

Configuration pfSense

UAuth : Portail captif dans le Cloud

Entr'ouvert SCOP – <http://www.entrouvert.com>

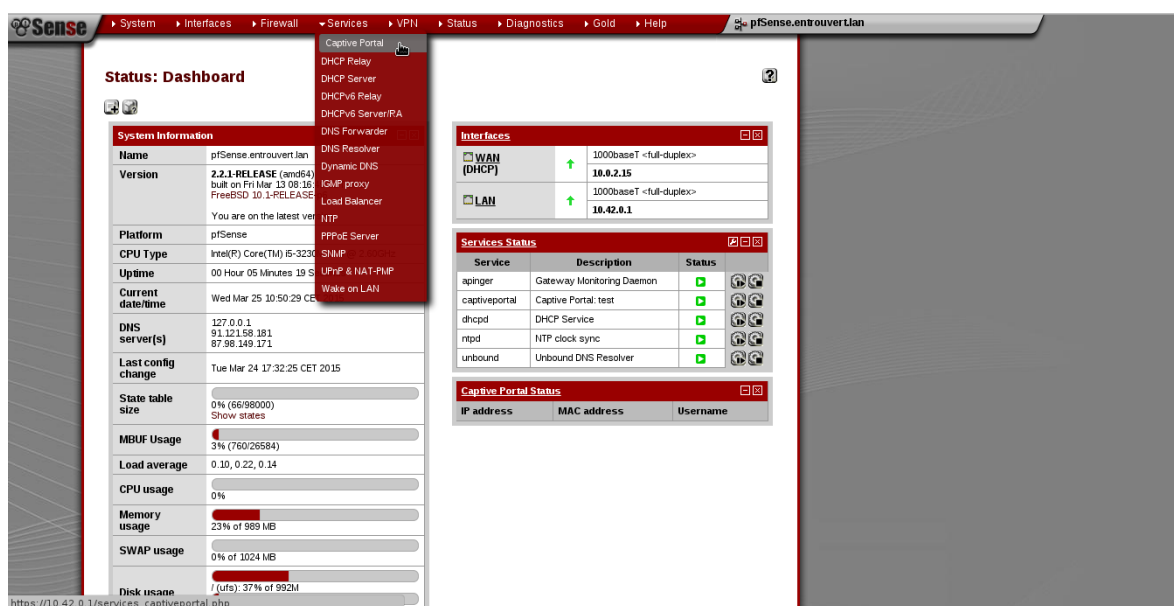
Table des matières

- 1 Configuration d'un portail captif pfSense 1
- 2 Test d'authentification 5

Ce document spécifie les étapes de configuration d'un portail captif pfSense pour son raccordement à la plateforme U-Auth.

1 Configuration d'un portail captif pfSense

Dans le menu **Services/Captive Portal**



ajouter une nouvelle zone :

The screenshot shows the 'Services: Captive portal: Edit Zones' configuration page in pfSense. The page has a red header with navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Edit Captive Portal Zones' and contains two input fields: 'Zone name' with the value 'eduspot' and 'Description' which is empty. Below the fields is a 'Continue' button.

Configurer la zone ainsi créée :

1. activer la zone :

The screenshot shows the 'Captive portal(s)' configuration page in pfSense. The page has a red header with navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Captive portal(s)' and contains several tabs: MAC, Allowed IP addresses, Allowed Hostnames, Vouchers, and File Manager. The 'Enable captive portal' checkbox is checked. The 'Interfaces' dropdown menu is set to 'WAN'. The 'Maximum concurrent connections' field is set to '0' (no limit). The 'Idle timeout' field is set to '0' minutes.

2. configurer l'URL de redirection vers le page de connexion U-Auth :

The screenshot shows the 'Captive portal(s)' configuration page in pfSense, specifically the 'Pre-authentication redirect URL' section. The page has a red header with navigation tabs: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Gold, and Help. The main content area is titled 'Captive portal(s)' and contains several tabs: MAC, Allowed IP addresses, Allowed Hostnames, Vouchers, and File Manager. The 'Pre-authentication redirect URL' field is set to 'https://u-auth.dev.entrouvert.org/pfsense-example'. The 'After authentication Redirection URL' field is empty. The 'Blocked MAC address redirect URL' field is empty.

