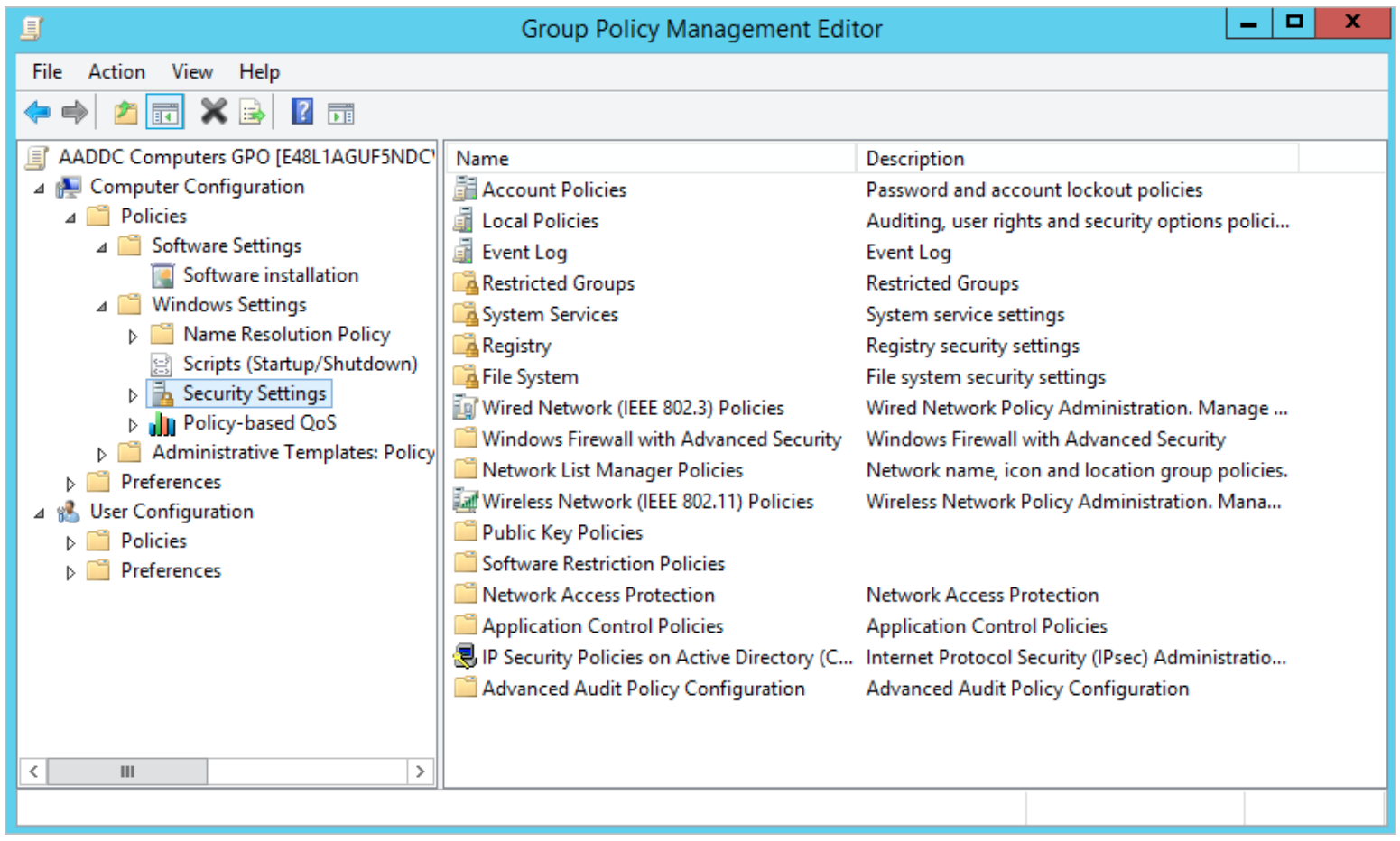
Windows Group Policy Management



- Apply security and admin setting across many computers
- Different than NTFS or Share permissions that control the use of the OS
- **Linked to Active Directory administrative boundaries**
  - Sites, Domains, Organization Units (OUs)

- Define by Groups, Locations, etc

Group Policy Management Editor - Windows

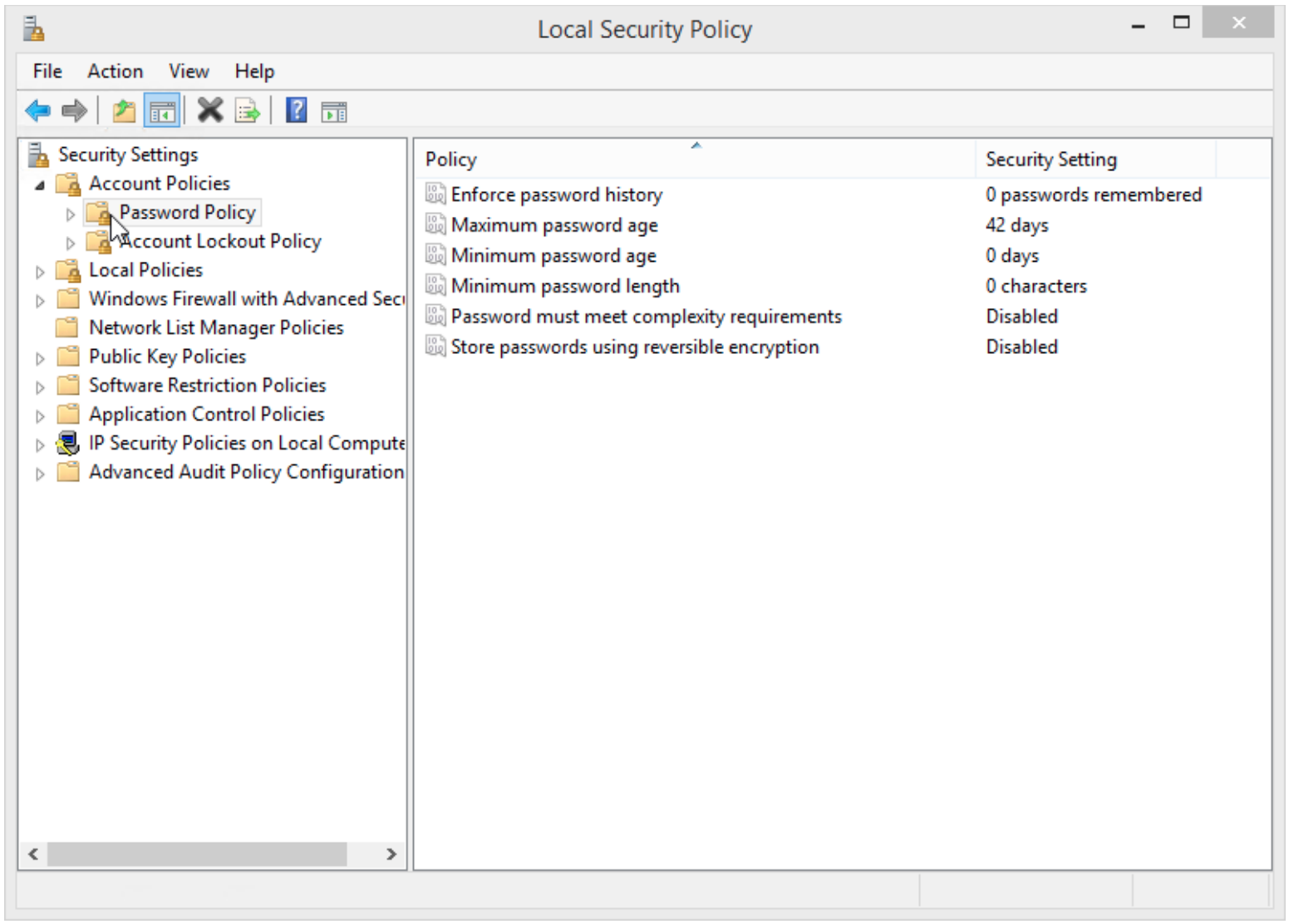


- **Administrative Policies**
  - Remove add or Remove Programs
  - Prohibit changing sounds
  - Allow font downloads
  - ONly allow approved domains to use ActiveX controls without prompt
- **Security Policies**
  - Specify minimum password length
  - Require smart card
  - Maximum security log size
  - Enforce user login restrictions

Password Security

1. **Complexity**
   - Length and character requirements
2. **Expiration**
   - Reset and time triggers
3. **Password history**
   - Reusage and retention

Local Security Policy - Password Policy - Windows



- **Enforce Password History**: determine the number of new unique passwords [1-24]
- **Maximum Password Age**: Password age [1-999 days]
- **Minimum Password Age**: Limit until request password change [1-998 days]
- **Maximum Password Lenght**: [1-20 characters]
- **Password Complexity:**
  - Not contain user account name or parts of full name
  - At least 6 characters lenght
  - At least three of four categories:
    - Uppercase [A-Z]
    - Lowercase [a-z]
    - Base 10 digits [0-9]
    - Non-alphabetic characters [!,@,#,$,...]

Account Lockout Policy

- **Account Lockout Duration**: Time (in minutes) for a locked-out account [0-99,999]
- **Account Lockout Threshold**: Number of failed logon attempts [0-999]
- **Reset Account Lockout Duration**: Period of time that must elapse before the account lockout counter is reset to 0 bad logon attempts. [1-99,999]

🛑 **Local Security Policy** applies policies for the host machine/local. 🛑 **Group Policy Management** applies policies for the organization through Active Directory Domains, Groups, OUs, etc.

1. Good practices - Password complexity

- AVOID single words or obvious passwords
  - Name of dog, parent, partner
- Use upper, lower case and special characters on each password
- At least 8 characters
  - Consider a phrase or set of words
- Prevent password reuse
  - System remember password history, requires unique passwords

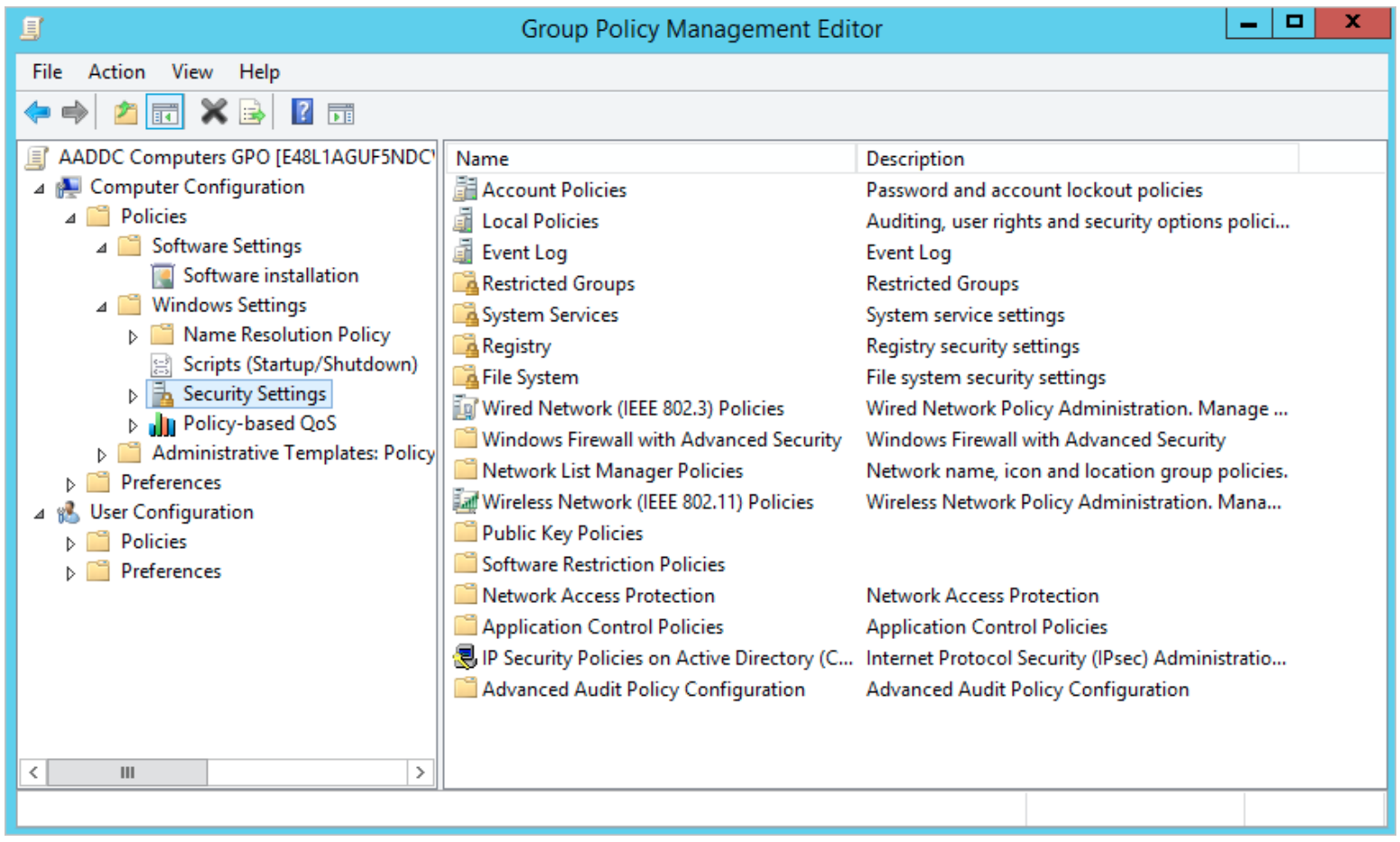
1.1 Good practices - Password expiration and recovery

- All passwords should expire
    - Change every **30 days, 60 days, 90 days**
- Critical systems might change more frequently
    - Every 15 days or every week
- The recovery process should NOT be trivial!
    - Some organizations have a very formal process

1.2 Good practices - Account lockout and disablement

- Always turn on the policy of Account Lockout to avoid brute-force try out
- Disable accounts is better than Delete account; Often users save data, encryption keys, etc; Makes easier to retrieve this information.

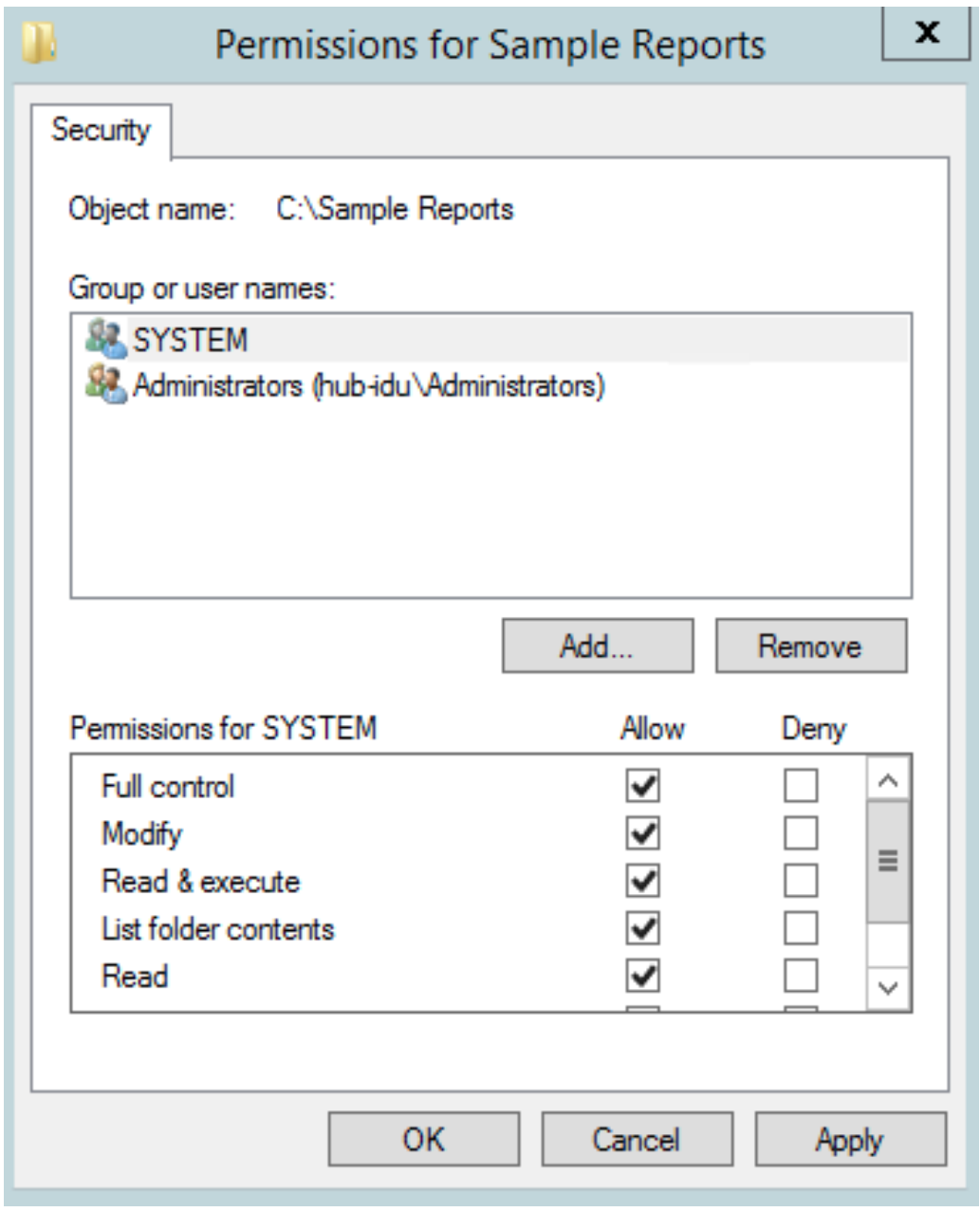
Group Policy Objects (AD DS)



- Set of rules that allow an administrator granular control over the configuration of objects in Active Directory, including user accounts, operation systems, applications and other AD objects. Can apply over multiple domains, groups and OU's.

Permissions - Windows

NTFS permissions are granted to users and groups on folders and files.



NTFS Permissions - Folder

- **Full Control** - Anything
- **Modify** - Read, Write and Delete Files and Subfolders
- **Read/Execute** - See contents and Run Programs
- **List** Folder Contents - See Contents of Folders and Subfolders
- **Read** - View Contents and Open data files
- **Write** - Write to Files and Create new files and folders

NTFS Permissions - File

- **Full Control** - Anything
- **Modify** - Read, Write and Delete files
- **Read/Execute** - Open and Run the file
- **List** Folder Contents - Open the file See Contents of Folders and Subfolders
- **Read** - Open the file
- **Write** - Open and Write to the file

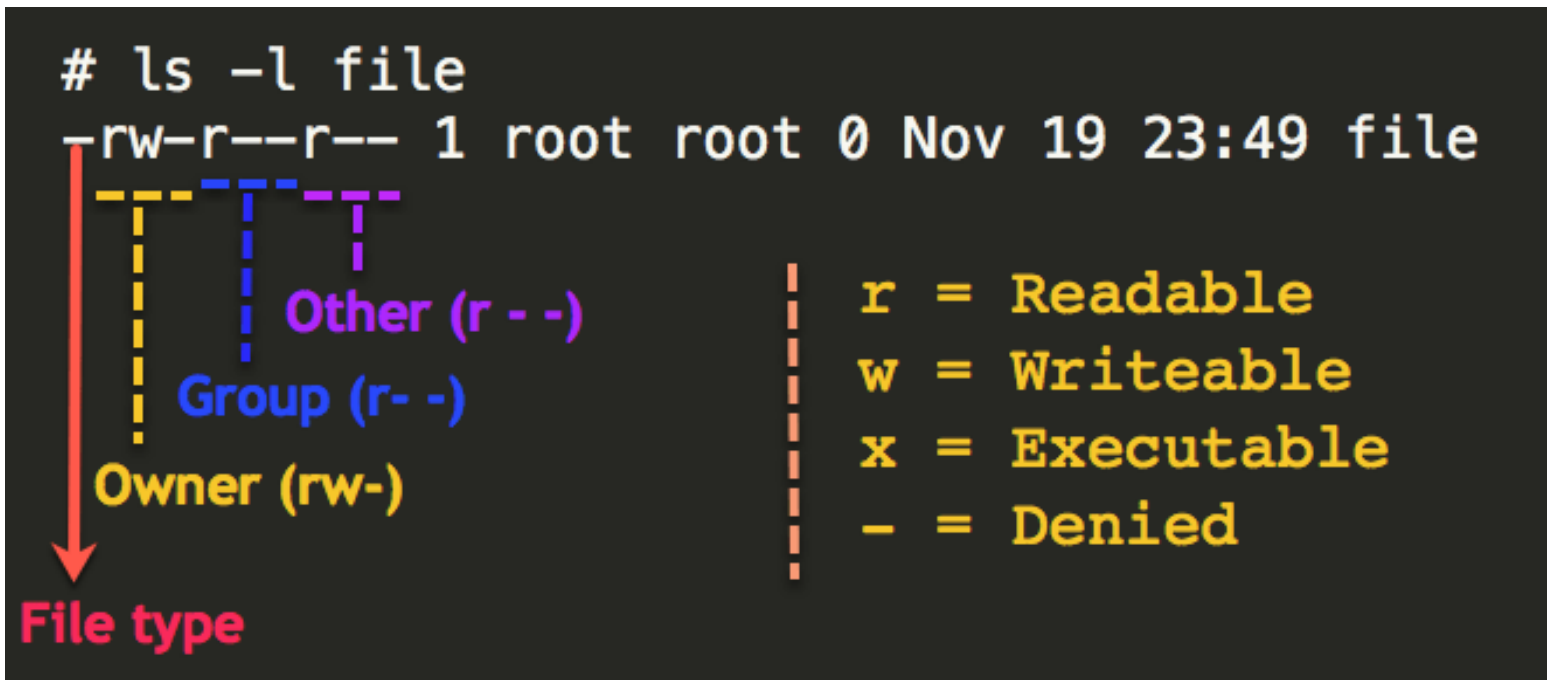
> 🛑 **Deny is stronger than allow**.

Moving and Copying NTFS Objects

1. **Copy and Move** from drive X: to Y: - will take the NTFS permissions of the **destination** drive.
2. **Copy** from drive X: to the same drive X: - **will loose the NTFS permissions.**
3. **Move** from drive X: to the same drive X: - **will inheritance the NTFS permissions**

Permissions - Linux

Linux has three permissions and they can be set for the owner, group or other.



r = read - open a file, view a file. **w = write** - edit a file, add or delete files for directories. **x = execute** - run a file, execute a program or script, CD to a different directory.

Owner	Group	Other
rwx	rwx	rwx

- Viewing the permissions on Linux command-line:

```
ls -l
```

```
-rwxrwxr-x 1 user user 31337 Feb 11 13:13 File
```

Using `chmod`

`chmod` *is the command and system call which is used to change the access permissions of file system objects on Unix and Unix-like OS.*

- Clear out the permissions of the **File** to have no read, write and execute permissions on **Other**:
  (The flag equals to nothing[o=] deny the permissions)

```
ls -l
```

```
-rwxrwxr-x 1 user user 31337 Feb 11 13:13 File
```

```
chmod o= File
```

```
ls -l
```

```
-rwxrwx--- 1 user user 31337 Feb 11 13:13 File
```

- Giving **read** and **write** permissions to **Group**:

```
ls -l
```

```
-rwx---r-- 1 user user 31337 Feb 11 13:13 File
```

```
chmod g=rw File
```

```
ls -l
```

```
-rwxrw-r-- 1 user user 31337 Feb 11 13:13 File
```

- Giving **all permissions** to everybody(Owner,Group and Other):

```
ls -l
```

```
-rwx---r-- 1 user user 31337 Feb 11 13:13 File
```

```
chmod a=rwx File
```

```
ls -l
```

```
-rwxrwxrwx 1 user user 31337 Feb 11 13:13 File
```

Using `chmod` on oldschool way:

The chmod command will take the octal value and combine them to associate the permissions on three different positions for the Owner, Group and Other/Everyone. This boils down to a simple binary rule: 0 = off | 1 = on.

Octal	Binary	Permissions
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwx

If you want to give all permissions to a group for example, the number will be 7 (4 + 2 + 1).

