# How to setup a Captive Portal using a webform

Version 1.0

PAN-OS 5.0.1

Johan Loos

johan@accessdenied.be

The captive portal is a method to authenticate the user before she can access resources in another zone. This scenario can be used if you want to present the user with a web form login page. User access is limited by an expiration timer (default 60 min) or an idle timer (default 15 min). When one of these timers expires, the user needs to re-authenticate.

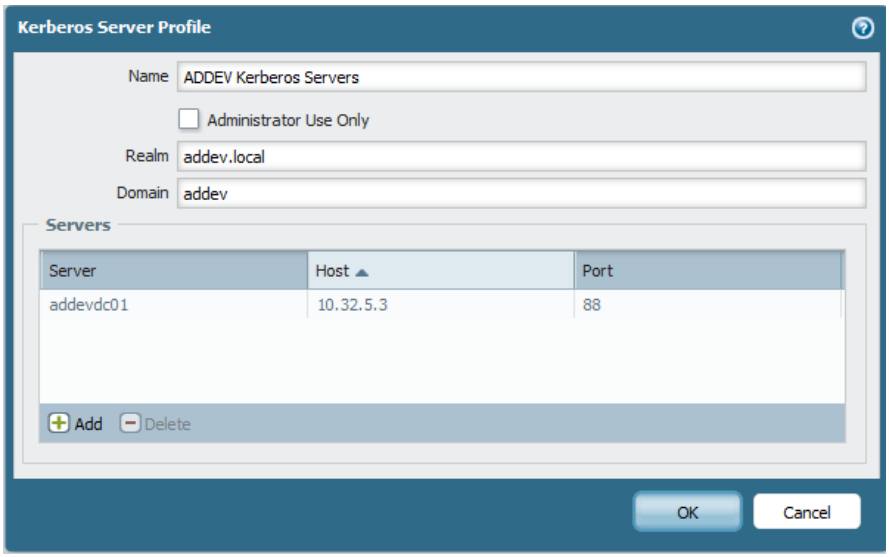
A captive portal can also be used for guests who need limited access to the Internet.

## Setup a captive Portal using a web form Task List

- △ Create a Server Profile
- △ Create an Authentication Profile
- △ Configure a Captive Portal
- △ Configure Captive Portal Settings
- △ Configure a Response Page
- △ Test
- △ Findings

### Configure a Server Profile

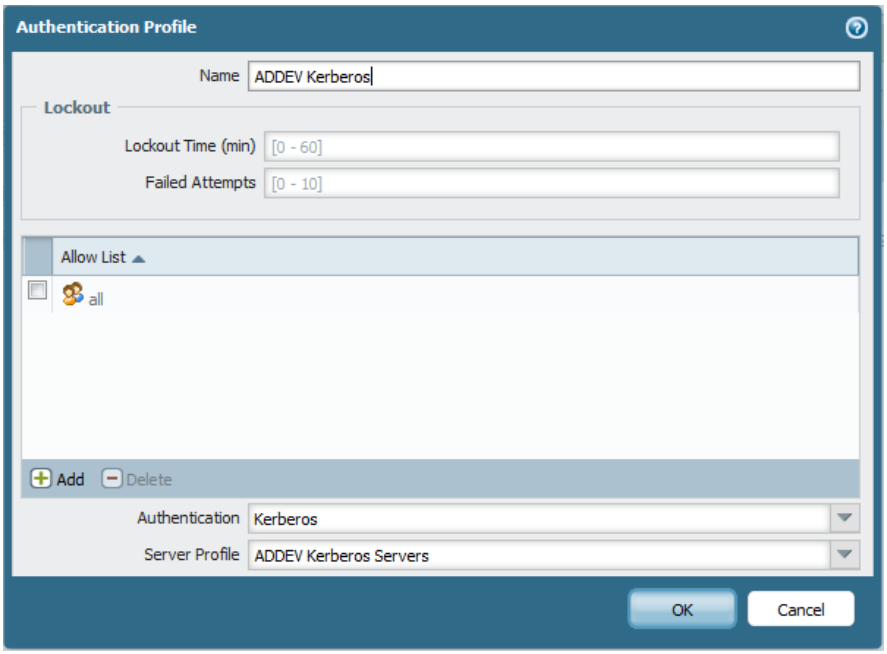
- Navigate to **Device | Server Profiles | Kerberos**, click **Add**
- On the **Kerberos Server Profile** page, type a name for your profile, type a realm (FQDN of your domain), domain (NETBIOS name), click **Add** to add your domain controllers to the list




