使用隔離訪客網路的靜態重定向的ISE配置示例

目錄

簡介

本檔案介紹如何為隔離訪客網路使用靜態重新導向設定思科身分識別服務引擎(ISE)以維持備援。還介紹了如何配置策略節點，以便客戶端不會收到不可驗證證書警告提示。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ISE中央Web驗證(CWA)及所有相關元件
- 驗證證書有效性的瀏覽器驗證
- Cisco ISE 版本1.2.0.899或更高版本
- 思科無線LAN控制器(WLC)版本 7.2.110.0或更高版本（首選版本7.4.100.0或更高版本）

附註：CWA在WLC和ISE上的中央Web身份驗證配置示例思科文章中進行了說明。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE 版本1.2.0.899
- Cisco Virtual WLC(vWLC)版本 7.4.110.0
- 思科調適型安全裝置(ASA))版本8.2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

在許多自帶裝置(BYOD)環境中，訪客網路與非軍事化區域(DMZ)中的內部網路完全隔離。 通常，訪客DMZ中的DHCP向訪客使用者提供公共域名系統(DNS)伺服器，因為提供的唯一服務是網際網路訪問。

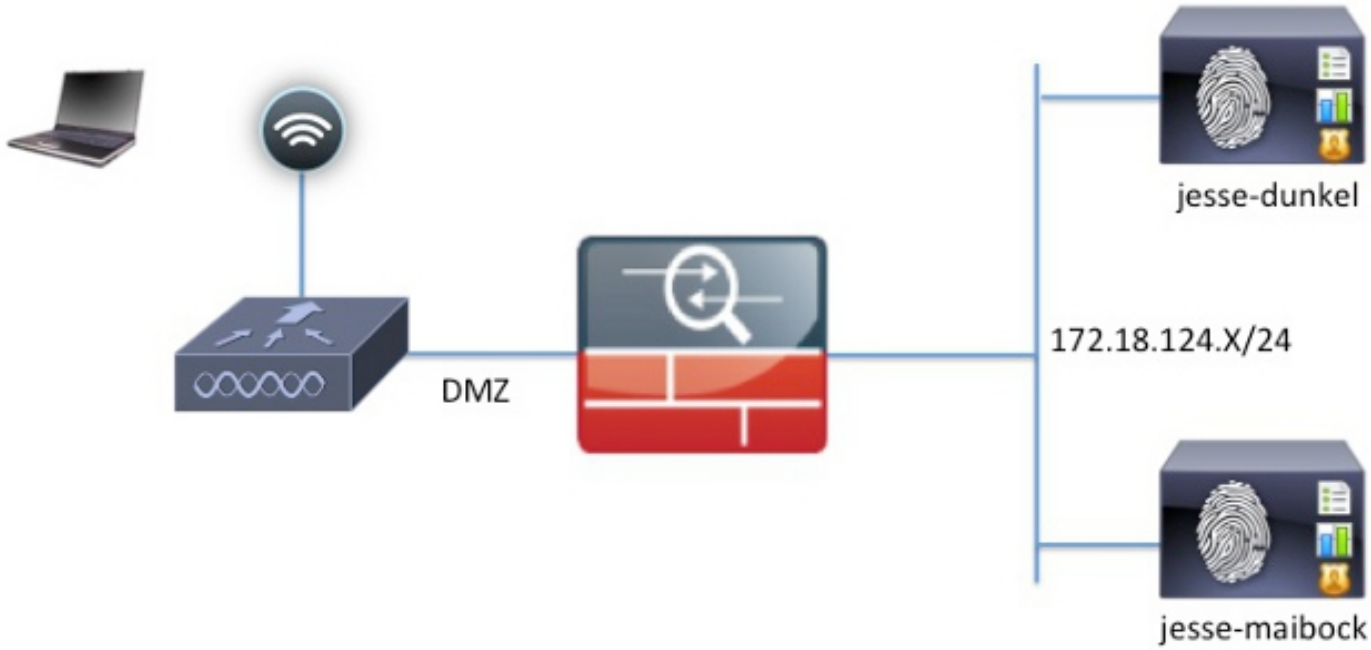
這會使ISE上的訪客重定向在版本1.2之前變得困難，因為ISE將客戶端重定向到Web身份驗證的完全限定域名(FQDN)。但是，在ISE版本1.2及更高版本中，管理員可以將訪客使用者重定向到靜態IP地址或主機名。

