
Networkforyou
Welcome
To
Network for you
Network security design
Networkforyou

Network security design:

- In campus networks, endpoints such as mobile devices and laptops are extremely vulnerable to security threats such as malware and ransomware, and they can become infected through various means, such as phishing email, malicious websites, and infected applications.
- For this reason, a solid network security design protects the endpoints from these types of security threats and enforces endpoint network access control by validating the identities of end users to determine who and what they are allowed to access in the network before they are granted access.
- Cisco Cyber Threat Defense (CTD) provides a Cisco-validated solution of best-in-class tools that helps you detect and mitigate advanced threats. Through CTD, security analysts gain visibility and control over advanced threats.

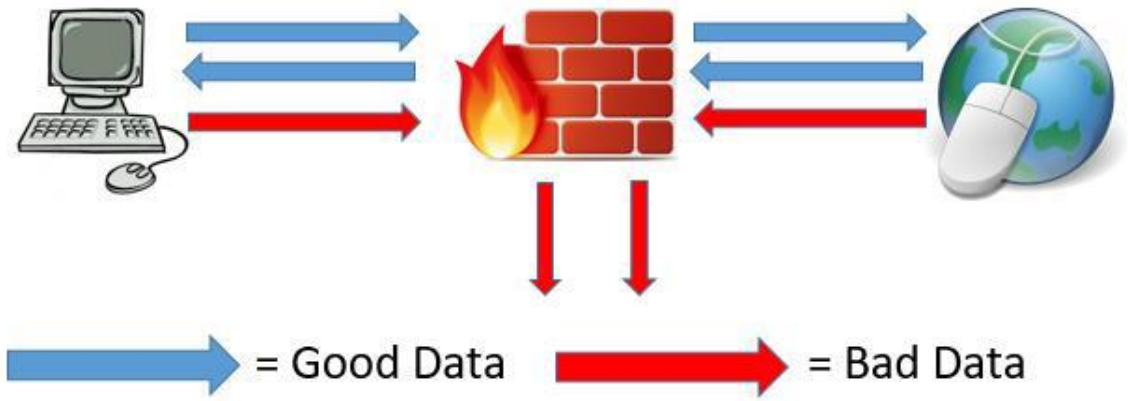
Endpoint Security:

- Connected devices such as desktops, laptops, PCs, mobile devices, smart Phones are endpoints or end device.
- Connected devices such as iPad, tablets and printers are endpoints or end device.
- Three endpoint security products acted independently provide endpoint protection.
- **Personal Firewalls, Antivirus Software, & Antispyware Software installed on endpoint.**
- These three security products defend Various Malware, Spyware and malicious traffic.
- **ESA (Email Security Appliance) & WSA (Web Security Appliance)** provide great solution designed to protect corporate users against threats.
- **The Cisco Email Security Appliance is an email security gateway product. It is designed to detect and block a wide variety of email-borne threats, such as malware, spam and phishing attempts.**
- **Cisco WSA (web Security Appliance) scans all traffic, ports, and protocols to detect and block spyware "phone-home" communications with the integrated Layer 4 traffic monitor. Based on this scanning, it identifies infected clients to help stop malware that attempts to bypass classic web security solutions.**
- **Personal firewalls, antivirus, antispyware & antimalware** can be used mitigate endpoint.
- **Antivirus program is installed on endpoint device to prevent & remove malicious software.**
- Most antivirus software uses signature-based detection and behavioral-based detection.
- Malware, including Trojans, spyware, worms, adware, ransomware, & viruses to protect.

