

CompTIA Security+

Lecture 09

SY0-701

Security Infrastructure

By
Dr. Khaled ELMenshawy

Lecture

09

LEARNING OUTCOMES

- Understanding firewalls.
- Understanding Access Control Lists (ACLs)
- Understanding IDS and IPS.
- Understanding Network Appliances.
- Understanding Port Security.
- Understanding how to securing network communications.
- Understanding SD-WAN and SASE.
- Understanding infrastructure considerations and infrastructure controls.

What is Network Infrastructure?

Network Infrastructure; is the separation of network components, which can be achieved either physically or logically.

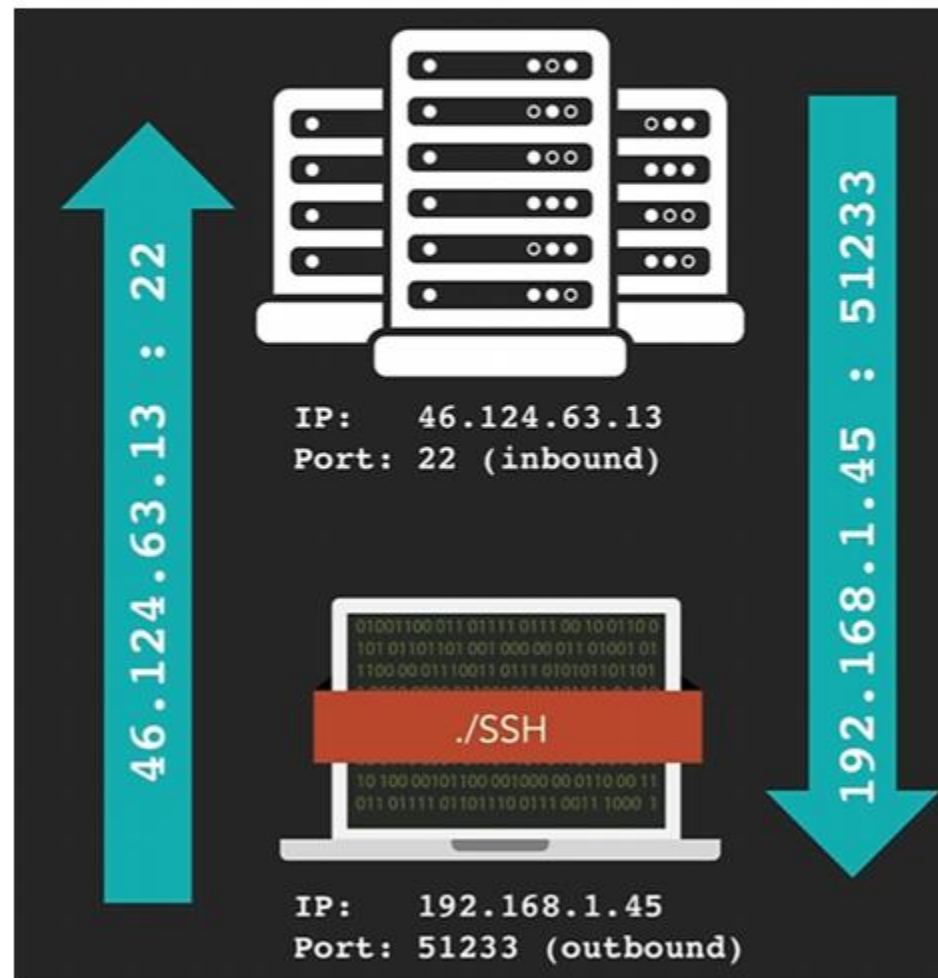


Network Infrastructure

- **Physically separation;** also called *Air Gapping*, is a security measure employed to protect sensitive information. An *Air Gap system is isolated from other networks*, both local and internet.
- **Logically separation;** creating *boundaries within a network that restrict access to certain areas* this is typically achieved through the use of *firewalls, virtual local area networks (VLANs)*, and other network devices that can control traffic based on rules and policies.

Ports:

- **Inbound port;** is used when a computer or server is listening for a connection.
- **Outbound port;** is going to be open by a computer whenever it wants to connect to a given server that is listening.



There is 65535 ports in the network divided as:

- ***Well Known port;*** is *numbered between zero and 1023*. Now these are called well-known ports because they're designated by **IANA**. they're going to be able to assign it to a commonly used port and protocol that everyone can use e.g., https: 443, Telnet : 23.
- ***Registered port;*** is *numbered between 1024 and 49151*. they all have to be used by vendors for their own proprietary protocols e.g., SQL server: 1433, RDP: 3389.
- ***Dynamic and private port;*** is *numbered between 49151 and 65535*. These ports can be used by any application at any time without having to be registered first with IANA.

