ISE with Static Redirect for Isolated Guest Networks Configuration Example

TAC **Document ID: 117620**

Contributed by Jesse Dubois, Cisco TAC Engineer.
Apr 23, 2014

Contents

Introduction

This document describes how to configure the Cisco Identity Services Engine (ISE) with static redirect for isolated guest networks in order to maintain redundancy. It also describes how to configure the policy node so that clients are not prompted with an unverifiable certificate warning.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ISE Central Web Authentication (CWA) and all related components
- Browser verification of certificate validity
- Cisco ISE Version 1.2.0.899 or later
- Cisco Wireless LAN Controller (WLC) Version 7.2.110.0 or later (Version 7.4.100.0 or later is preferred)

Note: CWA is described in the Central Web Authentication on the WLC and ISE Configuration Example Cisco article.

Components Used

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

- Cisco ISE Version 1.2.0.899
- Cisco Virtual WLC (vWLC) Version 7.4.110.0
- Cisco Adaptive Security Appliance (ASA) Version 8.2.5

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

In many Bring Your Own Device (BYOD) environments, the guest network is fully isolated from the internal network in a De−Militarized Zone (DMZ). Often, the DHCP in the guest DMZ offers public Domain Name System (DNS) servers to the guest users because the only service that is offered is internet access.

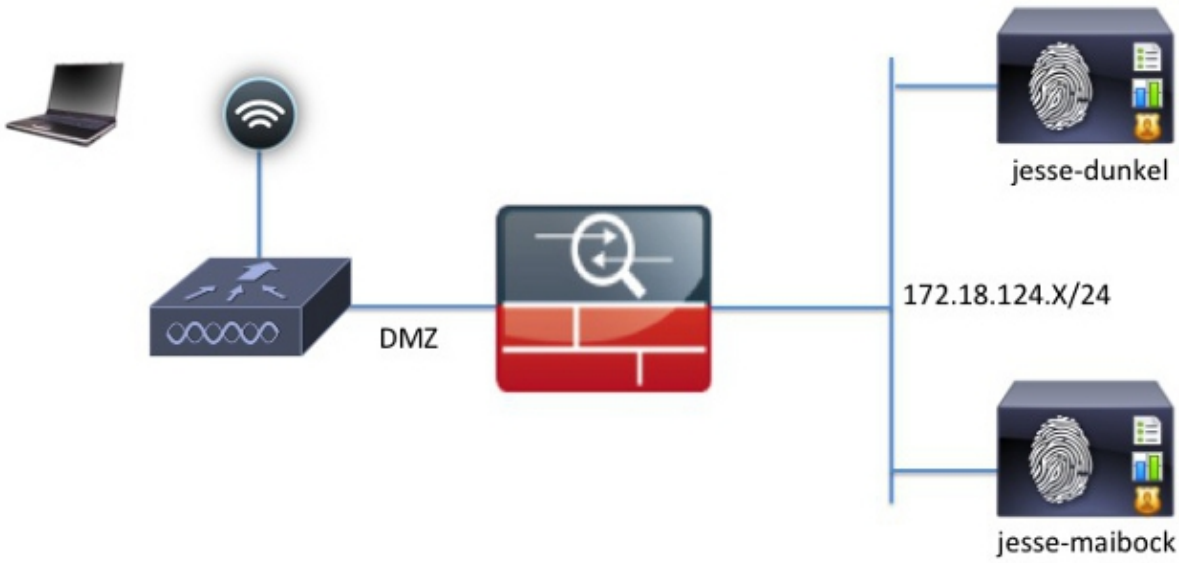
This makes guest redirection on the ISE difficult prior to Version 1.2 because the ISE redirects clients to the Fully Qualified Domain Name (FQDN) for web authentication. However, with ISE Versions 1.2 and later, administrators can redirect guest users to a static IP address or hostname.

Configure

Network Diagram

This is a logical diagram.

Note: Physically, there is a wireless controller in the internal network, the Access Points (APs) are on the internal network, and the Service Set Identification (SSID) is anchored to the DMZ controller. Refer to the documentation for Cisco WLCs for more information.



Configuration

The configuration on the WLC remains unchanged from a normal CWA configuration. The SSID is configured in order to allow MAC filtering with RADIUS authentication, and the RADIUS accounting points towards two or more ISE policy nodes.

This document focuses on the ISE configuration.