- AMP (Advanced Malware Protection) for Endpoints provides advanced malware protection for many operating systems.
- AMP for endpoints is an intelligent, enterprise-class advanced malware analysis solution.
- AMP protection solution blocks malicious network connections based on IP reputation.
- Personal Firewall is software applications can install on enduser machines to protect them.
- Personal Firewalls control host only and the traffic arriving at and leaving individual hosts.
- Personal Firewalls have been integrated into most modern Operating Systems now a days.
- Personal Firewalls have the ability to permit and deny the traffic based on the application.
- It has ability to define policies for different classes of network such as work, home & public.
- There are several solutions to provide hardware and software encryption of endpoint data.
- Apply, locally encrypt the disk drive with a strong encryption algorithm to protect endpoint.
- The encryption protects the confidential data from unauthorized access in every endpoint.
- The built-in MAC OS X Disk Utility enables to create secure disk images by encrypting files.
- BitLocker Full disk encryption feature included in several Windows operating systems OS.
- Other software such as TrueCrypt free encryption tool for Windows, Mac, & Linux systems.
- AMP, Cisco Threat Grid, Cisco AnyConnect, Cisco Umbrella, WSA, ESA, NGIPS, NGFW, FMC
- Cisco Stealth watch, and Cisco Identity Services Engine ISE etc to use for endpoint security.

Firewall Technologies:

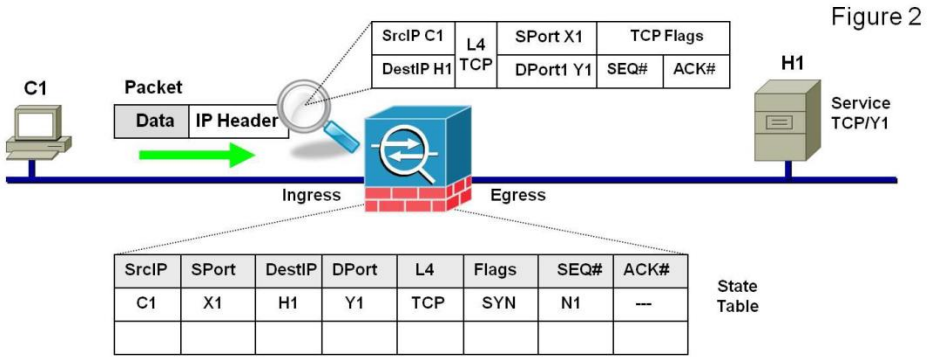
- The word firewall commonly describes a system or device or Software.
- Firewall is placed between a trusted network and an untrusted network.
- A firewall is security devices used to stop or mitigate unauthorized access.
- The only traffic allowed on the network is defined via the firewall policies.
- It grants or rejects access to traffic flows between untrusted & trusted zone.
- A firewall monitors and checks incoming and outgoing network related traffic.
- It decides to allow or block specific traffic based on defined set of security rules.
- A firewall can be hardware, software, or both or can be Cloud-based or Virtual.
- The first generation of firewall technology consisted of packet filters techniques.
- The second generation of firewall started with application layers technologies.
- Firewalls are relied upon to secure home and corporate networks from any attacks.

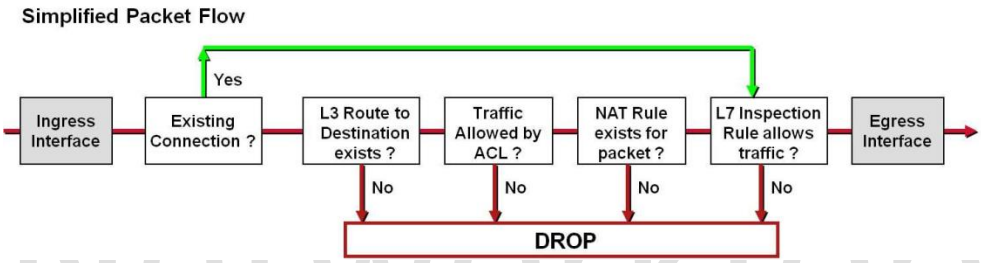


Stateful Firewall:

- It maintains the state of connection when packet is travelling for the appliance.
- State Full Firewall maintains the state of connection in the state table of Firewall.
- After adding information in state table, it forwards the packet to the destination.
- When it receives the reply-packet, it matches the packet information to state-table.
- If Firewall receive the reply packet if match packet is accepted otherwise drop.

