在思科無線網路上啟用強制網路門戶

在思科無線網路上啟用強制網路門戶

在移動性和合作性日益增強的業務環境中，越來越多的組織正在開放其網路環境，以便與業務合作夥伴、客戶和其他訪客進行受控資源共用。企業正在尋求更好的方法：

·為來訪客戶提供安全的無線網際網路接入
·允許業務合作夥伴有限地訪問公司網路資源
·為正在使用個人流動裝置的員工提供快速身份驗證和連線

Cisco Small Business無線接入點(AP)（例如WAP321或WAP561）可以輕鬆整合到現有有線網路中，以提供速度和安全性堪比典型有線連線的無線連線。

Cisco Captive Portal功能提供了一種方便、安全、經濟高效的方式，為客戶端和其他訪客提供無線接入，同時保持您的內部網路的安全性。訪客網路可以服務於許多重要的業務目的，包括簡化與合作夥伴的業務以及提高客戶滿意度和員工工作效率。

強制網路門戶可提供以下基本功能：

·帶有公司徽標的自定義訪客登入頁面
·能夠建立強制網路門戶的多個例項
·多個身份驗證選項
·能夠分配不同的權利和角色
·分配頻寬（上游和下游）的能力

如何設定強制網路門戶？

可以通過裝置GUI設定強制網路門戶，為快速和基本設定客戶可以使用設定嚮導啟用該功能，請參閱以下步驟：

使用安裝嚮導

從裝置GUI的主控制面板運行安裝嚮導。

按照嚮導螢幕操作。

啟用訪客訪問（強制網路門戶）。

為您的訪客網路指定一個名稱，例如「My Company- Guest」。

選擇安全型別。

如果使用者接受歡迎頁面中的服務條款後，您想要顯示特定網頁，請鍵入URL，然後鍵入此

URL可以是您的公司網站。

選擇「下一步」轉到下一頁。

現在，您的強制網路門戶設定已完成，您的客戶現在可以連線到您的訪客網路並獲得歡迎頁面。

要獲得門戶的高級設定和自定義，請從Captive Portal選單登入裝置GUI。

選擇「例項配置」(Instance Configuration)，您會發現嚮導建立了一個名為「wiz-cp-inst1」的例項名稱，您可以選擇此名稱或為「例項配置」建立新名稱，然後儲存。 如果選擇「wiz-cp-inst1」，螢幕將進入「例項配置」頁面。

您會注意到，安裝嚮導會自動將強制網路門戶例項名稱「wiz-cp-inst1」關聯到您在安裝嚮導期間建立的訪客SSID。

如果使用GUI建立例項，則現在需要關聯到您建立的訪客網路。
從下拉選單中選擇例項名稱「Guest」或由嚮導「wiz-cp-inst1」建立的實例。

從選單中選擇Web Portal Configuration以配置您的訪客歡迎頁面，從下拉選單中選擇例項名稱。

選擇強制網路門戶用於驗證客戶端的身份驗證方法：

·訪客 — 使用者不需要通過資料庫進行身份驗證。
·本地 — WAP裝置對經過身份驗證的使用者使用本地資料庫。
· RADIUS - WAP裝置使用遠端RADIUS伺服器上的資料庫驗證使用者。

如果選擇驗證方法「區域設定」，則需要建立本地使用者。

從選單中選擇本地。

輸入使用引數（使用者的名稱），選擇使用者配置檔案的引數。

Web門戶頁面自定義，現在您可以選擇上傳您的公司徽標和圖形，最多可以上傳3個圖形檔案，一個用於頁面背景（預設cisco-bkg），第二個用於公司徽標（預設cisco-log），第三個用於登入螢幕（預設log-key）。