Read	Write	Execute

Read	Write	Execute
r--	-w-	--x
4	2	1

Examples:

- Giving **read, write and execute** permission to everybody:

```
ls -l
```

```
-rwx---r-- 1 user user 31337 Feb 11 13:13 File
```

```
chmod 777 File
```

```
ls -l
```

```
-rwxrwxrwx 1 user user 31337 Feb 11 13:13 File
```

- Giving all permissions to the **owner**, read and write to **group** and no permissions to **other/everyone**:

```
ls -l
```

```
-r-x---r-- 1 user user 31337 Feb 11 13:13 File
```

```
chmod 760 File
```

```
ls -l
```

```
-rwxrw---- 1 user user 31337 Feb 11 13:13 File
```

Linux - File Ownership using `chown` (change file owner and group)

```
ls -l
```

```
-rwxrwxrwx 1 user001 user001 31337 Feb 11 13:13 File
```

```
sudo chown root File
```

```
ls -l
```

```
-rwxrwxrwx 1 root user001 31337 Feb 11 13:13 File
```

The chown command requires sudo

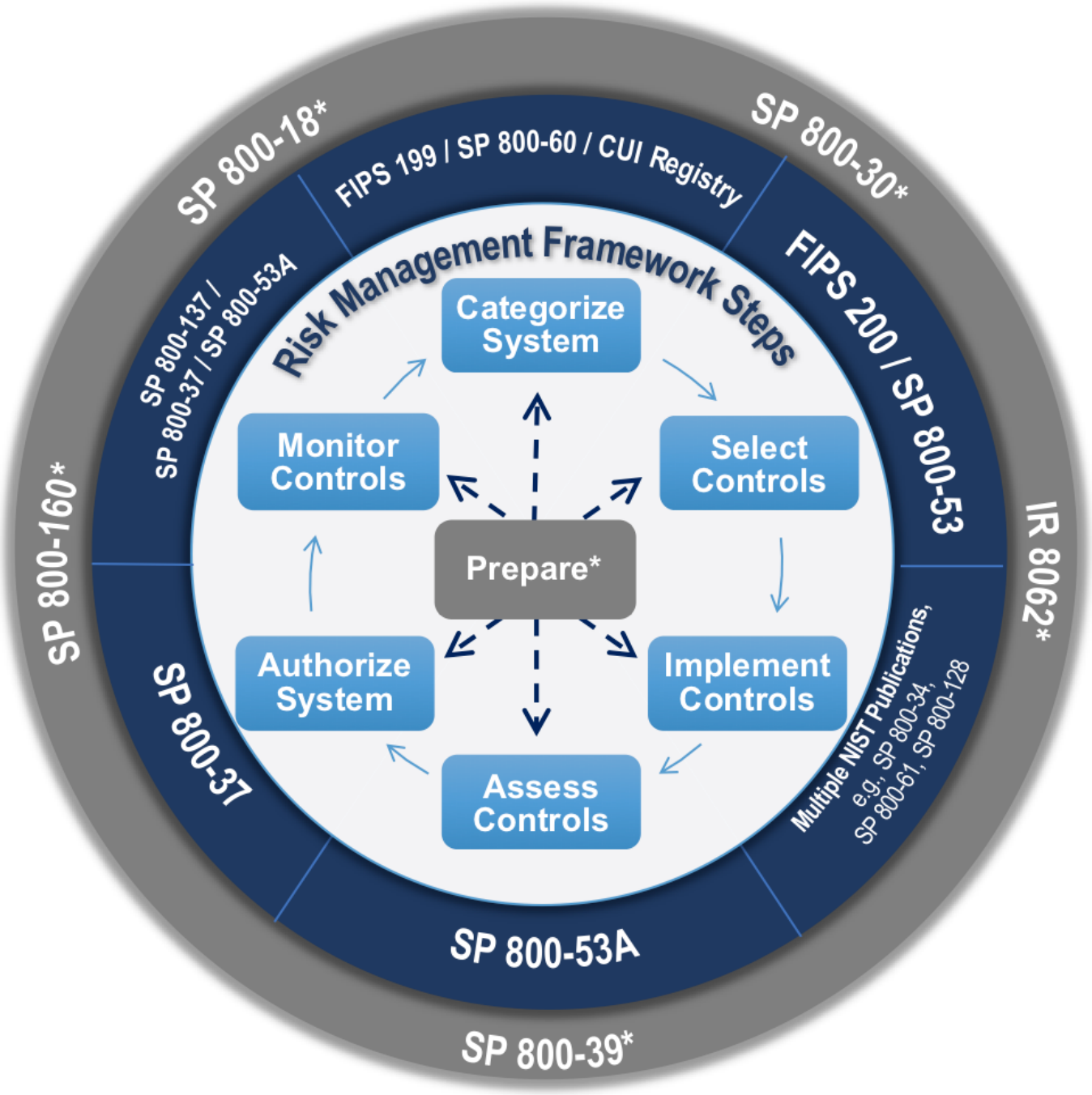
Linux - Changing the Password using `passwd`

```
sudo passwd
```

---

5. Risk Management

Risk management is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.



Defining Risk

- **Vulnerability:** A weakness; System flaw.
- **Threat:** Exploit vulnerabilities to harm assets.
- **Risk:** The likelihood of a THREAT exploiting a VULNERABILITY, resulting in a loss.

Formula:

THREATS x VULNERABILITY = RISK OR THREATS -> VULNERABILITY = RISK

1) Asset:

Is a part of an IT infrastructure that has a value. You can measure value either tangibly or intangibly. A gateway router is an example of an asset with tangible value, if it fails, you can easily calculate the cost to replace the router.

Example of assets:

Asset	**Info.**
Servers	The computers that offer shared resources
Workstations	The computers users need to do their job
Data	The stored, proprietary information an organization needs to operate
Applications	Specific programs an organization needs to use
Personnel	The people who work in an organization
Wireless access	Wireless access to the network
Internet services	The public or private-facing resources an organization provides to customers, vendors, or personnel via the Web or the Internet applications

2) Probability

Probability means the likelihood - over a defined period of time - of someone or something damaging assets.

Quantitative likelihood: *based on numbers and data, can be more easy to measure anually.*

Qualitative likelihood: *is more subjective like - LOW | MEDIUM | HIGH.*

3) Threat actors

A threat actor can be a malicious person, such as a hacker accessing corporate secrets.

The exam cover six types of threat actor:

1. **Script Kiddies**
    - Can be external or internal
    - Not Very sophisticated

    - Runs pre-made scripts without any knowledge of what's really happening

2. **Hacktivists**

    - Hacker + Activist
    - A hacker with a purpose - social change or a political agenda
    - Can be sophisticated
    - DoS, Web Site Defacing, Information Disclosure, Leaking private documents.

3. **Organized Crime**

    - Professional Criminals
    - Motivated by Money
    - Very sophisticated
    - Crime that's organized
        - *One person Hacks*
        - *One person Manages the exploits*
        - *One person Sells the data*
        - *Another Handles customer support*
    - Lots of capital to fund hacking efforts operational

4. **Nation States / APT**

    - Governments - National Security, Job Security; Always an external entity
    - Highest sophistication
        - Military control, utilities, financial control
    - Constant attacks, massive resources
        - Advanced Persistent Threat

5. **Insiders**

    - Has institutional knowledge
        - Attacks can be directed at vulnerable systems allowing the bad guy what, when and how to hit
    - Can be sophisticated
    - Extensive resources

6. **Competitors**

    - Many different motivaions - Espionage, harm reputation
    - High level of sophistication
    - Many different intents
        - Shut down your competitor during an event
        - Steal customer lists
        - Corrupt manufacturing databases
        - Take financial information

Risk Assessment

1. Vulnerability Assessment

- NIST SP 800-30
- CVE (Common Vulnerabilities and Exposures)
- Nessus scanner
- Penetration Testing

2. Threat Assessment

- **Environmental**: Natural disasters outside the control of humans
- **Manmade**: Any threat that is not environmental

- **Internal**: Threat generated by internal sources, usually an insider to the organization
- **External**: Threat generated from outside your infrastructure

Risk response techniques

After identified and analyzed risk, you must decide how to responde to the risks produced as a result of the analysis.

1) Risk Mitigation

Is an attempt to reduce the risk, or at least minimize its effects on an asset.

2) Risk Transference

Or Risk Sharing, deals with risk by sharing with third-party. Example buying insurance to protect against natural disasters.

3) Risk Acceptance

Means the organization has implemented controls and some risk remains **(residual risk)**. Remember that risk can never be completely eliminated.

> 🛑 **Residual risk** is what risk remains after all mitigation and reduction strategies have been implemented.

4) Risk Avoidance

Means thtat the organization could choose not to participate in activities that cause unnecessary or excessive risk.

Change management

Provide more uptime availability and decrease the risk for the entire organization.

- How to make a change
  - Upgrade software, change firewall configuration, modify switch ports
- One of the most common risks in the enterprise
  - Occurs very frequently
- Often overlooked or ignored
- Have clear policies
  - Frquency, duration, installation process, fallback procedures

Risk Frameworks

- NIST - Risk Management Framework SP 800-37
- ISACA Risk IT Framework

Security Controls

Control Types

The cornerstone of IT security is understanding security controls and how to apply them.

1. **Administrative Control** (People -> IT Security)
    - Laws
    - Policies
    - Guidelines
    - Best Practices
2. **Technical Control** (IT Systems -> IT Security)
    - Computer stuff
    - Firewalls
    - Password links
    - Authentication
    - Encryption
3. **Physical Control** (Physical World)
    - Gates
    - Guards
    - Mantraps
    - Keys

Activity Phase Control Types

1. **Deterrent control**: Deters the actor from **attempting** the threat. *(Warning Sign, SSH Login Banner)*
2. **Preventive control**: Deters the actor from **performing** the threat. *(Fence, Server Locks, Password Complexity, Firewall)*
3. **Detective control**: Recognizes an actor's threat. *(Background check, CCTV, IDS/IPS)*
4. **Compensating**: Provides alternative fixes to any of the above functions
5. **Corrective**: Mitigates the impact of a manifested threat. *(Backups can mitigate a ransomware; IPS can block an attacker)*

*Most of security controls are **preventive** phase controls*

Another Security Controls

- Mandatory Vacation
- Job Rotation
- Multi-person Control
- Separation of Duties
- Principle of Least Privilege

Defense-in-Depth

Every IT infrastructure might be looked at as a series of concentric shells. The location of these shells depends on the types of threats you are mitigating.

Defense in Depth uses **administrative, physical and technical controls**.

1) Physical Controls

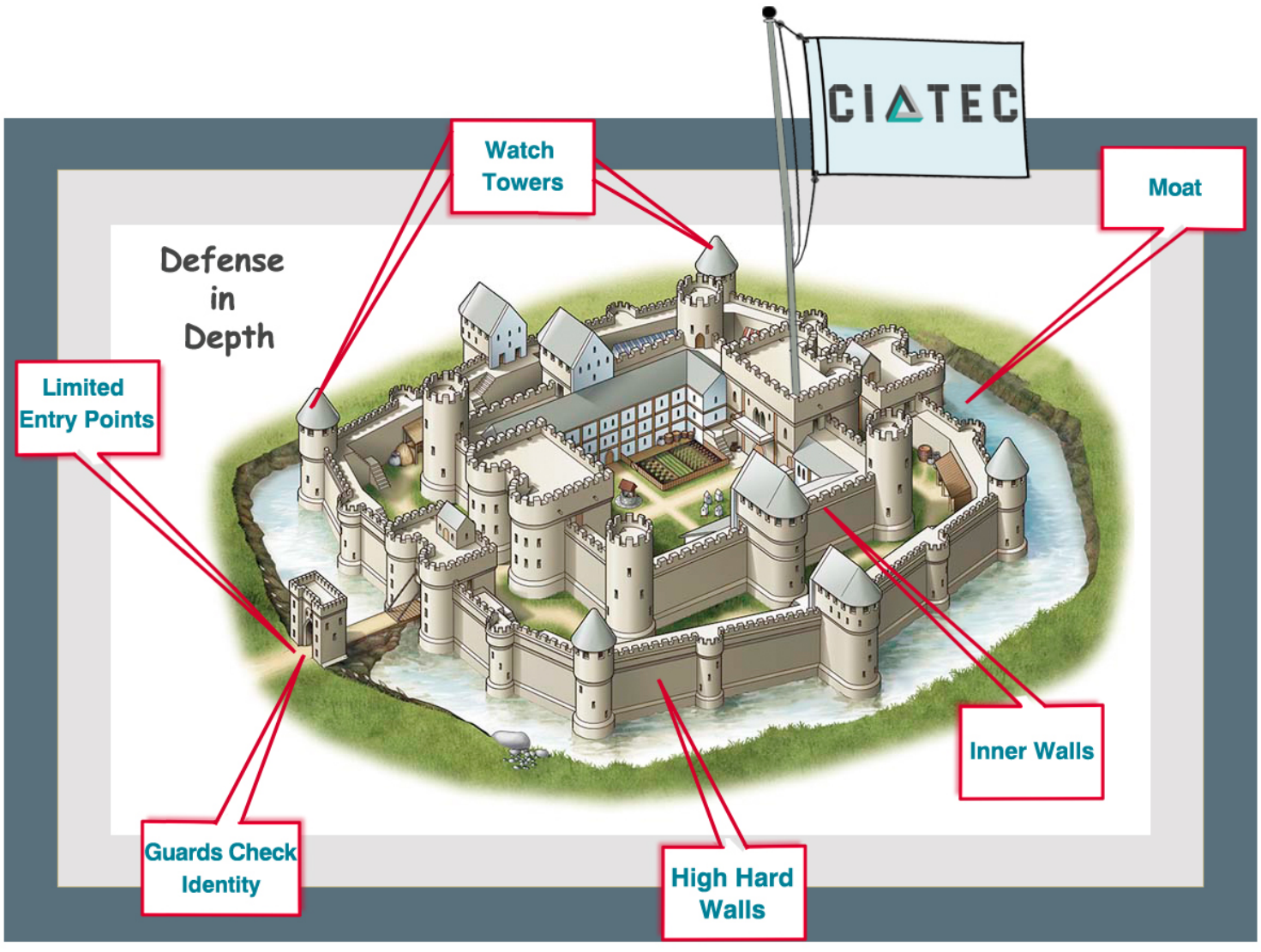
- Door locks, fences, rack locks, cameras, mantraps

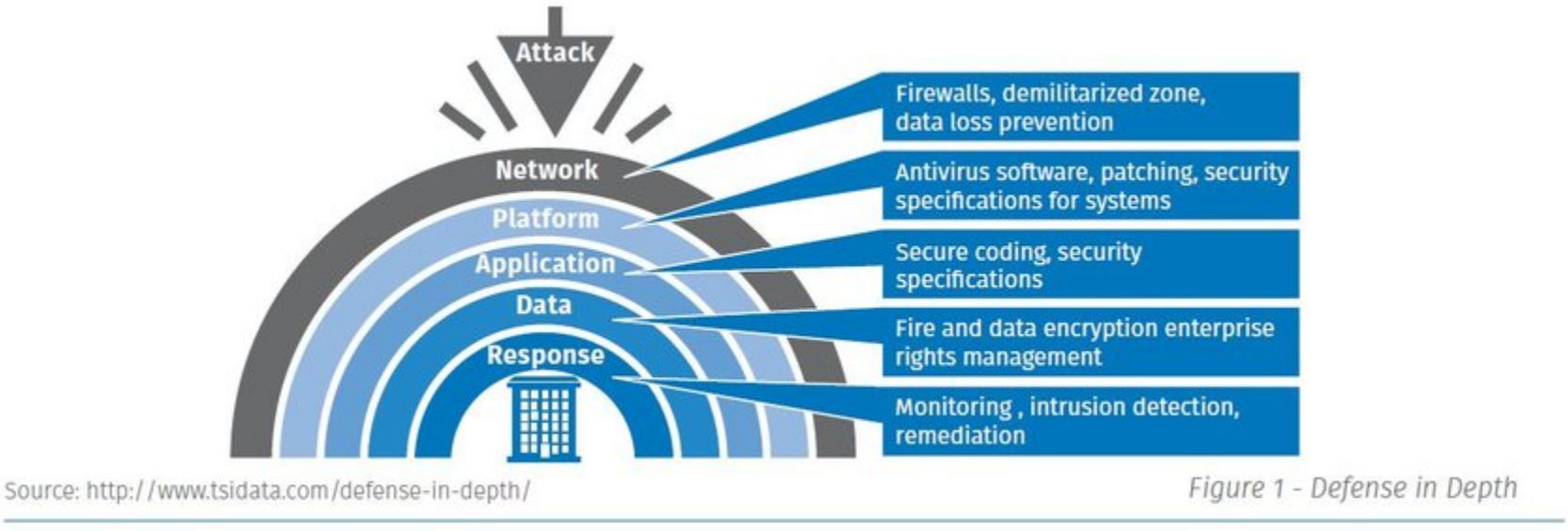
2) Technical Controls

- Hardware and software to keep things secure
- Firewalls, active directory authentication, disk encryption

3) Administrative Controls

- Policies and Procedures
- On boarding and off boarding
- Backup media handling





Source: http://www.tsidata.com/defense-in-depth/

Figure 1 - Defense in Depth

Redundancy

Repeating the same controls at various intervals.

Diversity

Try different set of security controls in a random pattern.

- **Vendor Diversity**: Uses several vendors to supply equipament and services.

IT Governance

All about rules and requirements applied to an organization that dictate how it conducts business, protects data, and obeys the law. Governance comes in the forms of laws, regulations, internal rules, and industry standards.

- Influences how the organization conducts IT security.
- In its most core function is to actually make the right set of security controls.

1. **Laws and Regulations**
    - Regulations:
        - **HIPAA - Health Insurance Portability and Accountability**, (USA); Extensive healthcare standards for storage, use, and transmission of health care information.
        - **SOX - Sarbanes-Oxley Act**, The Public Company Accounting Reform and Investor Protection Act of 2002.
        - **GLBA - The Gram-Leach-Bliley Act** of 1999; Disclosure of privacy information from financial institutions.
2. **Standards**
    - Governament Standards: NIST, ISO
    - Industry Standards: PCI-DSS (Payment Card Industry Data Security Standard)
3. **Best Practices**
4. **Common-Sense**

Frameworks

- Structure and organization
  - What works best for IT?
- Process management
  - Getting the IT 'product' to work best with the organization
- Best practices
  - Guidelines and examples for IT management; Cost effective, agile
- Training - for everyone

Industry-Standard Frameworks:

COBIT - Framework

Control Objectives for Information and Related Technologies

- Created by ISACA, formerly the Information Systems Audit and Control Association
- Focus on regulatory compliance, risk management and aligning IT strategy with organizational goals

ITIL - Framework

Information Technology Infrastructure Library

- Multiple stages of the IT lifecycle
- Multiple services:
  - Service Design
  - Service Transition
  - Service Operation
  - Service Strategy
  - Continual Service Improvement

🛑 By using these industry-specific frameworks, an organization can structure their IT departments to best serve the overall need of the organization.

Policies - *Document that defines how we're going to be doing something. Define Roles and Responsabilities.*

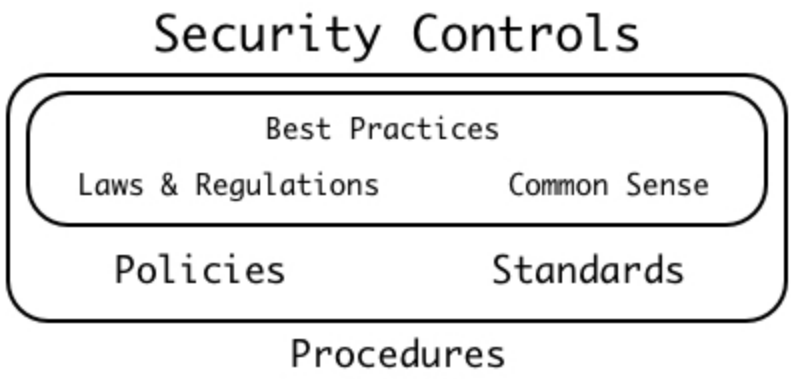
Procedures - *Step by step process of how to do something.*

- Security controls, Policies and standards help define and build the **Procedures**.

Organizational Standards

- Have much more detail than policies. Define the acceptable level of performance policy.

The security controls come from the policies and standards.



Security Policies

The Acceptable Use Policy (AUP):

- Defines what a person can or can not do when using company assets and equipament. *(The paper you sign before entry a job position).*

  🛑 An acceptable use policy (AUP) defines what users may and may not do with regard to **information systems, including e-mail**.

Data Sensitivity and Classification Policies:

- Define the importance or nature of the data. *(e.g. Applying labels on the Government, they use Top Secret, Classified, etc).*

Access Control Policies:

- How people get access to data or resources
- What type of data do users have access to.
- Data access and classification restrictions *(It cover a lot of things based on the job type).*

Password Policy:

- Password recovery
- Password retention
- Bad login attempt
- Password reuse
- Complexity

Care and Use of Equipament:

- How you maintain company equipament.

Privacy Policy:

- Are often for customers; defines how your data or usage will be shared with other resoruces. *(e.g. Services like Facebook etc).*

General Security Policies:

- **Social media policies**
  - Balance the company reputation with employee participation
  - Extension of your code of conduct
    - Define requirements and expectations
    - Identification as an employee
    - Personal responsibility
  - Confidential information
    - Public companies are legally bound
    - There's company spokesperson for public comments
- **Personal email policies**
  - Qualify the use of email - business use not personal use
  - Prohibit disruptive or offensive use
  - Compliance use
    - Some organizations are legally required to prohibit personal email
  - The line becomes hazy when browser-based email is used

Personnel Management

On boarding:

New hires or contractors

- Background check
- NDA (Non-disclosure agrement)
- Standard Operation Procedures
- Specialized Issues (e.g. Clean Desk)
- Rules of Behavior (e.g. Good AUP)

- General Security Policies (e.g. Personal Email, Social network...)

Off boarding:

When the employee leaves the company

- Disable accounts (never delete an account)
- Return Credentials
- Exit interview
- Knowledge transfer

Personnel Policies:

- Background Check
- Mandatory Vacation
- Job Rotation
- Separation of Duties
- Multi-person Control

Personnel Management Controls

- **Mandatory Vacation**:
    - Required
    - Prevents collusion
    - Dependency issues
    - Makes fraud harder
- **Job Rotation**:
    - Redundancy and Backup
    - Allows for cross-training
    - Makes fraud harder
- **Separation of Duties**:
    - Requires dual execution *(at least two people to do a sensitive function)*
- **Multi-Person control**:
    - Moren than one person required in a task/function

Role-Based Data Controls

- **System Owner**:
    - Management level role
    - Maintains security of the system (defines security policies and backup policies)
    - Defines a system administrator
    - Works with all **Data Owners** to ensure data security
- **System Administrator**:
    - Day-to-day administration of a system
    - Implement security controls
- **Data Owner**:

    - Defines the sensitivity of the data
    - Defines the protection of the data
    - Works with **System Owner** to protect data
    - Defines access to the data

- **User**:

    - Accesses and uses the assigned data responsibly
    - Has least privileged access to the application and data

- **Privileged**:

    - Has special access to data beyond the typical user (additional application and data permissions)
    - Works closely with **System Administrators** to ensure data security
    - Area manager, report creation, user and password changes

- **Executive User**:

    - **Read only** access but can look at **all business data**
    - Responsible for the overall operation of the application
    - Evaluates goals and makes decisions about future directions

Risk Management Frameworks

A framework is a description of a complex process, concentranting on major steps and the flows between the steps. **Describes the major steps and flows of the complex process of applying security controls in an organized and controlled fashion.**

Frameworks come from a variety of sources including:

- **Regulatory**
- **Non-Regulatory**
- **National**
- **Industry Standards (Best Practices)**

Popular RMF

National Standard and Regulatory:

- NIST SP 800-37

Non-Regulatory:

- ISACA IT Infrastructure

International Standard:

- ISO 27000

NIST Risk Management Framework:

Quantitative Risk Assessment

Is based on **objective data, typically numerical data**; Exact values, for instance, can be used to describe impact or loss of an asset.

Asset Value (AV)

When valuing an asset, consider not only the replacement cost, but also the revenue the asset generates, as this will be lost as well if the asset is not available.

Example:

Asset	Cost	Repair	Revenue	= Total
Router	€600	€500 x day	€2000 x day	€3100

Exposure Factor (EF)

The percentage of an asset that could be lost during a negative event. Realistically, you will not always lose 100% (1) of

the asset; you may lose only 20% (0.2) or 50% (0.5) for example.

Example:

Incident	**Exposure Value**
Flood	1 (100%)

Single Loss Expectancy (SLE)

Is the value that's computed simply by multiplying the asset's value by the exposure factor (percentage of loss).

Formula:
Single Loss Expectancy = Asset Value x Exposure Factor
SLE = AV x EF

Example (using data below):

AV	**x EF**	**= SLE**
€3100	1	€3100

SLE = €3100 (AV) x 1 (EF) = €3100

Annualized Rate of Occurrence (ARO)

How many times per year you would expect a particularly negative event to occur, resulting in a loss of the asset. **This value relates more to likelihood than impact.**

Example: Flood on Server room, base on data: one flood in about 10 years, 1/10 (0.1). [SLE x ARO = ALE]

Annualized Loss Expectancy (ALE)

Essentially looks at the amount of loss from the SLE and determines how much loss the organization could realistically expect in a one-year period.