Figure 2

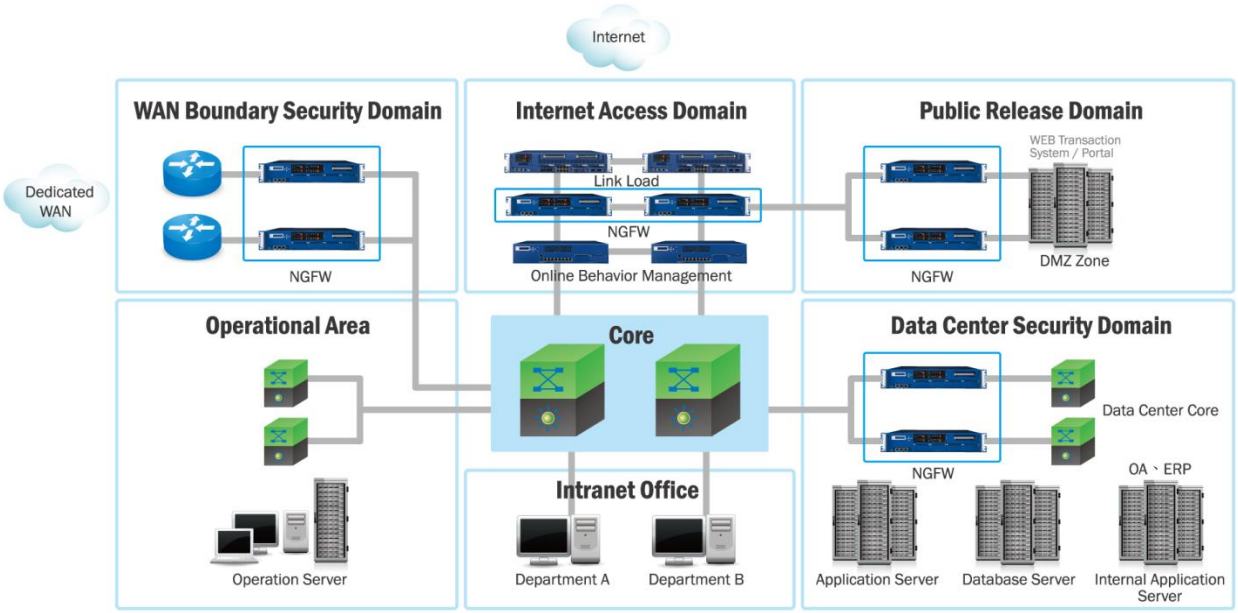




Next-Generation Firewall (NGFW):

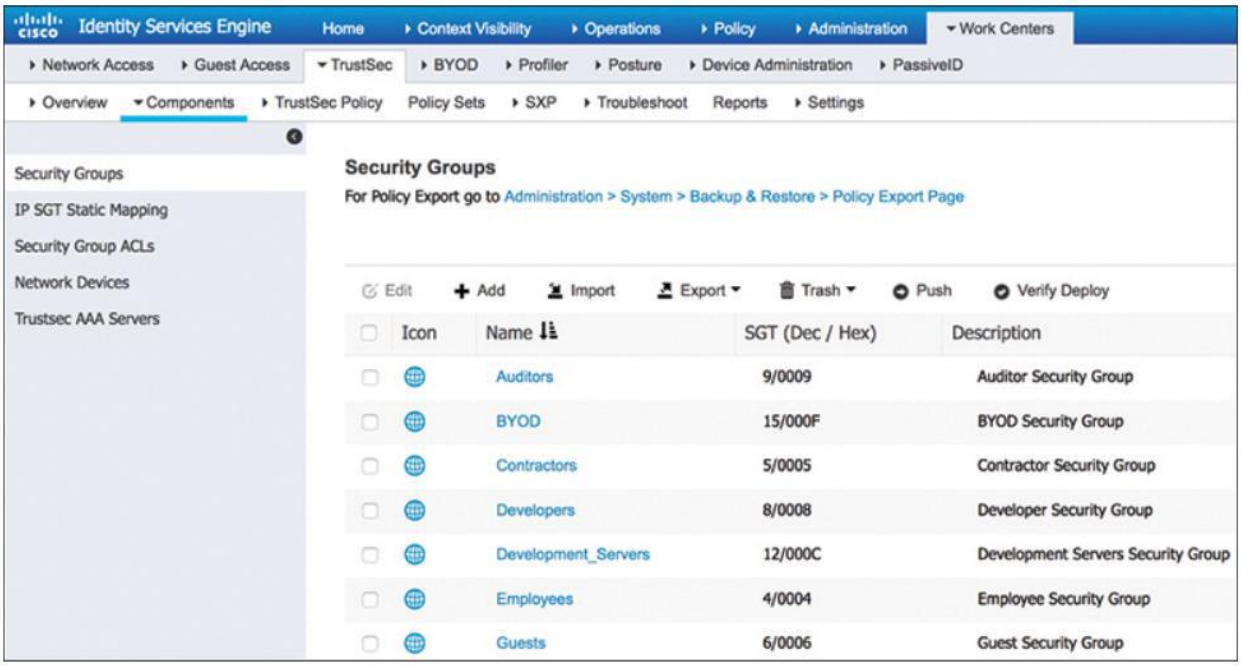
- While a traditional firewall typically provides stateful inspection of incoming and outgoing network traffic, a next-generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud-delivered threat intelligence.

