Carte de France pour UnivNautes

Design : http://perso.entrouvert.org/~thomas/univnautes/

Aspects techniques

Installation d'un proxy local sur UnivNautes via modif de la config de lighty :

- mod_proxy
- redirection vers le proxy :

```
     url.rewrite-once = (
+        "^/proxymap(/.*)$" => "$1",
         "^(/.*)$" => "/pffedportal.fcgi$1",
     )
```

- proxy lui-même :

```
+    proxy.server = (
+        "/" => ((
+                    "host" => "A.B.C.D",   # obligatoirement une IP
+        ))
+    )
```

Note : lighttpd ne sait pas modifier le nom d'hôte interrogé, qui sera donc celui du portail captif ! (par exemple eduspot.univ-truc.fr). Sur A.B.C.D il faut donc un serveur HTTP pour n'importe quel nom :

```
# machine A.B.C.D /etc/apache2/site-enabled/000-default
<VirtualHost *:80>
        ServerAdmin webmaster@entrouvert.com

        DocumentRoot /var/www/tile

        ProxyPass /osm/ http://tile.openstreetmap.org/
        ProxyPass /mapquest/ http://otile1.mqcdn.com/tiles/1.0.0/map/
        ProxyPass /mapquest-sat/ http://otile1.mqcdn.com/tiles/1.0.0/sat/
        ProxyPass /mapbox/ http://a.tiles.mapbox.com/v3/thomasnoel.map-d79og8w2/
        ProxyPassMatch ^/cm-([0-9]*)/(.*\.png)$ http://a.tile.cloudmade.com/fb5875a3c0324ae2bf26e0
2b96ea7c41/$1/256/$2

        CacheRoot /var/cache/apache2/mod_disk_cache/tile-univnautes.entrouvert.com/
        CacheEnable disk /
        CacheDefaultExpire 84600
        CacheDirLength 2
        CacheDirLevels 3

        ErrorLog /var/log/apache2/default-proxy-map_error.log
        CustomLog /var/log/apache2/default-proxymap_access.log combined
        LogLevel warn
        ServerSignature Off
</VirtualHost>
```

Présents : Frederick Bigrat, Jean-Marc Liger, Mikaël Ates, Pierre Cros, Dominique Launay, Mehdi Hached, Olivier Salaün

Le projet à été baptisé Univnautes et la liste univnautes@listes.entrouvert.com sera la liste de messagerie du projet.

Présentations

Entr'ouvert

Entr'ouvert a presenté l'équipe intervenant sur le projet :

- Pierre Cros : Gestion de projet relationnel
- Mikaël Ates : Gestion de projet technique
- Benjamin Dauvergne : En charge de la shibbolethisation de pfsense.
- Frédéric Péters : En charge de l'interface graphique
- Jérôme Schneider : Packaging, Maintien des plateformes de développement
  Entr'ouvert a par ailleurs évoqué l'arrivée sur le projet de Thomas Noël, Administrateur système et développeur, spécialiste du monde universitaire.

UNPIdF et partenaires

Frederick Bigrat a présenté l'UNPIdF et les partenaires impliqués dans le projet, en particulier les gens des projets Eduspot, Eduroam et le Siris. Chaque participants à la réunion a présenté son organisme/projet. Il y aura 6 ou 7 établissements partenaires supplémentaires dont le choix est en cours.
Olivier Salaün a présenté plus en détail le projet Eduspot, portail captif ayant pour SSID Eduspot et promouvant des règles communes pour tous ses membres en mettant l'accent sur la fédération d'identité.
Eduspot va suivre de très près le projet Univnautes : si celui-ci est jugé convaincant, la solution développée pourrait être retenue par Eduspot dans le cadre d'un déploiement universitaire large, voire au-delà. Olivier Salaün a d'ailleurs offert son aide sur les problématiques d'interopérabilité Lasso - Sibboleth.

Méthode de développement et de gestion de projet

Entr'ouvert utilise des méthodes de développement inspirés des méthodes agiles, itératives, qui valorisent les contacts fréquents et informels entre les différents partenaires.
Les réunions se tiendront à chaque fois qu'un des deux partenaires en exprimera le souhait et le compte-rendu des réunions se fera sur le wiki d'Entr'ouvert.

Présentation générale de la solution

Mikaël Ates a présenté la solution et ses 4 axes majeurs :

- Utilisation de pfSense, solution implémentant nativement l'ensemble des fonctionnalités nécessaires ;
- Assurer la compatibilité Shibboleth de pfSense grâce à la bibliothèque certifiée SAML 2.0 Lasso ;
- Remplacer l'interface de pfSense par une interface spécifique développée avec Django et modernisée ;
- Utiliser Nagios pour la supervision.

Points de vigilance

- Il a été rappelé que la solution ne devait pas être intrusive pour les fournisseurs d'identité (IdP), ne pas nécessiter de configuration complexe sur ces derniers. Entr'ouvert a confirmé que ses "bonnes pratiques" dans le cadre du déploiement de solutions samelisées interdisaient de déporter la complexité de la configuration au niveau de l'IdP.
- Entr'ouvert a rappelé que le projet ne portait pas sur le matériel. Pourtant, un certain de nombre de contrôleurs embarquent nativement un portail captif dont il faudra vérifier qu'il peut être désactivé.
- Concernant les logs, Entr'ouvert devra insister, lors de la présentation aux établissements partenaires, sur le fait que les logs des contrôleurs pourront être remontés vers le logiciel de supervision Nagios en utilisant le protocole SNMP. Il est important de montrer que le portail captif peu fonctionner en bonne intelligence avec le contrôleur.
- Dominique Launay a posé des questions concernant la sécurité et la possibilité en particulier d'une attaque de type "Man in the middle" ou ARP poisonning. Il a insisté sur la nécessité de mettre des listes ACL sur la borne et de ne pas permettre le dialogue direct entre machines. Mikaël Ates a indiqué qu'Entrouvert pouvait maintenir un document recensant quelques recommandations visant à assister les administrateurs dans la sécurisation de leur réseau.

