Et si l'infrastructure ENT servait à gérer le nomadisme !

Patrick Petit
DSI Grenoble Universités
351, Avenue de la bibliothèque 38041 Grenoble Cedex 9
Patick.Petit@grenet.fr

Philippe Beutin
DSI Grenoble Universités
351, Avenue de la bibliothèque 38041 Grenoble Cedex 9
Philippe.Beutin@grenet.fr

Jean-François Scariot
Service des Moyens Informatiques du Centre de Recherche INRIA Grenoble - Rhône-Alpes
655, avenue de l'Europe-Innovallée, Montbonnot 38 334 Saint Ismier Cedex
Jean-François.Scariot@inria.fr

Résumé

Le déploiement de points d'accès « sans fil » sur les campus pose des problèmes de sécurité et de responsabilité en cas de compromission ou d'attaque. Il est donc nécessaire de filtrer et de tracer finement les différentes informations sur les connexions pour constituer des journaux exploitables en cas de recours. Plusieurs solutions ont été étudiées comme les accès VPN ou les portails captifs. On se heurte souvent à des limitations techniques des produits ou des difficultés d'exploitation comme l'installation de logiciels spécifiques pour l'accès (exemple du client VPN). Cet article présente l'étude et l'évaluation d'une brique logicielle développée par SUN pour le déploiement sécurisé d'un portail utilisant les composants de la suite JES (Java Entreprise System). En configurant une de ces briques différemment, nous évaluons son adéquation à pallier les problèmes liés aux accès nomade. Nous montrons les apports de la solution ainsi que ses limitations.

Mots clefs

Portail captif, Nomadisme, Accès « sans fil », ENT

Introduction

Les différents établissements d'enseignement supérieur et de recherche ont été encouragés à réfléchir et à déployer, d'une part des environnements numériques de travail (ENT) et d'autre part des réseaux sans fil. Ces deux actions ont été promues dans des périodes proches. La problématique des accès aux réseaux locaux d'établissement via des équipements de type « sans fil » sont souvent traités par des équipes réseau alors que les ENT sont pris en charge par des équipes système ou développement. Le lien entre les deux est souvent faible à savoir un système d'authentification qui accède à un annuaire LDAP.

Le déploiement de points d'accès Wifi sur les campus pose des problèmes de sécurité et de responsabilité en cas de compromission ou d'attaque. Il est donc nécessaire de filtrer et de tracer finement les différentes informations sur les connexions pour constituer des journaux exploitables en cas de recours.

Plusieurs solutions ont été étudiées qui couvrent un large spectre allant des solutions d'accès à base de boîtiers VPN aux systèmes basés sur des portails captifs. Ces tests en grandeur nature nous ont montré que l'on se heurte souvent à des limitations techniques des produits ou à des difficultés d'exploitation comme l'installation de logiciels spécifiques pour l'accès (exemple du client VPN).

D'un autre côté, les ENT sont déployés pour offrir des services liés à l'identité de l'utilisateur qui se connecte. Ils offrent une page d'authentification, mais aussi un portail donnant accès à ses services. La sophistication du socle sous-jacent permet de tracer les différentes connexions à l'ENT et de suivre les sessions.

En rapprochant les deux projets, on s'aperçoit que le travail fait sur les deux études est voisin et qu'il ne manquerait pas grand-chose pour que ces projets se rejoignent.

L'organisation fonctionnelle de la DSI Grenoble-Universités nous a permis de faire ce lien entre le projet de nomadisme et le projet PEPSI lié à la mise en place d'une infrastructure déployée pour les ENT des cinq établissements d'enseignement supérieur et de recherche de l'académie de Grenoble.

L'infrastructure déployée pour les ENT est basée sur des éléments matériels (serveurs et équipements réseau) et sur la suite logicielle Java Enterprise System (JES) de l'éditeur Sun Microsystems. La mise en œuvre d'un des éléments de cette suite non mis en œuvre à l'origine, nous a permis de faire le lien entre les deux problématiques d'accès « sans fil » et d'ENT énoncées précédemment.

1 Solutions « sans fil » étudiées en dehors de l'ENT

Nous rappelons ici rapidement les éléments de l'étude que nous avons menée il y a déjà quelque temps et qui a fait l'objet de diverses publications ou présentations [1].

1.1 Les « portails d'accès » sans client

Les solutions que nous qualifions de « portail d'accès » (souvent appelés portails captifs) sans client offrent l'avantage d'être indépendantes des logiciels et du système d'exploitation des postes clients. On dispose rapidement d'un accès web (voir plus) sur tous types de systèmes d'exploitation. Il n'y a aucune intervention ou ajout de logiciel sur le poste.