- Click **OK**

### Create an Authentication Profile

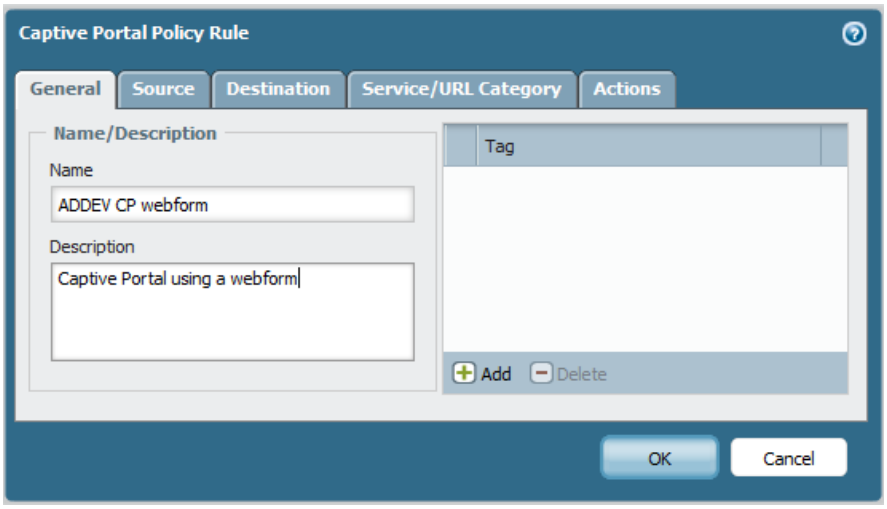
- Navigate to **Device | Authentication Profile**, click **Add**
- On the **Authentication Profile** page, type a name for your profile, select **Kerberos as Authentication**, and select your **Server Profile** you have created before