**請注意，此圖稿檔案的檔案大小需要5KB。

現在，您可以自定義您的Web門戶頁面，如新增接受使用策略、視窗標題和名稱等……

將驗證方法設為Guest的自定義頁面，這意味著不需要進行身份驗證，使用者只需接受服務條款並選擇Connect按鈕，輸入使用者名稱為可選。

驗證方法為Local的自定義頁面意味著使用者需要輸入使用者名稱和密碼進行驗證，然後使用者需要接受服務條款並選擇Connect按鈕。

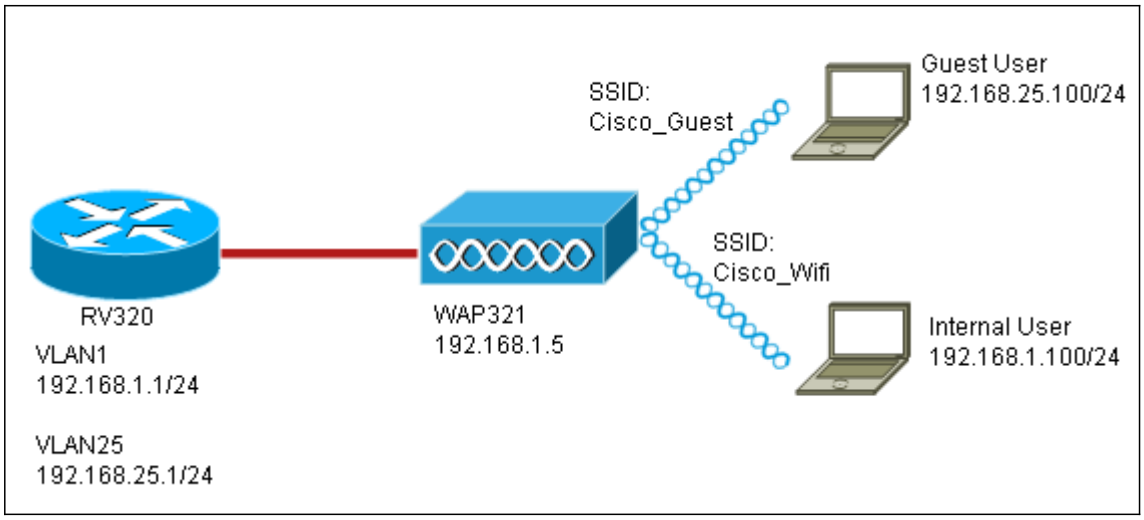
多VLAN環境中的強制網路門戶

在某些情況下，網路需要多個VLAN用於不同的用途，為不同的使用者組提供服務。一個常見的示例是訪客使用者使用單獨的網路，以防止未經授權的使用者訪問公司網路上的資源。有時

，由於相同的原因，多個無線網路需要可供不同的使用者使用。WAP321和WAP561可以使用強制網路門戶滿足這些需求，但需要在網路上增加一些配置。本節將討論該配置。

簡介 — 現有配置

本檔案假定網路組態已就緒。 在本範例中，有兩個網路，即主網路和訪客網路。 已配置用於為每個網路建立和提供DHCP地址的配置。 WAP321已配置為為每個網路廣播不同的SSID。 當前設定將如下所示：