Communication

Le projet est stratégique pour l'UNPIdF et sera accompagné d'une campagne de communication conséquente. Entr'ouvert accompagnera, à son niveau, cet effort de communication et profitera de ses nombreux contacts dans l'univers du logiciel libre pour contribuer à sa notoriété. Il y aura en particulier une journée d'étude consacrée à la gestion d'identité organisée par le Comité Réseau Université le 24 janvier. Même si celle-ci ne figure pas officiellement dans le planning, Entr'ouvert devra avoir avancé suffisamment en terme d'interface pour pouvoir offrir quelque chose qui puisse être présenté à cette occasion.
Mikaël Ates et Jean-Marc Liger ont aussi évoqué l'éventualité d'une communication commune aux JRES, c'est certainement une piste intéressante.

Divers

- Sur l'interface de connexion du SP se fait la sélection de l'IdP. Mikaël à évoqué comme piste pour éviter la liste déroulante un outil comme celui récemment présenté par Feide sur la liste du WG ULX de Kantara.
- Au moment de la connexion l'utilisateur doit être redirigé vers une page de l'UNIdF dans laquelle figurera l'éventuelle URL vers laquelle il souhaitait se diriger.
- Des développements supplémentaires pour permettre l'utilisation de la solution par des téléphones mobiles seront conduits dans un second projet.
- Entr'ouvert fournira une image iso pour les partenaires avec des instructions concernant l'installation.
- Toutes les options à l'exception de l'appliance ont été retenues
- L'intérêt de Supann a été évoqué. Comme les attributs ne sont pas remontés d'un IdP vers un SP, les attributs ne sont pas pris en compte.

Planning

Pour laisser un peu plus de temps pour les opérations de recettage début janvier, le planning a été revu comme suit :

- Première maquette après les fêtes : Première maquette le 4/01
- Recette première maquette le 28/01
- Version opérationnelle le 15/02
- Recette de la version opérationnelle le 15/03

À noter que la facturation ne peut être effectuée sur 2010. La première facture (accompte de 30%) sera donc envoyée à l'UNPIdF début janvier.

Prochaine réunion le mardi 7 décembre à 14H30 notamment avec les ingénieurs réseau des établissements partenaires où il sera question de l'intégration du portail captif dans des architectures où il y a déjà un contrôleur.

`Présents :`

- Frédérick Bigrat - UNPIdF
- Sabin Galuscan - Université de Versailles Saint-Quentin-en-Yvelines
- Cyrille Ghesquiere - Université Paris VIII
- Jean Marc Liger - Université de la Sorbonne / SIRIS
- Philippe Werle - Université Paris XIII
- Mikaël Ates - Entr'ouvert
- Thomas Noël - Entr'ouvert
- Fédéric Péters - Entr'ouvert

Rappel du principe du portail captif

`Présentation rapide des logiciels principaux employés :`

- pfSense 2.0, basé sur FreeBSD 8.1
- AuthSAML2, module de Authentic2 (python)
- Bibliothèque SAML 2.0 Lasso, et les dépendances OpenSSL, libXML2, libxmlsec

`Discussion sur les certificats nécessaires pour le portail captif et l'impact sur les métadonnées de fédération::`

La discussion a porté sur l'utilisation d'un **certificat commun** à plusieurs portails captifs, au niveau des échanges de la fédération et au niveau de la connexion HTTPS (page de connexion au portail).

Il existe une PKI avec une AC racine universitaire/CNRS : chaque université dispose de ses propres certificats qui seront bien validés par les navigateurs du marché. Dans ce cas, le déploiement d'un portail eduspot nécessitera d'acquérir les certificats, de les configurer au sein du portail (partie HTTPS et SAML 2.0) puis de déclarer les métadonnées de son portail au sein de la fédération.

Entr'ouvert indique que si chaque portail est déclaré indépendamment au niveau de la fédération (i.e. un certificat par portail), cela permettra de mettre en oeuvre des profils SAML 2.0 (qui ne sont pas déployés à ce jour), notamment le ***Single Logout IdP initiated via SOAP*** -- à la condition que le portail soit directement accessible en SOAP (http/https) par les IdPs.

Entr'ouvert indique qu'en cas de certificat commun à plusieurs portails (utilisé pour la fédération), il serait possible de ne faire qu'une déclaration de métadonnées pour de multiples portails. Cela empêcherait, pour ces portails, le déploiement de profils SAML où l'IdP adresse directement les SP et les IdP n'auraient pas connaissance du portail faisant une requête d'authentification au travers des échanges (mais pourrait relever l'adresse IP). Cependant, ce mode de déploiement pourrait être intéressant pour des organismes souhaitant déployer un portail captif et n'étant pas familiers avec l'obtention de certificats et l'enregistrement de services auprès de la fédération. Il serait alors nécessaire qu'un organisme prennent en charge la distribution de la clé privée et du certificat aux organismes souhaitant déployer un portail dans cette configuration.

À l'issue de cette discussion, penchant vers l'usage de multiples certificats seulement, Phillipe Werle a proposé de discuter de cette question avec le groupe RSSI. Cette discussion sera ensuite portée sur les listes EDUSPOT et Univnautes.

Discussion sur les attributs d'identités

Les attributs d'identités sont envoyés de l'IdP au portail au sein de l'assertion d'authentification.

Il avait été discuté lors de la précédente réunion les points suivants :

- Faire redescendre un attribut d'autorisation de l'université d'appartenance à l'université d'accueil. Entr'ouvert avait signalé que l'usage de cet attribut pourrait être couplé avec une liste noire des utilisateurs maintenue par les universités d'appartenance
- Faire redescendre l'attribut ***eduPersonAffiliation***

Cela a fait l'objet d'une discussion avec Olivier Salaün :

- La notion de contrôle d'accès basé sur un attribut n'a pas été abordée au sein du groupe de travail EDUSPOT mais ce serait intéressant ;
- Olivier émet cependant la recommandation suivante : moins d'attributs sont envoyés plus la solution est simple et robuste, donc ***a minima*** seul le NameID serait envoyé ;
- Il indique enfin qu'il est nécessaire de discuter de l'usage de l'attribut ***eduPersonAffiliation***.