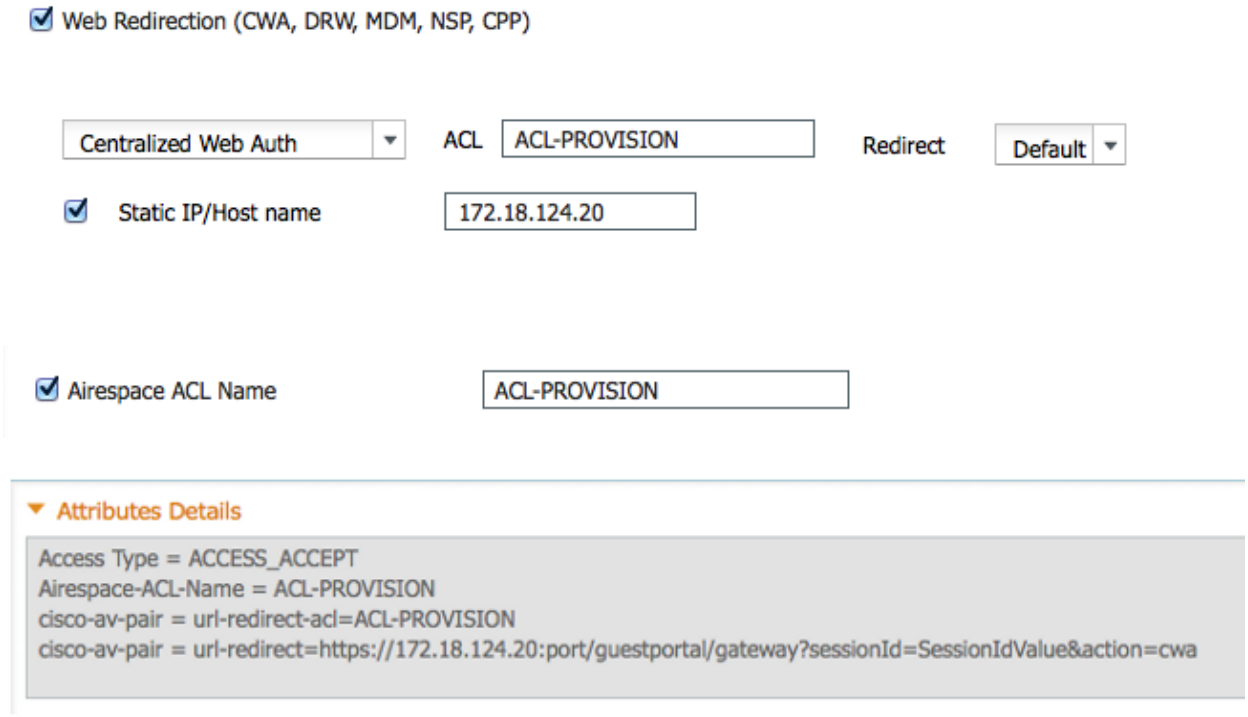
Note: In this configuration example, the policy nodes are ***jesse−dunkel*** (172.18.124.20) and ***jesse−maibock*** (172.18.124.21).

The CWA flow begins when the WLC sends a RADIUS MAC Authentication Bypass (MAB) request to the ISE. The ISE replies with a redirect URL to the controller in order to redirect HTTP traffic to the ISE. It is important that the RADIUS and HTTP traffic go to the same Policy Services Node (PSN) because the session is maintained on a single PSN. This is normally performed with a single rule, and the PSN inserts its own hostname into the CWA URL. However, with a static redirect, you must create a rule for each PSN in order to ensure that the RADIUS and HTTP traffic are sent to the same PSN.

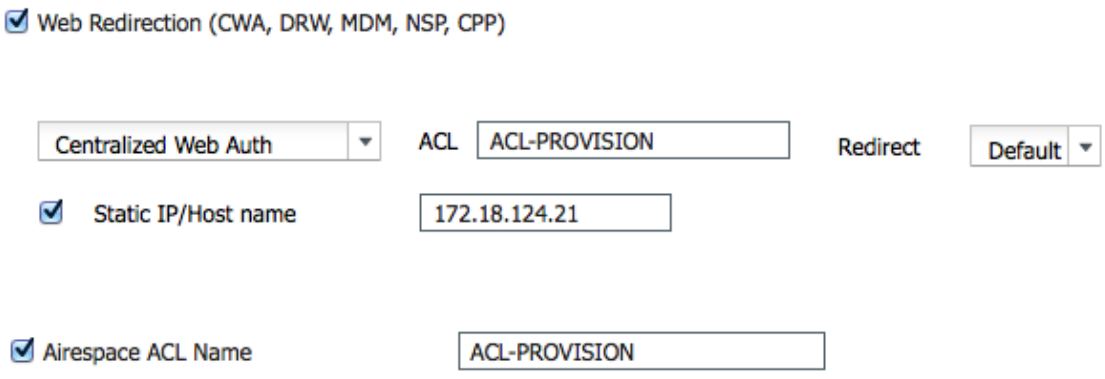
Complete these steps in order to configure the ISE:

1. Set up two rules in order to redirect the client to the PSN IP address. Navigate to ***Policy > Policy Elements > Results > Authorization > Authorization Profiles***.

