Compatibilité U-Auth

pfSense 2.2

- config radius
  - NAS-Identifier == "client"
- login déporté via un redirect "meta", vers une page de ce format :

```
<form method="post" action="https://pfsense.entrouvert.lan:8003/index.php">
   <input name="auth_user" type="text">
   <input name="auth_pass" type="password">
   <input name="auth_voucher" type="text">
   <input name="redirurl" type="hidden" value="http://perdu.com">
   <input name="accept" type="submit" value="Continue">
</form>
```

  - IP du serveur https distant à ajouter dans la whitelist
- et ça marche "aussitôt"

Meraki

- config radius
  - aucune configuration fine possible, tout est pré-cablé (PAP, NAS-Identifier = Cisco truc...)
  - l'interrogation radius comportera le "called-id" = mac de l'access point + ssid : c'est à partir de cela qu'il faudra trouver le client=....?
- la page "splash" du portail captif est une redirection, par exemple https://u-auth.eu/meraki/
  - url appelée sera : https://u-auth.eu/meraki/?login_url=https%3A%2F%2Fn57.network-auth.com%2Fsplash%2Flogin%3Fmauth%3DMMhmRGnVuWeblQgRcsPFUq1snIL5PRogX3kzOeOfA0pv1LFVI5XCa_clISe2lebARNQ7EVcSk8p31yt6iOvvlASOSTvbUJApF_u0B7B7xoPrd19tZeqZfjglRLC9Rdn58iJ8q_q4VGcyH4nkxcQUZXZwAk83WeFo2I9xchcATju89924sVyUTiog%26continue_url%3Dhttp%253A%252F%252Fwww.entrouvert.com%252F&continue_url=http%3A%2F%2Fwww.entrouvert.com%2F&ap_mac=00%3A18%3A0a%3A38%3A01%3Af0&ap_name=&ap_tags=&client_mac=c4%3A85%3A08%3Aa4%3Ab5%3Ae6&client_ip=10.94.69.36
    - login_url=https%3A%2F%2Fn57.network-auth.com%2Fsplash%2Flogin%3Fmauth%3DMMhmRGnVuWeblQgRcsPFUq1snIL5PRogX3kzOeOfA0pv1LFVI5XCa_clISe2lebARNQ7EVcSk8p31yt6iOvvlASOSTvbUJApF_u0B7B7xoPrd19tZeqZfjglRLC9Rdn58iJ8q_q4VGcyH4nkxcQUZXZwAk83WeFo2I9xchcATju89924sVyUTiog%26continue_url%3Dhttp%253A%252F%252Fwww.entrouvert.com%252F&continue_url=http%3A%2F%2Fwww.entrouvert.com%2F
    - ap_mac=00%3A18%3A0a%3A38%3A01%3Af0
    - ap_name=
    - ap_tags=
    - client_mac=c4%3A85%3A08%3Aa4%3Ab5%3Ae6
    - client_ip=10.94.69.36
- en cours : recherche doc sur création du POST ou du GET à renvoyer

PacketFence 4

Architecture

U-Auth est une application web, fournisseur de service de la fédération Renater. U-Auth affiche les IdP de la fédération et propose à l'utilisateur de lancer le SSO sur l'IdP de son choix.

U-Auth pilote un serveur LDAP. Un compte aléatoire est créé pour chaque utilisateur dès qu'il réussi son authentification via un IdP de la fédération.

Un serveur Radius est configuré pour diffuser les identités du serveur LDAP.

Le portail captif qui désire utiliser U-Auth est configuré pour :

- afficher la page de connexion de U-Auth à la place de la sienne (redirection HTTP, ou sinon dans le HTML)
- utiliser le serveur radius.

Une fois la connexion réussie et le compte LDAP crée, U-Auth envoie les données de connexion au portail captif (par un POST via le client wifi).

Le portail captif interroge alors le radius avec les données du compte. Radius vérifie l'information sur le LDAP et confirme l'accès au portail captif.

Pré-requis sur le portail captif (intégré ou non au contrôleur)

Cette architecture implique que le portail captif de départ sache faire de l'UAM (https://en.wikipedia.org/wiki/Universal_access_method) :

- rediriger sa page d'accueil de login vers une URL externe (redirect HTTP, sinon redirection dans le HTML (meta http-equiv="Refresh") voire javascript)
- accepter un POST login + mot de passe

Exemples de portails captifs UAM : PacketFence, Cisco Meraki, pfSense, … Si vous avec un portail captif et que vous désirez savoir s'il est compatible U-Auth (UAM), contactez Entr'ouvert.