1.1.1 « Portail d'accès travaillant au niveau de l'infrastructure »

Nous rangeons sous ce terme les « portails captifs » qui s'appuient sur l'ouverture de règles de filtrage (IPtables). Ces règles filtrent l'adresse MAC ou un couple adresse MAC / adresse IP de l'utilisateur : un couple qui peut être usurpé ! S'il n'y a pas de demande de fin de connexion, la règle de filtrage reste appliquée et l'accès reste ouvert pendant un temps défini.

Ces portails ne forcent pas le chiffrement des données. Or, certains sites web proposent encore de s'authentifier en Http (certains webmail). Le mot de passe peut alors être capturé en accès sans fil et compromettre ainsi l'ensemble des systèmes d'informations.

Une autre contrainte technique, qui s'avère problématique dans notre architecture actuelle, est que le portail repose sur le filtrage d'adresse MAC et doit donc être placé dans le même vlan que les bornes.

La solution Monowall (PfSense) correspond à ce fonctionnement.

1.1.2 « Portail d'accès de niveau applicatif »

Nous rangeons sous cette appellation les portails qui réalisent un traitement au niveau de la couche application. Un « portail d'accès de niveau applicatif » offre l'avantage dans notre contexte de pouvoir être déployé n'importe où dans le réseau.

1.1.3 Les Proxies Web

Pour éviter une configuration des postes client, les proxies web nécessitent de mettre en place un mécanisme de configuration relayé automatiquement soit par DNS, soit par DHCP. Le poste client doit ensuite passer par le proxy pour toute requête web. Dans ce cadre ont été testés les proxies Microsoft ISA Server 2004 et Squid.

1.1.4 Les Proxies Web en mode Transparent

Un proxy Web en mode transparent a la charge de traiter tous les flux web qui sont envoyés sur son interface quelque soit l'adresse IP de destination. Dans notre environnement réseau en mode routé, il est nécessaire d'adjoindre un mécanisme de redirection des flux. La redirection peut-être traitée sur :

- le routeur en utilisant des fonctionnalités de type « Route-map policy » ;
- un serveur DNS dédié translatant toute adresse vers le proxy ;
- les bornes qui proposent une redirection par SSID.

Dans ce cadre, les limites de Squid et de Bluecoat concernant les accès HTTPS nous ont amené à écarter ces solutions.

1.2 Les portails avec « client léger »

Un client est dit léger si les postes ne nécessitent pas de droits administrateurs et de redémarrage de la machine. Rentrent dans ce cadre des solutions comme le Cisco VPN 30XX série en mode webVPN (mais il n'intègre pas de traces des requêtes des utilisateurs) ou Array Networks SPX 3000 en mode SSL (mais son mode de fonctionnement de type réécriture a posé problème avec certains sites).

Le principal inconvénient de ce type de solution est qu'il dépend souvent d'une couche logicielle installée sur le poste client (ActiveX, JVM).

Récemment nous avons voulu tester le Bluecoat RA série. Il fonctionne sur Windows 2000/XP/Vista et Mac OS X 10.4 mais Linux n'est pas supporté avec le « RA connector ». Nous n'avons pas investigué davantage la solution.

1.3 Les portails avec « un client lourd »

Toujours dans notre taxonomie « propriétaire », un client est dit lourd si l'installation nécessite le droit de l'administrateur ou un redémarrage du poste de travail.

Les solutions dans ce contexte impliquent souvent de créer une interface réseau, et par là même, nécessitent des droits d'administration sur le poste travail pour être installées.

La solution retenue il y a 2 ans et actuellement en place, fait appel à un boîtier spécialisé avec un client lourd du type VPN IPsec. Nous n'avons pas approfondi ce point car la solution en place est dans l'ensemble satisfaisante. Elle s'appuie majoritairement sur des boîtiers VPN Cisco 3030.

Nous avons étudié les fonctionnalités du Cisco ASA 5500 serie SSL/VPN version 8.0. Ce serveur d'application propose un nouveau client VPN trois fois plus léger en téléchargement qu'un client VPN IPSec. Ce dernier implémente le protocole TLS sur UDP, qu'ils ont nommé

DTLS[1]. Il est disponible sous Windows 2K / XP / Vista, Mac OS X 10.4 / 10.5, Linux Intel 2.6.x et, prochainement, Windows Mobile 5&6. Hormis le droit d'administration, il ne nécessite pas de redémarrage du poste.

1.4 Le WPA et WPA2 (802.11i)

À l'heure actuelle, le problème majeur d'une solution WPA est la traçabilité des utilisateurs : assurer la correspondance entre l'authentification effectuée par un serveur RADIUS et l'adresse IP fournie par un serveur DHCP. En effet, le mécanisme RADIUS intègre l'affectation d'une adresse IP mais seulement pour les protocoles point à point (PPP). Dans le cas d'un accès sans fil, on doit s'appuyer sur un serveur DHCP pour fournir les adresses IP. Le serveur RADIUS dans le cadre d'un accès sans fil n'a donc pas la visibilité de l'adresse IP affectée à un utilisateur.

