Network Security

DOMAIN 4.0

MODULE 14

Network Security Topics

Common Security Concepts

Common Attack Types

Spoofing-based Attacks

Hijacking and MITM

Social Engineering

Network Segmentation

Private VLANs

Single Organization Authentication

Extending Authentication

Authorization

Network Device Hardening

Wireless Security

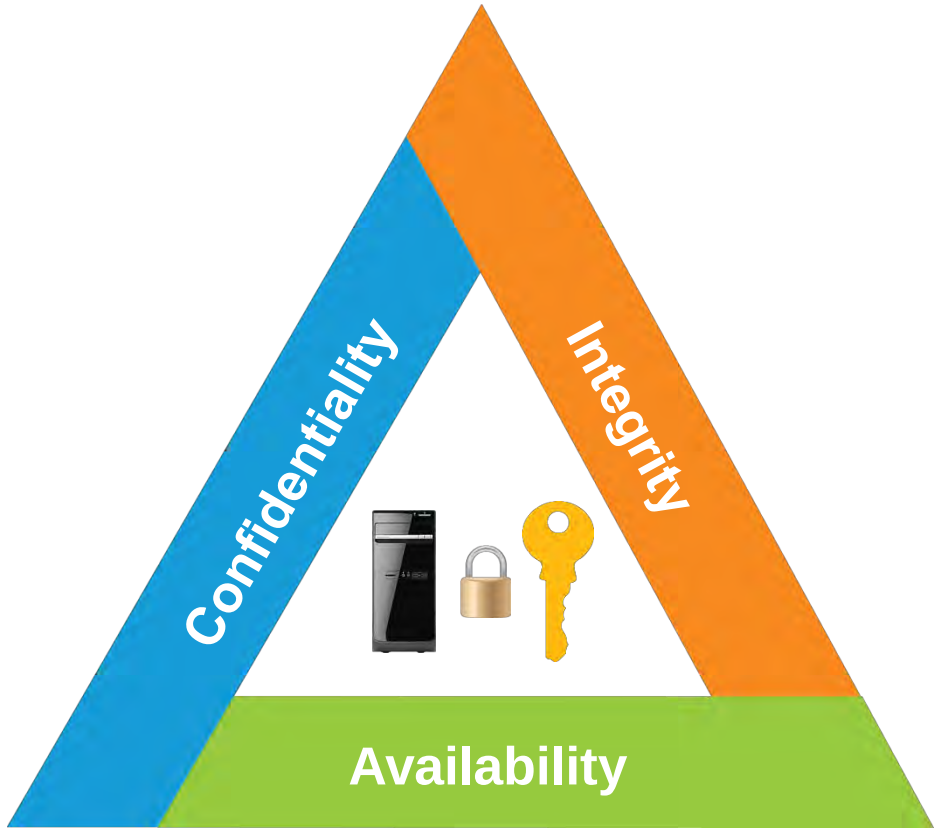
Remote Access Security

IoT Security

Physical Security

Common Security Concepts

The CIA Triad



Common Security Terms

Term	Definition
Asset	Anything of value that could be compromised, stolen, or harmed, including information, systems, personnel, physical resources, and reputation
Threat	Any event or action that could potentially cause damage to an asset or an interruption of services
Vulnerability	A condition that leaves the system and its assets open to harm
Exploit	A technique that takes advantage of a vulnerability to perform an attack
Risk	The likelihood of a threat occurring, as well as its potential damage to assets
Attack	The active attempt by a threat actor to break into and exploit a vulnerable system, data, or other resource
Breach	The result of a successful attack. Can include theft, destruction, or loss of availability of data, a system, or other resources
Exposure	The level, usually expressed in percentage, to which a resource is at direct risk of attack
Social engineering	The practice of using deception and trickery against human beings as a method of attack

Common Security Terms (cont'd)

Term	Definition
Control	A countermeasure that you put in place to avoid, mitigate, or counteract security risks due to threats or attacks; also known as a safeguard
Role-based access	Granting permissions to resources based on a user's job duties; permissions are granted to the role, as opposed to a specific person
Least privilege	A principle that states that a subject (user, computer, application) should be given only those privileges needed for it to complete its task
Zero trust	A security model that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data Zero trust states that trust in itself is a vulnerability Zero Trust also assumes that there is no traditional network edge • Networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location
Defense in depth	The practice of providing security in multiple layers for more comprehensive protection against attack

Risk Management

The process of identifying, assessing and controlling threats to your network and assets

You implement policies, procedures, and technology to reduce threats, vulnerabilities, and consequences

IT risk management does not lie with the IT department alone

- A data breach could serious cause financial, legal, and reputational damage to the organization
- Senior leadership and all company departments must be involved
- Everyone in the organization must take ownership of risk

Risk Management Process

1. Identify as many specific risks as possible:
   - Malware, hacking, insider, natural disaster, fire, failed equipment, Internet/telecom loss, supply chain problems, accidents
   - Consider all sources including internal, external, vendors, partners
2. Prioritize the risks based on either:
   - Monetary cost to the company annually (cost of incident x expected annual frequency)
   - Probability x severity
3. Determine how you will deal with the risk:
   - Mitigate (put administrative and technical controls in place to reduce the risk or harm)
   - Avoid (get rid of the asset or stop engaging in the risky activity)
   - Transfer (buy insurance to cover any loss if the threat is realized)
   - Deny (pretend it will never happen)
4. Draw a line for when you will stop trying to mitigate the risk
   - Unforeseen risks, and risks that are not worth the effort go below the line
     - “Don’t speed $100 protecting a $10 item!”
     - “If an airplane fell on our building, that would be catastrophic, but the likelihood is too small for us to move our location”
   - Have a contingency/disaster recovery plan for dealing with everything below the line

Security Risk Assessments

Assessment Type	Description
Posture Assessment (aka Security Assessment) *Includes all of the below:*	A point-in-time view of how secure your network is against attack • Create a complete map of your entire attack surface • Data, devices, OSes, apps, networks, etc. • Document every possible avenue of attack • Make recommendations to discovered weaknesses
Threat Assessment	Look outside your organization to determine what threats exist that could potentially lead to problems • Hackers • Natural disasters • Terrorists / sabotage • Regional instability
Vulnerability Assessment	Look inside your organization for structural flaws and weaknesses • People • Processes • Technology
Penetration Testing	A controlled, active attempt (usually by a hired 3rd party) to bypass your controls and break into your network

Business Risk Assessments

Process Assessment

1. Document critical business processes
2. Identify potential risks to these processes
3. Determine how to protect the processes from identified risk
4. Determine what controls are already in place, and what control gaps need to be corrected

Vendor Assessment

- An evaluation and approval process to determine if prospective vendors and suppliers can meet your standards and obligations once they are under contract
- Determine if any of your vendors, suppliers, partners put your network or organization at risk
  - Does your customer data leave the vendor's production systems?
  - Does the vendor support single sign-on?
  - Does the vendor have an employee security awareness program?
  - Would security incidents at the vendor expose your organization to attack/legal/financial/reputational jeopardy?
  - Does the vendor have security policy gaps that would put you at risk?
  - Are there any risks to your supply chain that could affect you?

Separation of Duties

AKA Segregation of Duties

Designed to prevent conflicts of interest

Limit one person from having too much power

If not implemented, can result in:

- Fraud
- Undetected errors
- Unauthorized privilege escalation

Separation of Duties Examples

Approve giving a user elevated privilege and then assign the privilege

Backup and restore data

Create a purchase order and approve that order

Enter a journal entry and approve the entry

Deposit cash and perform reconciliation of bank statements

Create a new vendor and make vendor payments

Maintain credit limits and release credit holds

Order products and account for the inventory

Threat Types

External

- Hackers
- Malware
- Phishing
- DDoS
- Ransomware

Internal

- Accidents
- Negligence
- Malicious Insider
  - contractors, vendors, disgruntled employees, industrial espionage

Zero-day Attacks

AKA 0-day

An attack against a vulnerability for which there is currently no fix

Security defenses are designed to mitigate known flaws

Attackers highly value zero-day exploits because they often go unnoticed for a log time

The average time gap between discovering and patching a new vulnerability is 69 days

Can be mitigated by a proactive, defense-in-depth approach

There is an arms race between threat actors finding and trying to exploit a vulnerability, and the vendors working to release a patch to fix it

Common Vulnerabilities and Exposures (CVE)

A reference-method for publicly known information-security vulnerabilities and exposures

The program uniquely identifies vulnerabilities

- Associates specific versions of code bases (e.g., software and shared libraries) to those vulnerabilities
- The use of CVEs ensures that two or more parties can confidently refer to a CVE identifier (ID) when discussing or sharing information about a unique vulnerability
- Used by hackers and security professionals alike

Each record contains an identification number, a description, and at least one public reference

Currently, there are 164,777 CVE Records that you can download or search

https://cve.mitre.org/

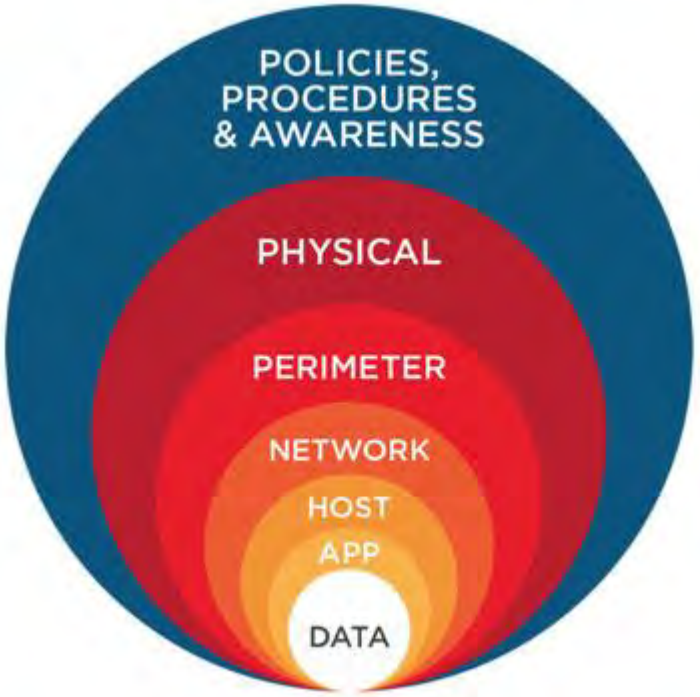
https://www.cve.org/

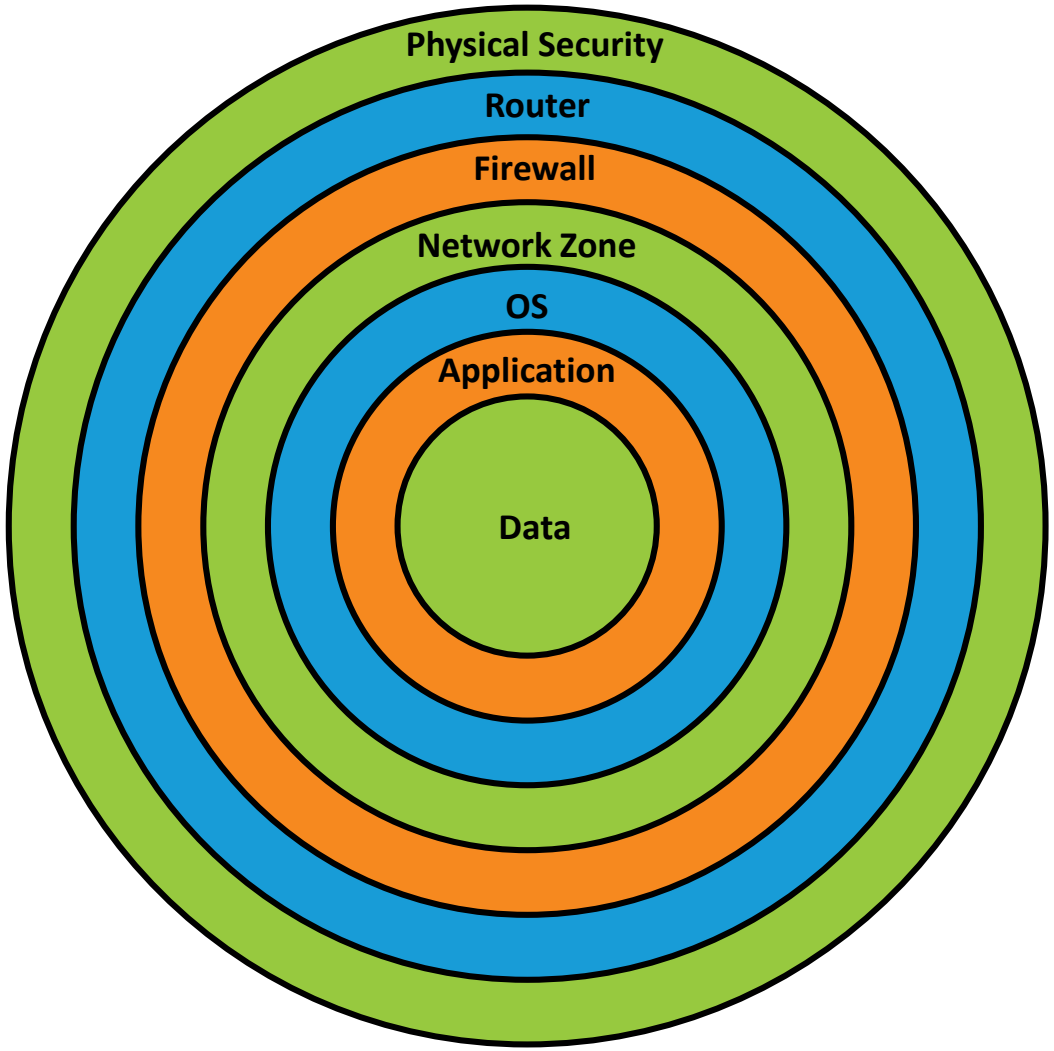
Control Types

Type	Examples
Physical	Closed-circuit surveillance cameras Motion, sound, or thermal alarm systems Lighting / guided paths Security guards Picture IDs / badges / PIV or CAC cards Barred windows Access control locks Mantraps, turnstiles
Technical	Encryption Antivirus / Anti-Malware Software / Patching Firewalls / ACLs SIEM / IDS / IPS Active Directory Group Policies
Administrative	Policies Procedures Company rules

Defense in Depth

The practice of providing security in multiple layers for more comprehensive protection against attack





80 / 20 Rule

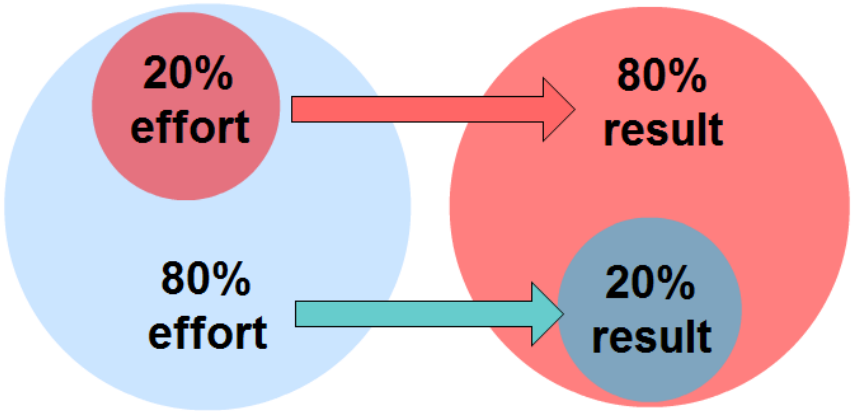
You can address 80% of your risk with 20% of the effort

Mitigate 80% of vulnerabilities by focusing on top 20% of technical controls:

- Remove anything unnecessary including services, protocols, and defaults
- Keep patch levels, anti-malware, and IDS signatures current
- Implement strong authentication and access control

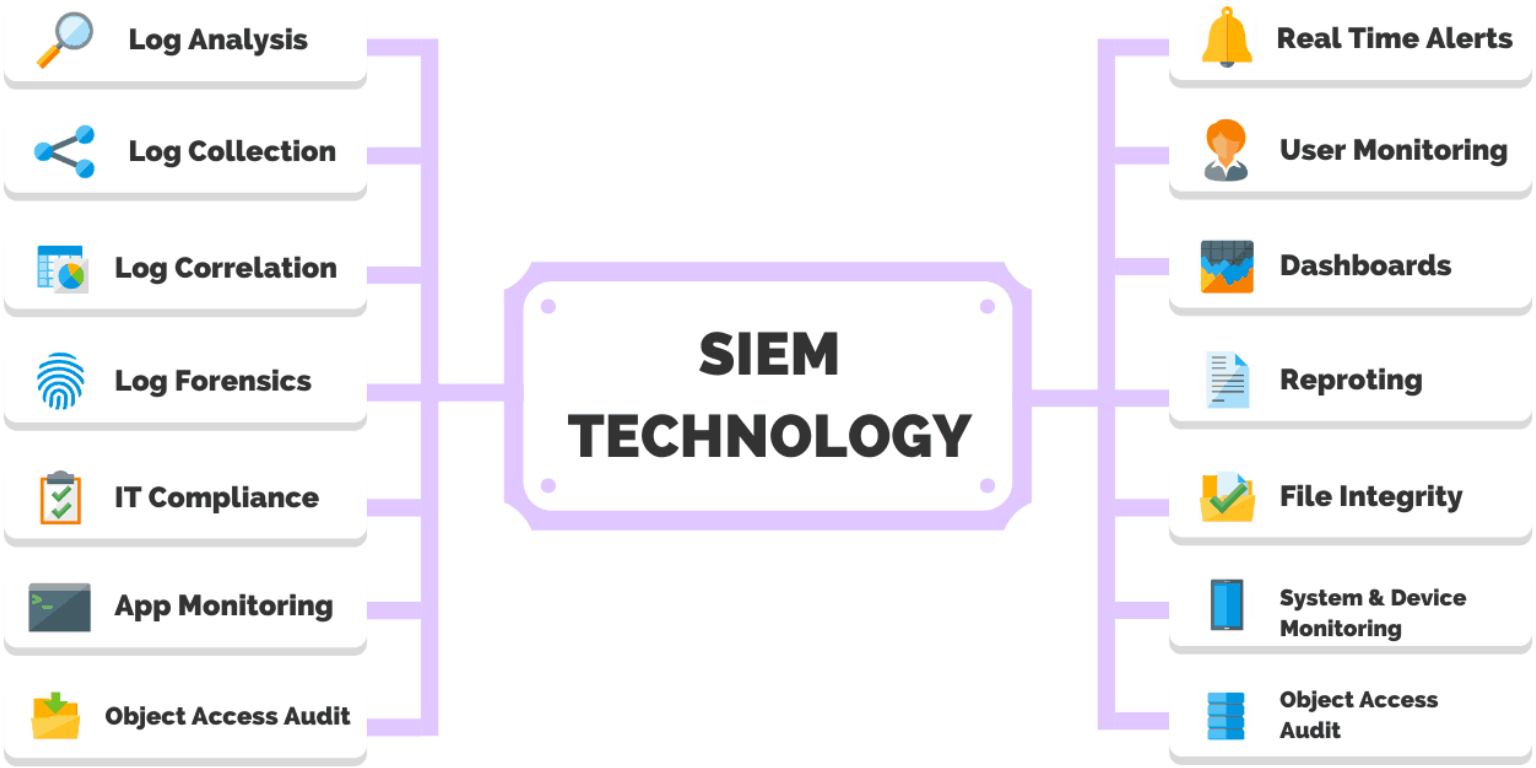
Works even better within defense in depth

- 80/20 rule at each layer
- The attack surface at each layer then starts out smaller



Security Information and Event Management (SIEM)

A software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure



Common Attack Types

Malware

A computer program that is deliberately created to cause harm to a computer, network or user

Can perform malicious tasks:

- Recording keystrokes
- Altering programs or settings
- Data theft
- Deleting, modifying or encrypting sensitive/financial information

Types of Malware

Term	Definition
Virus	Self-replicates by inserting its code in a legitimate program or file
Worm	A virus that can clone itself and self-spread across a network
Trojan Horse	Disguises itself by hiding inside a legitimate program. When the user executes the program, the malicious code is also run.
Spyware	Collects user activity and account information without a user's knowledge
Phishing	Sending malicious email designed to trick people into falling for a scam
Logic Bomb	Malware that lies dormant until triggered by a date or event
Buffer Overflow	Deliberate insertion of too much data into a program, causing the program to crash or behave differently. Often used to gain unauthorized access or execute malicious commands.

Types of Malware (cont'd)

Term	Definition
Ransomware	Files are encrypted or locked until the user pays a ransom. Supposedly, once the ransom is paid, the attacker releases the keys to unlock the files.
Keylogger	Monitors and records everything a user types.
Rootkit	Replaces key components of your operating system so it can run undetected
Bot	A combination of Trojan, virus and worm that performs automated malicious tasks on command
Backdoor	A covert communication channel that bypasses authentication or other main functions of a program
Adware	Uses unsolicited advertising techniques such as popups and browser redirection to generate revenue or download additional malware

Malware Countermeasures

Keep antivirus/antimalware programs up-to-date

Educate users to not click suspicious links or open unsolicited emails

- Show plenty of examples so they know how to recognize what is “suspicious”

Implement IDS/IPS on the network

Disable scripts in email

Scan attachments

Implement strict software installation policies

Disallow jailbroken or rooted mobile devices on the network

Restrict user privileges on a system

Password Attacks

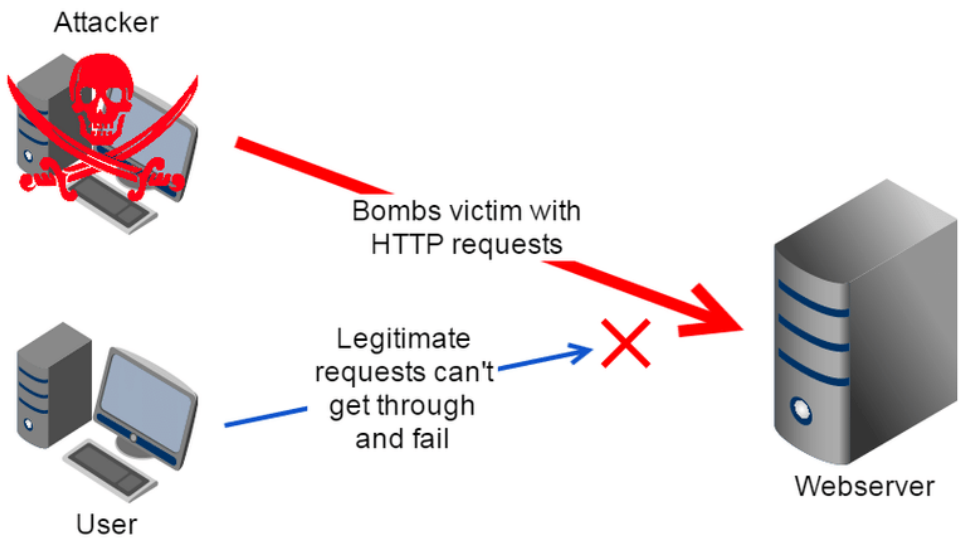
Attack Type	Description	Countermeasures
Dictionary	An automated tool that tries a long list of potential passwords to see if one works	Require passwords to be long, complex, unusual, and changed regularly; require multi-factor authentication
Rainbow Table	A dictionary in which the passwords have been pre-computed into hashes (the format in which the password is stored on the OS)	Same as above
Brute Force	Systematically trying every possible combination of letters, numbers, and symbols until the password is discovered	Same as above, with special emphasis on password length
Pass-the-Hash	The attacker captures a password hash, and rather than attempting to crack it, uses the hash in place of the normal characters to authenticate	Disable OS settings that permit password hash dumps from memory
Social Engineering	Using trickery to get a user to divulge their password	User education

Denial-of-service (DOS)

An attack meant to shut down a machine or network, making it inaccessible to its intended users

Common methods include:

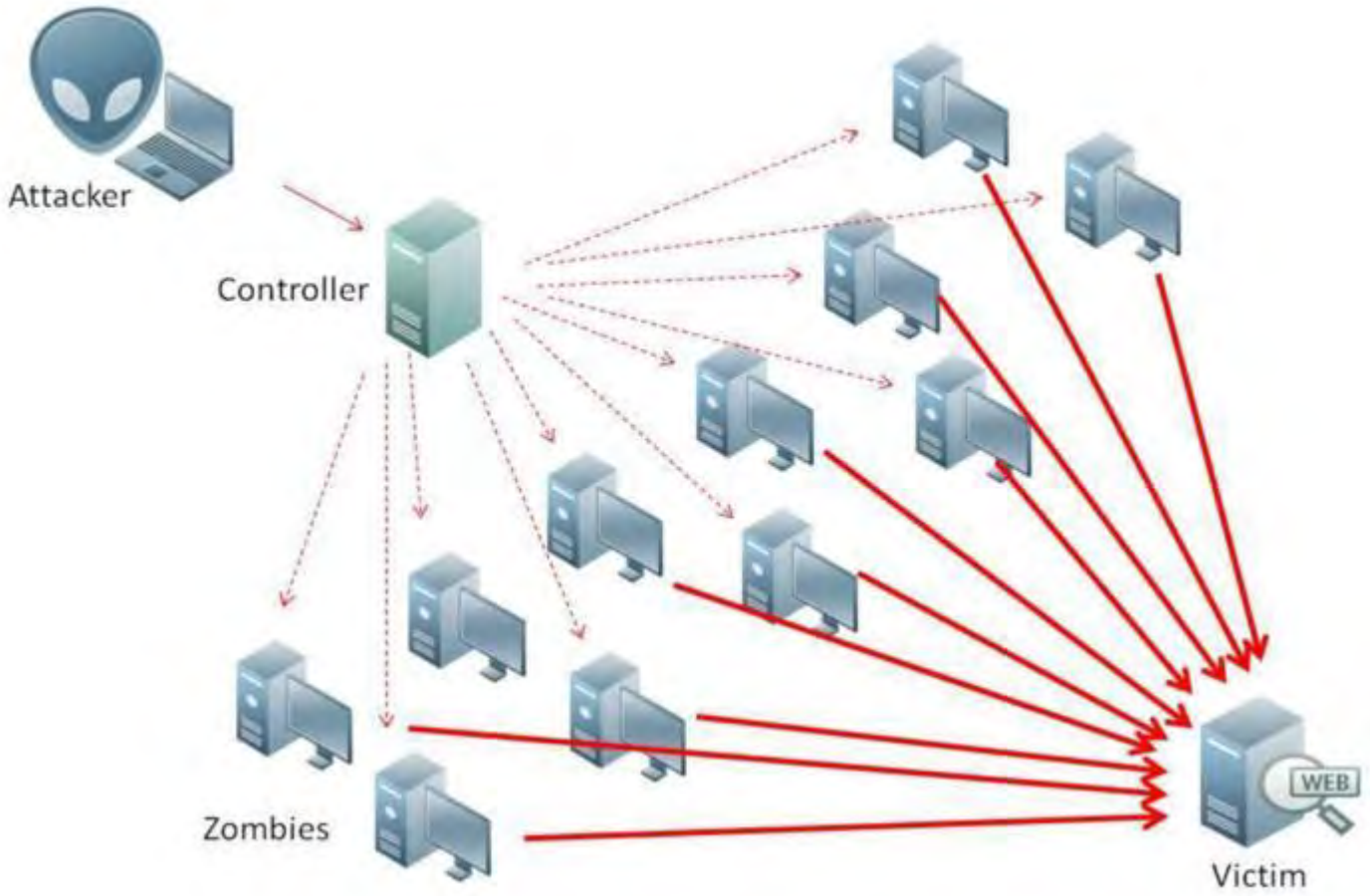
- Flooding the target with traffic
- Sending a machine malicious code that triggers a crash
- Consuming all of the CPU, memory, or disk resources
- Consuming all of the allowed concurrent connections



Distributed Denial-of-service (DDOS)

Compromise multiple machines

Use them in a coordinated attack against a target



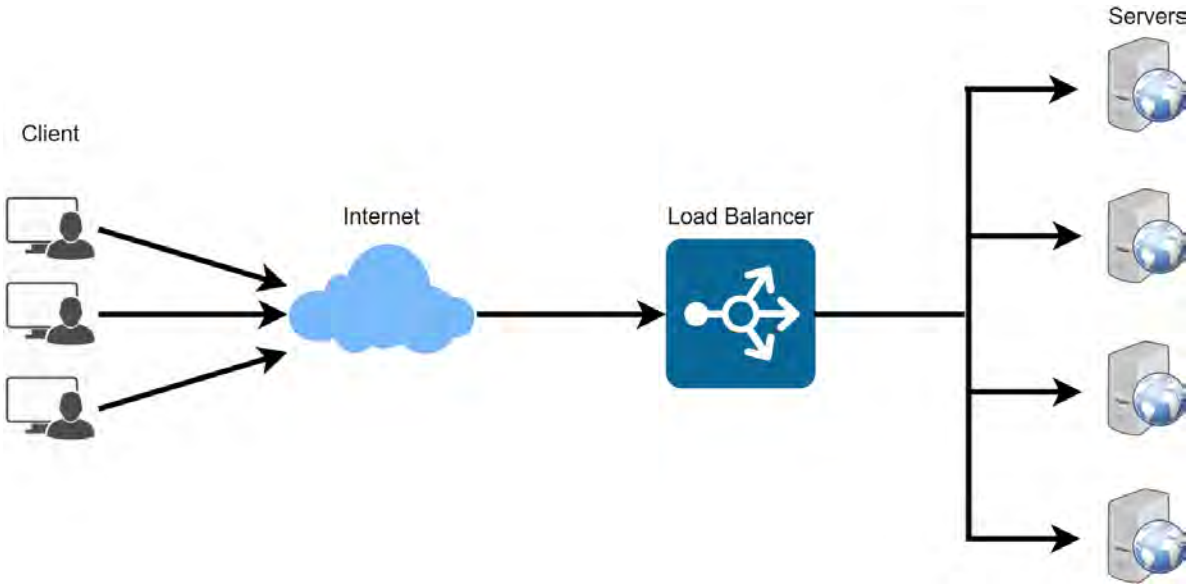
DoS/DDoS Countermeasures

Load balancing / distributed systems

Use an upstream router to filter traffic

Using a cloud-based content delivery network

- Maintain duplicate systems around the world
- Direct visitors to the nearest system



Distributed Content Delivery Example

Botnet/Command and Control

Compromise many machines (zombies) including:

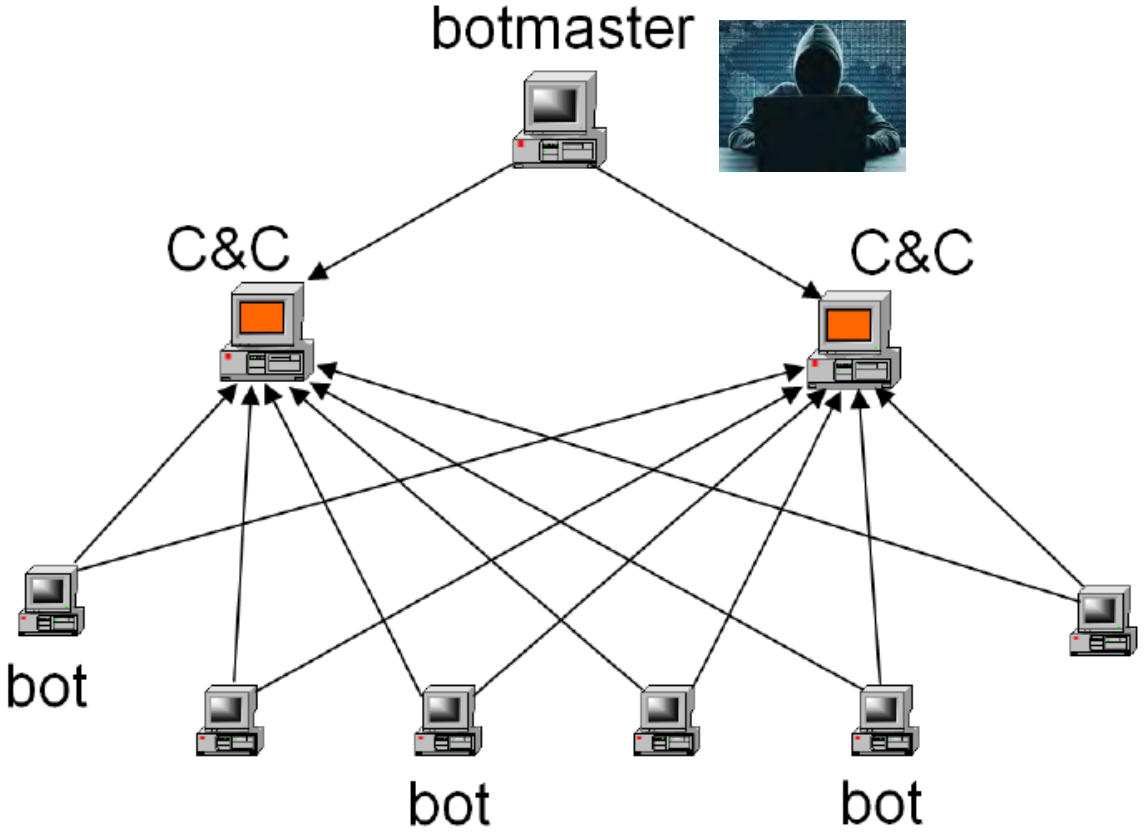
- Computers
- Mobile devices
- IoT devices
- Infrastructure devices (Wi-Fi routers)
- Network-based copiers/printers

Zombies are regionally / locally controlled by a command and control center

Botnets can be used to:

- Launch DDoS attack
- Steal personal data
- Mine cryptocurrency

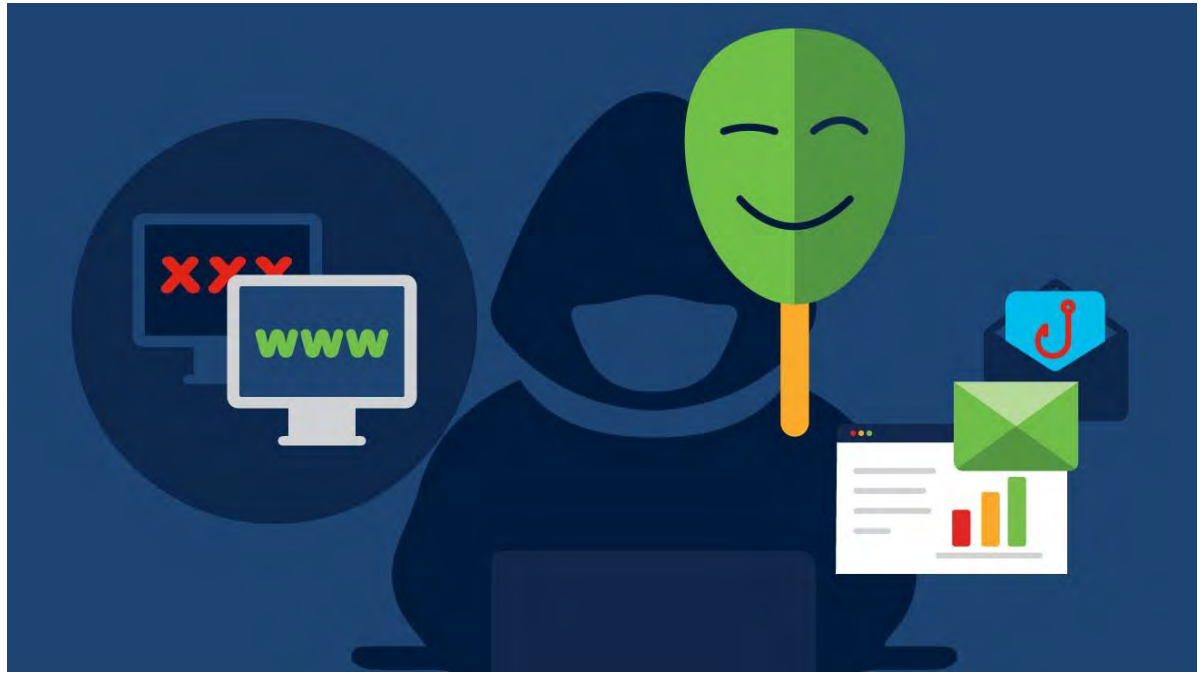
Botnets can also be rented out as Malware-as-a-Service (MaaS)



Spoofing-based Attacks

What is Spoofing?