What is a Protocol?

- **Protocols;** is a defined set of rules and conventions that *governs the communication and data exchange between devices or systems* that specifies the format and the sequence of messages that are going to be used for those communications.
- As Cybersecurity professional the following *should be memorized*:
- Port Number.
 - Protocol used.
 - TCP/UDP support.
 - Basic description.

Port No.	Connection	Name	Description
21	TCP	File Transfer Protocol (FTP)	Used to transfer files from a host to host.
22	TCP	Secure Shell (SSH)	Provide us with secure remote terminal access.
		Secure Copy Protocol (SCP)	Securely copy files between a local host and a remote host or between two remote hosts
		Secure File Transfer Protocol (SFTP)	Uses secure shell encryption to provide a high level of security for sending and receiving file transfers
23	TCP	Teletype Network (Telnet)	Insecure remote control of another machine using text-based environment.
25	TCP	Simple Mail Transfer Protocol (SMTP)	Responsible for sending emails.
53	TCP/UDP	Domain Name System (DNS)	Used to translate domain names into IP addresses
69	UDP	Trivial File Transfer Protocol (TFTP)	Used with network-based operating systems for sending configuration files or network booting of an operating system.

Port No.	Connection	Name	Description
80	TCP	Hypertext Transfer Protocol (HTTP)	Used for retrieving webpages.
88	TCP	Network Authentication Protocol (Kerberos)	Used for authenticating service requests between trusted hosts across an untrusted network.
110	TCP	Post Office Protocol v 3.0 (POP3)	Used for retrieving email from a mail server.
119	TCP	Network News Transfer Protocol (NNTP)	Used for accessing news groups.
135	TCP/UDP	Remote Procedure Call (RPC)	Used to facilitate the communication between different system processes.
137, 138, 139	TCP/UDP	NetBIOS	Used inside of a Windows domain environment to be able to share things like file and printer in a local Windows environment.
143	TCP	Internet Message Access Protocol (IMAP)	Used for retrieving email from a mail server.

Port No.	Connection	Name	Description
161	UDP	Simple Network Management Protocol (SNMP)	Used to manage network devices.
389	TCP	Lightweight Directory Access Protocol (LDAP)	Facilitate directory services.
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)	Provides a secure web communication process.
456, 587	TCP	Simple Mail Transfer Protocol Secure (SMTPS)	Secure SMTP communications to send our emails.
514	UDP	Syslog	Used for sending log messages.
636	TCP	Lightweight Directory Access Protocol secure (LDAPS)	Used for LDAP Secure over an SSL/TLS connection that is encrypted.
993	TCP	Internet Message Access Protocol over SSL/TLS (IMAPS)	The secure version of IMAP.

Port No.	Connection	Name	Description
995	TCP	Post Office Protocol v 3.0 over SSL/TLS (POP3S)	The secure version of POP3.
1433	TCP	Microsoft SQL server	Facilitate communication with SQL Server.
1645, 1646	TCP	Remote Authentication Dial-In User Service (RADIUS)	Provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
1812, 1813	UDP		
3389	TCP	Remote Desktop Protocol (RDP)	Enables remote desktop access.

What is Firewall?

Firewall; is a network security device that *monitors incoming and outgoing network traffic* and decides whether to allow or block specific traffic *based on a defined set of security rules*.

Firewalls can be hardware-based appliances or specialized software installed on a client or server to perform this function.



Types of firewall:

- Packet Filtering Firewalls; are Layer 4 firewalls, they *check packet header based on IP address and port number*. these are faster firewalls but *can not prevent IP spoofing, packet fragmentation attacks, or attacks against the TCP handshake*.
- Stateful Firewalls; are *tracking the state of all inbound and outbound connections and requests* of the network. (MITM attack | must be updated regularly)
- Kernel Proxy Firewalls; A firewall that is integrated into an operating system's core, *minimal impact to performance on our network*, even while conducting its *full inspection of the packet at every single layer*.

- **Proxy Firewalls**; are placed between an internal or external connection in a network, and they are *going to make connections on behalf of your other endpoints*.
- **Circuit level** analyzes (TCP) handshaking between packets to identify legitimate traffic and block unauthorized access attempts (*Layer 5 OSI model*).
 - **Application level** *examines the content of the packets (deep packet analysis)* and work in *layer 7 OSI model*, thus, *application-level gateways have larger impact to the performance and efficiency of the firewalls*. For this reason, most application-level proxies are going to be best positioned inside of the network when they are *located as closely as possible to the application server* that we are trying to protect.