The Four Generations of Firewalls		
Generation	**Capability**	**Attributes**
First	Packet Filtering	Basic Network Policy
Second	Deep Packet Inspection	Application Identification
Third (“Next Gen”)	Layer 7	User ID, Content Policy
Fourth	Cloud	Cloud Control Plane



TrustSec

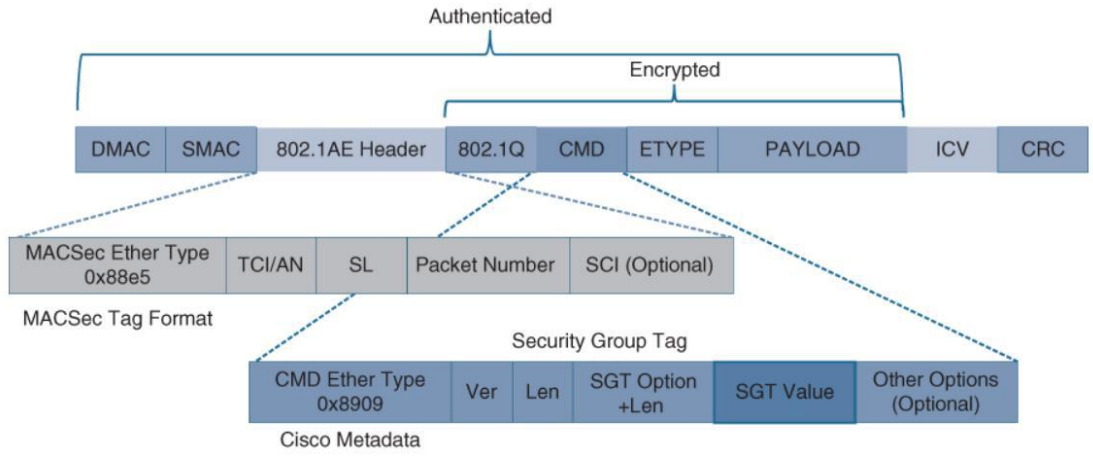
- TrustSec is a next-generation access control enforcement solution developed by Cisco to address the growing operational challenges related to maintaining firewall rules and ACLs by using Security Group Tag (SGT) tags.
- TrustSec uses SGT tags to perform ingress tagging and egress filtering to enforce access control policy.
- Cisco ISE assigns the SGT tags to users or devices that are successfully authenticated and authorized through 802.1x, MAB, or WebAuth. The SGT tag assignment is delivered to the authenticator as an authorization option (in the same way as a ACL).
- After the SGT tag is assigned, an access enforcement policy (allow or drop) based on the SGT tag can be applied at any egress point of the TrustSec network.