The act of disguising a communication from an unknown source as being from a known, trusted source

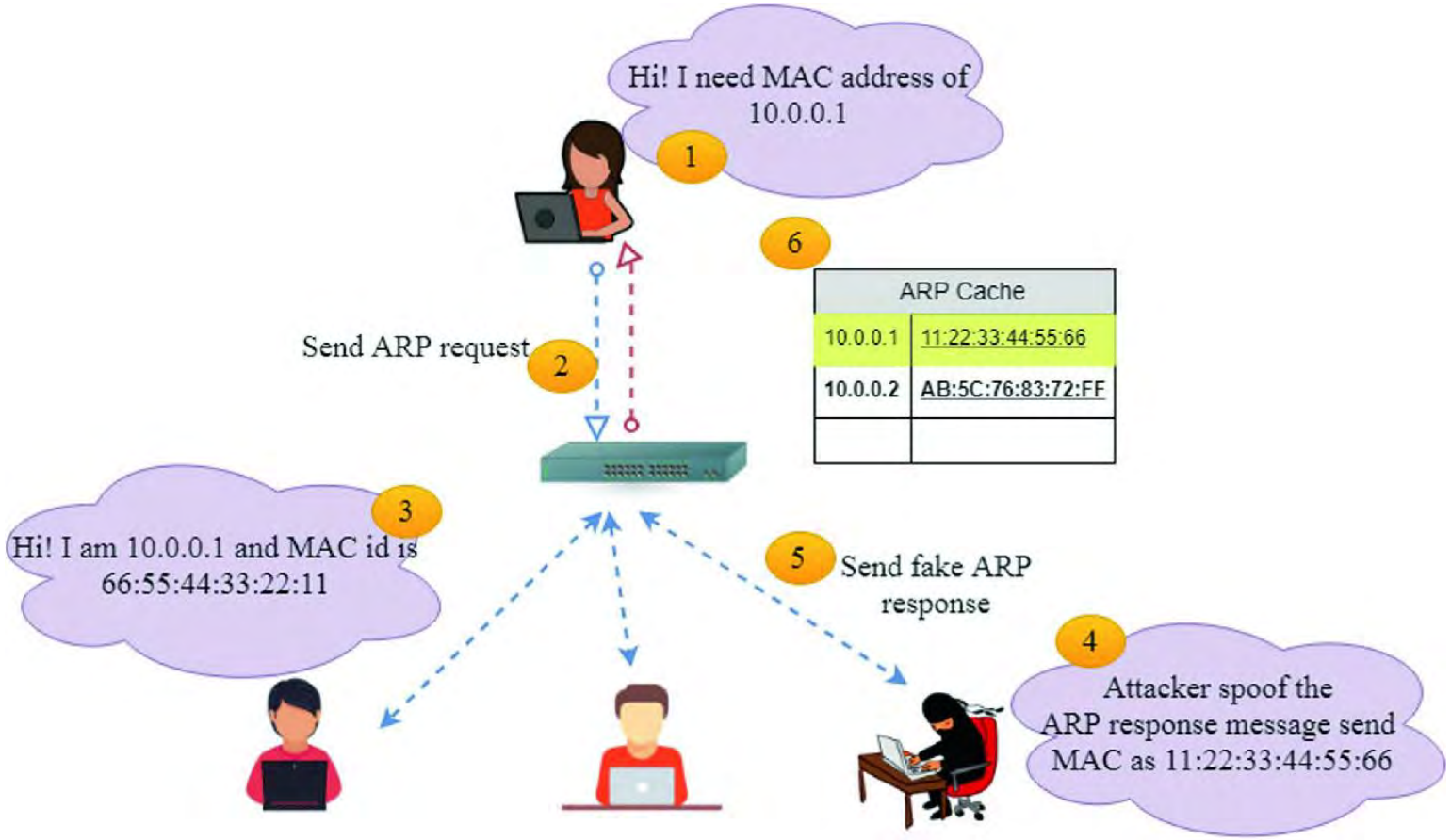


ARP Spoofing

Attacker pollutes a device ARP cache with fake ARP replies

Fake MAC address is mapped to the desired IP address in the victim's ARP cache

Victim sends traffic to the attacker's machine, rather than the legitimate destination



MAC Spoofing

AKA ARP poisoning

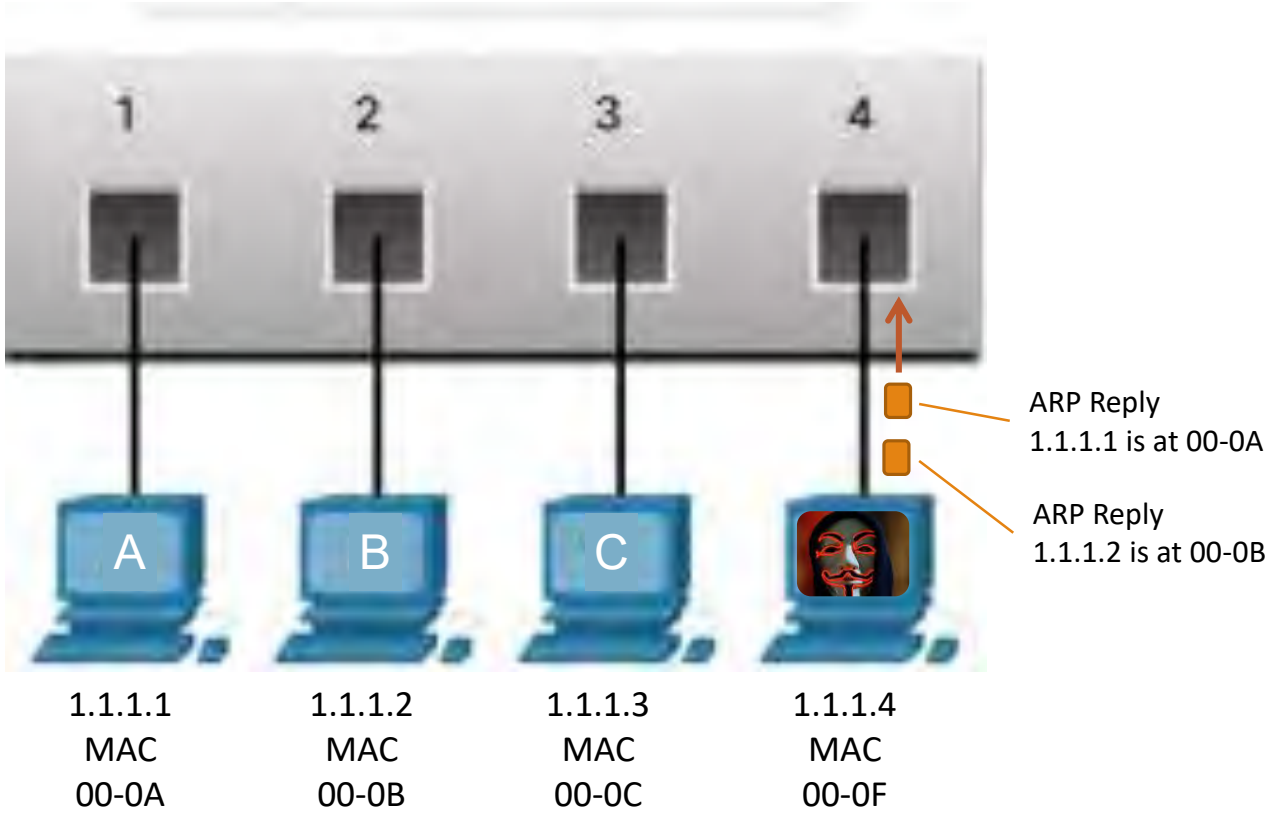
An ARP spoofing attack intended to corrupt a switch's MAC table

Fake ARP replies are sent from the attacker machine into the switch

The switch associates the attacker's port with the desired destination MAC address

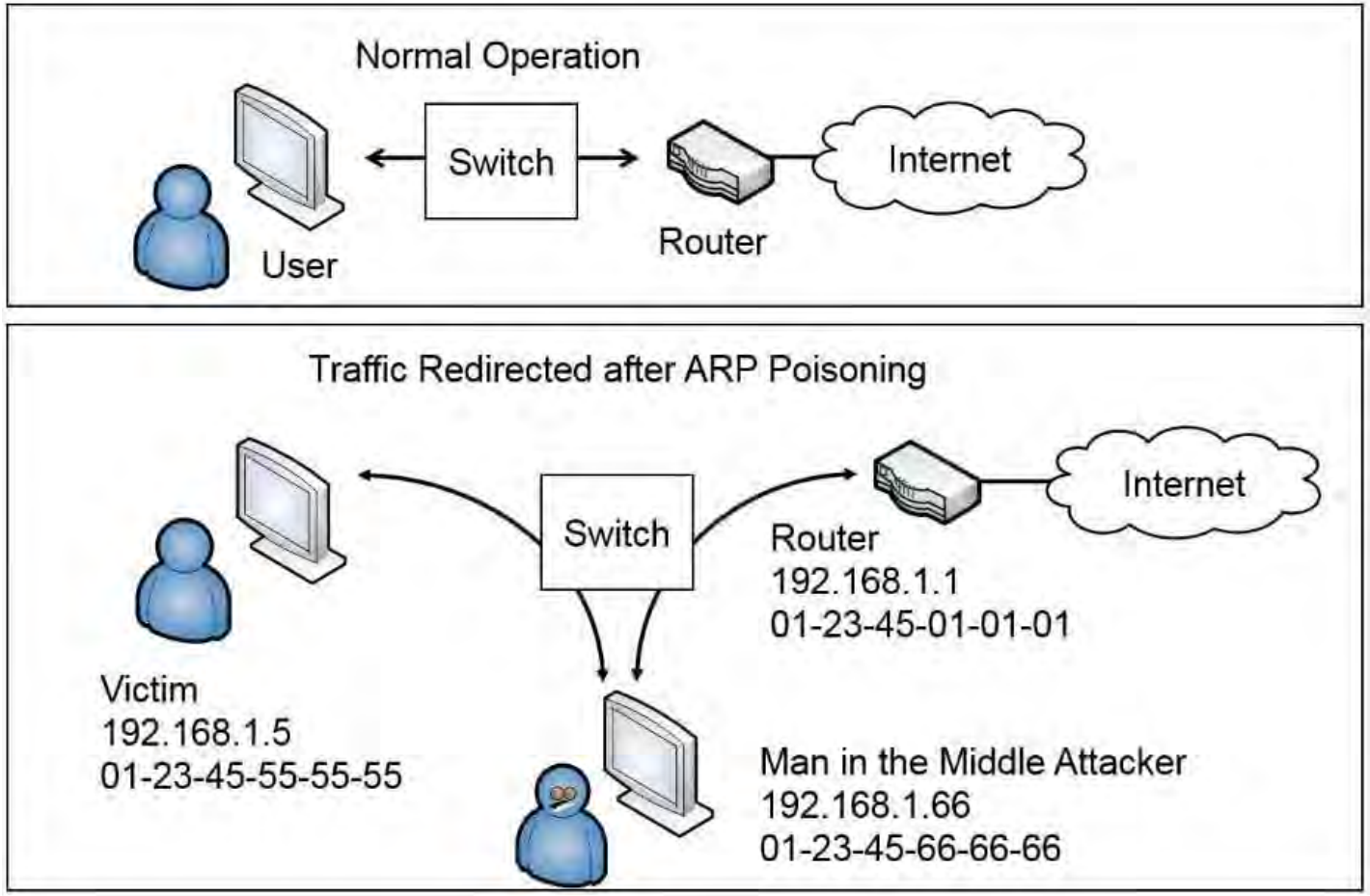
The switch then forwards traffic meant for a legitimate destination to the attacker

MAC Spoofing/ARP Poisoning Example



Port	MAC
1	00-0A
2	00-0B
3	00-0C
4	00-0F 00-0A 00-0B

ARP Poisoning Attack Example



IP Spoofing

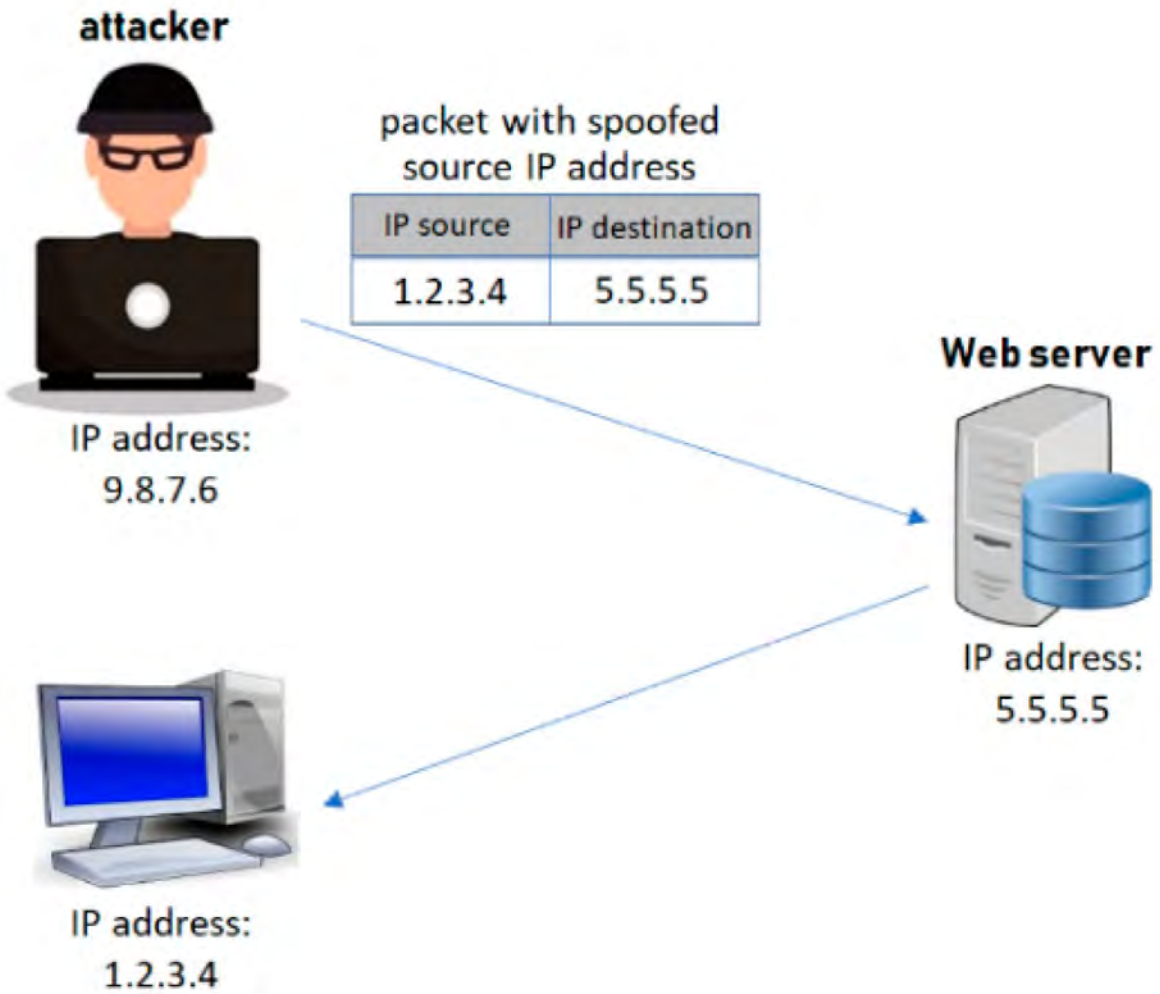
Sending a packet with someone else's IP address as the source

Routers almost never check IP source addresses for validity

The destination responds to the victim rather than the attacker

Often used:

- In DoS attacks
- To generate noise and misdirection on the network to hide a real attack

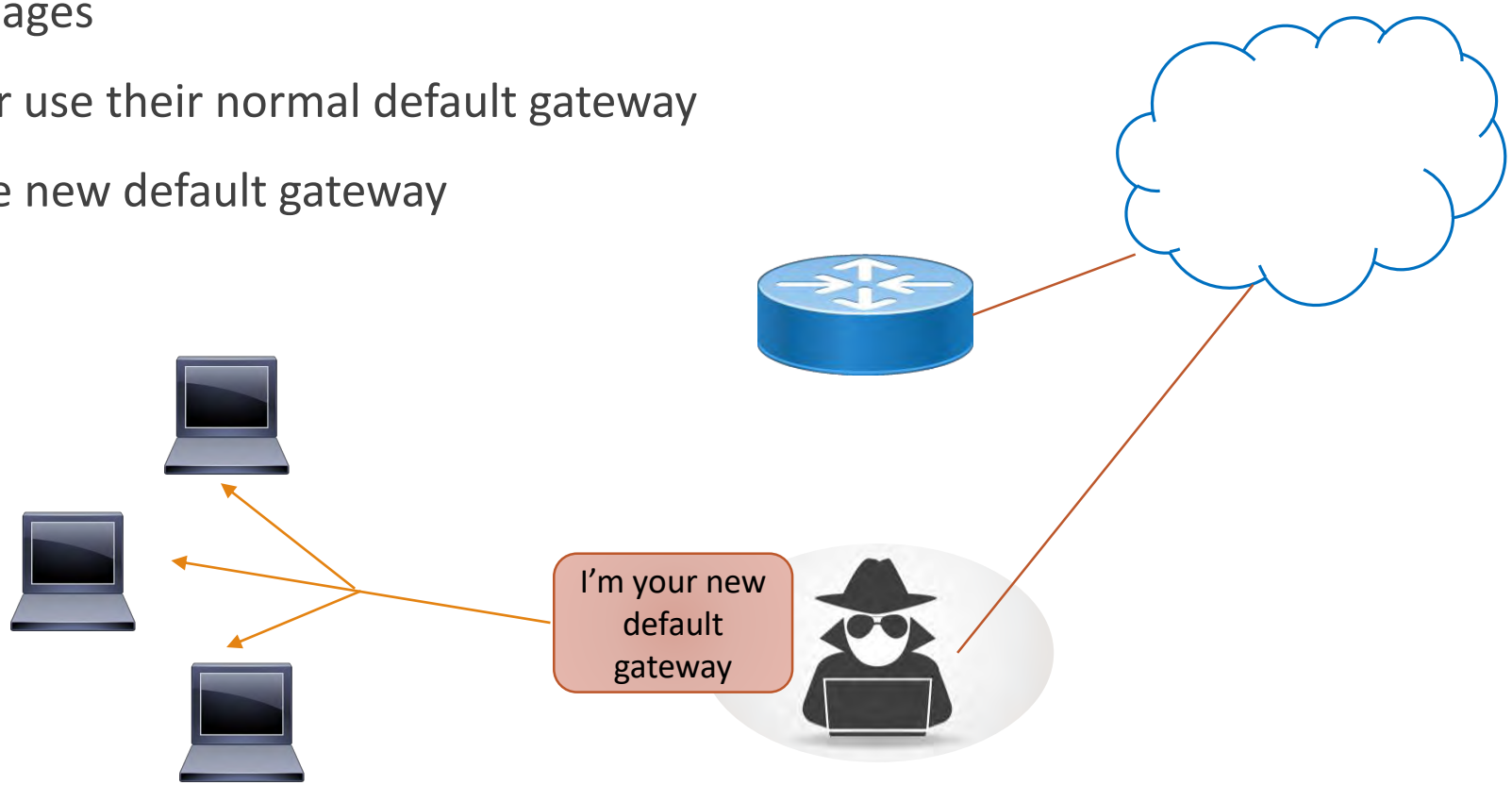


Router Redirect

Fraudulent ICMP messages

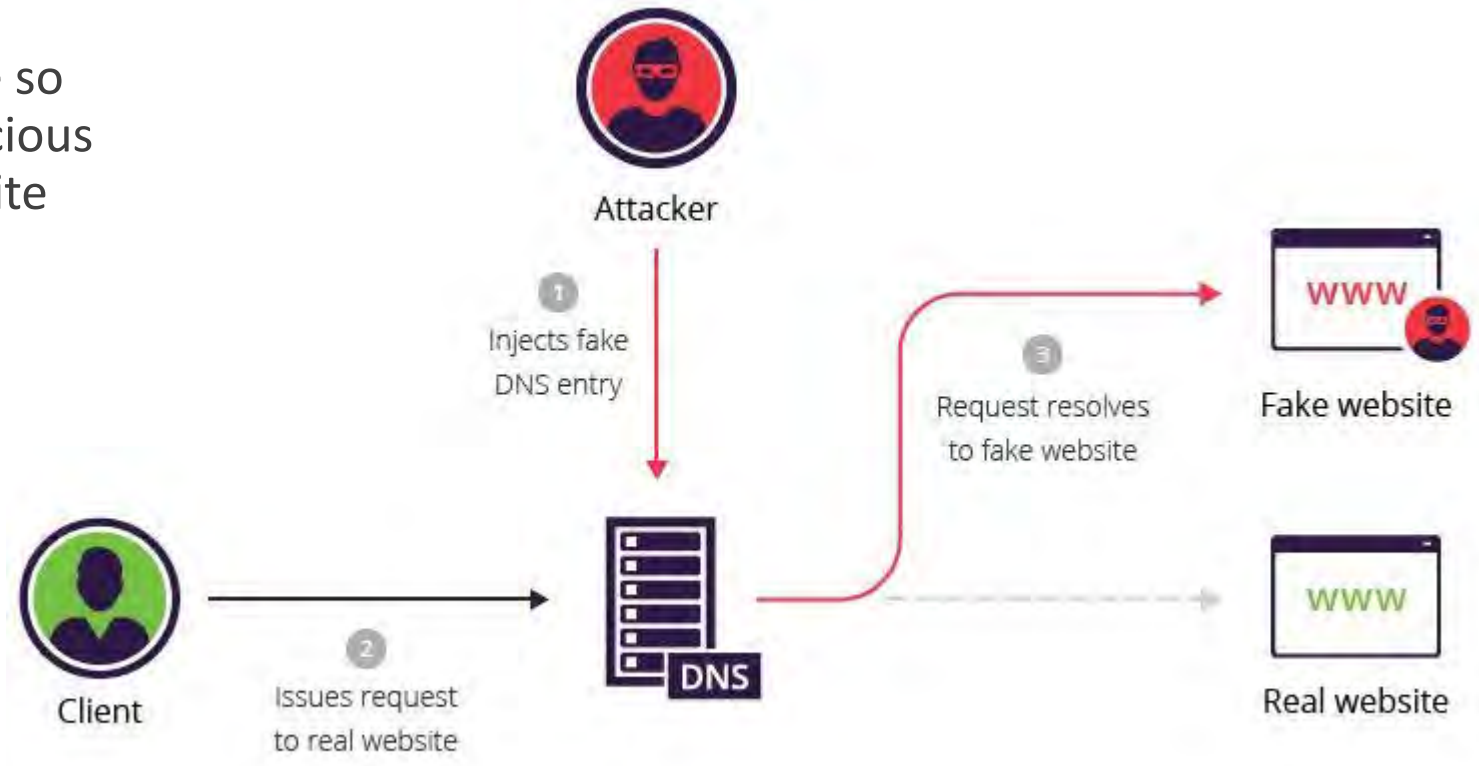
Tells hosts to no longer use their normal default gateway

Use the attacker as the new default gateway



DNS Poisoning

Polluting a DNS server's cache so that clients are sent to a malicious site rather than the real website

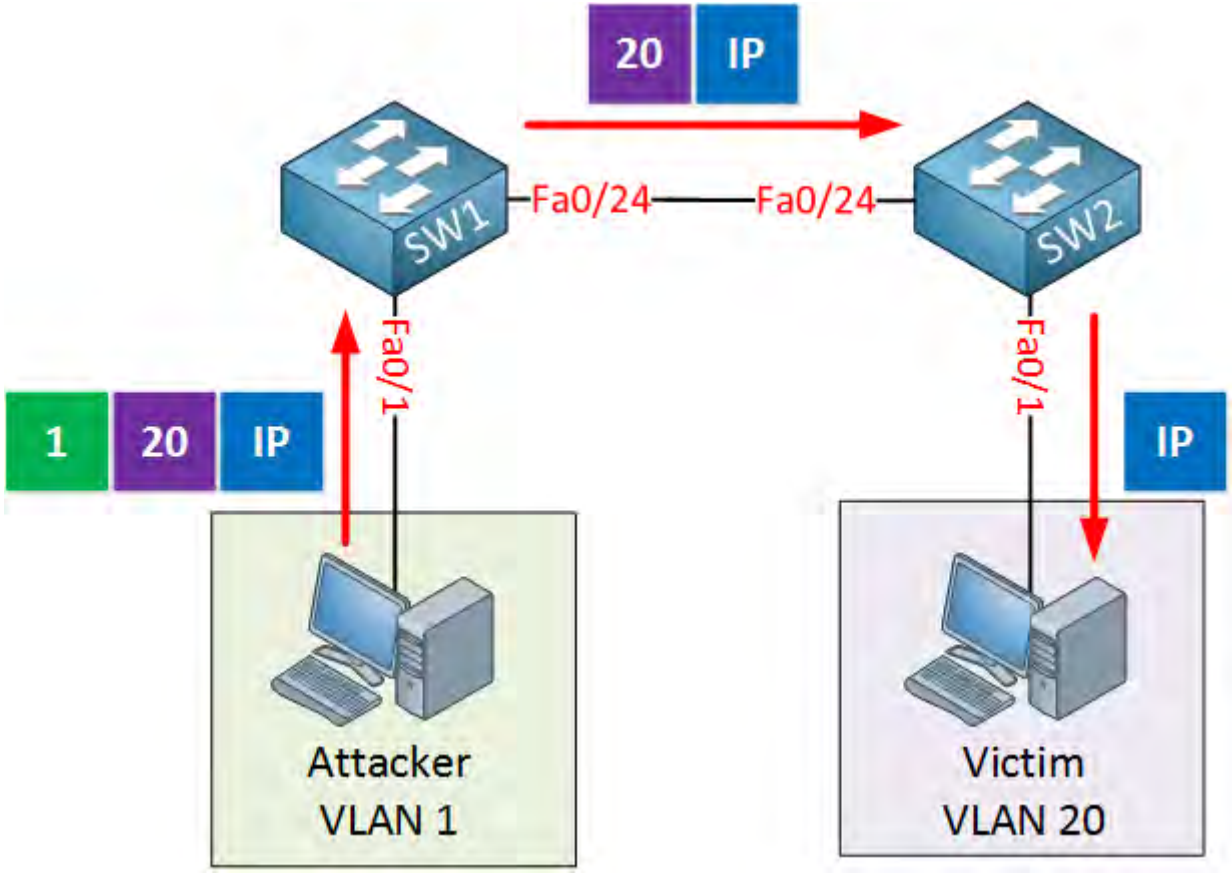


VLAN Hopping

Allows the attacker to bypass network segmentation restrictions

Attacker device pretends to be a switch

- Negotiates a trunk link with a real switch
- The victim switch then sends all VLAN traffic to the attacker



Rogue Devices

A rogue device is any unauthorized device that can interfere with normal network functionality

Device Type	Description	Countermeasure
Rogue DHCP	Any device such as a wireless router that leases improper IP addresses to clients	Configure DHCP snooping on the switch to filter DHCP traffic from untrusted sources
Rogue Access Point (AP)	A wireless access point that has been installed on a secure network without explicit authorization from the administrator. Can wreak havoc even if the intent is not malicious.	Regularly scan for the presence of unauthorized access points. Work in tandem with other admins and scanners to triangulate the physical location of the rogue.
Evil Twin	A maliciously installed rogue AP. Uses the same SSID as the legitimate WAP so users mistakenly connect to it	Same as above, paying special attention to devices with a stronger signal than the others
Fake Router	An attacker device that sends spoofed ARP or ICMP redirect messages to direct clients to it rather than the real gateway	Hard-code the router's MAC address in the switch's MAC table Disallow ICMP redirect on the network

