

Vnútrofiremné prepojenie zamestnancov

Ak pracujete v IT oblasti, je celkom bežné, že počas práce nevyužívate len váš osobný počítač, ale pristupujete aj na viacero iných systémov vo firemnej sieti. Pokiaľ sedíte v kancelárii nie je to najmenší problém. Situácia sa však mierne komplikuje ak nestíhate a potrebujete si prácu vziať so sebou domov alebo na služobnú cestu. Firemný notebook máte síce so sebou, ale k plnohodnotnej práci vám chýbajú systémy, ktoré sa nachádzajú v lokálnej sieti vašej firmy.

Tento problém sa dá riešiť viacerými spôsobmi v závislosti od toho, aké prostriedky na firemných systémoch využívate. Ak sa jedná iba o zdieľané súbory, môžete si ich napríklad prekopírovať na lokálny disk. Po čase používania týchto riešení však pravdepodobne zistíte, že sú v porovnaní s priamym prístupom vo firme časovo oveľa náročnejšie a menej pohodlné. Navyše vzniká množstvo rôznych kópií a verzií rovnakých súborov a budete musieť stráviť ďalší čas riešením problémov s ich synchronizáciou.

Ideálne riešenie by v tomto prípade malo zamestnancom umožniť služby poskytované firemnými systémami využívať zo sietí vonkajších. Ak by sme ale jednotlivé služby publikovali napr. forwardovaním portov na firewalle, bezpečnosť celého riešenia (a zároveň celej firemnej siete) by klesla na mieru bezpečnosti najmenej bezpečnej publikovanej služby. Preto je lepšie sprístupniť všetky služby jednotným spôsobom využívajúcim šifrovanie prenosov prípadne i viac-faktorovú formu autentifikácie používateľov. Takýmto riešením môže byť napríklad umožnenie vzdialeného prístupu do firemnej siete pomocou VPN - virtuálnej privátnej siete (z angl. virtual private network).

Ako VPN funguje

VPN siete sú často prevádzkované ako klient-server aplikácie, čoho príkladom môže byť OpenVPN alebo implementácia PPTP v MS Windows. VPN server vtedy beží priamo na firewallovom systéme a pri svojom spustení vytvorí virtuálne sieťové rozhranie (virtuálnu sieťovú kartu) a tým aj ďalší subnet firemnej siete. Server očakáva spojenia na vonkajšom rozhraní firewallového systému a vykonáva autentifikáciu VPN klienta, ktorý sa pripája z vonkajšej siete pomocou klientskej aplikácie. Po úspešnom overení je klientskému systému pridelená IP adresa z virtuálneho subnetu. Medzi serverom a klientom je následne vytvorený šifrovaný tunel, ktorým sú bezpečne prenášané všetky pakety smerované do a z lokálnej siete. Samozrejme spojenia medzi VPN a lokálnou sieťou je možné obmedzovať pomocou pravidiel firewallu a tým jednoducho určiť, ku ktorým systémom sa klienti môžu dostať.