   These images show the information for profile name ***DunkelGuestWireless***:

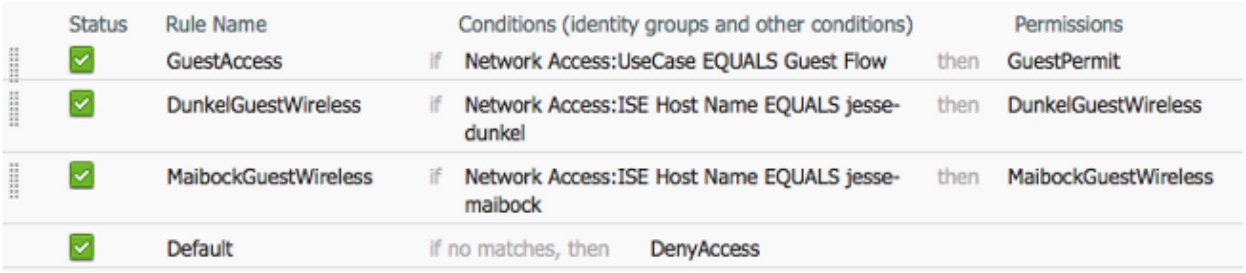


   These images show the information for profile name ***MaibockGuestWireless***:

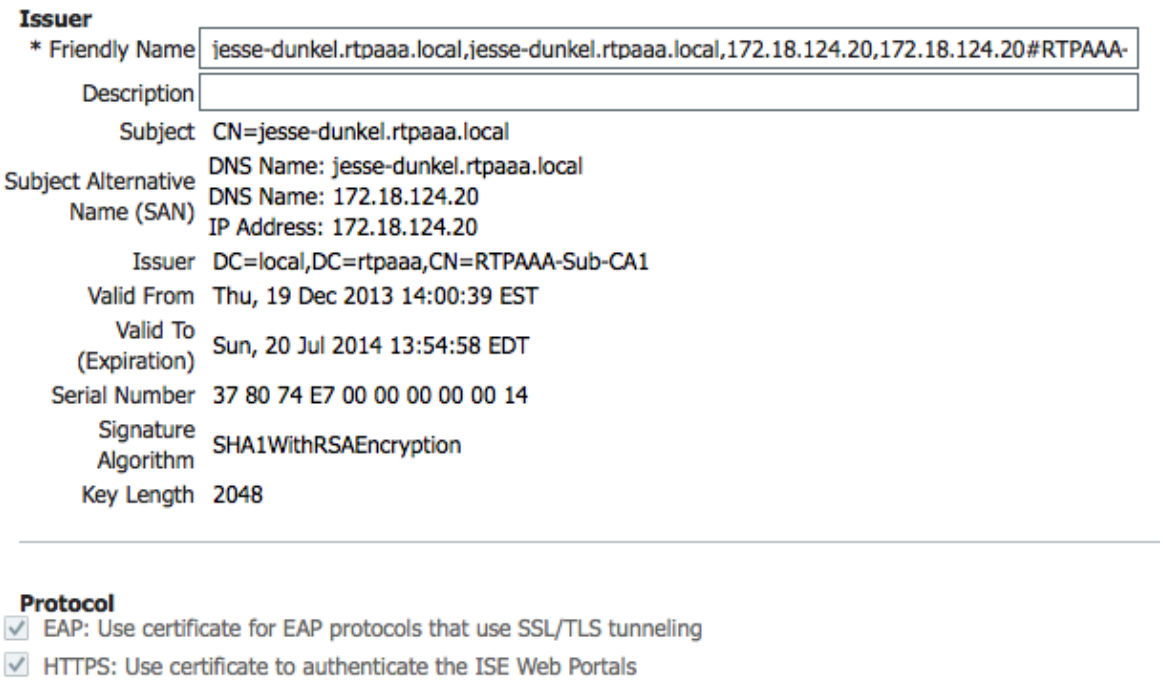


Note: The ***ACL−PROVISION*** is a local Access Control List (ACL) that is configured on the WLC in order to allow the client to communicate with ISE upon authentication. Refer to the Central Web Authentication on the WLC and ISE Configuration Example Cisco article for more information.