1.4.1 Solutions pour la traçabilité

Pour régler le problème de traçabilité, plusieurs solutions existent :

- Un script de corrélation d'information entre les journaux des serveurs DHCP ISC et Radius a été développé par Rock Papez. Reste un point qui ne peut pas être traité par un script : forcer l'affectation d'adresse IP par un serveur DHCP. Sans cette fonctionnalité, une personne sur le réseau peut s'approprier une adresse IP et les journaux perdent alors tout leur sens.
- Gérer le vlan « sans fil » au niveau du routeur. Les routeurs Cisco implémentent à partir de l'IOS 12.3.14(T), une fonctionnalité « DHCP Accounting » qui permet d'envoyer les logs DHCP du serveur DHCP embarqué vers un serveur Radius et des fonctionnalités de contrôle des enregistrements de la table ARP avec les enregistrements DHCP : « DHCP Secure IP Address Assignment, DHCP Authorized ARP, ARP auto-logoff ». Cette solution s'applique également pour de l'authentification en 802.1X sur les commutateurs du réseau filaire.
- Gérer le vlan « sans fil » avec un contrôleur**.** Pour le produit ***Cisco WLC***, hormis la gestion centralisée des bornes et le protocole LWAP qui permet de disposer le contrôleur comme on le souhaite dans le réseau, ce qui nous intéresse ici c'est la fonctionnalité « DHCP Address Assignment Required » qui autorise à sortir du réseau local les seuls postes qui ont obtenu une adresse IP par un serveur DHCP. Dans notre cas, on pourra compléter la solution en utilisant un serveur DHCP intégré sur les bornes ou sur un routeur Cisco pour renvoyer les logs vers un serveur Radius.

1.4.2 Proxyfication radius et gestion de journaux

La gestion des traces est, de notre point de vue, un problème important qu'il fallait régler absolument pour envisager un déploiement opérationnel du WPA. La solution de gestion des traces avec un routeur Cisco en IOS 12.3.14(T) est satisfaisante et simple à déployer. Il s'agit juste de mettre un routeur en coupure pour ce ou ces réseaux.

1.4.3 Avantages et inconvénients de WPA et WPA2

Cette solution prometteuse offre les avantages suivants :

- pas d'accès au réseau avant authentification ;
- mécanisme d'authentification indépendant des serveurs RADIUS intermédiaires ;
- après authentification, l'utilisation d'un client VPN IPSec n'est pas bloquée ;
- solution ouverte et gratuite (utilisation d'un standard, logiciel client gratuit) ;
- sécurisation des flux efficace (chiffrement TKIP ou AES+CCMP) ;
- gestion de l'affectation dans un vlan choisi ;
- journaux (logs) contenant les données essentielles (identifiant, heures de connexions, point d'accès utilisé, adresse MAC et adresse IP) ;
- intégration au projet EDUROAM en accord avec la charte RENATER et les réseaux d'éducation et de recherche.

Elle ne peut toutefois pas faire oublier les inconvénients listés ci-après :

- l'installation d'un client EAP-TTLS est nécessaire pour utiliser le gestionnaire sans fil de Windows ;
- les droits de l'administrateur sont nécessaires pour l'installation du client ;
- un patch est nécessaire pour utiliser WPA2 sous Windows XP, les drivers de la carte réseau doivent eux aussi être à jour ;
- configuration du client EAP.

2 Architecture ENT mise en place

Avant de présenter les fonctions de la brique logicielle assurant le traitement de l'accès à l'Internet, nous précisons sa place dans l'architecture globale de l'ENT basée sur une partie des briques logicielles de la suite logicielle JES.

Notre ENT est commun aux 5 établissements de l'académie de Grenoble :

- Université Joseph Fourier – Grenoble 1
- Université Pierre Mendès-France – Grenoble 2
- Université Stendhal – Grenoble 3
- Institut National Polytechnique de Grenoble
- Université de Savoie.

2.1 Contexte lors du choix de la plateforme

Lors de l'appel d'offre du ministère en 2002 concernant les ENT, nous avons répondu en partenariat avec l'éditeur Sun. Nous attendions de ce dernier un apport de solutions, d'une part sur la gestion de l'identité qui nous semblait

[1] DTLS : Datagram Transport Layer Security

déjà être un aspect fondamental, d'autre part sur de l'infrastructure logicielle permettant de créer de façon « aisée » des portails de services.

Ce partenariat faisait suite à une longue étude de solutions menées dans le cadre du portail du projet Greco [3]. Nous attendions de l'éditeur des solutions qui nous permettent :

- de profiter d'une infrastructure à haute disponibilité ;
- d'avoir un portail d'accueil qui délivre de l'information et des services ciblés pour ce type d'accès ;
- de bénéficier d'outils d'administration fournis par le socle ;
- de générer des journaux des opérations réalisées.

