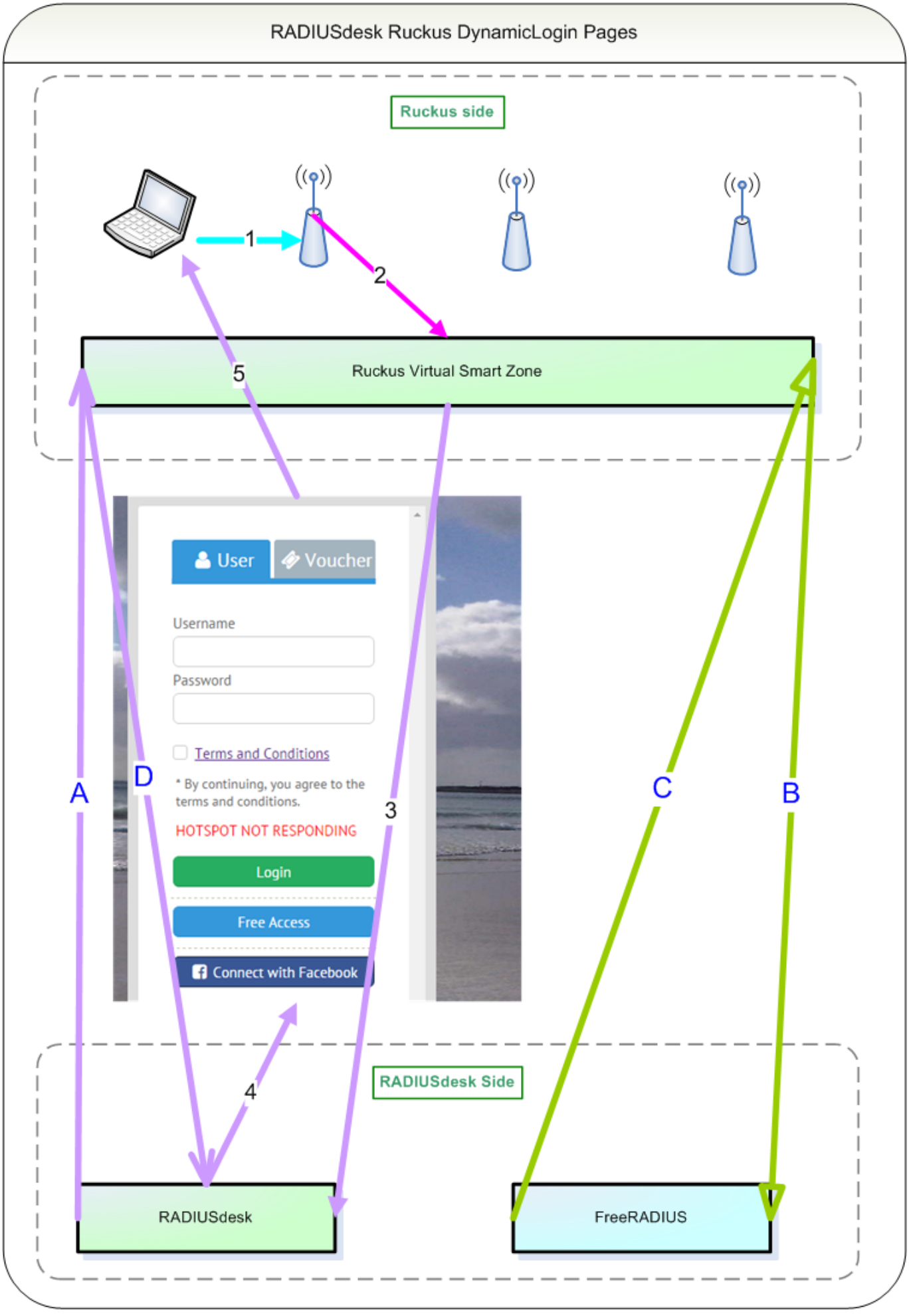
Dynamic Login Pages for Ruckus

- As of May 2016 the latest SVN of RADIUSdesk support three captive portals with its **Dynamic Login Pages**.
  - Mikrotik
  - CoovaChilli
  - Ruckus
- This page will go into more technical detail on the Ruckus implementation of the Dynamic Login Pages.

How does it work?