Entr'ouvert précise les points suivants :

- Pas de difficulté à traiter un attribut d'autorisation une fois celui-ci défini.

- Les autres attributs pourront servir
  - soit à enrichir les logs
  - soit à affiner la décision de contrôle d'accès

La décision de contrôle d'accès peut notamment avoir une portée qui dépasse la simple autorisation d'accès au réseau. Elle pourrait notamment porter sur la limitation de la bande passante ou les services autorisés.

Il est donc nécessaire dans un premier temps de **définir ces décisions (les usages) et les attributs entrant dans ces décisions (noms/valeurs)**. Une discussion conjointe Unvinautes et EDUSPOT à ce sujet est nécessaire.

Traçabilité, logs, législation

Entr'ouvert rappelle que le ***nameID*** permet d'obtenir l'identité réelle (nom, prénom, établissement, etc.) auprès de l'IdP. L'IdP doit gérer l'enregistrement des assertions d'authentification délivrées. Le ***nameID***, même ***transient***, est un identifiant unique délivré par l'IdP et associé au compte informatique d'un usager. Il n'existe pas de meilleur identifiant délivré par l'IdP tel que pourrait l'être un uid ou une adresse mail. (Le nameID est une valeur aléatoire prise dans un espace grand.)

Philippe Werle, souligne le fait qu'il est nécessaire pour des questions de législation sur les opérateurs que le portail puisse enregistrer les informations suivantes : nom, prénom, organisation, identifiant, adresse IP, adresse MAC le cas échéant, date et heure de connexion, et cela dès l'ouverture du service et non pas au travers d'une opération ***a posteriori***.

Il est donc nécessaire de **valider le prérequis légal de traçabilité** et les attributs requis (nom, prénom, organisation...) et notamment ceux à faire redescendre dans l'assertion. Une discussion conjointe Unvinautes et EDUSPOT à ce sujet est nécessaire.

`Démonstration de l'exploitation du portail, présentation des interfaces::`

Supervision

Les efforts vont être concentrés sur l'extension du serveur SNMP déjà intégré à pfSense. Ainsi le portail fournira un maximum d'information sur son état via ce protocole. Le portail intègre par ailleurs de nombreux outils qui permettent de le superviser (notamment des graphes de suivi type ***rrd***) et de faire des diagnostics.

Interfaces de connexion

Philippe Werle indique que la page de connexion doit préciser que « se connecter implique acceptation des CGU (disponibles en ligne) » .

Une discussion conjointe Unvinautes et EDUSPOT sur les textes apparaissant par défaut sur les interfaces est nécessaire.

`Interfaces d'accueil (après succès de la connexion)::`

Frédérick Bigrat demande que le clic sur l'URL demandée au départ s'ouvre dans un nouvel onglet.

Virtualisation

La solution est testée chez Entr'ouvert sur des machines en KVM (base Linux Debian). FreeBSD est connu pour fonctionner sur VMWare et VirtualBox, qui seront les solutions utilisées par les sites de test / pré-déploiement.

En terme de performance, il est possible que FreeBSD ne puisse pas proposer dès maintenant les mêmes qualités que d'autres OS, notamment pour tout ce qui est I/O. Mais cela ne gênera pas les tests.

IPv6

Entr'ouvert souligne les soucis que pose IPv6, liés principalement au fait que le portail captif de pfSense est fortement lié à IPv4, mais aussi que les machines IPv6 sont en général dual IPv4/IPv6 et enfin que le protocole IPv6 a été conçu dans une optique «une IP publique par machine» qui peut encore poser des soucis de changement de pratique de sécurité.

Entr'ouvert émet à ce jour des réserves sur l'intégration d'IPv6 dans la solution, notamment au regard d'un déploiement en pratique d'IPv6.

Redondance

Le protocole CARP intégré à FreeBSD est géré par pfSense : il sera la solution technologique pour gérer la redondance (***fail-over***)

Performances

Frederick interroge Entr'ouvert sur les performances du portail. Entr'ouvert n'a pas encore mené de tests de charge (***NB : ils seront fait prochainement***). Cependant, les briques logicielles impliquées sont performantes : FreeBSD est un excellent noyau réseau, Lasso est une des implémentation les plus performantes dans le traitement des flux SAML 2.0, la partie Python/Django est gérée via lighttpd en FastCGI.

Logs

Entr'ouvert indique que les logs seront stockés localement et/ou exportés (***syslog***).

Ergononomie & infographie

Entr'ouvert demande à être mis en contact le plus tôt possible avec le(s) prestataire(s) en charge des recommendations sur l'ergonomie, le design, l'infographie, etc.

Entr'ouvert évoque une version pour mobile (i.e. petits écrans type iPhone/Android) : sera étudiée dans un autre projet.

Démonstration de l'installation depuis une clé USB

Livraison

EO explique qu'un soucis technique dans la production d'une image ISO est survenu récemment (le 4 janvier matin) et remettra les livrables au plus tard en fin de semaine.

- Un ISO téléchargeable (régulièrement mis à jour) : http://isos.univnautes.entrouvert.com/
- Une documentation consultable en ligne (régulièrement mise à jour): http://wiki.entrouvert.org/Univnautes/DocumentationLivrable

Frederick a présenté globalement le projet et insisté sur la différentiation entre Eduspot et Eduroam. Entr'ouvert a ensuite exposé les principes techniques généraux et les briques logicielles retenues.