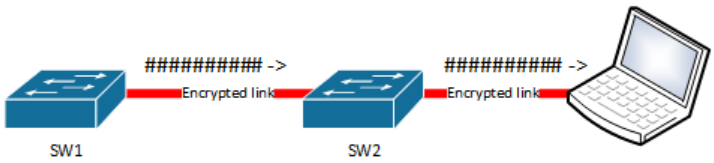


MACsec (Media Access Control security):

- **MACsec is an IEEE 802.1AE standards-based Layer 2 hop-by-hop encryption method**; this means the traffic is encrypted **only on the wire between two MACsec peers** and is **unencrypted as it is processed internally within the switch.**
- This allows the switch to look into the inner packets for things like SGT (Security Group Tag) tags to perform packet enforcement or QoS prioritization.
- MACsec also leverages onboard ASICs to perform the encryption and decryption rather than having to offload to a crypto engine, as with IPsec.
- MACsec is based on the Ethernet frame format; however, an additional 16-byte MACsec Security Tag field (802.1AE header) and a 16-byte Integrity Check Value (ICV) field are added.
- This means that all devices in the flow of the MACsec communications must support MACsec for these fields to be used and to secure the traffic.

- MACsec provides authentication using Galois Method Authentication Code (GMAC) or authenticated encryption using Galois/Counter Mode Advanced Encryption Standard (AES-GCM).

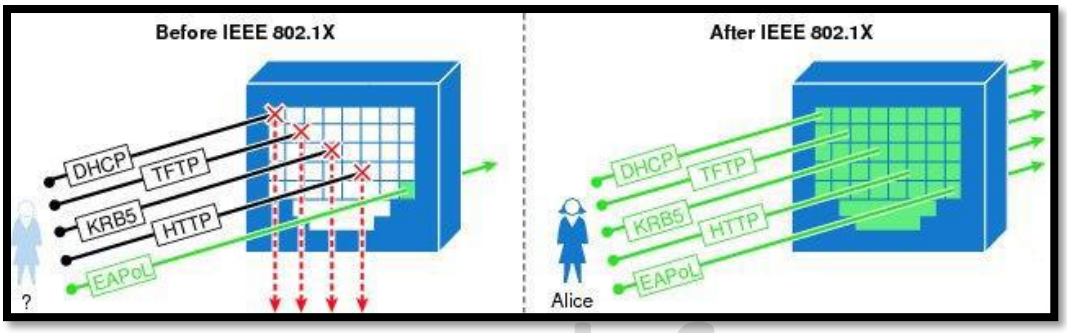




Implement 802.1X:

- IEEE 802.1x (Dot1x) is a standard set by the IEEE 802.1 working group Organization.
- **IEEE 802.1X (Dot1x) commonly referred or called Dot1x Port Based Authentication.**
- **IEEE 802.1X (Dot1x) authentication is an OSI Model Data Link Layer (Layer 2) protocol.**
- IEEE 802.1X (Dot1x) provide **port-based network access control using authentication**.
- IEEE 802.1X (Dot1x) authentication method service is called **port-level authentication**.
- IEEE 802.1x (Dot1x) is defined as a standard for **"Port-Based Network Access Control".**
- The protocol used in IEEE 802.1x (Dot1x) is called EAP Encapsulation over LANs (EAPOL).
- IEEE 802.1x (Dot1x) **uses Extensible Authentication Protocol (EAP)** to exchange messages.
- IEEE 802.1x (Dot1x) which referred Dot1x is used mainly for port-based authentication.

- Dot1x can be used to prevent unauthorized devices from gaining access to network.
- Dot1x standards provide authentication & authorization services at network port level.
- IEEE 802.1x (Dot1x) provide real security for wired and wireless networks at layer two.
- IEEE 802.1x (Dot1x) authentication is a Client and Server based authentication protocol.
- Before authentication, identity of endpoint is unknown & all traffic is blocked except EAPoL.
- Once the user credentials are successfully verified, then other user traffic is permitted.