JES réunit plusieurs fonctionnalités très différentes :

- persistance des données réalisée par un annuaire LDAP ;
- environnements d'exécution réalisés par des serveurs Web et d'application ;
- gestion des authentifications et des autorisations réalisée par un ensemble de programmes (servlets) Java ;
- intégration d'informations et de services réalisée par un serveur de portail et d'accès sécurisés.

Notre plus grande attente portait sur la partie liée au SSO et à la gestion déléguée des autorisations d'accès aux applications accessibles depuis le portail. C'était pour nous la clé de voûte du système et nous pouvons constater aujourd'hui que cette problématique couvre grand nombre de domaine du système d'information.

Différents composants de la suite JES étant intégré au gestionnaire d'identité, nous avons choisi de les mettre en œuvre, non par leurs qualités fonctionnelles, mais pour leur rapidité à être déployées, sachant que par la suite nous pourrions nous tourner vers des briques différentes si le besoin s'en faisait sentir. À ce jour, tel n'est pas le cas, les briques mises en œuvre donnent satisfaction. Pour plus d'information le lecteur pourra consulter le mémoire d'ingénieur CNAM analysant différentes solutions [4].

2.2 Architecture logicielle

L'architecture logicielle de portail fournie par Sun

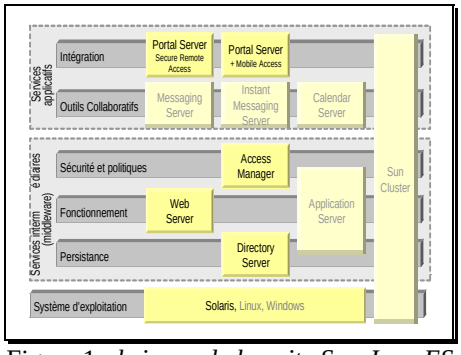

Figure 1 : *briques de la suite Sun Java ES*

comprend un ensemble d'éléments, du serveur web au système d'exploitation, en comptant des composants de haute disponibilité. L'ensemble de la suite JES est libre de droit d'utilisation. Certains composants sont aujourd'hui passés dans le libre comme *Directory Server* proposé sous *OpenDS*, *Access Manager* devenu *OpenSSO* ou *OpenPortal* pour *Portal Server*. La Figure 1 détaille les briques mises en œuvre dans notre ENT.

Dans la figure suivante, nous voyons les liens entre les différents éléments de Sun Java ES.

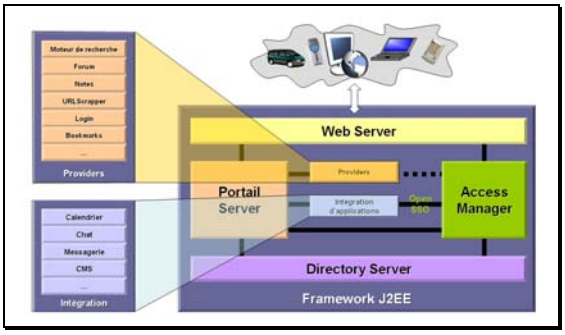

Figure 2 : *interaction des briques JES*

2.2.1 Directory Server

C'est le serveur d'annuaire LDAP qui fournit la persistance des données propres à l'ENT : comptes utilisateurs et leur personnalisation, droits, configurations… Il gère plus de 90 000 entrées et une centaine de rôles.

2.2.2 Access Manager

Il assure les services d'authentification, d'accréditation et de journalisation. Il propose une console d'administration très puissante permettant des modifications à chaud, une finesse de détails basée sur l'héritage, et une gestion d'identité complète. *Access Manager* manipule des organisations auxquelles sont rattachées des services (portail, mode d'authentification, fédération, configurations…), des utilisateurs, des rôles, des politiques d'accès et des sous-organisations.

Access Manager est plus amplement détaillé dans le paragraphe 2.4.

2.2.3 Portal Server

C'est un moteur de génération de portail intégrant les normes communes du marché comme les JSR168 ou JSR268. Il permet de créer un portail « simplement » avec une interface graphique. Chaque utilisateur se voit attribuer un portail logique (description XML) et un ensemble de fichiers pour le générer selon son appartenance à une organisation, ses rôles et ses personnalisations. Nous avons fait le choix de conserver une description logique du portail identique à tous les établissements afin de pouvoir proposer des services d'une autre université aux utilisateurs. *Portal Server* comprend aussi un ensemble de protocoles complémentaires pour afficher le portail sur des clients mobiles (WML, cHTML…). Il intègre également

un moteur de recherche pouvant indexer tout site et tout contenu, à la manière d'un crawler.

2.2.4 Portal Server Secure Remote Access

SRA fournit une passerelle d'accès sécurisée à l'intranet depuis l'Internet. Elle est détaillée dans le chapitre 3.

2.2.5 Web Server

C'est un serveur Web et d'applications. Il intègre un moteur d'exécution du code Java présent dans *Access Manager* ou *Portal Server*. Il est toutefois possible d'utiliser d'autres serveurs d'applications certifiés J2EE. L'avantage de *Web Server* est d'être déjà intégré dans l'installation de la suite logicielle, d'avoir une interface d'administration graphique et d'être très performant.

