CCNP Security - SISAS
Layer 3 Authentication – HTTP / HTTPS

About Layer 3 Authentication

- Performed through HTTP/HTTPS by redirecting users to a web portal
  - not supported for machine authentication, only for user authentication
- Portal can reside on the NAD (switch, WLC)
  - Named Local Web Authentication (LWA)
  - Rarely implemented because it is decentralized
- Portal can reside on the ISE
  - Named Central Web Authentication (CWA)
  - Widely deployed as it is centralized
- User / supplicant requires IP address to complete the process
  - Starting with IOS code 12.2(55)SE, switch enforces by default an ACL on the port, which allows DHCP traffic, named Auth-Default-ACL
  - Otherwise static pre-authentication ACL needs to be deployed

About Layer 3 Authentication

- In both LWA and CWA
  - Authentication is performed by the RADIUS server
- It is supported for wired and wireless access
  - Not for VPN access yet
  - For VPN, both ISE and VPN gateway need to support it
- Use-cases
  - Mainly deployed for visitors, guest services
  - Required for Bring Your Own Device implementation
    - Alternative to Enterprise Mobility Management solution
    - Supported only in CWA mode

Local Web Authentication

- Enterprise assets will perform MAB or 802.1x in general
  - Also known as standalone web authentication
  - Makes use of authentication-proxy service via HTTP
  - MAB and 802.1x will thus also be enabled in most cases
  - LWA will be used as a fallback method on the switch port
    - Because you never know who connects on a switch port, employee or guest
    - Can be used as the single authentication method, but rarely deployed
- Authorization restriction
  - Does not support VLAN assignment, mainly because CoA is not supported in this deployment
  - Per-user ACL not supported, instead use proxy-ACL
    - same concept, still uses VSA’s, but different ACL syntax

The image cannot be displayed. Your computer may not

LWA Configuration Steps on Supplicant

» None

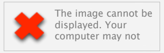
- Just a browser, because LWA is not a authentication protocol
- It is just a web authentication method
- There is no negotiation between supplicant and NAD
- NAD just intercepts HTTP/HTTPS sessions from supplicant and redirects user to the web portal
  - NAD requires a layer 3 address (SVI) for this to work

» Device Requirements

- IP address
- DNS resolution required for redirection-URL

LWA Configuration Steps on NAD

- Enable AAA
  - `aaa new-model`
- Configure login default authentication list
  - `aaa authentication login default group`
- Define LWA profile
  - `ip admission name <auth_name> proxy http`
  - `fallback profile <profile_name>`
  - `ip admission <auth_name>`
- Enable LWA on switch port facing the user
  - `authentication order webauth`
  - `authentication fallback <profile_name>`



LWA Configuration Steps on NAD

- Enable device tracking and HTTP/HTTPS server
  - `ip device tracking`
  - `ip http server`
  - `ip http secure-server`
- Enforce authentication on switch port facing the supplicant
  - `authentication port-control auto`
- Define RADIUS server settings
  - `radius-server host <IP> key <radius key>`
- Optionally configure other global/interface level settings
  - RADIUS Service-Type will be Outbound
  - In most IOS codes, it is not being send in the RADIUS Access-Request message, without command **`radius-server attribute 6 on-for-login-auth`**

LWA Configuration Steps on ISE

- Configure RADIUS integration with NAD
- Configure authentication policy
  - Possibly match on RADIUS Service-Type to make the policy unique
- Configure authorization policy
- Optionally integrate with External Servers for authentication
  - Otherwise define username/password in Local Users Store

Central Web Authentication Work Flow

- Uses a two phase process
- Phase 1
  - Uses MAB authentication
  - MAB will fail, as ISE is not aware of client’s MAC address
  - ISE will be configured to authorize the client, even though it failed authentication
    - Continue action in authentication policy for failed authentication
  - Intermediate Authorization received from ISE will be
    - Redirect-ACL, in order to capture client’s HTTP / HTTP traffic for redirection
    - Redirect-URL, in order to redirect client to ISE portal
    - Optionally, ACL in order to restrict client’s network access

Central Web Authentication Work Flow

- Phase 2 starts if user initiates HTTP / HTTPS traffic
- Phase 2
  - User is redirected to ISE's web portal
  - It has to pass portal authentication via username/password
  - If authentication succeeds, ISE will send a RADIUS Change of Authorization (CoA) message to the NAD
  - As a result, NAD will perform a re-authentication of the client via MAB
  - Authentication will fail again, just like in Phase 1
  - Final authorization is received from ISE and applied by NAD on the port
  - Final authorization uses the special condition of **`Network Access Use Case Equals GuestFlow`**

RADIUS CoA

- Per RADIUS RFC
  - Request is always initiated by the NAD
  - NAD is the RADIUS client and ISE is the RADIUS server
- CoA is a RADIUS extension defined in RFC 3576
  - Allows the RADIUS server to initiate a RADIUS request
  - Uses UDP 1700 per Cisco, can be changed to UDP 3799 for RFC compliance
- CoA common uses-cases
  - Central Web Authentication
  - Profiling and Posture assessment
  - External triggers like SIEM and MDM / EEM
- CoA messages are reliable (always acknowledged)
  - NAS issues a CoA-Request
  - NAD replies with CoA-ACK or CoA-NAK