- **Formula**:

  ALE (Annualized loss expectancy) = SLE x ARO

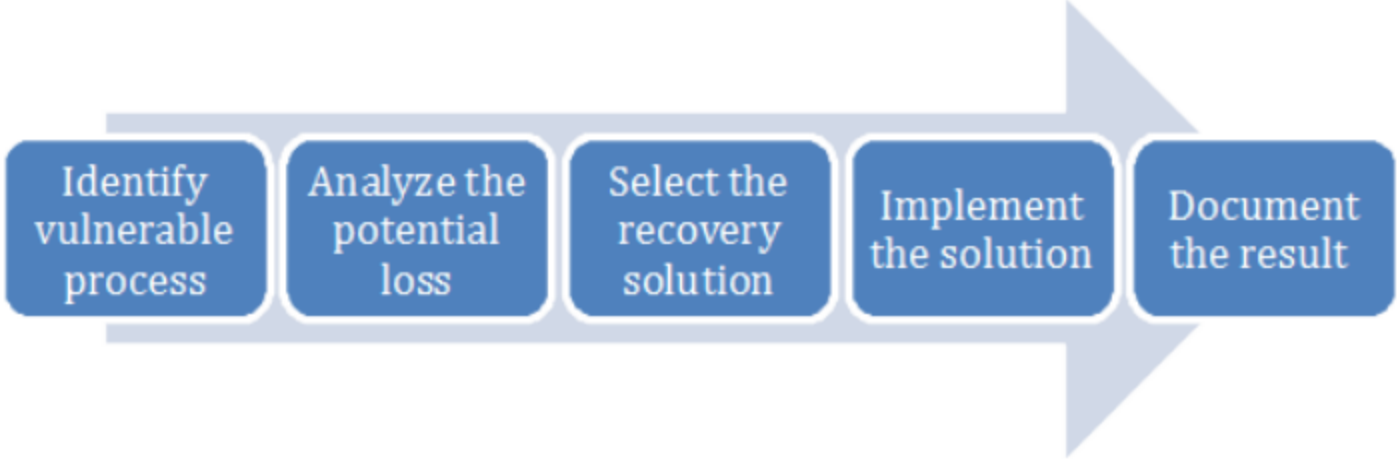
  - **SLE x ARO = ALE**

Evaluating risk

- Risk register
  - Every project has a plan, but also has risk
  - Identify and document the risk associated with each step
  - Apply possible solutions to the identified risks
  - Monitor the results
- Supply chain assessment
  - Get a product or service from supplier to customer
  - Evaluate coordination between groups

- Identify areas of improvement
- Asses the IT systems supporting the operation
- Document the business process changes

Business Impact Analysis



Designed to mitigate the effects of an incident, **not to prevent an incident**.

- Determine mission process. *(make sure servers are up)*
- Identify critical systems.
- Single point-of-failure. *(using Defense-in-Depth...)*
- Identify resource requirements.
- Identify recovery priorities. *(prioritize most important steps to kepp whatever essential function running)*

Types of Impact

- **Property**
  - The risk to buildings and assets
- **Safety | Life | People**
  - Some environments are too dangerous too work
- **Finance (Credit, Cash flows...)**
  - The resulting financial cost
- **Reputation**
  - An event can cause status or character problems
- **Privacy**
  - Some compliance requires a public privacy statement
    - Gramm-Leach-Bliley Act (financial information)
    - HIPAA (health care), etc

Privacy Impact Assessment (PIA) and Privacy Threshold Assessment (PTA)

PTA

The **first step** in the compliance process

- **Identify** business processes that are **privacy-sensitive**
- Determines if a privacy impact assessment is required

PIA

Determine the impact on the privacy of the individuals who data is beign stored; and ensure that the organization has sufficient security controls applied to be within compliance of applicable laws or standards.

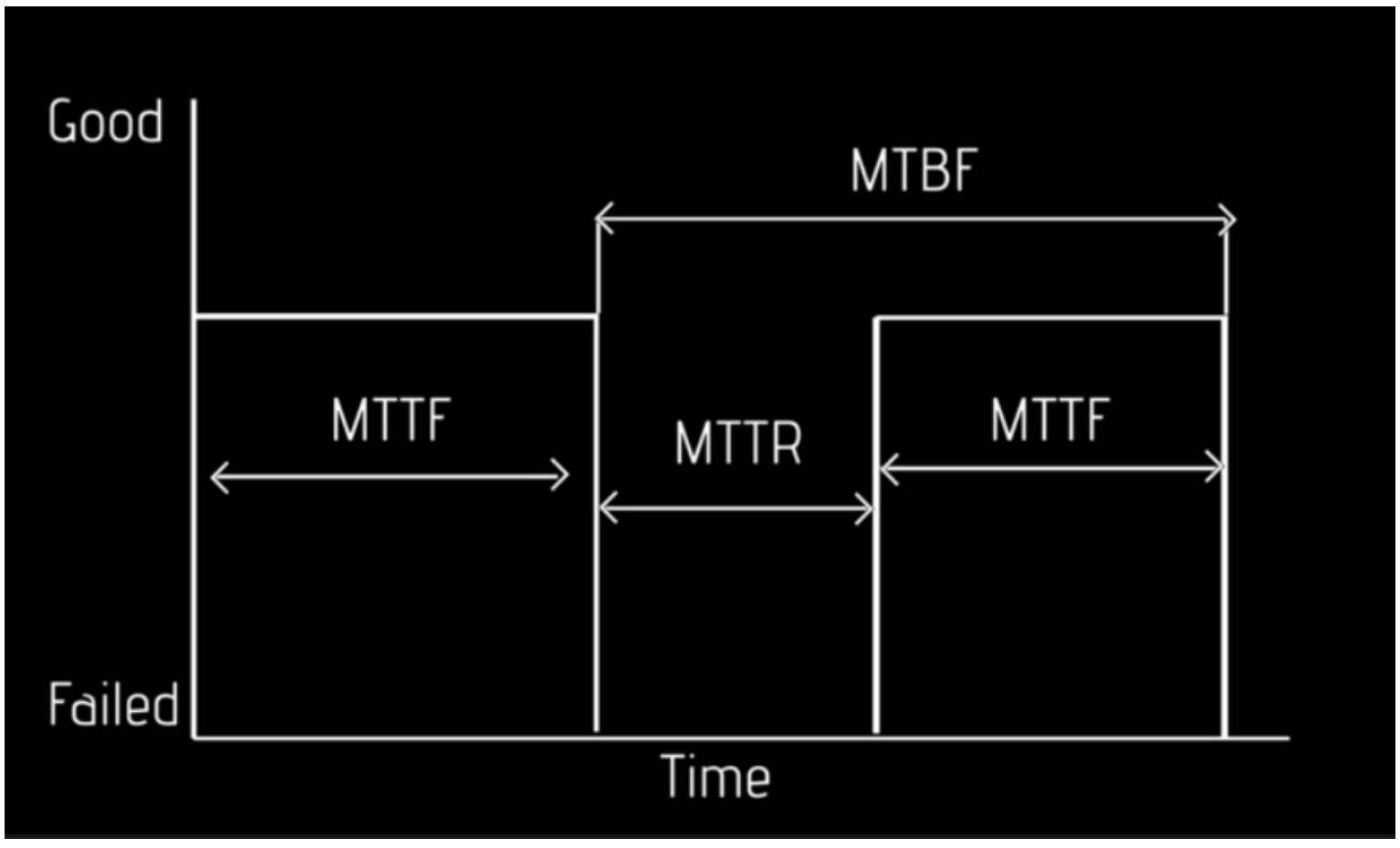
- Ensures compliance with privacy laws and regulations
- **What PII is collected, and why**
- **How the PII data will be collected, used, and secured**

  🛑 To create a **(PIA) - Privacy Impact Assessment**, the organization needs to perform a **(PTA) - Privacy Threshold Assessment** on its infrastructure to locate **personal information**, what personal info. is stored and from whom the personal info is collected.

PTA and PIA - in order to understand the impact of the loss of personal information can do to a particular business.

Calculating Impact

Determine how long the particular equipament going to last. (qualitative)



- **MTTF = Mean Time to Failure**
  - The expected lifetime of a non-repairable product or system
- **MTTR = Mean Time to Repair**
  - Mean time to repair
- **MTBF = Mean Time Between Failure**
  - Predict the time between failures

Recovery Time Objective (RTO):

- Maximum amount of time that a resource may remain unavailable before an unacceptable impact on other system resources occurs.
- Get up and running quickly
- Get back to a particular service level

Recovery Point Objective (RPO):

- Defines the amount of time that will pass between an incident and recovery from backup.
- How much data loss is acceptable?

- Bring the system back online; how far back does data go?

  🛑 *Recovery priorities help define what needs to be addressed to maintain business continuity.*

Maximum Tolerable Downtime (MTD):

- The maximum tolerable downtime (MTD) indicates how long an asset may be down or offline without seriously impacting the organization.

Calculating uptime and availability

- Expressed as a percentage over time
  - 99.999% availability
- 'Availability' is a negotiated definition
  - Especially if it's part of your bonus

Availability %	Downtime per year
99.8%	17.52 hours
99.9% ("three nines")	8.76 hours
99.95%	4.38 hours
99.99% ("four nines")	52.56 minutes
99.999% ("five nines")	5.26 minutes
99.9999% ("six nines")	31.5 seconds
99.99999% ("seven nines")	3.15 seconds

Source: Wikipedia, "High Availability"
http://en.wikipedia.org/wiki/High_availability

- **e.g. - The 'four nines' (99.99%) - means that during the year, you could be down for a total of 52 minutes and 56 seconds.**

Removing single points of failure

A **single point of failure** is a part of a system that, if it fails, will stop the entire system from working.

- A single event can ruin your day
  - Unless you make some plans
- Network configuration
  - Multiple devices
- Facility / Utilities
  - Backup power, multiple cooling devices
- People / Location
  - A good hurricane can disrupt personnel travel
- There's no practical way to remove all points of failure (money drives redundancy)

Organizing Data

The first step to dealing with data security is **organization**.

- Analyze individual chuncks of data (such as databases, files, access control lists..)
- Determine the importance - **the sensitivity of data.**

Data Sensitivity | Labeling

- **Public Data**: Has no restrictions. (stills needs integrity and availability)
- **Confidential Information**: Limited to authorized viewing as agreed by the parties involved.
- **Private Information**:social security number, passport number, PII - Peronally identifiable information...
- **Proprietary Information**: Information owned by a company that gives a certain competitive advantages. (e.g. The secret formula of Coca-Cola).
- **PII - Personally Identifiable Information**: Individual information (Name, birth, morther's name, biometric information, SSN, passport number)
- **PHI - Protected Health Information**: Not only Health information, PII may include on PHI.

Data Roles

- **Data Owners**: Legally responsible for the data, can be entity responsible.
- **Steward**: Responsible for data accuracy, privacy, and security; Associates sensitivity labels to the data and ensure compliance with any applicable laws and standards.
- **Custodian**: Manages the access rights to the data; Implements security controls; Sometimes the same person as the data steward.
- **Privacy Officer**: Ensures data adhere to privacy policies and procedures. Set policies, implements processes and procedures.

User Roles

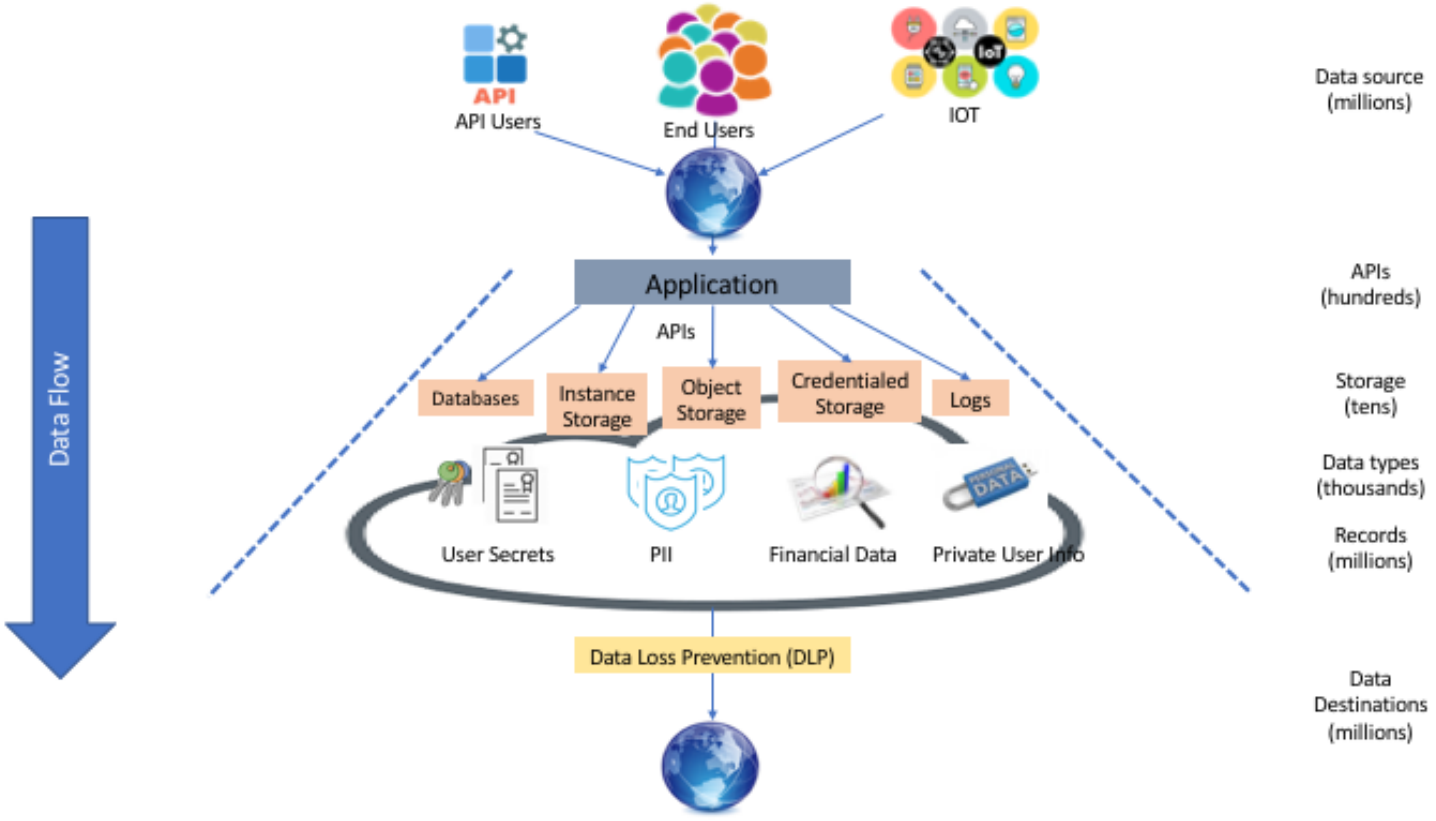
- **Users**: Assigned standard permissions to complete tasks. | Must understand how system functions works and have proper security training to recognize common issues (Malware, etc).

- **Privileged Users**: Increased access and control over the data or system. (e.g. a Normal user can run anti-malware software, but the privileged can updated then).
- **Executive Users**: Concentrates on strategic decisions including policy review, incident response and disaster recovery.
- **System Administrator**: Has complete direct control over the data or system. (Can remove or add users, applying permissions, and doing system maintance...)
- **Data Owner | System Owner**: People or organizations who have legal ownership of this particular data set or particular system.

Data Loss Prevention (DLP)

Data Loss Prevention (DLP) is the practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data. Organizations use DLP to protect and secure their data and comply with regulations.

- The DLP term refers to defending organizations against both data loss and data leakage prevention.



Organizations typically use DLP to:

- Protect Personally Identifiable Information (PII) and comply with relevant regulations
- Protect Intellectual Property critical for the organization
- Achieve data visibility in large organizations
- Secure mobile workforce and enforce security in Bring Your Own Device (BYOD) environments
- Secure data on remote cloud systems

Agreements Types

Business Partnership Agreement (BPA):

Most common used in private sector.

- Primary entities
- Time frame
- Financial issues
- Management

Service Level Agreement (SLA):

Used in private sector.

- Agreement between who is getting the service and service provider
- Service to be provided
- Minimum up-time
- Response time (contacts)
- Start and End date

Interconnection Security Agreement (ISA):

Is a technical Agreement used on public sector.

- Statement of Requirements
  - *Why are we interconnecting?*
  - *What system is interconnecting?*
- System secuirty considerations
  - *What information is interconnecting?*
  - *Where is this information going?*
  - *What services are involved?*
  - *What encryption is needed?*
- Topological drawing
- Signature authoring
  - Time frame for the interconnection
  - Technical and security reviews from them

Memorandum of Understanding/Agreement (MOU / MOA):

Agreement used in public sector.

- The purpose of the interconnection

- Relevant authorities *(Who is on charge?)*
- Specify the responsabilities
    - Downtime
    - Billing
- Define the terms of the agreement
    - Cost
- Termination/reauthorization

---

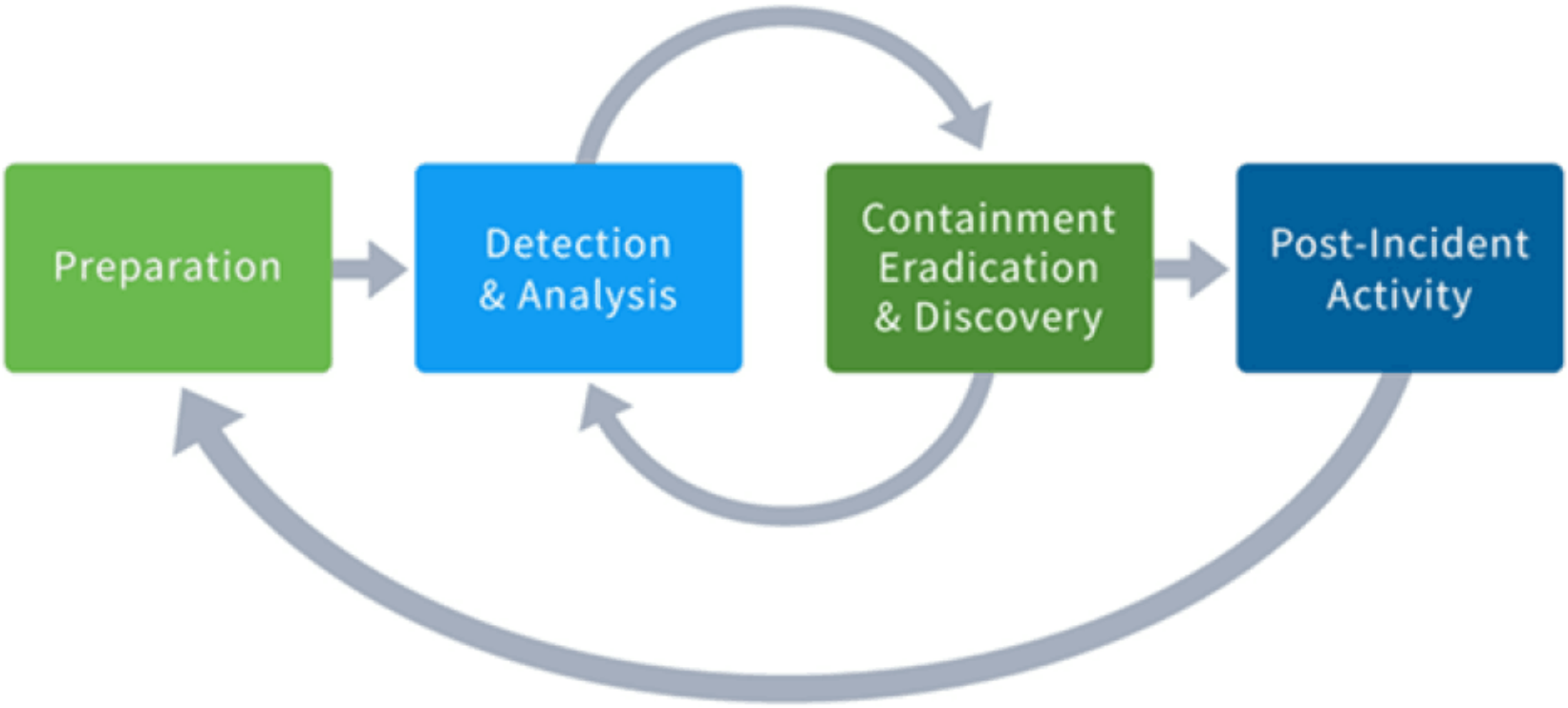
6. Incident Response & Forensics

Incident response is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.

Examples of incident categories

- External/removable media
    - Attack used removable media
- Attrition
    - Brute-force attack
- Web
    - Attack executed from a web site or web-base application
- Email
    - Attack executed from an email message or attachment
- Improper usage
    - Attack resulted from a violation of the Acceptable Use Policy (AUP)
- Loss or theft of equipment
    - Laptop or mobiel device stole
- Many others

Incident Response Process



NIST SP800-61 - Computer Security Incident Handling Guide

NIST SP800-61

The popular guideline for Incident Response process is the **NIST SP800-61 - Computer Security Incident Handling Guide**

- The incident response lifecyle:
    - **Preparation**
    - **Detection and Analysis**
    - **Containment, Eradication, and Recovery**
    - **Post-incident Activity**

1) Preparation

- Who's doing what
- Incident handling hardware and software
    - Laptops, removable media, forensic software, digital cameras, etc
- Organize types of incidents that might happen
- Incident analysis resources
    - Documentation, network diagrams, baselines, critical file hash values
- Incident mitigation software
- Policies needed for incident handling

2) Detection & Analysis

- Many different detection sources
    - Different levels of detail, different levels of perception
- Large amout of 'volume'
    - Attacks are incoming all the time
    - How do you identify the legitimate threats?
- Incidents are almost always complex
    - Extensive knowledge needed

Incident precursors

- An incident might occur in the future
- Web server log: vulnerability scanner in use
- Montly patch release
- Direct threats

Incident indicators

- When an attack is underway / or an exploit is successful
- Can be identified by IDS/IPS
- Anti-virus software identifies malwares
- Host-based monitor detects a configuration change
    - Constantly monitors system files
- Network traffic flows deviate from the norm
    - Requires constant monitoring

3) Containment and Isolation

- Mitigate the damage
- Stop the attack
- Sandboxes
    - The attacker thinks they're on a real system
- Segregate the network
- Shutdown the system
- Turn off a service

Recovery after an Incident

- Eradicate the bug
    - Remove malware
    - Disable breached user accounts
    - Fix vulnerabilities
- Recover the system
    - Restore from backups
    - Pull from snapshots
    - Hire replacement personnel
    - Monitor to ensure good operation
    - Tighten down the perimeter

Reconstitution

- Recovery may take a long time
    - Large-scale incidents require a large amount of work
- The plan should be efficient
    - Start with quick, high-value security changes
        - Patches, firewall policy changes
    - Later phases involve much 'heavier lifting'
        - Infrastructure changes, large-scale security rollouts

4) Lessons learned or Post-incident Activity

- Learn and improve
    - No system is perfect
- Post-incident meeting
    - Invite everyone affected by the incident
- Document the incident
    - Timestamp of the events
    - How did the incident plan work?
        - Did the process operate successfully?
    - What would you do differently next time?
    - Which indicators would you watch next time?
        - Different precursors may give you better alerts

Incident Response Plan

Cyber Incident Response Team - CIRT

This group is responsible for responding to security breaches, viruses and other potentially catastrophic incidents in enterprises that face significant security risks. In addition to technical specialists capable of dealing with specific threats, it should include experts who can guide enterprise executives on appropriate communication in the wake of such incidents. The CIRT normally operates in conjunction with other enterprise groups, such as site security, public-relations and disaster recovery teams.

- A group of people whose job is to response to all incident
- Full or part time - or both
- IT Security Team
- IT Department
- Human Resources
- Legal
- Public Relations

Document incident types / Category definitions

- Physical access
- Malware Phishing
- Social engineering
- Data access

Roles and Responsabilities

- Users
- Help Desk
- Human Resources
- Database manager
- Incident Hotline
- IR manager/ IR officer
- IR team

Reporting Requirements / Escalation

- Determine Severity
- Based on severity have a clear chain of escalation
- Informing law enforcement

Practice

- Annual scenario drills

Digital Forensics

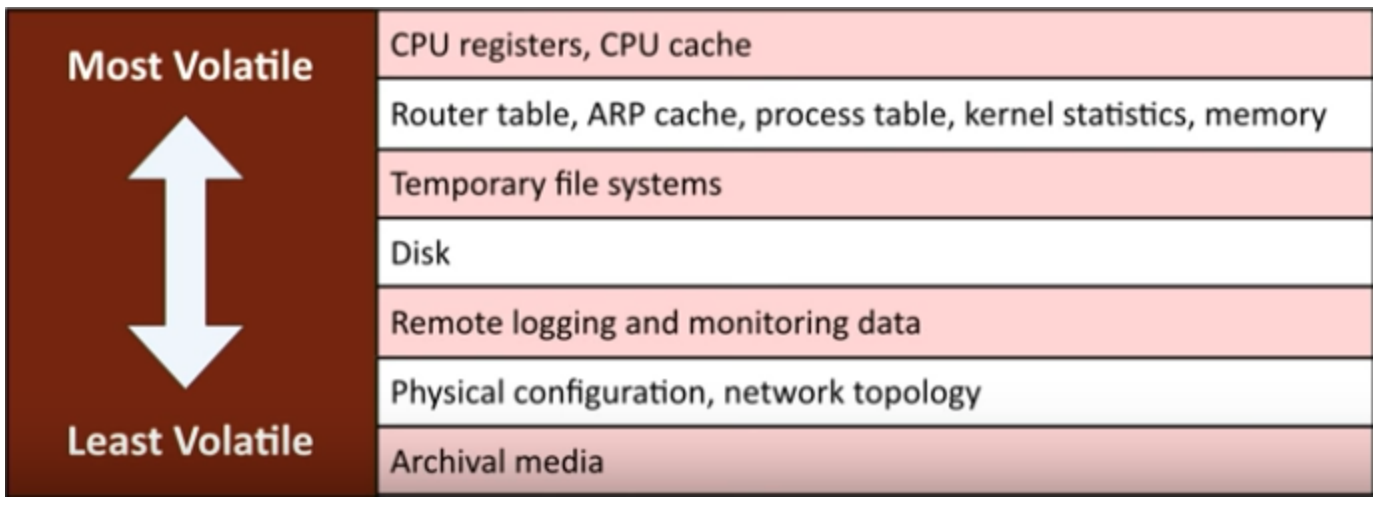
Digital forensics is the process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events.