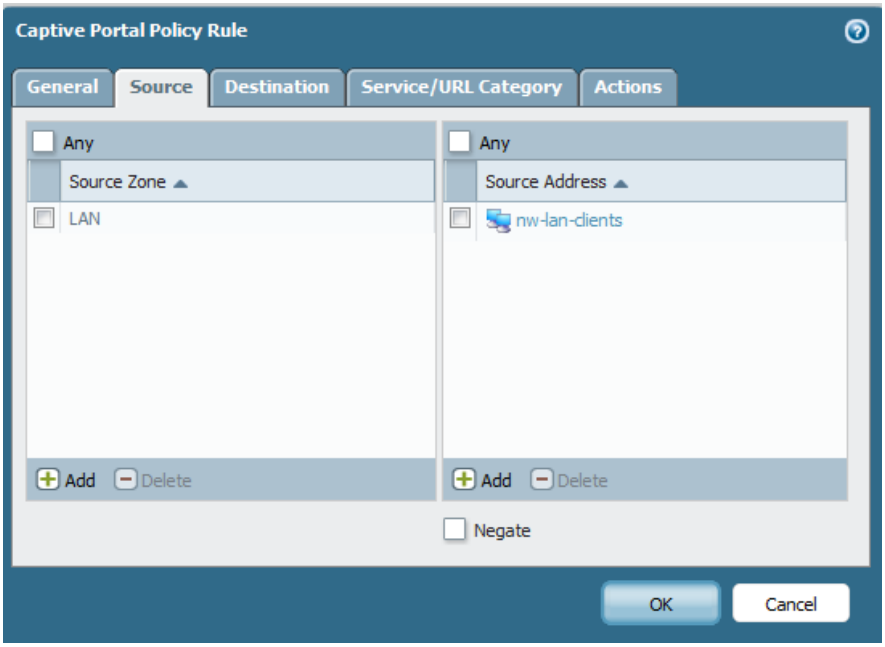

- Click **OK**

## Configure a Captive Portal

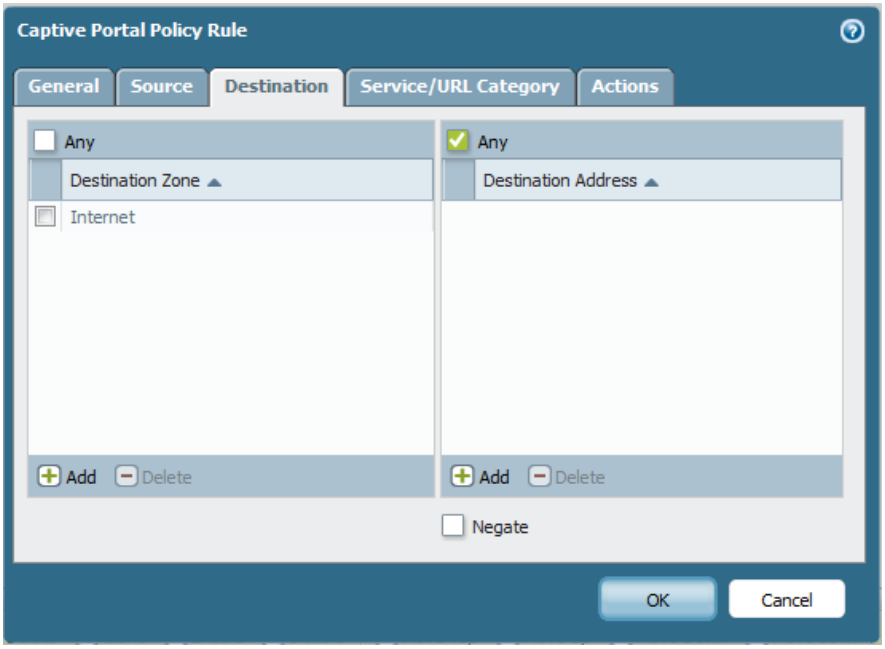
- Navigate to **Policies | Captive Portal**, click **Add**
- On the **Captive Portal Policy Rule** page, on the **General** page, type a name for your Captive Portal



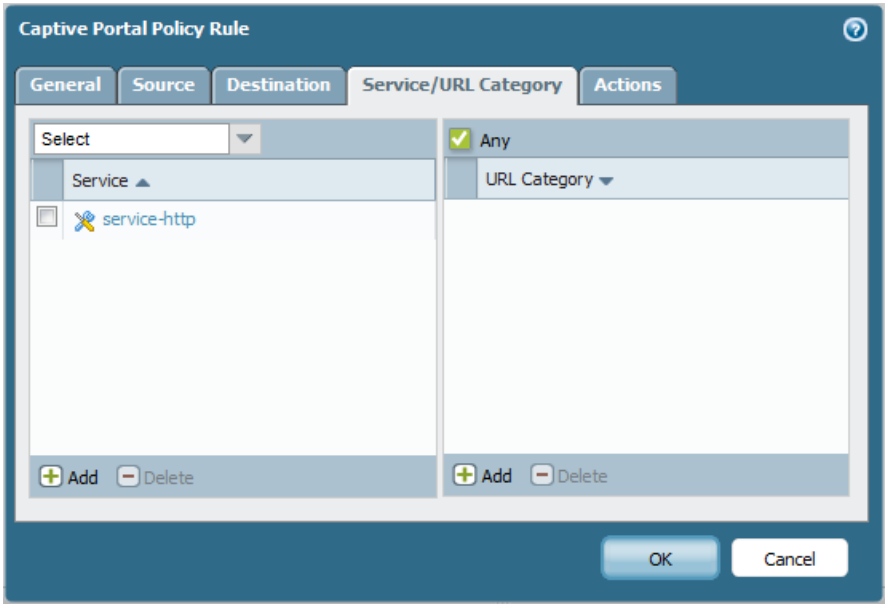

- On **Source** page, select a Source Zone and Source Address



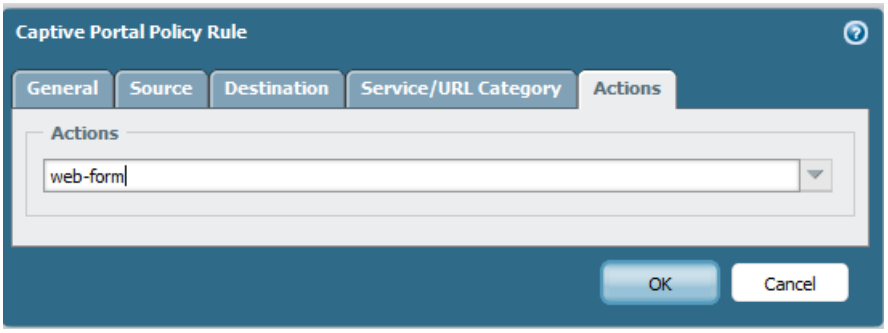

- On **Destination** page, select a Destination Zone and Destination Address




- On **Service/URL Category** page, accept or add a service, or specify a URL category