Transparents présentés par EO

2010120-univnautes.odp - présentés par Pierre Cros

Partenaires du projet

8 établissements sont partenaires du projet :

- Université Paris I
- Université Pierre et Marie Curie
- Paris XIII
- Université de Versailles
- SIRIS
- INALCO
- ENSIE
- Paris VIII

4 établissements sont retenus comme bétâ-testeurs pour déboguer les aspects opérationnels majeurs de la première version qui sortira le 4 janvier, avant de la soumettre aux autres partenaires :

- Paris XIII
- Université de Versailles
- SIRIS (Jean-Marc)
- Paris VIII

Méthodes de gestion de projet / développement

Entr'ouvert fonctionne avec des méthodes itératives et met donc les partenaires à contribution afin que le projet colle le plus possible à leurs besoins réels.
Chaque partenaire est libre de se créer un compte sur le Wiki d'Entr'ouvert afin d'accéder aux pages du projet : http://wiki.entrouvert.org/Univnautes
Outre ce wiki, le projet existe dans un logiciel de suivi de projet (redmine) qui peut-être utilisé pour suivre les développements, rapporter des bugs, etc : https://dev.entrouvert.org/projects/portail-captif (la création de compte sur le Redmine doit être demandée à Entr'ouvert à l'adresse <<MailTo(univnautes AT entrouvert DOT NOSPAM com)>>)

Entr'ouvert souhaite multiplier autant que faire se peut les contacts rapides et informels. La liste de discussion du projet, vecteur privilégié de ces échanges, est unpidf-univnautes@listes.univ-paris1.fr

Rappel sur l'architecture

- Le portail est en mode coupure, il agit en temps que passerelle.
- Il a été évoqué l'intérêt de définir un VLAN pour le hostpot. Les communications réseau de ce VLAN seraient routées par le portail captif.
- Le contrôle des stations autorisées se fera sur les adresses MAC et IP. Il est donc nécessaire que les contrôleurs puissent faire remonter ces informations au portail.

Supervision des contrôleur et du portail

- Il a été évoqué le besoin de pouvoir activer un agent SNMP sur le portail pour pouvoir le superviser.
- La supervision des contrôleurs se fera par l'activation sur les contrôleurs d'un agent SNMP interrogeable depuis le portail.
- La supervision dépend du support par les contrôleur du protocole SNMP et des MIB standards.

Échange d'attributs

- Il y a une liste des attributs échangés par les universités sur le site Shibboleth du CRU
- Il a été évoqué la possibilité que les IdP Shibboleth incluent 2 attributs dans les assertions d'authentification pour les SP portail captif :
  - Le premier serait une decision d'accès au service
  - Le second serait l'affiliation de la personne
- Il a été discuté le bien fondé de confier à l'université hébergeant l'IdP de prendre la décision d'accès au hotspot d'une autre

université.
- Il a été proposé de discuter de cette question avec le CRU/Renater/EDUSPOT pour avoir leur vision sur le projet EDUSPOT.

Pages de connexion et d'accueil

- Le portail captif utilise son propre "where are you from" employé sur la page de connexion pour une question d'ergonomie : Un champs de saisie permettrait à l'utilisateur des mots clés lui permettant de réduire cette liste. A chque saisie de lettre la liste se réduirait jusqu'à ce que l'utilisateur puisse identifier son université d'appartenance.
- Suite à une connexion réussie sur le portail, il sera affiché une page d'accueil. Cette page pourra être affichée en pop-up en redirigeant le navigateur de l'utilisateur directement sur l'URL du site initialement demandé.
- Il a été évoqué la problèmatique de la fenêtre pop-up et donc la proposition suivante a été faite : l'utilisateur serait redirigée vers la page d'acceuil de l'université hôte et l'URL du site initialement demandé serait mis en avant sur cette page en requérant que l'utilisateur clique sur ce lien.
- L'interface de configuration permettra de personnaliser la page d'accueil par défaut ou d'injecter directement une page conçue par ailleurs.
- La page d'accueil par défaut, personnalisable au travers de l'interface d'administration, devra avoir une présentation figée afin que l'utilisateur retrouve un affichage "familier" même si le contenu informatif de la page variera en fonction de la personnalisation.
- Sur la page de connexion et sur la page d'accueil seront présenté des liens vers la charte informatique et sur une page explicative des différents services wifi : EDUROAM et EDUSPOT.

À faire par Entr'ouvert

- Faire une liste des pré-requis pour l'installation, sur le matériel, l'architecture réseau, éventuellement les compétences nécessaires
- Valider la stabilité de pfSense 2.0 (beta4 actuellement) par rapport aux besoins des premiers déploiements
- Mettre en place le dépôt présentant les développements modifiants pfSense
- Faire en sorte que le portail captif fournisse des infos par SNMP exploitables par les systèmes de supervision déjà installés dans les universités partenaires.
- Étudier la possibilité de redondance / haute dispo(tolérance aux panne)
- Positionner un cookie pour présélectionner le dernier IdP utilisé (common domain cookie ?)
- Échanger avec le CRU/RENATER/EDUSPOT pour aborder les questions suivantes :
  - La liste des fournisseurs d'identités maintenue dans le cadre d'Eduspot sera t'elle disponible, et sous quelle forme (webservice idéalement)? Il est en effet nécessaire de pouvoir ajouter simplement au portail les urls accesible pour l'authentification. Il s'agit de déclarer les points d'entrée applicatifs des IdPs et des serveurs CAS. Il est donc nécessaire d'avoir un moyen simple d'ajouter les URLs des serveurs CAS (Celles des IDP SAML étant découverte lors de l'ajout des métadonnées).
  - Quelle sera la politique de sécruité en terme de service offert à l'usager EDUSPOT (ports et protocoles)?
  - Quelle sera la poltique envers la décision d'autorisation et de contrôle d'accès ("Accès universel")? Quels sont les attributs à considérer dans les assertions d'authentification?

À faire par Frédérick

- Fournir la liste des partenaires avec leurs coordonnées
- Fournir un inventaire des contrôleurs utilisés par les partenaires (marque, modèle, version firmware/OS)
- Envoyer à Entr'ouvert le résultat du travail de Themesis

Divers

- SSID retenu pendant le développement du projet sera Eduspot-test

Planning

- Première maquette après les fêtes : première maquette le 4/01
- Recette première maquette le 28/01
- Version opérationnelle le 15/02
- Recette de la version opérationnelle le 15/03

Prochaine réunion le 12 janvier à 9H30 dans la même salle.