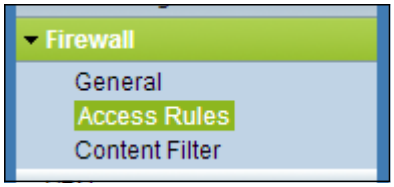


配置完成後，將在網路上啟用InterVLAN路由，以便所有無線客戶端都可以訪問強制網路門戶，從而啟用網路連線。

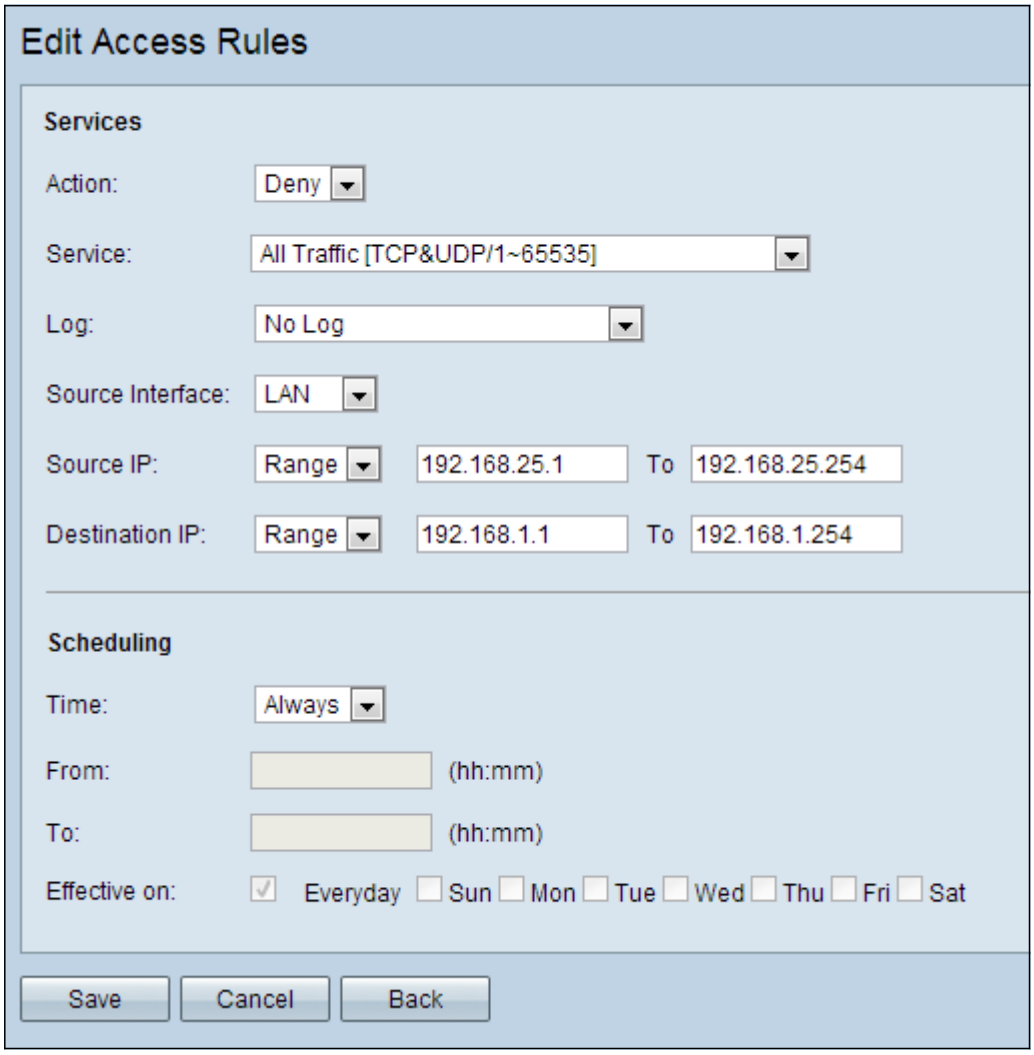
組態

首先，在核心路由器上啟用InterVLAN路由（本例中為RV320）。要配置此功能，請轉至Port Management > VLAN Membership以啟用InterVLAN路由。檢查頁面左側的VLAN 1和VLAN 25，然後點選Edit。在InterVLAN Routing列中，按一下每個的下拉框並選擇Enabled。儲存設定。

現在，所有使用者都應該能夠訪問強制網路門戶，但他們也可以訪問主VLAN或訪客VLAN上的任何資源。 要限制訪問，請在RV320上配置訪問控制規則。 轉到Firewall > Access Rules以配置此限制。



在頁面底部，點選新增。 我們希望為方案新增總共2個訪問規則。 首先，配置拒絕從192.168.25.x/24訪客子網訪問192.168.1.x/24內部子網的規則，如右圖所示。



按一下頁面底部的「儲存」，然後按一下「上一步」。 現在新增另一個規則，這次將操作設定為「允許」，將目標IP設定為「單一」。將規則配置為允許從192.168.25.x/24子網到192.168.1.5（當前配置為WAP321靜態IP）的訪問。 此規則將置於我們剛才建立的deny規則之前，允許從訪客網路發往192.168.1.5的流量，但不允許從主網路中發往任何其他位置。

完成後，訪問規則頁面應如下所示。

要在此設定中配置強制網路門戶，只需按照第一節中針對需要配置強制網路門戶的每個網路的步驟進行操作。

檢視與本文相關的影片……

[按一下此處檢視思科的其他技術對話]