2.2.6 Système Solaris 10

Nous avons fait le choix d'installer ces éléments sur des plateformes Solaris 10 plutôt que Linux au vu des performances système pour ce contexte particulier.

2.3 Architecture matérielle

Une grande attention a été apportée à l'architecture matérielle d'hébergement afin qu'elle garantisse un haut niveau de fiabilité. Des mécanismes d'équilibrage de charge et de détection de pertes de service sont notamment utilisés par le biais du cœur de réseau (routeur Cisco 6500).

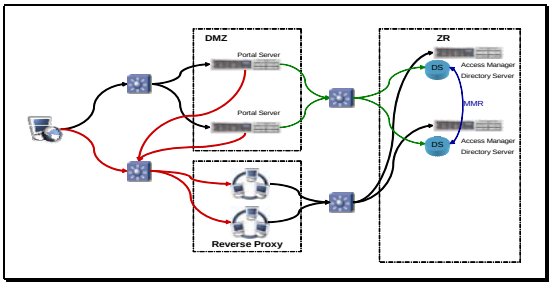

Figure 3 : *architecture matérielle de l'ENT*

L'architecture comporte une DMZ[2] hébergeant les deux serveurs de portails ; une ZR[3] hébergeant deux serveurs d'annuaires en configuration Multi-Mastering et les serveurs Access Manager. Un ensemble de Reverse Proxy assure le filtrage vers la zone retranchée et fait office de terminateur SSL.

2.3.1 Quelques chiffres

Le nombre d'utilisateurs potentiels est de plus de 80 000. Le 10 septembre 2007, 2 554 utilisateurs se sont connectés avec succès sur le premier serveur d'authentification, 2 767 sur le second serveur et 2 309 authentifications ont été générées par l'extension d'OpenSSO, soit un total de 7 630 sessions. Des pointes de trafic de 2 500 sessions simultanées ont été observées.

2.4 Gestionnaire d'accès

Access Manager est conçu pour fournir des services d'authentification, d'autorisation et de gestion de sessions pour les applications Java, les applications Web et les applications orientées services. Il fournit aussi des services de fédération d'identité.

Il permet de couvrir de nombreux besoins de notre environnement et offre de multiples possibilités d'évolution et d'intégration. Nous détaillons maintenant certaines des fonctionnalités les plus marquantes.

2.4.1 Authentification, autorisations et journalisation

Il est possible d'associer à un utilisateur un ensemble de services par rapport à ses fonctions (rôles) ou à son appartenance à une entité (organisation), ainsi qu'un mode d'authentification. *Access Manager* est fourni avec un grand nombre de modules d'authentification déjà intégrés : LDAP bien sûr, mais aussi Active Directory, Certificats, JDBC, MSISDN, Radius, SAML (2.0), SecurId, etc. et la possibilité de les chaîner.

La partie Single Sign On (SSO) permet de gérer les accès à des applications autant qu'à des pages Web avec une grande finesse d'administration et un héritage fort. Les systèmes de SSO sont basés sur un modèle client/serveur dont la partie cliente est généralement incluse dans l'application (mode intrusif). Il est possible d'éviter cette intrusion dans les applications de type Web par l'utilisation d'un module complémentaire au serveur qui héberge l'application.

2.4.2 Administration fine et dynamique

Access Manager permet :

- une gestion hiérarchique des entités et des utilisateurs ;
- une notion de rôle avec priorités permettant de proposer des services aux utilisateurs selon leur appartenance à une entité, à une fonction, à un groupe…
- une console d'administration qui permet de gérer les différents paramètres, les identités, et d'administrer les différentes briques de la suite Sun JES comme le portail ou le SRA.

2.4.3 Haute disponibilité

Il est possible de rendre l'ensemble des briques hautement disponible avec tolérance de panne. La récupération de session est assurée par Message Queue qui n'a pas été retenue pour l'instant.

[2] DMZ : zone démilitarisée

[3] ZR : zone retranchée

3 Solution étudiée

Dans cette architecture, et pour simplifier l'accès web aux nomades à l'intérieur de nos campus, nous nous sommes intéressés à la brique *Secure Remote Access*. À l'origine, elle est conçue pour authentifier et sécuriser les flux provenant de l'Internet vers l'Intranet. Dans le cas qui nous intéresse, nous voulons inverser le sens des échanges, à savoir identifier, sécuriser et tracer un flux interne qui souhaiterait accéder à l'Internet.

3.1 La brique SRA

Portal Server Secure Remote Access [2] est initialement prévu pour sécuriser les accès Internet au réseau interne, comme le montre la Figure 4.