Fichiers

2010120-univnautes.odp	6,25 Mo	04 mai 2012	Pierre Cros

L'image iso a été livrée par Entr'ouvert, testée par les beta-testeurs et peut maintenant être diffusée auprès des autres partenaires pour qu'ils l'utilisent également. Entr'ouvert a fait une démonstration de l'installation et du fonctionnement du portail captif.

Questions et réponses

- Est-ce que la clé privée est contenue dans l'image => Non. Elle peut être crée ou chargée via l'interface d'administration de pfSense. L'interface permet la création d'AC et l'émission de certificats. Via l'interface d'administration, on peut configurer le certificat du serveur HTTPS (pour le site web du portail captif) et celui du SP (pour les échanges SAML avec les IdP). Ils peuvent être (et seront certainement) différents ;
- Peut-on utiliser la solution en paravirtualisation ? => en paravirtualisation (typiquement kvm) il existe des drivers virtio pour FreeBSD ; cependant selon Entr'ouvert ils ne sont pas encore à un stade suffisamment stables pour être utilisés en production à ce jour.
- Est-ce qu'il faut deux interfaces réseau «physiques» pour faire tourner la solution ? => Non. Il faut deux interfaces, elles peuvent être réelles ou virtuelles (via des VLAN ou via des cartes réseaux simulées sur un guest en virtualisation) ;
- Est-ce qu'il faut déclarer son SP pour pouvoir tester ? => Non. Pendant la phase de test, tout le monde teste avec le même SP déjà déclaré (univnautes.entrouvert.lan et clé+certificat fournis dans l'image). La déclaration des SP n'interviendra qu'au moment de la mise en production. La documentation expliquera les étapes à suivre pour configurer les certificats au niveau d'Univnautes.
- Est-ce qu'on peut mettre une adresse de réseau IP (a.b.c.d/n) dans le fichier whitelist statique ? => Oui ;
- Est-ce qu'on peut désactiver le NAT ? => À l'étude ;
- Est-ce qu'on peut blacklister des IP/services en entrée et en sortie => Oui via les règles du firewall de pfSense. Des règles seront proposées par défaut, qui pourront être activées ou désactivées ;
- Pourquoi la solution est-elle en 32 bits et pas en 64 => parce que le 32 bits marche sur toutes les plate-formes, il est plus simple de générer et valider une image ISO plutôt que deux. Par ailleurs, il n'y aurait pas vraiment de gain à utiliser une image 64 bits ;
- Est-ce qu'il y a un timeout permettant une déconnexion au bout d'un certain temps ? => Oui. Paramétrable et positionné par défaut à 1H ;
- Est-ce qu'il y a possibilité d'avoir des logins concurrents (c'est à dire simultanés) ? => Non ;
- Est-ce que le filtrage par adresse Mac est possible ? => À l'étude.
- Pourra-t-on avoir un système de log personnalisé ? => oui, des hooks seront disponibles dans le code pour ajouter des fonctionnalités lors d'une authentification (pour les logs mais aussi, si besoin, pour la validation du compte en fonction des attributs reçus).

Attributs pour la traçabilité et pour l'autorisation d'accès

Si le choix est fait par CRU/Renater/Eduspot de fonder une politique d'autorisation d'accès sur des attributs, il faut s'entendre sur ces derniers. Une discussion interne sera menée par les différents partenaires avec le CRU. La combinaison eduPersoPrincipalName + CN + email semble intéressante. eduPersonEntitlement pourrait aussi être utilisé pour l'autorisation. Mais la discussion doit s'engager pour vérifier en particulier si Eduspot : * Doit connaître l'identité complète de la personne (c'est vraisemblable, il faut pouvoir identifier la personne pendant 1 an...) ; * Souhaite laisser la politique d'accès à la discrétion des universités hôtes ou faire en sorte que cette politique soit homogène d'une université à l'autre ; * Savoir quel type de population Eduspot souhaite autoriser.

Entr'ouvert a montré que la solution est déjà techniquement capable de gérer les attributs pour la traçabilité et pour la gestion des accès.

Supervision

pfSense propose une interface de supervision (examen des logs, graphes rrd, etc) mais permet surtout de communiquer en SNMP (Entr'ouvert doit vérifier si la V3 est supportée) dans les deux sens (y compris trap).

Réponse du 13 janvier : seul SNMP V1 est supporté par le serveur SNMP installé sur pfSense (bsnmp). Cependant on pourra ajouter des règles sur le firewall local pour limiter l'accès SNMP à certaines IP/Mac uniquement.

Problèmes rencontrés

- Shibboleth ne peut pas faire de Single Logout si bien que l'utilisateur n'est pas déconnecté de l'IdP tant qu'il n'a pas fermé son navigateur. Un message explicite devra être affiché après déconnexion sur le portail pour prévenir l'usager de cet état de fait ;
- pfSense est entièrement bâti autour de IPv4. Le passage à IPv6 est une solution qui doit être envisagée pour l'avenir mais qui demandera des changements en profondeur.

ToDo Entr'ouvert

- Fournir une ***check list*** qui servira de support à la recette ;
- Adapter l'ergonomie pour respecter les recommandations de Temesis (attendues de la part de Frédérick Bigrat)
- Permettre le rafraîchissement manuel via la console de la liste des metadatas et de la whitelist. Typiquement, cela permettra de tester sans délais un IdP venant d'être déclaré ;
- Il faut utiliser le SSID eduspot-test (***déjà effectif***);
- Supprimer le qwerty sur la console ;
- Vérifier quelle version de SNMP est gérée par pfSense (***réponse ce 13 janvier : v1 uniquement***);
- Cacher certains éléments de l'interface d'admin de pfSense ;
- Regarder si on peut désactiver le NAT ;
- Rendre l'interface d'administration accessible du WAN et pas du LAN par défaut, avec une option de configuration permettant de paramétrer la chose ;
- Étudier puis valider la redondance (***fail over***) avec CARP ;
- Faire un fichier ***changelog*** récapitulant les changements d'une version à l'autre.