2. Configure the authorization polices so that they match on the ***Network Access:ISE Host Name*** attribute and provide the appropriate authorization profile:



Now that the client is redirected to an IP address, users receive certificate warnings because the URL does not match the information in the certificate. For example, the FQDN in the certificate is ***jesse−dunkel.rtpaaa.local***, but the URL is ***172.18.124.20***. Here is an example certificate that allows the browser to validate the certificate with the IP address:



With the use of Subject Alternative Name (SAN) entries, the browser can validate the URL that includes the IP address ***172.18.124.20***. Three SAN entries must be created in order to address the various client incompatibilities.

3. Create a SAN entry for the DNS Name and ensure that it matches the ***CN=*** entry from the Subject field.

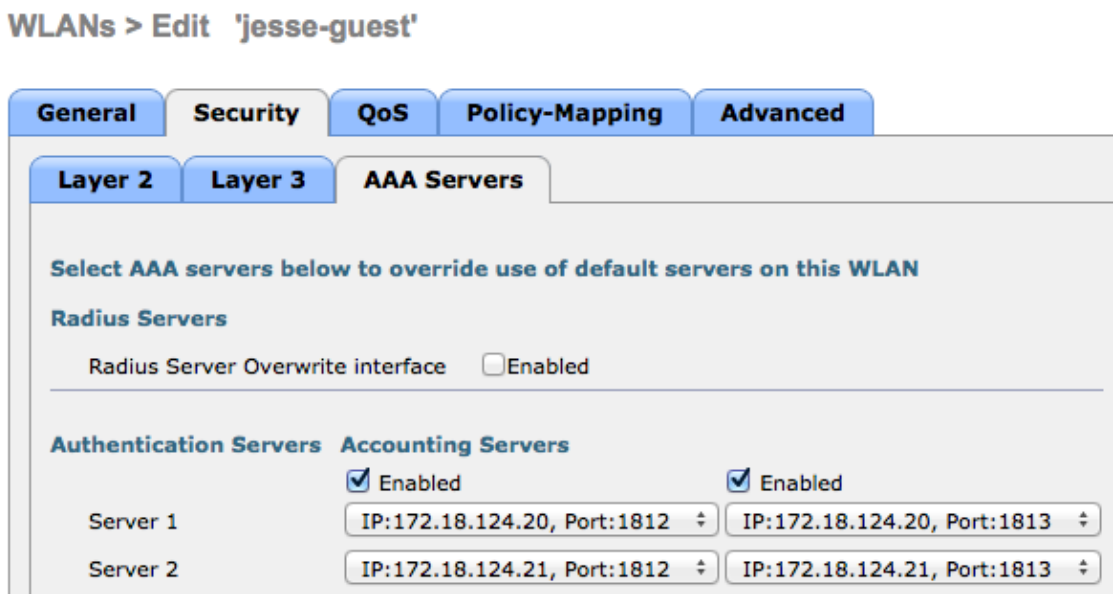
4. Create two entries in order to allow clients to validate the IP address; these are for both the DNS Name of the IP address as well as the IP address that appears in the IP Address attribute. Some clients only refer to the DNS Name. Others do not accept an IP address in the DNS Name attribute but instead reference the IP Address attribute.

   Note: For more information about certificate generation, refer to the ***Cisco Identity Services Engine Hardware Installation Guide, Release 1.2***.

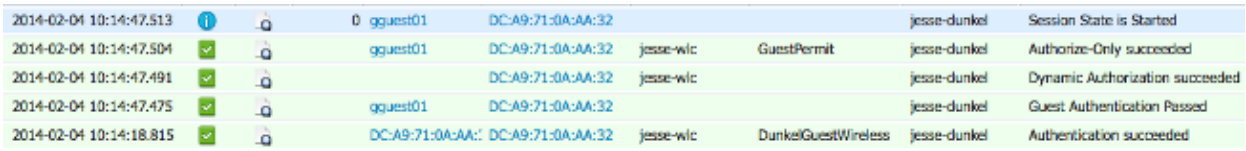
Verify

Complete these steps in order to confirm that your configuration works properly:

1. In order to verify that both of the rules are functional, manually set the order of the ISE PSNs that are configured on the WLAN:



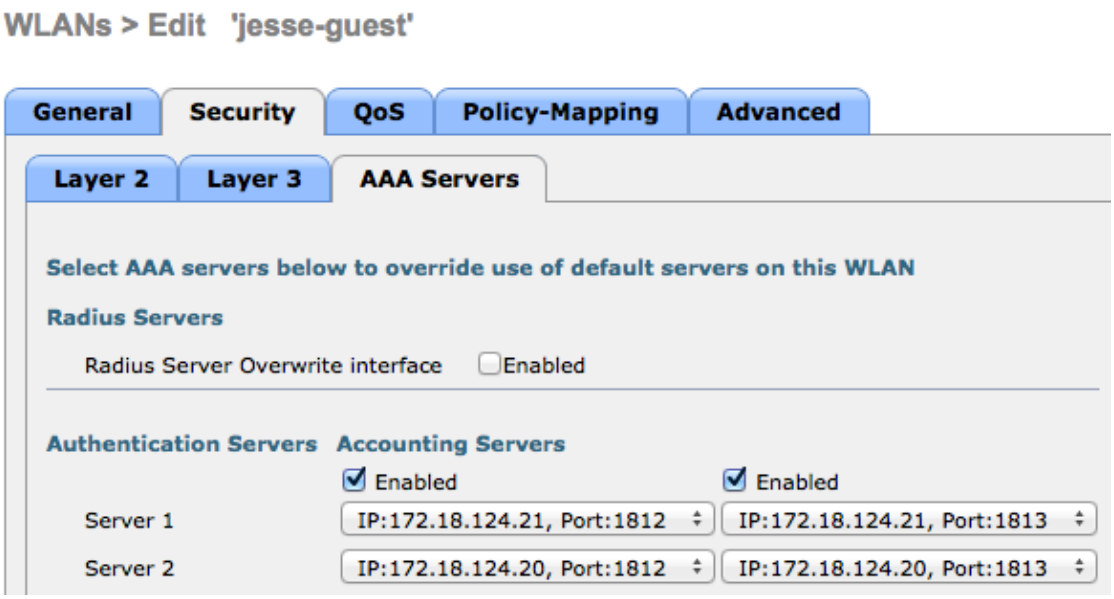
2. Log into the guest SSID, navigate to ***Operation*** > ***Authentications*** in the ISE, and verify that the correct authorization rules are hit:



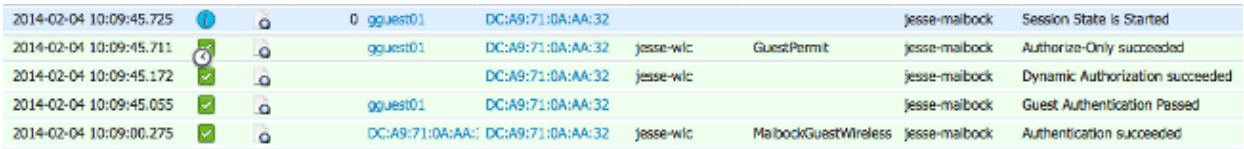
   The initial MAB authentication is given to the ***DunkelGuestWireless*** authorization profile. This is the rule that specifically redirects to ***jesse−dunkel***, which is the first ISE node. After the ***gguest01*** user logs in, the correct final permission of ***GuestPermit*** is given.

3. In order to clear the authentication sessions from the WLC, disconnect the client device from the wireless network, navigate to ***Monitor*** > ***Clients*** on the WLC, and delete the session from the output. The WLC holds the idle session for five minutes by default, so in order to perform a valid test, you must begin anew.

4. Reverse the order of the ISE PSNs under the guest WLAN configuration:



5. Log into the guest SSID, navigate to ***Operation*** > ***Authentications*** in the ISE, and verify that the correct authorization rules are hit:



For the second attempt, the ***MaibockGuestWireless*** authorization profile is correctly hit for the initial MAB authentication. Similar to the first attempt to ***jesse−dunkel*** (Step 2), the authentication to ***jesse−maibock*** correctly hits the ***GuestPermit*** for the final authorization. Because there is no PSN−specific information in the ***GuestPermit*** authorization profile, a single rule can be used for authentication to any PSN.

Troubleshoot

The Authentication Details window is a powerful view that displays every step of the authentication/authorization process. In order to access it, navigate to ***Operations*** > ***Authentications*** and click the magnifying glass icon under the Details column. Use this window in order to verify that the authentication/authorization rule conditions are configured properly.

In this case, the Policy Server field is the primary area of focus. This field contains the hostname of the ISE PSN by which the authentication is serviced:

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

Compare the Policy Server entry to the rule condition and ensure that the two match (this value is case sensitive):

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

Note: It is important to remember that you must disconnect from the SSID and clear the client entry from the WLC between tests.

Updated: Apr 23, 2014 Document ID: 117620