

La xarxa privada virtual de la Universitat Pompeu Fabra: com garantir a la comunitat universitària un accés universal a la col·lecció digital

Autors:

Antoni Borràs
Servei d'Informàtica de la Universitat Pompeu Fabra
C/ Ramon Trias Fargas, 25-27
08005 Barcelona
Tel. 93 542 16 93
Fax: 93 542 17 99
A/e: antoni.borras@upf.edu

Carme Cantos
Biblioteca de la Universitat Pompeu Fabra
C/ Ramon Trias Fargas, 25-27
08005 Barcelona
Tel. 93 542 17 27
Fax: 93 542 17 99
A/e: carme.cantos@upf.edu

Roger Esparó
Biblioteca de la Universitat Pompeu Fabra
C/ Ramon Trias Fargas, 25-27
08005 Barcelona
Tel. 93 542 17 27
Fax: 93 542 17 99
A/e: roger.esparo@upf.edu

Marc Vives
Servei d'Informàtica de la Universitat Pompeu Fabra
Pl. de la Mercè, 10-12
08002 Barcelona
Tel.: 93 542 2772
Fax: 93 542 25 41
A/e: marc.vives@upf.edu

Resum

Des de l'any 1997, la Biblioteca de la Universitat Pompeu Fabra (UPF) ofereix als seus usuaris la possibilitat d'accedir a la seva col·lecció digital des de fora de les instal·lacions de la Universitat.

Els ràpids avenços tecnològics produïts en els serveis comercials d'accés a Internet (ADSL, cable, etc.) van convertir en obsoleta la solució adoptada en aquell moment.

En aquesta comunicació s'explica la solució SSL-VPN que la Biblioteca de la UPF ha implementat durant l'any 2004, per garantir als seus usuaris l'accés a la col·lecció digital amb independència del lloc des d'on s'hi accedeix i/o de la tecnologia de connexió a Internet que s'utilitza.

Paraules clau

col·lecció digital, accés, Internet, xarxa privada virtual, SSL-VPN

1. Introducció

Els darrers anys el món de les biblioteques, i especialment el de les biblioteques universitàries i de recerca, ha experimentat un gran canvi com a conseqüència de la incorporació en els seus fons de documentació publicada en format digital i distribuïda per Internet.

La col·lecció digital ha suposat moltes i importants millores per als usuaris, entre les quals destaquen: tenir accés immediat des de qualsevol ordinador autènticat sense que calgui traslladar-se físicament a la biblioteca, poder consultar simultàniament una mateixa publicació, tenir possibilitat de fer cerques sobre el text complet, i la interconnexió entre bases de dades bibliogràfiques o butlletins de sumaris i el text complet.

Des dels seus orígens, la Biblioteca de la Universitat Pompeu Fabra (UPF) ha apostat clarament per construir una col·lecció digital àmplia i rellevant, formada

per 7.000 títols de revistes electròniques, 160 bases de dades, i més de 1.000 llibres i diccionaris electrònics.

Aquesta col·lecció és possible gràcies a una forta inversió econòmica i suposa un gran esforç tecnològic i organitzatiu. Per aquests motius és imprescindible rendibilitzar-ne al màxim l'ús. Per tal de potenciar-lo, la Biblioteca de la UPF ha treballat per millorar-ne l'accés des del catàleg i des del web de la Biblioteca, i també ha realitzat un important pla de difusió i promoció de la col·lecció digital.

Tot i que les llicències o contractes que se signen amb els proveïdors de recursos electrònics estipulen que la condició d'accés sigui la de formar part de la comunitat universitària de la UPF, la major part de proveïdors controla l'accés als seus productes en funció de l'origen de la petició a Internet, és a dir, mitjançant una verificació de l'adreça IP. Per aquest motiu, molts membres de la comunitat universitària no poden utilitzar aquests recursos per a la seva tasca investigadora i/o docent quan es troben fora de la Universitat, ja sigui quan treballen o estudien des de casa seva, quan estan de viatge, etc.

En aquesta comunicació s'explica quina solució ha seleccionat i implementat la Biblioteca de la UPF durant l'any 2004 per permetre l'ús de la col·lecció digital a tots els membres de la comunitat universitària, amb independència de la tecnologia utilitzada i del lloc físic des del qual s'hi accedeix.