3. configurer l'authentification Radius :

- protocole d'authentification : PAP
- adresse IP du serveur U-Auth : 176.31.146.80
- secret partagé : testing123

pfSense.entrouvert.lan

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Authentication

☐ No Authentication

☐ Local User Manager / Vouchers

☒ RADIUS Authentication

☒ Allow only users/groups with 'Captive portal login' privilege set

RADIUS Protocol

☒ PAP

☐ CHAP_MD5

☐ MSCHAPv1

☐ MSCHAPv2

Primary Authentication Source

Primary RADIUS server

IP address: 176.31.146.80
Enter the IP address of the RADIUS server which users of the captive portal have to authenticate against.

Port:
Leave this field blank to use the default port (1812).

Shared secret: testing123
Leave this field blank to not use a RADIUS shared secret (not recommended).

4. définir un nom local pour le portail captif :

pfSense.entrouvert.lan

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

HTTPS login

☒ Enable HTTPS login
If enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name: pfsense.example.org
This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL Certificate: webConfigurator default (54f0a0b99b5d6)

5. desactiver le HTTPS Forwards

pfSense.entrouvert.lan

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

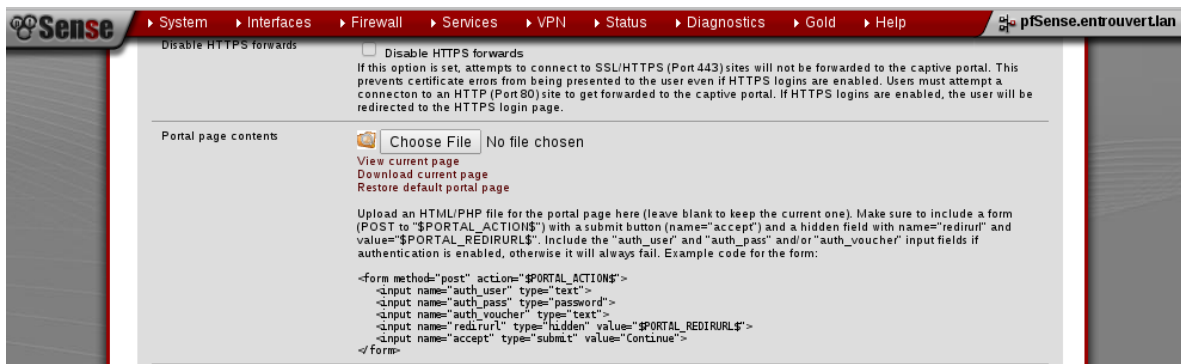
HTTPS server name: pfsense.example.org
This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in your certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL Certificate: webConfigurator default (54f0a0b99b5d6)

Disable HTTPS forwards

☒ Disable HTTPS forwards
If this option is set, attempts to connect to SSL/HTTPS (Port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

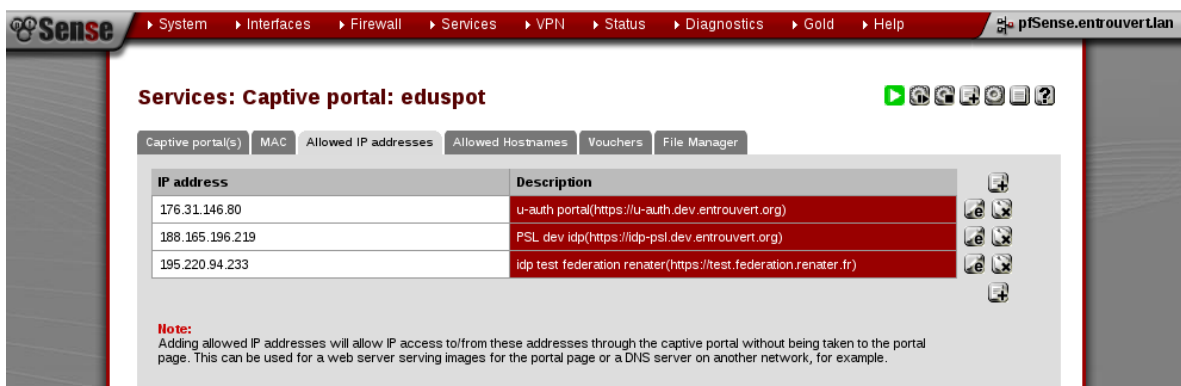
6. personnaliser la page d'authentification du portail captif en chargeant un fichier html contenant obligatoirement la variable \$PORTAL_REDIRECTURL\$:



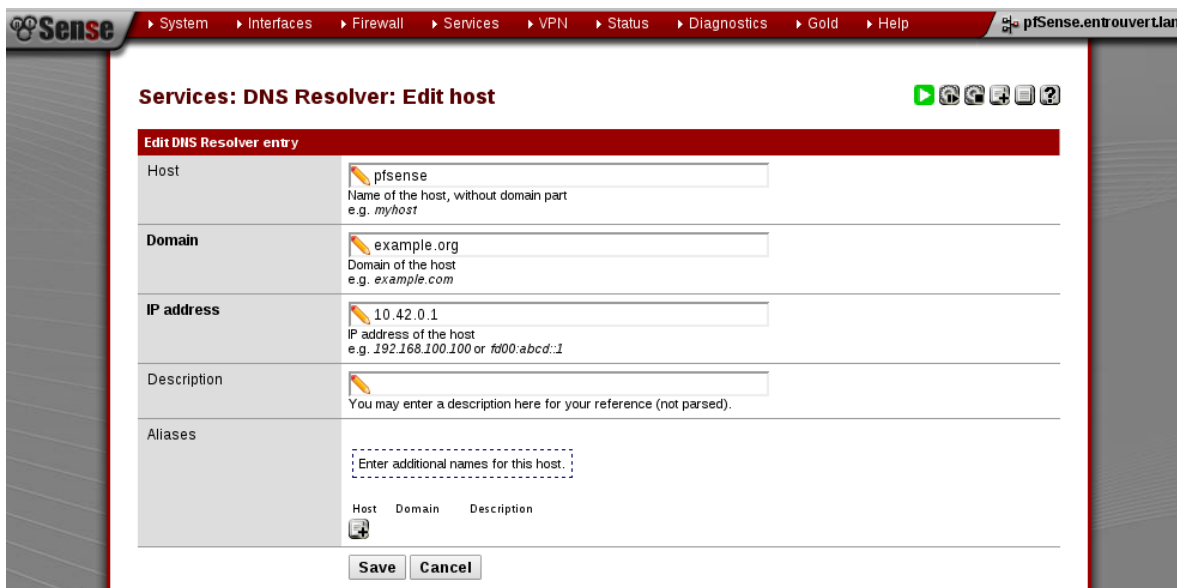
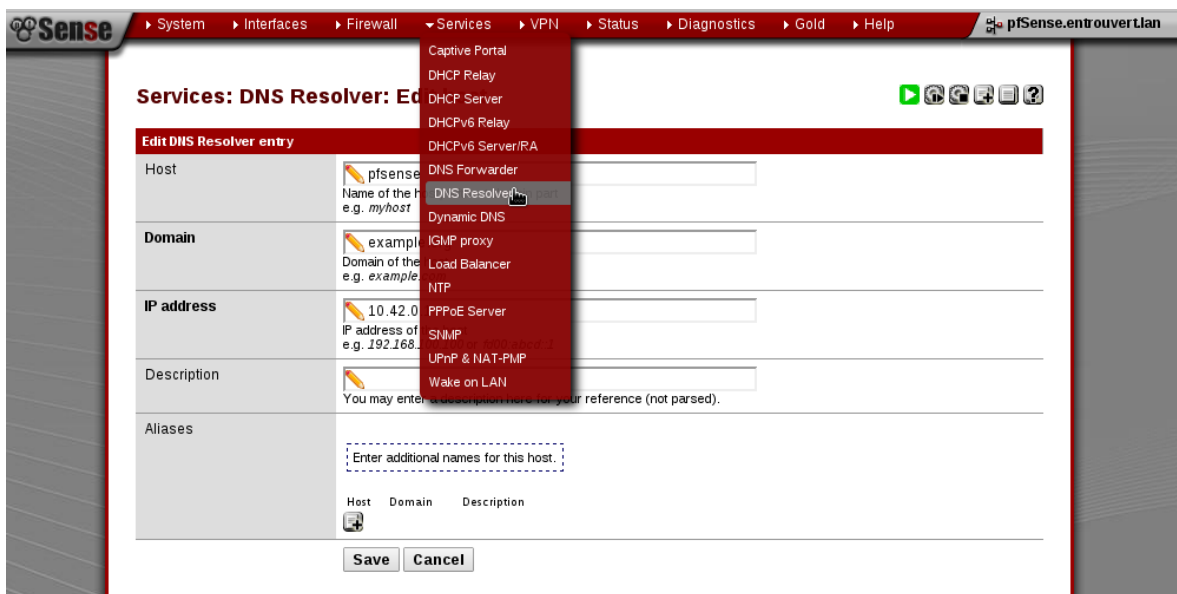
Exemple de fichier :

```
<html>
  <head>
    <title>You are being redirected to authentication page</title>
  </head>
  <body>
    <h3>You are being redirected to authentication page</h3>
    <p>If you are not redirected, please
    <a id="redirect" href="$PORTAL_REDIRURL$">click here</a></p>
    <script type="text/javascript">
      var redir = document.getElementById('redirect');
      redir.href += window.location.search;
      window.location.href="$PORTAL_REDIRURL$" + window.location.search;
    </script>
  </body>
</html>
```