設定

網路圖表

這是一個邏輯圖。

> **附註**：在物理上，內部網路中有一個無線控制器，接入點(AP)位於內部網路上，服務集標識(SSID)固定到DMZ控制器。如需詳細資訊，請參閱Cisco WLC的說明檔案。



組態

WLC上的組態與正常的CWA組態相同。SSID配置為允許使用RADIUS身份驗證進行MAC過濾，並且RADIUS記帳指向兩個或多個ISE策略節點。

本文檔重點介紹ISE配置。

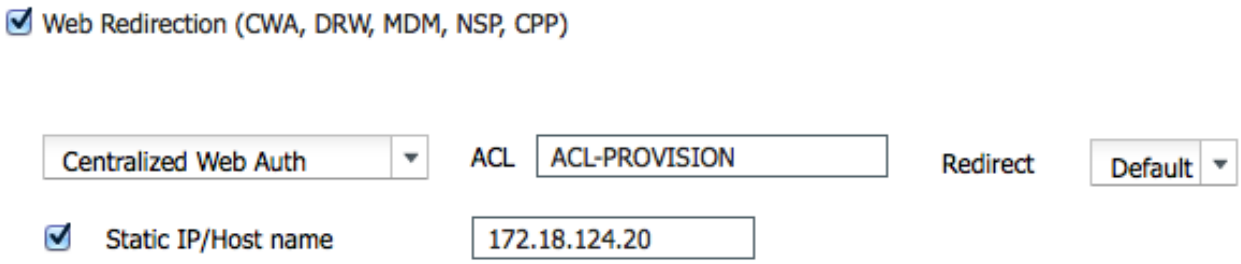
> **附註**：在此配置示例中，策略節點是**jesse-dunkel**(172.18.124.20)和**jesse-maibock**(172.18.124.21)。

CWA流程在WLC向ISE傳送RADIUS MAC身份驗證繞行(MAB)請求時開始。ISE會使用重定向URL回覆控制器，以便將HTTP流量重定向到ISE。RADIUS和HTTP流量必須前往同一個原則服務節點(PSN)，因為作業階段是在單個PSN上維持的。這通常使用單個規則執行，並且PSN會將自己的主機名插入CWA URL。但是，使用靜態重定向時，您必須為每個PSN建立規則，以確保RADIUS和HTTP流量傳送到同一個PSN。

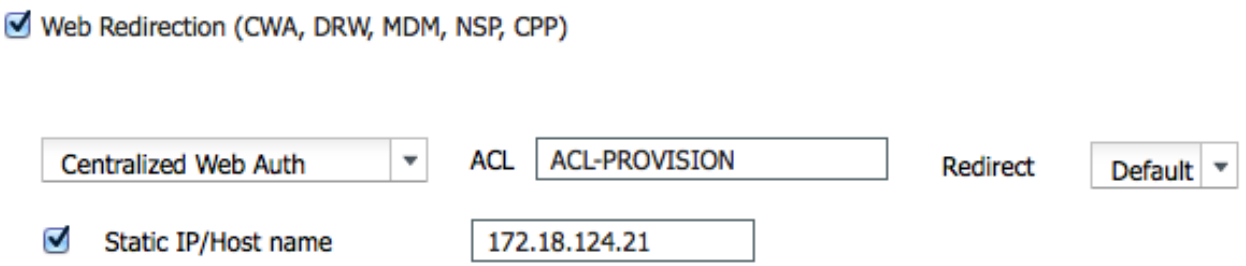
完成以下步驟以配置ISE:

1. 設定兩個規則以將客戶端重定向到PSN IP地址。導航到**Policy > Policy Elements > Results > Authorization > Authorization Profiles**。