- **Next-Generation Firewall**; is made to overcome the limitation of stateful firewall by being aware of application and their behaviors.
- **Unified Threat Management Firewall (UTM)**; provides the ability to *conduct numerous security functions in a single device* such as firewalls, intrusion prevention systems (IPS), gateway antivirus and antispam, virtual private network concentration, content filtering, load balancing, and data loss prevention .

The largest issue with using a UTM device is that they become a *single point of failure* in the network. i.e., *if we lose that device, we lose our entire security stack*.

- **Web Application Firewall**; is going to be *focused on the inspection of HTTP / HTTPS traffic* to prevent common attacks against web applications, including things like cross-site scripting and SQL Injections.
- **Inline configuration**; the device is going to be *placed between the network firewall and the web servers*.
 - **Out-of-band configuration**; the device is *receiving a copy of all the traffic that was destined for your web server* using a mirrored or SPAN port of a switch. In this case it *works like an intrusion detection system (IDS)* because it sees all the information and it can then alert on it but can not block it.

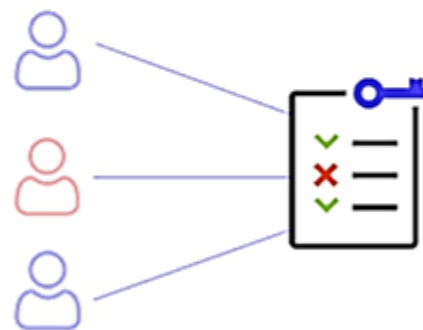
- **Web Application Firewall**; is going to be *focused on the inspection of HTTP / HTTPS traffic* to prevent common attacks against web applications, including things like cross-site scripting and SQL Injections.
- **Inline configuration**; the device is going to be *placed between the network firewall and the web servers*.
 - **Out-of-band configuration**; the device is *receiving a copy of all the traffic that was destined for your web server* using a mirrored or SPAN port of a switch. In this case it *works like an intrusion detection system (IDS)* because it sees all the information and it can then alert on it but can not block it.

What is Access Control Lists (ACLs)?

Access Control Lists (ACLs); is made up of rules that either allow or deny access to a computer environment.

They are *used to filter traffic in and out of a specific device*. Those devices can be network devices that act as network gateways or endpoint devices that users access directly.

Access Control List

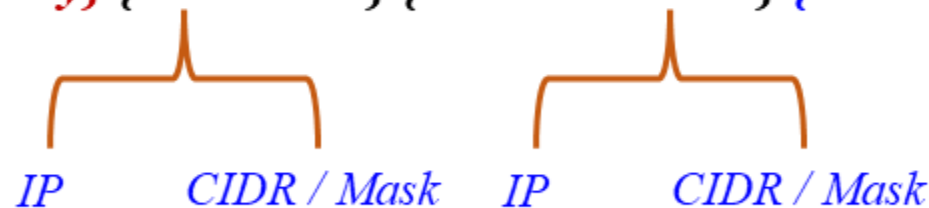


- Configuring ACLs on firewalls is done by using either a *web-based interface* or a *text-based command line interface*.
- ***When configuring ACLs***, the *order in which they are listed is always important* because it will specify the order of the actions that are taken on a particular piece of traffic. *Actions will always be performed in a top-down manner inside of an access control list*. The traffic *will first be compared against the first rule, and then if it matches the condition, the action will be applied, and it will no longer perform the rest of the ACL*. For this reason, we always use the specific rules at the top of the list and then the more generic rules towards the bottom of the list to give us the best levels of protection.

- Access control list rules are going to be made up of some key pieces of information, including the *type of traffic*, the *source of traffic*, the *destination of the traffic*, and the *action that should be taken against that traffic*.

General Form of ACLs command

{ACL Name or Number} {Outbound | Inbound} {Permit | Deny} {Source IP} {Destination IP} {Port No.}



*Access list **outbound** **deny** 0.0.0.0/0 0.0.0.0/0 **port 23***

What is IDS and IPS?

IDS; Intrusion Detection System is a network security tool that *monitors network traffic and devices for malicious activity*, suspicious activity or security policy violations *and alerts and logs* when such activity is discovered.

IPS; Intrusion Prevention System is a network security tool (which can be a hardware device or software) that continuously *monitors a network for malicious activity* and *takes action to prevent, alert, and log it*, including reporting, blocking, or dropping it, when it does occur.