Hijacking and MITM

On-path Attack

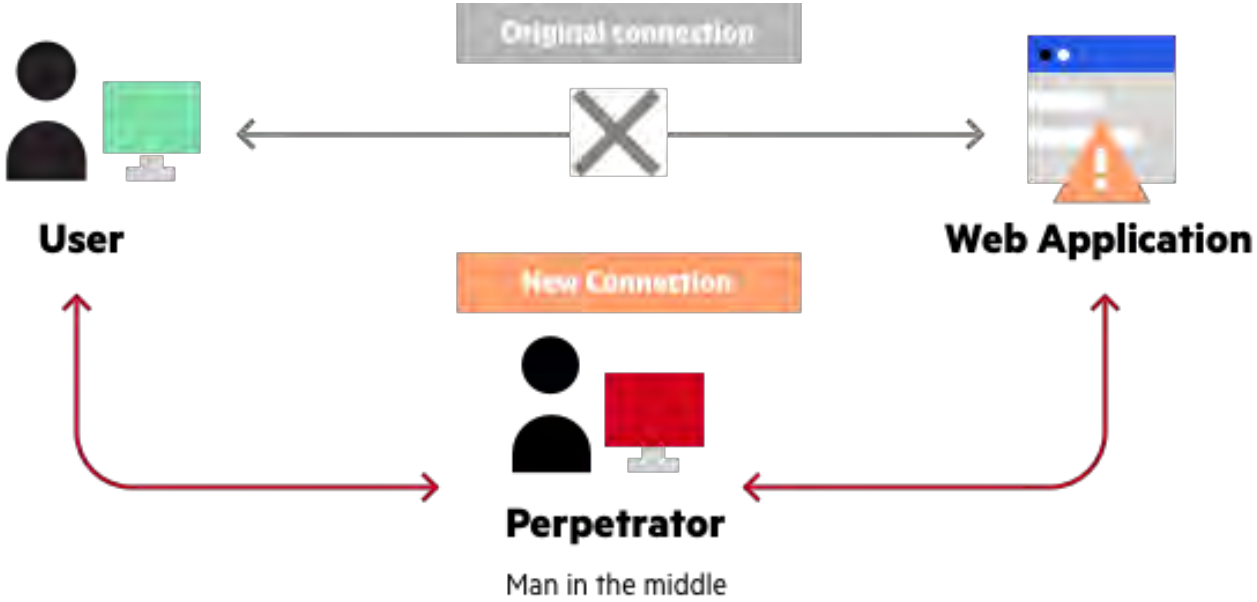
Previously know as Man-in-the-Middle (MITM) attack

The attacker uses ARP/MAC/DNS spoofing to redirect clients to the attacker machine

The attacker machine acts as a relay while sniffing traffic that passes through it

If the website requires HTTPS, the attacker creates two separate sessions:

- One with the client (typically unencrypted)
- One with the website



Session Hijacking

1. An attacker steals an authenticated user's HTTP (session) cookie
   - The cookie is meant to keep the user authenticated for a period of time after initial login
2. The attacker then masquerades as the authenticated user

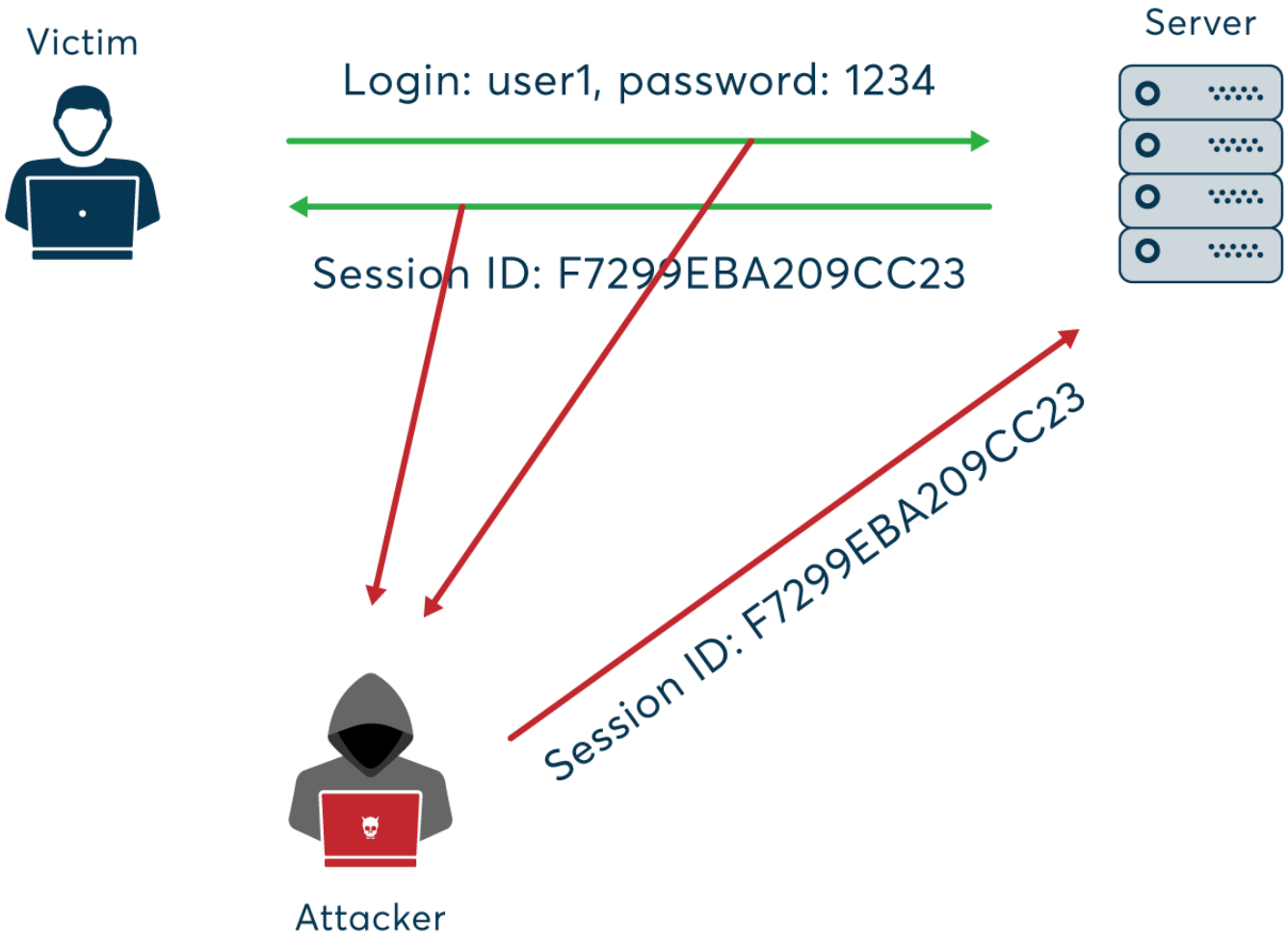
Often performed by:

- Sniffing traffic and extracting the clear text cookie
- Using social engineering to get a user to click a malicious link to either:
  - Steal the user's session ID
  - Replace the user's session ID with one the attacker has pre-obtained (and therefore knows)

<u>Old school session hijacking:</u>

1. The attacker uses sniffing to watch and predict incrementing TCP sequence numbers between the client (victim) and the server
2. The attacker deauthenticates the client, taking over the client's session with the predicted next TCP sequence number

Session Hijacking Example



Deauthentication Example

Performed after the victim has authenticated

Can be used to capture, hijack or replay a connection

1. The attacker sends spoofed TCP RST packets to the victim
2. The victim thinks the server/WAP wants to reset the connection
3. The victim drops the connection
4. As the victim reconnects to the server:
   - The attacker captures an ARP packet for replay against a WAP
   - The attacker has compromised the victim with malicious commands

Countermeasures:

- Use WPA3 in Wi-Fi connections
- Use packet sequence numbers and/or time stamps
- Digitally sign packets

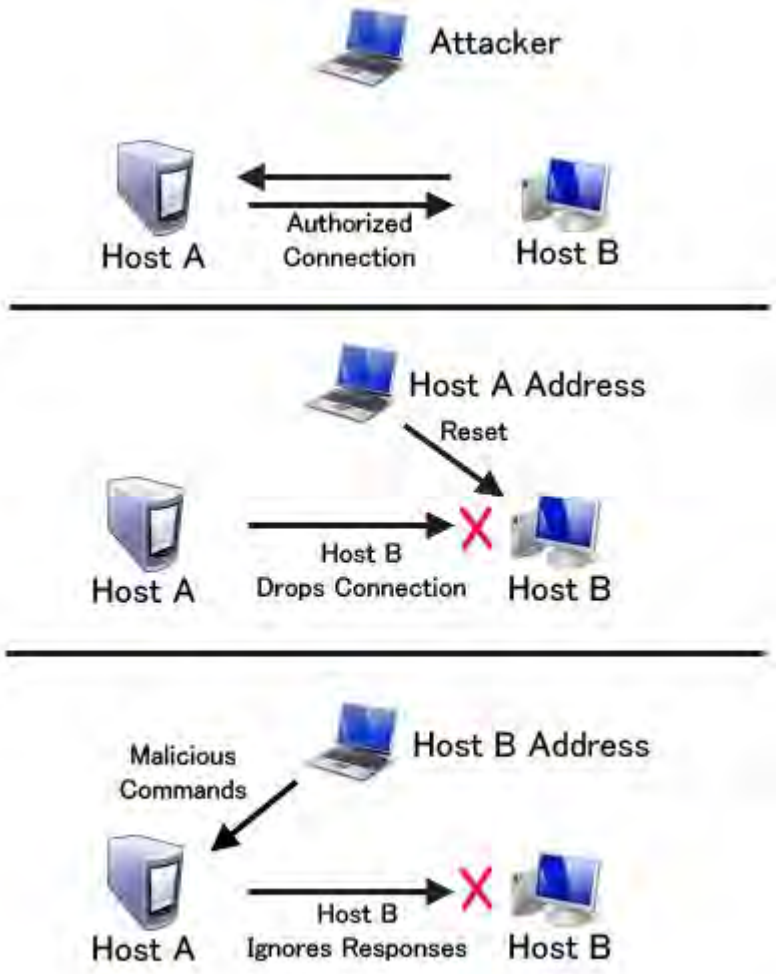


Figure 2: Session Hijacking

On-path Attack Countermeasures

Hard-code router MAC addresses in switches

Require telecommuters to use VPNs

Regularly clear the company's local DNS server cache against pollution

Require HTTP TLS encryption on the webserver

Implement HTTP Strict-Transport-Security (HSTS) on the webserver

- Lets a web site tell browsers that at no time is it allowed to use HTTP for the connection

Use a long random number or string as the session key

- So it can't be predicted or guessed

Require that the session key be regenerated after a successful login

Social Engineering

What is Social Engineering?

The psychological manipulation of people into divulging confidential information or performing actions that they shouldn’t do

Common Social Engineering Attacks

Attack Type	Description
Impersonation	Calling the victim inside the company and pretending to be someone the user trusts; an authority figure or IT support
Phishing	Sending a fake email to a user to entice them into opening a malicious attachment or clicking a malicious link Variants include: vishing, smishing, spear phishing, whaling
Tailgating	An unauthorized person follows an authorized person into the secure or restricted area WITHOUT the consent of the authorized person
Piggybacking	An unauthorized person follows an authorized person into the secure or restricted area WITH the consent of the authorized person
Shoulder Surfing	An unauthorized person spies over your shoulder as you type; can be done directly or across the room with a mobile device and special camera software
Ransomware	A form of malicious software that encrypts data and then demands a paid ransom for the decryption key
Dumpster Diving	Going through someone's trash to find discarded, but still valuable/sensitive information

Ransomware Example

Dumpster Diving

Social Engineering Countermeasures

Train employees to:

- Follow authentication and authorization strict protocols
- NEVER give out passwords/sensitive information via phone

Periodically test training effectiveness

Ensure all guests are escorted while onsite

Ensure the mailroom, server room, phone close and other sensitive areas are locked and monitored at all times

Keep an updated inventory of all communication equipment

Use multi-factor authentication

Use multiple layers of anti-virus/anti-phishing defenses at all gateways

Ensure all documents containing private information are shredded/secured

Network Segmentation

Network Segmentation

VLANs/Subnets with Router ACLs

- More efficient network performance
- Contain threats from spreading
- May require re-architecting the network
- May add complexity through programming and maintaining additional ACLs

Firewalls

- Separate trusted from untrusted zones
- Many rules introduce complexity when used internally
- Risk of misconfiguration
- Added cost

Router Access Control Lists (ACLs)

Important

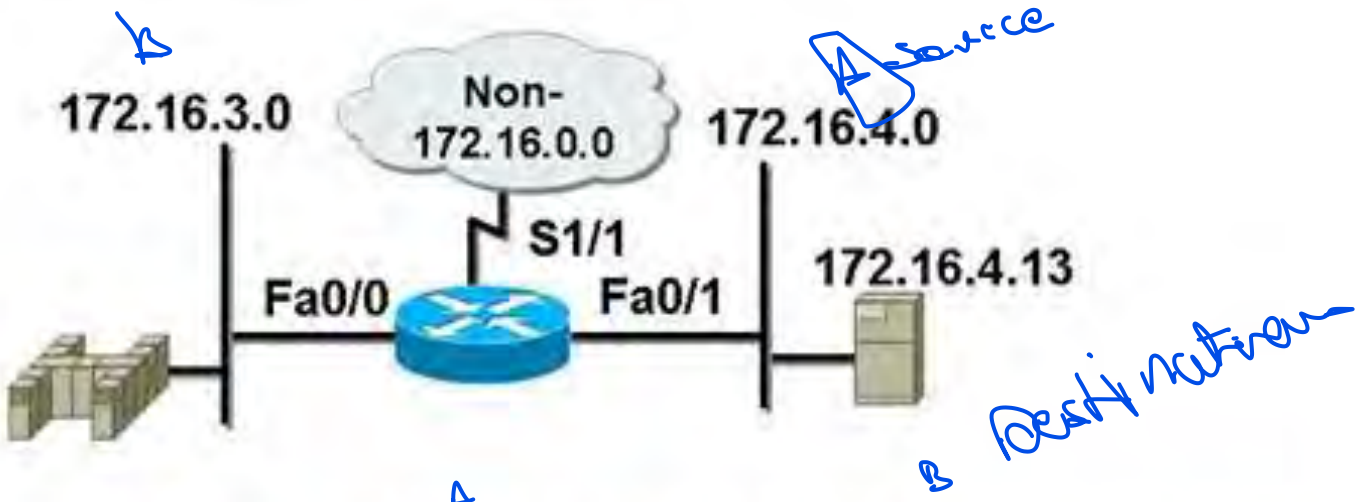
Using ACLs involves the following:

1. Creating the actual rule
2. Applying the rule to an interface
3. Choosing if the rule is for inbound or outbound traffic on the interface

The best way to use ACLs is to draw a diagram to visualize data flows:

- Draw a simple topology map of involved devices (computers, routers, VLANs/subnets)
- Use arrows to show permitted traffic flows
- Determine permitted/denied protocol, source and destination IPs and ports
- Figure out the most strategic interface and direction on which to apply the rules
- Use your diagram as a reference as you implement the ACL
- Consider asking a friend/colleague to check you work, based on the desired outcome shown in your diagram

Router ACL Example



A B

access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21 port

access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20 port

access-list 101 permit ip any any

when creating a ACL dont let people iontoi the4 router

Key Points to Remember When Using ACLs

An ACL can have multiple rules

The rules are arranged from top to bottom

A packet is checked against the rules one by one until there is a match

- After that, no more rules are checked for that packet

Ensure that rules on top do not negate rules on the bottom

- Example: If your first rule is “permit ip any any” then all IP traffic will pass through, even if successive rules seek to block certain types of traffic

Put your most specific rules first (at the top of the ACL rules list)

Keep in mind that most ACLs have an implicit “deny all” at the end of the list

- If you deny certain kinds of traffic, be sure to have a “permit any any” rule at the very end to allow everything else

Firewall Rules

Firewalls use ACLs in much the same way as routers

Some host-based firewalls allow you to specify an application rather than specific ports

- It tracks ports that the application dynamically uses

Some firewall appliances allow you to create “objects” representing hosts, IP addresses, services and the like

- These objects can be reused in different rules

Most firewalls can track entire sessions and block traffic accordingly. They watch for:

- Missing TCP handshakes
- Suddenly changing ports
- Suspicious packets or payloads

Some firewalls allow you to download the latest malicious signatures from the vendor

- Or they send a sample to the vendor for analysis

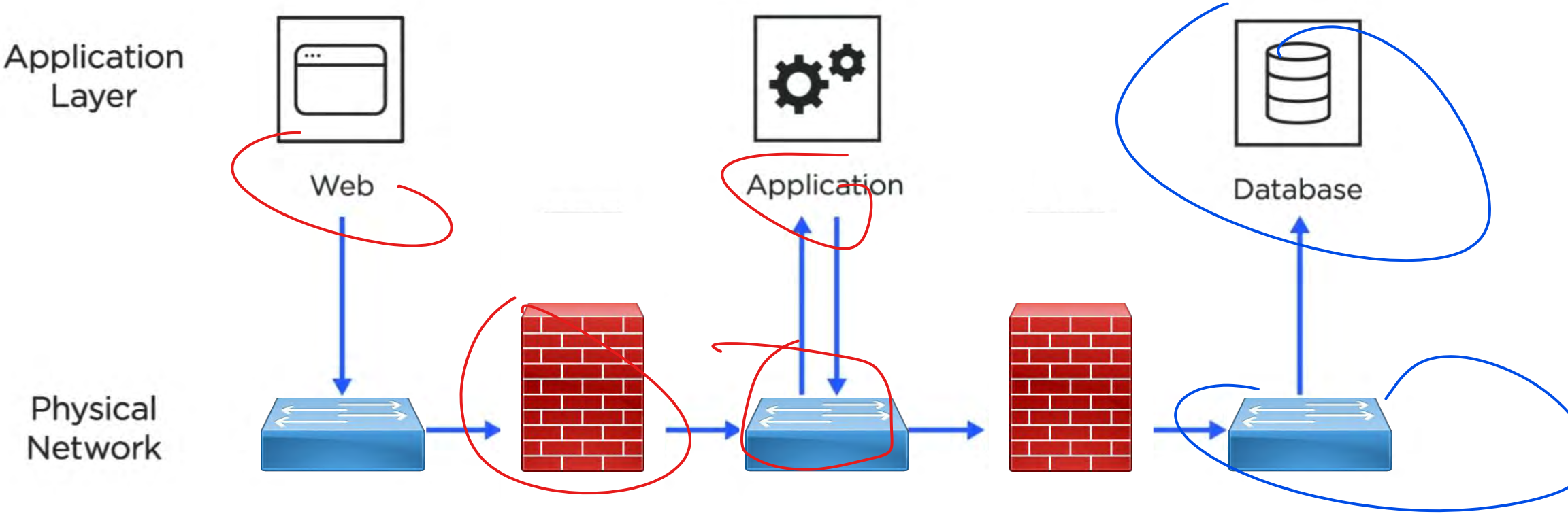
Firewall Rules Example

No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	20.1.1.1	80	Accept
2	TCP	10.1.1.2	20.1.1.1	80	Deny
3	TCP	10.1.1.0/24	20.1.1.1	80	Deny
4	TCP	10.1.1.3	20.1.1.1	80	Accept
5	TCP	10.2.2.0/24	20.2.2.5	80	Deny
6	TCP	10.2.2.5	20.2.2.0/24	80	Deny
7	TCP	10.3.3.0/24	20.3.3.9	80	Accept
8	TCP	10.3.3.9	20.3.3.0/24	80	Deny
9	IP	0.0.0.0/0	0.0.0.0/0	0-65535	Deny

the wasys tyhis works that everry packets comes and thgere iis a amatch the ip or the poty ot the denstnation get denied

this means any source or desntnation is denied we could salso ied the wiord NAY

VLAN / Firewall Segmentation Example



Screened Subnet

AKA DMZ

A separate, untrusted network segment between the Internet and the private network

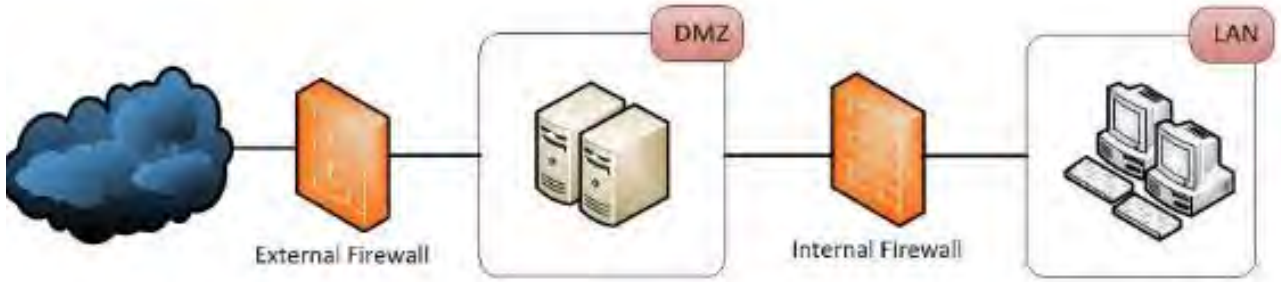
Usually protected by two firewalls (inside and outside)

- The outside firewall can also be a packet filtering router (creating a “dirty DMZ”)

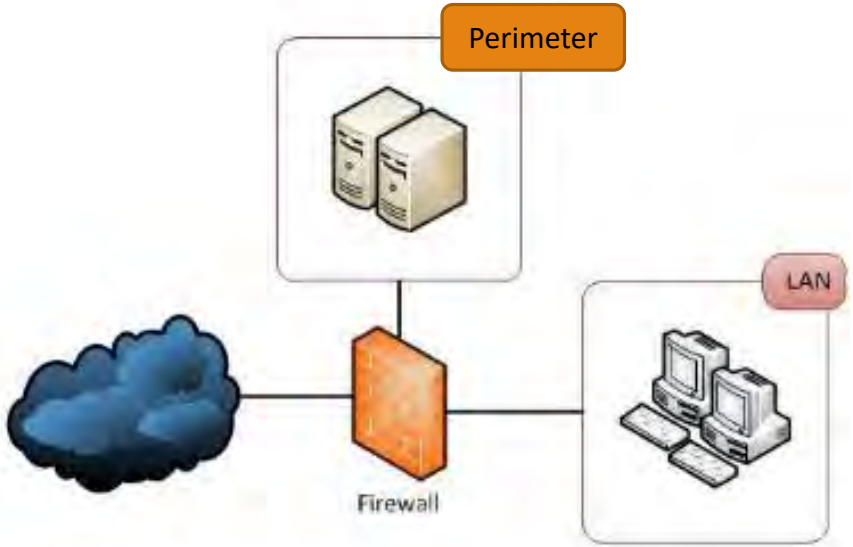
You put bastion hosts (public facing servers) in the screened subnet

The DMZ can use public or private IP addresses

DMZ vs Perimeter Network Example



VS.



SDN Segmentation

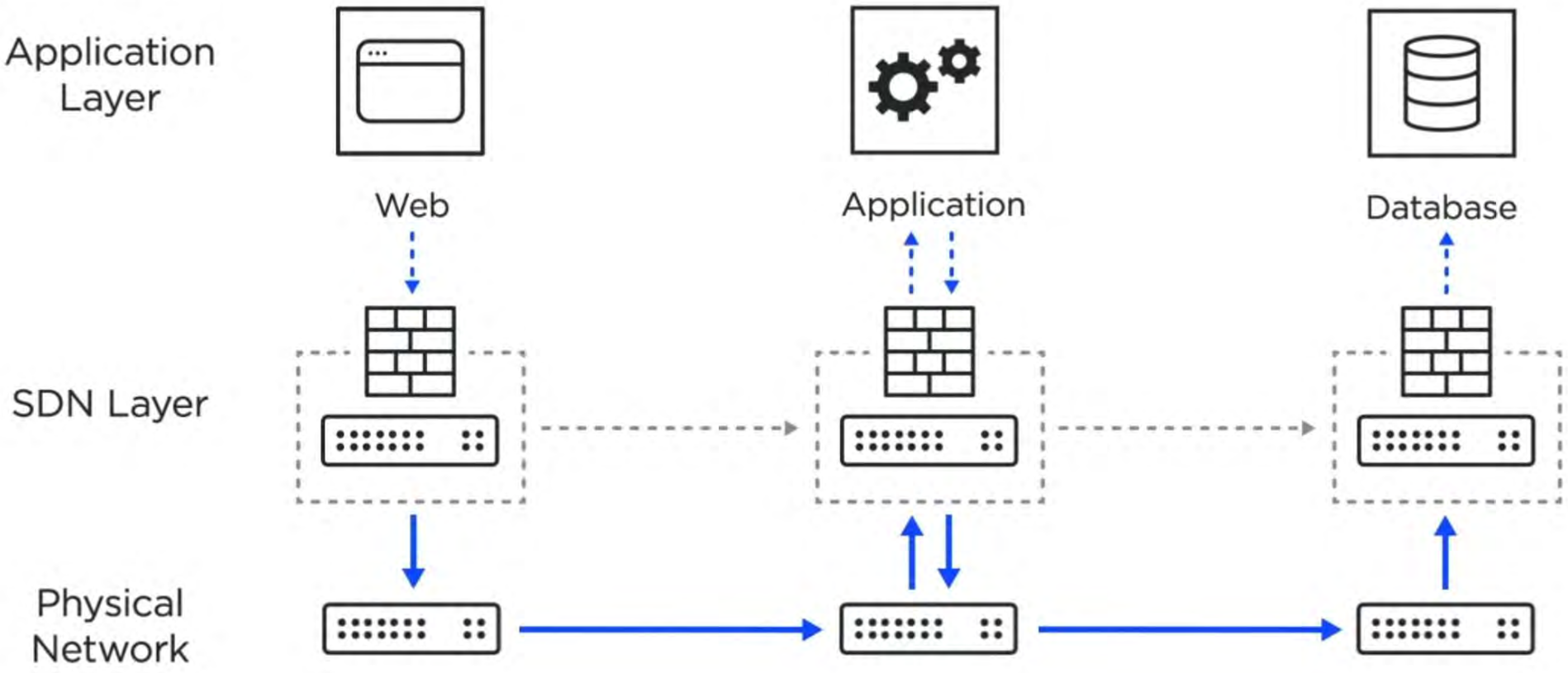
Centralized controllers that are abstracted from physical hardware provide greater network automation and programmability

Network operators use it to create policies to funnel packets through a distributed set of firewalls

Can be complex to implement

- Especially if an application does not fit into network boundaries
- SDNs focus on network policy more than security visibility in workloads and application flows

SDN Segmentation Example



Micro-segmentation (Host-Based Firewalls)

Host-based segmentation (micro-segmentation per host/workload)

Each OS has native firewall capabilities

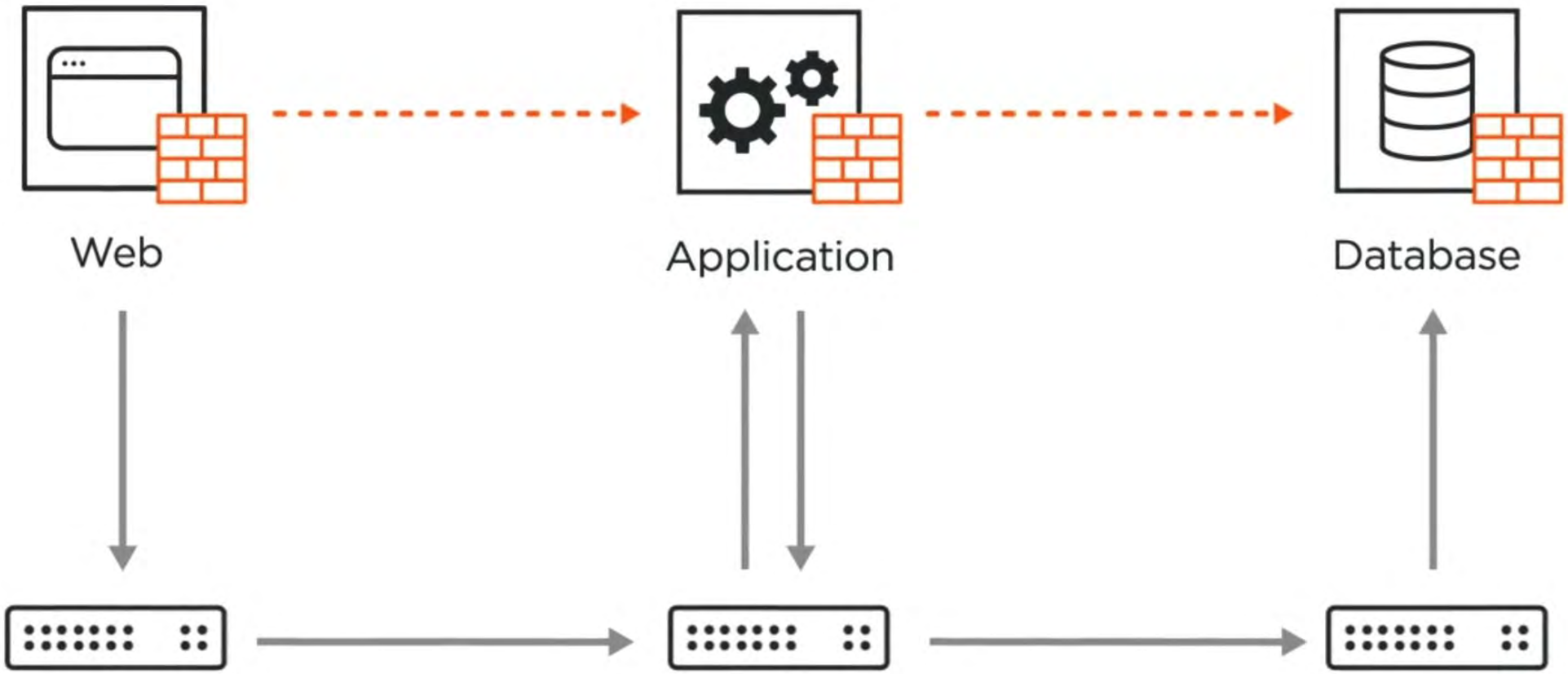
- Linux iptables
- Windows Defender Firewall with Advanced Security

Uses whitelists to block all traffic except that which is explicitly permitted

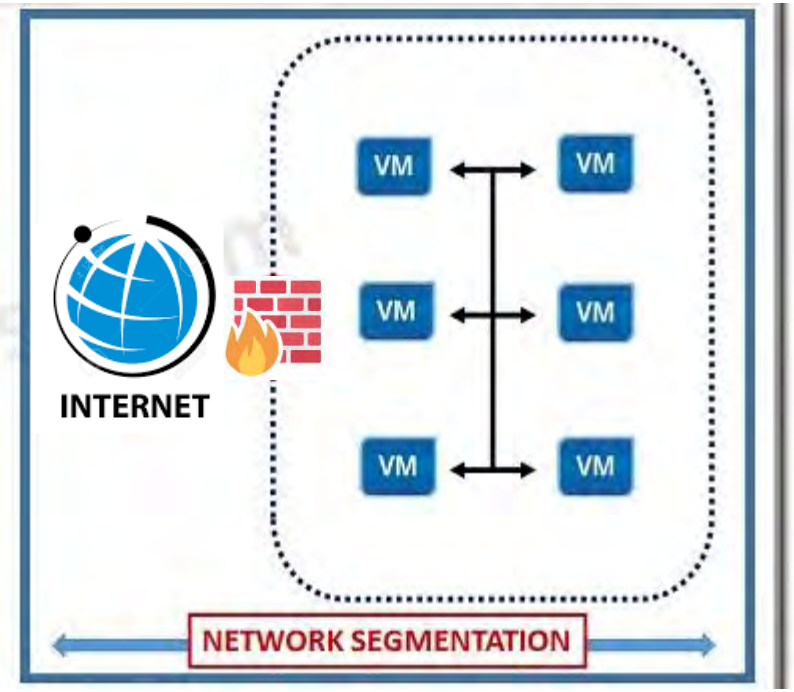
Use workload telemetry to create a map of cloud and on-premises compute environments and applications