OpenVPN

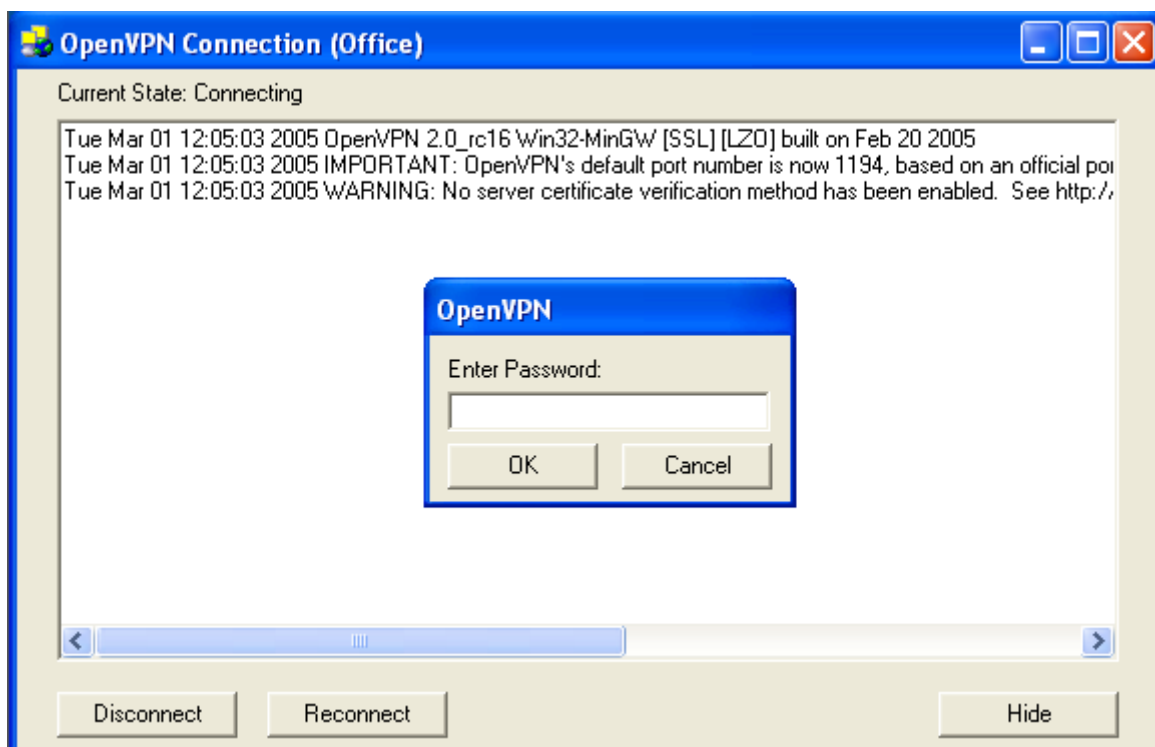


V našom návrhu vzdialeného prístupu do firemnej siete sme sa rozhodli pre open source softvérové riešenie OpenVPN. Dokáže vytvoriť šifrovaný VPN tunel medzi hostiteľskými stanicami alebo do vlastnej siete. S využitím architektúry klient-server je schopný zaistiť

priame spojenie medzi počítačmi za NATom a to bez potreby NAT akokolvek konfigurovať. Tento program bol vyvinutý Jamesem Yonanem a publikovaný pod licenciou GNU General Public License (GPL).

Umožňuje overiť nadviazované spojenie pomocou zdieľaného kľúča, digitálneho certifikátu alebo užívateľského mena a hesla. V nastavení multiklient-server je vydaný serverom pre klientov autentizačný certifikát, ktorý používa elektronický podpis a certifikačnú autoritu. K tomu využíva knižnice OpenSSL rovnako ako pre podporu protokolov SSLv3 a TLSv1.

OpenVPN je k dispozícii pre rôzne operačné systémy ako je Solaris, Linux, OpenBSD, FreeBSD, NetBSD, Mac OS X, a Windows a disponuje mnohými bezpečnostnými a ovládacími funkciami. Skladá sa z binárnej aplikácie pre klienta a server, konfiguračného súboru a jedného alebo viacerých súborov s kľúčmi v závislosti na použitej metóde overovania.



Vnútrofiremné služby

Aby mal vzdialený prístup cez OpenVPN do privátnej siete svoje opodstatnenie musíme ešte špecifikovať služby, ktoré bude táto sieť poskytovať. Týkajú sa hlavne vzájomnej komunikácie, lepšej kolaborácií pri práci a zdieľania dôležitých dokumentov.