Types of IDS:

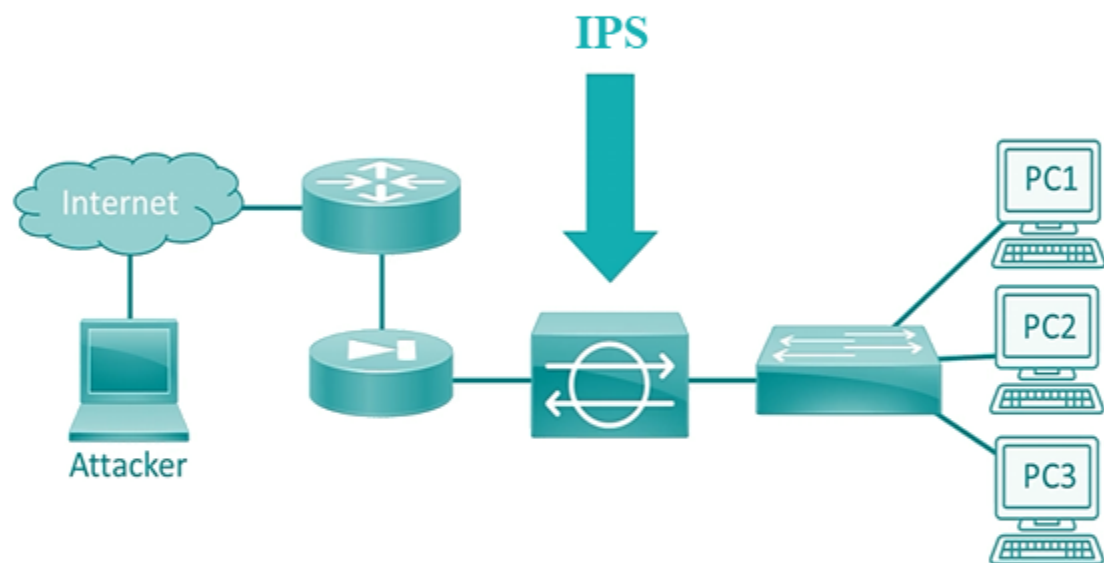
- Network Intrusion Detection Systems (NIDS); are *detecting unauthorized network access or attacks*. These systems are designed to verify, categorize, and report on a threat.
- Host Intrusion Detection Systems (HIDS); are *looking for suspicious network traffic going to or from a single server or endpoint*. It is a piece of software installed on a server or endpoint.
- Wireless Intrusion Detection Systems (WIDS); are *detecting attempts to cause a denial of service on the wireless network*, such as flooding authentication requests.

Intrusion detection systems operate either using:

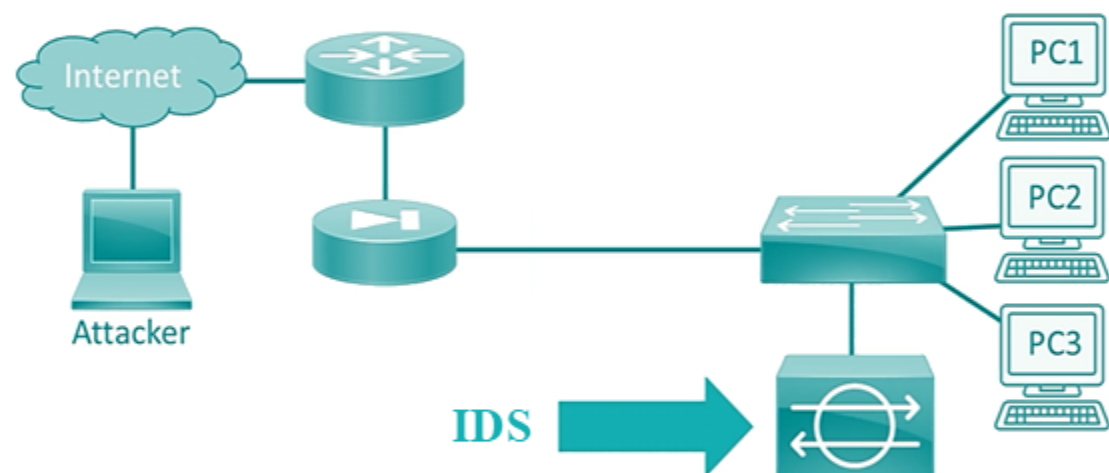
- **Signature-based IDSs**; are *analyzing traffic based on defined signatures*, and they can only recognize attacks *based on the previously identified attacks* that exist inside of its database.
 - **Pattern-matching**; is going to *focus on a specific pattern of steps* that are being recognized during an attack (NIDS and WIDS).
 - **Stateful-matching**; is going to *focus on a known baseline of a system* and reporting any changes to that state (HIDS).

➤ Anomaly-based IDSs; are going to *analyze traffic and compare it to a normal baseline of traffic* to determine whether there is a threat that is occurring. This is known as behavioral-based detection because it reports on anything outside of the normally-expected behaviors, but this can also *result in a higher rate of false positives*.

