Enable a Captive Portal on your Cisco Wireless Network

Enabling Captive Portal on your Cisco Wireless Network

In an increasingly mobile, collaborative business environment, more organizations are opening up their network environments for controlled sharing of resources with business partners, customers, and other guests. Businesses are seeking better ways to:

- Provide secure wireless Internet access to visiting customers
- Enable limited access to company network resources for business partners
- Provide rapid authentication and connectivity for employees who are using there personal mobile devices

A Cisco Small Business wireless access point (AP), such as the WAP321 or WAP561, can be easily integrated into the existing wired network to provide a wireless connectivity with speed and security rivaling a typical wired connection.

The Cisco Captive Portal feature provides a convenient, secure, cost-effective way to offer wireless access for clients and other visitors while maintaining the security of your internal network. A guest network can serve many important business purposes, including streamlining business with partners and providing enhanced customer satisfaction and improve employee productivity.

Captive Portal can provide the following basic functionality:

- Customized guest login page with company logos
- Ability to create multiple instances of the captive portal
- Multiple authentication options
- Ability to assign different rights and roles
- Ability to assign bandwidth (upstream and downstream)

How to Setup Captive Portal?

Captive Portal can be setup via the device GUI, for fast and basic setup customer can use the setup wizard to enable the feature, please see steps below:

Using the Setup Wizard

Run the setup wizard from the main dashboard of the device GUI.

Follow the wizard screens.

Enable Guest access (Captive Portal).

Give your guest network a name, for example “My Company- Guest”.

Select a security type.

If you have a specific web page you want to show after users accept the terms of service

from the welcome page, type in the URL and then next, this URL can be your company website.

Select Next to go to the next page.

Now your Captive Portal setup is complete, now your customer is able to connect to your guest network and get the welcome page.

For advance Setup and customization of the portal, please login to the Device GUI, from the Captive Portal menu.

Select Instance Configuration, you will notice the wizard created an Instance name called “wiz-cp-inst1” you can choose this name or create a new name for your Instance Configuration and then save. If you choose the “wiz-cp-inst1” the screen will take you to the Instance Configuration page.

You will notice that the setup wizard automatically associated captive portal instance name “ **wiz-cp-inst1**” to the Guest SSID you’re created during the setup wizard.

If you created the instance using the GUI, now you need to associate to the guest network you created.
From dropdown menu select the Instance Name “Guest”, or the instance that was created by the wizard “**wiz-cp-inst1**”.

From the menu select Web Portal Configuration to configure your guest welcome page, choose the instance name from the drop down menu.

Select the authentication method for Captive Portal to use to verify clients:

- Guest — The user does not need to be authenticated by a database.
- Local — The WAP device uses a local database to authenticated users.
- RADIUS — The WAP device uses a database on a remote RADIUS server to authenticate users.

If you choose verification method “Locale” then you need to create local users.

From the menu choose Local.

Enter the use parameter (name of the user), choose the parameters for the user profile.

Web Portal Page Customization, now you have the choice to upload your company logo and graphics you can upload up to 3 graphic files, one for the page background (Default cisco-bkg) second for the company logo (default, cisco-log) and third for the login screen (default, log-key).

** Please note the file size for this artwork file need to be 5KB.

Now you can customize your web portal page, like add Acceptance Use Policy, window title and name and so on…

Customized page with verification method as Guest, this means no need to authenticate, user will only need to accept the terms of service and select the Connect button, entering the user name is optional.

Customized page with verification method as Local this means user need to enter there user name and password to authenticate, and then user will need to accept the terms of service and select the Connect button.

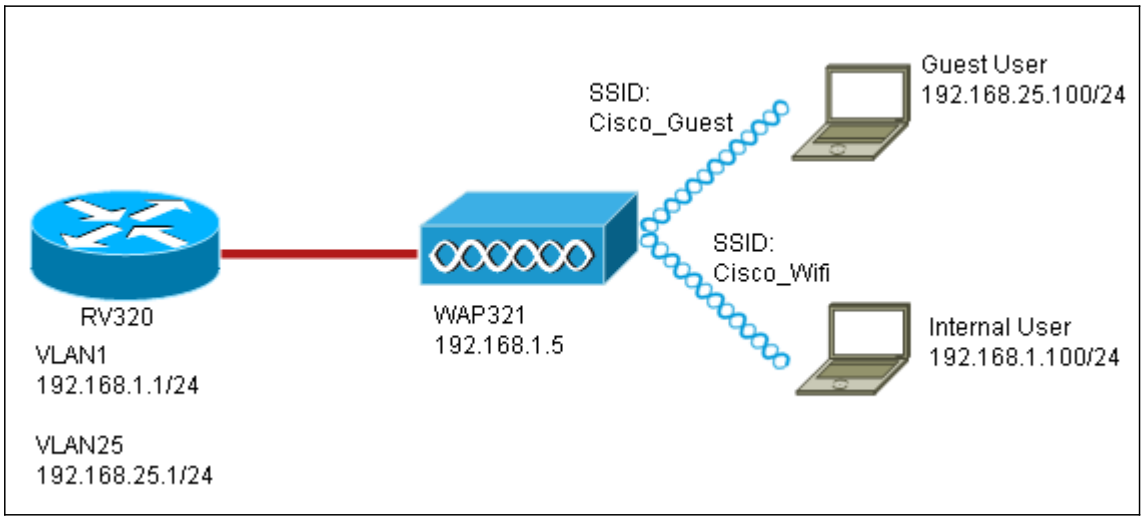
Captive Portal in a Multi-VLAN Environment

In some cases a network has need of multiple VLANs for different purposes, servicing

different groups of users. A common example is a separate network for Guest Users to prevent unauthorized users from accessing resources on the corporate network. Sometimes there are multiple wireless networks that need to be available to different users for the same reason. The WAP321 and WAP561 can meet these needs using the Captive Portal, but do require a bit of additional configuration on the network. This section will go over that configuration.