   這些影象顯示了配置檔名稱**DunkelGuestWireless**的資訊：

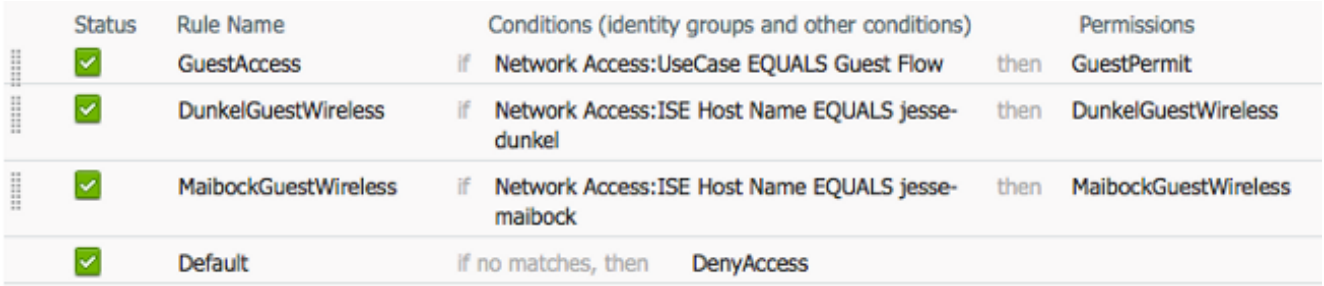


   這些影象顯示了配置檔名稱**MaibockGuestWireless**的資訊：



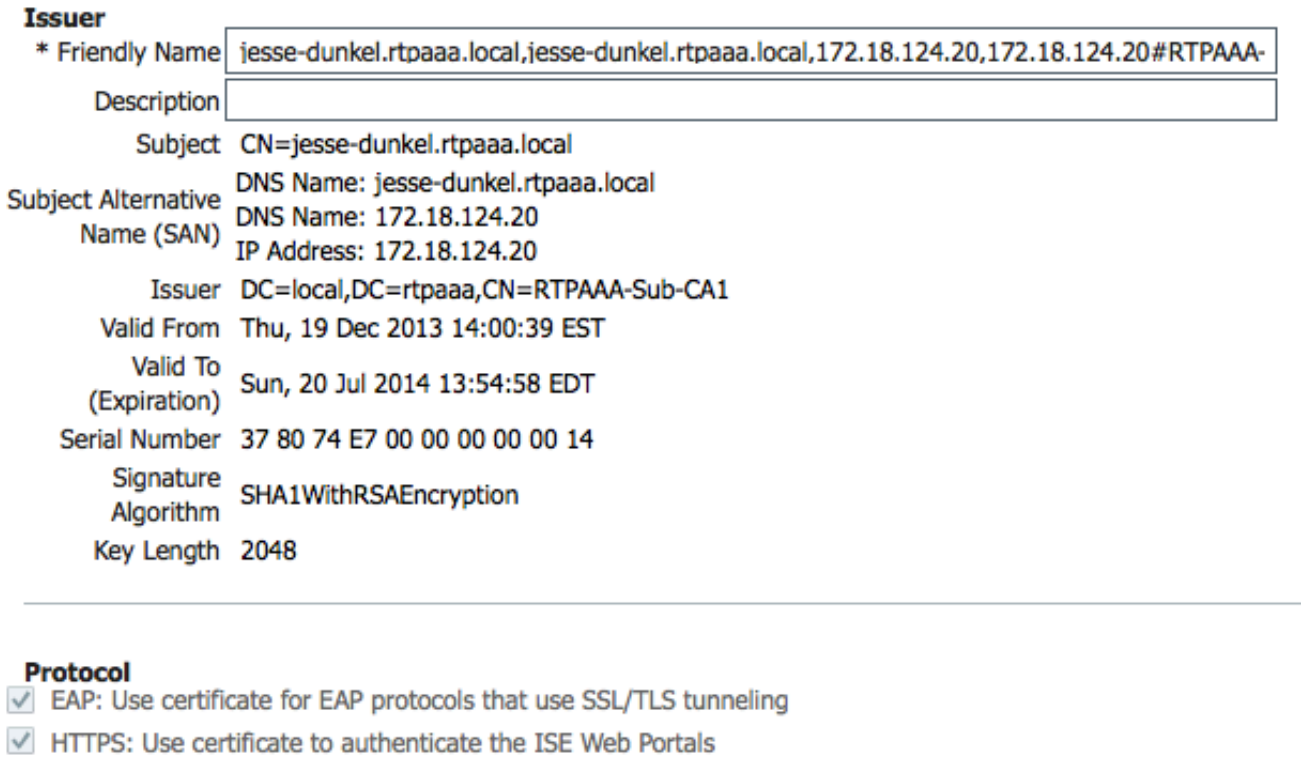
附註：ACL-PROVISION是在WLC上配置的本地訪問控制清單(ACL)，用於允許客戶端在身份驗證時與ISE通訊。如需詳細資訊，請參閱WLC和ISE上的中央Web驗證和ISE組態範例Cisco文章。