- *Statistical.*
- *Protocol.*
- *Traffic.*
- *Rule or heuristic.*
- *Application-based.*



IPS is placed right near the border of the network, right behind your firewall.



IDS is placed right through a mirrored port of the backbone switch.

What is Network Appliance?

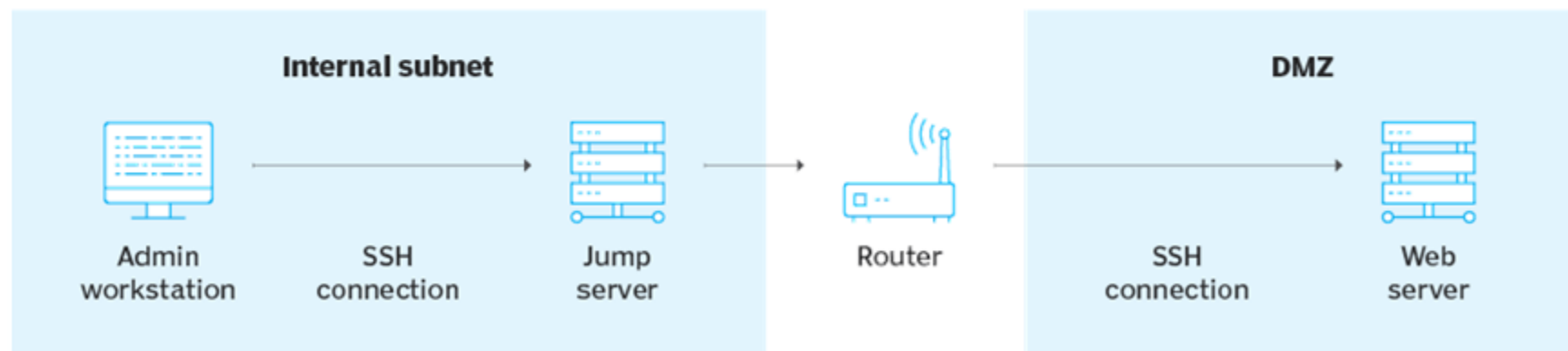
Network Appliance; is a *dedicated hardware device with pre-installed software that is designed to provide specific networking services* like security, data storage, or server functions inside of a network infrastructure.

There are common four different kinds of Network Appliances:

- Load balancers.
- Proxy servers.
- Sensors.
- Jump servers.

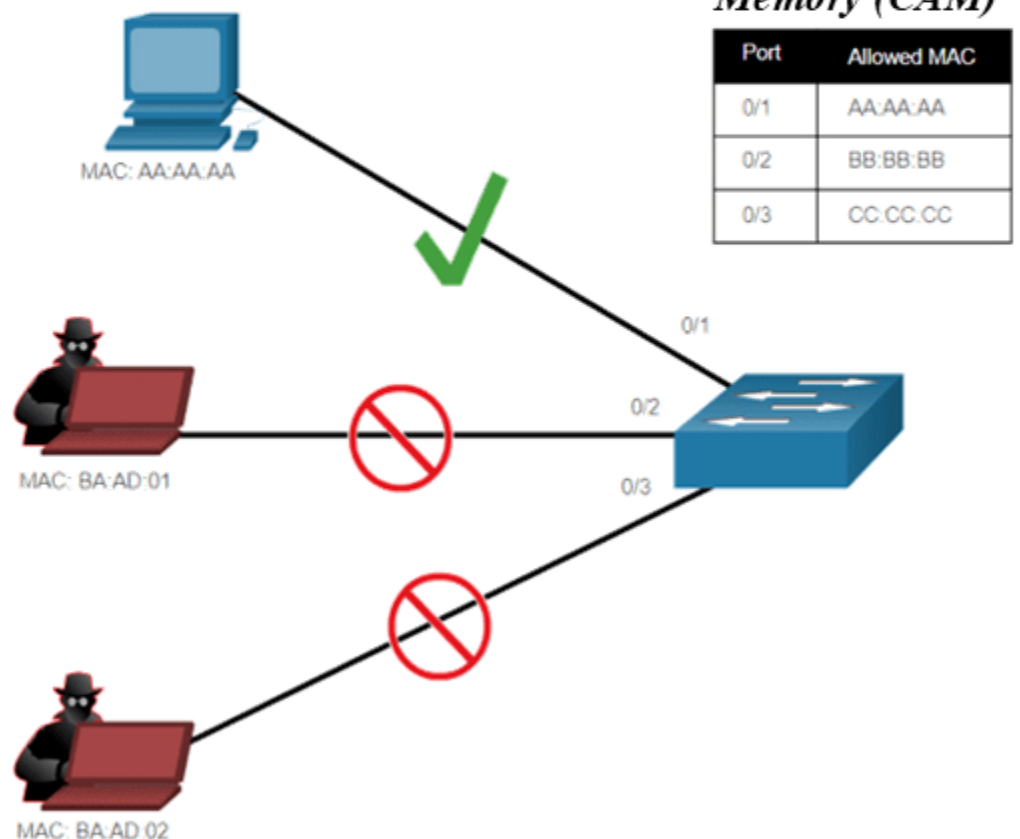
- **Load balancers;** are designed to *distribute the network or application traffic across multiple servers*. This distribution enhances the efficiency of server use and it helps to prevent any single device from being overwhelmed by the users' demands.
- **Application delivery controller (ADC);** is the advanced version of a load balancer which *perform load balancing between application servers and includes functions like SSL termination, HTTP compression and content caching*.
- **Proxy servers;** acts as an *intermediary between a client and a server* to provide various functions like content caching, request filtering, and login management to improve the efficiency and control access to our resources within a given network. Also, it offer authentication protocols, secure tunnel, and routing traffic.