Divers

- Frederick Bigrat va envoyer à Entr'ouvert le catalogue des bonnes pratiques en matière d'ergonomie fait par Temesis. La solution devra respecter ce catalogue qui comprend 217 points ;
- Un infographiste proposera par ailleurs plusieurs modèles de page d'accueil ;
- Frederick Bigrat a initié le plan de communication visant à porter le projet à la connaissance des personnes devant être sensibilisées.

Planning

- Journée gestion d'identité CRU/Renater le 24 janvier avec une communication de Frédérick Bigrat accompagné par Pierre Cros
- Recette le 28 janvier (réunion à 14h, même salle)
- Livraison de la **version finale le 15 février** et organisation d'une journée de formation dans la foulée.
- Mise en production pour les universités test autour du 1er mars
- Recette de la version finale le 15 mars et discussions autour des évolutions futures envisageables

Prochaine réunion le 28 janvier à 14H, même salle (ou une plus grande :))

Chaque établissement partenaire a listé, grâce au document de recette, les problèmes rencontrés lors de l'installation et de l'utilisation de la version de test. Il en ressort les points suivants :

- La solution marche globalement pour tout le monde
- l'UPMC a rencontré des problèmes lors des déconnexions/reconnexions, Jean-Luc doit faire remonter le message d'erreur à EO.
- Benoit a quelques incertitudes dans la configuration du contrôleur Aruba (qui héberge le dhcp chez eux), Philippe a proposé de tester leur configuration pour vérifier son niveau de sécurité.
- La whitelist permet de récupérer la liste des IdP en production mais il faut ajouter manuellement les IP des IdP de la fédération de test.
- SNMP : Entr'ouvert doit documenter les oid utiles relatives au portail captif

Attributs

Benoît a proposé au CRU que le SP sélectionne ses clients grâce au eduPersonAffiliation, et que l'IdP choisisse les catégories d'utilisateurs qu'il autorise ou non grâce à l'attribut eduPersonEntitlement.
Réponse provisoire de eduspot : on ne filtre pas. Toute personne capable de s'identifier reçoit un accès.
Cependant, il faut pouvoir bloquer une personne instantanément au niveau du portail. Il faut disposer d'un système de blacklist (locale et/ou générale). On retient le ***eduPersonPrincipalName*** comme attribut pour ce faire, et on le fait apparaître dans les logs.
La question devra être posée à eduspot de savoir si on récupère le display name pour l'afficher à l'utilisateur (montrer à l'utilisateur qu'il est connu peut-être un élément d'une politique de sécurité).

ToDo Entr'ouvert

Thomas Noël a présenté la dernière version de la solution et les demandes suivantes ont été formulées :

- Regarder combien de temps les logs sont stockés et si un logrotate est mis en place.
- Permettre d'ajouter des métadonnées depuis l'interface d'administration (pour intégrer des IdP extérieurs à la fédération).
- Développer la procédure de mise à jour afin qu'elle se fasse automatiquement depuis l'interface d'admin avec un temps d'interruption du service trés réduit et en conservant la configuration.
- Indiquer «entity ID» plutôt que «URL» dans l'interface dans l'onglet Univnautes
- L'installateur demande wan puis lan, mais affiche ensuite lan avant wan => homogénéiser si possible
- Regrouper les onglets intéressants au début sur "services : captive portal"
- Mettre un logo univnautes sur la page de connexion de l'interface d'admin
- Système de blacklist sur EPPN
- Documentation des OID SNMP

Divers

- Interface wan doit avoir accés total au réseau IP, ne doit pas être filtrée sur les ports à proposer aux clients
- Charge : Il n'y a pas de problème majeur, mais il faut des machines avec des entrées sorties qui "marchent bien". Il est fait remarqué que gigabit et virtualisation ne seront sans doute pas compatibles.
- Les messages envoyés par Entr'ouvert sur la liste UNPIdF du projet n'ont pas été diffusés et c'est dommage car cela aurait certainement clarifié à la fois certains problèmes soulevés pour l'installation et la problématique des certificats. Frédérick Bigrat doit s'assurer de la bonne diffusion des messages d'Entr'ouvert sur cette liste désormais (Thomas Noël en whitelist ?) et permettre la diffusion des précédents messages. Il est important de mettre la liste univnautes@entrouvert.com en copie lorsque l'on souhaite qu'Entr'ouvert soit informé.
- Éléments évoqués furtivement pour la Phase 2 : bloquage des adresses MAC, intégrer un IdP à la solution

Prochaine réunion mardi 15 après-midi (heure exacte et lieu à confirmer).

Question en attente

Est-ce qu'on garde le SSID eduspot ou est-ce qu'on le fait évoluer vers eduspot-nom-de-l-univ ? La question doit être posée à Renater. On peut garder eduspot et avoir à côté un SSID nom-de-l-univ qui renvoie vers la même solution. Mais pour les établissements mitoyens ça ne permet pas de faire la différence.