Cinématique

Error executing the **plantuml** macro (Missing partial wiki_external_filter/_macro_image with {:locale=>[:fr, :en], :formats=>[:pdf], :variants=>[], :handlers=>[:raw, :erb, :html, :builder, :ruby, :rsb]}. Searched in: * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/wiki_external_filter/app/views" * "/usr/share/redmine/plugins/redmine_tags/app/views" * "/usr/share/redmine/plugins/redmine_entrouvert/app/views" * "/usr/share/redmine/plugins/plantuml/app/views" * "/usr/share/redmine/plugins/localizable/app/views" * "/usr/share/redmine/app/views")

Notes

- L'utilisation d'un LDAP permet d'utiliser un portail captif utilisant des comptes LDAP au lieu de radius.
- Les comptes invités sont des comptes directement gérés dans U-Auth.

Backoffice pour un site (un établissement)

Un site (typiquement, un établissement) qui utilise U-Auth, dispose d'un accès à un backoffice dédié pour :

- indiquer les IdP qu'il veut utiliser parmi ceux de la fédération (accès "administrateur du site")
- gérer des comptes invités (accès "gestionnaire d'invités")
- modifier des éléments de présentation de la page d'accueil (logotypes, textes, css, ...)

Système d'administration

Le "super administration" d'U-Auth crée les site et les comptes backoffice correspondants.

Parametrage

Parametrage

Tips: http://blog.clemanet.com/freeradius-et-openldap/

Installation freeradius et openldap

```
 # apt-get install freeradius freeradius-ldap slapd ldap-utils
```

Ajout du schema radius dans le ldap

```
# cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/radius.schema
# echo "include /etc/ldap/schema/radius.schema" > /tmp/schema-convert
# mkdir /tmp/ldap_schema && slaptest -f /tmp/schema-convert -F /tmp/ldap_schema
```

Ouvrir le fichier /tmp/ldap_schema/cn=config/cn=schema/cn={0}radius.ldif et remplacer:

```
  dn: cn={0}radius
    objectClass: olcSchemaConfig
    cn: {0}radius
```

par:

```
  dn: cn=radius,cn=schema,cn=config
    objectClass: olcSchemaConfig
    cn: radius
```

Puis supprimer les lignes suivantes à la fin du fichier:

```
  structuralObjectClass: olcSchemaConfig
  entryUUID: d3f8dbfa-297a-1031-9222-176c711ae4e0
  creatorsName: cn=config
  createTimestamp: 20120503144845Z
  entryCSN: 20120503144845.283270Z#000000#000#000000
  modifiersName: cn=config
  modifyTimestamp: 20120503144845Z

# ldapadd -Y EXTERNAL -H ldapi:/// -f /tmp/ldap_schema/cn\=config/cn\=schema/cn\=\{0\}radius.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=radius,cn=schema,cn=config"
```

Configuration du module ldap

Editer /etc/freeradius/modules/ldap

```
server = "127.0.0.1"
  identity = "cn=admin,dc=entrouvert,dc=org"
  password = motdepassecomplique
  basedn = "dc=entrouvert,dc=org"
  filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
  dictionary_mapping = ${confdir}/ldap.attrmap
```

Activation de ldap pour l'authentification

Dans le fichier /etc/freeradius/sites-available/default:

```
Section authorize {
    ...
    ldap
    ...
    }
```

puis

```
authenticate {
    ...
        Auth-Type LDAP {
            ldap
        }
    ...
    }
```

Tester la connexion

Arrêter le serveur:

```
   # service freeradius stop
```

Lancer le serveur en mode debug:

```
# freeradius -X
```

Vérifier si le serveur répond bien:

```
radtest <user> <passwd> 127.0.0.1 1 testing123
```

par exemple:

```
# radtest 99c543e03c1649de87de47044c86cce3 fef3db94593e4944a8b2cf103b890ea8  127.0.0.1 1 testing12
3
Sending Access-Request of id 98 to 127.0.0.1 port 1812
    User-Name = "99c543e03c1649de87de47044c86cce3"
    User-Password = "fef3db94593e4944a8b2cf103b890ea8"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 1
    Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=98, length=20
```