The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

Forensic procedures

- Collect and protect information relating to an intrusion
  - Many different data sources and protection mechanisms
- RFC 3227 - Guidelines for Evidence Collection and Archiving
  - A good set of best practices
- Standard digital forensic process
  - Acquisition, analysis, and reporting
- Must be detail oriented

Order of Volatility



- The order of volatility is a process that enumerates **when**, **where**, and **how** to **gather the data/evidence before the data changes or disappears**. (How long does data stick around?
    - Some media is much more volatile than others;
    - Gather data in order from the most volatile to less volatile

Memory

- Caches
- Routing tables
- ARP tables

Data on the Disk

- Optical, flash drives
- Cache files, temp files
- Write blocks enabled tools

Remotely logged data

- Web site data
- Remote file server logs
- Backups

Backups

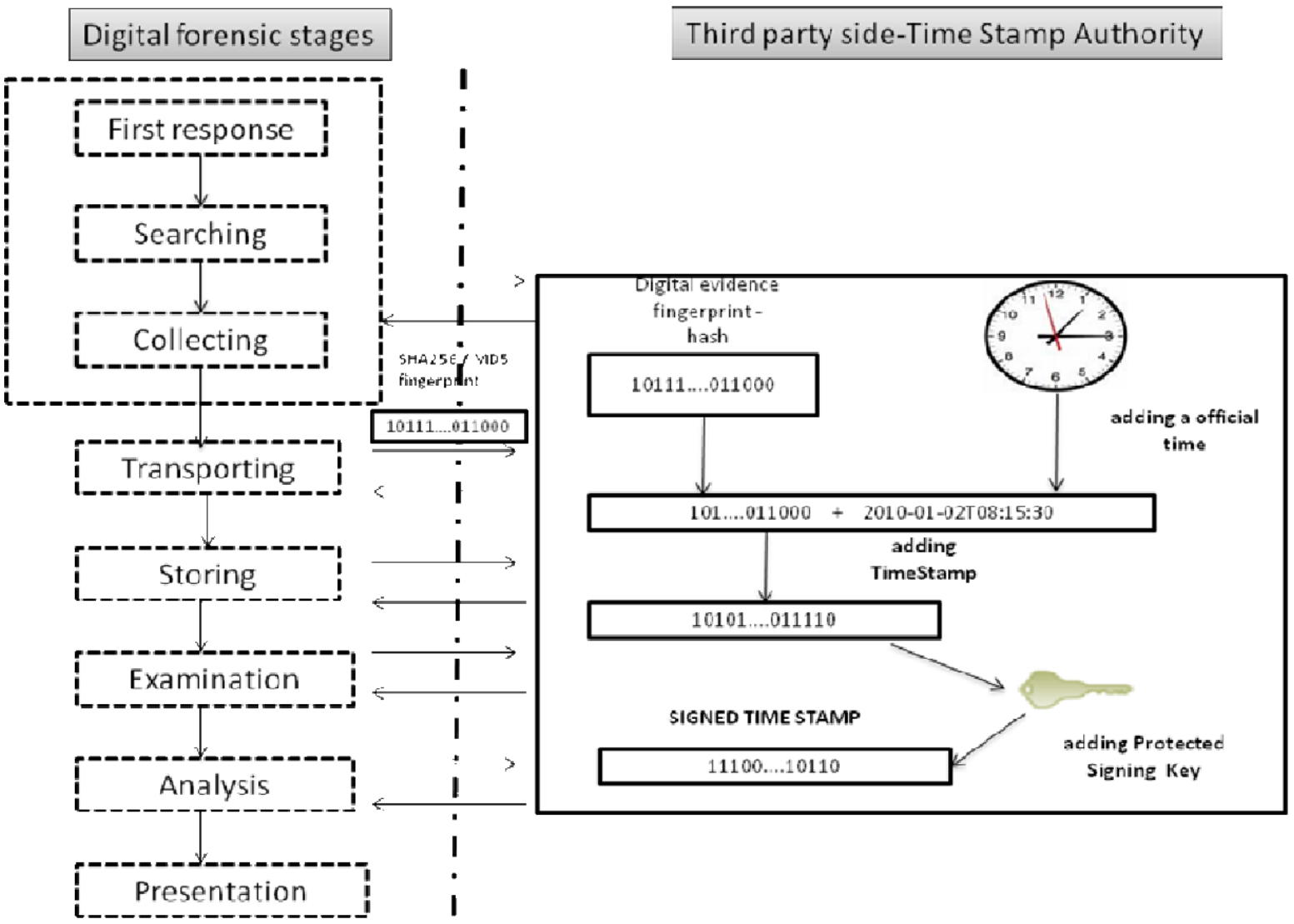
- Trends
- Low volatility takes time to gather data

Chain of Custody

The whole idea of Chain of Custody is to show good integrity of the evidence itself.

- Gathering Evidence - data is of high integrity
    - Control evidence - Maintain integrity
- Everyone who contacts the evidence
    - Avoid tampering
        - Use hashes
- Label and catalog everything
    - Seal and store

Chain of Custody Process



1. Define the Evidence
2. Document collection method
3. Data/time collected
4. Person(s) handling the evidence
5. Function of person handling evidence (qualified person)
6. All locations of the evidence (e.g inital collection, moved to law enforcement...)

Forensic Data Acquisition

Checklist of issues you should consider when you're performing Digital Forensics.

1. **Capture the system image**
    - Bit-for-bit, byte-for-byte
    - Software imaging tools - bootable device
    - Remove the physical drive
    - Get the backup tapes
2. **Netwrok traffic and logs**
    - Firewalls log a lot of information
    - IDS/IPS logs
    - Raw network traffic data
        - Stream-to-disk
        - An exact recording of network communication
            - Rebuild images, email messages, browser sessions, file transfers
3. **Capture video**
    - Security cameras, mobile devices
    - Record time offset
4. **Take Hashes**
    - Ensure that there's no tampering
    - MD5 (Message Digest 5)
        - 128 bits, displayed as hexadecimal
        - Chance of duplication is one in 2^128
        - CRC (Cyclical Redundancy Check)

        - 32 bits, displayed as hexadecimal
        - One in 2^32
    - Create an MD5 hash for an image, file, or groups of files
        - Data can be verified at any time

5. **Take screenshots**
    - Capture the state of the screen
    - External capture (Camera, Mobile device)
    - Internal capture (PrintScreen)
6. **Interview witnesses**
7. **Track man hours**

Contingency Planning

Attempts to mitigate adverse incidents to preserve business continuity.

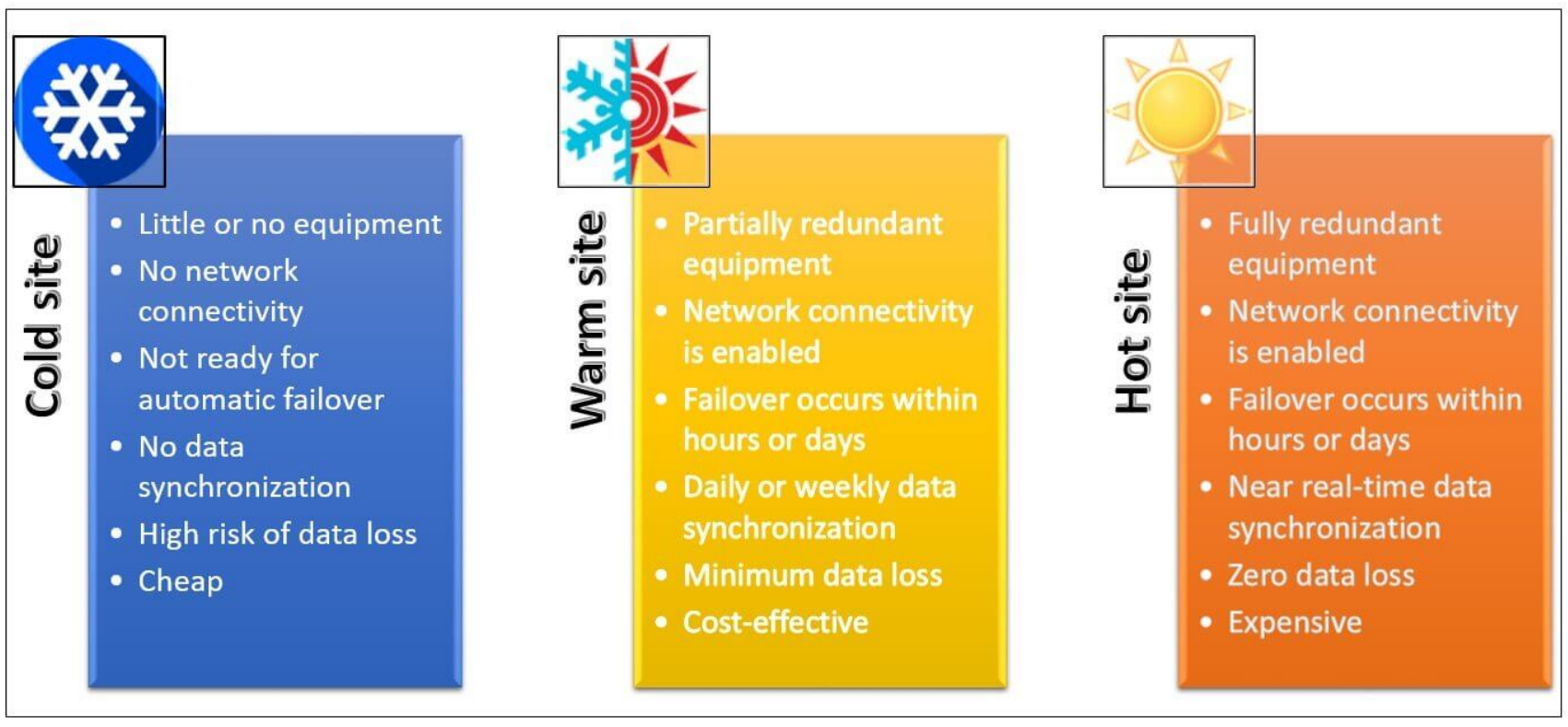
- How do we recover from a specific type of a disaster?
- What to do for keep the **Business Continuity** going?

Evidences on Computer forensics

1. **Documentary evidence** - directly supports or proves a definitive assertion.
2. **Exculpatory** - evidence proves innocence.
3. **Inculpatory** - evidence proves guilt.
4. **Demonstrative evidence** - which can be in the form of charts, graphs, drawings, and so forth, is used to help nontechnical people, such as the members of a jury, understand an event.

Disaster Recovery - Evacuation Plan

Backup Sites:



- **Cold site**

- **Empty site, no hardware, no data, no people**
- **It takes weeks to bring online**
- Basic office spaces (e.g building, chairs, AC...)
- No operational equipment
- Cheapest recovery site

🟡 Warm site

- **Somewhere between cold and hot - Just enough to get going (Big room with rack space, you bring the hardware)**
- Hardware is ready and waiting - you bring the software and data
- **It takes days to bring online**
- Operational equipment but little or no data

🔴 Hot site

- **Exact replica of production systems**
- Applications and software are constantly updated
- Flip a switch and everyting moves
- **It take hours to bring online**
- Real-time synchronization
- Almost all data ready to go - often just a quick update
- Very expensive

Order of Restoration

1. Power
2. Wired LAN (is open and running)
3. ISP link (running)
4. Active Directory/DNS/DHCP server (up and cooking)
5. Account servers
6. Sales and account workstations
7. Production servers
8. Production workstation
9. Wireless access
10. Peripherals (Printers, Camers, Scanners, faxes...)

Annual exercises - Continuity of Operations

- **Failover**
  - Simple means the process of making recovery site happen.
- **Alternative Processing Sites**
  - Different types of processing sites
- **Alternative Business Practices**
  - Manual transactions, paper receipts, phone calls for transaction approvals
  - These must be documented and tested before problem occurs
- **After-action Reports (AAR)**
  - A clear and detailed documentation of everything that happened so that if it ever happens again you'll be ready to handle any form of business contingency planning.

🛑 Through planning and practice is what makes recovery plans successful when disasters occur

🛑 A **fail-safe device** responds by not doing anything to cause harm when the failure occurs.

🛑 A **fail-secure device** responds by making sure the device is using a secure state when a failure occurs.

Backups 📄

Media for Backups

- External hard-drive
- Tape
- Cloud

Offsite Backup

Remote backup is **good for natural disasters** in general (fire, flood, water pipe burst, hurricane, tornando).

- Vaulting
  - Send your backup media to an outside storage facility
  - E-valuating - Send the data electronically
- Organization-owned site or 3rd-party
  - Usually a secure facility
- Backups require extensive protection
  - Data loss and thef is a significant concern
- Many compliance mandates (SOX, HIPAA, etc)

🛑 **Location selection** have legal implications and Data sovereignty (data that resides in a country is subject to the laws of that country)

Cloud Backup

Cloud backups work beautifully, however, they have one big downside and that is they take up a tremendous amount of time to get the initial backups going.

Snapshots

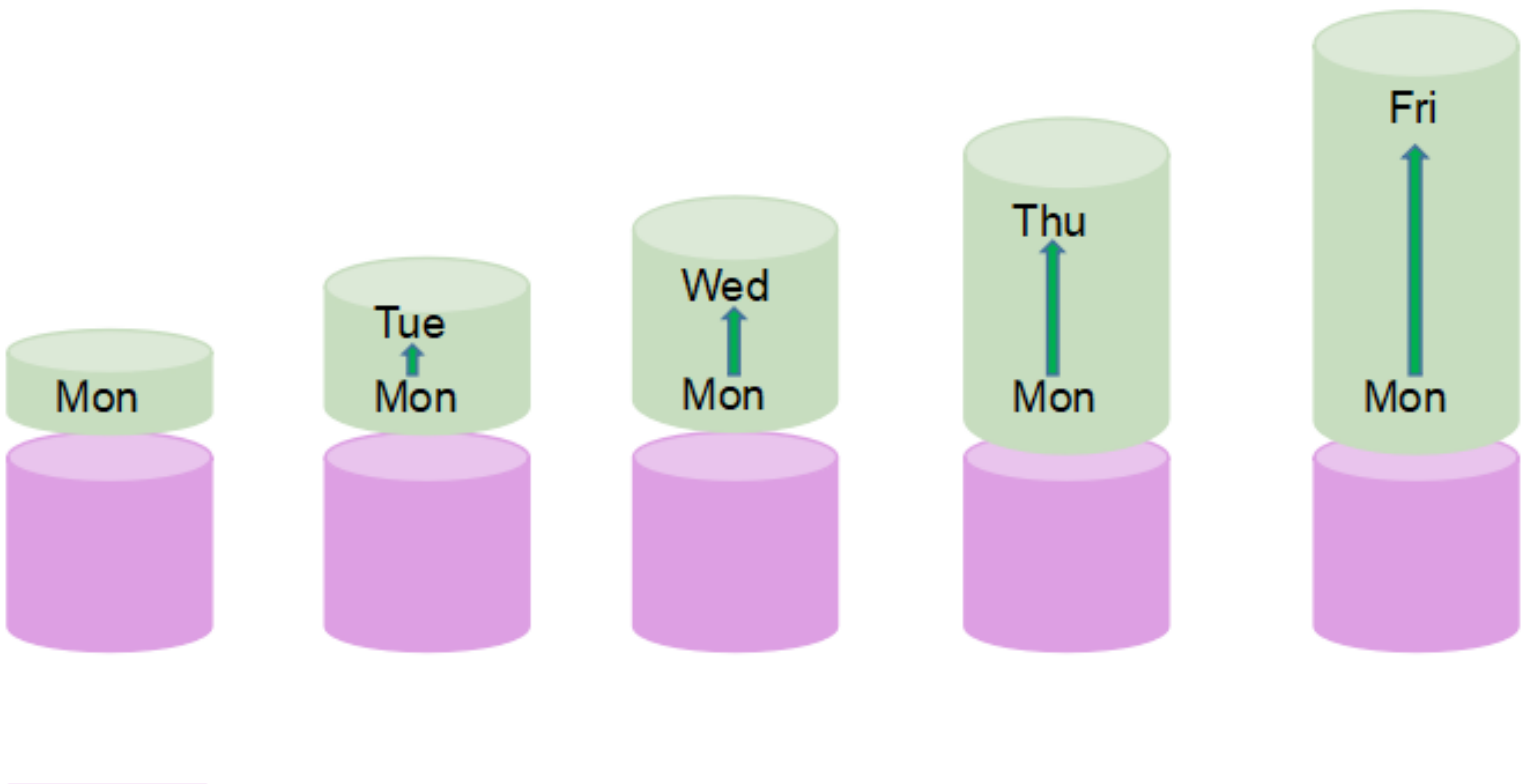
Snapshots typically under **virtual machines** and they are an absolute perfect way of making a copy of something that's happened in the past.

Backup Utilities

- Protect from unexpected downtime
  - Malware infection
  - Ransomware
  - Server defacement
- Real-time file sync
  - rsync
- Regular partial backups - hourly incremental backups
- Full backups - complete file backups
- Complete coverage, fast recovery

Differential Backup

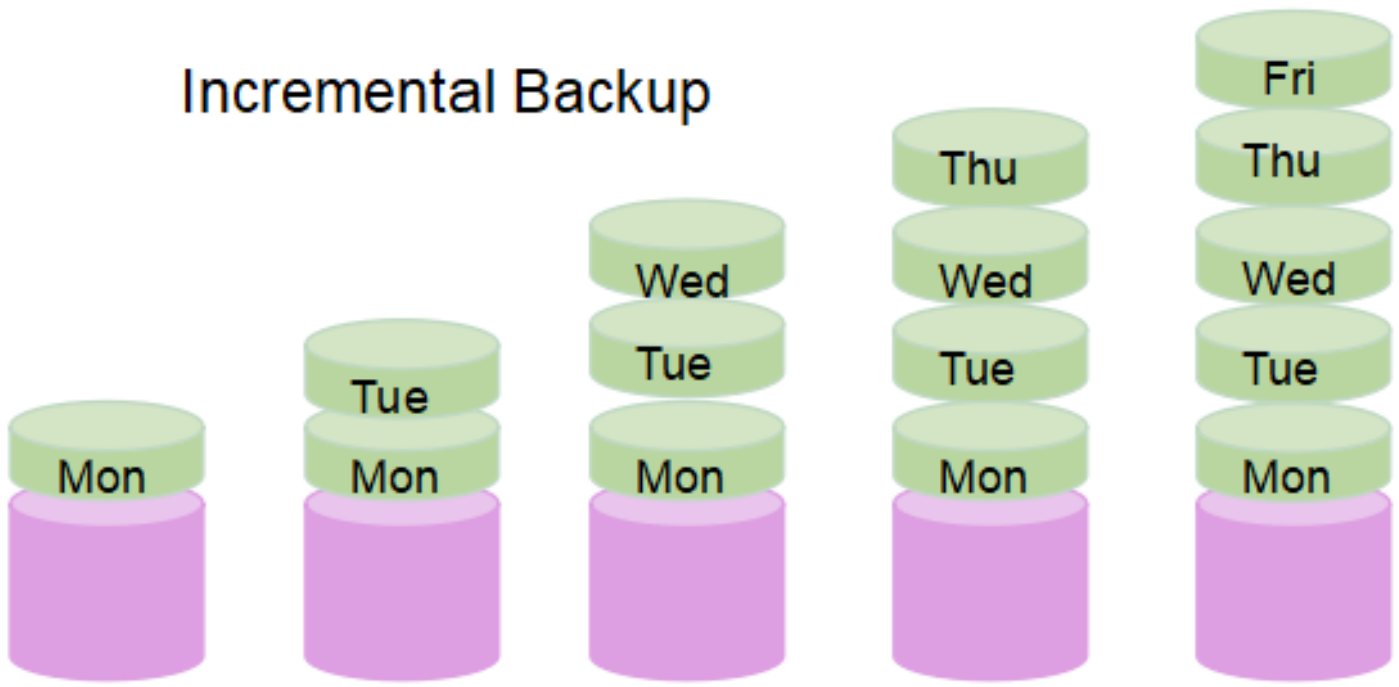
- Backup all the changes since the last full backup



- *Differential there are less backup sets but they get bigger.*

Incremental Backup

- Only backs up changes made from last backup



- *Incremental more backup sets but smaller.*

Type	Data Selection	Backup	Restore Time	Archive Attribute
Full	All selected data	High (one tape set)	Low	Cleared
Incremental	New files and files modified since the last backup	Low (multiple tape sets)	High	Cleared

Type	Data Selection	Backup	Restore Time	Archive Attribute
Differential	All data modified since the last full backup	Moderate (no more than 2 sets)	Moderate	Not cleared

---

7. Testing the Infrastructure

Vulnerability Scanning Tools 👁‍🗨

- **Advanced IP scanner** - Advanced IP Scanner is fast and free software for network scanning. It will allow you to quickly detect all network computers and obtain access to them. With a single click, you can turn a remote PC on and off, connect to it via Radmin, and much more.
- **Nmap** - Nmap is a free and open-source network scanner. Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection.
- **MBSA - Microsoft Baseline Security Analyzer** (determine the security state of a system by assessing missing security updates and less-secure security settings; report good information for vulnerability assessment)
- **`traceroute`/`tracert` command** - show how packets get from host to another endpoint. Traceroute is helpful to see what routers are being hit, both internal and external.

Scan Types:

1. **Non-intrusive**: Gather information, don't try to exploit a vulnerability.
2. **Intrusive**: You'll try out the vulnerability to see if it works.
3. **Non-credentialed scans**: the scanner can't login to the remote device.
4. **Credentialed scan**: You're a normal user, emulates an insider attack.

`Intrusive` vs. `Non-intrusive`

Almost all vulnerability assessments are **non-intrusive**. Scanning systems, gather information and identifying

vulnerabilities are different than corrupt the entire database.

`Credential` vs. `Non-credential`

A **Credential Vulnerability Asssessment** basically means you've got usernames and passwords as a part of your assessment. **Non-credential** you don't touch on usernames and passwords on assessments.

Vulnerability Scanning Assessment

The purpose of Vulnerability Scanning is to identify vulnerabilities cause by lack of security controls, common misconfigurations, and so on.