2. Punt de partida

L'any 1997 la Biblioteca de la UPF es va plantejar per primera vegada facilitar l'accés als recursos electrònics des de fora la Universitat. En aquell moment l'únic accés a Internet d'ús domèstic del que es podia disposar era de baixa velocitat: les diverses operadores de comunicacions oferien serveis d'accés Internet mitjançant mòdem (Infovía, Retenet, etc.). Moltes vegades aquest servei s'oferia en modalitat 'marca blanca', és a dir, no era ofert directament a l'usuari per part de l'operadora sinó mitjançant un intermediari (un banc, un fabricant d'ordinadors, una universitat, etc.) .

La modalitat 'marca blanca' va permetre a la UPF personalitzar l'adreça IP amb què es realitzava la connexió, i amb l'ajuda d'un servidor proxy-web, es va

aconseguir obrir l'accés als recursos d'informació electrònics de pagament des de l'exterior de la Universitat a tots aquells membres de la comunitat universitària que utilitzessin l'accés remot proveït per la UPF.

Aquesta solució aviat va quedar obsoleta pel dinamisme del mercat. Per un costat, molts usuaris utilitzaven serveis d'accés remot a Internet diferents del de la UPF, o es volien connectar des de llocs diferents al seu domicili. Per l'altra, l'aparició de la tarifa plana i, més endavant, la irrupció de noves tecnologies molt més potents que el mòdem, com l'ADSL i el cable. Aquests factors van fer que es plantejés la necessitat de buscar nous mecanismes.

L'accés a Internet ha esdevingut un servei universal que funciona lliurement d'acord amb les lleis de l'oferta i la demanda. Aquesta solució, en què s'obligava als usuaris de la UPF a utilitzar l'accés a Internet proveït per la Universitat per poder gaudir d'un determinat servei, va esdevenir obsoleta.

3. Selecció del producte

3.1. Anàlisi de possibles solucions

El Servei d'Informàtica i la Biblioteca de la UPF van iniciar la cerca d'una solució tecnològica que permetés a tots els membres de la seva comunitat l'accés, de manera fàcil i còmoda, als recursos de pagament independentment de la tecnologia, l'operador o el tipus d'ordinador que s'utilitzés.

Un dels primers passos d'aquesta tasca de cerca fou analitzar les solucions implementades per altres organitzacions que havien abordat el problema abans. Les solucions trobades es podien classificar en dos grans grups: les basades en l'intercanvi d'informació amb el proveïdor del recurs i les que utilitzaven xarxes privades virtuals (VPN) basades en l'ús del protocol IPSec.

OPCIÓ 1: Intercanvi d'informació amb el proveïdor

Dins aquesta categoria trobem els projectes PAPI (versió 1.0), Athens i altres sistemes similars. Es basen en la creació de mecanismes d'autenticació sòlids amb el proveïdor d'informació, normalment basats en infraestructura de clau

pública PKI (public key infrastructure), intercanvi de *cookies* en el navegador o l'utilització de *web-services*.

De seguida es van desestimar aquestes solucions ja que no eren universals. El fet que fos necessari que el proveïdor adaptés el seu programa informàtic per permetre el mecanisme d'autenticació adoptat podia originar problemes de compatibilitat amb molts dels recursos que la Biblioteca tenia contractats.

A més, en alguns casos hi podia haver una dificultat addicional, que és el de requerir, com a intermediària, una entitat que garantís l'autenticitat de la petició.

OPCIÓ 2. Sistemes VPN

Per VPN s'entenen les xarxes privades virtuals basades en protocols d'encapsulació com IPSec. En aquest cas, l'establiment d'un 'túnel' entre l'usuari i la Universitat fa que el proveïdor rebi una petició provinent de la Universitat, independentment de la localització real de l'usuari. Aquesta possibilitat va semblar, d'entrada, més interessant que l'anterior, ja que permetia solucionar el problema per a tots els recursos electrònics sense haver de contactar amb els seus proveïdors.

No obstant, ràpidament es van detectar una sèrie de dificultats. La principal era la necessitat d'instal·lar el client VPN a l'ordinador de l'usuari. Per una banda, era impossible garantir l'existència del programari per a tots els sistemes operatius (Windows, Linux, MAC, etc.) o dispositius (ordinadors, PDA, etc.) que podien tenir els usuaris, i de l'altra, instal·lar-se i configurar-se el client VPN podia ser complex per a l'usuari, tal com l'experiència amb l'accés via mòdem havia demostrat.