- Consider the following Visio diagram showing the login process. Afterwards we will discuss the various parts in the diagram.


RADIUSdesk Ruckus DynamicLogin Pages
Ruckus side
1
2
5
Ruckus Virtual Smart Zone
User
Voucher
Username
Password
Terms and Conditions
* By continuing, you agree to the terms and conditions.
HOTSPOT NOT RESPONDING
Login
Free Access
Connect with Facebook
A
D
3
C
B
4
RADIUSdesk Side
RADIUSdesk
FreeRADIUS

A User connecting to the Captive Portal

- **Step 1** A User connects to an SSID on the Access Point that is open and which terminates into a Captive Portal.
- **Step 2** The Access Point contacts the controller to determine which log-in page should be served to the user.
- **Step 3** In our case the controller is configured in such a way that the login page is served from the RADIUSdesk server.
- **Step 4** RADIUSdesk use components from the query string to determine how the page which is served to the user will look.
- **Step 5** The user sees a login page on his or her web browser.

A User that logs in on the Captive Portal

With this we assume the user provided valid credentials and clicked the submit button.

- **Step A** The submit button initialize a POST to the RADIUSdesk server. (Not shown in the diagram). Once this POST request is received by the RADIUSdesk server, the RADIUSdesk server in turn contacts the Ruckus Virtual Smart Zone to authenticate the user.
- This is another POST request between the RADIUSdesk server and the Ruckus Virtual Smart Zone using a well defined API and known shared secret between the two. The User never sees this shared secret, thus security is not compromised. This request can be either http or https.
- **Step B** The Ruckus Virtual Smart Zone sends an Auth request to the FreeRADIUS server using the RADIUS protocol.
- **Step C** The FreeRADIUS server replies with either an **Auth Accept** or **Auth Reject**. (If it is Accept the user will be allowed onto the Internet through the Access Point)
- **Step D** The Ruckus Virtual Smart Zone sends a reply to the RADIUSdesk server which in turn will reflect the result on the login page.

- Social Logins like Facebook, Twitter and Google use the same principle but log in twice, first with a temp user with a limited profile and after a successful social login the assiciated Voucher or Permanent user.
- See the pages on Social Logins for more details.

What to configure

- There are two important things to configure on the RADIUSdesk side
  - The shared secret (referred as the **Northbound Portal Interface Password** in Ruckus)
  - Associate the Login Page with some detail on the login URL that the Smart Zone creates on the user's browser.
- There are two important things to configure on the Smart Zone:
  - The **Northbound Portal Interface Password**.

- The Login Page.

RADIUSdesk -> Northbound Portal Interface Password

- Setting the shared secret or **Northbound Portal Interface Password**. This secret will be the same for all Smart Zone controlles which contact the RADIUSdesk server.
- Edit the **/usr/share/nginx/html/cake2/rd_cake/Config/DynamicLogin.php** file.

```
sudo vi /usr/share/nginx/html/cake2/rd_cake/Config/DynamicLogin.php
```

- Adjust the following value to your liking, keeping in mind it will also be set on the Smart Zone.