802.1X Components:

- The IEEE 802.1x framework defines three roles in the authentication process:
- **Supplicant (Client or Host)**
- Supplicant is the user or device that wants access the wireless or wire network.
- Supplicant, client or host is the device or user requiring authentication.
- Supplicant is also known Client, as 802.1x Port-Based Authentication.
- Supplicant is the Workstation that is connected through Network Access Switch.
- Supplicant is the workstation request for accessing the network resources.
- Supplicant is the Workstation or Client must be using 802.1x Client software.
- Supplicant could be an end-user device, a printer, Fax machine, PC or an IP phone.
- The supplicant is the 802.1x software that runs on the endpoint or end Device.
- All Windows Operating System has own common native supplicant for wired networks.

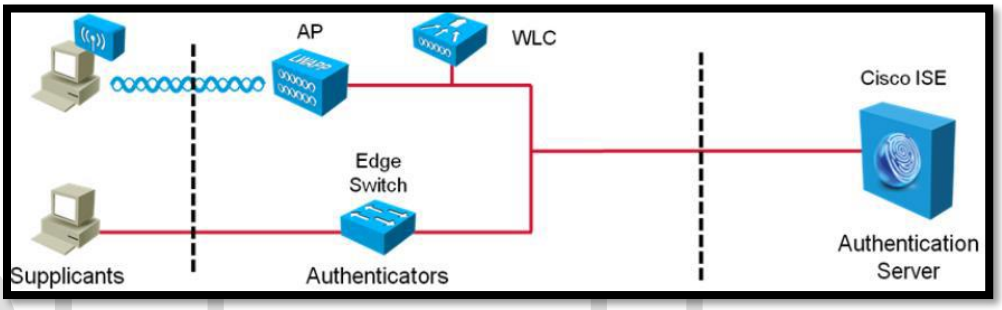
Authentication Server:

- **Authentication Server is a device that processes authentication such as RADIUS**.
- Authentication Server is the device that authenticates the Supplicant or client.
- The entity that validates the identity of the supplicant and notifies the authenticator.
- Authentication Server notifies authenticator to allow or deny the client request.

- For example, RADIUS server, such as ACS, can provide authentication server services.

Authenticator (Switch, AP):

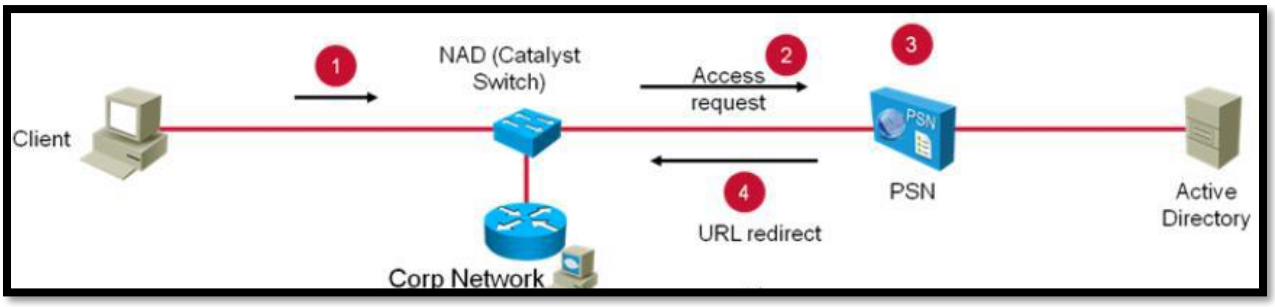
- **Device between supplicant & authentication server that facilitates authentication.**
- The client, user or supplicant is normally directly connected to the authenticator.
- For example, switch or wireless access point provide authenticator services to clients.
- Authenticator is the network device that is acting as a “gatekeeper” to the network.
- Authenticator is typically a Cisco Layer 2 or 3 Switch or Wireless LAN Controller (WLC).

