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 :))