Introduction

This document describes the new features in Identity Services Engine (ISE) that allows redirection to take place with third-party network access devices (NADs).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Guest flow on ISE
- DNS and DHCP protocols

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalys 2960 series switch
- Cisco ISE, Release 2.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information
Advanced features like Guest, Posture and Bring Your Own Device (BYOD) in modern networks, require direct communication between client device and AAA server. In previous ISE versions this was accomplished by sending a dynamic redirect URL and Access Control List (ACL) to the NAD.

There are two mandatory attributes that are sent in an authorization profile for redirection in attribute-value pairs (AVs):

- Cisco AV pair – Redirect URL: The URL value is dynamic and it is created for each session. The important parts of redirect URL are Policy Service Node Fully Qualified Domain Name (PSN FQDN) and Session ID.
- Cisco AV pair – Redirect ACL: This AV pair contains an ACL name that must exist on the NAD. With the help of this ACL, the NAD decides if the packets should be redirected or allowed through the NAD.

Traditional redirection approach can only be implemented with Cisco NAD devices. For third party NAD support, static URL redirection had been added in ISE 2.0. While this approach is more platform independent, it still requires HTTP redirection support on the NAD.

Starting with ISE 2.1 a new style of redirect has been added. This approach does not require HTTP redirection support on the NAD. The main idea behind this method is to use the ISE as a DNS sinkhole.

DNS and DHCP server functionality have been added to the ISE 2.1 release in order to use it as a DNS sinkhole. Now ISE server can assign IP addresses to the users that need to be redirected and define itself as a DNS server. This allows ISE to redirect user connections to itself without any web server functionality on the NAD. However, the NAD should still support Change of Authorization (COA) and dynamic VLAN assignment.

In ISE, this approach can be used for these redirection flows:

- Guest flow: The ISE answers to any DNS request initiated by the user with its own IP address. This response causes the client to establish an HTTP connection with ISE. In this connection, ISE returns the redirect URL using the standard HTTP code 302 page moved.
- BYOD/Posture (Anyconnect only) – in both scenarios, the Native Supplicant Provisioning (NSP) application or Anyconnect Posture module initiates a connection to enroll.cisco.com, which gets redirected to ISE using the same steps as guest flow.

Packet Flow
1. NAD starts MAB process for the connected device. The MAB process on Cisco switches starts according to authentication method priority and not before the first frame is received from the end device.

2. MAB access-request is sent to ISE.

3. ISE evaluates authentication and authorization policy for incoming access request. During authorization policy evaluation, the Network Device Type (NAD level setting) is compared with the Network Device type defined in the authorization profile. Only authorization profiles for matching Network Device Type can be selected.

   **Note:** For Guest VLAN redirect, ISE needs to select an authorization profile that contain Web Redirection (CWA, MDM, NSP, CPP) and VLAN assignment. The client need to be assigned to a network segment that has ISE as the only DHCP server.

1. ISE returns an Access-Accept with VLAN information.
2. Switch authorizes the port and applies the VLAN settings.
3. Client initiates DHCP discover. If the PC is located in the same segment as ISE, the packet reaches the ISE directly. In case of L3 connectivity between client and ISE, the ISE IP should be configured as an IP helper address on the NAD for DHCP relay.
4. ISE adds the client information to its DHCP binding table. Client IP and MAC are used by ISE for session lookup.
5. DHCP Offer is sent to the client. In this offer, the ISE IP address is specified as the DNS server.
6. User opens a web browser and navigates to google.com which triggers a DNS request to ISE.
7. ISE checks if the target FQDN belongs to External Domains. If it does, then ISE sends this request to a DNS server defined in the DHCP pool settings. If not ISE returns its own IP address in response.
8. The web browser initiates a TCP connection to ISE and requests for google.com.
9. At this stage ISE looks up the authenticated session for incoming HTTP GET request. This is important for building the correct Redirect URL.

   **Note:** ISE uses these rules for the session lookup:
   1. Lookup IP in DHCP binding
   2. Lookup MAC by IP
   3. Lookup session by MAC

1. ISE responds with HTTP 302 page moved to the redirect URL.
2. User is thus redirected to guest portal and the entire guest flow configured on ISE takes place here.
3. After a successful guest authentication, the ISE runs through the Authorization Policies once more to check if any new attributes were added to the session and if the endpoint during guest flow requires Change of Authorization (CoA). Once the next authorization policy is identified, ISE prepares the CoA request.
4. The CoA request/CoA ACK exchange takes place between ISE and NAD. A Port Bounce or Admin Reset CoA is a must as this triggers obtaining a new IP address in the final VLAN. The NAD needs to support Radius or SNMP CoA for this step to work.
5. Accounting-Request Stop for the disconnected session is sent to ISE. ISE acknowledges this request by sending an Accounting-Response.
6. ISE starts a session stitching timer (20 seconds by default). During this time all session
attributes (ex: GUEST_TYPE, Use case=Guest Flow) are kept by ISE. In case a new access request for the same calling station ID is received during this time, all session attributes are bound to the new session.

7. A new MAB access-request is sent for the end device after CoA port bounce.
8. ISE identifies the Authentication/Authorization policy for the new request. At this stage ISE uses session attributes and/or endpoint attributes for the correct policy selection.
9. An Access-Accept is sent with the final VLAN information. A Downloadable Access Control List (DACL) can be sent instead, to restrict traffic on the default VLAN as well.
10. Switch authorizes the port in the new VLAN and applies a DACL if included.