2. 配置授權策略，使其在**網路訪問：ISE主機名**屬性上匹配，並提供相應的授權配置檔案：



Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then	GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then	DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then	MaibockGuestWireless
✓	Default	if no matches, then DenyAccess		

現在使用者端重新導向到IP位址，使用者會收到憑證警告，因為URL與憑證中的資訊不相符。例如，證書中的FQDN是**jesse-dunkel.rtpaaa.local**，但URL是**172.18.124.20**。以下是允許瀏覽器使用IP地址驗證證書的示例證書：



使用主題備用名稱(SAN)條目，瀏覽器可以驗證包含IP地址**172.18.124.20**的URL。必須建立三個SAN條目以解決各種客戶端不相容問題。

3. 為DNS名稱建立SAN條目，並確保它與主題欄位**中的CN=**條目匹配。

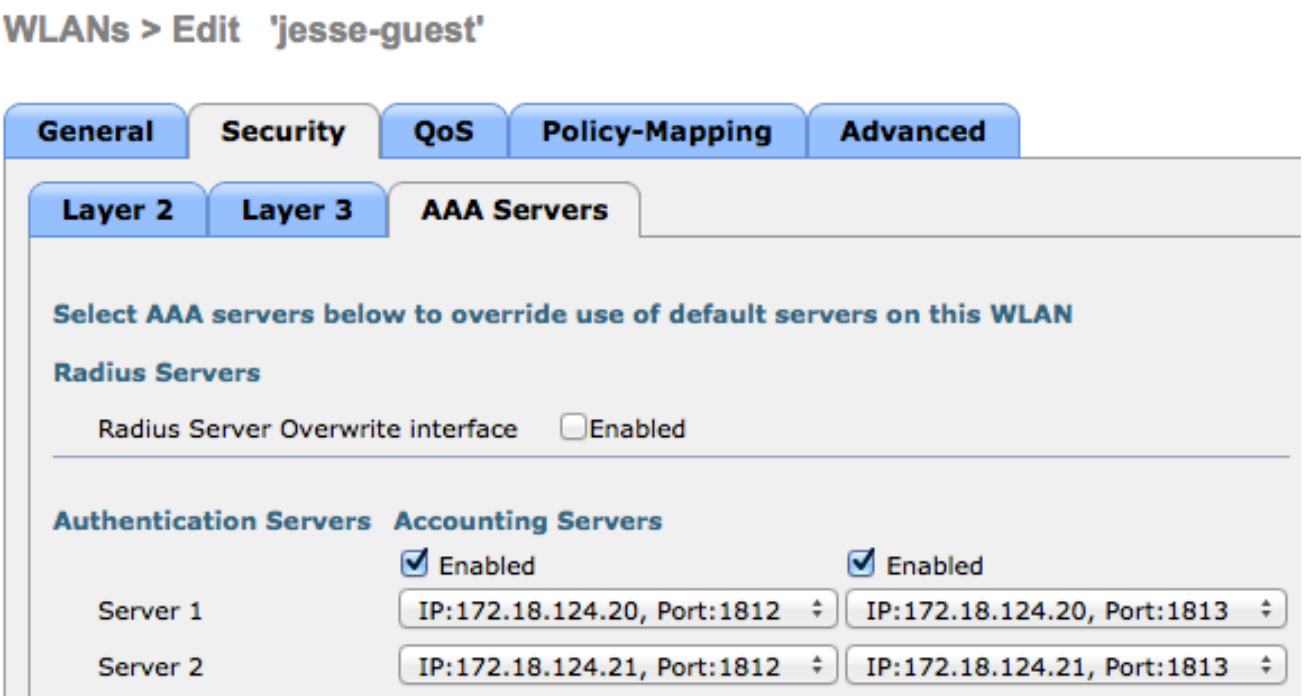
4. 建立兩個專案以允許使用者端驗證IP位址；這些名稱既用於IP地址的DNS名稱，也用於IP地址屬性中顯示的IP地址。某些使用者端僅引用DNS名稱。其他使用者不接受DNS名稱屬性中的IP地址，而是引用IP地址屬性。