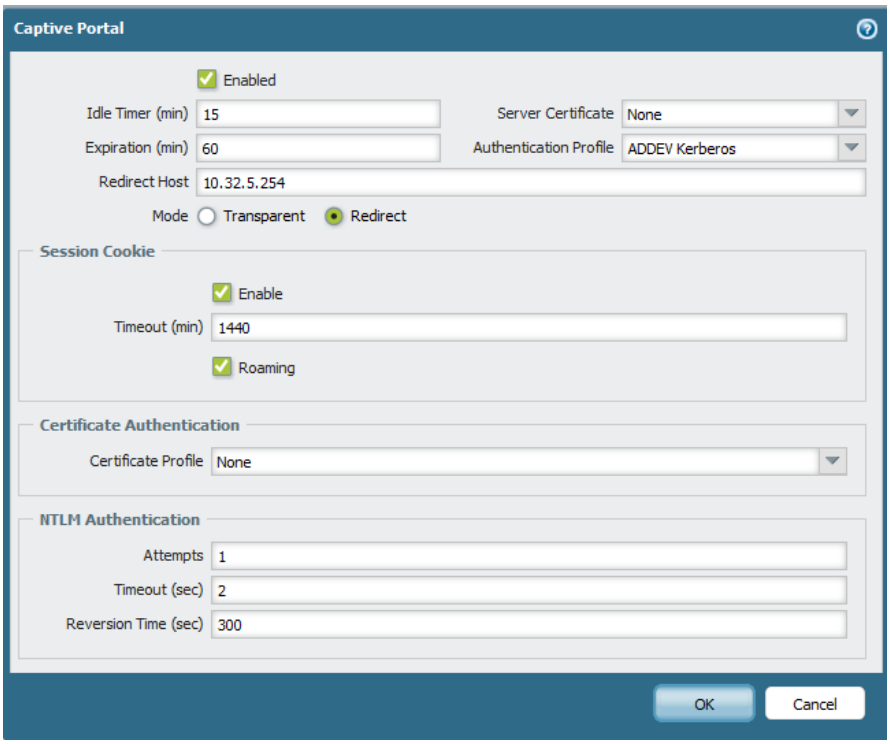

- On **Actions** page, select web-form




- Click **OK**

## Configure Captive Portal Settings

- Navigate to **Device | User Identification | Captive Portal Settings** and click **Edit**
- On the **Captive Portal** page, select an authentication profile, and select **Redirect** as mode
- In the **Redirect Host** field, type the IP address of the Ethernet interface you want to use captive portal on. In my case it is the IP address of the interface which belongs to the LAN zone
- On **Session Cookie** select **Enable**, **Roaming** and define a **Timeout**
- When you enable Roaming and the IP address of the client changes, re-authentication is not performed. When you specify a session cookie timeout, the user needs to re-authenticate again