Configure

Configure ISE

1. Create Network Device Profile

For this particular example, a Cisco switch been used as NAD. Therefore, the existing Cisco Network Device Profile been duplicated and modified as required. Navigate to Administration > Network Resources > Network Device Profiles and add new profile.

![Network Device Profile List](image)

- Name: Cisco_Guest_VLAN
- Description: Generic profile for Cisco network access devices
- Vendor: Cisco

   Supported Protocols
    - RADIUS
    - TACACS+
    - TrustSec

![Change of Authorization (CoA)](image)

- CoA by RADIUS
  - Default CoA Port: 1719
  - Timeout Interval: 5 seconds
  - Retry Count: 2

- Disconnect
  - RFC 1910

![Port Configuration](image)

- Port Configuration
  - Role: Disabled
  - Command: subscriber-template-activate
  - Redirection: Terminated-Health

2. Create Network Device

Navigate to Administration > Network Resources > Network Devices in order to add new device.
a. Note setting for Network Device Profile.

b. All other settings are standard.

3. Configure DHCP Server

The DHCP server pool is bound to a particular ISE node and its interface. Navigate to Administration > System > Settings > DHCP & DNS Services > Add

- **Scope Name** needs to be configured.
- Select the node on which DNS and DHCP services that should be running and the interface on that node that should be used.

- **Domain Name**
- **DHCP Address range**
- **Subnet mask**
- **Network ID**
- **Exclusion address range**
- **Default gateway**
- **DHCP lease time**

- **External DNS servers**

- **External Domains**

- **DHCP scope name** needs to be configured.

- Select the node on which DNS and DHCP services that should be running and the interface on that node that should be used.
c. Define the DHCP IP address range, default gateway, addresses excluded from scope and the DHCP lease time.

d. Optionally, define external DNS server IP addresses. These should be queried for External Domains.

e. Optionally, define external domains names. The ISE queries external DNS servers and returns the actual IP address instead of its own.

4. Configure Authorization Profile

Navigate to Policy > Policy Elements > Results > Authorization > Authorization Profiles. Two authorization profiles are needed for the complete guest flow:

- Redirect authorization profile (CWA1)
- Permit Access authorization profile (PermitCWA2)

![Authorization Profile CWA1](image)

- Network Device Profile: Only authentication requests coming from NADs assigned to this profile may result in this authorization profile,

![Network Device Profile](image)

- VLAN Tag ID 1

![VLAN Tag ID](image)

- Web Redirection (CWA, MDM, NSP, CPP)

![Web Redirection](image)
b. VLAN settings: VLANs defined here must exist on the NAD. The ISE interface configured for DHCP should either belong to this VLAN or should to be configured as IP helper on gateway servicing this VLAN.

c. Redirect settings: For current example Central Web Authentication was defined as redirect type, and sponsored guest portal been defined as a guest portal. The form still asks for the Redirect ACL name. Since the network device profile has been reconfigured for static URL redirect, this ACL name will never be sent to the NAD.

5. Configure the Authorization Policies for Guest Access

Navigate to Policy > Authorization. Configure two policies: one for redirect action and the other for user access after authentication on Guest Portal.

a. The first authorization policy matches Wired MAB as an authentication method and the redirect authorization profile is assigned as a result.
b. The second authorization policy can be based either on session attributes (Use case = Guest Flow/Guest Type/ External AD group if guest users authenticated using AD) or on endpoint attributes (Endpoint Identity group). Device registration needs to be enabled on the guest portal to use Endpoint Identity Group.

Configure NAD

The Cisco switch has been configured for MAB on the interface and has COA support.

**Note:** The Cisco Technical Assistance Center (TAC) does not offer any support for configuration of Third-Party NADs.

Verify

A successful guest flow looks like this in ISE Operations > Radius Livelog:

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>User</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-01-01 21:32:50</td>
<td>e.</td>
<td>32:32:32:32:32:32</td>
<td>32.32.32.32</td>
</tr>
<tr>
<td>2010-01-02 00:00:00</td>
<td>c.</td>
<td>31:31:31:31:31:31</td>
<td>31.31.31.31</td>
</tr>
<tr>
<td>2010-01-02 00:00:00</td>
<td>b.</td>
<td>30:30:30:30:30:30</td>
<td>30.30.30.30</td>
</tr>
<tr>
<td>2010-01-02 00:00:00</td>
<td>a.</td>
<td>29:29:29:29:29:29</td>
<td>29.29.29.29</td>
</tr>
</tbody>
</table>

a. This is the first MAB authentication. The authorization profile with redirect is selected as a result.

b. This is the guest authentication. After this action ISE does a policy re-evaluation to decide if CoA is needed.

c. A CoA was successfully completed.

d. This is the second MAB authentication. The authorization profile for guest access is selected as a result.

Troubleshoot

Check if IP address is assigned to the client correctly. This can be done by collecting a packet capture on the client or ISE.

This capture from the client shows a successful DHCP handshake with the DNS IP same as the ISE.
Check if ISE is properly acting as a DNS sinkhole. A packet capture can help confirm if the request is going to ISE and if the ISE responds to it with its own IP address:

Check if the HTTP redirect works properly. After it gets the resource IP address and establishes a TCP connection to ISE, the client sends an HTTP GET request to the ISE. This can be confirmed in a client side packet capture:

At the same time, ISE determines if any session exists for this client. This process of session lookup on ISE can be checked in prrt-management log:

After the session lookup, ISE returns the redirect URL to the client in an HTTP 302 response: