CCNP Security - SISAS EndPoint Profiling

What is Profiling ?

- Profiling
  - Allows ISE to learn attributes about network connected endpoints
  - Based on the profile, it will assign endpoint to appropriate identity groups
  - Groups can be used in authorization policy for smarter network access control decisions
  - Especially useful for devices that perform MAB, but not only
- Two types of profiling
  - Static profiling, where endpoint is manually assigned to a group
  - Dynamic profiling, where endpoint attributes are dynamically learned through the use of probes
- By default, dynamic profiling is turned off
  - Endpoints are still automatically profiled based on MAC address
  - However, only device vendor can be detected, so it's not very specific

Dynamic Profiling

- Automatic fingerprinting of the endpoint based on several probes
  - ISE needs to be configured to listen for probes
  - NAD needs to be configured to send probes
- RADIUS, highly recommended
  - Inspects RADIUS attributes from the authentication Request
  - Inspects RADIUS accounting for IP-MAC binding, required for NMAP scanning or DNS resolution of endpoint
  - Used also for IOS Device sensor feature, supported starting with 15.0(2) on switches and 7.2.110.0 on WLC

Most Commonly Used Probes

- HTTP
  - ISE interprets HTTP messages from CWA or SPAN
  - Gathers User-Agent from HTTP packet, used to identify the operating system on the device
    - Crucial for mobile device profiling
- DHCP
  - ISE interprets DHCP messages from DHCP-Relay or SPAN
  - Gathers User-Agent from DHCP packet, used to identify the operating system on the device
  - Gathers DHCP hostname
    - Important for mobile device profiling
  - Useful only in DHCP environments

Less Commonly Used Probes

- NMAP
  - TCP/UDP port scanning for operating system detection
- SNMP query send by ISE
  - Used only in case NAD does not support device sensor
  - Triggered by RADIUS accounting or SNMP trap
  - Reads CDP/LLDP/ARP/MAC data
- DNS resolution performed by ISE
  - Reverse DNS query for PTR records to get the FQDN of the endpoint
  - Query initiated only if device profiles through other probes: RADIUS, DHCP, HTTP, SNMP
- Netflow samples
  - Detects abnormal traffic (profiled printer making skype calls on the Internet)

Profiling Policies

- ISE has a large database of built-in profiling policies
  - Can profile many devices out-of-the-box, given that enough data is received from probes
  - Additional policies can be manually configured, or you can edit the built-in ones
  - Logical profile is a container with associated profiling policies
- ISE has a built-in hierarchy for device profiling, in the form of parent-child, for example
  - Parent policy is named Apple-Device
  - Child policy attached to the parent policy can be Apple-iPad or Apple-iPhone
- Profiling policies are built on a set of conditions for device identification
  - In order to be profiled as Apple-iPad, conditions for both parent and child policy need to be satisfied

Profiling Policies Settings

- Minimum Certainty Factor
  - How sure is ISE about endpoint being identified
  - Integer value which needs to be met in order for endpoint to be assigned to be profile policy
- Associated CoA type
  - When endpoint is profiled and assigned to a specific group, do you want CoA to be performed
- Rules
  - Each rule is a condition matching on collected endpoint attributes
  - Each rule ahs an associated action, most commonly being to increase the Certainty Factor
    - NMAP SCAN is an alternative action

Profiling Result

- It can happen that the device is authorized by ISE before being accurately profiled
- Thus, usually CoA is also deployed with profiling
  - Allows to change device authorization after being profiled
- In general, by deploying ISE in phases, all devices will be profiled before going to Closed Mode
- Because of profiling, CoA is triggered when
  - Endpoint profiled for 1st time
  - Endpoint statically assigned to a group
  - Endpoint removed from ISE database
  - Endpoint dynamically changed identity group membership

ISE Authorization Flow with Profiling

- How AAA order of processing is changed
  - Endpoint Authentication
  - Initial Authorization Policy pushed (endpoint not profiled yet)
  - Profiling data is received or asked for
  - Device is profiled and assigned to a identity group
  - ISE triggers CoA requesting endpoint re-authentication
  - Endpoint Authentication
  - Final authorization matching the conditions for the identity group
- Because authorization rules are processed top-down
  - Order of rules is very important

Profiling Configuration Steps on NAD

- Configure RADIUS accounting to ISE
  - `aaa accounting dot1x default start-stop group`
- Configure NAD to relay endpoint IP address in RADIUS Access-Request message, requires device tracking to be enabled
  - `radius-server attribute 8 include-in-access-req`
- Configure DHCP-Relay
  - `ip helper-address <ise_ip>`
- Configure NAD to relay endpoint DHCP class attribute in RADIUS Access-Request message
  - `radius-server attribute 25 access-request include`
- Configure NAD to send Netflow samples and SNMP traps to ISE

Profiling Configuration Steps on ISE

- Ensure that Enable Profiling Service check box is selected on the PSN
  - By default it is
- Enable Profiling Probes
  - Activates interpretation of probe messages
- Enable CoA for Profiling
- Optionally, tune the profiler conditions and policies
  - Configure authorization policies using as condition the profiled endpoints
- Most deployments use a separate physical port on ISE to receive data from probes
  - Probes may send hug amount of data, especially if SPAN is used
  - SPAN is, in general not recommended for performance
  - It leaves a dedicated port just for regular RADIUS authentication

NAD 802.1x Port Modes

- Single Host (default)
  - Single MAC address allowed in data domain
  - Second MAC address results in violation action
- Multi Domain
  - Single MAC address allowed per domain (voice and data)
  - Second MAC address for each domain results in violation action
- Multiple Authentication
  - Single MAC address allowed in voice domain
  - Multiple MAC addresses allowed in data domain
    - VLAN authorization possible, single VLAN supported
- Multiple Host
  - Only first MAC address is required to authenticate
  - No ACL and Redirect URL support

IOS Device Sensor Overview

- Scales profiling service on ISE
  - Highly recommended to be deployed
  - Less data with more details for ISE to interpret
  - The NAD gathers endpoint attributes through CDP, LLDP and DHCP
    - CDP and LLDP need to be enabled on the NAD
  - Sends the collected endpoint attributes to ISE through RADIUS accounting messages
    - Uses Cisco AV pairs

DHCP Device Sensor Configuration Steps

- Configure a list of DHCP options to be collected
  - `device-sensor filter-list dhcp list <list_name>`
  - `option name host-name`
  - `option name client-identifier`
  - `option name client-fqdn`
  - `option name class-identifier`
- Activate the DHCP sensor option
  - `device-sensor filter-spec dhcp include list <list_name>`

CDP Device Sensor Configuration Steps

- Configure a list of CDP TLV's to be collected
  - `device-sensor filter-list cdp list <list_name>`
  - `tlv name device-name`
  - `tlv name capabilities-type`
  - `tlv name platform-type`
- Activate the CDP sensor option
  - `device-sensor filter-spec cdp include list <list_name>`

LLDP Device Sensor Configuration Steps

- Configure a list of LLDP TLV's to be collected
  - `device-sensor filter-list lldp list <list_name>`
  - `tlv name port-id`
  - `tlv name system-name`
  - `tlv name system-capabilities`
- Activate the LLDP sensor option
  - `device-sensor filter-spec lldp include list <list_name>`

Device Sensor Common Configuration

- Enable RADIUS accounting
  - `aaa accounting dot1x default start-stop group`
  - `aaa accounting update newinfo`
  - `radius-server vsa send accounting`
- Globally activate IOS sensor
  - `device-sensor accounting`
  - `device-sensor notify all-changes`
- Globally activate CDP and LLDP
  - `cdp run`
  - `lldp run`

Device Sensor Verification

- Verify probe functionality
  - `show lldp`
  - `show cdp`
  - `show device-sensor cache all`
- Verify collected data per endpoint
  - `show device-sensor cache mac <mac_address>`
- Verify that collected data is being sent to ISE
  - `show aaa method-lists accounting`
  - `debug radius accounting`

Q&A