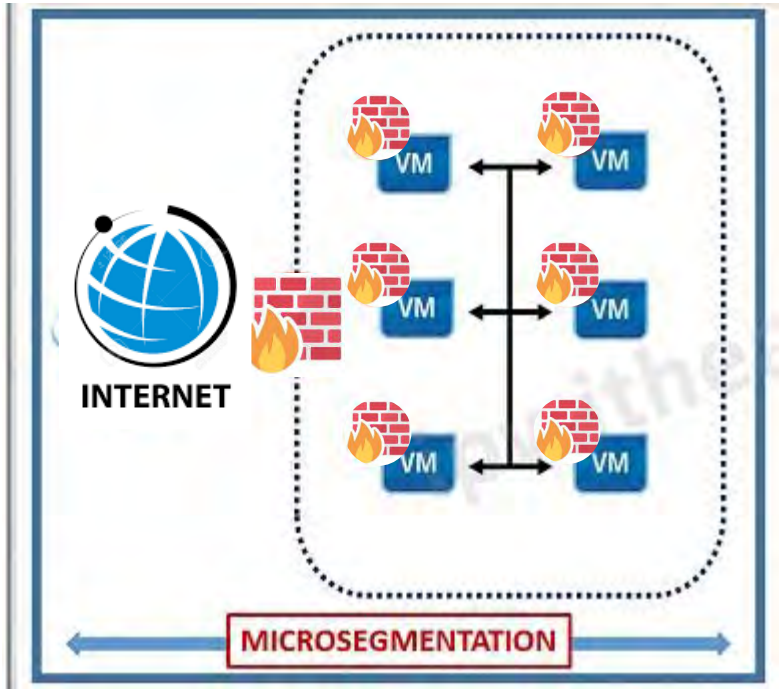
- Use the map to visualize what must be protected
- Possible to enforce segmentation down to the process level, rather than specific ports

Micro-segmentation Example



Network Segmentation vs Microsegmentation Example





Honeypot

Deliberately vulnerable computer / network segment

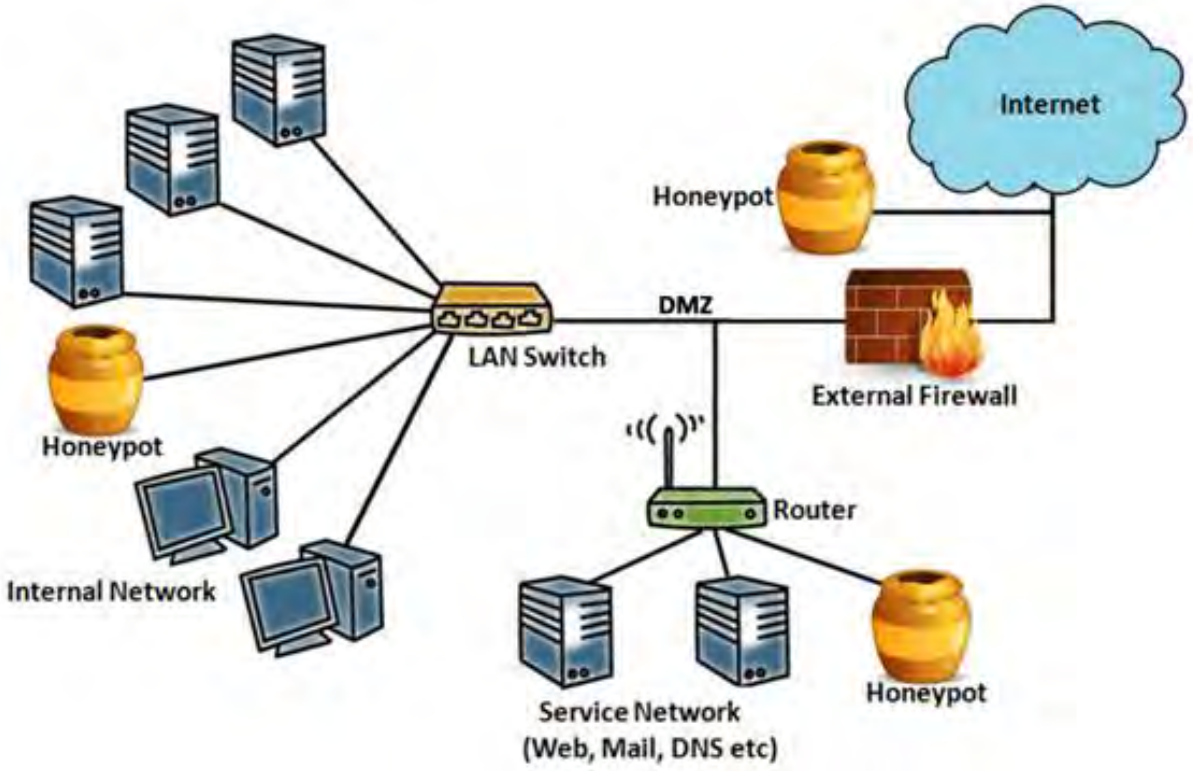
Meant to keep an attacker busy and away from the actual network

Logs activity and can send alerts to the administrator

Gains valuable information about attacker activity

Can be a real device or software simulation

- Real devices run the risk of actually being compromised and then used as a jump point to attack the actual network



Private VLANs

What is a Private VLAN?

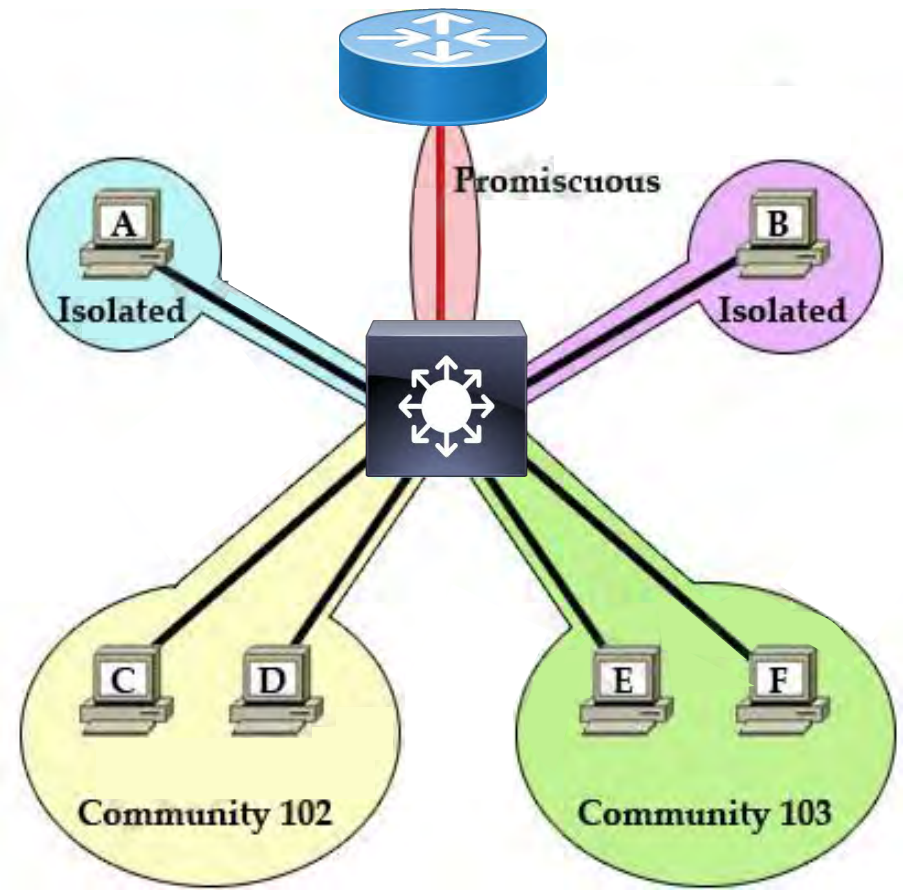
Also known as port isolation

Allows you to have a “VLAN inside a VLAN”

Divides the “Primary” VLAN into “Secondary” sub-VLANs

The secondary VLAN can be one of the following types:

- Community
  - Switchports can communicate with the primary VLAN, but not any other secondary VLANs
  - Hosts in the same community VLAN can communicate with each other
- Isolated
  - Like a community VLAN
  - However, hosts within the same isolated VLAN CANNOT communicate with each other



Private VLAN Ports

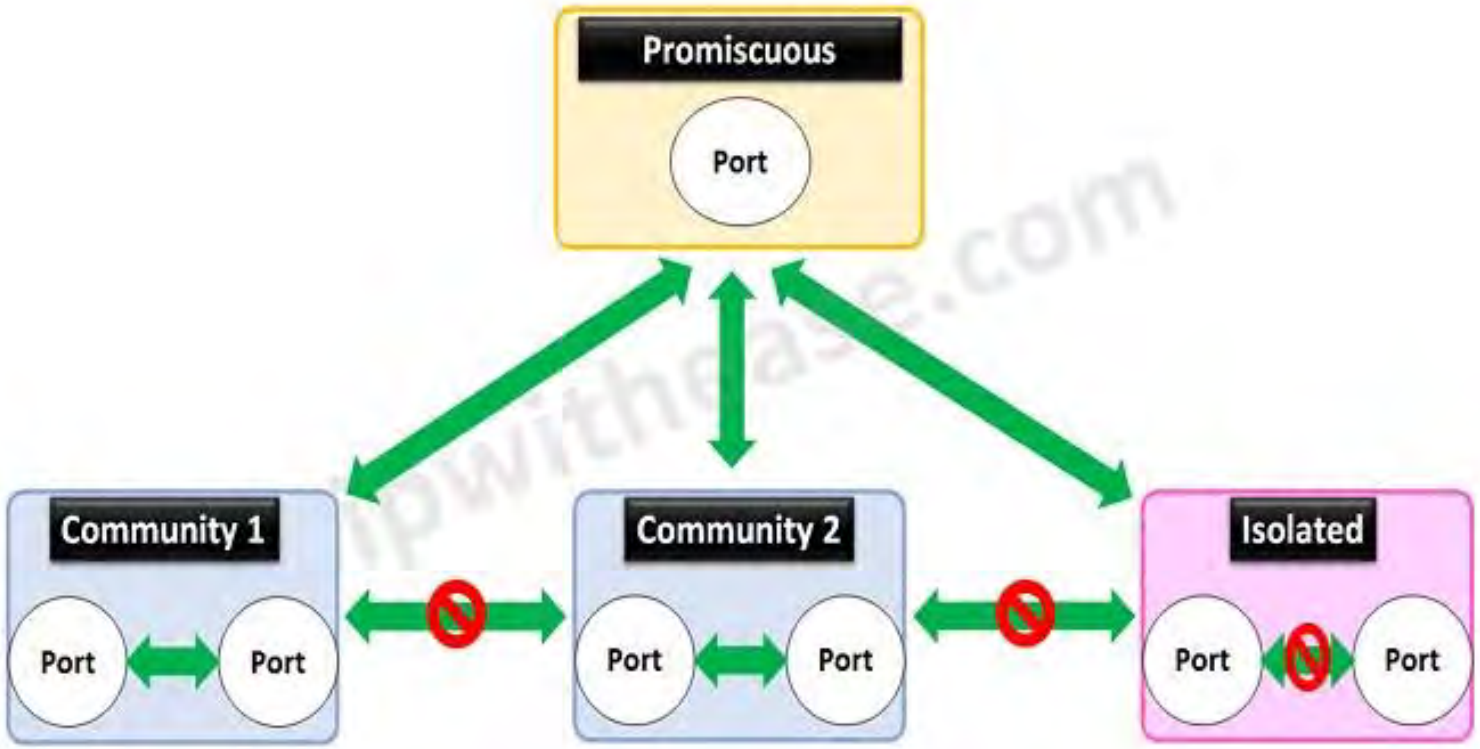
Promiscuous (P-Port)

- The switch port that connects all VLANs to the router/firewall/outside world
- Can communicate with anything connected to any primary or secondary VLAN

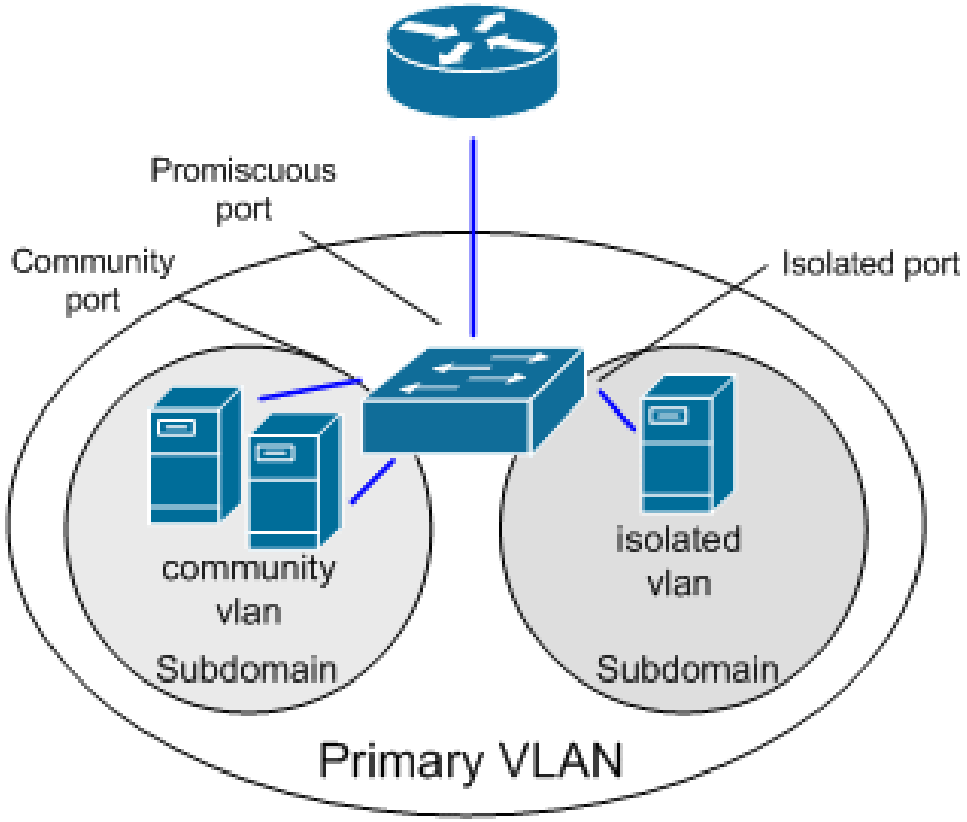
Host (further breaks down into two types):

- Isolated Port (I-Port)
  - Connects the one host to its isolated VLAN
  - Only communicates with the P-Port so host traffic can go to the outside world
- Community Port (C-Port)
  - Connects the host to the community VLAN
  - Can communicate with other C-Ports and the P-Port

Private VLAN Conceptual Example



Private VLAN Implementation Example



Private VLAN Common Applications

Hotels

- Each floor can be its own VLAN
- Each room on a floor can connect to the Internet, but is separate from the other rooms

Cloud providers

- Customers are restricted to their own VLANs – cannot communicate with other customers
- Each customer can have PVLANs to segment their own network
- Customers can reuse the same IP addressing schemes

Single Organization Authentication

Local Authentication

Authentication credentials are stored on the device

Instead of using an external login service such as Active Directory, “Login with Google”, etc., you authenticate using an account that exists on that device only

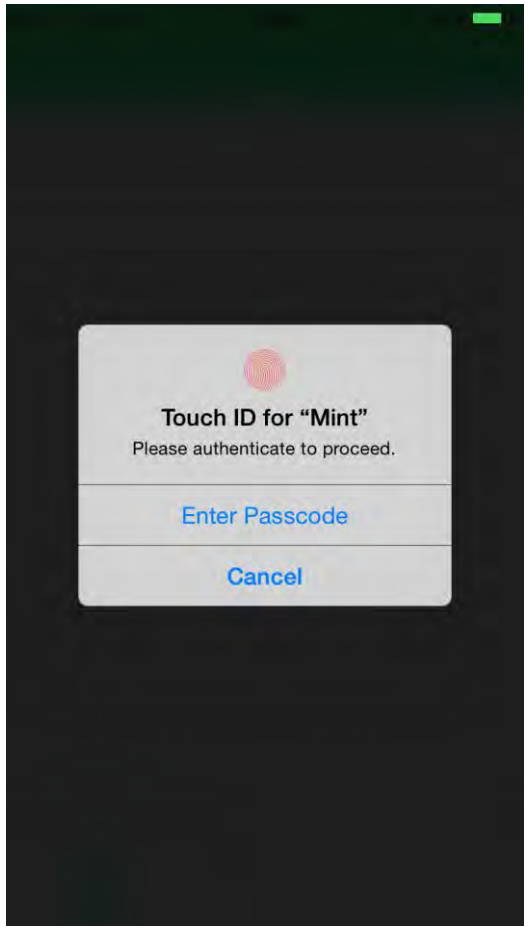
Local accounts do not exist on other devices

- If you log in locally, you can only access permitted resources on that device
- They are good for accessing a computer that is not joined to a domain

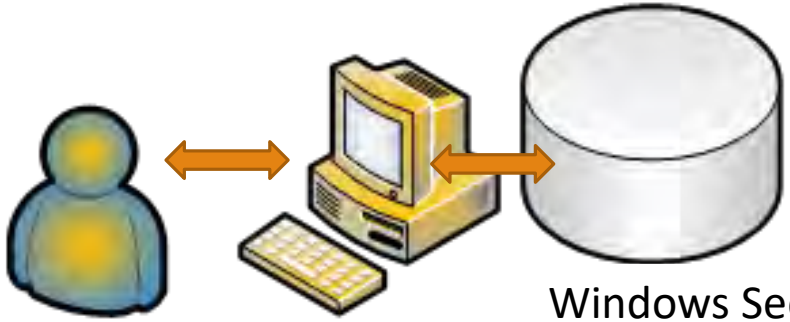
If you make a remote connection to another device, you will have to supply credentials stored on the other device, not yours

- Can get confusing if both devices have accounts with the same username
- Those users are NOT the same, even if the names and passwords are the same

Local Authentication Examples



The username, password, fingerprint, etc. is stored in the device's local security database



Windows Security Account Manager (SAM) local database

Directory Service Authentication

A directory service (DS) is a network-based authentication system

Users, computers, services and resources are logically grouped under a single security umbrella (domain)

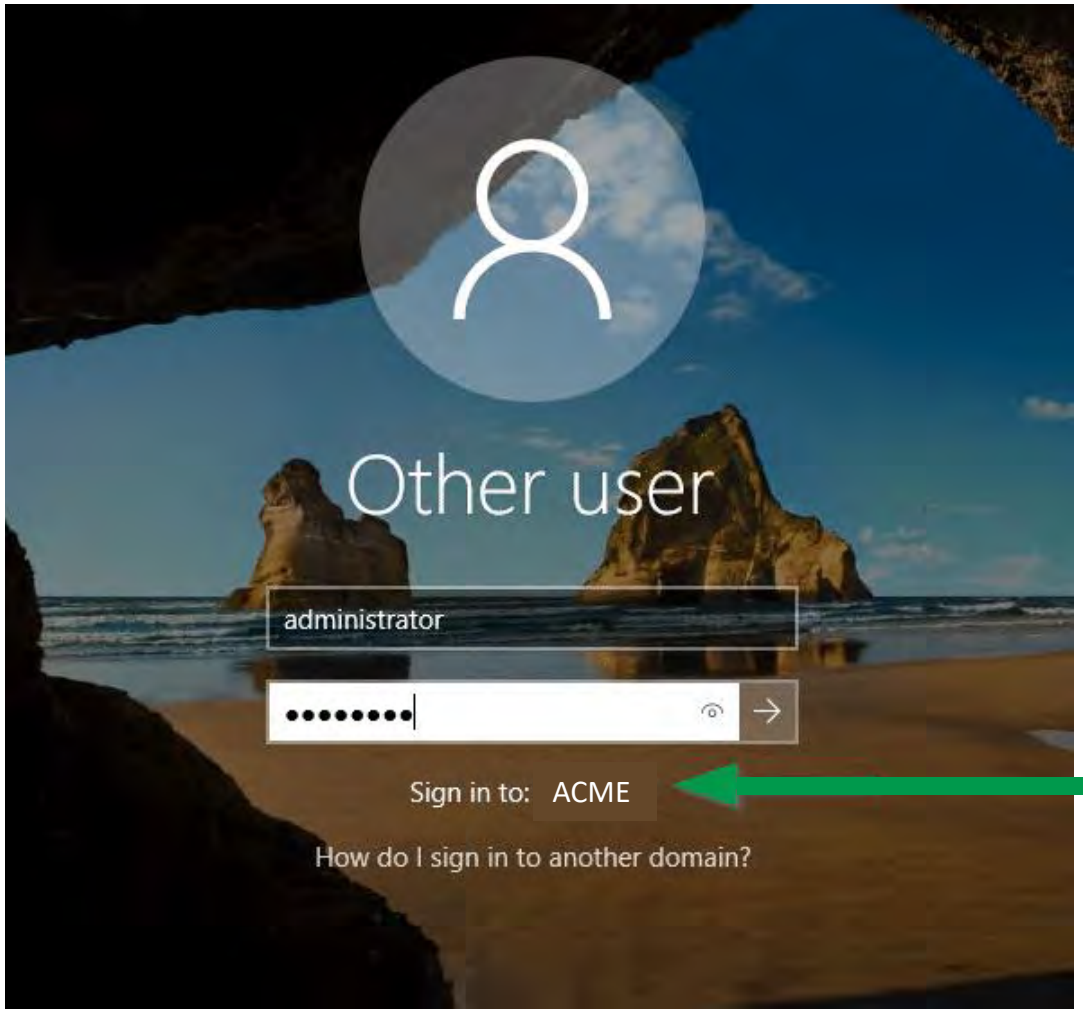
A user only has to log on once to access multiple resources on the network

Resources that belong to the same domain will not require the user to authenticate again
- The user still must have authorization to use the resource

Most directory service products follow the ITU standard X.500 naming convention
- Objects are organized in a hierarchical structure with a DNS-style “domain name” at the top of the hierarchy

Microsoft has a popular directory service named “Active Directory”
- The servers that host Active Directory are called “domain controllers”
- It uses Kerberos v5 as the authentication protocol
- It also uses LDAP to locate objects in the DS database

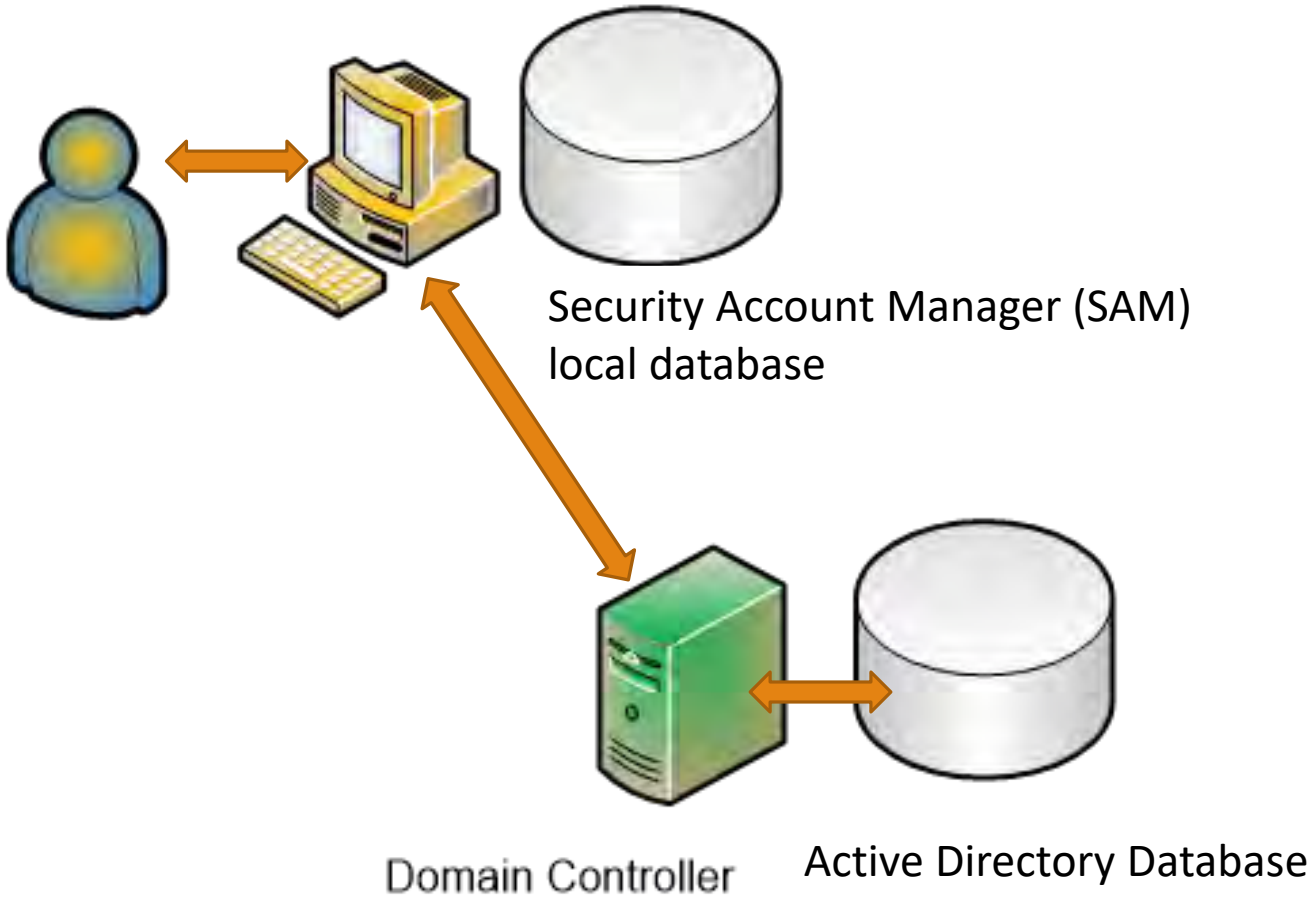
Active Directory Login Screen Example



Domain name

Active Directory Authentication Example

1. The user sits at a computer that is a member of the domain
2. The computer gives the user the option to choose:
   - Log on to the domain
   - Log on locally
3. The user chooses to log onto the domain
4. The client computer forwards the logon request to the domain controller
5. The domain controller verifies the user's credentials
6. The client computer presents the user with a desktop
7. The user is allowed to connect to domain resources from the client

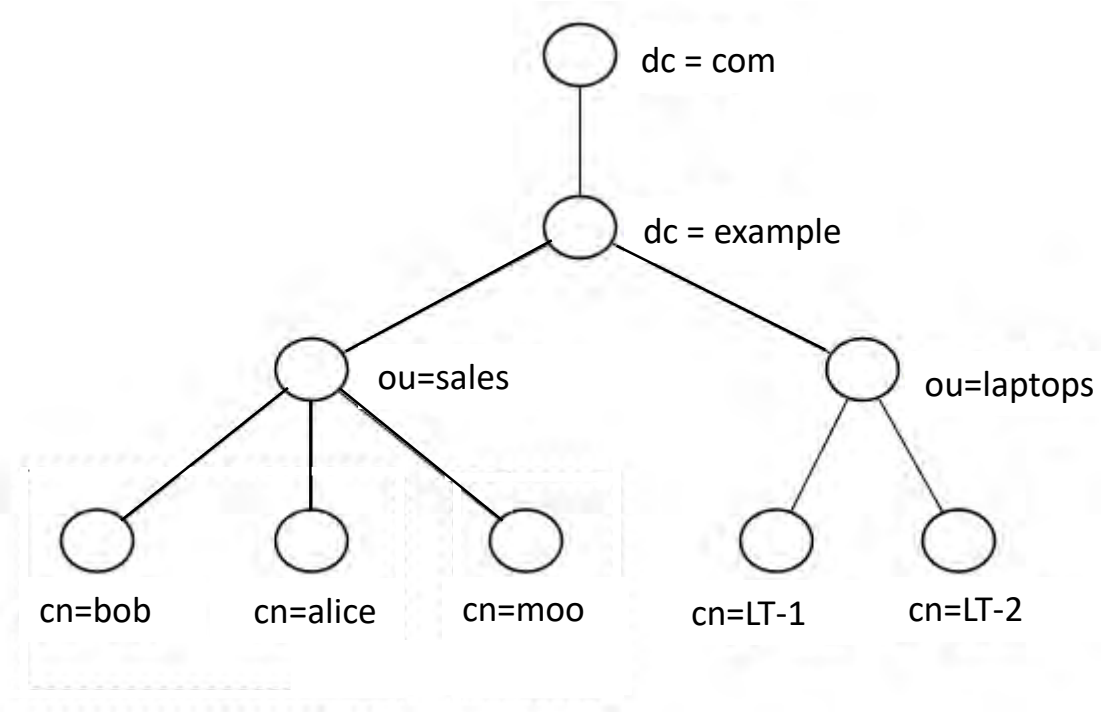


X.500 Naming Convention

X.500 is an ITU standard
- Ensures that every production-level user, computer and service has a globally unique name

X.500 structure can be overlaid on DNS structure
- DNS can be used to locate certain X.500 objects:
  - Computers (A records)
  - Services (SRV records)

X.500 Name levels:
- DC = domain component
  - DNS style domain names
- OU = organizational unit
  - Containers that represent company-chosen divisions such as departments, job roles, device types, security levels
  - Can contain other OUs and CN objects
  - Similar in function to a folder in a file system
- CN = common name
  - A leaf object (does not contain other objects)
  - Represents users, group names, computers, service accounts



Note: Do not mistake an OU for a group. A group is an alternate ID that multiple users share. Deleting a group will not delete its member users. An OU is a container. If you delete the OU, you also delete all objects (users, groups, computer accounts) inside that OU.