- **Network sensors;** are designed to *monitor, detect, and analyze traffic and data flow across the network in order to identify any unusual activities*, potential security breaches, performance issues, or other types of operational inefficiencies.
- **Jump servers;** is a dedicated *gateway* used by system administrators to *securely access devices located in different security zones within the network*. Jump servers are hardened, monitored and don't store any valuable information.



What is Port Security?

Port Security; is a common security feature found on network switches that allows administrators to restrict which devices can connect to a specific port based on their network interface card's MAC address. Port security mitigate MAC flooding attack which floods the switch with MACs converting the switch to act as a HUB.



- Stopping MAC flooding and MAC spoofing by using 802.1x authentication (EAP) which utilize other mechanisms to do the actual authentication process like using RADIUS or TACACS+. For 802.1x authentication to work, it is going to require the use of three different roles:
- ***The supplicant;*** is the *device or the user that's requesting access to the network.*
 - ***The authenticator;*** is the *device through which the supplicant is attempting to access the network*, (e.g., network switch, a wireless access point, etc.).
 - ***Authentication service;*** is the *centralized device that performs the authentication*, and this is usually going to be configured as a RADIUS or TACACS+ server.

Extensive Authentication Protocol (EAP):

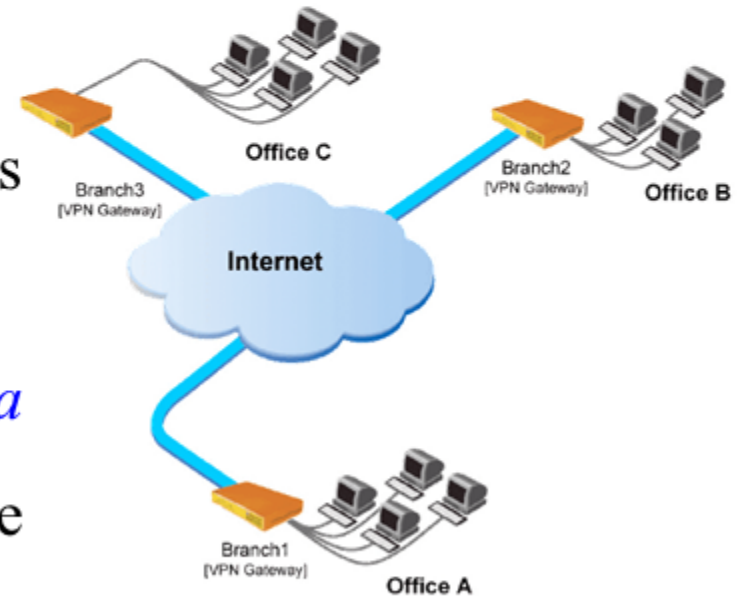
- **EAP-MD5**; is *one-way authentication process utilizes simple passwords*. Ensure using a long, strong, and complex password in order to maintain the security of the system.
- **EAP-TLS**; is *using public key infrastructure with a digital certificate* being installed on both the client and the server as a form of authentication.
- **EAP-TTLS**; is *requiring a digital certificate on the server, but not on the client*. Instead, the *client is going to use a password* for its part of the authentication process, which makes it a little bit more secure than the traditional EAP-MD5.

- **EAP- FAST**; FAST stands for the flexible authentication via secure tunneling, and this *uses a protected access credential instead of a certificate* to establish mutual authentication between two devices.
- **PEAP**; supports mutual authentication by *using a server certificate and your Microsoft Active Directory database* in order to authenticate a password from your given client.
- **LEAP**; developed by Cisco, and this stands for the *Lightweight EAP*. It is a proprietary protocol for Cisco devices so, it will work only on Cisco based devices.