3.2. La solució adoptada

Totes aquestes solucions presentaven unes limitacions no desitjades i, sobretot, no resultaven completament satisfactòries pel que fa a la qualitat del servei que es volia prestar. La solució que es va valorar que complia el major nombre de requeriments va ser la de les xarxes privades virtuals basades en *proxy* de reescriptura, anomenades sistemes SSL-VPN.

Tot i que aquesta solució no estava pensada per ser aplicada a biblioteques, sinó que era una eina dissenyada per aconseguir una bona seguretat en transaccions mercantils o en xarxes dedicades al teletreball, es va veure que les seves funcionalitats es podien adaptar satisfactòriament.

Per explicar el funcionament de les SSL-VPN s'utilitzarà un exemple. Un usuari vol accedir des de fora de la UPF a la base de dades ISI Web of Knowledge (<http://isiknowledge.com/>) que, com la resta de recursos de pagament, només és accessible des d'una adreça IP de la UPF. La URL que haurà de demanar al navegador per accedir-hi mitjançant el servei SSL-VPN és la que es mostra a la figura 1.

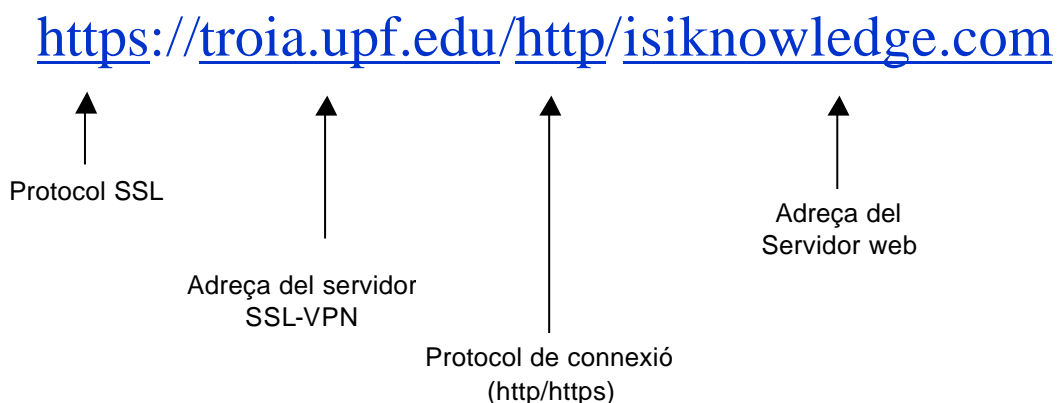


Fig. 1. URL utilitzant el servei SSL-VPN

En aquesta URL es pot veure que la informació es demana de manera encriptada (https), que se sol·licita al servidor SSL-VPN de la UPF (<http://troia.upf.edu>), i la que la informació de la URL a què es vol accedir (<http://isiknowledge.com/>) és una part més de la URL que s'utilitza per fer la connexió.

Una vegada el servidor SSL-VPN rep la petició, autentica l'usuari, demanant nom d'usuari i contrasenya i validant-lo mitjançant un servidor d'autenticació; demana la pàgina al servidor web el qual li serveix al reconèixer que ha estat sol·licitada per un ordinador amb adreça IP de la Universitat; reescriu totes les URL que conté de tal manera que comencin per <https://troia.upf.edu/http/...>; i posteriorment envia la pàgina al navegador de l'usuari.

Un cop l'usuari s'ha connectat al servidor SSL-VPN, aquest li reescriu, seguint l'estructura esmentada, totes les URL que vagi enllaçant en el curs de la seva navegació.

El funcionament d'un servidor d'aquest tipus és un híbrid entre les dues solucions explicades anteriorment: d'alguna manera es pot entendre com un servidor *proxy*, al posar-se al mig de la connexió entre navegador i servidor web i, per això, a vegades es parla de **proxy de reescriptura** (al basar el seu funcionament en la reescriptura de les URL), però també es pot entendre com un equip de VPN, al crear un 'túnel SSL' amb el navegador, per la qual cosa també s'anomena **SSL-VPN**.

L'únic requisit que tenen les solucions SSL-VPN és la utilització dels protocols *http/https* i de pàgines *html* en la connexió amb el proveïdor d'informació. Això suposa que les pàgines web construïdes amb *Flash* no siguin compatibles amb un sistema SSL-VPN, ja que el sistema no pot reescriure les URL que contenen les pàgines.