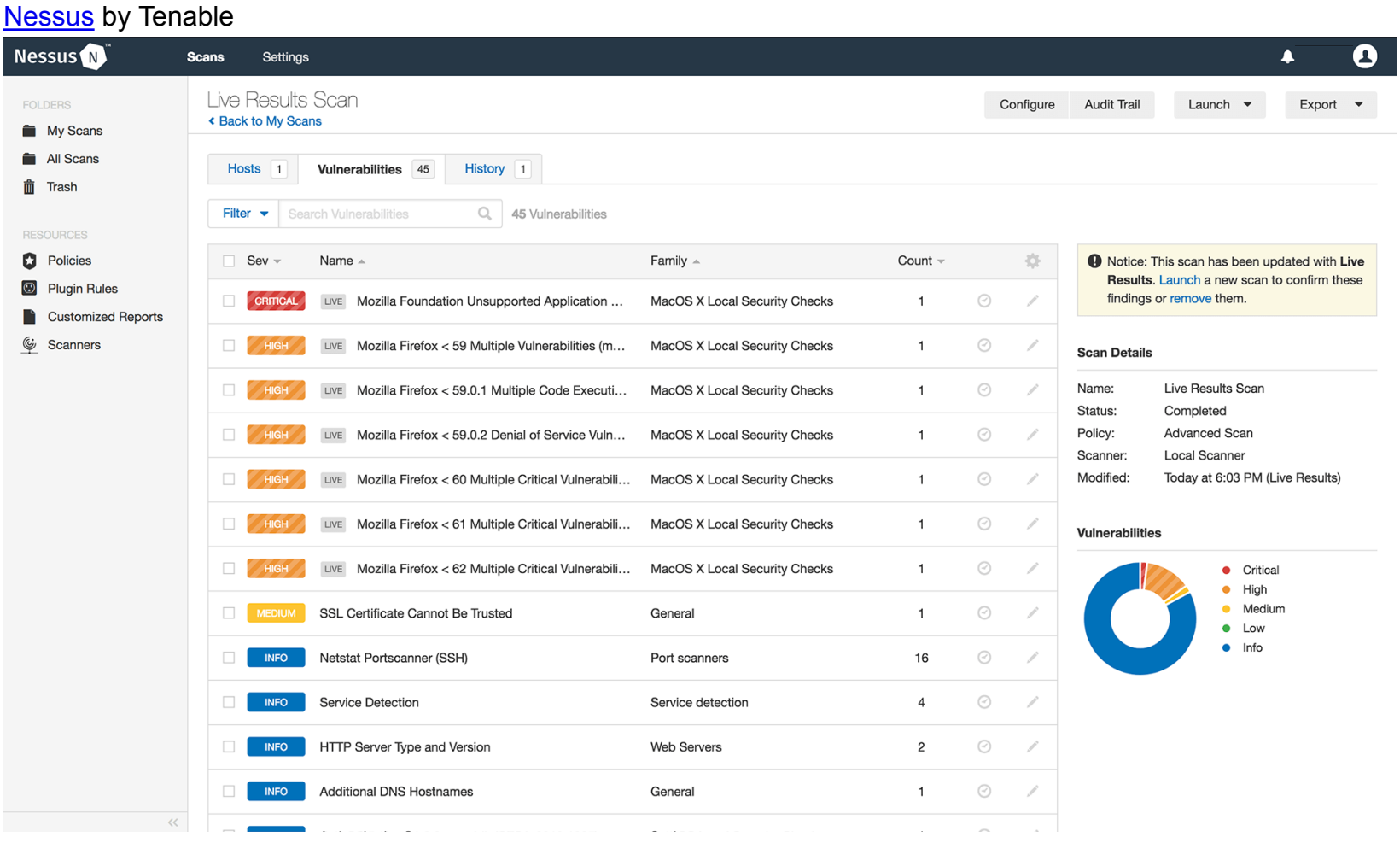
Vulnerability Scan Results:

- **Lack of security controls**
  - No firewall
  - No anti-virus
  - No anti-spyware
- **Misconfigurations**
  - Open shares
  - Guest access
  - DNS/SPF records
- **Real vulnerabilities**
  - Especially newer ones
  - Occasionally the old ones

🛑 *Sometimes Vulnerability Scanners show **False Positives** (a vulnerability is identified that doesn't really exist) or **False Negatives** (a vulnerability exists, but the scanner didn't detect it). To deal with this, update to the latest signatures and patch it.*

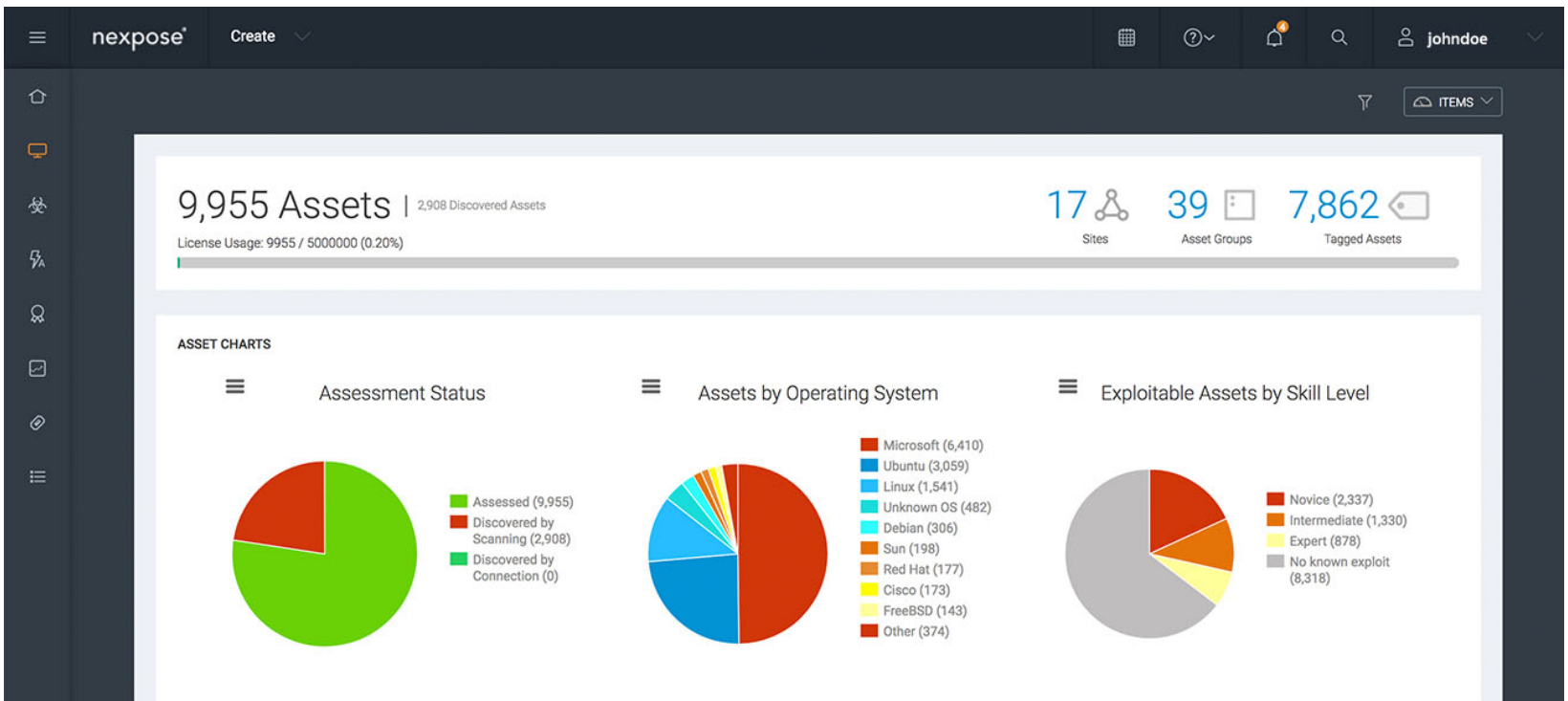
Vulnerability Assessment Tools

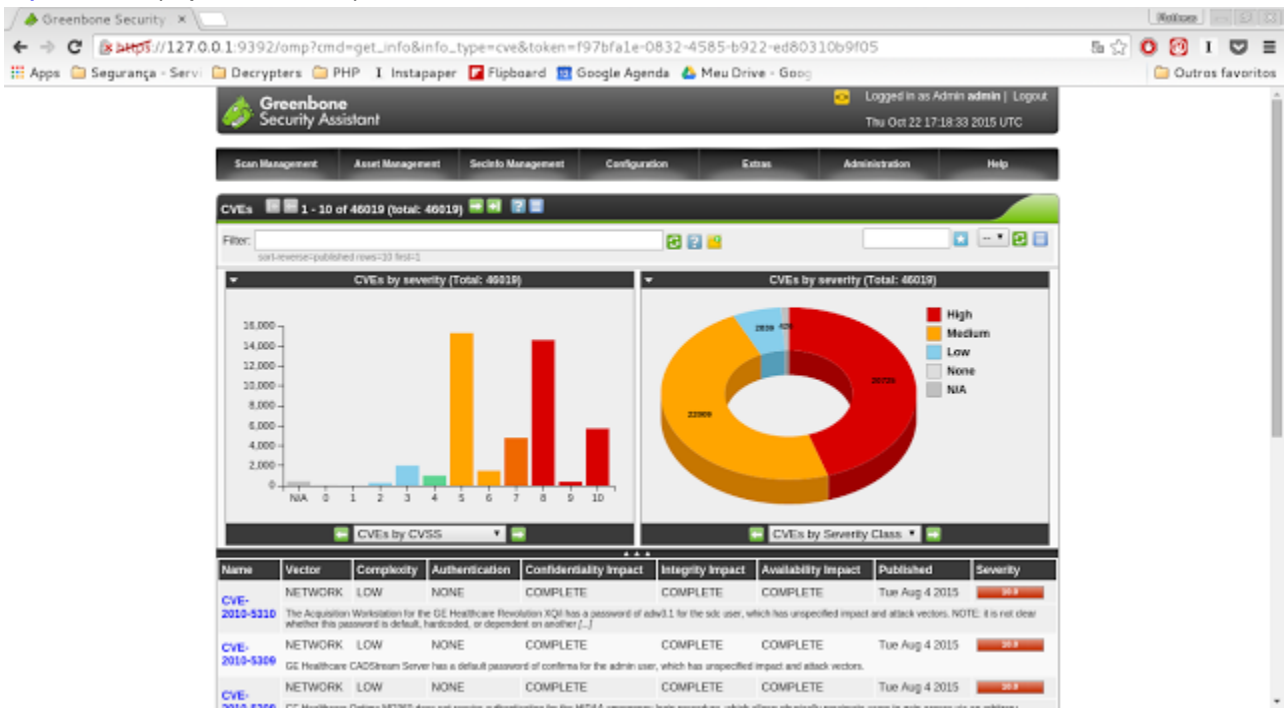
- Nessus by Tenable



- Nexpose by Rapid7

- [OpenVAS](#) (Open Source)





Principles of Social Engineering 🗣️👤

1. **Authority**
    - Impersonate or imply a position of authority
2. **Intimidation**
    - Frighten by threat
3. **Consensus / Social proof**
    - To convince of a general group agreement
4. **Scarcity**
    - The situation will not be this way for long
5. **Urgency**
    - Works alongside scarcity / act quickly, don't think
6. **Familiarity**
    - To imply a closer relationship
7. **Trust**
    - To assure reliance on their honesty and integrity

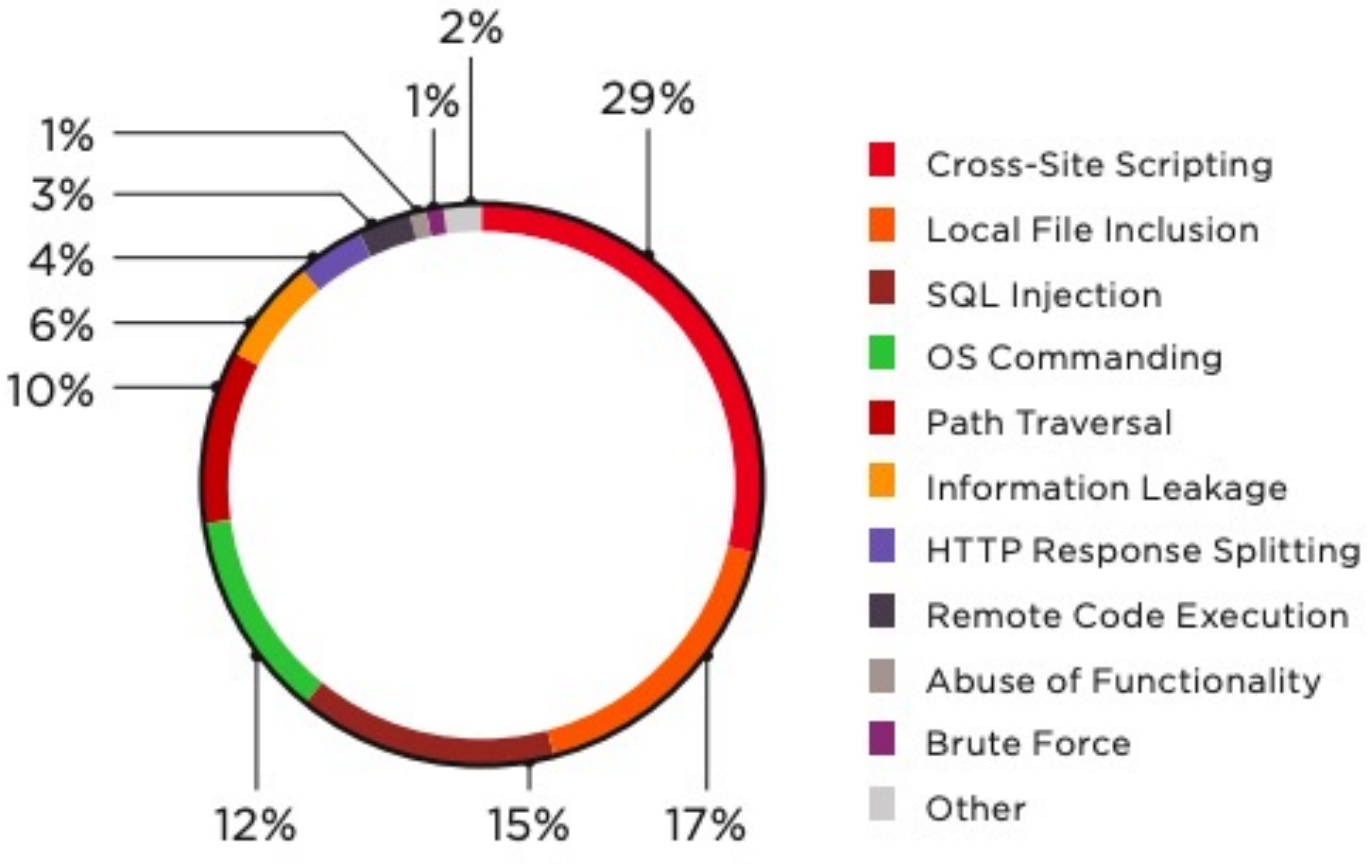
Social Engineering Attacks

- **Phishing** - the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication
- **Spear Phishing** - Directed towards a specific person or company
- **Vishing** - Uses Voice calls/telephone system to get private information
- **Hoax** - Warns someone that something bad is happening when its not *(e.g Virus Alert)*
- **Watering Hole Attack** - An attempt to infect websites that a group of end users would normally go to gain access to their information or network. *(e.g Local Coffee Shop Network)*
- **Whaling** - Spear phishing tha targets senior management and executives
- **Tailgating** - *(e.g leave computer unlocked, door etc)*
- **Shoulder Surfing** - technique used to obtain private information by looking over the victim's shoulder, either from keystrokes on a device or sensitive information being spoken and heard, also known as eavesdropping
- **Impersonation** - Pretend to be someone you aren't
- **Dumpster Diving** - Used to retrieve information that could be used to carry out an attack on a computer network.

Common Web Application Attacks

OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source: OWASP



2018 | Source: ptsecurity

- **Cross-site scripting (XSS)** - Client-side script injected into trusted web site
    - **Reflected XSS** - non-persistent, allow scripts to run in user input
    - **Stored XSS** - script is stored in back-end database
- **XML injections** - Used to manipulate or compromise the logic of an XML application or service *(e.g change the price of a product on ecommerce)*
- **Cross-site Request Forgery (XSRF, CSRF)** - forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing.
- **Click-jacking** - Also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page.
- **Session Hijacking** - Inject information on middle of connection *(e.g Grabbing the request and copying the Session ID from the Cookie).*
- **Code Injection** - is the general term for attack types which consist of injecting code that is then interpreted/executed by the application. This type of attack exploits poor handling of untrusted data. These types of attacks are usually made possible due to a lack of proper input/output data validation.
- **Comand Injection** - ommand injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
- **SQL injection (queries)**
    - `inner join`
    - `select from`
    - `insert into`
- **LDAP injection (queries info)**
    - Based on X.500 protocol
        - DC = Domain Component
        - OU = Organizational Unit
        - CN = Common Name
- **Buffer Overflow** - overflows the input directly to the memory
- **Integer Overflow** - overflow an input variable (e.g typing a large number on calculate forcing an error)

Applications Vulnerabilities

- **Race Condition** - A race condition is a flaw that produces an unexpected result when timing of actions impact other actions. An example may be seen on a multithreaded application where actions are being performed on the same data. Race conditions, by their very nature, are difficult to test for.
- **Improper Input Handling** - Improper Input Handling is the term used to describe functions such as validation, sanitization, filtering, or encoding and/or decoding of input data. Improper Input Handling is a leading cause of critical vulnerabilities that exist in today's systems and applications. (SQL injections, buffer overflows, DoS, etc).
- **Improper Error Handling** - Errors are supposed to show least information about the system, to avoid additional information like Network Information, Memory Dump, Stack Traces, database dumps, etc.
- **Memory/buffer vulnerability**
    - **Memory Leak**
        - Unused memory is not properly released
        - Begins to slowly grow in size
        - Eventually uses all available memory
        - System crashes
    - **Integer Overflow**
        - Large number into a smaller sized space
        - Where does the extra number go?
        - You shouldn't be able to manipulate memory this way
    - **Buffer Overflow**
        - Overwriting a buffer of memory
        - Spills over into other memory areas
- **Null-Pointer deference** - Null pointer errors are usually the result of one or more programmer assumptions being violated. Most null pointer issues result in general software reliability problems, but if an attacker can intentionally trigger a null pointer dereference, the attacker might be able to use the resulting exception to bypass security logic or to cause the application to reveal debugging information that will be valuable in planning subsequent attacks.
- **Resource exhaustion**
- **Weak cipher suites and implementations**
    - *The suite*:
        - Encryption Protocol (AES, 3DES, etc)
        - Length of the encryption key (128 bits, 256 bits etc)
        - Hash used for integrity check (SHA, MD5 etc)
- **Misconfiguration / Weak configuration**
- **Default configuration** - *(e.g user:admin / pass:password)*
- **DLL injection**
    - Bad guys didn't write the application, but they could write an external library and manipulate the OS or application to run the library
- **System sprawl / undocumented assets**
    - Hundred of projects, test platforms, active OS, production VMs
    - Keeping track is a challenge
    - Easy to miss a forgotten computer
        - Under a desk
        - Part of a retired application
    - Not part of regular security patches
- **Zero-days**
    - New threats - *(The WannaCry (2017) ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging*

from hundreds of millions to billions of dollars).
    - WannaCry ransomware hit on May 12, 2017 and the patch had been available since March 14.

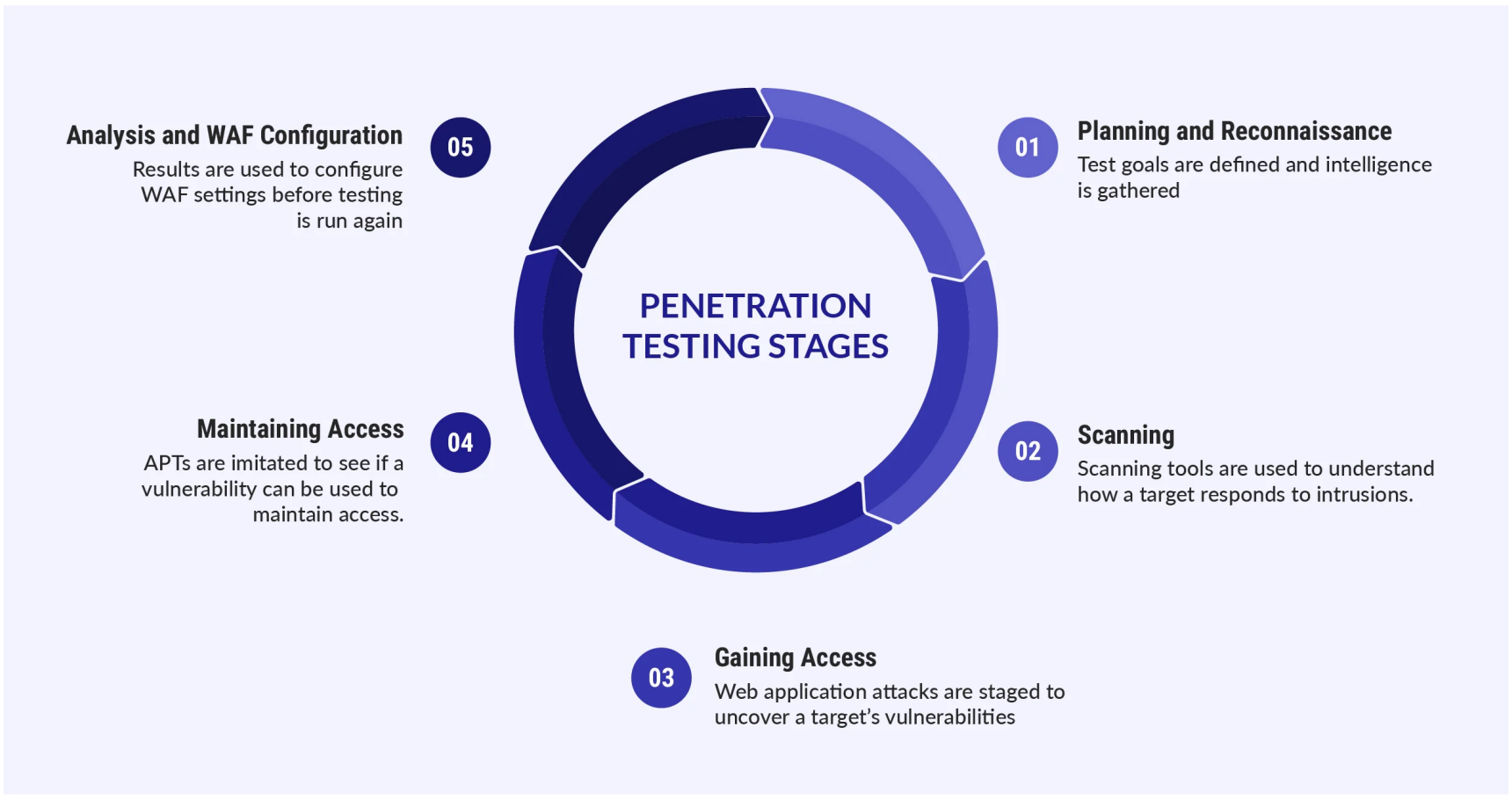
- **Improper certificate and keymanagement**

    - Manage your keys and certificates
    - What will be the organizations certificate authority?
    - How will intermediate CAs be created and managed?
    - Who will validate and sign the organization's certificate?
    - and many more questions about the process

Physical Vulnerabilities

- Untrained users
- Improperly configured accounts
    - Accounts without a need / abandoned and unnecessary accounts
    - Accounts with administrative access
    - Technical issue and process issue
- Vulnerable business processes

Penetration Testing / Pentesting



Is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually.

- **Penetration test** will actually try to grab the data itself.
- **Vulnerability assessment** at no time will ever actually try to grab the data.

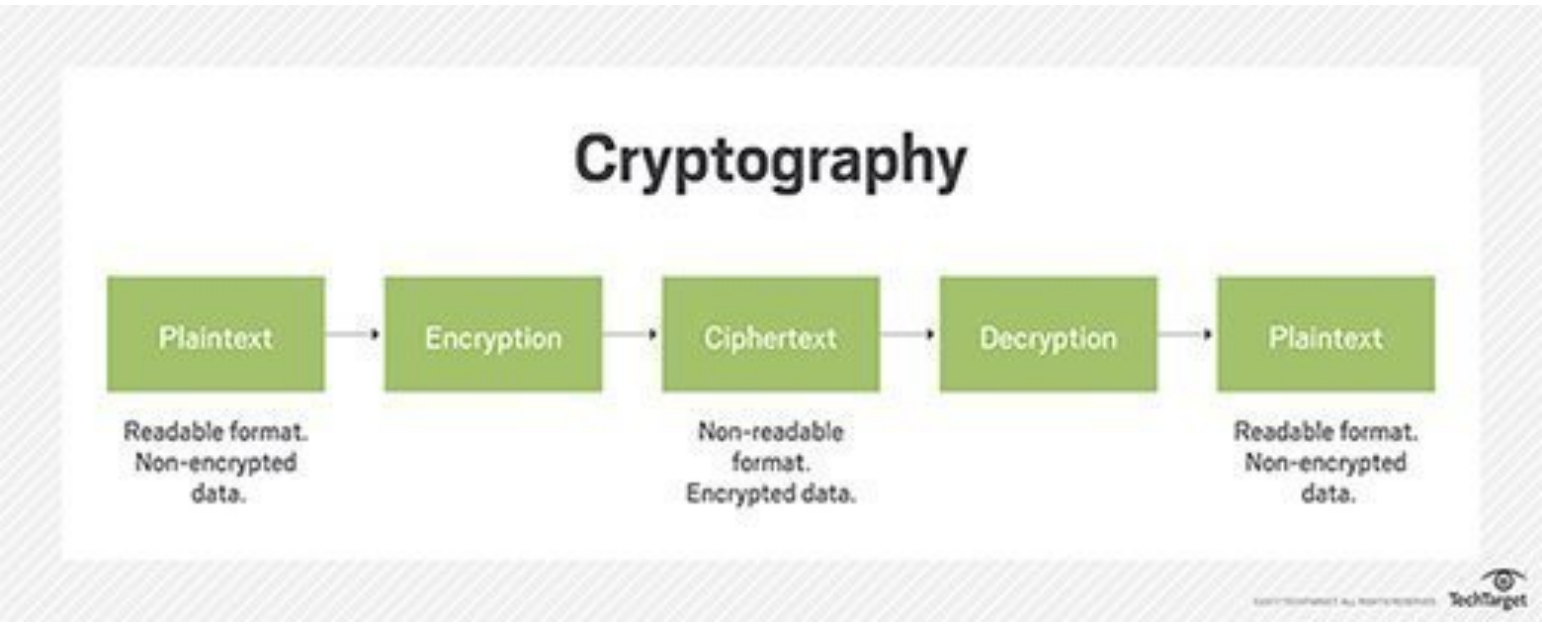
Pentesting Process

1. **Reconnaissance**
2. **Scanning**
3. **Gaining Access**
4. **Maintaining Access**
5. **Expanding to other systems**
6. **Avoid Detection**

Principles

- **Authorization**
  - Define the targets
  - Attack model
    - White box - have extensive knowledge about the target
    - Black box - attacker know nothing about the target
    - Gray box - somewhere between the two
- **Discover Vulnerabilities**
  - Reconnaissance
    - Passive Discovery
    - Semi-passive discovery
    - Active discovery
  - Try to get Information
- **Exploit vulnerabilities**
  - Pivotting
  - Persistance
  - Privilege Escalation

8. Cryptography



Cryptography is the practice of disguising information in a way that looks random.