Intro – Existing Configuration

This document assumes that a network configuration is already in place. In this example, there are two networks, the main network and the guest network. The configuration to create and serve DHCP addresses to each network has already been configured. The WAP321 has already been configured to broadcast a different SSID for each network. The current setup will look like this:

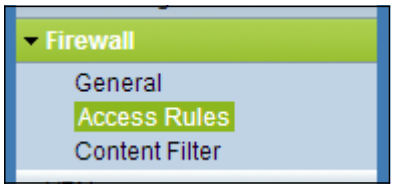


When the configuration is complete, InterVLAN routing will be enabled on the network so that all wireless clients can access the Captive Portal, enabling network connectivity.

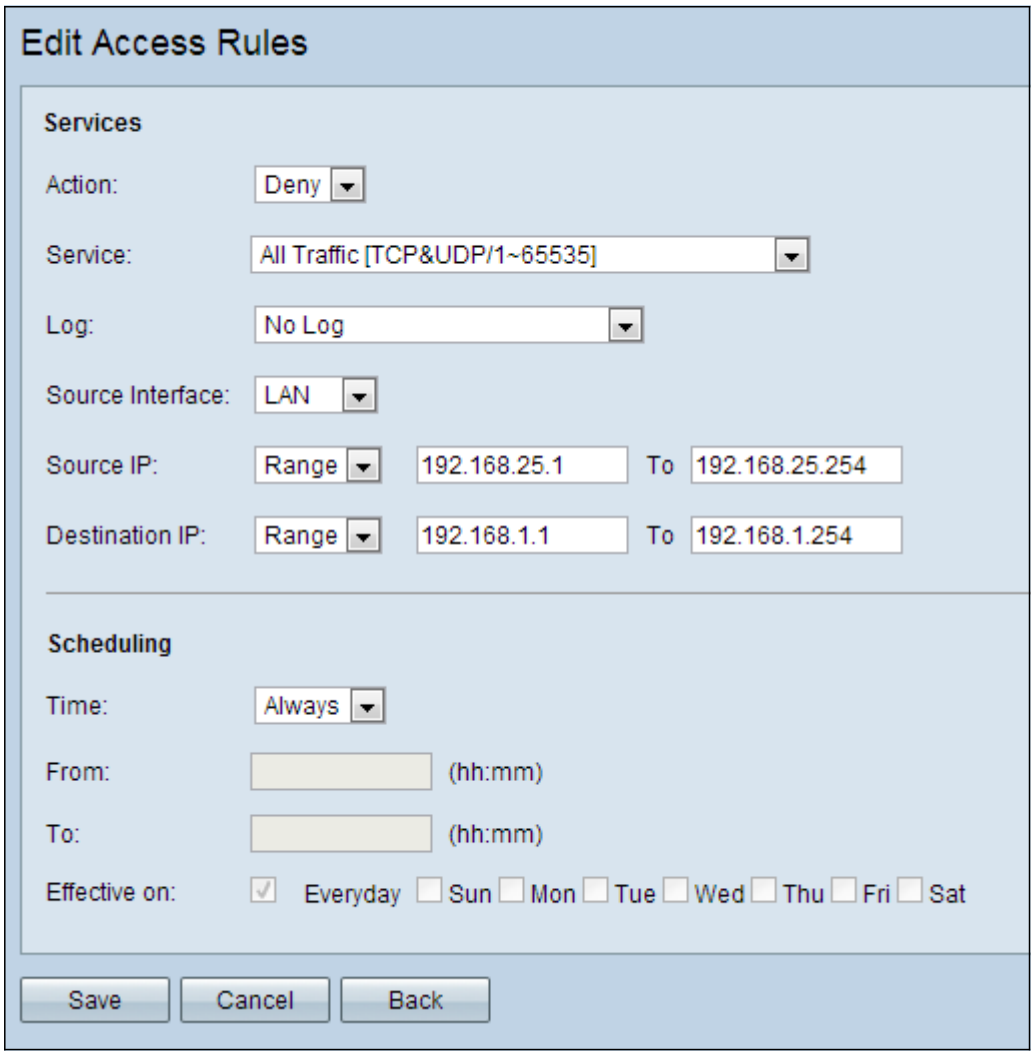
Configuration

First, enable interVLAN routing on the core router, in this case a RV320. To configure this go to Port Management > VLAN Membership to enable InterVLAN routing. Check both VLAN 1 and 25 on the left of the page and click Edit. In the InterVLAN Routing column, click on the dropdown box for each and select Enabled. Save the settings.

Now all users should be able to access the captive portal, but they can also access any resources on either the main VLAN or the Guest VLAN. To restrict access, configure an access control rule on the RV320. Go to Firewall > Access Rules in order to configure this restriction.



At the bottom of the page, click Add. We want to add a total of 2 access rules for our scenario. First, configure the rule denying access from the 192.168.25.x/24 guest subnet to the 192.168.1.x/24 internal subnet, as displayed to the right.



Click Save at the bottom of the page, then click back. Now add another rule, this time set the action as “Allow” and the destination IP as “Single.” Configure the rule to allow access from the 192.168.25.x/24 subnet to 192.168.1.5, which is currently configured to be the WAP321 static IP. This rule will be placed ahead of the deny rule we just created, allowing traffic to 192.168.1.5 from the guest network and nowhere else on the main network.

When you are finished the access rules page should look like this.

To configure captive portal in this setup, simply follow the steps from the first section for each network you need to configure the captive portal.

View a video related to this article...

Click here to view other Tech Talks from Cisco