Securing Network Communications

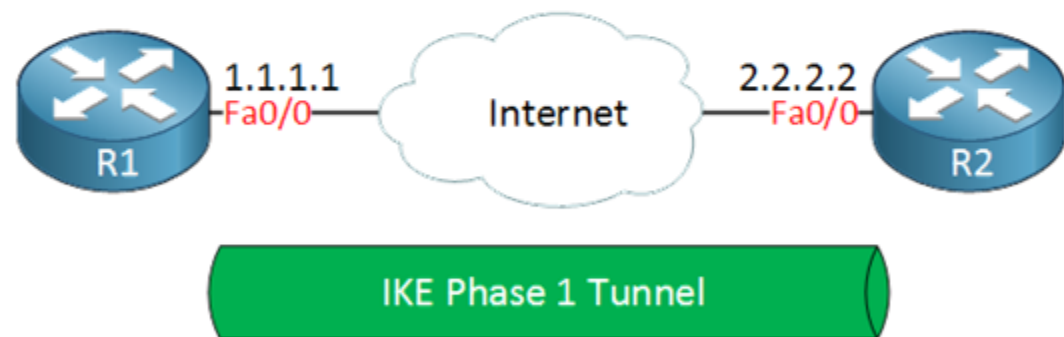
➤ **Virtual Private Network (VPN);** is used to *extend a private network across a public network* to allow users to securely send and receive data across a shared or public network.

- **Site to Site VPN;** used to interconnect two sites and provide an inexpensive alternative to a dedicated leased line.
- **Client to Site VPN;** used to connect individual devices directly to the organization's network
- **Clientless;** used to *secure remote access VPN tunnels using a web browser*, and it doesn't require any software or hardware clients to be configured.



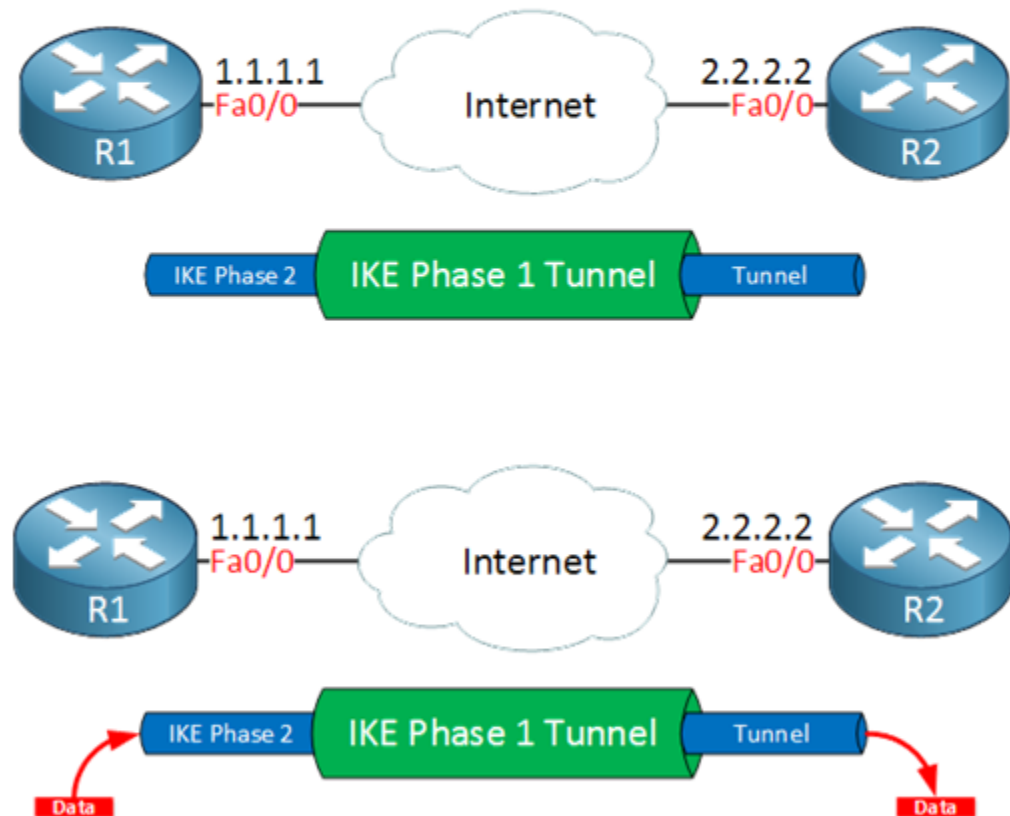
There are five main steps in the process of establishing and using a secure VPN tunnel when you're using IPSec:

- 1. Request to start a key exchange;* Is the first step in IPSec / VPN connection is to request key exchange.
- 2. Internet Key Exchange IKE Phase 1;* two peers will negotiate about the encryption, authentication, hashing. In this phase, an Internet Security Association and Key Management Protocol (ISAKMP) session is established.