   附註：有關證書生成的詳細資訊，請參閱**思科身份服務引擎硬體安裝指南1.2版**。

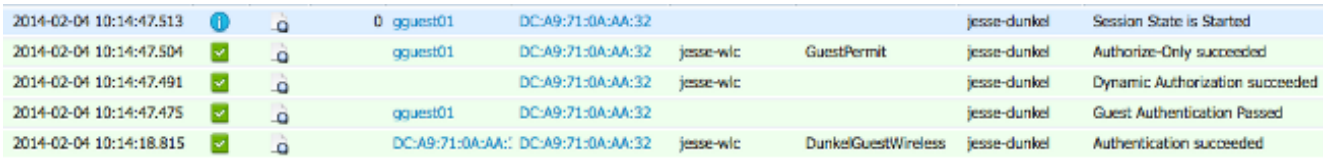
驗證

完成以下步驟，確認您的組態是否正常運作：

1. 為了驗證兩個規則是否都正常工作，請手動設定WLAN上配置的ISE PSN的順序：



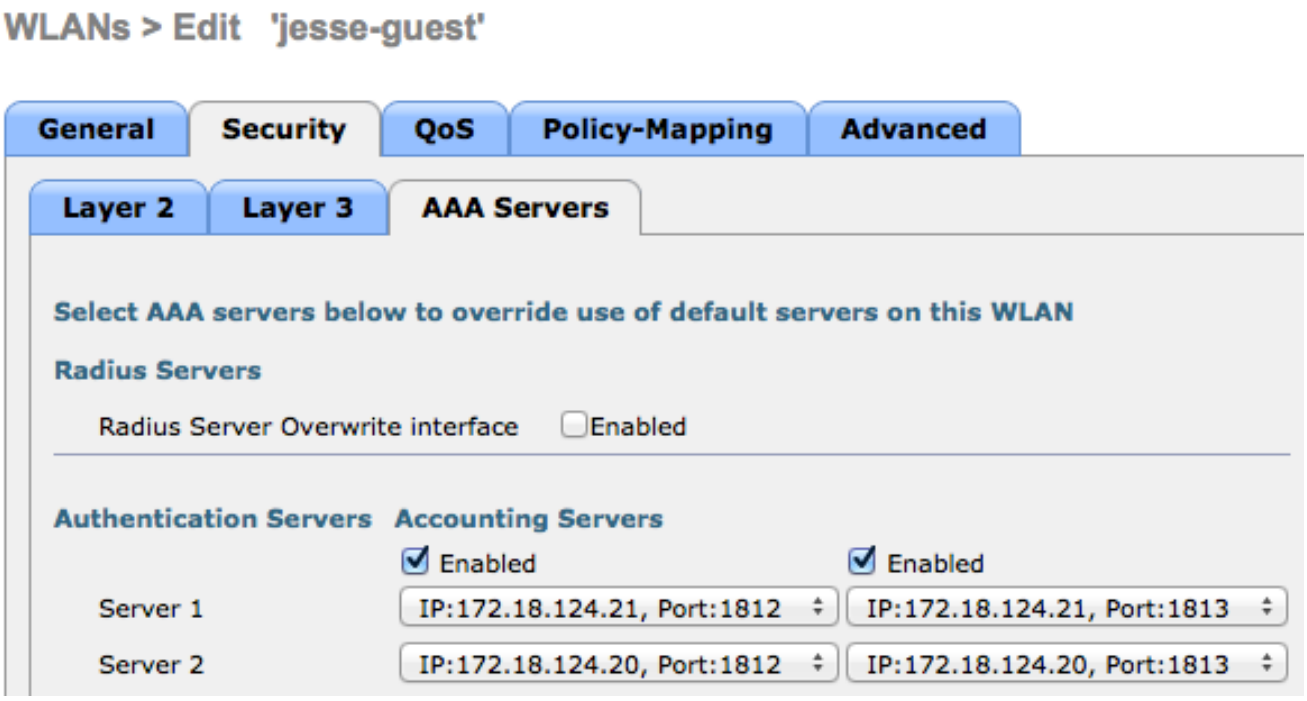
2. 登入訪客SSID，在ISE中導航到**Operation > Authentications**，並驗證是否達到了正確的授權規則：