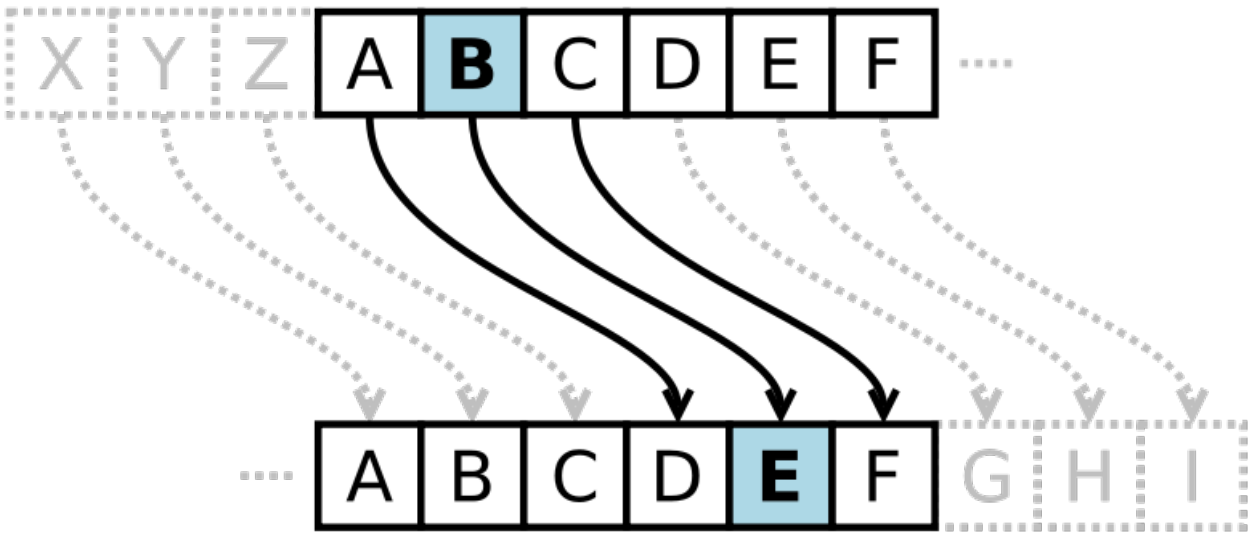
- Provide confidentiality and integrity
- Used for authentication and access control
- Non-repudiation
  - You said it. You can't deny it

Cryptography Terms

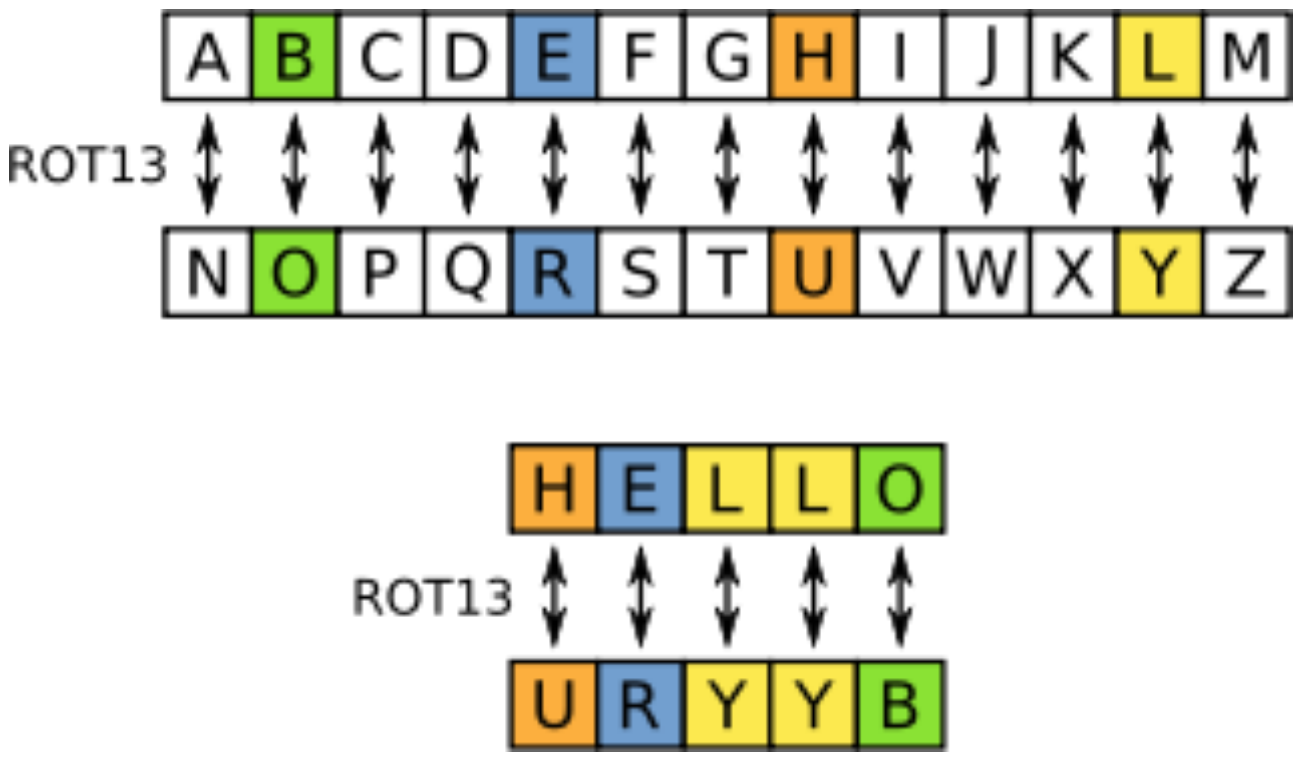
- **Plaintext**
  - An unencrypted message (in the clear)
- **Ciphertext**
  - An encrypted message
- **Cipher**
  - The algorithm used to encrypt and decrypt
- **Cryptanalysis**
  - The art of cracking encryption
  - Researchers are constantly trying to find weaknesses in ciphers
    - Mathematically flawed cipher is bad for everyone

Classic Algorithms - by Substituition

- **Caesar Cipher** - *The earliest known and simples ciphers.*
  - It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.



- **ROT13** - Rotate by 13 places
  - Substitute one letter with another
  - e.g., `"URYYB"` is `"HELLO"`



- **Vigenère Cipher** - *Employs the Caesar cipher as one element of the encryption process + the key.*

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- **Kerkchoff Principle** - *The crypto algorithm should be public and the key is the secret.*

Where to Encrypt & Decrypt?

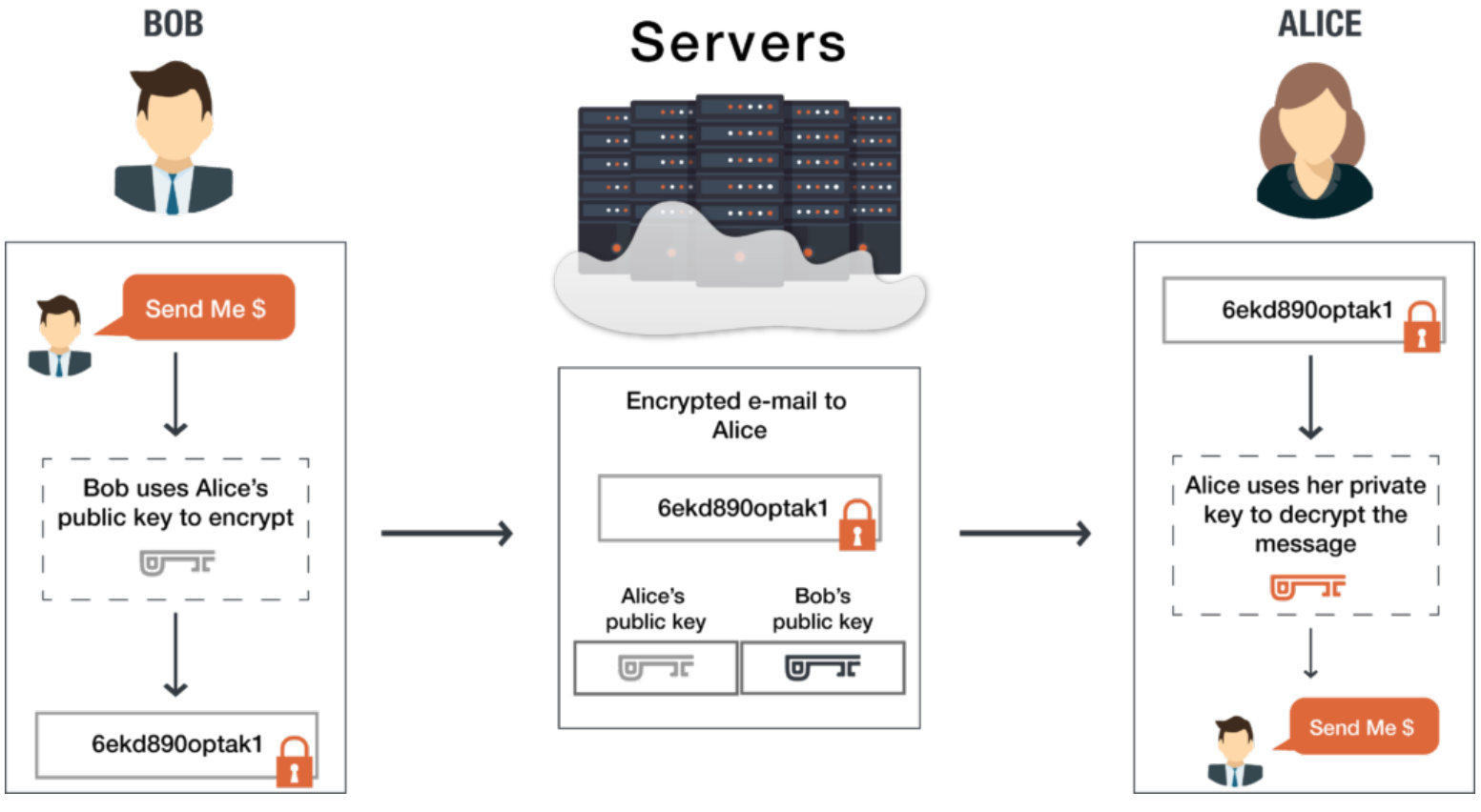
- **Data-in-Transit** / **Data-in motion**: Transport / Network
  - Not much protection as it travels
    - Many different switches, routers, devices
  - Network-based protection:
    - Firewall, IPS
  - Provide transport encryption:
    - TLS, IPsec
- **Data-at-Rest**: Resides in storage
  - Hard drive, SSD, flash drive, etc
  - Encrypt the data
    - Whole disk encryption
    - Database encryption
    - File or/ folder-level encryption
  - Apply permissions
    - Access control lists
    - Only authorized users can access the data
- **Data-in-use** / **Data-in-process**: RAM & CPU
  - The data is in memory or CPU registers and cache
  - The data is almost always decrypted

Symmetric Encryption

- **One Single Key** / **Session Key to encryption and decryption**
- Primary way to encrypt data
- **Ephemeral Key** / **Session key**:
  - Temporary
  - Provides perfect forward secrecy
  - Is possible to Share a symmetric session key using asymmetric encryption:
    1. *Client encrypts a random (symmetric) key with a server's public key*
    2. *Ther server decrypts this shared key and uses it to encrypt data*
    3. *This is the session key*
- Very fast to use
  - Less overhead than asymmetric encryption
  - Often combined with asymmetric encryption
- 128-bit or larger symmetric keys are common

Asymmetric Encryption

- **Uses a Key pair**:
  - **Public Key** - Anyone can see this key; give it away
  - **Private Key** - Keep this private
- Larger keys than symmetric encryption; Common to see key lengths of 3,072 bits or larger



Symmetric key from Asymmetric keys -

Cryptosystem 🔑🗝️

Defines **key properties**, communication requirements for the **key exchange**; actions through encryption and decryption process.

(Ex: Using asymetric encryption to exchange Session keys after that communicate using Symmetric encryption.)

- **Key escrow** (also known as a “fair” cryptosystem) is an arrangement in which the **keys** needed to decrypt encrypted data are held in **escrow** so that, under certain circumstances, an authorized third party may gain access to those keys.

Symmetric Cryptosystems

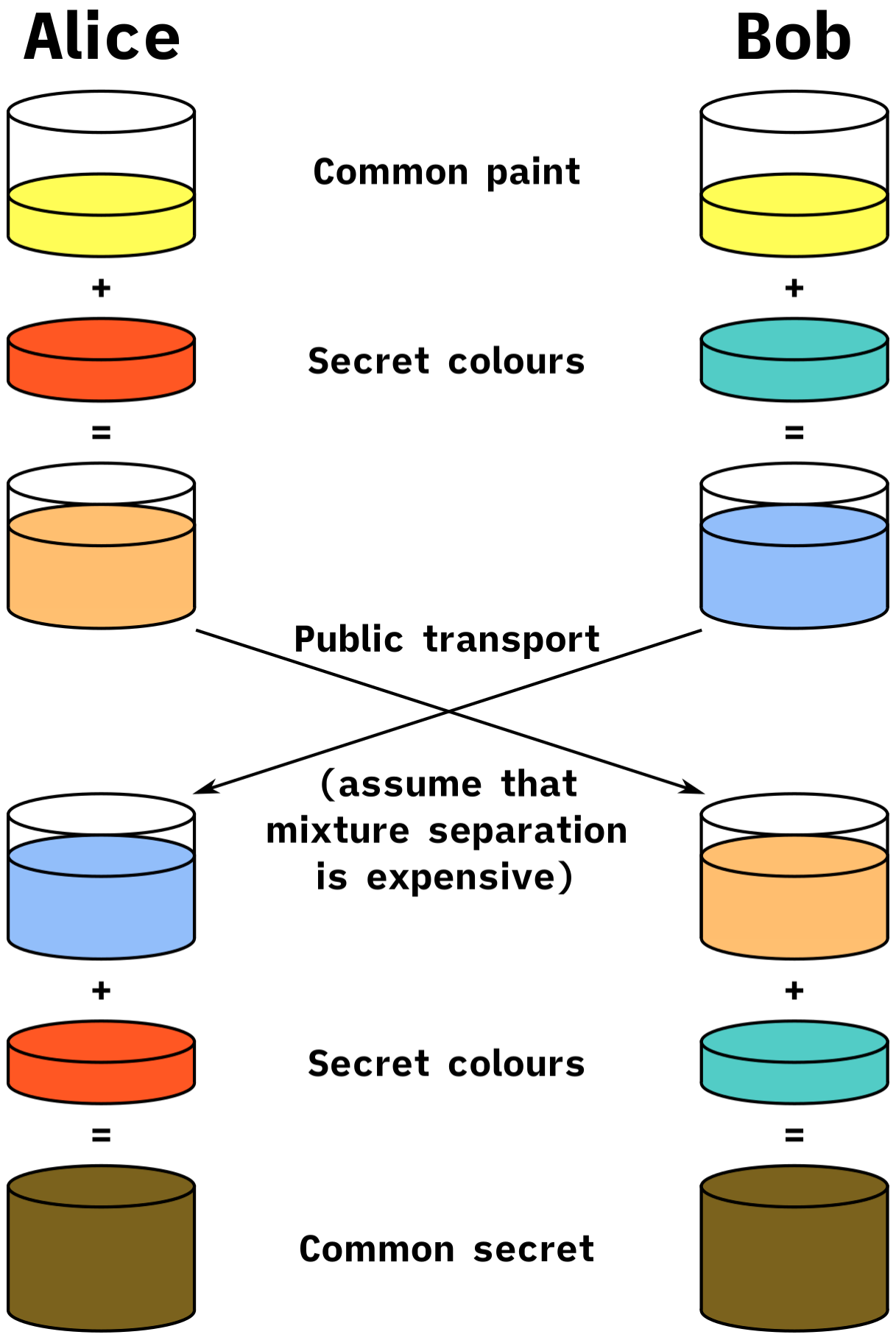
Algorithm	Block or Streaming	Block Size	Rounds	Key Size	Notes
DES	Block	64-bit	16	56 bits	Uses five modes of operation: ECB, CBC, CFB, OFB and CTR.
Blowfish	Block	64-bit	16	32-448 bits	Public domain algorithm.
Twofish	Block	128-bit	16	128, 192 and 256 bits	Public domain algorithm.
3DES	Block	64-bit	16	168 bits (56 x 3)	Repeats DES process 3 times.
AES	Block	128-bit	10, 12, or 14	128, 192 or 256 bits	Encryption standard for the US Gov.; Used in WPA2
RC4	Streaming	N/A	1	40-2048 bits	Used in WEP, SSL and TLS; largely deprecated in current technologies.

Rounds: Repeating the XOR/left-shift iteration X times.

Asymmetric Algorithms

Diffie-Hellman

- **Uses key exchange protocol**
- **DOES NOT** use Public or Private keys
- **DOES NOT** itself encrypt or authenticate
    - It's an anonymous key-agreement protocol
- Used for Perfect Forward Secrecy (PFS)
    - Ephemeral Diffie-Hellman (EDH or DHE)
    - Combine with elliptic curve cryptography for ECDHE
- **The image below explain with an analogy the complex mathematical process of the key exchange on DH:**



- Diffie Hellman groups help by defining the size or type of key structure to use:

Diffie Hellman Groups

Group	Size
Group 1	768-bit modulus
Group 2	1024-bit modulus
Group 5	1536-bit modulus
Group 14	2048 bit modulus
Group 19	256-bit elliptic curve
Group 20	384-bit elliptic curve
Group 21	521-bit elliptic curve

RSA

Rivest Shamir and Edelman - Asymmetric algorithm, **generates the private and public key**.

- The first practical public-key cryptography systems
  - Encrypt, decrypt, digital signatures
- Based on the product of two large prime numbers
- Now released into the public domain
  - Used extensively for web site encryption and digital rights management

DSA (Digital Signature Algorithm)

- A standard for digital signatures
  - Is a modification of Diffie-Hellman key exchange for use in digital signatures
- **Combine** with **elliptic curve cryptography**
  - **ECDSA - Elliptic Curve Digital Signature Algorithm**
  - Fast and efficient digital signatures

ECC - Elliptic Curve Cryptography

- Used for encryption, digital signatures, pseudo-random generators, and more
- Can create a smaller key than RSA, provides the same security with increased performance (more faster).
- Instead of numbers, use curves
  - Uses smaller keys than non-ECC encryption
  - ECDSA - Elliptic Curve Digital Signature Algorithm

PGP - Pretty Good Privacy

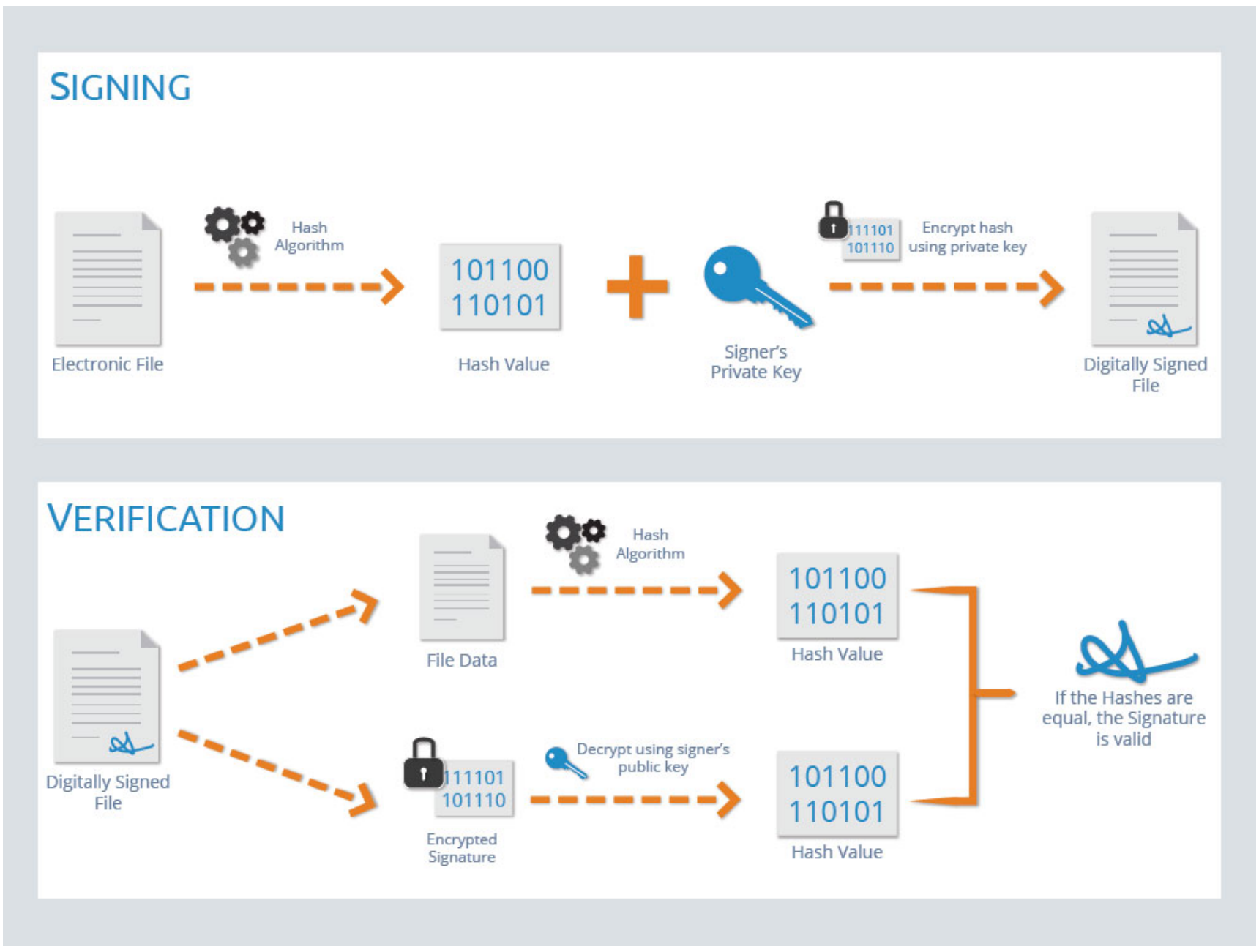
- Popular asymmetric encryption
- OpenPGP
- Provide privacy and authentication for data communication.
  - Used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP Certificates

- **Symantec Corp.**
    - Enterprise Solution
    - Encrypts Massa storage
    - Signing
    - Disk Encryption
    - BitLocker
    - FileVault
    - Enterprise Cloud Solutions
- **OpenPGP**
    - Free
    - Encrypted email
    - PKI Support
    - S/MIME
- **GPG (GNU Privacy Guard)**
    - Free Toolset
    - File and Disk encryption

Certificates and Trust

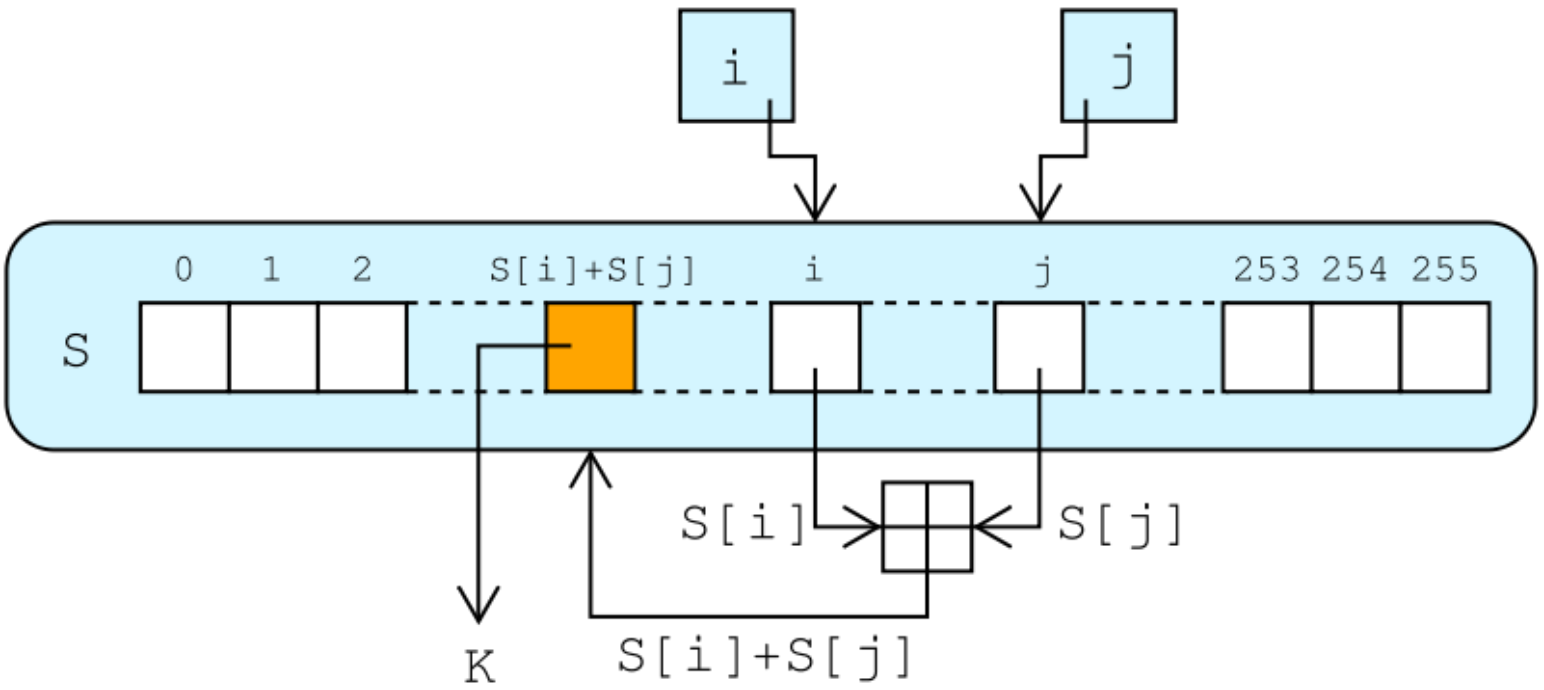
- Certificates include a **public key** and at least one **Digital signature**.
- **Digital Signature**
    1. To create a digital signature for a document
    2. **Signing:** You hash the document using your private key.
    3. **Verification:** Others can verify your digital signature with your public key.