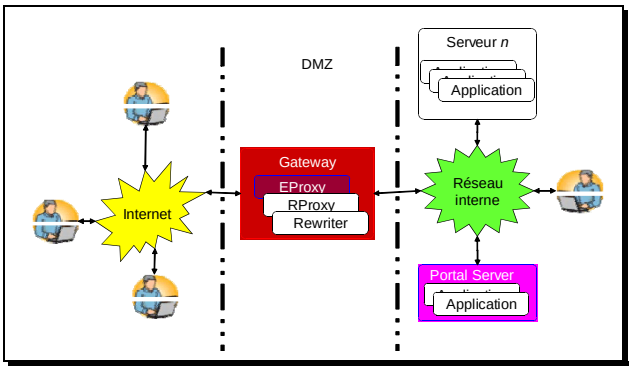

Figure 4 : Fonctionnement « secure » du portail

Le Portal SRA se compose des éléments suivants :

- Gateway
- Rewriter - Rewriter proxy (optionnel)
- Proxylet
- Netlet - Netlet proxy (optionnel)
- Netfile

3.1.1 Gateway

Le composant Gateway est le point d'entrée vers les ressources internes de type Web et non Web en relation avec le serveur de portail. Ce composant agit comme un frontal dont la visibilité doit être importante.

Les configurations affectant le fonctionnement et les droits d'accès se font via l'interface du portail, elles sont enregistrées dans l'annuaire de l'ENT.

Il est possible d'autoriser une ou plusieurs url en accès sans authentification.

3.1.2 Rewriter

L'objectif du Rewriter est de permettre un accès à des contenus Web après authentification. Pour cela, il utilise des règles de réécriture qu'il applique sur les flux Web qui transitent entre le navigateur de l'utilisateur et le serveur Web délivrant le contenu. Les mécanismes de récriture effectuent la transformation des URL relatives en URL absolues et ajoutent un préfixe à l'URL ciblée.

Exemple : pour accéder à la page de l'intranet http://intranet.univ.fr/index.html par la Gateway, le Rewriter préfixe l'URL ciblée avec la sienne : https://gateway.univ.fr/http://intranet.univ.fr/index.html.
Les liens à l'intérieur de la page sont modifiés afin de préfixer tous les liens contenus par l'url de la gateway : images, css, liens, scripts…

Si la Gateway fonctionne en HTTPS, tous les échanges avec le poste client sont chiffrés. Afin de limiter le nombre de ports vers les destinations demandées sur la gateway, les requêtes HTTP du Rewriter peuvent être redirigées dans une session sécurisée vers le composant Rewriter Proxy qui se chargera de contacter le serveur web destinataire.

Il n'y a pas de téléchargement de logiciel : aucune action n'est à effectuer sur le poste client.

3.1.3 Proxylet

Ce composant de SRA fournit un accès à des pages Web via la gateway et après authentification. La proxylet se présente sous la forme d'une applet Java téléchargée sur le poste utilisateur. Elle fonctionne comme un serveur proxy. Elle configure les paramètres proxy du navigateur afin que les flux soient redirigés sur l'applet, puis elle redirige le flux qui lui parvient en HTTPS (de préférence) vers la Gateway.

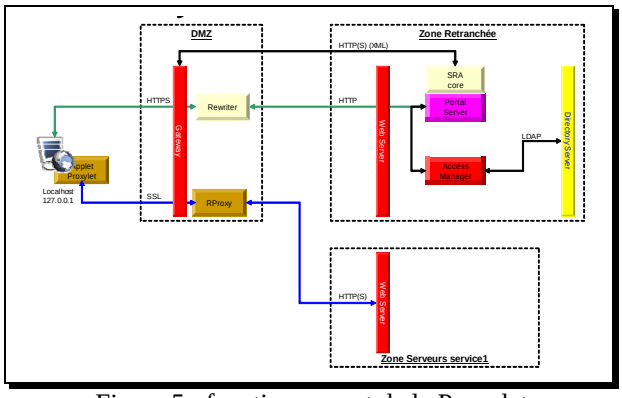

Figure 5 : fonctionnement de la Proxylet

Par opposition au rewriter, elle n'effectue aucune modification de contenu ni de requête (voir aussi le paragraphe 3.2.3).

3.1.4 Netlet

La Netlet permet l'accès à des applications internes (s'appuyant sur le protocole TCP) depuis un point quelconque de l'Internet. C'est une Applet Java téléchargée sur le poste client qui ouvre un tunnel SSL entre celui-ci et la Gateway. Elle peut établir des connexions en utilisant les protocoles IMAP, POP, Telnet…

La Netlet se configure avec la console d'administration d'*Access Manager* ou *Portal Server* selon la version.

Dans la console d'administration de l'ENT, on définit un numéro de port qui correspond à un service sur un serveur interne. De son côté le client doit configurer son application cliente vers le *localhost* et ce port ouvert par l'applet.

Exemple : l'administrateur a fixé le port 58412 pour accéder en SSH sur le server *monserveur.univ.fr*. L'utilisateur doit donc configurer son client SSH avec les paramètres localhost et le port 58412.