RADIUS CoA

- CoA common instructions
  - Request the NAD to re-authenticate the endpoint
  - Request the NAD to terminate the session (port bounce)
- CoA instructions use Cisco AV Pair
  - `subscriber:command=disable-host-port` for port shutdown
  - `subscriber:command=bounce-host-port` for port bounce
  - `subscriber:command=reauthenticate` for re-authentication
- CoA makes use of the RADIUS session-ID
  - Cisco VSA, part also of the URL Redirect
  - Session-ID is a HEX value generated by NAD when issuing the RADIUS authentication request

CWA Configuration Steps on Supplicant

» None

- Just an ISE supported browser, because CWA is not a authentication protocol
- It is just a web authentication method
- There is no negotiation between supplicant and NAD
- NAD just intercepts HTTP/HTTPS sessions from supplicant and redirects user to the web portal
  - NAD requires a layer 3 address (SVI) for this to work

» Device Requirements

- IP address
- DNS resolution required for redirection-URL

CWA Configuration Steps on NAD

- Enable AAA
  - `aaa new-model`
- Configure 802.1x default authentication list
  - `aaa authentication dot1x default group`
- Configure authorization list, as Phase 1 always includes authorization
  - `aaa authorization network default group`
- Enable MAB on switch port facing the supplicant
  - `mab [eap]`
- Enforce authentication on switch port facing the supplicant
  - `authentication port-control auto`

CWA Configuration Steps on NAD

- Enable device tracking and HTTP/HTTPS server

  ```
  ip device tracking
  ip http server
  ip http secure-server
  ```

- Define RADIUS server settings

  ```
  radius-server host <IP> key <radius key>
  ```

- Configure CoA with the same RADIUS server

  ```
  aaa server radius dynamic-author
  client <server_ip> server-key <string>
  ```

- Configure the redirect ACL on the switch (allow DHCP, DNS and ISE access on TCP port 8443)
- Optionally configure other global/interface level settings

The image cannot be
displayed. Your
computer may not

CWA Configuration Steps on ISE

- Configure RADIUS integration with NAD
  - also for CoA
- Configure authentication policy
  - MAB authentication rule to pass, even though authentication fails
- Configure authorization policy for Phase1
  - Redirect-URL and Redirect-ACL
- Configure authorization policy for Phase2
  - Optional, just Access-Accept is enough
- Optionally integrate with External Servers for authentication
  - Otherwise define username/password as Guest Account

CWA Verification and Troubleshooting

» Verification

- `show authentication session`
- `show authentication interface <if_number>`
- `show aaa servers`

» Troubleshooting

- `show authentication session interface <if_number>`
- `show epm session ip`
- `show ip access-list interface`
- `debug radius authentication`
- `debug aaa coa`

ISE Guest Services

- Nothing else but what we've seen in CWA
- ISE supports full lifecycle management for guest access
  - Admin Portal, used to manage global policies for sponsors and guest users, runs on Admin Persona
  - Sponsor Portal, used to manage guest user accounts, runs on PSN Persona
  - Guest Portal, used to authenticate guests, runs on PSN persona
  - All three portals run by default over TCP 8443, can be changed
- Guest Portal scalability
  - Supports multiple guest portals
  - Each guest portal is managed by one or multiple sponsors
  - Each guest portal can be customized

The image cannot be displayed. Your computer may not

Guest Services Configuration Steps

- On supplicant and NAD, same as in CWA
- On ISE, same as in CWA
  - Optionally create sponsor accounts and groups
  - Optionally configure guest account settings
  - Optionally customize guest portal
- On ISE, same as in CWA
  - Optionally create sponsor accounts and groups
- If guest credentials are stored on ISE
  - Provision user credentials as Guest Account
    - This default requirement can be changed

Bring Your Own Device - BYOD

- Enterprise assets will perform MAB or 802.1x in general
    - Supplicant on assets is automatically deployed and configured
    - Operation is transparent to the user
- Many enterprises are opening up for BYOD
    - Allows you to come to work with your own device
    - To be considered enterprise, it has to use 802.1x authentication
    - Challenge is configuration of 802.1x on user’s devices
- ISE allows employees to enroll their own devices
    - Supplicant on devices will be automatically configured for 802.1x and enrolled in PKI
    - Process achieved through CWA with self-service and device registration being enabled
    - Once enrolled, user will be assigned to the ActivatedGuest group of users, which can be used as a condition in authorization policies

The image cannot be displayed. Your computer may not

BYOD Device Onboarding

- Mostly used for mobile assets
  - Smartphones, tablets, laptops
- As mobile assets lack Ethernet card in general
  - Deployment is done via Wi-Fi
  - Wired is also supported
- Wireless Deployment Options
  - Single SSID
  - Dual SSID

The image cannot be displayed. Your computer may not

Wi-Fi Deployments

Single SSID

- Provisioning and network access through same SSID
- Rarely used, because of complications
  - VLAN change is required after provisioning
  - Provisioning SSID has to be secured, requires layer 2 authentication
  - Guest support not recommended, due to layer 2 authentication

Dual SSID

- Provisioning happens through one SSID
  - Deployed with CWA (and AD authentication in general)
  - Guest support is recommended, as layer 2 authentication is open
- Network access happens through second SSID
  - After successful 802.1x provisioning
  - Automatic SSID change can be triggered by the provisioning process

The image cannot be displayed. Your computer may not

Q&A