Després de comprovar que cap dels recursos de la col·lecció digital de la UPF contenen pàgines dissenyades amb *Flash*, es va decidir adoptar la solució SSL-VPN, la qual presenta els següents avantatges:

- Compleix l'objectiu d'assegurar l'accés als recursos electrònics amb independència del lloc físic des d'on es faci.
- Permet l'accés controlat mitjançant verificació d'adreces IP.
- És una solució universal, amb independència del navegador, del sistema operatiu i del proveïdor d'Internet utilitzat.
- És compatible amb les tecnologies de connexió a Internet actuals (mòdem, cable, ADSL, etc.).
- S'integra amb el directori LDAP (lightweight directory access protocol), de manera que només permet l'accés als membres de la comunitat universitària, tal com estableixen les llicències.
- No requereix la instal·lació de cap programari a l'ordinador de l'usuari.

4. Implementació

Una vegada decidida l'opció tecnològica, es va procedir a la selecció del fabricant. Al tractar-se d'una tecnologia emergent, l'elecció va ser difícil: les funcionalitats dels productes variaven entre fabricants, molts fabricants no tenien implantació en el nostre territori i existien també projectes incipients de creació de 'proxys' de reescriptura de programari lliure. Va ser necessària una anàlisi de les solucions disponibles en el mercat per trobar aquella que en més gran mesura podia garantir l'èxit del projecte.

L'opció finalment escollida fou la família 'VPN Gateway' del fabricant *Nortel Networks*. Aquest producte satisfieia les necessitats de la Universitat, s'integrava perfectament amb la infraestructura de xarxa i els mecanismes d'autenticació a utilitzar, i tenia una bona relació qualitat / preu.

Per tal d'instal·lar el producte es van adquirir dos servidors *Alteon VPN Gateway 3050* amb llicència de 25 usuaris simultanis cadascun d'ells. Els dos equips estan configurats en alta redundància: una avaria en un dels servidors no afecta la prestació del servei. L'empresa *Sistemas Avanzados y Tecnologia (Satec)* va realitzar la configuració i posada en marxa de l'equipament escollit.

4.1. Autenticació d'usuaris

La col·lecció digital de la UPF està formada per recursos contractats directament per la Biblioteca i pels recursos que conformen la Biblioteca Digital de Catalunya, que el Consorci de Biblioteques Universitàries de Catalunya (CBUC) contracta mitjançant subscripcions cooperatives.

D'acord amb les llicències que la UPF i el CBUC signen amb els proveïdors quan contracten un recurs electrònic, els col·lectius de la Universitat que hi poden accedir des de fora de les seves instal·lacions són:

- Estudiants de la UPF: estudiants matriculats a títols oficials (estudis de 1er, 2on i 3er cicle) i estudiants matriculats a títols i diplomes propis de la Universitat (màsters i cursos de postgrau en què el títol és expedit per la UPF)

- Personal docent i investigador de la UPF
- Personal d'administració i serveis de la UPF

Un cop es van determinar, amb la col·laboració de l'Assessoria Jurídica de la UPF, els col·lectius de la Universitat que corresponien exactament a les tipologies abans esmentades, es va iniciar l'estudi de com realitzar l'autenticació d'usuaris en el servei SSL-VPN.

Un dels requeriments que es van tenir en compte al seleccionar el producte SSL-VPN era que utilitzés el protocol LDAP per a l'autenticació dels usuaris. La UPF disposa d'un directori LDAP que conté tota la seva comunitat universitària i que s'utilitza per a la autenticació d'usuaris en l'ús de diferents aplicacions, entre elles l'accés al *Campus Global*, que és la Intranet de la UPF. Per a l'ús del SSL-VPN també es va decidir utilitzar el directori LDAP per a l'autenticació d'usuaris.

A més, la UPF també disposa de SAU (Servei d'Accreditació Universitària), que és una aplicació que determina a quins serveis i aplicacions tenen dret cadascuna de les persones que formen la comunitat universitària. Entre altres funcions, SAU alimenta el directori LDAP de la Universitat. Per tal d'habilitar l'autenticació d'usuaris al SSL-VPN es va haver d'afegir aquest com un servei a SAU i com un camp del directori LDAP. D'aquesta manera el sistema SSL-VPN només permet l'accés quan el nom d'usuari i la contrasenya són correctes i corresponen a un usuari que té dret a accedir al servei sol·licitat.