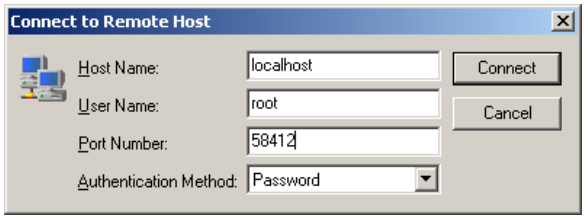

Figure 6 : *configuration du netlet*

Un composant complémentaire, le Netlet Proxy, permet de prolonger le tunnel chiffré au-delà de la Gateway, dans une zone retranchée par exemple et de limiter le nombre de ports ouverts entre la gateway et les services demandés.

3.2 Évaluation de la solution

Sun Microsystems met à disposition plusieurs versions de JES. Les dernières versions en date sont JES2005Q4 (*Portal Server* 6 & *Portal Server Secure Remote Access* 6) et JES5 (*Portal Server* 7.1 update 1 & Po*rtal Server Secure Remote Access* 7). JES 2005Q4 avait été testé il y a quelques temps et répondait à nos besoins. Il reste à valider si la version 7, qui est une évolution majeure et actuellement en cours de tests, assure la continuité des fonctionnalités.

3.2.1 Choix du système d'exploitation

JES est disponible pour RedHat EL WS/AS/ES 2.1, RedHat EL WS/AS/ES 3.0, Microsoft Windows (développement / Évaluation seulement), Solaris 8, 9 et 10. Au vu des versions de RedHat préconisées et du support uniquement en version d'évaluation pour Windows, le choix se porte tout naturellement vers Solaris 10. La stabilité et les performances en sont d'ailleurs bien meilleures pour ces produits conçus initialement sur ce système.

3.2.2 Les produits JES2005Q4 et JES5

Même si, à la base, on retrouve les mêmes briques, les systèmes sont disposés et se configurent différemment. L'interface d'administration de la version JES2005Q4 a été scindée en plusieurs éléments dans la nouvelle révision JES5.

Sous JES2005Q4, l'installation est la suivante : un serveur avec les briques *Directory Server*, *Access Manager*, *Portal Server*, *Secure Remote Access Core* et la console d'administration. Sur le second serveur, les éléments SRA Gateway, Rewriter, Proxylet et Netlet. Il faut au préalable avoir installé et configuré la suite JES sur le premier serveur. La Proxylet se configure avec l'interface web d'*Access Manager*. La Gateway se démarre en ligne de commande sur la Gateway elle même.

Sous JES5 l'installation ne peut être effectuée qu'une fois installés les OS, les couches réseau, et après avoir ouvert les communications entre les deux serveurs. L'installation est alors la suivante : installer et configurer JES5 sur le premier serveur avec les briques *Directory Server*, *Access Manager*, *Portal Server*, *Secure Remote Access* et *Monitoring Console*. Le second serveur reçoit les éléments *Secure Remote Access*. La Proxylet se configure sous l'interface Web *Portal Server* du premier serveur. Les services de la Gateway se démarrent à partir de la même interface.

3.2.3 Les services de la SRA

Le mode Rewriter : ce mode engendre la réécriture de toutes les URL contenues dans une page. Même si, dans tous les sites testés, nous n'avons pas rencontré de dysfonctionnement (sauf en cas de certificat SSL divergent), il n'en reste pas moins que cette méthode est susceptible de poser des problèmes avec certains sites web. Le coût de la réécriture grève les performances et rend la solution inexploitable en dehors d'utilisation bornées, comme par exemple une page de présentation ou de configuration. Les lenteurs de ce mode ont été constatées aussi bien en version JES2005Q4 qu'en version JES5 et nous ont incités à ne pas poursuivre les tests.

Le mode Netlet : il ne présente pas d'intérêt pour l'instant. Une première étude avait évalué le potentiel mais la solution VPN IPsec correspond plus à nos besoins.

Le mode Proxylet : la charge effectuée pour les tests ne permet pas de juger des performances, cependant aucun ralentissement d'accès n'a été constaté.

Sous JES2005Q4 les logs d'accès sont écrits sur le serveur de portail. Les logs sont détaillés et présentent toutes les informations dont nous avons besoins pour tracer un utilisateur : date, client ID, url,… Sous JES5 les logs d'accès sont écrits sur la Gateway .

Il faut aussi constater que le Proxylet ne fonctionne que sous les navigateurs suivants : Microsoft Internet Explorer 6.0 et supérieur, Netscape 6.0 et supérieur, Mozilla 1.0 et supérieur, Firefox 1.0 et supérieur.

3.2.4 Architecture et portée de l'outil

Pour évaluer la solution, nous avons déployé l'architecture matérielle détaillée dans la Figure 7. À terme, nous comptons mettre en place une architecture redondante intégrée dans l'ENT comme décrite dans la Figure 8.