Problèmes rapportés à traiter

- Dans l'annuaire Paris 3 y a les entrées des anciens étudiants pour lesquels on ne souhaite pas donner un accès Eduspot. Il faudrait pouvoir filtrer en fonction d'un attribut.
- Fuite mémoire à Paris I. Problème de perf globale sur leur wifi. Demande s'il ya d'autres limites que le nombre de lease pour Eduspot et il n'y en a. Il faut jouer sur la plage DHCP et sur les délais (DHCP et session du portail captif). Thomas indique qu'il va faire un bilan des bonnes valeurs qui ont
  été déterminées sur les sites en production, et mettre la documentation d'Univnautes à jour sur ce sujet.
- Lille : augmentation de la plage DHCP parce qu'ils montent vite en nombre de lease, ils sont passés sur un /22. Voir le nombre de lease, le total en entête (permet d'augmenter le plage DHCP si on est en limite, y a une accroche dhcp par les smartphone même quandil n'y pas de connexion). Et mettre une alerte par mail aux admins quand on atteint un certain seuil de lease. Lease time est asses elevé par défaut, il faut peut-être le baisser à 1h (juste au-dessus de la durée d'expiration de la session).
- Inalco : Ça bloque quand on active pas le NAT. Volonté de connecter à 2 serveurs syslog en même temps (EDIT : c'est possible jusqu'à 3).
- Siris : fichier de lock qui n'est pas supprimé dans le répertoire /tmp à corriger. Bug qui nécessite de redémarrer le portail captif après téléchargement de la liste des IdP. Mais ça n'arrive pas à chaque fois (peut-être uniquement quand la liste a changé ?). Ça n'existe que depuis la mise à jour de juillet sans doute. Thomas va relire le script de téléchargement et chercher un éventuel problème. Échanges à prévoir pour préciser les choses.
- Schéma de connexion manquant à mettre dans la documentation
- Sabin : sous FX la page d'accueil après authent met une minute à se charger ? Benoit a vraisemblablement expliqué la cause : cela se produit lorsque FX essaye de contacter les serveurs de révocation OCSP.
- Problème de déconnexion : pas de fin de session (mais la durée paramétrable) et pas de logout (problème de Shibboleth). Le problème est connu et fait partie des problématiques portail captif. Aucune solution définitive n'existe.

Carte de France

Entr'ouvert a présenté le nouvel écran de connexion d'univnautes (à partir de la prochaine version disponible deuxième quinzaine de janvier). Il se base sur une carte de France des IdP de la fédération Renater et permet de multiplier les modes d'accès (voix, clic sur la carte ou dans la liste, recherche textuelle) à l'IdP de son université d'orignie. L'interface est pensée pour fonctionner avec les appareils mobiles. Thomas va envoyer l'URL de la maquette sur la liste afin d'avoir des premiers retours/remarques/critiques.

Fonctionnalités à développer en 2013

Entr'ouvert fait un certain nombre de propositions suite aux besoin exprimés par les différents universités utilisatrices.

IdP local

Il faudrait augmenter les capacité de l'IdP local pour lui permettre de :

- créer des comptes en masse
- créer des comptes provisoires et permettre d'avoir une date d'activation du compte en plus de la date de fin de validité
- Gérer les attributs pour permettre le contrôle d'accès

Plutôt que de continuer à développer cet IdP local un peu restrictif pour lequel les besoins vont croissant, Entr'ouvert recommande l'installation d'un véritable IdP intégré à la solution et qui servira de base pour le POC (Proof of concept) IdP Cloud.

POC IdP Cloud

Entr'ouvert propose, sous forme de démonstrateur, la mise à disposition d'un fournisseur d'identité multi-protocole (SAML,OpenId, Google, Facebook...) dans le Cloud ou hébergé par les universités qui le souhaitent. Ça se décompose comme suit :

- Déploiements d'hôtes IdP à la volée :
  - génération de fichiers d'hôtes virtuels apache2 ;
  - génération de settings django ;
  - outils systèmes de lancement des hôtes ;
  - intégration d'une css pour les pages utilisateurs (couleur des titres, paragraphes, liens, etc.) et d'une image de l'université (pour la bannière)
  - Déport de la page de Login sur le cloud ;
  - Tests de charge et premières optimisations.

- Interface minimale de souscription permettant entre autres paramètres de souscription de recueillir le nom de domaine, un certificat, un css et une image.

- Interface minimale d'administration et de supervision des hôtes.

POC système de contrôle d'accès

Entr'ouvert propose, sous forme de démonstrateur, la mise à disposition d'un environnement de fédération d'identité, qui facilite le travail des administrateurs, sécurise l'accès aux applications et permet une granularité très fine. Il se décomposerait comme suit :

- Couplage IdP et Reverse-Proxy pour le support multi-protocolaires ;
- Intégration au Reverse-Proxy d'un module de contrôle d'accès gérant les attributs d'identités et les rôles ;
- Interface d'administration pour définir une politique de contrôle d'accès en fonction des utilisateurs, de leurs attributs, de leurs rôles et du service ou des URLs demandés ;
- Support du protocole de délégation d'autorisation XACML ;
- Démonstration avec une application typique des universités à définir.

Divers

- Le contrôle sur les attributs peut être un frein au développement d'Eduspot. Si on exige des attributs 50% des IdP Shibboleth ne fonctionnent plus. Il faut prendre cette dimension en compte.

- Journée nationale sur la fédération d'identité en avril/mai sur Paris et dans deux ans la même journée mais en province. Entr'ouvert doit participer.

Expériences utilisateurs et problèmes rencontrés

- Fuite mémoire constatée par Benoit. Il semble y avoir un processus tcpdump à 50 Meg et plusieurs processus python à 30 Meg. Benoit doit faire remonter l'info exacte à Thomas lors de la prochaine fuite constatée.
- Roland utilise univnautes dans des salles en self service et se trouve confronté à un problème de logout pour les utilisateurs qui ne ferment pas leur navigateur.
- À Descartes ça marche mais avec le SSID EDUSPOT
- Musée National d'Histoire Naturelle : ça marche bien les gens de l'upmc se connectent chez lui parce que ses bornes sont plus puissantes :)
- Paris 1 : 30 utilisateurs, surtout paris 1, peu d'utilisateurs parce qu'il y a 3 ssid en parallèle.
- Siris : Frédérick est demandeur de nouveaux contacts pour les mettre dans la liste univnautes (Sébastien kita nouveau directeur), Jean-Marc envoie un mail.

Statistiques et débuggage

Comment tester la connexion à l''IdP d'une université particulière dans un autre établissement ? Il faur faire remonter les infos aux administrateurs Shibboleth de chaque établissement qui doivent regarder dans les logs univnautes, dans les logs Shibboleth.
On peut faire une page pour que les utilisateurs puissent rapporter les problèmes constatés (lister les problèmes types sur la page pour faciliter la saisie), permettre la configuration dans l'interface d'admin de l'adresse mail à laquelle le message est envoyé dans l'interface admin. Évolution chiffrée par Entr'ouvert à 3 jours de travail.