4.2. Com s'ofereix el servei

La Biblioteca volia oferir el servei de manera que fos molt senzill i còmode d'utilitzar i alhora molt visible.

El servei s'ofereix a través del lloc web de la Biblioteca, amb el botó *Connexió a recursos-e* tal com es veu a la figura 2. El botó només es veu en el cas que un usuari es connecti des de fora de la xarxa de la UPF. El control sobre la visualització del botó es realitza a través de la IP del client amb una funció JavaScript.



Fig. 2. Pàgina inicial del web de la Biblioteca des de fora de la xarxa UPF

El botó mostra *Connexió a recursos-e* o *Desconnexió de recursos-e* en funció de si el servei SSL-VPN no està activat o sí que ho està.

El fet que el web de la Biblioteca faci servir marcs (*frames*) ha suposat haver d'incorporar la funció JavaScript a cadascun d'ells –n'hi ha sis de diferents, multiplicats per tres idiomes, a part de la pàgina inicial també en tres idiomes-. Si no es fessin servir marcs, només modificant les tres plantilles de les pàgines, una per cada idioma, i regenerant les pàgines n'hi hauria hagut prou.

Una vegada es clica el botó de *Connexió a recursos-e* apareix una pàgina on els usuaris s'han d'identificar amb el seu nom d'usuari i contrasenya.

El servei SSL-VPN porta per defecte a una pàgina per a la introducció del nom d'usuari i de la contrasenya en què només es pot configurar el logotip de la capçalera i on no es pot incorporar cap explicació (fig. 3).

UNIVERSITAT POMPEU FABRA
Barcelona

Your login status is: not logged in

Username:

Password:

Login Service: default

Fig. 3. Pantalla de connexió per defecte del servei SSL-VPN

Així doncs, es va haver de crear la pàgina *Connexió a recursos electrònics des de fora de la UPF* (fig. 4) simulant la del propi servidor SSL-VPN. En aquesta pàgina s'ha pogut incorporar el text d'ajuda i amagar el desplegable *Login service*. L'opció *Login service* és útil per poder autenticar usuaris a diferents bases de dades, però si es deixa marcat *default* va buscant a totes les bases de dades disponibles sense haver de seleccionar-ne una. La UPF ha decidit configurar *default* de manera que sigui transparent per als usuaris.

Biblioteca de la UPF. Connexió a recursos electrònics des de fora de la UPF. Microsoft Internet Explorer

Arriba Eixida de Favorits Herramientas Ayuda

Direcció http://www.upf.edu/bib/recursos/acces_fora.htm

BIBLIOTECA
UNIVERSITAT POMPEU FABRA [Castellano](#) [English](#) [Catàleg UPF](#) [Inici](#) [Mapa Web](#)

Connexió a recursos electrònics des de fora de la UPF

Atenció! Aquest servei és en fase de proves, i durant aquest període només està disponible pel personal docent i investigador i pel personal d'administració i serveis que actualment està contractat per la Universitat.
(Els estudiants heu de seguir les següents [instruccions](#))

Els **recursos electrònics** -bases de dades, revistes, llibres i diccionaris electrònics- contractats per la Biblioteca de la UPF es poden consultar des de fora de la UPF establint la connexió des d'aquí. Abans de connectar-vos, llegiu detingudament tota la informació sobre el funcionament del servei, requeriments i condicions d'ús.

Connexió

Introduïu el vostre codi d'usuari i contrasenya de **Campus Global**. Aquest servei us portarà a la pàgina inicial del web de la Biblioteca i des d'aquí podreu navegar per tots els continguts i podreu consultar els recursos electrònics contractats per la Biblioteca de la UPF.

Codi:


Contrasenya:

[Funcionament del servei](#) [Requeriments](#) [Condicions d'ús](#) [Dubtes i suggeriments](#)

Fig. 4. Pàgina web de connexió a recursos-e des de fora de la UPF

Si un usuari s'equivoca a l'introduir el seu nom d'usuari o contrasenya, el servidor SSL-VPN mostra la pàgina original d'accés amb un missatge d'error. Aquesta pàgina, com ja s'ha dit, no es pot configurar, i tampoc es pot redirigir a una altra, de manera que pot ser confusa pels usuaris, ja que demana informació que no es rellevant, com ara el *Login service* que s'ha eliminat de la pàgina d'accés elaborada per la UPF. Aquesta incidència, que ja està notificada al proveïdor, està pendent de solució.