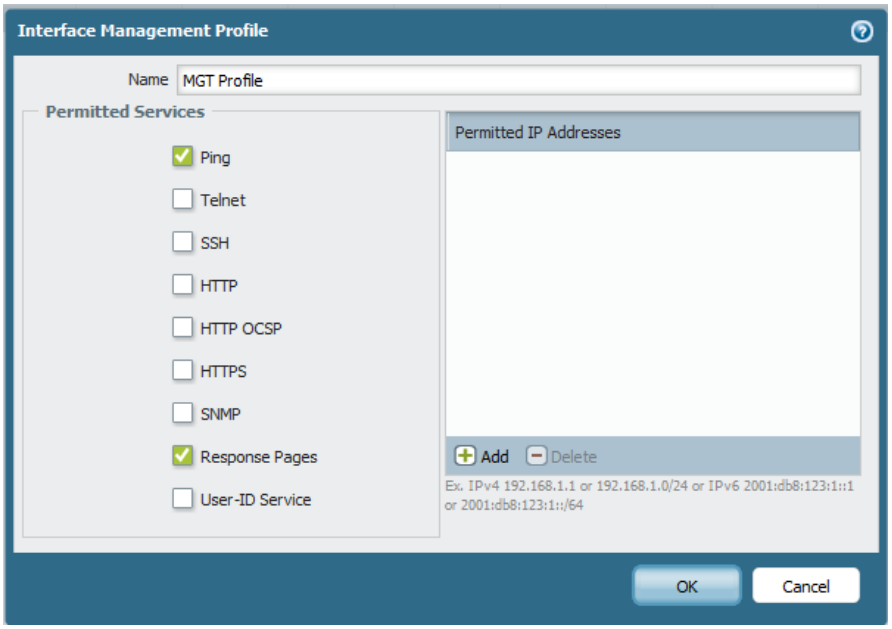



- Click **OK**

## Configure a Response Page

When you assigned an Interface Management Profile on your interface where your captive portal is listening on, you have to select Response Pages under Permitted Services.

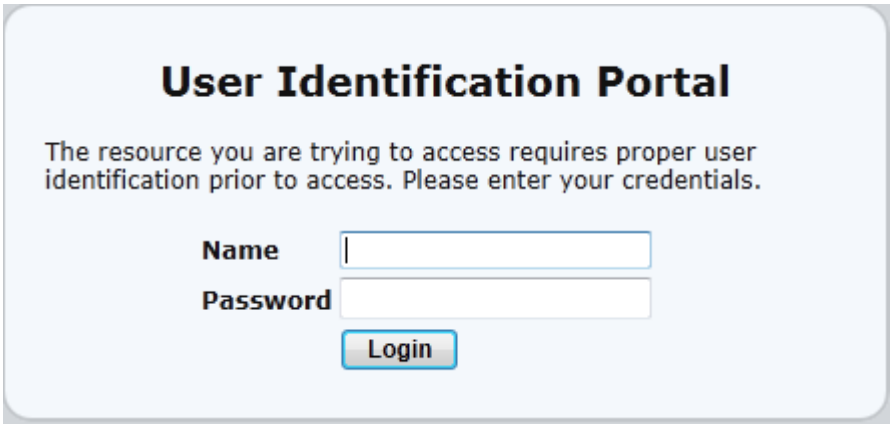
- Navigate to **Network | Network Profiles | Interface Mgmt**, select your management profile and select **Response Pages**



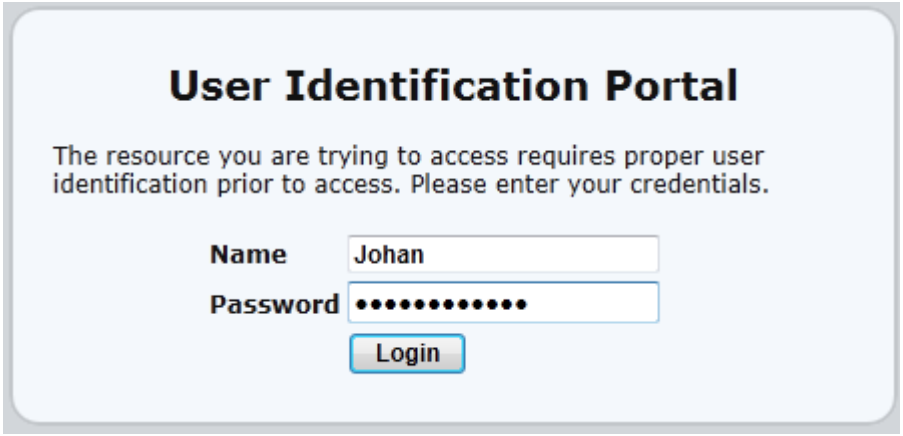

- Click **OK**

## Test

- From a client computer open a web browser and type a URL. Your Palo Alto will intercept this traffic and prompt the user to login




- Enter your domain credentials and click **Login**




- After successful login, the user is allowed access to the website
- On your Palo Alto firewall, you can view the session

```
admin@PA-VM> show user ip-user-mapping all

IP             Vsys   From    User                            IdleTimeout(s) MaxTimeout(s)
-------------- ------ ------- ------------------------------- -------------- -------------
10.32.5.52     vsys1  CP      addev\johan                     638            3338
Total: 1 users

admin@PA-VM>
```

## Findings

When the currently logged on user account logs off and another user logs on to the same workstation, the user is granted access. This because the session is still active on the firewall and the second user will use the existing session from the previous authenticated user. The workstation has the same IP address for both users.