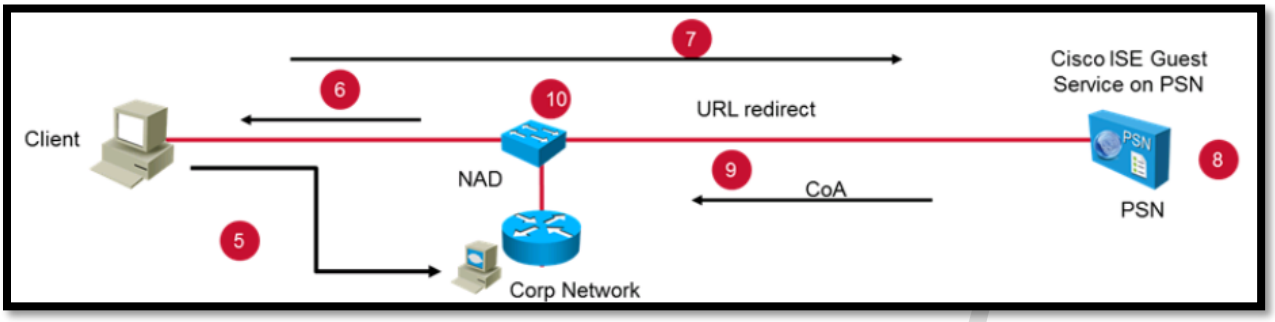


Web Authentication:

- Web Authentication enable authentication & authorization via HTTP or HTTPs portal.
- Web Authentication Automatic HTTP or HTTPs redirection to authentication portal.
- Web Authentication is deployed for visitors, guests and optionally as 802.1X fallback.
- Web Authentication method is supports by both wired access and wireless access.
- In Web Authentication user is redirected to Cisco ISE web service for authentication.
- Cisco ISE sends CoA request to the Network Access Device after the authentication.
- Basically, CWA is for interactive users who have web browser, manually enter details.
- Multiple devices will require the configuration to enable Central Web Authentication.
- Such as a redirection ACL, and ISE need authentication and Authorization rules set up.
- Central Web Authentication (CWA) is the process in which web-based authentication.
- When Client failed to authenticate via Dot1x or MAB, Client is redirected to Web Portal.
- Authorization profile configured on Authentication server will authorize this guest login.
- Central Web Authentication are, it configures along with dot1x and MAB authentication.
- Switch must run HTTP & HTTPS service & have redirect ACL to support Central WebAuth.
- Central Web mostly often used for centralized guest authentication and authorization.
- The user is authenticated in the web portal hosted on Cisco Identify Service Engine (ISE).

- Central Web Authentication (CWA) makes use of 802.1x or MAB to trigger the process.
- Central Web Authentication is L3 authentication method endpoint requires an IP address.





Implement MAB:

- MAB is term, which is stands for Media Access Control Authentication Bypass.
- MAB allow controlling devices to access the Network at OSI Reference Model Layer 2.
- Authentication server performs authentication lookup using MAC address as a credential.
- MAC Authentication Bypass feature is a MAC-address-based authentication mechanism.
- MAB can be implemented over devices, which do not support 802.1x authentication.
- MAB is used to authenticate non-802.1x capable devices such as printers, IP phones.
- MAB is working over MAC address it is independent of Usernames and passwords.
- MAB can also be implemented over the IEEE 802.1x (Dot1x) supported devices.
- MAB is not secure authentication method compared to other authentication methods.
- MAB is not a strong authentication process it can be overcome by MAC address spoofing.
- When enable MAB on switchport, switch drops all frames except first frame to learn MAC.
- Once the switch has learned the Media Access Control address of the connected device.

- The Switch then contacts and authentication server to check if it permits the MAC address.
- ISE authenticate MAB devices either based on Calling Station ID or Username & Password.
- If Process Host Lookup is enabled, then Authentication is done based on Calling Station ID.
- If Process Host Lookup is disabled, then Authentication is done on username & password.
- By default, Media Access Control only supports a single endpoint (device) per switchport.
- MAB also supports dynamic values from your RADIUS server such as ACL or VLAN etc.
- Media Access Control Authentication Bypass can be deployed as standalone authentication.