7. Autoriser le portail captif à accéder à U-Auth et les fournisseurs d'identité de la fédération :

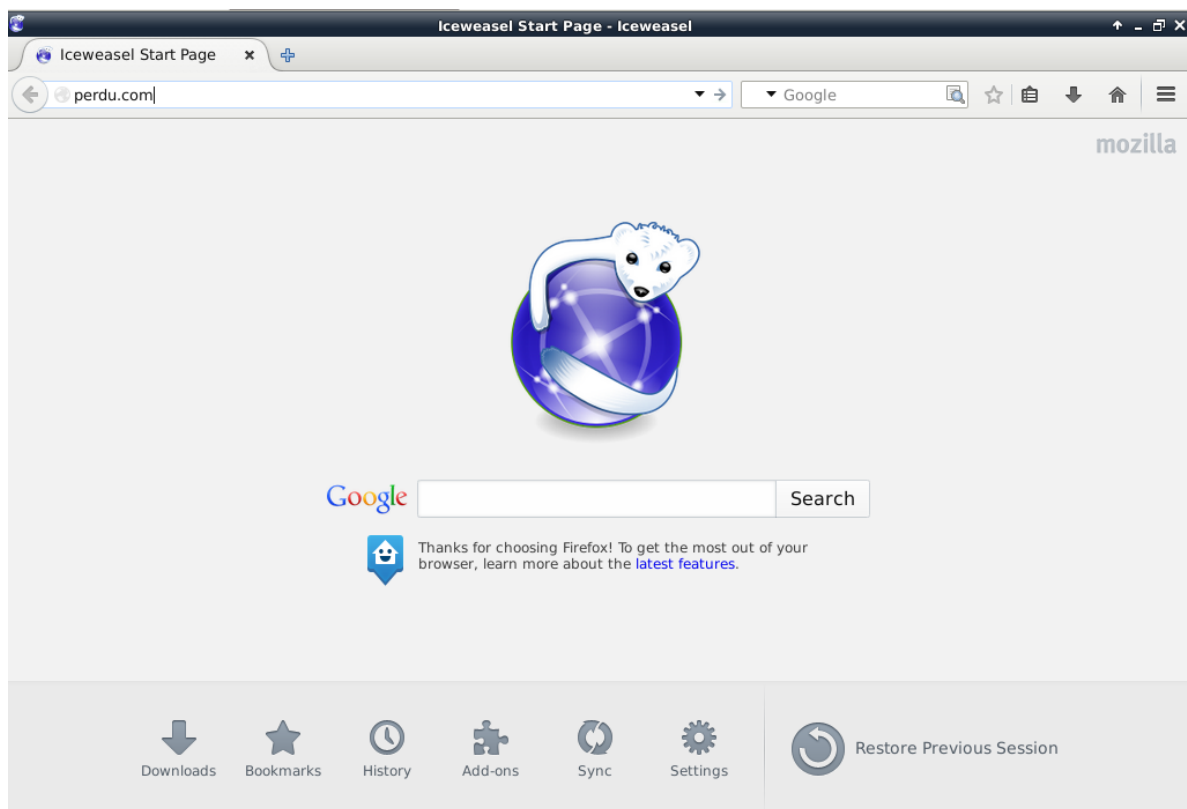


8. Dans le resolver DNS local rajouter le nom et l'adresse locale du portail captif :

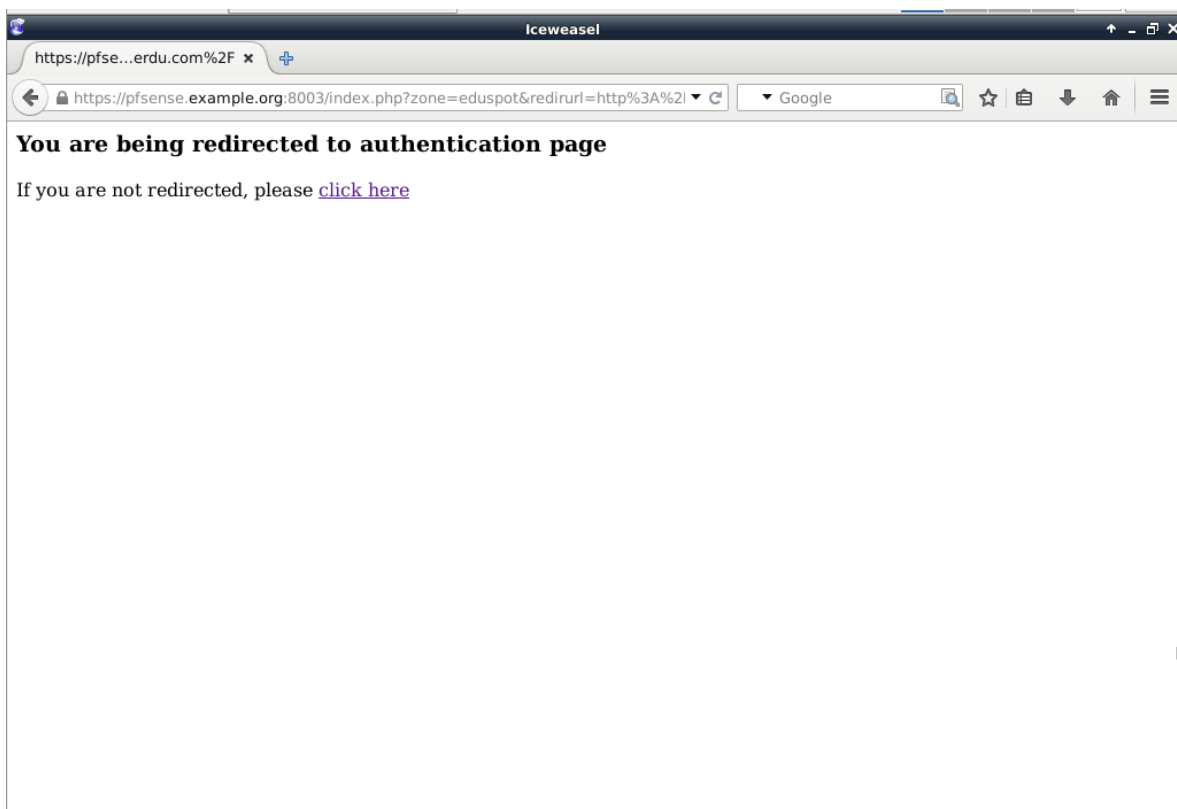