Stream ciphers & Block modes

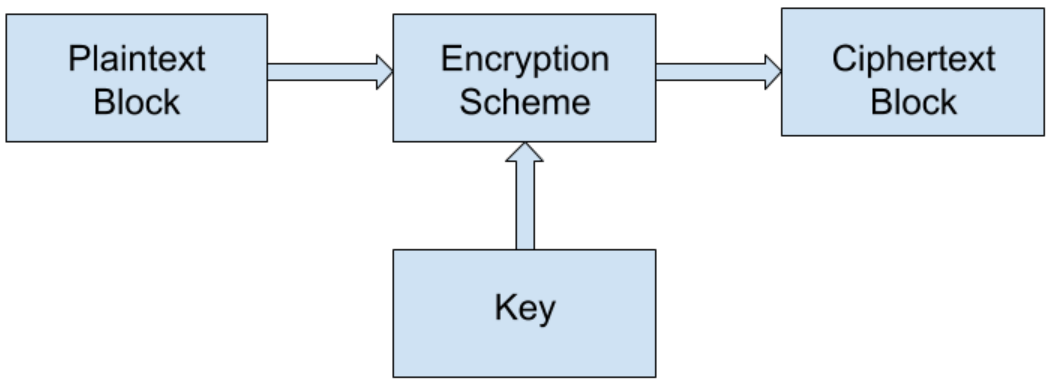
Stream ciphers

- Encryption is done one bit or byte at a time
  - Provides high speed, low hardware complexity
- Used with symmetric encryption
  - Not used in asymmetric encryption
- The starting state should never be the same twice
  - Key is often combined with an initialization vector (IV)



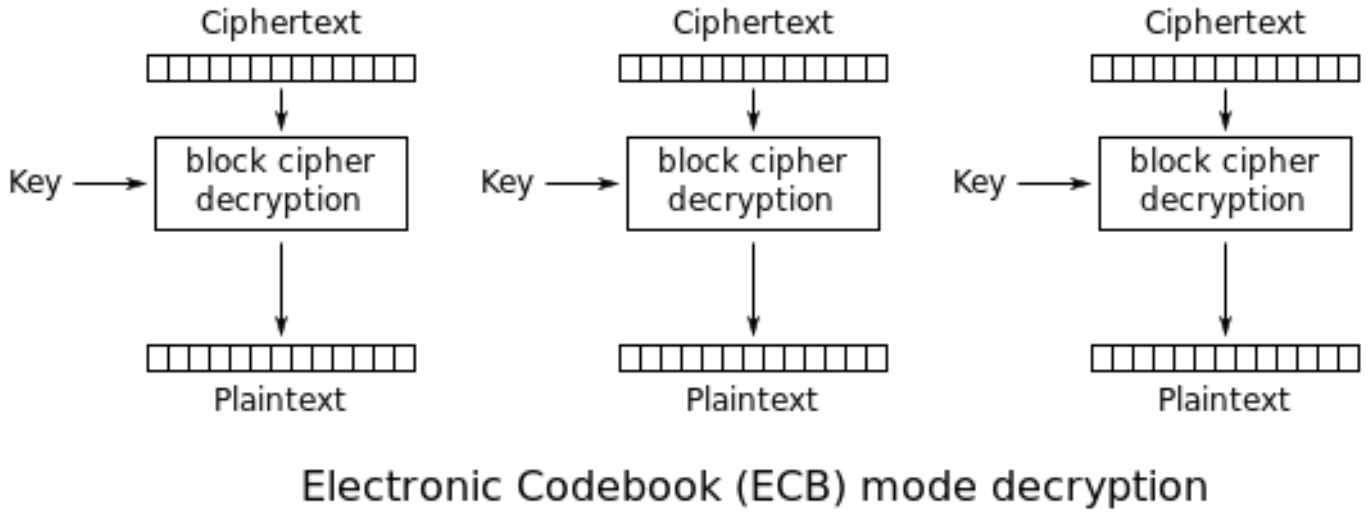
Block modes

- Encrypt fixed-length groups
  - Often 64-bit or 128-bit blocks
  - Pad added to short blocks
  - Each block is enrypted or decrypted independently
- Symmetric encryption
  - Similar to stream ciphers
- Block cipher modes of operation
  - Avoid patterns in the encryption
  - Many different modes to choose from



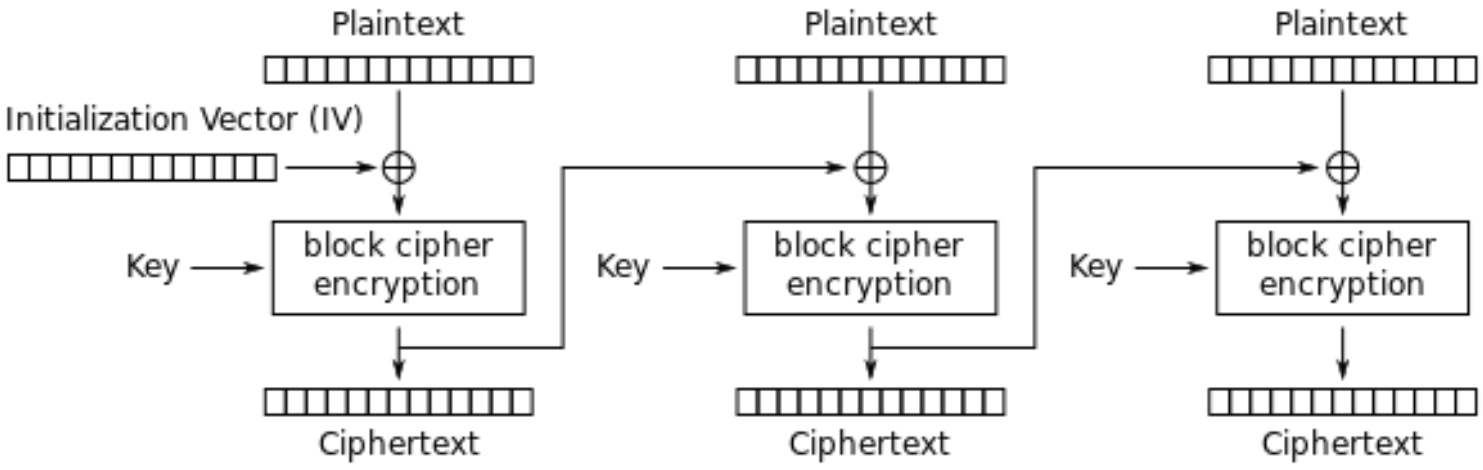
Block Cipher Modes

- **ECB - Eletronic Code Block** *(deprecated because nowdays is a week method that always produces the same output results with same input)*
  - Each block is encrypted with the same key. Identical plaintext blocks create identical ciphertext blocks



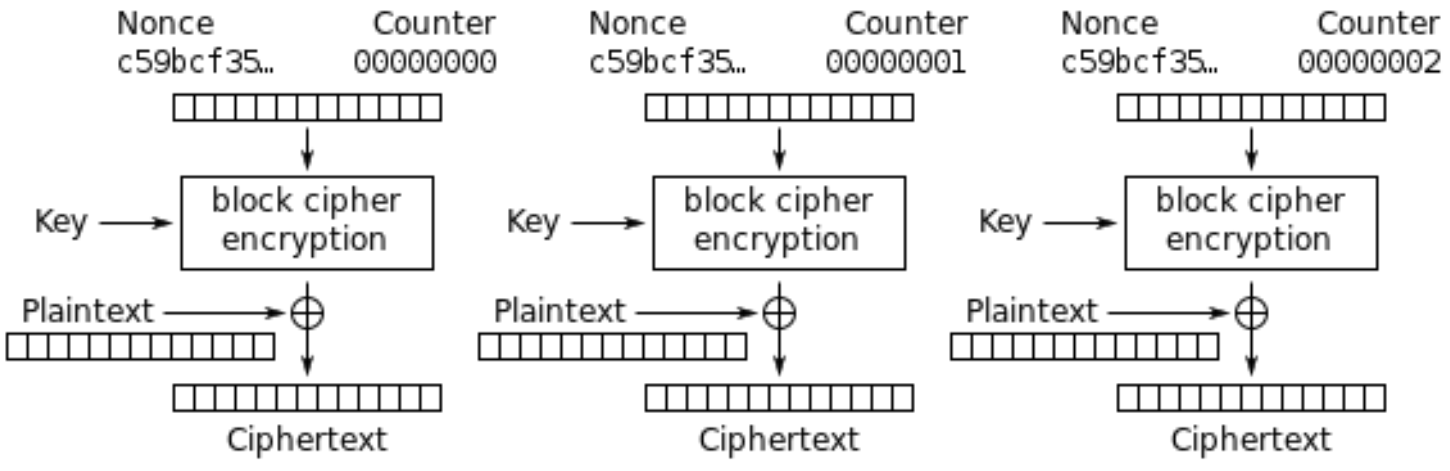
Electronic Codebook (ECB) mode decryption

- **CBC - Cipher Block Chaining**
  - Popular mode of operation
  - Each plaintext block is XORed with the previous ciphertext block
    - Adds additional randomization
    - Uses an initialization vector for the first block



Cipher Block Chaining (CBC) mode encryption

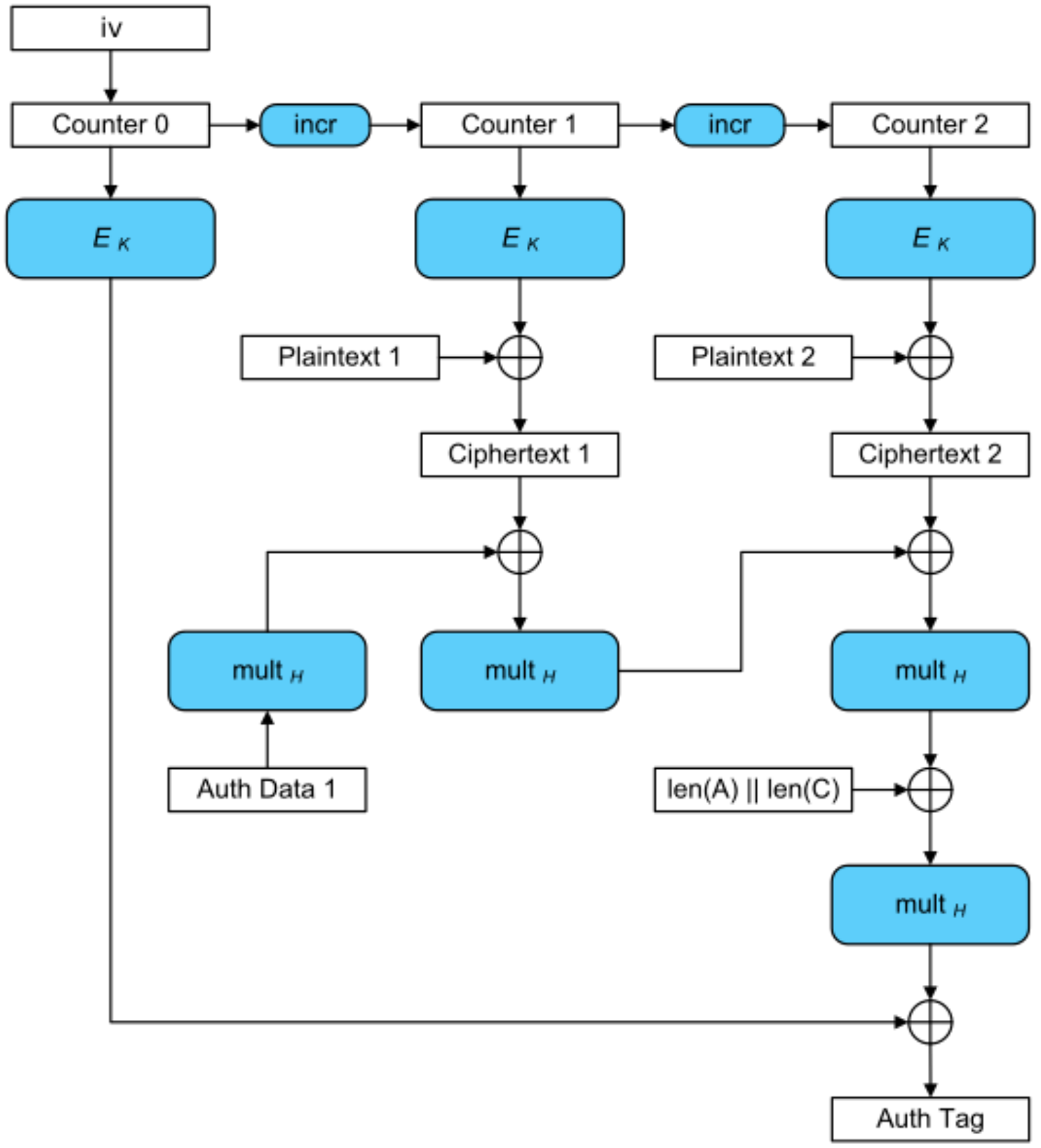
- **CTR (Counter)**
  - Block cipher mode / acts like a stream cipher
    - Encrypts successive values of a 'counter'
  - Plaintext can be any size, since it's part of the XOR
    - e.g., 8 bits at a time (streaming) instead of a 128-bit block



Counter (CTR) mode encryption

- **GCM (Galois/Counter Mode)**
  - Encryption with authentication
    - Authentication is part of the block mode

        - Combines Counter Mode with Galois authentication
    - Minimum latency, minimum operation overhead
        - Very efficient encryption and authentication
    - Commonly used in packetized data
        - Network traffic security (wireless, IPsec)
        - SSH, TLS



- *All block modes below uses IV, which ensures the output block is uniquely different*
- *A **Binary Block** is a plaintext converted into 16-bit, 64-bit or 128-bit binary ciphertext.*

Hashes

One-way encryption providing integrity.

- Impossible to recover the original message from the digest
- Used to **store passwords** providing **confidentiality**.

Hash	**Algo.**
MD5	128 bit hash

Hash	Algo.
SHA-1	160 bit hash
SHA256	256 bit hash

Examples:

```
String: hello world!

MD5 Hash: FC3FF98E8C6A0D3087D515C0473F8677
SHA-1 Hash: 430CE34D020724ED75A196DFC2AD67C77772D169
SHA256 Hash: 7509E5BDA0C762D2BAC7F90D758B5B2263FA01CCBC542AB5E3DF163BE08E6CA9
```

🛑 If you change a single character, the entire Hash value changes. **See the example below, changing the last character '!' to '.'**

- String: **hello world!**
  - `MD5 Hash: FC3FF98E8C6A0D3087D515C0473F8677`
- String: **hello world.**
  - `MD5 Hash: 3C4292AE95BE58E0C58E4E5511F09647`

Message digest

A message digest or hash, can be used to verify the integrity of a message by comparing the original hash to one generated after receipt of the message. If the two match, then integrity is assured. If they do not match, then the message was altered between transmission and receipt.

Hashing Algorithms

MD5 - Message Digest Algorithm

- First published in April 1992
- Replaced MD4
- 128-bit hash value
- 1996: Vulnerabilities found
  - Not collision resistant

SHA - Secure Hash Algorithm

- Developed by NSA

SHA-1

- Widely used
- 160-bit digest
- 2005: Collision attacks published

SHA-2 Family

- SHA-256 | minor version: SHA-224
- SHA-512 | minor version: SHA-384

SHA-3

- Uses a hash function called Keccack and has the same length of SHA-2.
- SHA-1 and SHA-2 have been replaced by the latest iteration of SHA known as SHA-3.

HMAC

Hash Message Authentication Code - Used in conjunction with symmetric key both to authenticate and verify integrity of the message.

- Verify data **integrity** and **authenticity**
    - No fancy asymmetric encryption is required
- Used in network encryption protocols
    - IPsec, TLS
- Requires each side of the conversation to have the same key

RIPEMD

RACE Integrity Primitives Evaluation Message Digest.

- Not very common
- Open Standard
- 128, 168, 256, 320 bit digests *(RIPEMD-128, RIPEMD-256, RIPEMD-320)*
- *Original RIPEMD was found to have collision issues (2004)*
    - Effectively replaced with RIPEMD-160 (no known collision issues)
    - Based upon MD4 design but performs similar to SHA-1

Practical use of Hashing 🛠️

- **Verify a downloaded file**
    - Hashes may be provided on the download site
    - Compare the donwloaded file hash with the posted hash value

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit (Installer)	Torrent	2020.2	3.6G	ae9a3b6a1e016cd464ca31ef5055506cecfc55a10f61bf1acb8313eddbe12ad7
Kali Linux 64-Bit (Live)	Torrent	2020.2	2.9G	e90e0cfb4bc8fc640219dba66c9fe4308c9502164e432c47a30af50ce9cb3ba2

- **Password storage**
    - Instead of storing the password in the clear, store a salted hash
    - Compare hashes during the authentication process

Keystretching

Combine a very long salt and a huge number of hashing iterations to make cracking even more harder. (e.g Hashing the hashed password `N` times)

Two most popular Key stretching libraries/ functions:

- **PBKDF2** (Password-Based Key Derivation Function 2) algorithm
    - Part of RSA public key cryptography standards (PKCS #5, RFC 2898)
- **bcrypt**
    - Generates hashes from passwords
    - An extension to the UNIX crypt library
    - Uses Blowfish cipher to perform multiple rounds of hashing

Example:

- **PBKDF2**

```
Password: 123456


Hash:
rYoSDg62evyzhE1+lWBa9A==:YaeMu71c8KU3H0RYFPle0Q==
```

- **bcrypt**

```
Password: 123456


Hash:
$2b$10$vES9mCPsE10//vOc1u01XeUVmJrZyHGMPaRfo39OIUoJ2g7iPtDnu
```

🛑 **Key streaming** - involves sending individual characters of the key through an algorithm and using a mathematical XOR function to change the output.

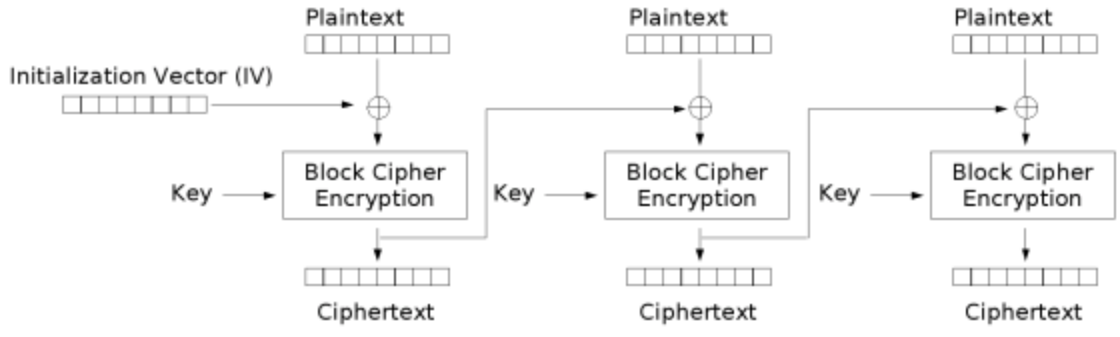
Cryptographic nonce

Cryptographic randomization schemes

- Used once - 'for the nonce'/ for the time being
- A random or pseudo-random number
    - Somehting that can't be reasonably guessed
    - Can also be a counter
- Use a nonce during the login process
    - Server gives you a nonce
    - Calculate your password hash using the nonce
    - **Each password hash sent to the host will be different**, so a replay attack won't work

Initialization vectors

- Is a type of nonce
    - Used for randomizing an encryption scheme
    - The more random the better
- Use in encryption ciphers, WEP, and older SSL implementations



Cipher Block Chaining (CBC) mode encryption

Salt

- A nonce most commonly associated with password randomization, making the pasword hash unpredictable.
- Salt is an arbitrary value
- Usually created by the application or OS storing passwords, added to the end of the password before it is hashed
- Makes cracking harder

  🛑 If the password database is breached, you can't correlate any passwords because **even users with the same password have different hashes stored**.

Salt Example:

1. Password: `123456`
2. Salt: `s4Lt1337=`
3. Add salt: `123456s4Lt1337=`
4. Hash function: `B2099F11CC4D34E9E8EED83E83D815732986D50097CA765BB8AFB355EABFFFB9`

Wireless Security

WEP - Wireless Equivalency Privacy

- 64/128 bit RC4 ICV
- **RC4** - Rivest Cipher 4 Stream Cipher Algorithm
- **ICV** - Integrity Check Value

  🛑 Very old and insecure; Don't use WEP!

WPA - Wi-Fi Protected Access

- Uses RC4 with TKIP (Temporal Key Integrity Protocol)
  - Initialization Vector (IV) is larger and an encrypted hash
  - Every packet gets a unique 128-bit encryption key
- **Personal | WPA-PSK**
  - TKIP + PSK
  - 64/128 bit RC4 MIC
  - Everyone uses the same 256-bit key
- **Enterprise | WPA-802.1X**
  - TKIP + RADIUS
  - 64/128 bit RC4 MIC
  - Authenticates users individually with an authentication server (e.g., RADIUS)

Temporal Key Integrity Protocol

- Mixed the keys
    - Combines the secret root key with the IV
- Adds sequence counter
    - Prevents replay attacks
- Implements a 64-bit Message Integrity Check
    - Protecting against tampering
- TKIP has it's own set of vulnerabilities
    - Deprecated in the 802.11-2012 standard

WPA2 - Wi-Fi Protected Access v2

- **802.11i** IEEE standard
- Enterprise
    - CCMP + RADIUS
    - 128 bit AES MIC
- Personal
    - CCMP + PSK
    - 128 bit AES MIC
- AES (Advanced Encryption Standard) replaced RC4
- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) replaced TKIP
- **CCMP**
    - Uses AES for data confidentiality
    - 128-bit key and a 128-bit block size
    - Requires additional computing resources
    - **CCMP provides Data confidentiality (AES), authentication, and access control**

	Authentication	Encryption	Suitable for corporate WAN	Suitable for home and small business WLAN
WEP	none	WEP	poor	less than good
WPA (PSK)	PSK	TKIP	poor	best
WPA2 (PSK)	PSK	AES-CCMP	poor	best
WPA (full)	802.1x	TKIP	better	good (expensive)
WPA2 (full)	802.1x	AES-CCMP	best	good (expensive)

Cryptographic Attacks 🗡️ 🔑

- **Known Plaintext Attack (KPA)**
    - The attacker knows at least one sample of both the plaintext and the ciphertext.
- **Brute Force**
    - Online - keep trying the login process (very slow), most accounts will lockout after a number of failed attempts.
    - Offline - force the hash, calculate a password hash, compare it to a stored hash; require a large computational resource requirement.
- **Dictionary Attack**
    - Is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.
- **Rainbow Table (dictionary of hashes)**
    - Pre-built set of hashes; The calculations have already been done
    - Need different tables for different hashing methods (Windows is different than MySQL)
    - Rainbow tables won't work with salted hashes
- **Collision Attack | Birthday Attack**
    - Is the same hash value for two different plaintexts. The attacker will generate multiple versions of plaintext to match the hashes. *(e.g In a classroom of 30 students, what is the chance of two students sharing a birthday? - about 70%)*

- **Replay Attack**
  - A hash with no salt, no session ID tracking, no encryption, can easily grabbed and replayed by an attacker.
- **Downgrade attack**
  - Makes it change the encrypted connection to the older one *(e.g. to cleartext; HTTPS to HTTP).*
- **Weak implementations**
  - One weak link breaks the entire chain.
  - Examples:
    - 802.11 WEP - The RC4 can be recovered by gathering enough packets; The algorithm didn't sufficiently protect the key
    - DES - Relatively small 56-bit keys; modern systems can brute force this pretty quickly

Hiding information

Obfuscation

1. Hidden sensitive data - providing confidentiality
2. Make the source code difficult to read
   - But it doesn't change the functionality of the code

Steganography

- The art of hide information inside the data (hide data within data), and can be encrypted.