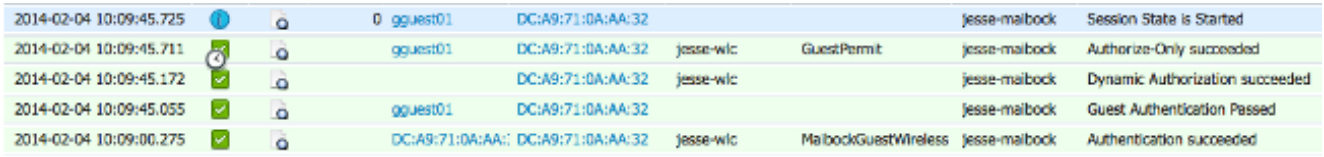
初始MAB身份驗證將賦予DunkelGuestWireless**授權**配置檔案。這條規則專門重定向到**jesse-dunkel**，這是第一個ISE節點。**gguest01**使用者登入後，會指定**GuestPermit**的正確最終許可權。

3. 若要從WLC清除驗證作業階段，請斷開使用者端裝置與無線網路的連線，在WLC上導覽至**Monitor > Clients**，然後從輸出中刪除作業階段。預設情況下，WLC會保留閒置作業階段五分鐘，因此若要執行有效測試，您必須重新開始。

4. 在訪客WLAN配置下反向ISE PSN的順序：



5. 登入訪客SSID，在ISE中導航到**Operation > Authentications**，並驗證是否達到了正確的授權規則：



對於第二次嘗試，**MaibockGuestWireless**授權配置檔案已為初始MAB身份驗證正確命中。與第一次嘗試**jesse-dunkel**（步驟2）類似，**jesse-maibock**的驗證會正確命中最終授權的**GuestPermit**。由於**GuestPermit**授權配置檔案中沒有特定於PSN的資訊，因此可以使用單個規則對任何PSN進行身份驗證。

疑難排解

Authentication Details視窗是一個功能強大的檢視，可顯示身份驗證/授權過程的每個步驟。要訪問它，請導航到**操作>身份驗證**，然後按一下「詳細資訊」列下的放大鏡圖示。使用此視窗驗證身份驗證/授權規則條件是否配置正確。

在這種情況下，策略伺服器欄位是主要關注領域。此欄位包含用於進行身份驗證的ISE PSN的主機名：

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

比較策略伺服器條目與規則條件，並確保兩者匹配（該值區分大小寫）：

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

附註：必須記住，在測試之間必須斷開與SSID的連線，並從WLC清除客戶端條目。