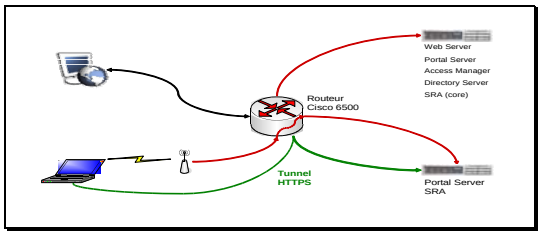

Figure 7 : *Architecture SRA*

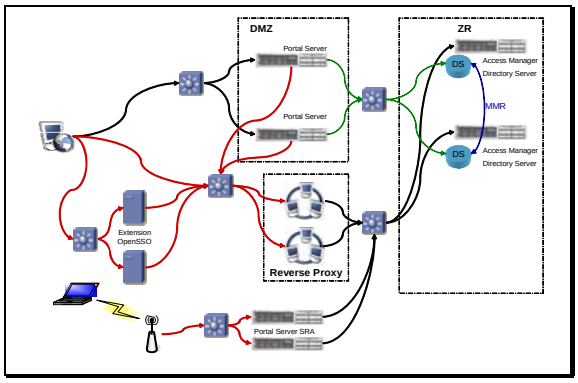

Figure 8 : *Architecture matérielle visée*

L'avantage d'intégrer les accès nomades (plus généralement, les accès sur des réseaux non sécurisés) dans l'ENT nous permet de proposer à l'utilisateur un portail dédié, fournissant le mode d'authentification correspondant à son profil et à la stratégie de sécurité mise en place et qui lui est appliquée. La centralisation du mode d'authentification par *Access Manager* nous permet de proposer des services multiples d'authentification (LDAP, RADIUS, Active Directory, JDBC…) mais aussi de fédération d'identité. L'ensemble est hautement disponible et cohérent. La souplesse de certains modules d'authentification permet de créer facilement des comptes temporaires (par exemple dans une base Radius), sans incidence sur le Système d'Information, et de proposer un contenu correspondant au profil de l'utilisateur (étudiant, personnel, visiteur, fédération…). La mire de choix de profils, des mécanismes d'authentification et de services accessibles est assurée par la brique *Portal Server*. Celle-ci gère dynamiquement un ensemble de portails « dédiés » et cela en fonction de la politique de sécurité.

Le système offrira également à l'utilisateur nomade l'authentification unique dès son entrée dans le SI. À terme, l'utilisateur sera redirigé vers la Gateway.

Conclusion

Cette solution prometteuse offre les avantages suivants :

- indépendant du système d'exploitation du poste client ;
- pas de configuration à réaliser[4] ;
- la Proxylet peut-être poussée vers l'utilisateur ;
- solution peu onéreuse comparée aux systèmes du même secteur ;
- pas d'équivalent à notre connaissance en terme de principe de fonctionnement ;
- cette solution, couplée à l'ENT, permet d'utiliser le profil de l'utilisateur et de lui fournir un contenu personnalisé et un service en conséquence (accès Internet), en droits comme en restrictions ;
- le code de la Proxylet, comme celui du portail, est open source.

Elle ne peut toutefois pas faire oublier les inconvénients listés ci-après :

- nécessite l'installation de JRE sur le poste de travail (pas de redémarrage) ;
- seul les navigateurs IE, Netscape, Mozilla et Firefox sont supportés ;
- il peut arriver qu'une mauvaise fermeture de l'applet entraîne que la configuration du proxy dans le navigateur reste active ;
- mise en œuvre de la solution JES qui peut être délicate (surtout la désinstallation) sans formation particulière, mais robuste une fois installée.

Seule la « Proxylet » de la brique *Sun Portal Server Secure Remote Access* présente, pour l'instant, un intérêt. La version JES2005Q4 répond à notre problématique. Le mode Rewriter pourra être un complément pour des accès vers des pages simples.

Ce travail a également permis de mettre en accord deux projets dissemblables. D'un côté, un projet « réseau » d'accès nomade sécurisé et, de l'autre, un projet SI d'accès unique personnalisé.

Bibliographie

[1] Éric Jullien (DSI Grenoble Universités), Le nomadisme : problématique et solutions, JRES, Marseille, novembre 2005.

[2] Sun Java System Portal Server 6 2005Q4 Deployment Planning Guide, chapitre 2 : Portal Server Secure Remote Access Architecture. Http://docs.sun.com/source/819-4155/2-sra.html

[3] Christine Lacombe, The GreCO-Universities portal, Eunis, Porto, juin 2002

[4] Philippe Beutin, « Infrastructure logicielle de portail : mise en œuvre d'une solution complète. », mémoire d'Ingénieur CNAM, 31 mars 2005.

[4] Conditions de fonctionnement de la Proxylet : un navigateur adéquat et la JRE installée.