Kerberos

A ticket-based authentication protocol

Allows the user and server to authenticate each other

The user only has to log on once to access various network-based resources

- When the user logs on, they are given a ticket-granting ticket (TGT)
- When the user tries to access a resource, the server hosting the resource accepts the TGT and gives the user a session ticket
- The user uses the session ticket to repeatedly access the same resource
  - Usually there is a time limit of 10 – 12 hours, after which a new ticket must be assigned
- The user can reuse the TGT for a limited time period to obtain session tickets from other servers

Microsoft Active Directory uses Kerberos v5 as its authentication protocol

Lightweight Directory Access Protocol (LDAP)

Search and edit protocol for an X.500-compliant directory service

Authenticates connections by cross-checking usernames and passwords stored in the LDAP (directory service) database

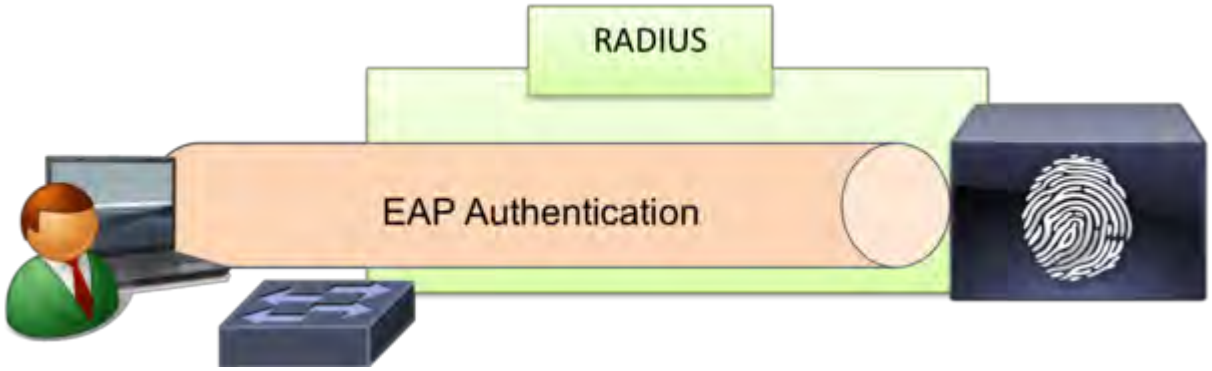
Used in Microsoft Active Directory, IBM Tivoli, Red Hat Directory Services and others

Extending Authentication

Extensible Authentication Protocol (EAP)

An authentication framework that supports nearly all credential types including:

- Passwords
- One time passwords
- Pre-shared keys
- TLS
- MD5 hashing
- Key exchange
- Biometrics
- Smart cards and tokens



Used originally to extend remote access authentication to more than a username and password

Now used in remote access authentication, RADIUS, and Wi-Fi (WPA2/WPA3 Enterprise)

Multifactor Authentication

Two or more forms of authentication are required to log in

Examples:

Username and password + One-time code (OTC) sent to the user’s phone

Username and password + biometric authentication

Smart card + PIN

RSA token generated number + PIN

Typical Multifactor Authentication Example

RADIUS

Remote Authentication Dial-in User Service

Used to grant network access

Handles remote authentication and related services for network access control

- All authentication is forwarded to a centralized server
- Provides centralized authentication, authorization, and accounting (AAA) management for users and devices that connect to the network

Open standard that allows vendor interoperability between any AAA client and server

- Works well with 802.1x
- More accounting options than TACACS+
- UDP 1812 for authentication and authorization
- UDP 1813 for accounting

TACACS+

Terminal Access Controller Access-Control System Plus

A competitor to RADIUS

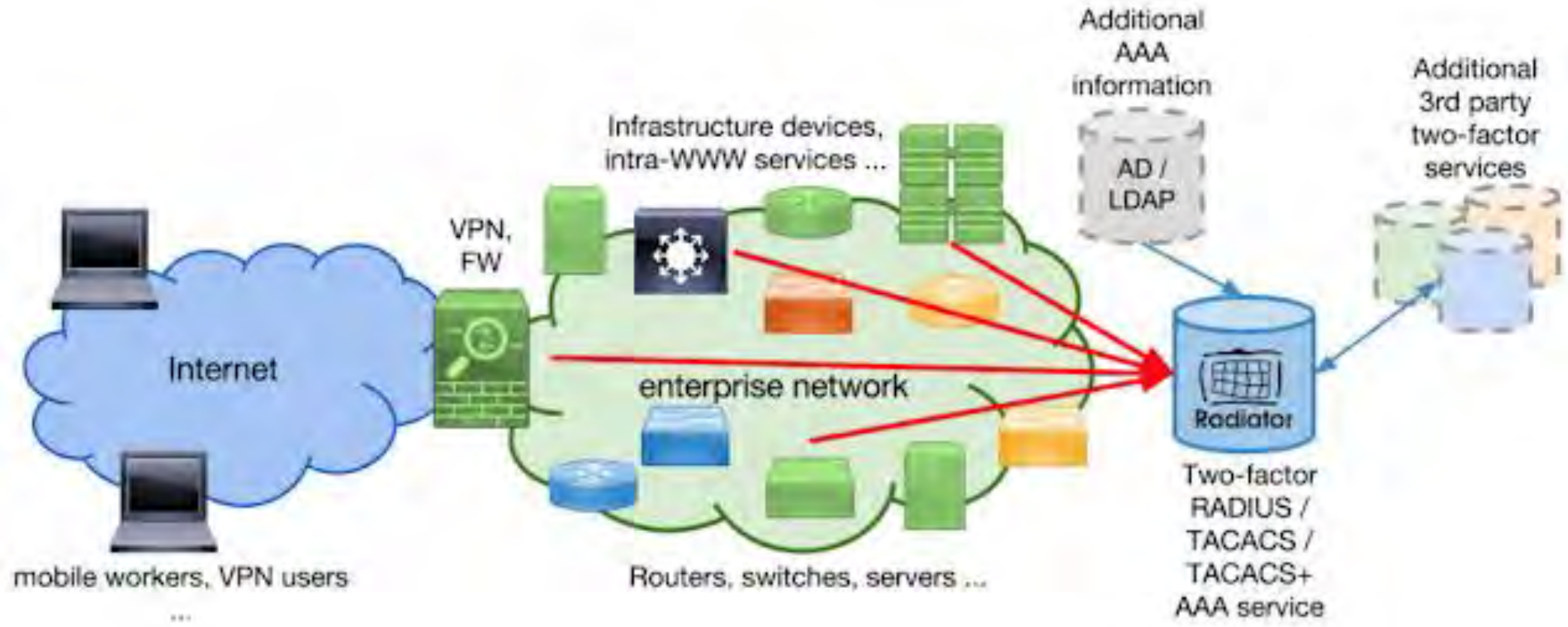
Used for device administration

Developed by Cisco, then released as an open standard

Does not support 802.1x

TCP 49

AAA Example


Additional
AAA
information
Additional
3rd party
two-factor
services
Infrastructure devices,
intra-WWW services ...
AD /
LDAP
VPN,
FW
Internet
enterprise network
Radiator
Two-factor
RADIUS /
TACACS /
TACACS+
AAA service
mobile workers, VPN users
...
Routers, switches, servers ...

802.1x

IEEE standard for port-based network access control

Based on Extensible Authentication Protocol

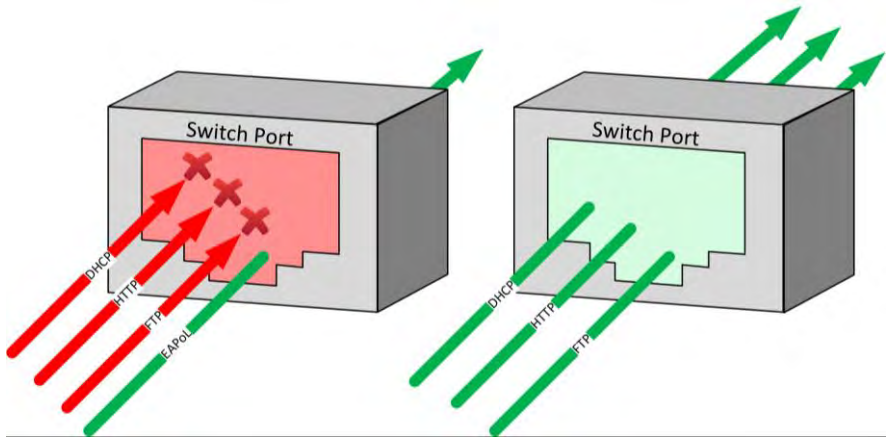
- Created to support certificates, biometrics, tokens, and other non-password-based credentials

Used to secure the network edge

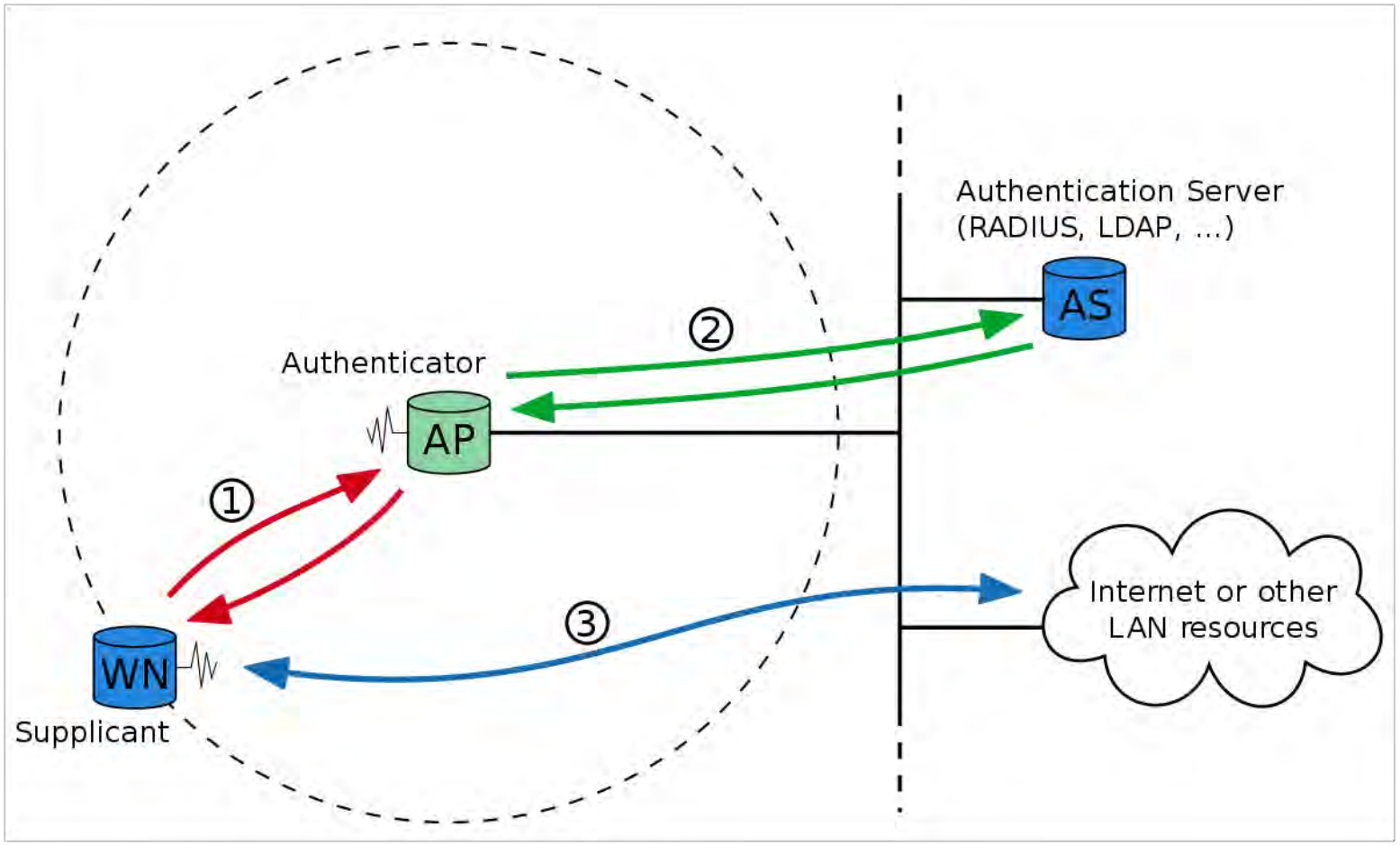
A client (supplicant) is detained at a captive portal (switchport, WAP)

They cannot continue into the network until the user is authenticated and authorized by a RADIUS server

Depending on the product, can support nearly any credential type



802.1x Wi-Fi Example



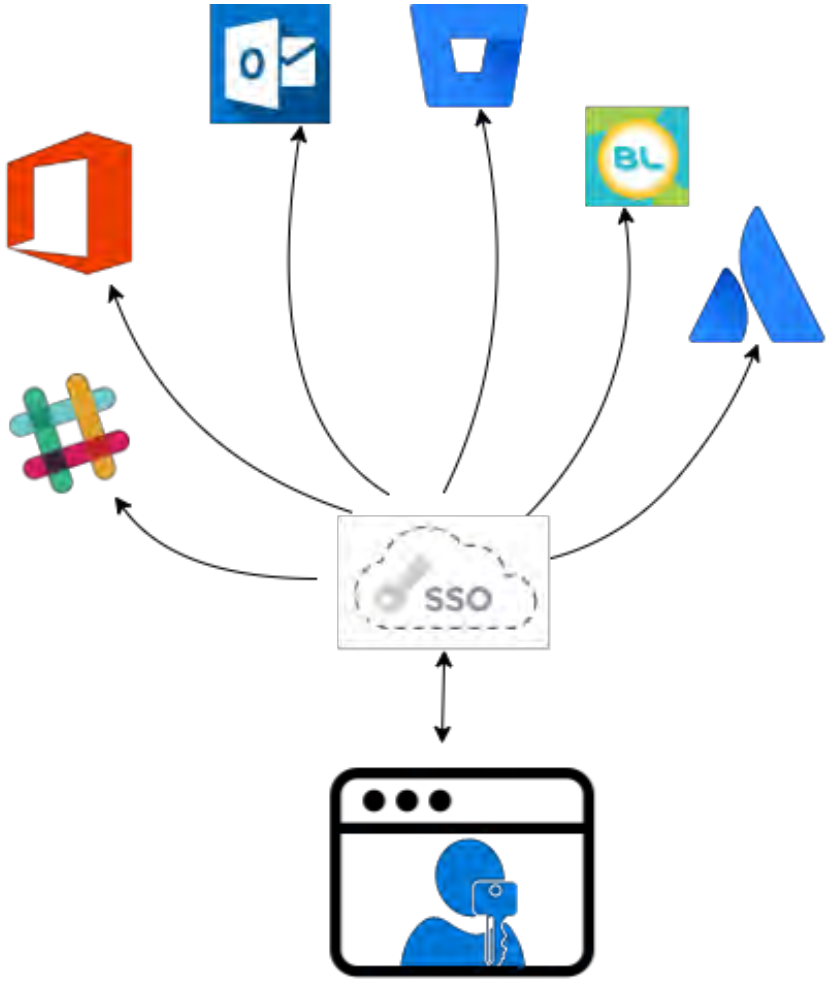
Single Sign-on (SSO)

A generic term for a centralized user authentication service

Coordinates authentication across unrelated systems

- Built on the concept of federated identity
- A user's identity attributes are shared across trusted but autonomous systems

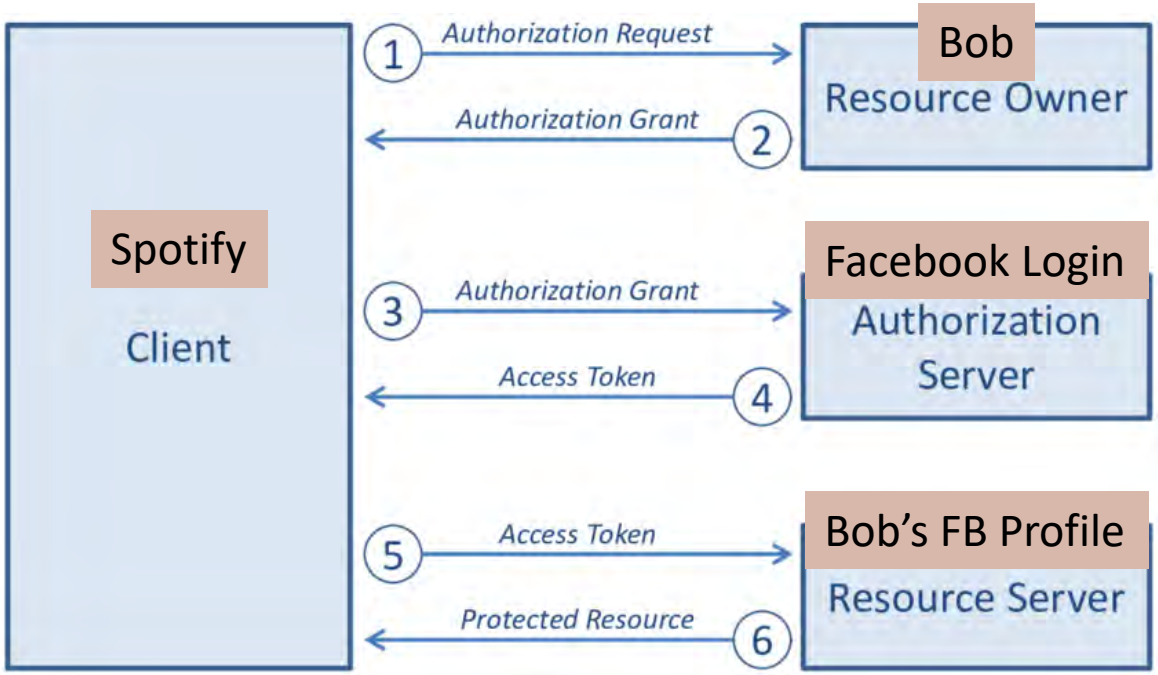
One set of login credentials can be used to access multiple applications and sites

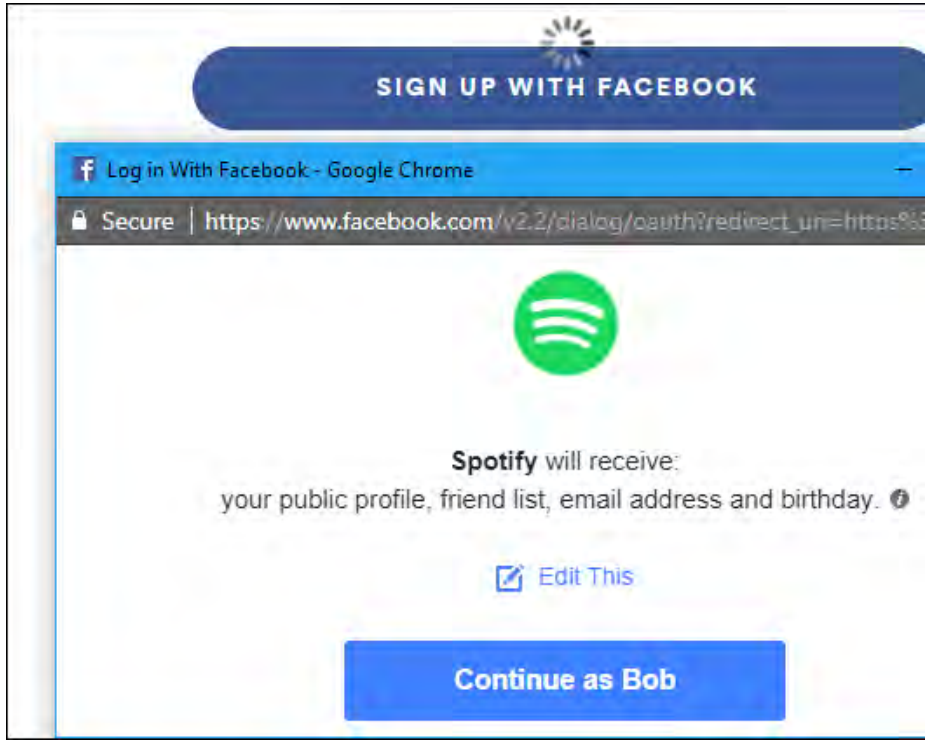


SSO Types

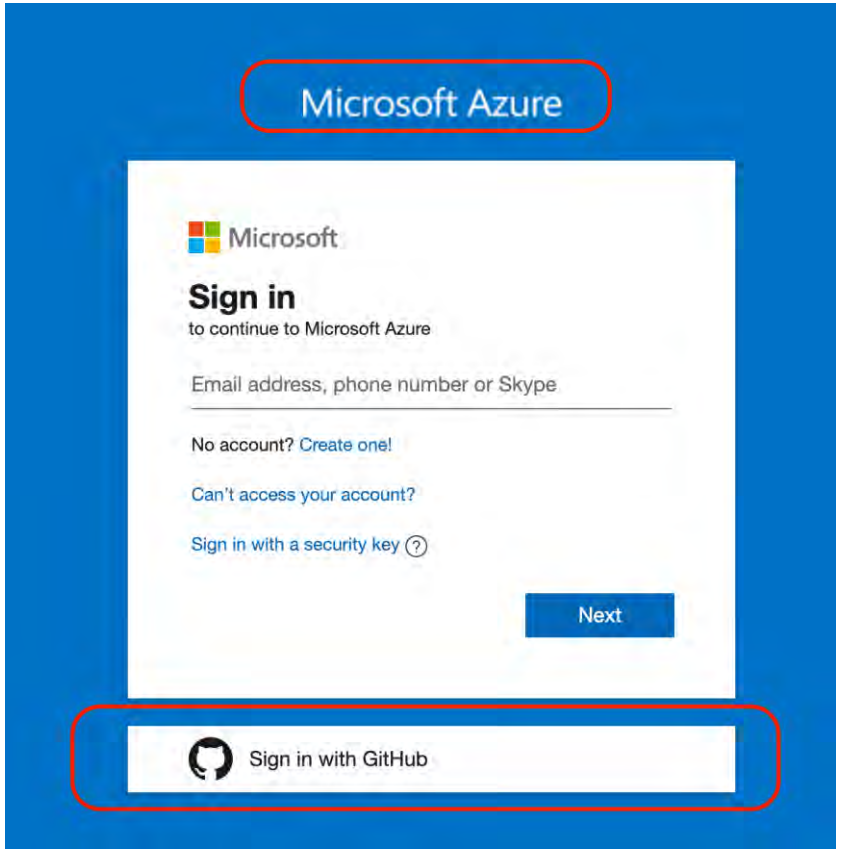
Type	Description
Open Authorization (OAuth)	• An open-standard *authorization* protocol • Internet users can grant an app (or website) access to their information on another website without giving the app the password • Used by Amazon, Google, Facebook, Microsoft, Twitter, etc. to permit users to share information about their accounts with third-party apps or websites without giving those apps the password • Well-suited for mobile apps
OpenID Connect (OIDC)	• Sits on top of Oauth 2.0 • Enables a user to log in to a service using their Facebook or Google account rather than entering a separate set of user credentials

OAuth Example





OpenID Connect Examples

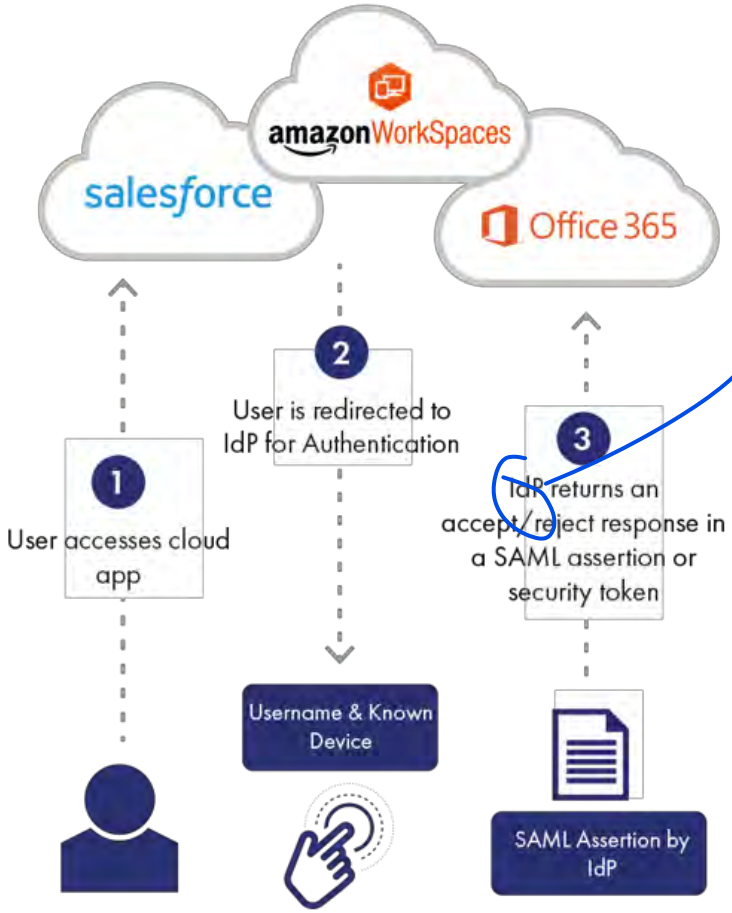


SSO Types (cont'd)

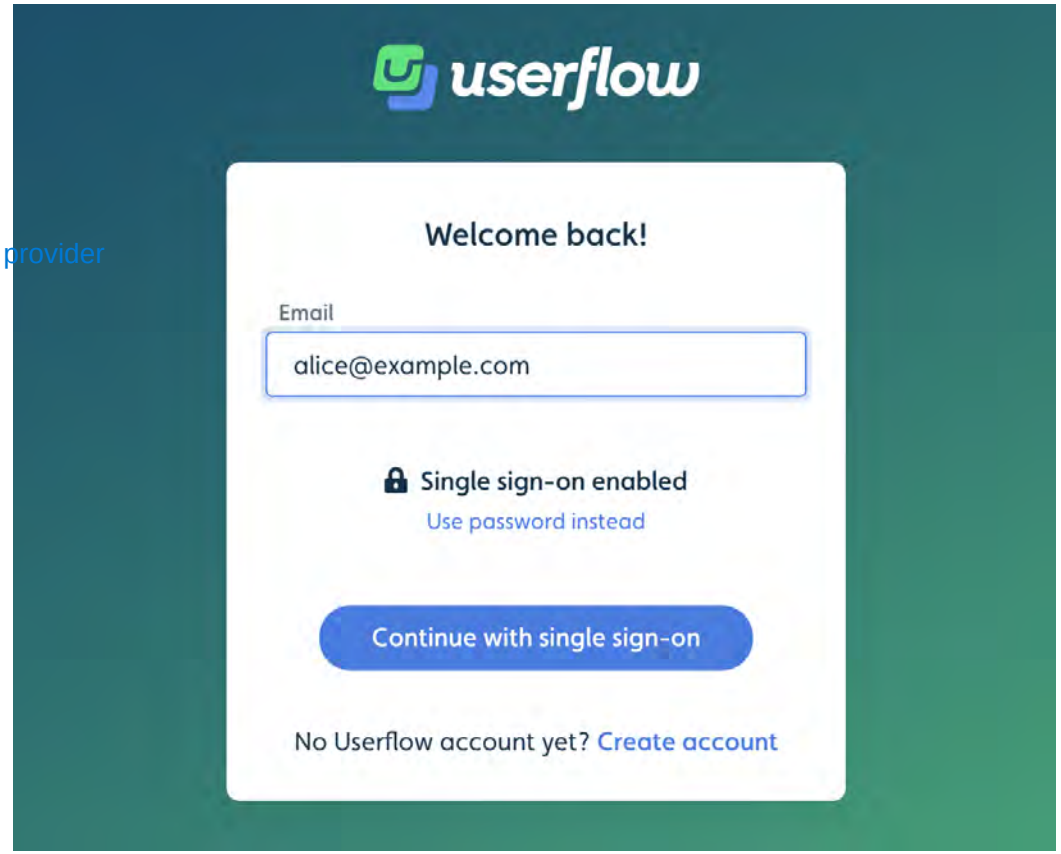
Important

Type	Description
Security Assertion Markup Language (SAML)	• An open *authentication* standard used by many enterprises to allow users access to multiple unrelated resources (including cloud based) from a single login • The various resource servers check with the identity provider server to see if the user has already logged on
Kerberos	Considered a type of SSO You can log into one domain, and still be trusted by other domains to access their resources
Smart card authentication	Not traditional SSO, but hardware that facilitates the same process Smart card contains the user's certificate Activated by inserting the card in a reader with the user providing a secret PIN

SAML Examples



this stands for identiy provider



Authorization

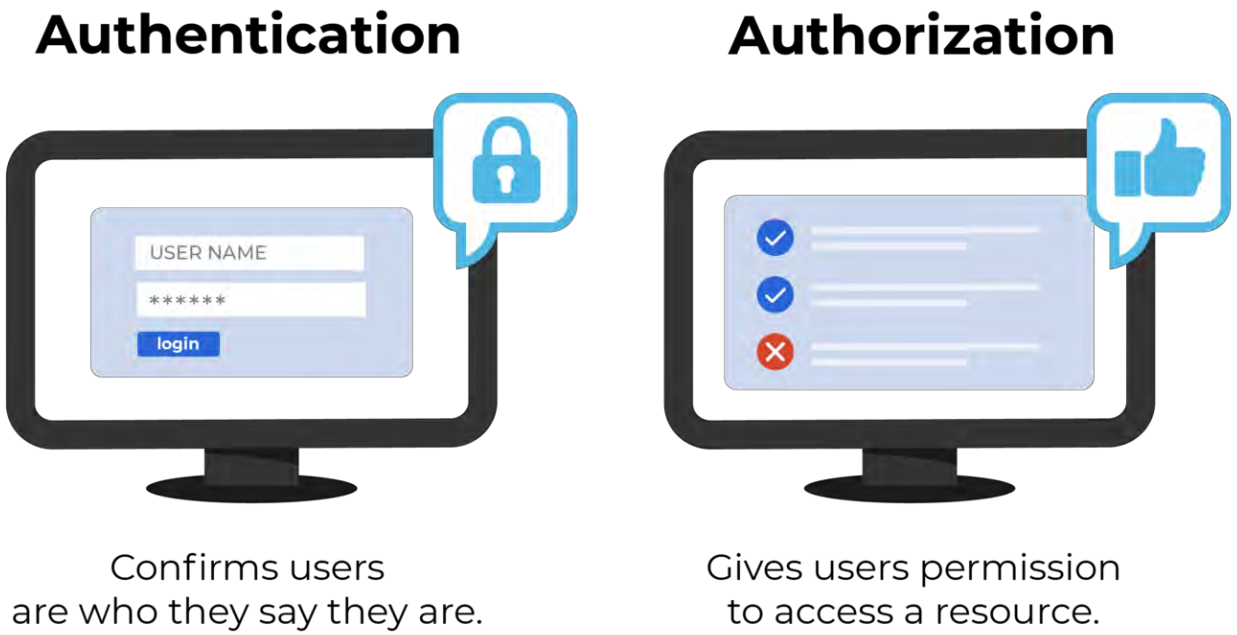
What is the Difference Between Authentication and Authorization?