3. ***IKE Phase 2***; The IKE phase 1 tunnel is only used for management traffic. We use this tunnel as a secure method to establish the second secure tunnel called the *IKE phase 2 tunnel* or *IPsec tunnel* and for management traffic like keepalives.

Once IKE phase 2 is completed, we have an IKE phase 2 tunnel (or IPsec tunnel) that we can use to protect our user data. This user data will be sent through the IKE phase 2 tunnel.



4. **Data Transfer**; is protecting user data by sending it through the IKE phase 2 tunnel.
5. **VPN Termination**; when there is no user data to protect then the IPsec tunnel will be terminated after awhile.

Original IP Packet



AH Tunnel Mode



ESP Transport Mode



What is SD-WAN and SASE?

SD-WAN; Software-Defined Wide Area Network, or SD-WAN is a *virtualized approach to managing and optimizing wide area network connections to effectively route traffic between remote sites*, data centers, and cloud environments.

SASE; Secure Access Service Edge or SASE is used to *consolidate numerous networking and security functions into a single cloud-native service* to ensure that secure and seamless access for end users can be achieved regardless of their actual physical location.

- **Placement of devices;** including things like your routers, your switches, and access points can greatly influence both the performance and security of entire network. *The proper placement will ensure optimal data flow minimizes latency, and it provides a robust defense against potential security breaches.*
- **Security zones and screened subnets;** security zone is a *distinct segment within a network, often created by logically isolating the segment using a firewall or other security device.* a screened subnet can also be created to act as a *protective layer or buffer zone between an organization's internal network and an untrusted external network* like the Internet.

- **Attack surface;** is *the sum of all the potential vulnerabilities and risk points inside of a system*, a network, or an application.
- **Connectivity methods;** refers to *how different components of a network are going to communicate with each other and with our external networks*.
- **Device attributes;** referring to whether or not the *device is considered to be active or passive, and if it is going to be placed in line or as a tap or monitor inside of the network architecture*.
- **Failure mode;** will determine *how a device behaves when it encounters an error or malfunction*. There are two primary failure modes that we can utilize, and these are known as *fail-open* or *fail-closed*.

What is Control?

Control; is a *measure or safeguard that is implemented to mitigate potential risks and to protect an organization's assets*. Selecting effective controls ensures that we can prevent breaches and to minimize vulnerabilities while ensuring that our resources are being used efficiently.

Selecting effective controls:

Key principles; consider the key principles of *least privilege*, *defense in depth*, *utilizing a risk-based approach*, *conducting lifecycle management*, and *focusing on open design principles* to secure our infrastructure.

- **Least privilege;** a user or system should *only have the necessary access rights* that they need to perform their duties.
- **Defense in depth;** emphasizes the *use of multiple layers of security to ensure that if one control fails, that our other controls will still be ready to stop a potential threat* from successfully exploiting our infrastructure.

- **Risk-based approach;** the *prioritization of controls based on the potential risks and vulnerabilities that are specific to the organization's infrastructure.*
- **Lifecycle management;** regularly *reviewing, updating, and retiring our controls* that align with the always changing threat landscape that we're experiencing.
- **Open design principles;** is focused on *creating transparency and accountability* by ensuring that our infrastructure and our controls undergo rigorous testing and scrutiny to ensure they're effective and being implemented securely.

Steps to Select effective controls:

- ***Assessing the current state of the security***; is evaluating the current state of security and the threats and vulnerabilities that are specific to the organization.
- ***Conducting gap analysis***; is evaluating the requirements that you should need to achieve the desire security measure from the current state of security.
- ***Set clear objectives***; is determining the purposes that you want to cover such as securing data, enhance network security, etc., this is vey important for choosing right controls.

- ***Benchmarking***; is comparing the organization's processes, performance, and security metrics against the industry's best practices.
- ***Conducting cost-benefit analysis***; the chosen controls need to be cost effective. So, it is important to find the right balance between the level of security that you want to achieve versus the amount of financial and other resources that are going to have to achieve that level of security.

- *Stakeholder involving*; all the selection processes should be monitored by the stakeholders for improvement.
- *Create monitoring and feedback loops* ; to ensure that the chosen controls remain effective over time.