El servei SSL-VPN incorpora una utilitat de seguretat que esborra l'històric de pàgines web visitades durant la sessió oberta amb el navegador. La UPF ha deshabilitat aquesta opció per no haver de demanar als usuaris més accions que les estrictament necessàries.

Un cop autenticats, el servei porta els usuaris a la pàgina inicial del web de la Biblioteca i a partir d'aquest moment, i sense fer cap altre pas, ja estan connectats. Mentre s'està connectat apareix la icona  a la part inferior dreta del navegador i la URL que hi ha al camp *Dirección* del navegador comença per ***https://troia.upf.edu/http/***.

Per accedir als recursos electrònics s'han d'utilitzar els enllaços que hi ha a les pàgines del web de la Biblioteca. Per exemple, si es vol consultar les revistes electròniques de l'editorial Elsevier (ScienceDirect) s'ha d'anar, un cop connectats, a la pàgina de *Revistes electròniques* i fer un clic sobre l'enllaç, de manera que la URL que es visualitza, tal com es veu a la figura 5, és:

<https://troia.upf.edu/http/www.sciencedirect.com/>

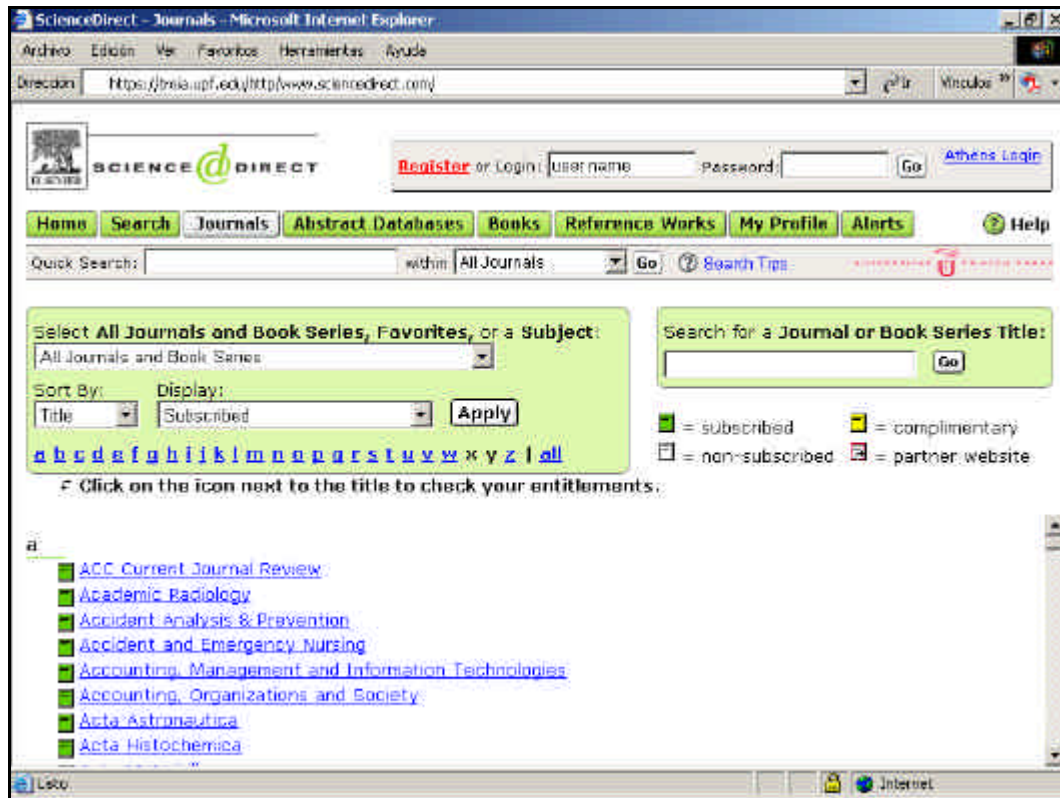


Fig. 5. Pàgina de ScienceDirect connectada a través del servidor SSL-VPN

Abans d'activar el servei SSL-VPN els recursos electrònics s'obrien a la mateixa pantalla sense els marcs de la Biblioteca, però ara, per facilitar la navegació i no perdre la connexió al servidor SSL-VPN, s'ha optat per obrir els recursos en una finestra nova. No obstant, si es fa clic a la icona *Home* del navegador, o es fan servir els *Favorites* es perd la connexió al servidor SSL-VPN i llavors cal tornar a connectar-se.