Common steganography techniques:

- **Network Based** - Embed messages in TCP packets
- **Use an image** - Embed the message in the image itself
- **Invisible watermarks** - Yellow dots on printers can reaveal serial number and timestamps

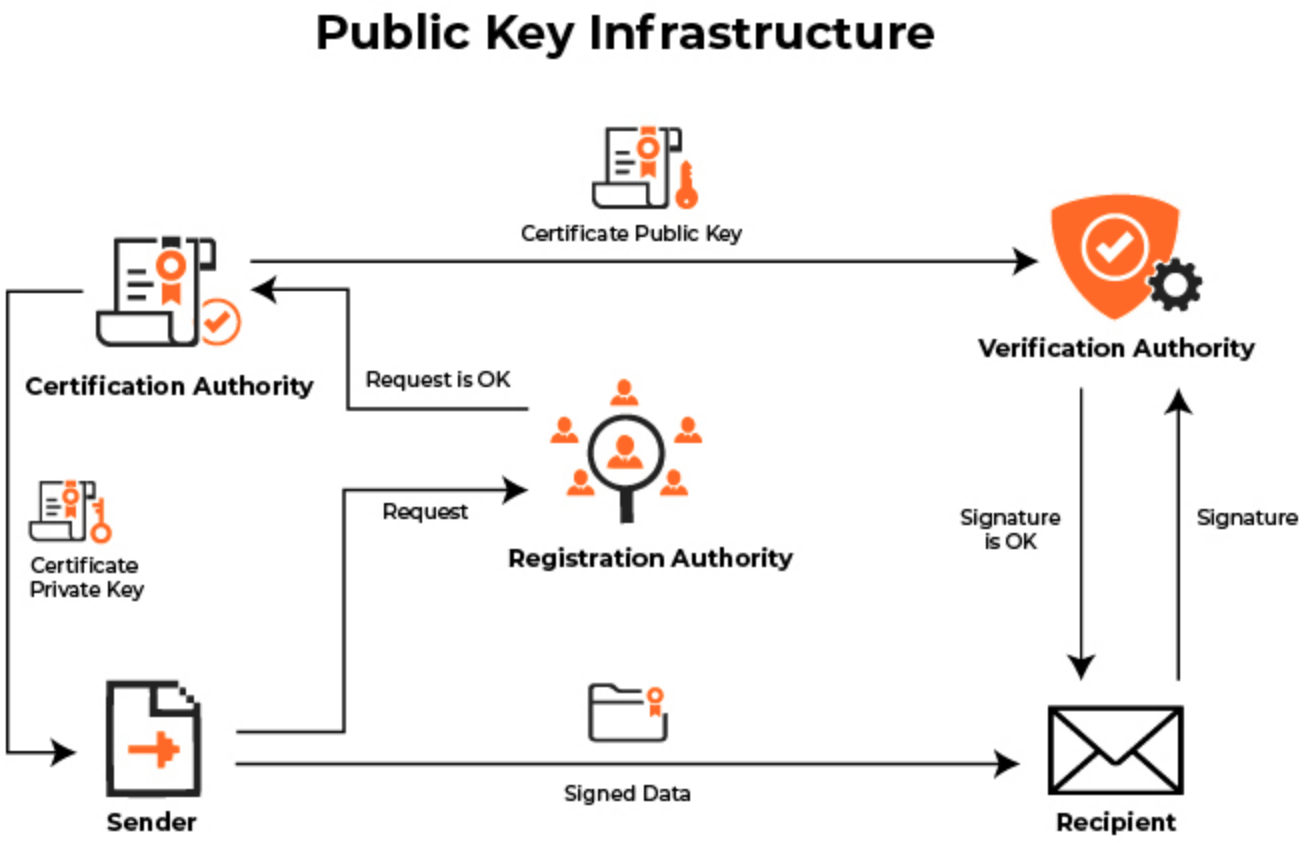
PKI - Public Key Infrastructure

Is a system consisting of **hardware, software, policies and procedures** that **creates, manage, distributes, uses, store and revoke DIGITAL CERTIFICATES.**

- Also refers to the binding of public keys to people or devices
    - The certificate authority (CA)
    - It's all about trust

PKI is the way we do internet. Uses a hierarchical structure with root servers.

- Certificate Authority (CA): Issues the certificates (Verisign, Thawte, etc).

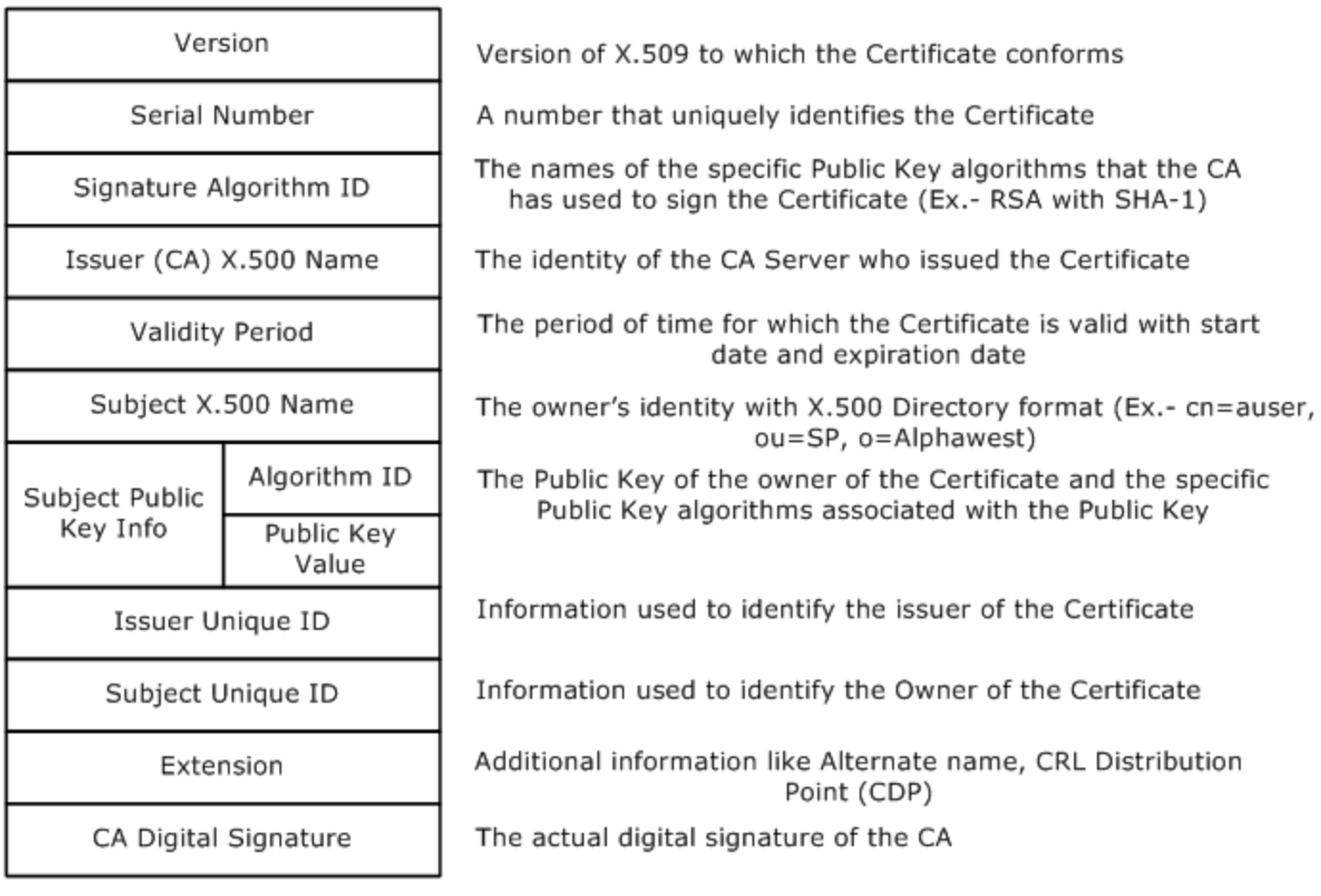


Key Management lifecycle ♻️

- **Key generation**
    - Create a key with the requested strength using the proper cipher
- **Certificate generation**
    - Allocate a key to a user
- **Distribution**
    - Make the key available to the user
- **Storage**
    - Securely store and protect against unauthorized use
- **Revocation**
    - Manage keys that have been compromised
- **Expiration**
    - A certificate may only have a certain 'shelf life'

Digital Certificates

- A public key certificate
    - Binds a public key with a digital signature
    - And other details about the key holder
- A digital signature adds trust
    - PKI uses Certificate Authority for additional trust
    - Web of Trust adds other ursers for additional trust
- Certificate creation can be built into the OS
    - Part of Windows Domain Services
    - 3rd-party Linux options



Commercial certificate authorities

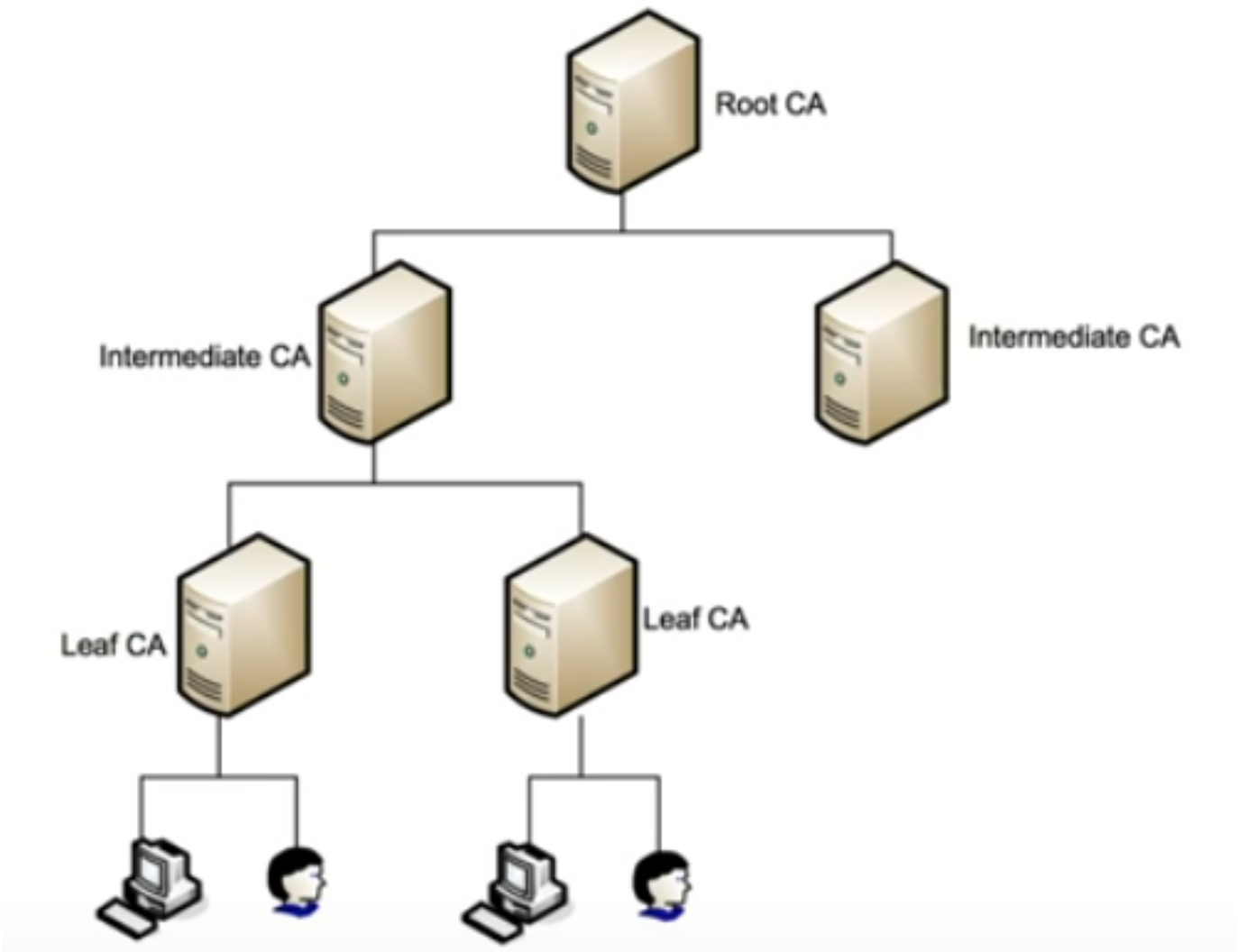
- Built-in your browser
- Purchase your web site certificate
    - It will be trusted by everyone's browser
- Create a key pair, send the public key to the CA to be signed
    - A certificate signing request (CSR)
- May provide different levels of trust and additional features

Private certificate authorities

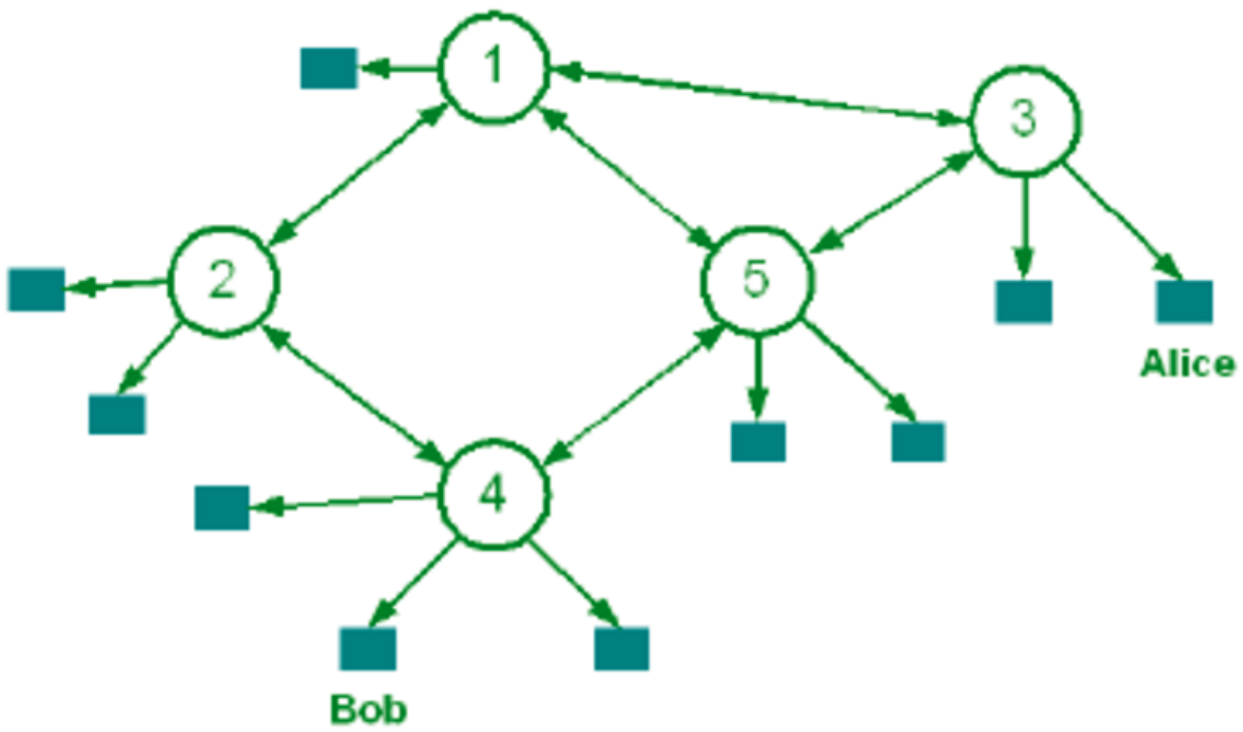
- You are your own CA
    - Build it in-house
    - Your devices must trust the internal CA
- Needed for medium-to-large organizations
    - Many web servers and privacy requirements
- Implement as part fo your overall computing stragey
    - Windows Certificate Services, OpenCA

PKI trust relationships

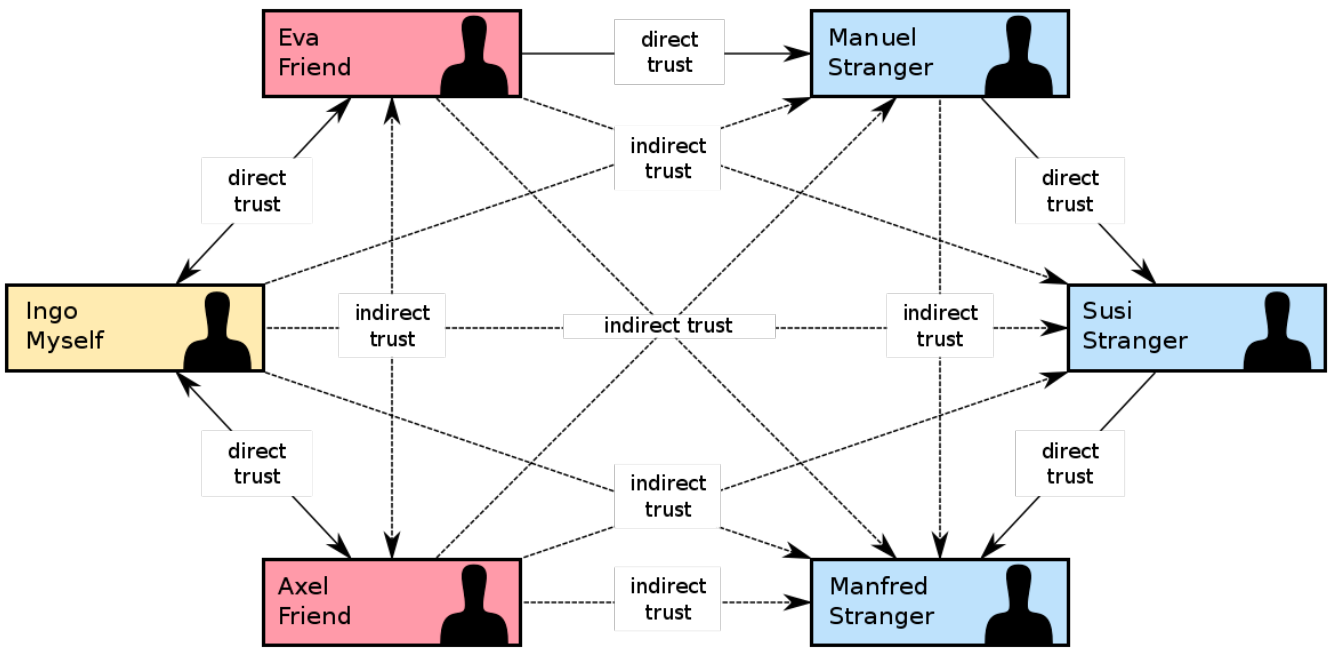
- **Single CA**
    - Everyone receives their certificates from one authority
- **Hierarchical**
    - Single CA issues certs to intermediate CAs
    - Distributes the certificates management load
    - Easier to deal with the revocation of an intermediate CA than the root CA



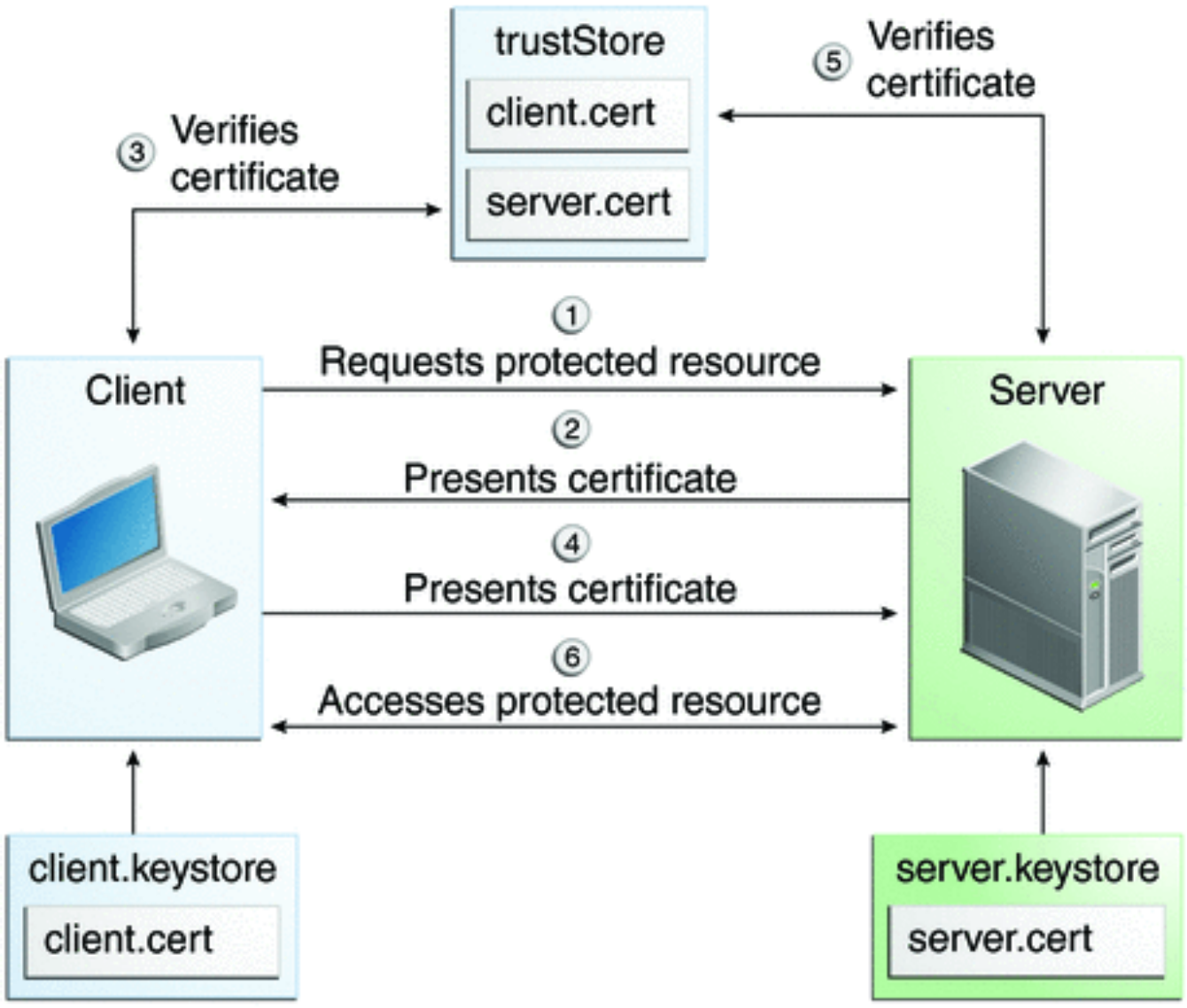
- **Mesh**
  - Cross-certifying CAs
  - Doesn't scale well



- **Web-of-trust**
  - Everyone is an authority
  - Alternative to traditional PKI



- **Mutual Authentication**
  - Mutual authentication requires both sides of a communications session to authenticate to each other.



🛑 **Certificate chaining** - Chain of trust; List all the certs between the server and the root CA; **The chain starts with the SSL certificate and ends with the Root CA**.

CRL - Certificate Revocation List ❌

A list of serial numbers of certificates that have been revoked or are no longer valid, therefore should not be relied on.

OCSP - Online Certificate Status Protocol

Is a more **modern version of CRL** that are used today, have a **better performance**.

🛑 **OCSP stapling** - The certification holder verify their own status instead of CA server; OCSP status is 'stapled' into the SSL/TLS handshake, digitally signed by the CA

🛑 Early Internet Explorer versions did not support OCSP

Types of Certificates

Root certificate

The public key certificate that identifies the root CA (Certificate Authority)

- Everything starts with this certificate
- The root certificate issues other certificates
  - Intermediate CA certificates
  - Any other certs

Web server SSL certificates

- Domain validation certificate (DV)
  - Owner of the certificate has some control over a DNS domain
- Exntended validation certificate (EV)
  - Additional checks have verified the certificate owner's identity *(the green name on the address bar)*
- Subject Alternative Name (SAN)
  - Extension to an X.509 cert
  - Lists additional identification information
  - Allows a certificate to support many different domains
- Wildcard domain
  - Certificates are based on the name of ther server
  - A wildcard domain will apply to all server names in a domain (e.g., *.google.com)

Self-signed certificates

- Internal certificates don't need to be signed by a public CA
  - Your company is the only one going to use it
  - No need to purchase trust for devices that already trust you
- Build your own CA
  - Issue your own certificates signed by your own CA
- Install the CA certificate/trusted chain on all devices

Machine and computer certificates

- You have to manage many devices
  - Often devices that you'll never physically see
- How can you truly authenticate a device?
  - Put a certificate on the device that you signed
- Other business processes rely on the certificate
  - Access to the remote access VPN from authorized devices
  - Management software can validate the end device

User certificates

- Associate a certificate with a user
  - A powerful electronic 'id card'
- Use as an additional authentication factor
  - Limit access without the certificate
- Integrate onto smart cards
  - Use as both a physical and digital access card

Email certificates

- Use cryptography in an email platform
  - You'll need public key
- Encrypting emails
  - Use a recipient's public key to encrypt
- Receive encrypted emails
  - Use your private key to decrypt
- Digital signatures
  - Use your private key to digitally sign an email
  - Non-repudiation, integrity

Code signing certificate

- Developers can provide a level of trust
- The user's OS will examine the signature
    - Checks the developer signature
    - Validates that the software has not been modified

List of All Ports for Security+ Exam

Port	Description
20	File Transfer Protocol - FTP Data
21	File Transfer Protocol - FTP Control
22	SSH - Secure Shell Remote Login Protocol / SCP / SFTP
23	Telnet
25	SMTP - Simple Mail Transfer Protocol
49	TACACS+ - Login Host Protocol
53	DNS - Domain Name System
67	DHCP - Bootp-server (Outgoing DHCP)
68	DHCP - Bootp-client (Incoming DHCP)
69	TFTP - Trivial File Transfer Protocol
80	HTTP
88	Kerberos - Secure Encrypted Login
110	POP3 - Post Office Protocol (Email)
119	NNTP - Network News Transfer Protocol
123	NTP - Network Time Protocol
137, 138, 139	NETBios Protocol
143	IMAP 4 - Internet Message Access Protocol (Email)
161, 162	SNMP - Simple Network Management Protocol
389	LDAP - Lightweight Directory Access Protocol

Port	Description
443	HTTPS - HTTP over TLS/SSL
445	SMB
464	Kerberos
465	SMTP/SMTPS over SSL
500	ISAKMP - Internet Security Association and Key Management Protocol - IPSec
514, 6514	SysLog Servers & SysLog TCP over TLS
636	LDAP over SSL
860	iSCSI - Internet Small Computer Systems Interface
993	IMAP 4S - IMAP over TLS/SSL (Email)
995	POP3 over SSL
989, 990	FTP - FTP Data and Control over TLS/SSL
1194	OpenVPN
1645, 1646	RADIUS
1812, 1813	RADIUS
1701	L2TP - Layer 2 Tunneling Protocol (IPSec - used in VPN)
1723	PPTP - Point-to-Point Tunneling Protocol - VPN
3389	RDP - Remote Desktop Protocol
5060, 5061	SIP - Session Initiation Protocol