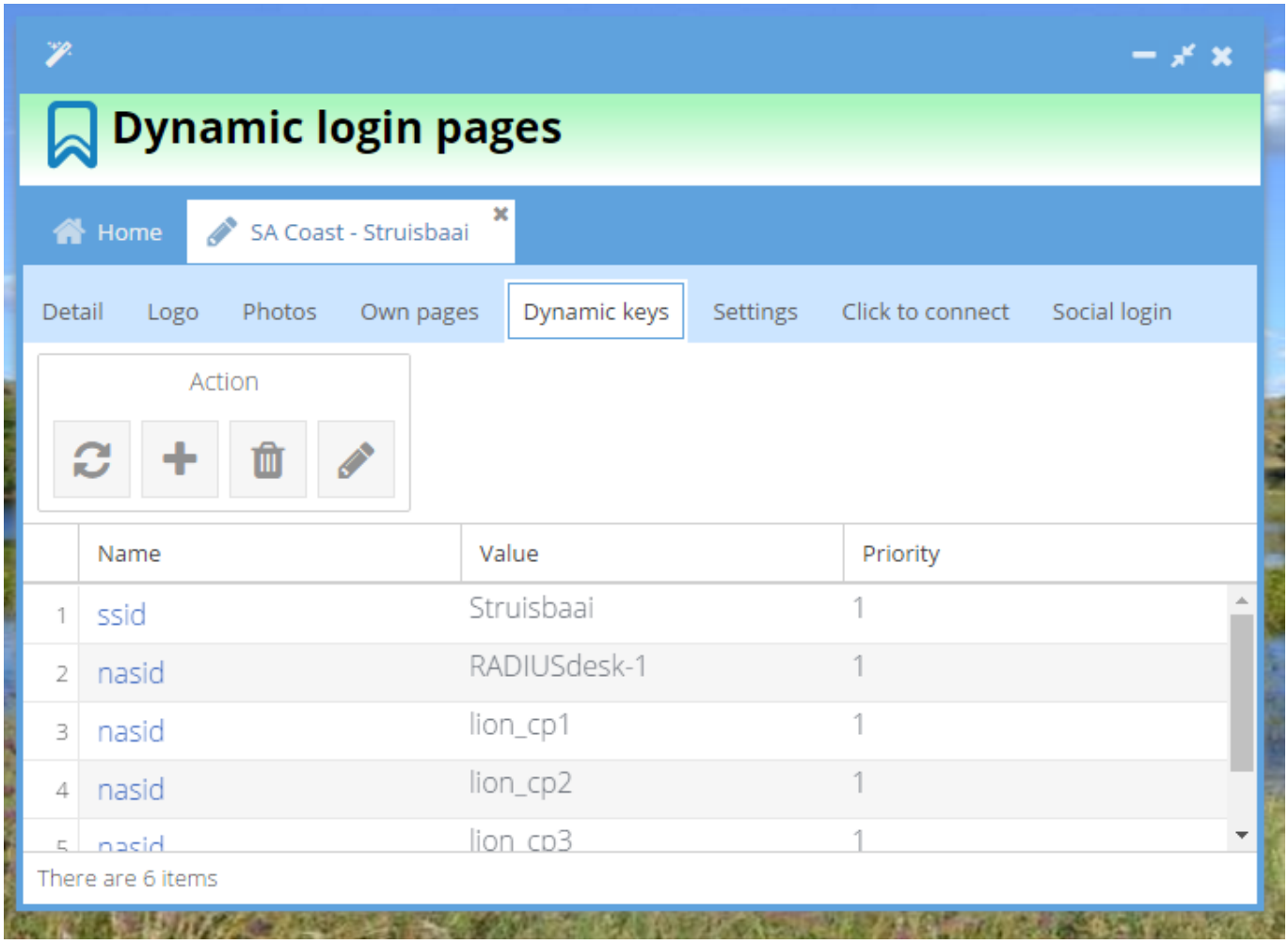
```
$config['DynamicLogin']['ruckus']['northbound']['password'] =
'stayoutnow123!';
```

RADIUSdesk -> Dynamic Login Page Association

- The Dynamic Login Pages knows what login page to serve by looking up pre-defined associations from the query string that the user's browser displayes.
- This query string is typically formulated by the Captive Portal (or the controller) and will look something like this:

http://rd01.wificity.asia/rd_login/ru/d/index.html?nbiIP=146.63.10.10&client_mac=ENC777773756677867868678376778678&sip=www.radiusdesk.com&wlan=100&reason=Un-Auth-Captive&proxy=0&wlanName=radiusdeskn&ssid=Struisbaai&mac=AA:AA:AA:AA:AA:AA&dn=www.radusdesk.com

- You then need to take one or more of these items in the query string and add it to the login page that you want to show to the user on that particular Access Point.
- Log onto RADIUSdesk. Open the Dynamic Login Page applet. Select the entry of your choice and edit it.
- Under the **Dynamic Keys** we added ssid ⇒ Struisbaai. See the following screenshot.



- This way we can use the same Dynamic Login Page to serve Mikrotik, CoovaChilli or Ruckus captive portals, and it will look exactly the same on all of them!

Rukus setup

- We are not going to repeat the info from the Rukus tech note. There are however just one bit of information from this page that you will need.
- Under **Hotspot Service** you need to specify a login page. Replace the IP / Hostname with that of your RADIUSdesk server.

http://rd01.wificity.asia/cake2/rd_cake/dynamic_details/ruckus_browser_detect.html