Per desconnectar la sessió cal fer clic a l'opció *Desconnexió de recursos-e* del marge superior dret de la pantalla. En cas que no s'utilitzi el servei durant deu minuts, el sistema es desconnecta automàticament. El temps de desconnexió és configurable.

4.3. Proves

Abans de posar en explotació el servei SSL-VPN es van realitzar una sèrie de proves per comprovar si tenia un funcionament adequat.

Aquestes proves s'agrupen de la següent manera:

4.3.1. Proves de visualització dels botons de connexió i desconnexió

La funció Javascript que es va programar per a la visualització dels botons de *Connexió a recursos-e* i *Desconnexió de recursos-e* es va desenvolupar per a navegadors Microsoft Internet Explorer 6.0.

Un cop vist el correcte funcionament amb aquest navegador, es van fer una sèrie de proves per verificar la seva compatibilitat amb els altres navegadors suportats a la UPF i d'ús estès a Internet : Mozilla 1.7.2 i Netscape 6.2. El resultat de les proves va ser satisfactori.

Per tal de poder realitzar les proves de visualització dels botons de *Connexió a recursos-e* i *Desconnexió de recursos-e*, en el Javascript es va parametritzar un conjunt de números IP de la xarxa UPF de forma que la connexió simulés que s'estava accedint al web de la Biblioteca des de l'exterior de la xarxa de la Universitat.

4.3.2. Prova de càrrega i proves de compatibilitat amb els recursos electrònics contractats

Es va realitzar una prova de càrrega dels servidors SSL-VPN en què també es va provar la compatibilitat d'accés a tots els recursos electrònics contractats per la UPF.

Per fer-ho es van repartir tots els recursos electrònics entre un grup de quinze membres del personal de la Biblioteca, de manera que durant un període de noranta minuts cadascú provés el funcionament d'uns sis recursos.

Durant la prova, els tècnics del Servei d'Informàtica van comprovar el rendiment dels equips SSL-VPN amb aquests quinze usuaris simultanis. La prova de càrrega va ser tot un èxit, ja que l'equipament va rendir adequadament i el personal que va realitzar les proves no va experimentar cap incidència relacionada amb la càrrega.

Per provar la compatibilitat de tota la col·lecció digital el personal de la Biblioteca es va connectar a totes les bases de dades, llibres, diaris i diccionaris electrònics, així com dos o tres revistes de cadascun dels paquets o serveis d'accés contractats per la Biblioteca.

Els elements que s'havien de tenir en compte al provar els recursos eren:

- Connexió: calia comprovar que el recurs electrònic reconegués que la connexió es realitzava des d'una adreça IP de la UPF i n'acceptés l'accés.
- Visualització: un cop dins del recurs, s'havia de comprovar que les pàgines web del recurs es visualitzaven correctament, tant en les pantalles de cerca, d'ajuda, així com a les pantalles de resultat.
- Realització de cerques: durant la prova s'havien de realitzar diferents cerques sobre el recurs, i verificar que el sistema no donava cap error.
- Visualització del text complet: un cop recuperats els resultats de les cerques, calia comprovar que es podia visualitzar sense problemes el fitxer que contenia el text complet.

Un cop fetes les proves, les quinze persones que les van realitzar van passar els resultats i les possibles incidències a l'equip que duia el projecte per tal d'elaborar-ne un informe. En aquest informe es van detallar els set recursos que van mostrar problemes i una explicació de les incidències, acompanyades d'impressions de pantalles.

Aquest informe es va enviar a l'empresa *Nortel Networks*, la qual ha comunicat que els problemes han quedat resolts en la nova versió del producte que sortirà a finals del mes de setembre del 2004.

5. Activació i difusió

El mes de juliol del 2004 es va activar el servei en període de proves restringit al personal docent i investigador i al personal d'administració i serveis de la UPF. Durant el període de proves es manté, per als estudiants, el sistema convencional que es basa en l'ús de mòdem i de l'accés a Internet proveït per la UPF.

Un cop el Servei d'Informàtica va posar en explotació els servidors que conformen el servei SSL-VPN, des de la Biblioteca es va procedir a activar el servei a través del seu web.