Authentication = you prove your identity

Authorization = once authenticated, you are granted permission to perform certain tasks

The two go hand in hand

- It is not useful to have one without the other



Common Authorization Enforcement Mechanisms

Permissions (listed in an object's ACL)

- Examples: read, write, execute, delete, list

User rights (special powers attached to the user's token when they log on)

- Examples: change system time, log on locally, backup and restore, add workstations to the domain, shut down the system, take ownership of files or other objects

Local computer policies

Active Directory Group Policy

Firewall rules, router ACLs, proxy rules

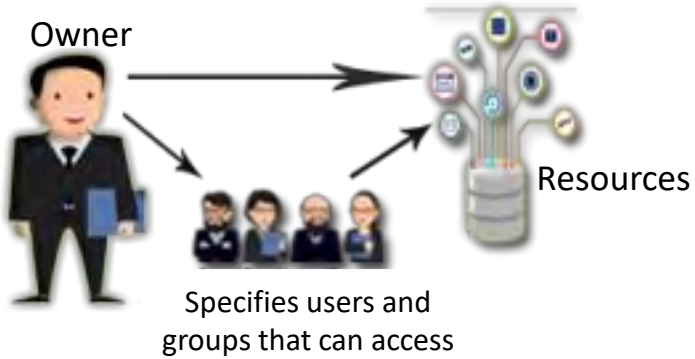
ABAC authorization engine

Access Control Types

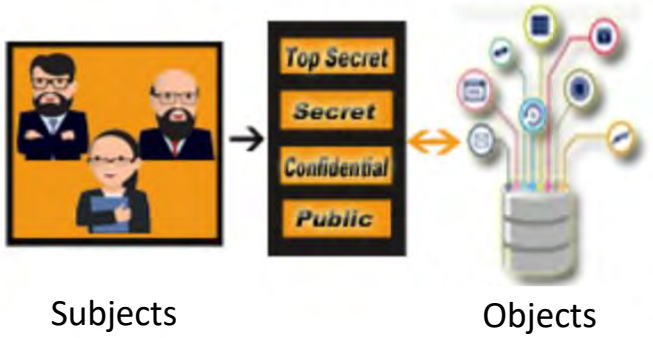
Type	Description
Discretionary (DAC)	• The resource owner assigns permissions at their discretion • The owner may or may not be the administrator
Mandatory (MAC)	• Objects (resources) have sensitivity levels • Subjects (users, processes, service accounts) have clearance levels • Subjects can only access objects for which they have clearance
Role-based (RBAC)	• A type of DAC in which permissions are granted based on a user's job or role • Microsoft uses groups to implement RBAC
Rule-based (RuleBAC)	• Permissions granted at that moment in time to that specific object based on a set of rules • Used by firewalls and in router ACLs to permit or deny individual packets
Attribute-based (ABAC)	Permissions granted dynamically based on additional information (attributes) about a user, the environment, and the asset Example: a grocery store uses your age to determine if you can buy certain products

Access Control Type Examples

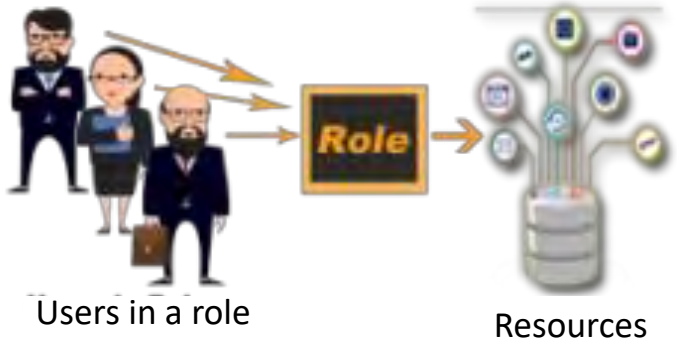
Discretionary Access Control (DAC)



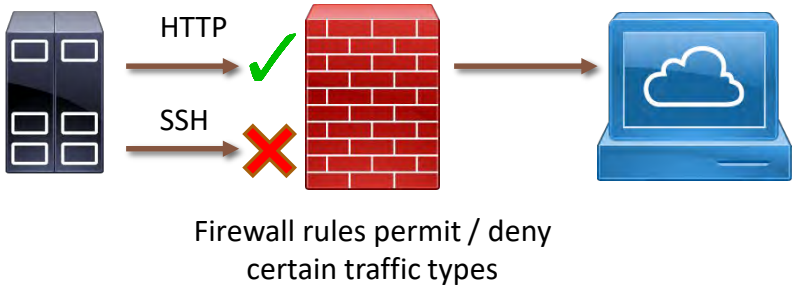
Mandatory Access Control (MAC)



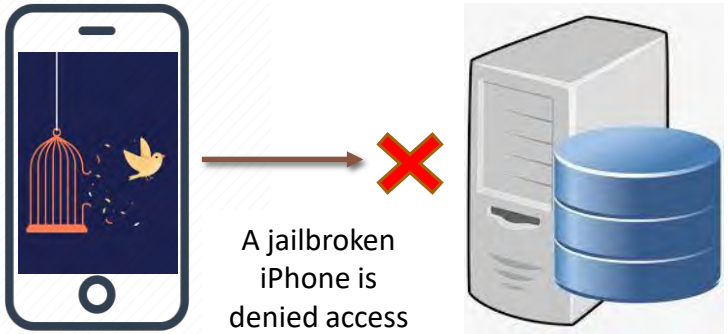
Role-Based Access Control (RBAC)



Rule-Based Access Control (RuleBAC)

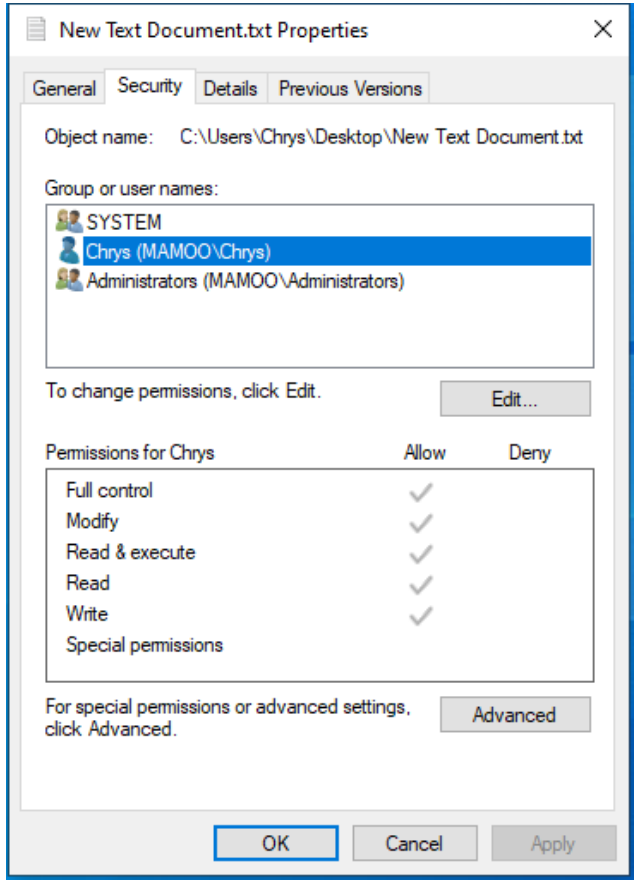


Attribute Based Access Control (ABAC)

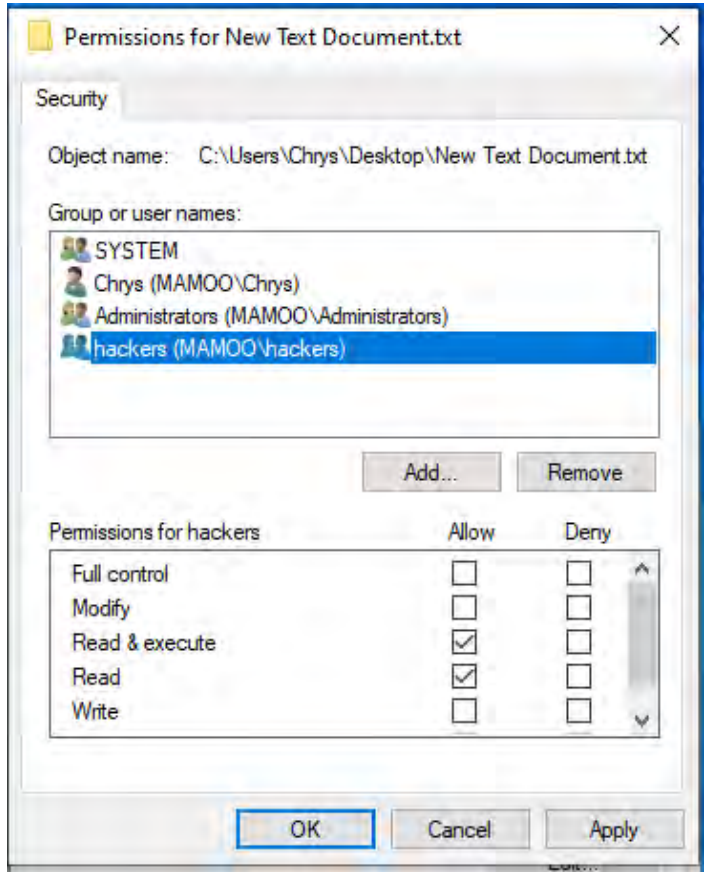


Windows NTFS ACL Examples

DAC



RBAC

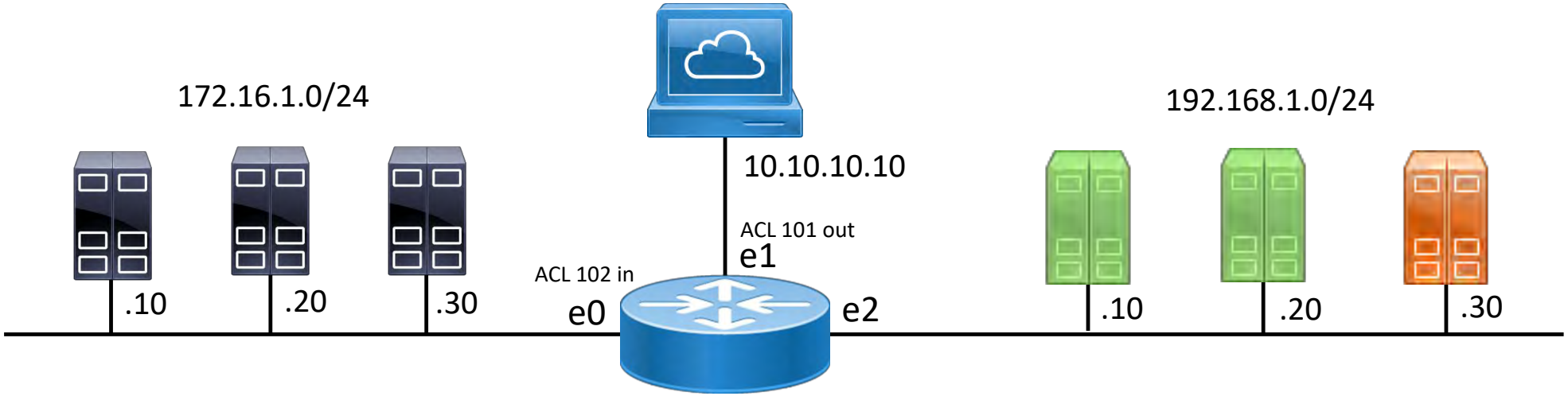



```
C:\WINDOWS\system32>net localgroup hackers
Alias name     hackers
Comment

Members

-------------------------------------------
ihacku
moo
The command completed successfully.
```

Router ACL (RuleBAC) Example

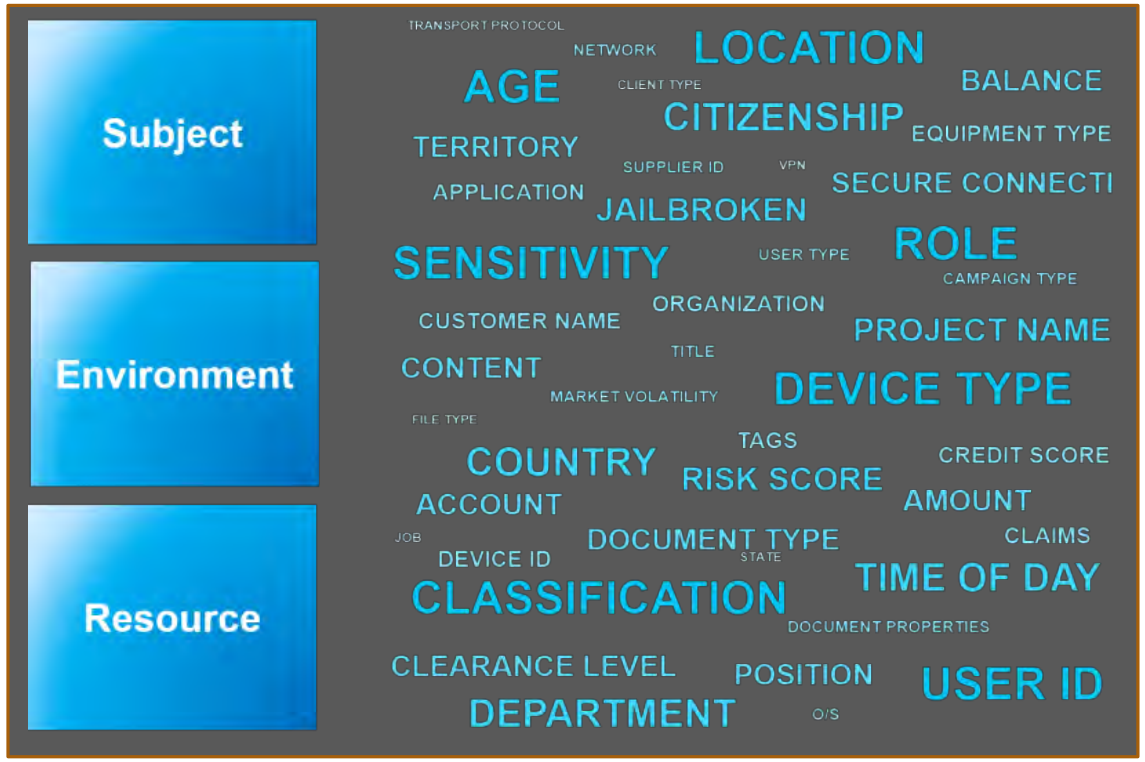



```
Access-list 101 permit ICMP   host 192.168.1.30      host 10.10.10.10
Access-list 101 permit TCP    any                    host 10.10.10.10 http
Access-list 101 permit UDP    any                    host 10.10.10.10 snmp

Access-list 102 deny   IP     172.16.1.0 0.0.0.255   192.168.1.0 0.0.0.255
Access-list 102 deny   TCP    172.16.1.0 0.0.0.255   host 10.10.10.10      ssh
Access-list 102 permit IP     any                    any
```

ABAC Examples

- An engineer that is reassigned to a new project
  - They can automatically access information related to the new project but not the previous one
- An account executive is reassigned to a new territory
  - They are automatically able to view and perform operations on accounts and products in the new territory
  - But can no longer access anything from the old territory
- A finance manager can only download docs when they are physically in the US
- An HR manager is assigned to an overseas project
  - They can only access the PII data of the employees in that country



Network Device Hardening

Basic of the Basics

Change default configurations including passwords

Disable unnecessary services and features

Require passwords for any type of login or privilege escalation

Update/patch the device regularly

Use the highest encryption level possible

Physically/environmentally protect the device

Follow manufacturer/industry best practices

Switch Security

Disable Unneeded Switchports

Disable Unneeded Network Services

Change Default Passwords

Do not use well-known training passwords such as “P@ssw0rd”, “cisco”, or “sanfran”

Set Adequate Password Complexity/Length

Require a console password

Require a password for privileged tasks

If possible, disable remote access
- Or only permit SSH, not telnet
- Even better, use TACACS+ to authenticate

Change the default VLAN

Provide physical security for the switch

Rogue Device Detection on Switches

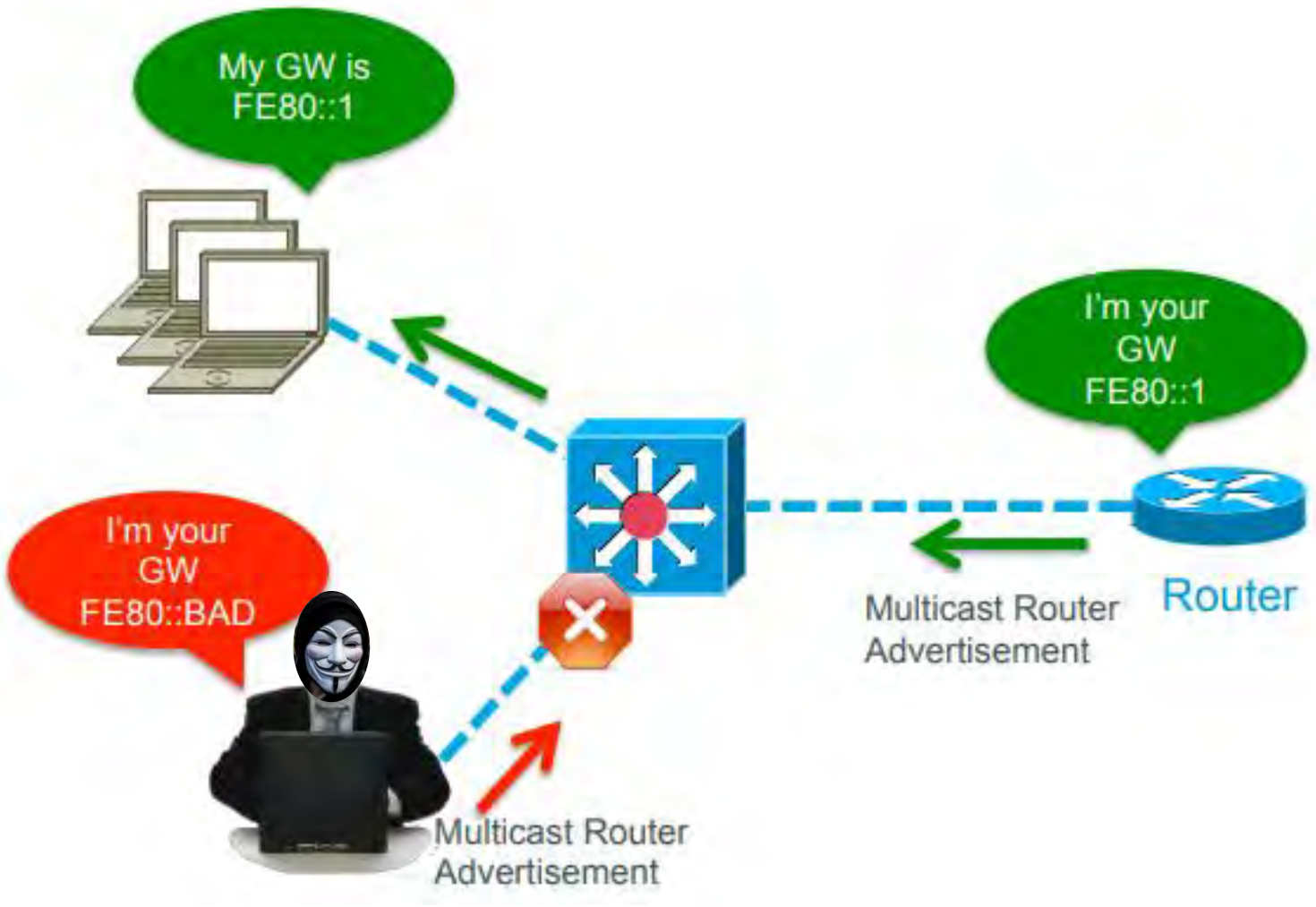
Router Advertisement (RA) Guard

- Protects against rogue or malicious routers
- IPv6 routers issue router advertisements to announce themselves, the network ID (IPv6 prefix) and other information
- RAs are not encrypted and can be spoofed
- You can configure a switch to inspect IPv6 router advertisements
- If the RAs don’t match preset criteria (source MAC, source IPv6 address, etc.), they are thought to come from a rogue device
- Unwanted or rogue RAs can be blocked by the switch

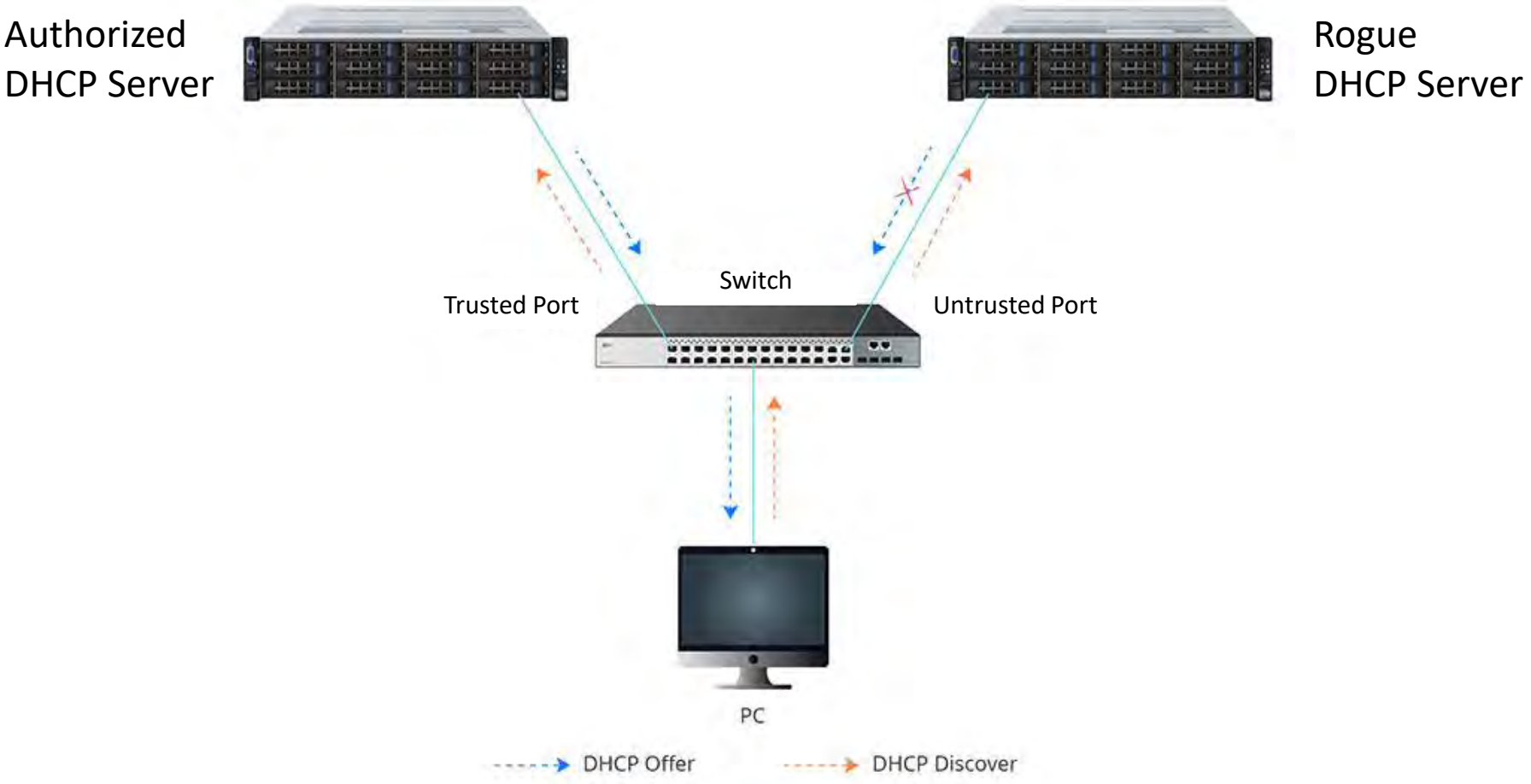
DHCP Snooping

- Classifies switchports as either trusted or untrusted
- A DHCP offer message can only be sent through a trusted port
- Otherwise, it will be dropped

Router Advertisement (RA) Guard Example



DHCP Snooping Example



Router Security

Patch or update the operating system/firmware to the latest version

Disable unused ports and services

Set passwords on console access, remote administration, and elevated prompt

Restrict hosts that are allowed to make remote administrative connections

Use the highest encryption level wherever possible

Enable warning banners on login

Provide physical protection for the router

Dynamic ARP Inspection

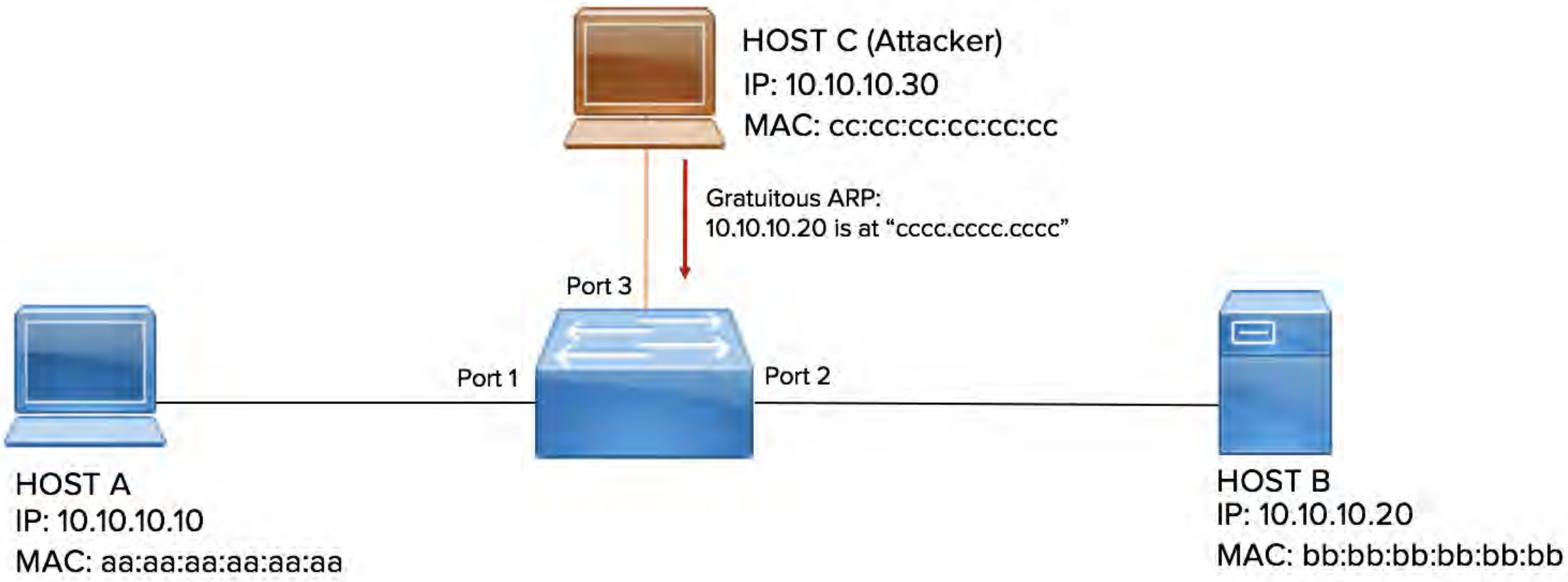
A security feature that validates Address Resolution Protocol (ARP) packets in a network

Allows a network administrator to intercept, log, and discard ARP packets with invalid MAC address to IP address bindings

Invalid ARP packets are dropped

Protects the network from certain “man-in-the-middle” attacks

Dynamic ARP Inspection Example



Control Plane Policing (CoPP)

An application of quality of service (QoS) technologies in a security context

- Configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to the control plane of routers and switches
- Protect the device control plane against reconnaissance and denial-of-service attacks
- Helps maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch

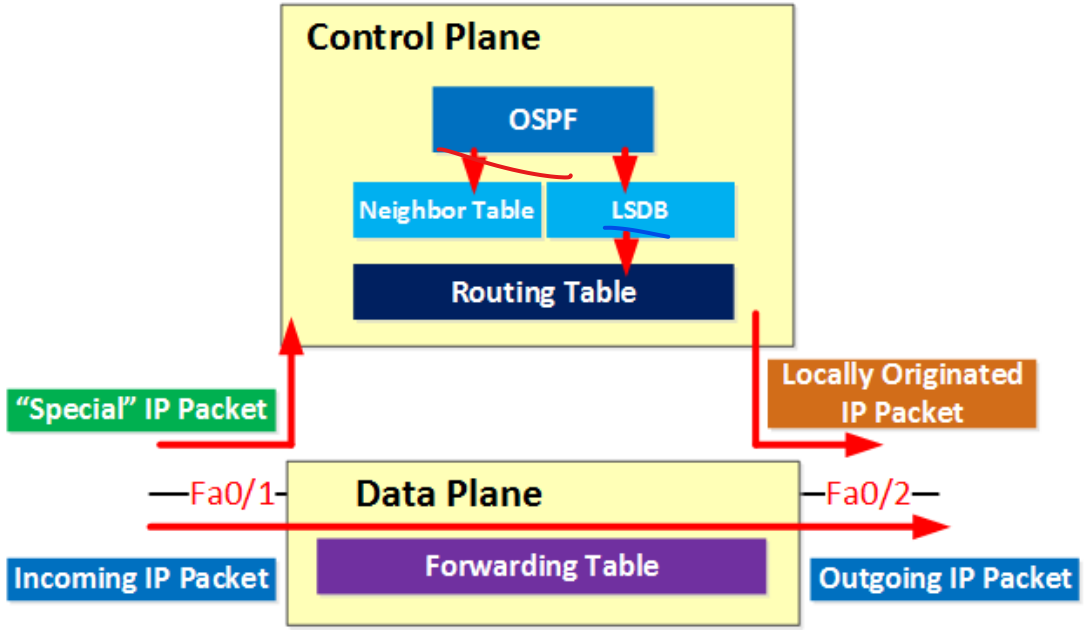
A router or switch can be logically divided into four functional components or planes:

- Data plane (most traffic travels through here)
- Management plane
- Control plane
- Services plane

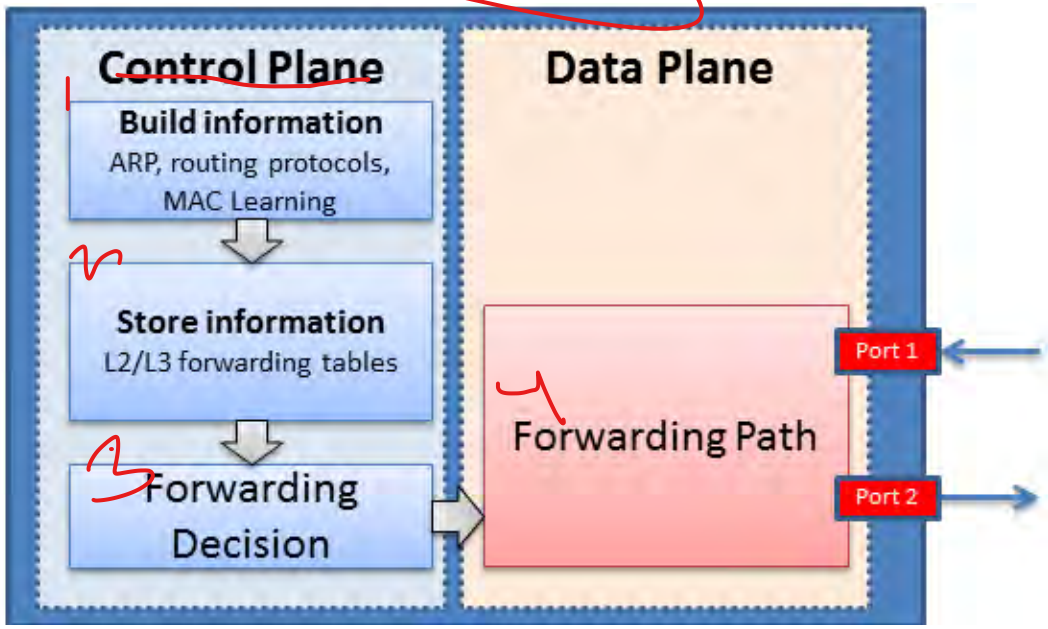
Handles routing protocol updates, keepalives, network management packets

Router and Switch Control Plane Examples

Router



Switch



Additional Network Security Best Practices

Use SNMPv3 (encrypted version) micro soft doesnt supportr this version

Change SNMP community strings

Implement port security on switches

- Limit number of devices on a switchport
- Block unknown MAC addresses
- Hard-code MAC address table with known MAC-to-port mappings / sticky learn correct MAC address

Implement a good patch management and firmware update system

If possible, implement a cloud-based AIOps SIEM system

- At least implement a good IDS/IPS

Wireless Security

Wireless Security Layers

You need to protect the:

- Connection
- Wireless signal
- Device
- End user
- Data
- Network

Common Wi-Fi Threats

Incomplete configuration/misconfiguration

Denial of Service

Sniffing and passive capturing

Rogue access points

Evil twin attacks

Hacking of lost or stolen devices

Freeloading using some else wifi

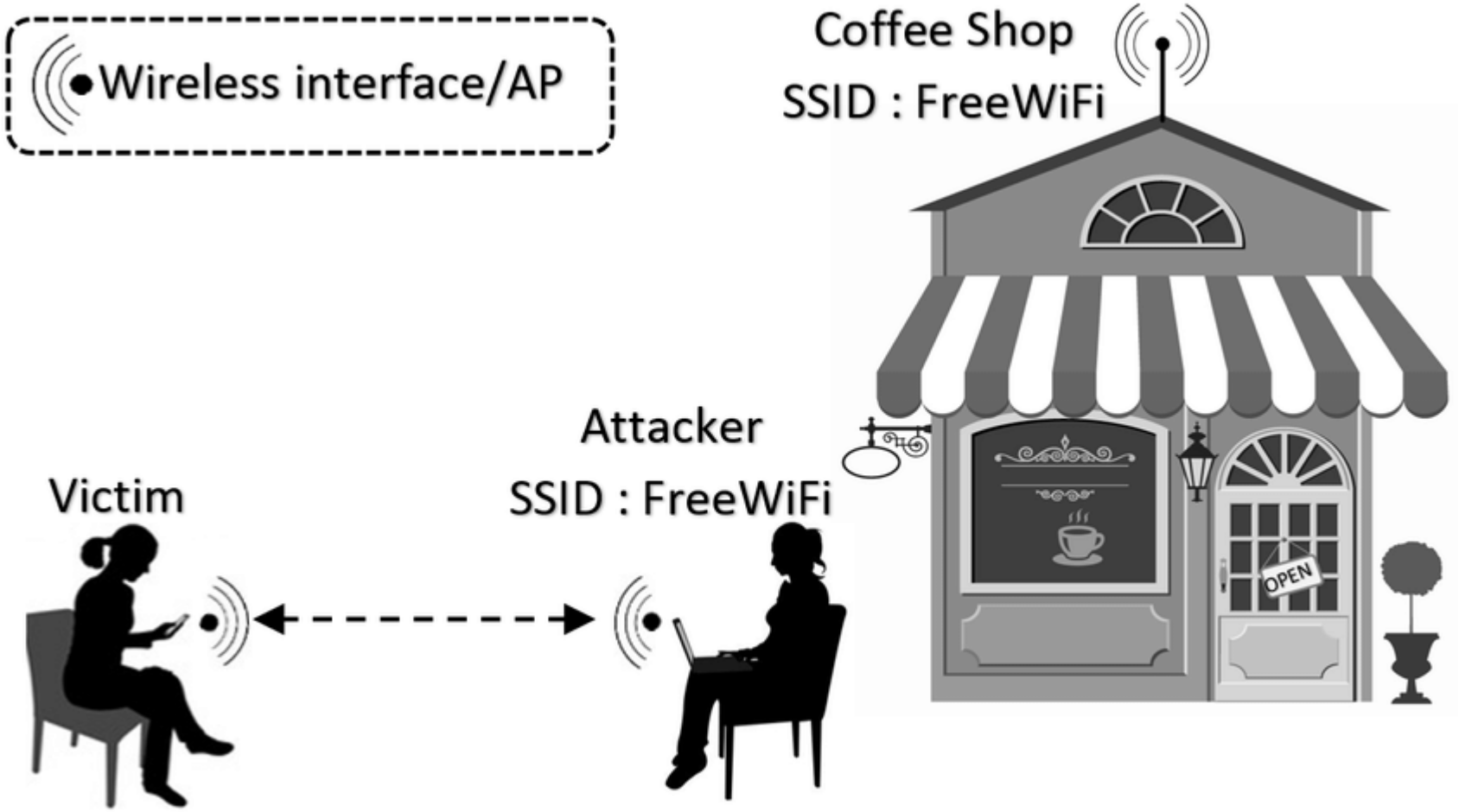
Network injection

MAC spoofing

Man-in-the-Middle attacks

Ad-hoc or non-traditional networks

Evil Twin Attack Example



ALT Evil Twin Example

Wireless Configuration Best Practices

Strategically place antennas to always point inward into the building/complex

If possible, maintain low power levels on WAPs

- Add more WAPs to make up for coverage gaps

Change the default SSID

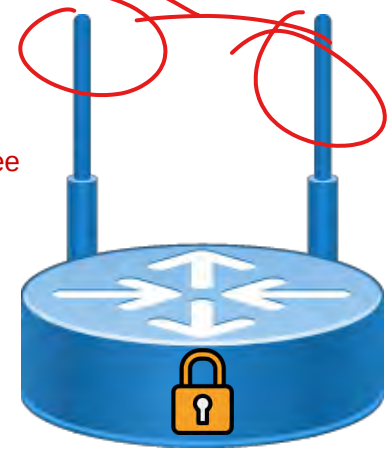
Ensure remote router login is disabled

Ensure router access password is set and firewall protection is enabled

Ensure MAC Address filtering is enabled on routers/access points

Ensure SSID broadcasts are disabled at access points and passphrase is changed frequently

use 180 o r90 degree



SSID Settings Best Practices

Hide SSID when practical

Keep passphrases free of SSID, network/company name, or anything that is easy to figure out

Ensure there is a firewall/packet filter between AP and Intranet

Keep wireless network strength low enough avoid detection outside organization

Regularly ensure there are no issues with setup/configuration

Use extra traffic encryption

Authentication Best Practices

When practical, implement MAC filtering on the Access Point

Use captive portals for legal protection and to enforce user/device registration

Use the highest security standard possible (WPA3 or WPA2)

- Prefer 802.1x authentication over a pre-shared key

Ensure access points are in secure locations

Ensure all wireless drivers are up-to-date

Ensure network is disabled when it isn’t needed

Additional Wireless Security Best Practices

Use different SSIDs and VLANs to isolate users / devices by security level:

- Guests
- Wireless clients

Enroll devices (including BYOD) into Mobile Device Management to:

- Implement Geofencing
- Enforce end point protection
- Enforce separation of business and personal data
- Disallow jailbroken or rooted devices on the network

Realize that MDM and endpoint security software is *not* used to protect the mobile device, but instead used to protect the network *from* mobile devices

Remote Access Security

Remote Access Risks

Home computers are often accessed by multiple people

- Home users visit various websites
- Execute many different pieces of software

The home computer can become compromised

- It can act as a launch point for an attacker to hack the business network
- Home computers usually use weak passwords or no passwords at all

Teleworkers often work from public areas

- Hotels, airport and coffee shop hotspots
- You never know who else is around on the network

Most consumer-ready antivirus products won’t stop sophisticated hackers targeting your organization

Remote Access Risk Countermeasures

Establish a remote access policy

Limit the use of remote access

Require multifactor authentication

Require unique credentials

Encrypt data and connections

Require separation of personal and company data

Back up and store data in a secure online location
- Separate from the device itself

Use endpoint protection (firewall, antivirus)

Require clients to prove “health” before being allowed to connect
- Use 802.1x and a Network Policy Server
- Require minimum antivirus and patch levels, firewall settings, etc.