2 Test d'authentification

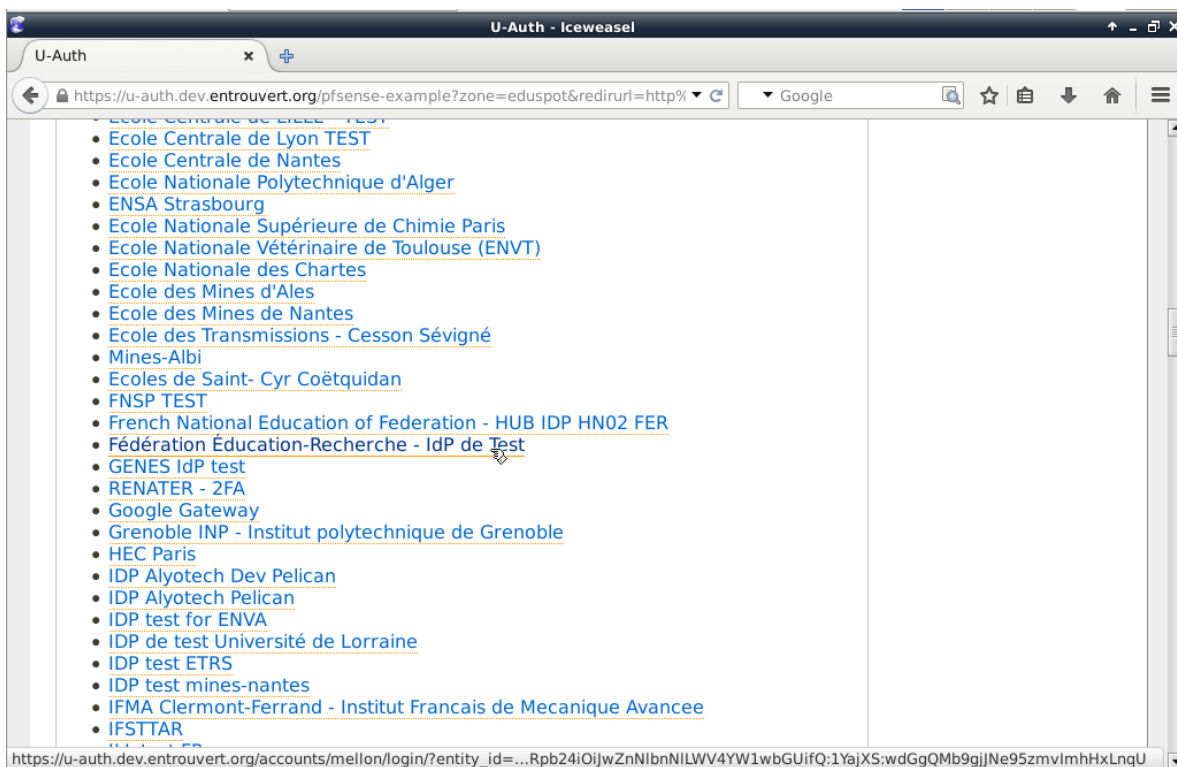
Depuis un poste interne au réseau du portail captif aller sur une page (par exemple <http://perdu.com>) :



La page personnalisée, redirigeant vers U-Auth, sera affichée :



Si l'accès à la plateforme U-Auth a été bien autorisée au niveau du portail captif, la page de votre organisme avec la liste des fournisseurs d'identité sera affichée :



En choisissant un fournisseur d'identité, également autorisé au niveau du portail captif, la mire de connexion est affichée :