L'activació va consistir a habilitar els botons de *Connexió a recursos-e* i *Desconnexió de recursos-e* al marge superior dret de totes les pàgines del web de la Biblioteca. Paral·lelament es va actualitzar el contingut de la pàgina *Connexió als recursos-e des de fora de la UPF* de l'apartat *Els serveis que oferim* (fig. 6). També es va actualitzar aquesta informació a les diferents guies temàtiques i a les pàgines d'accés directe a bases de dades, revistes, llibres i diccionaris electrònics.



Fig. 6. Pàgina web on s'explica com connectar-se als recursos electrònics

La difusió de l'activació del servei es va realitzar mitjançant missatges de correu electrònic.

Per una banda es va enviar un missatge a tot el personal de la Biblioteca, explicant el nou servei, a quins usuaris anava destinat, com s'utilitzava, quins

problemes s'havien detectat fins al moment i quines eren les persones de contacte per si hi havia qualsevol incidència.

Per l'altra, es va enviar un missatge a totes les persones a les que anava destinat el servei durant el període de proves explicant com fer servir el nou servei.

Després del període de prova es considera l'activació d'aquest servei un èxit, amb una molt bona acollida per part dels usuaris, especialment per part dels professors i investigadors. Amb l'inici del curs 2004-2005 s'engegarà el servei com a definitiu ampliant l'abast també als estudiants i portant a terme una difusió més exhaustiva.

6. Conclusions

Les biblioteques necessiten rendibilitzar al màxim les seves col·leccions digitals, i per fer-ho cal fomentar al màxim el seu ús, mitjançant una bona difusió i la implementació de solucions que facilitin el seu accés i la seva utilització.

La solució que la Biblioteca de la UPF havia ofert fins al moment no era compatible amb totes les tecnologies de connexió a Internet disponibles al mercat, a banda de no ser una solució senzilla d'utilitzar. Per això la Biblioteca va apostar per trobar i implementar un nou servei que fos universal i que fos fàcil per a l'usuari.

Aquest requeriment, més el fet que aquesta solució no era un producte específic per a biblioteques, va complicar força la seva implementació.

En aquest sentit cal esmentar que la col·laboració conjunta, entre el Servei d'Informàtica i la Biblioteca, en la selecció i implementació d'aquesta solució, ha permès resoldre amb èxit tots els problemes que es van anar produint i ha permès oferir a la comunitat universitària un servei de valor afegit que ha tingut una molt bona acollida.

Això demostra que el treball conjunt i la suma de les sinèrgies d'informàtics i bibliotecaris aporten a la institució un alt índex de resultats i d'èxit en els projectes empresos.

Bibliografia

Agència Catalana de Certificació. *Serveis de certificació ditigal*. CatCert, 2004. "Què és la certificació ditigal?". <http://www.catcert.net/web/mon/quees.jsp>. [Consulta: 15/09/2004]

Armstrong, E.; et. al. (2003). *The Java Web Services Tutorial*. <http://java.sun.com/webservices/docs/1.1/tutorial/doc/>. Sun Microsystems. [Consulta: 15/09/2004]

Eduserv, Athens. Bath: Eduserv, 2004. <http://www.athensams.net/>. [Consulta: 15/09/2004]

Fratto, M. (2003). "The SSL Alternative". *Network computing*. <http://www.nwc.com/showitem.jhtml?docid=1423f3>. [Consulta: 15/09/2004]

Juniper Networks. Cop. 1998-2004. "VPN Decision Guide: IPsec or SSL VPN Decision Criteria". http://www.juniper.net/solutions/literature/white_papers/350037.pdf. [Consulta: 15/09/2004]

Nortel Networks. Cop. 1999-2004. "VPN Gateway 3050". http://www.nortelnetworks.com/products/01/vpn_gtwy_3050/doclib.html. [Consulta: 15/09/2004]

PAPI. RedIRIS, cop. 2003. <http://papi.rediris.es>. [Consulta: 15/09/2004]

Strayer, T.W. (2004). "Privacy issues in virtual private networks". *Computer communications*. Vol. 27, issue 6 (April), p. 517-521. <http://dx.doi.org/10.1016/j.comcom.2003.08.016>. [Consulta: 15/09/2004]

Webmaster E-learning Resources. *Selección de tutoriales y cursos sobre Tecnologías de la Información*. Webmaster, 2004. "VPN Tutorial de VPN'S". <http://www.wmaster.es/cursos/introvpn.doc>. [Consulta: 15/09/2004]