Enroll all remote access mobile devices in Mobile Device Management

Captive Portal

Requires visitors to agree to legal terms

Can be used to register devices and users

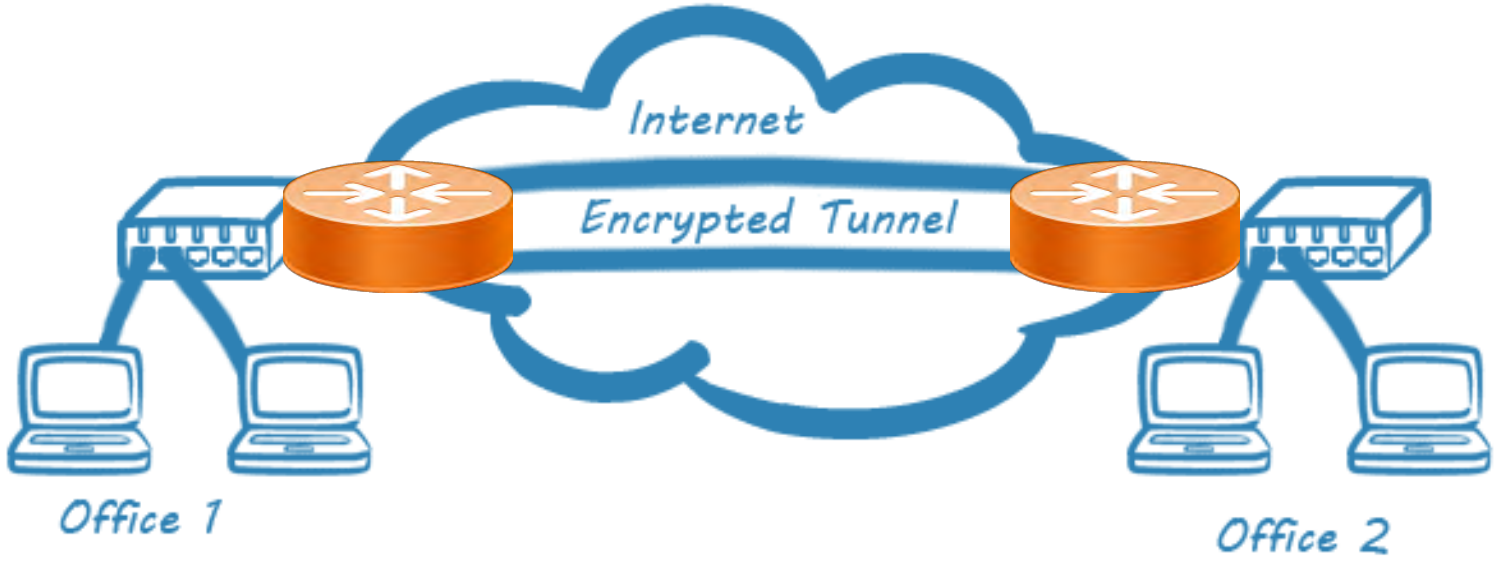
- Require users to register with their email address
- Grant them a temporary PIN
- Make them change the PIN when they first log on
- Capture the MAC address of the user's device

Site-to-Site VPNs

IPSEC tunnel mode VPN between routers

Clients at both sites have no knowledge that their traffic is being sent through a tunnel

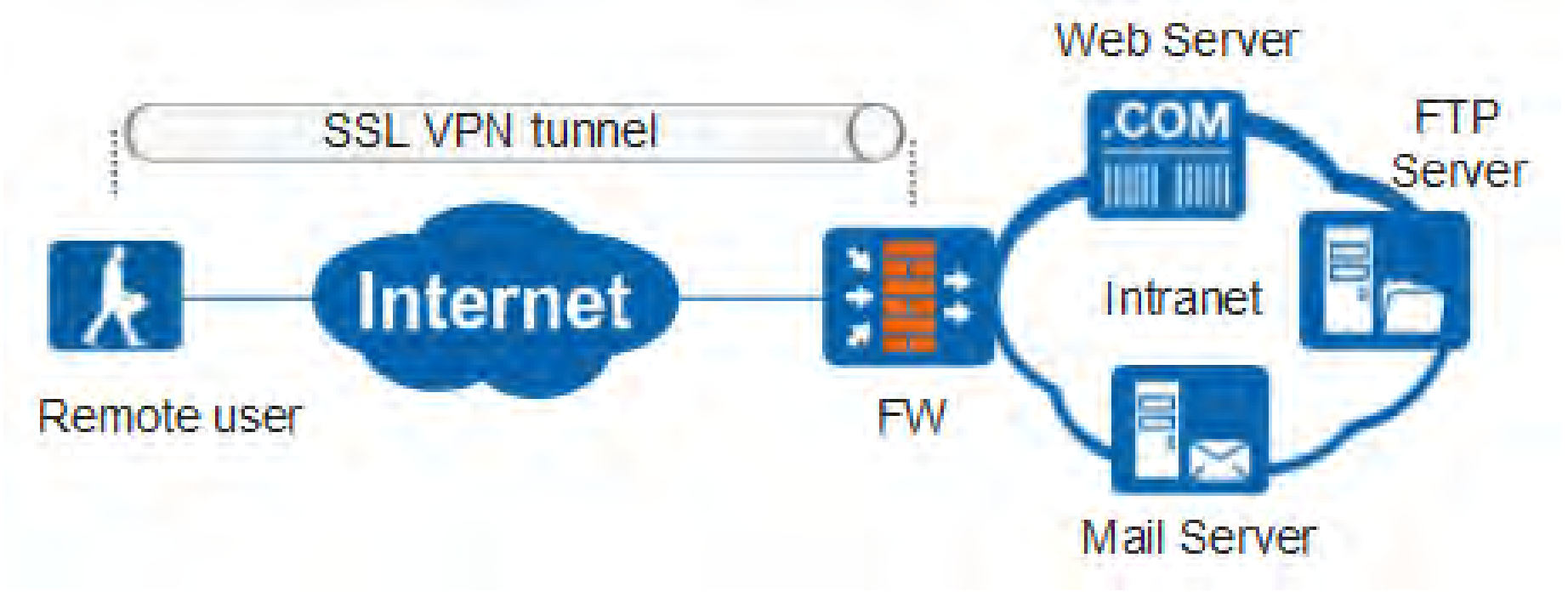
Ensure that the two sites have different IP subnets (otherwise you can’t route between them)



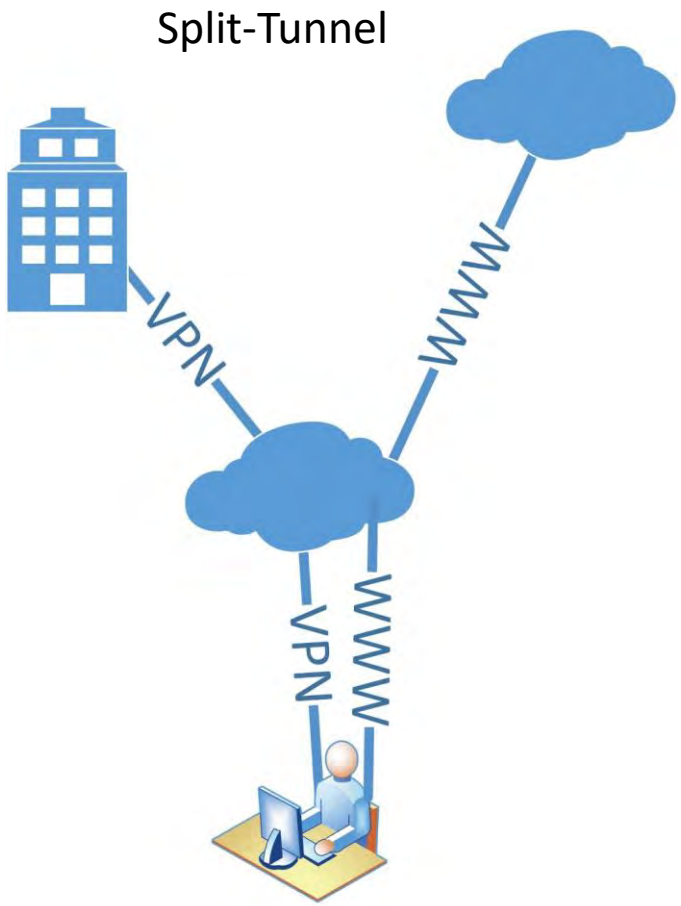
Client-to-Site VPN Types

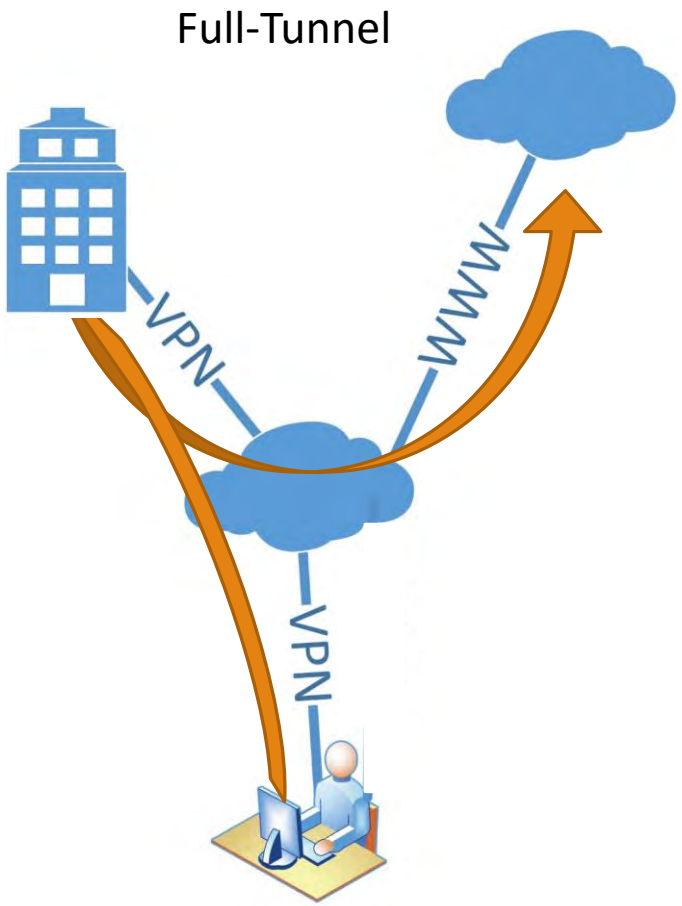
VPN Type	Description	Considerations
Clientless	• AKA SSL VPN • User uses any browser to make an HTTPS connection	• Easiest for the end user • Passes through firewalls • Requires a VPN-terminating
Split tunnel	• The remote client launches a VPN when connecting to the corporate network • If the client is just surfing the Internet, no VPN is created • The client can do both at the same time	• Requires configuration by the administrator • Traffic to the Internet will have no additional performance encumbrances
Full tunnel	• The remote client always maintains a VPN to the corporate network • All traffic, even to the Internet, is first sent to the corporate network, and then routed to the Internet as necessary	• All client traffic is passed through the corporate network • The company has full control of all client traffic • Performance is likely to suffer

Clientless SSL VPN Example



Client Split-Tunnel vs Full Tunnel Examples





IPSEC vs SSL

IPSEC	SSL
Workstation configuration required	Browser-based from any computer
Must be terminated at the firewall	Can pass through a firewall
Administrator can configure VPN then restrict user access	Limited access if user does not have the right to install applications
Access as if client machine is on the LAN	Need to use web applications to ensure access
Has a pre-shared key in addition to user password	Vulnerable to password compromise

SSH Security Risks

Unauthorized SSH servers

Unpatched SSH software

Vulnerable SSH configuration

SSH port forwarding allows attackers to use an encrypted connection to bypass firewall restrictions
- You can’t inspect the packet contents

Private keys could become compromised
- Most SSH implementations allow users to configure their own key files
- Could be used to create rogue host keys and backdoors

SSH is generally integrated with other operating system components
- Could be misused to enable unauthorized privilege escalation

Staff and contractors that leave or are terminated might not have their access to SSH servers revoked in a timely manner

Remote Desktop

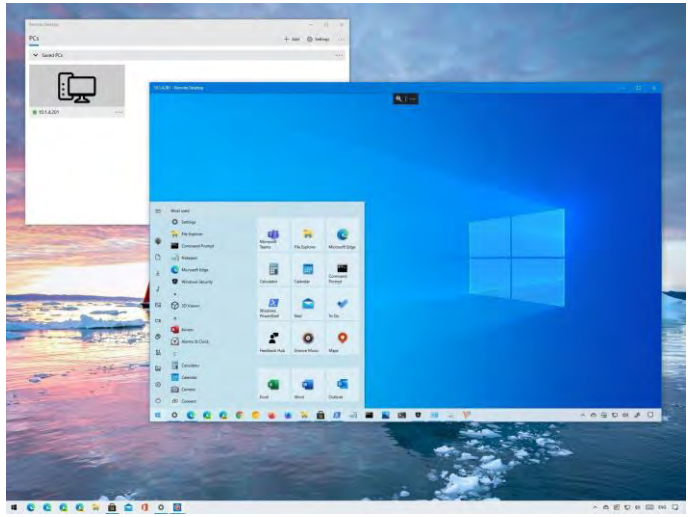
Client-to-server connection

Uses Remote Desktop Protocol

TCP 3389

Requires an unobstructed connection to the server

- Port forwarding at the firewall
- VPN into the network
- Client and server on the same network segment

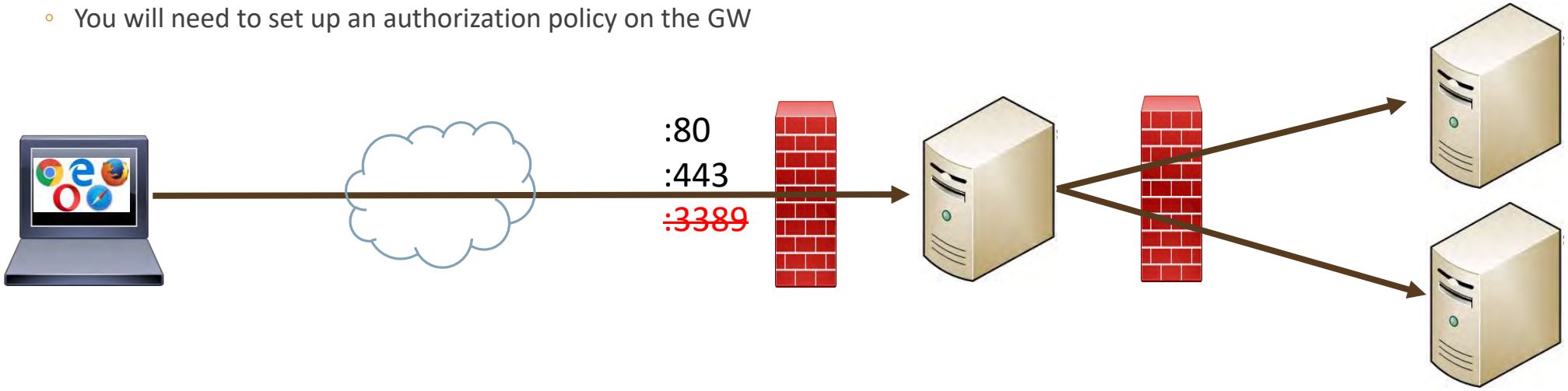


Remote Desktop Gateway

A feature of Windows Server

Allows Internet clients to use a browser to access corporate resources

- Place RD Gateway in the DMZ
  - Gateway uses Windows Remote Desktop Services and Internet Information Services (IIS web service)
- Clients outside establish an SSL tunnel to the GW
  - User can authenticate using a password or smart card
- GW acts as a relay between the client and the internal resources
  - You will need to set up an authorization policy on the GW



VNC

VNC is a competitor to Remote Desktop

- Small piece of software
- A VNC client connects to a VNC server
- You can see and interact with the user's desktop
- VNC by default uses TCP port 5900
- There are many separate VNC products
  - TightVNC, RealVNC, UltraVNC, TinyVNC and others

Note:
Do not confuse VNC with VPN.

- VNC provides remote control of a computer at some other location allowing users to operate that computer as if they were sitting in front of it.
- By contrast, a Virtual Private Network (VPN) simply connects you to a remote network, but does not provide a desktop for you to use.
- Rather, you use your own desktop to access the resources that exist on that network

VNC Security Considerations

Not all VNC products require a password to make a connection

Many VNC versions have software bugs allowing Denial-of-Service, buffer overflows, and remote code execution

- A search for “vnc” at cve.mitre.org returns 126 records

Virtual Desktop

Virtual Desktop refers to two things:

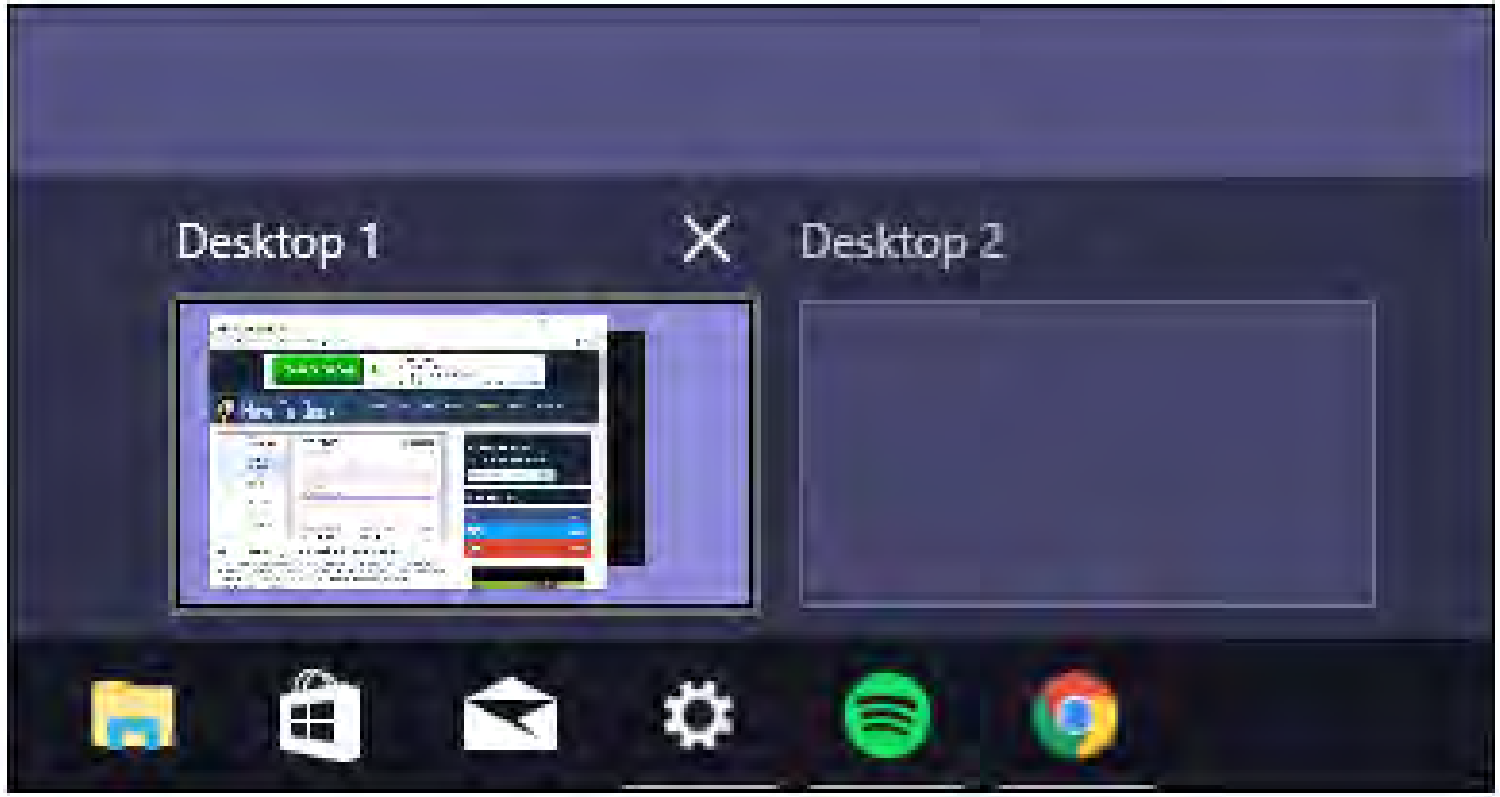
Multiple, separate desktops on a computer

- Each displays a different desktop, open windows and apps, for the same user
- The user can switch between the desktops
- Available on Linux, macOS, and Windows 10

Virtual Desktop Infrastructure (VDI)

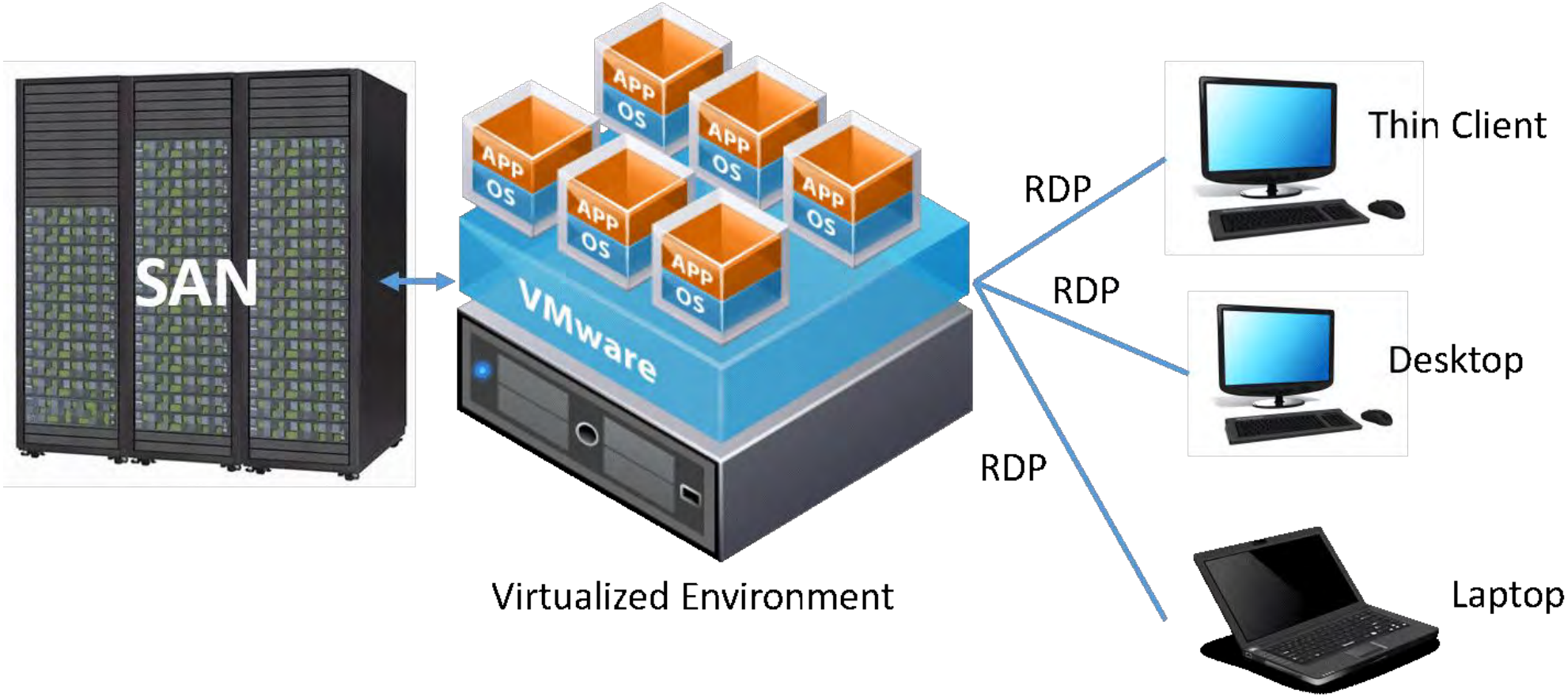
- The hosting of desktop environments on a central server
- Clients connect to the VDI server to live-stream their desktop
- Each desktop runs as a virtual machine (VM) on the server
- The client sends mouse clicks and keyboard strokes to the server
- The server sends a view of the desktop back to the client
- All computing is done on the server in the VM
- Depends on a good network infrastructure

Multiple Virtual Desktops on a PC Example



Virtual Desktop Client Examples

Virtual Desktop Infrastructure Example



Mobile Device Management

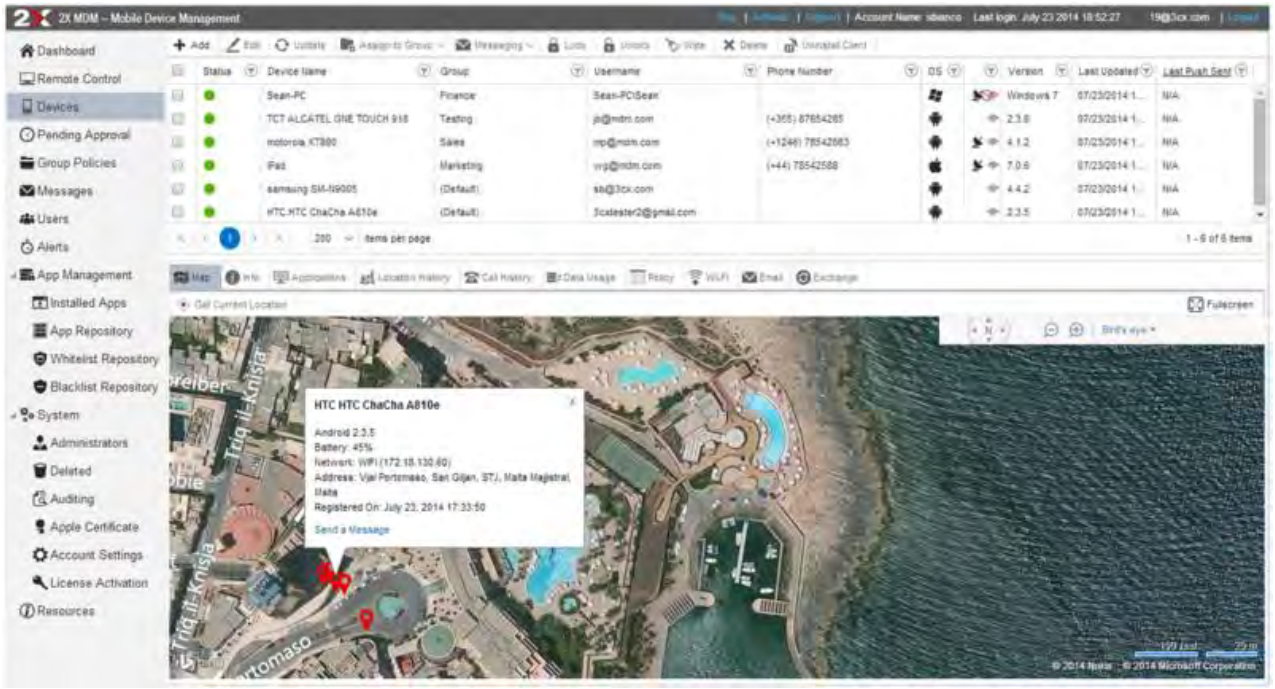
Administration of mobile devices

Typically a third-party product
- Often cloud-based

A user enrolls their device in the system

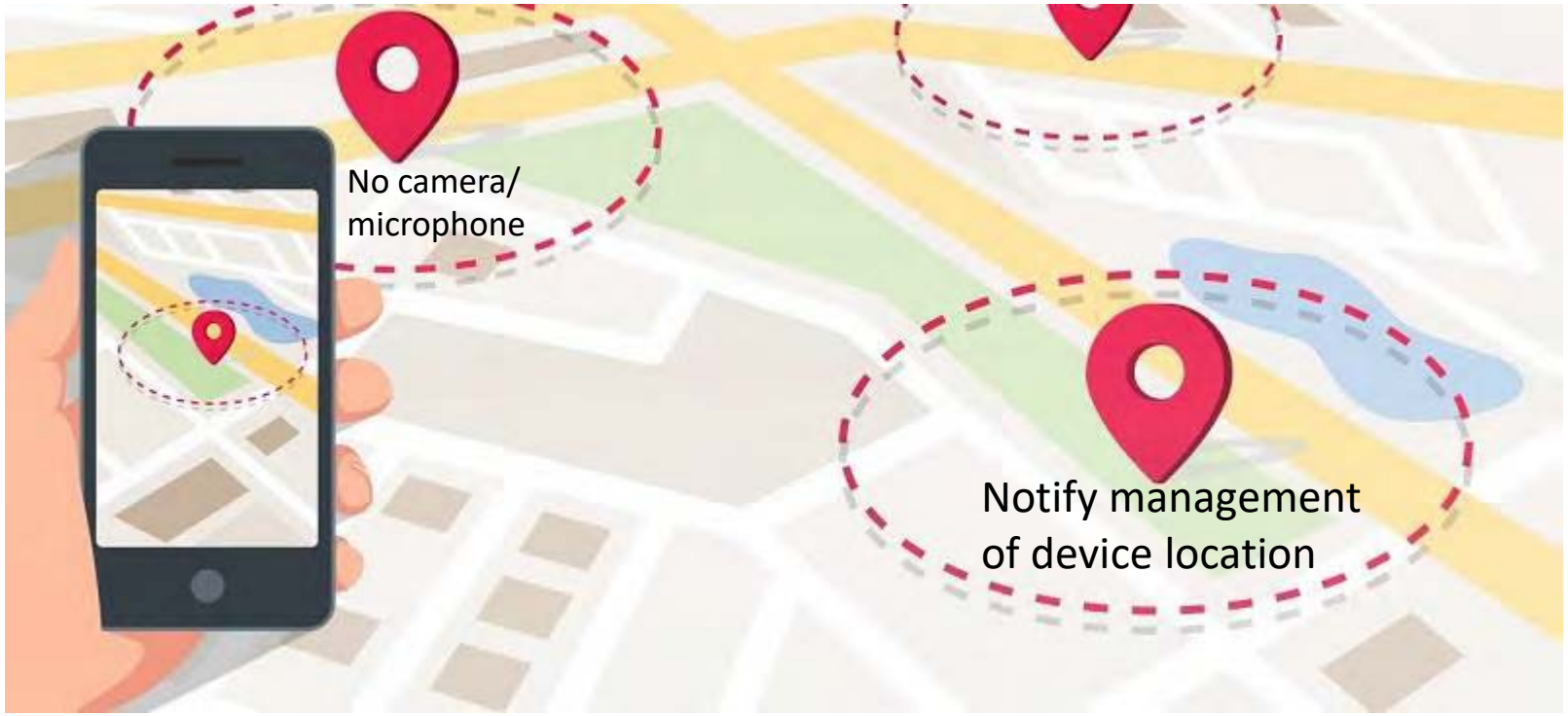
Agent software is installed on the device
- Used to enforce device compliance