Il faudrait aussi logguer le passage dans la white liste non authentifié et comparer avec les connexions réussies pour pouvoir produire un taux de réussite. Cela permettrait d'avoir pour chaque serveur le pourcentage de retour et le pourcentage d'accès ouvert. Regarder ensuite si on met ça dans les logs de pfsense pour analyse ou si on délègue ça à un analyseur de log ou encore si on fait ça nous même. Initier une discussion là-dessus au sein de la liste quand on saura ce qu'il est possible de faire.

Ce qui peut être fait : logguer les "demandes de connexion", au moment où l'utilisateur clique sur le lien qui envoie vers la redirection POST vers sont IdP.

On a déjà les logs de succès d'une connexion. On pourrait donc avoir un analyseur qui fasse le différentiel entre les demande de connexions et les connexions réussies, et dise combien de demandes semblent avoir échouées (sans savoir pourquoi, cependant, car l'IdP ne dira rien). Évolution chiffrée par Entr'ouvert à 2 jours de travail.

Développement en cours

Difficultés

Beaucoup de problèmes liés à des mises à jour concomittentes : Python 2.7, pfsense 2.02, Freebsd 8.3, difficile à suivre.

Intégration de la délégation de la gestion des comptes IdP

Prévu pour début juin.
On va développer une interface à part pour la gestion de la délégation de compte. Identification pourrait se faire via la fédération (on va utiliser la technologie qui est déjà intégrée au produit). Une possibilité d'implémenter ça : si un utilisateur se loggue sur l'IdP avec tel attribut, je l'autorise à créer des comptes invités (l'attribut EduPersonEntitlement fera l'affaire). Chaque tétablissement pourra personnaliser cet attribut dans l'interface d'administration.

La durée de validité des comptes invités est fixée par défaut pour les gestionnaires habilités à créer ces comptes. S'il faut un compte qui dure plus de temps c'est l'admin qui s'en occupe.

L'intérêt d'avoir un IdP séparé a été soulevé, pour des raisons de perf, pour la maintenabilité et l'autonomie par rapport à pfSense. Mais Thomas a rappelé qu'on pouvait mettre une machine avec seulement l'Idp local activé (sans le reste d'univnautes).

Discovery service

Prévu pour la mi-juin
La question de l'hébergement du service n'est pas encore tranchée. Mais si le serveur est HS, il faut de toute façon que ça continue à marcher.

Formation

La 1/2 journée de formation restante aura lieu en octobre dans le cadre du process de formation UNR.

Évolution de l'interface de connexion

Frédérick a proposé l'idée d'avoir une carte de France permettant de cliquer sur les régions, puis sur son université. Mais on a pas l'info géographique dans les metadata.
Ce problème de localisation des IdP devrait être remonté à Renater. Attention toutefois parce que même si on a ces coordonnées on va pas mettre un serveur de carte sur univnautes et l'utilisateur n'est pas connecté... ce qui empêche l'utilisation de services comme Open Street Map our Googlemaps.

La prochaine réunion est fixée au 28 juin après-midi.

Notes pour la création des ISO

Bases de la construction

Mode d'emploi de base : http://devwiki.pfsense.org/DevelopersBootStrapAndDevIso

Il faut réussir un premier build_iso.sh avant de continuer les adaptations...

Remarques :

- toujours rester en csh
- ne jamais utiliser pkg_add, toujours utiliser les ports

Installation des ports

Aller dans /usr/ports et installer les paquets nécessaires à univnautes (voir liste ci dessous)

Installation du port lasso spécifique à UnivNautes (lasso pre-2.4)

Voir README.txt dans le dépôt (source:freebsd-ports/lasso/)

Création d'ISO univnautes

Source : /usr/home/pfsense/tools/builder_scripts/build_iso.sh

Chercher l'installation de lua et ajouter les paquets nécessaires à univnautes

```
--- a/builder_scripts/build_iso.sh
+++ b/builder_scripts/build_iso.sh
@@ -142,6 +142,14 @@ rm -f $PFSPKGFILE
 (pkg_info | grep bsdinstaller) > $PFSPKGFILE
 (pkg_info | grep grub) >> $PFSPKGFILE
 (pkg_info | grep lua) >> $PFSPKGFILE
+# univnautes
+(pkg_info | grep ^bash) >> $PFSPKGFILE
+(pkg_info | grep ^python2) >> $PFSPKGFILE
+(pkg_info | grep sqlite3) >> $PFSPKGFILE
+(pkg_info | grep ^openssl) >> $PFSPKGFILE
+(pkg_info | grep ^xmlsec1) >> $PFSPKGFILE
+(pkg_info | grep ^wget) >> $PFSPKGFILE
+(pkg_info | grep ^lasso) >> $PFSPKGFILE
+(pkg_info | grep ^bsnmp-ucd) >> $PFSPKGFILE
 set -e
```

Puis ajouter la construction et l'ajout du virtualenv (à écrire)

Création d'images pour upgrades

à écrire

Généralités

- Cadre du projet Eduspot : http://www.cru.fr/services/eduspot/index * Liste publique : unpidf-univnautes@listes.univ-paris1.fr * Liste privée Entr'ouvert : univnautes@listes.entrouvert.com * Sources du projet : http://repos.entrouvert.org/univnautes.git * Image ISO installable : http://isos.univnautes.entrouvert.com/

Documentation d'utilisation

La documentation d'utililisation de l'application est en ligne : http://doc.entrouvert.org/univnautes/stable/

Autres documentations

- Participer aux test des futures versions : http://doc.entrouvert.org/univnautes/stable/participer.html
- DocumentationLivrable
- ListeDeVerifications
- NotesBuildIso (création image ISO)

Comptes-rendus de réunion

- CR de la réunion de lancement
- CR de la réunion du 7 décembre 2010
- CR de la réunion du 4 janvier 2011
- CR_réunion_12_janvier_2011
- CR_réunion_28_janvier_2011
- CR réunion du 22 mai 2012
- CR réunion du 04 décembre 2012