IT admins can:
- Push policy, configurations and software to devices
- Remove unauthorized software from devices
- Verify that devices are not rooted, jailbroken, or otherwise out of compliance
- Containerize and separate business from personal data
- Enable geofencing to track devices and allow/disallow hardware features such as camera and microphone in sensitive areas



MDM Capabilities

MDM Geofencing Example



In-Band vs Out-of-Band Management

In-Band management requires you to use the regular production network to remotely administer the servers and devices

- It assumes that the network is intact and functioning
- The security risk is that you are making a highly privileged connection from a remote location
- If not carefully secured, remote access capabilities could be compromised and exploited by an attacker

Out-of-Band management requires that you set up alternate connectivity to the devices

- It assumes that the network is down, and that you need to access the devices to get the network functioning again

Securing Out-of-Band Management

Install a console server that has USB, RS-232, and/or Ethernet connections to the various servers and network devices

Ensure that:

Wake-on-LAN-capable devices, including UPSes, can be started/rebooted from the console server

The console server can automatically fail-over to OOBM, and then fail-back to the primary network

The console server can use multiple access methods including:

- Redundant copper and fiber Ethernet connections
- Built-in high-speed cellular 4G LTE
- Built-in Wi-Fi
- Integrated V.92 dialup modem (for a secure and reliable connection over the POTS network)

Securing Out-of-Band Management (cont'd)

Make sure that the console server has high-level security features for secure access to critical network devices:

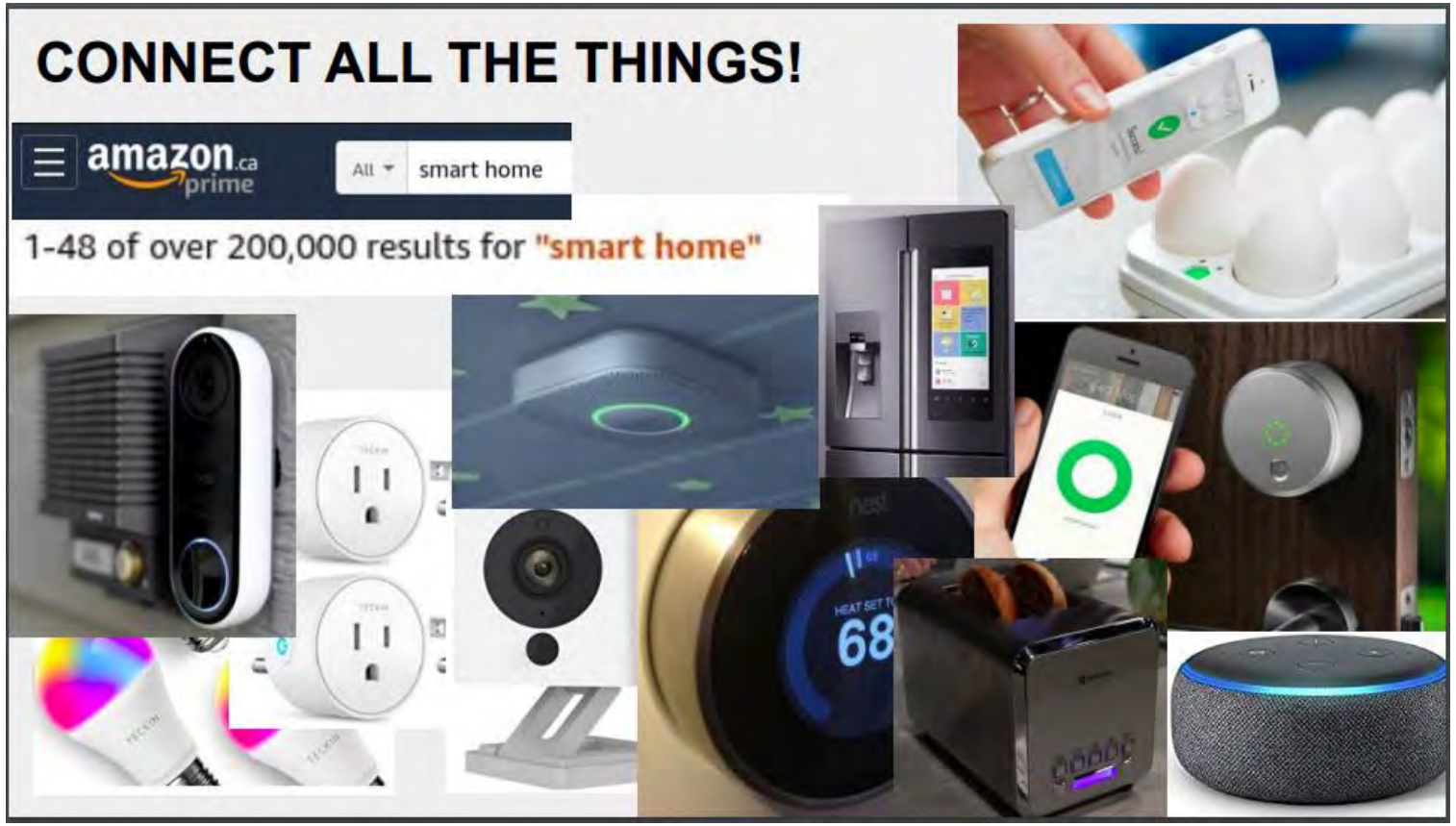
- Strong authentication schemes such as RADIUS, TACACS+, LDAP, Kerberos, MFA to comply with existing network security policies
- Built-in usernames and passwords and support for encryption protocols such as SSH, SSL/TLS, IPSec VPN, SNMPv3, Telnet, and HTTPS for secure management sessions
- Packet filtering to ensure the Console Server can be kept secure from unauthorized access
- Support SLIP and PPP for remote user dial-in

IoT Security

Why Care About IoT Security?

Do you really want an attacker

- running your home?
- watching your baby?
- disrupting your factory floor assembly line?
- using your office router to mine bitcoins?



Baby Monitor Hacking Stories

“A family near London, Ontario, was terrified when their baby monitor suddenly began playing creepy music and a voice told them they were being watched”

“A couple in New York City didn't understand why their 3-year-old was telling them he was afraid of the man in his monitor. Then one night in April they heard the voice for themselves”

“A Kansas mother was putting her son down in the crib when she looked at the baby monitor camera and realized it was following her movements. "Every single hair on my body stood up. I was freaked out,"

Unmanaged IoT Device Examples

Office devices and peripherals	Printers, VoIP phones, smart TV screens and monitors, Bluetooth keyboards, headsets, etc.
Building automation	HVAC systems, security systems, lighting systems, cameras, vending machines, etc.
Personal or consumer devices	Smartphone, smart watch, gaming consoles, Apple TV, Slingbox, digital assistants (Amazon Echo, Google Home, etc.), cars.
Industry-specific devices	Industrial control systems (PLCs, HMIs, robotic arms, etc.), medical devices (patient monitoring systems, mobile imaging systems, infusion pumps, communication badges, etc.), retail (barcode scanners, POS system, loss prevention, etc.), warehouse (inventory systems).
IT infrastructure	Access points, routers, switches, firewalls, baseboard management controllers of servers.

OWASP IoT Top 10 Vulnerabilities

1 Weak, Guessable, or Hardcoded Passwords
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 Insecure Network Services
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 Insecure Ecosystem Interfaces
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

OWASP IoT Top 10 Vulnerabilities (cont'd)

4 Lack of Secure Update Mechanism
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 Use of Insecure or Outdated Components
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6 Insufficient Privacy Protection
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

OWASP IoT Top 10 Vulnerabilities (cont'd)

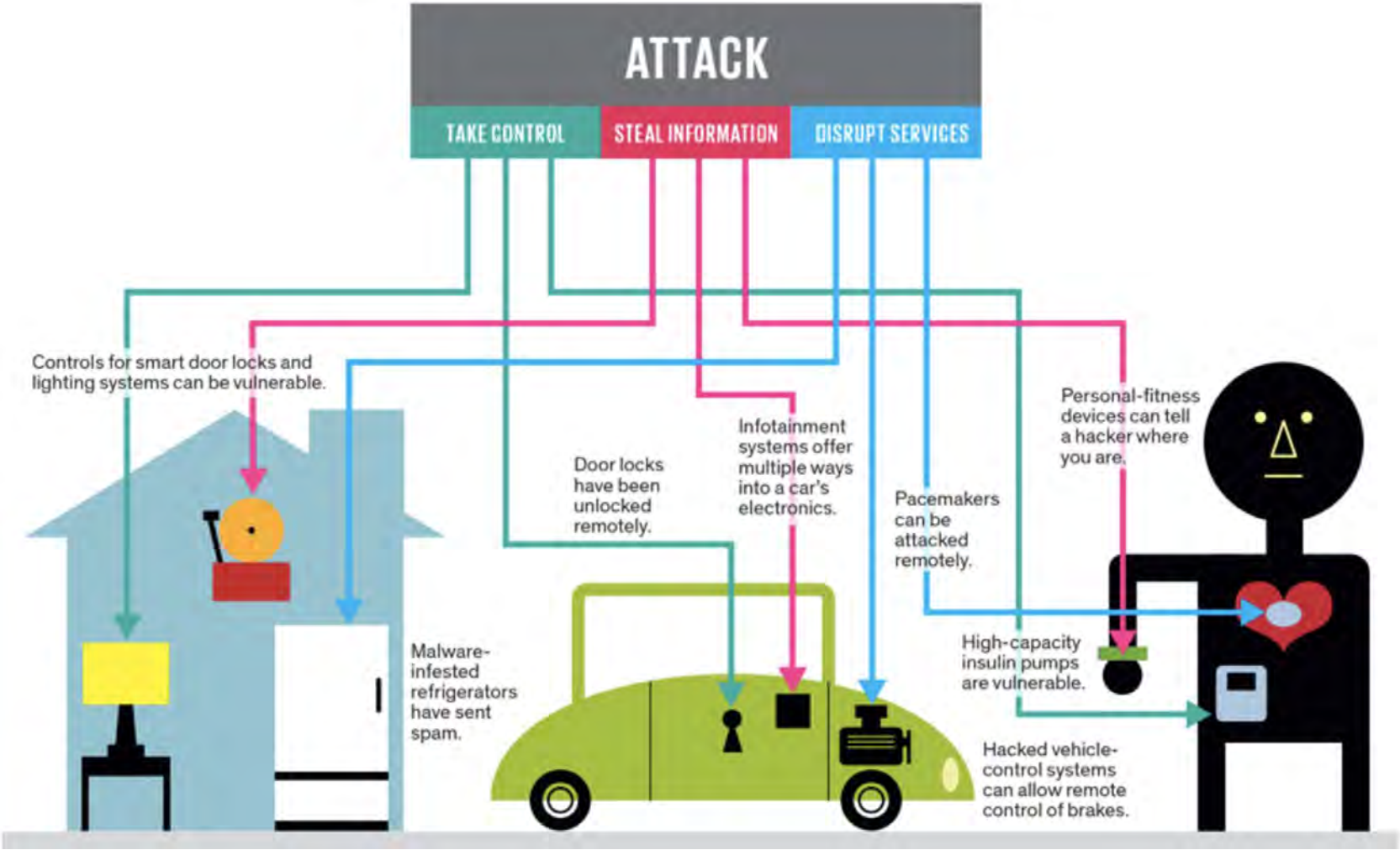
7 Insecure Data Transfer and Storage
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 Lack of Device Management
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 Insecure Default Settings
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 Lack of Physical Hardening
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

IoT Attack Vectors Example



IoT Security Device Best Practices

Approach security as a unified, integrated, holistic system

- Have an IoT security policy!

Disable any services that provide direct remote access/remote control

- Example: built-in HTTP server on cameras/baby monitors

Prefer to connect to a control server/IoT hub, rather than the device itself

- Implement the strongest available authentication mechanism

Disable guest and demo accounts if enabled

Change default passwords

IoT Security Device Best Practices (cont'd)

Implement any existing password lockout feature

Turn off unnecessary ports and vulnerable services

Patch vulnerabilities and update firmware if available

Install regular updates when possible

Protect devices from physical tampering

Ensure that a remotely accessed vehicle has only one identity

IoT Security Network Best Practices

Have a separate network for smart devices

Take care not to connect over insecure networks (like public Wi-Fi)

Only allow trusted IP addresses to access the device from the Internet

Disable telnet (TCP 23)

Disable UPnP ports on routers

IoT Security Network Best Practices (cont'd)

Locate control system networks and devices behind firewalls, and isolate them from the business network

Implement IDS/IPS on the network

Implement end-to-end encryption using PKI when possible

Use VPNs to manage devices and control systems when possible

Monitor traffic on port 48101 as infected devices tend to use this port

Recommendations for Managing IoT in the Enterprise

Assess and inventory your enterprise IoT devices

- You cannot secure things if you don't know they exist
- Complete an inventory of all devices connected to your network
- Use that information to build policies and implement controls to ensure devices are appropriately monitored and secured

Prioritize device classification and protection, and use it to build the appropriate controls

- Use your inventory to understand how and where devices are used, how they drive the business, what critical data they have or activities they perform, and how they may be exploited or manipulated
- This will help ensure your security policies are effectively applied
- Refer to IoT security frameworks from NIST and the Center for Internet Security (CIS) for guidance

http://info.armis.com/rs/645-PDC-047/images/State-Of-Enterprise-IoT-Security-Unmanaged-And-Unsecured.pdf

Recommendations for Managing IoT in the Enterprise (cont'd)

Raise awareness on the growing IoT security risks

- Demonstrate to stakeholders that unmanaged devices are more vulnerable than managed computers
- At the same time IoT devices are not as well protected as managed computers,
- They can't accommodate standard security agents and be easily patched

Anticipate future threats by implementing the appropriate solution(s), providing device visibility, risk assessment, threat detection, and protection specific to unmanaged and IoT devices

http://info.armis.com/rs/645-PDC-047/images/State-Of-Enterprise-IoT-Security-Unmanaged-And-Unsecured.pdf

Physical Security

What is Physical Security?

The protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution

This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism

Goals of Physical Security

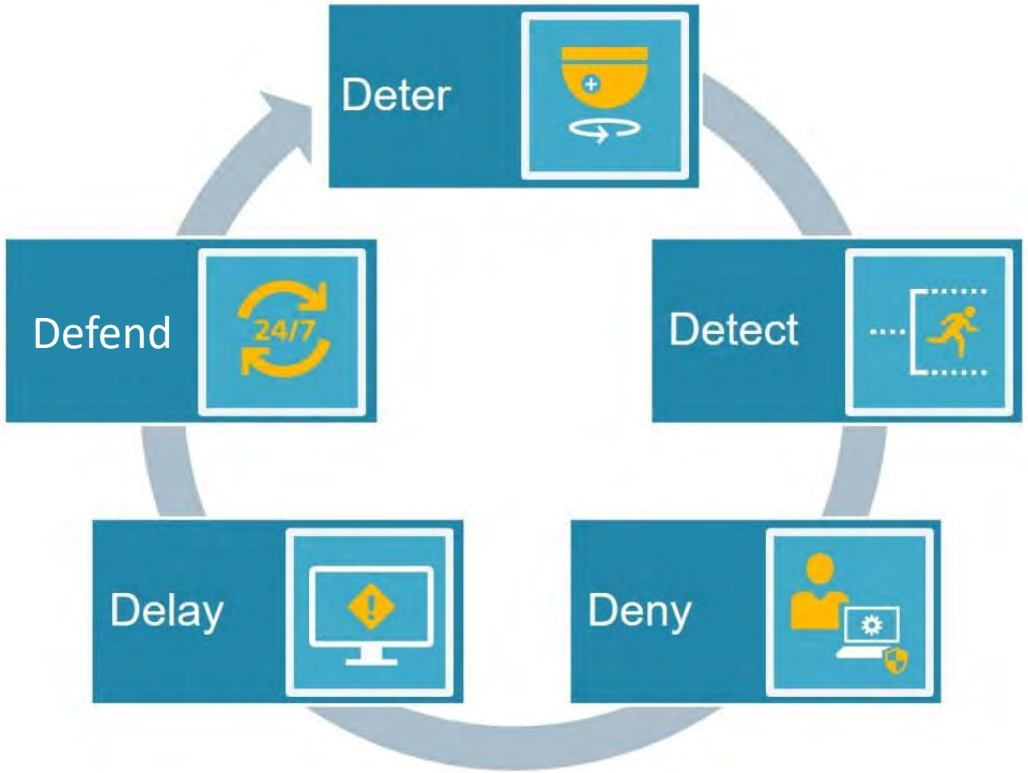
Deter
- Make the property or target unattractive so attackers will go elsewhere

Detect
- If someone penetrates a secure area, make sure they are spotted

Deny
- Allow access to authorized parties, but deny access to others

Delay
- If someone gets in, slow them down

Defend
- Respond to a breach

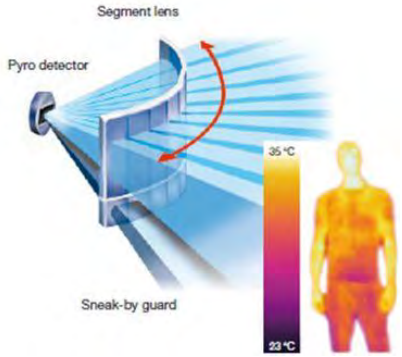


Physical Security Mechanisms

Fencing
Gates
Guards
Cameras
Motion sensors
Lighting
Traffic flow

Doors
Locks
Landscape
Asset tags
Tamper detection
Badge readers

Access control doors
Metal detectors
X-ray scanners
Bollards
Road blockers
CPTED



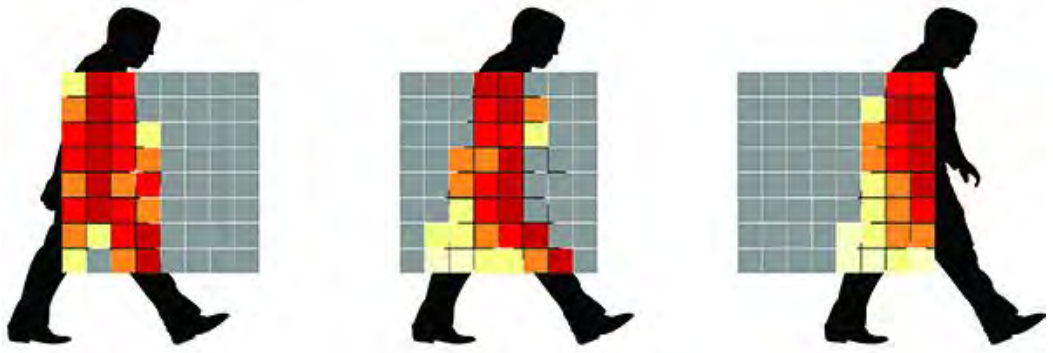
Cameras and Motion Detection

Passive infrared detector

- Most common implementation
- Picks up heat signature of objects within field of view
- Detects changes in the amount of infrared radiation

Thermal camera

- Not really a camera
- Creates a picture composite based on temperature differences between objects in the field of view
- Excellent range; very efficient in detection through smoke, fog, total darkness, or camouflaged objects
- Costly and cannot recognize individuals



Cameras and Motion Detection (cont'd)

Video Motion Detection Camera (VMD)

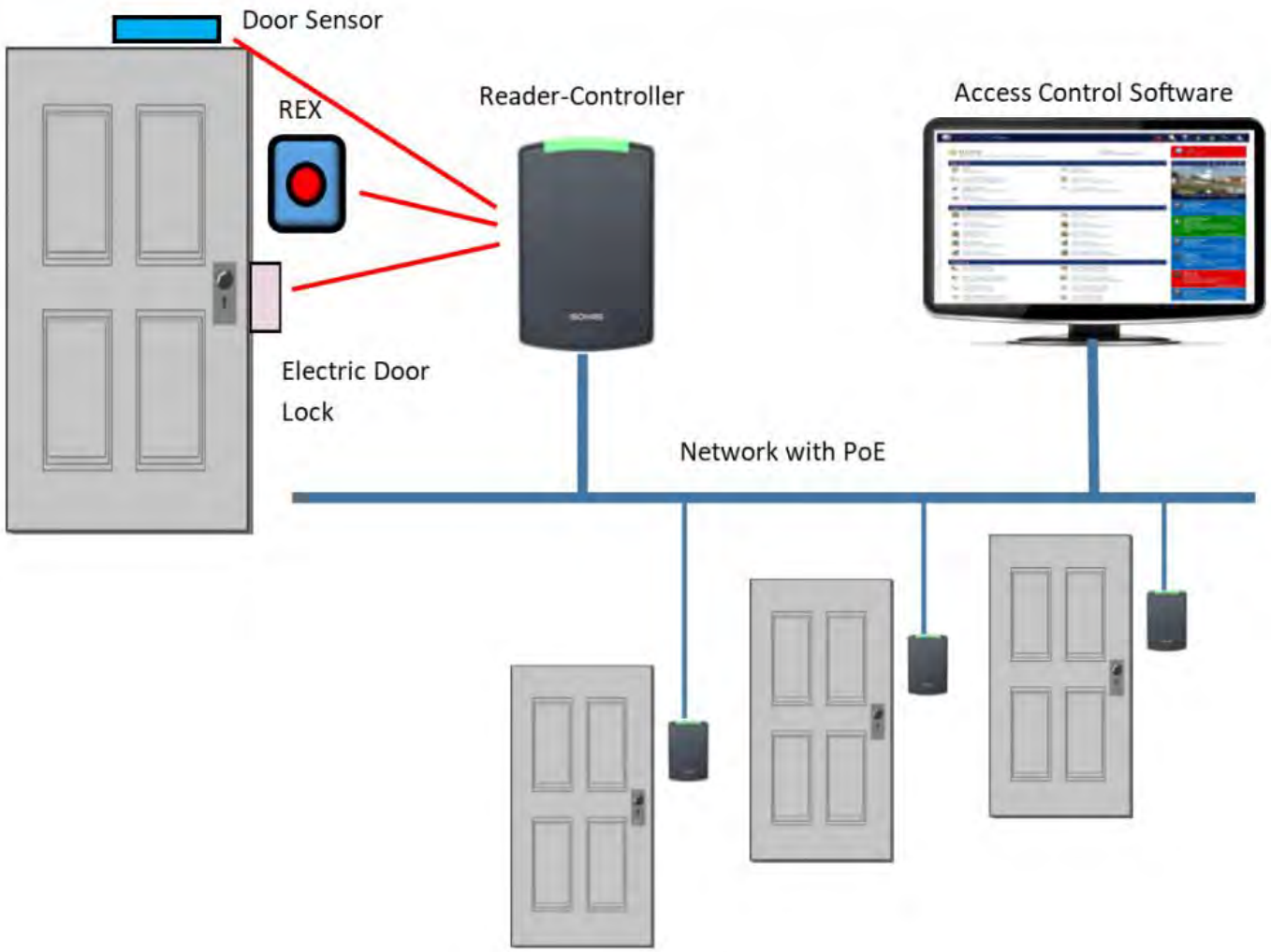
- Combines the function of a security camera with added software analytics
- Examines the image as it is being captured
- VMDs dependent on good light, a high-quality image, and good analytics software
- Inexpensive, but could become expensive if you are trying to cover a large area

Radar

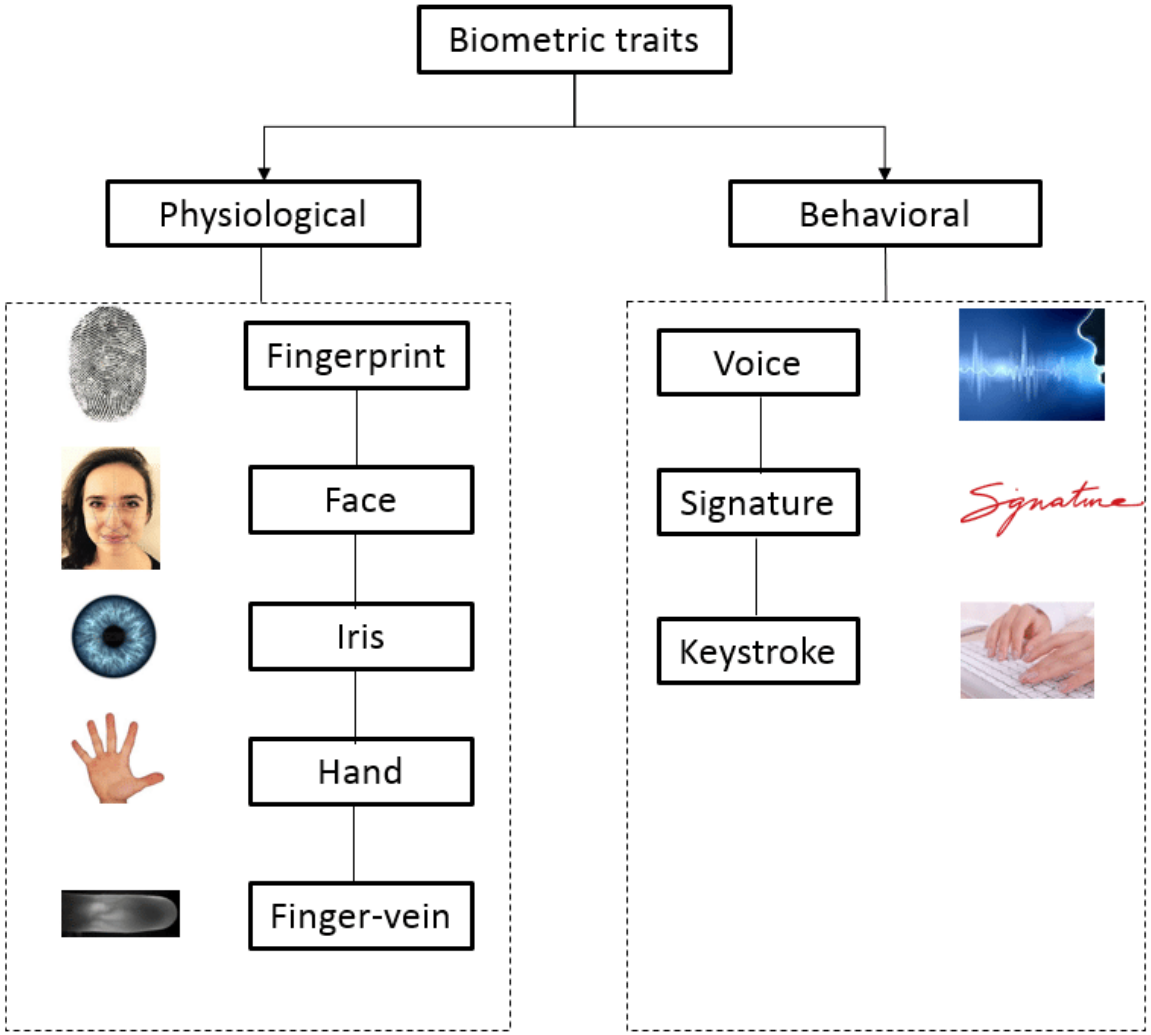
- Works by transmitting radio waves and receiving the same waves bounced off objects in its field of detection
- Doesn't need visible light; can pass through rain, fog, falling snow and smoke
- You can deploy in specific zones
- Cost effective

Crime Prevention Through Environmental Design

Access Control Hardware



Types of Biometric Authentication



Fingerprint		Iris	
Finger Vein		Retina	
Facial		Gait	
Palm Vein		Hand Geometry	
Handwriting		Speech	

Asset Tags

MyAssetTag.com
AlumiGuard® Matte
Anodized Aluminum
Cancel

PROPERTY OF
COMPANY NAME
ADDITIONAL TEXT
T-12345

CUSTOM TEXT
0001
YOUR COMPANY

YOUR TEXT
C051896

Property of
Asset Management In
123456

Security Throughout the Asset Lifecycle

Ensure that no data remains before disposal

Ensure that outside support cannot access private keys or sensitive business data

Track inventory, monitor traffic and behavior, keep patch and antivirus levels up-to-date

Define the business need for the asset
Ensure purchase is properly approved

Ensure image is fully patched and secured before deployment

Track where devices have been deployed. Require end user accountability for assigned devices

Locking Racks and Cabinets

Protect patch panels and devices from tampering or theft

Ensure that airflow is not reduced

Consider where to place the rack UPS

Try to keep the rack out of casual reach

Ensure that spare keys are available in case of emergency

Access Control Vestibule

AKA mantrap

Walking through the entry requires two steps

- Enter the vestibule from the outside
- Enter the inside from the vestibule

The visitor must spend a short moment in the vestibule before they can enter the building

An intruder can be safely contained until law enforcement arrives

Smart Lockers

A storage solution that has integrated technology built into it

- Used by apartment mailrooms to secure package delivery and stop theft
- Companies can also benefit from using smart lockers
- Assets such as equipment, supplies, and documents can be managed and distributed in a controlled manner

Smart lockers track the assets they store (“content surveillance”)

- Passive RFID tags are considered reliable and cost-effective

Users must individually identify themselves before a locker door will open

- Usually by entering an account number, followed by a PIN
- Higher security environments can include swipe cards, smartphone apps, or biometric scans for authentication

Smart Locker Example

Employee Training

70-20-10 Model for Learning:

- Original model created in the 1980's for maximizing learning and development effectiveness
- 70 percent of user knowledge comes from job-related experiences
- 20 percent from interactions with others (social learning, coaching, mentoring, collaborative learning with peers)
- 10 percent from formal educational events

In 2014 the model was updated to 55-25-20