Alfresco

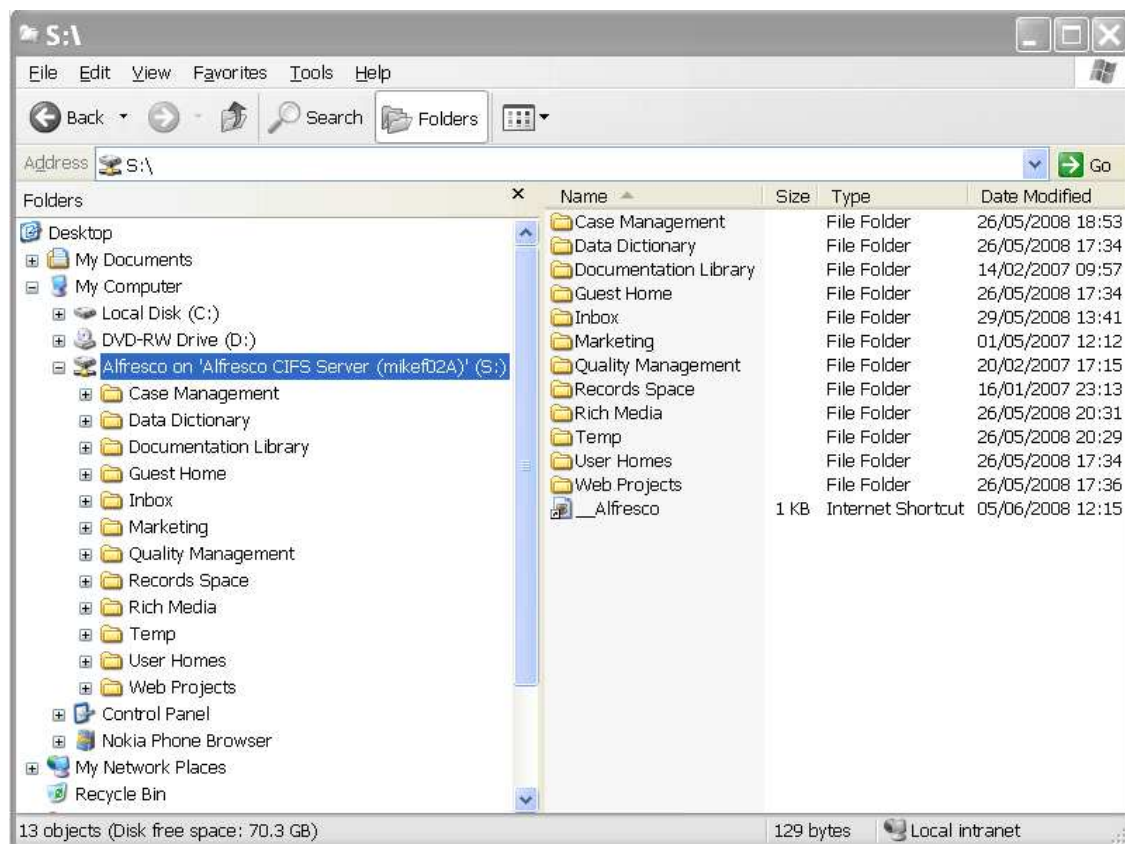


Alfresco je na JEE (Spring, Hibernate) postavený open source, ECM (Enterprise Content Management) systém, ktorý má za úlohu sprehľadniť, zjednodušiť a zrýchliť spoluprácu tak ako aj

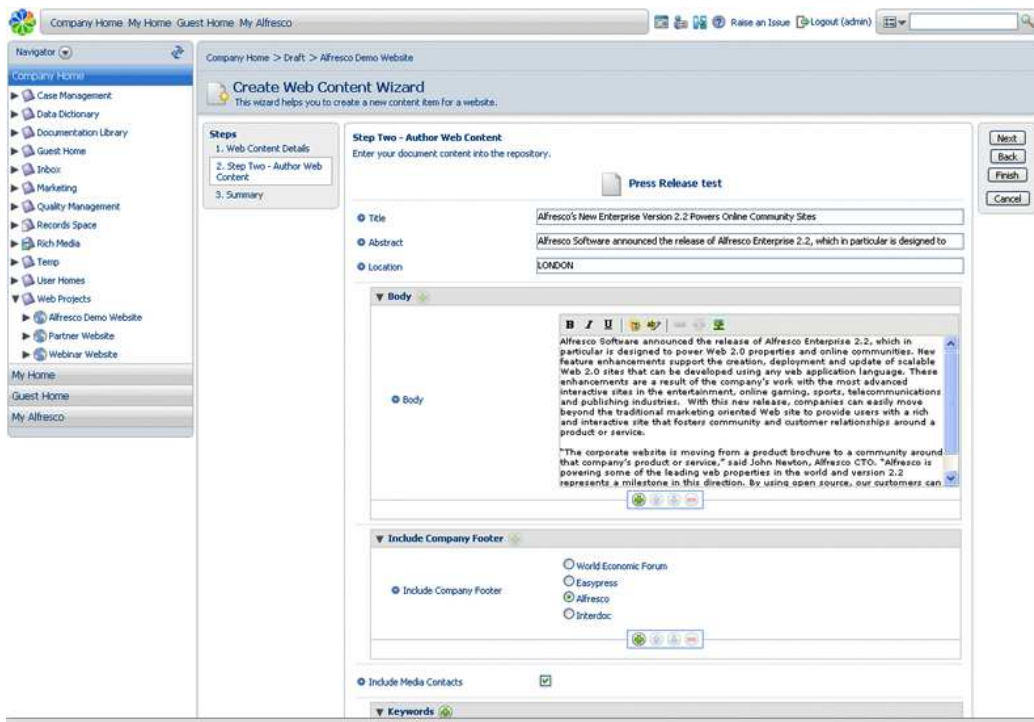
tok informácií a dát vo firme. Alfresco je produktom rovnomennej spoločnosti, ktorá bola založená v roku 2005 Johnom a Johnom Powellom. Asi hlavnými dôvodmi pre vznik tohto projektu boli podľa jeho autorov vysoká cena a náročnosť podobných produktov. Preto sa vývojári orientovali výhradne na open source technológie. Dá sa predpokladať, že jedným z dôvodov bola aj konkurencia ku Microsoft SharePointu.

Alfresco bude poskytovať v našej sieti nasledujúce prostriedky:

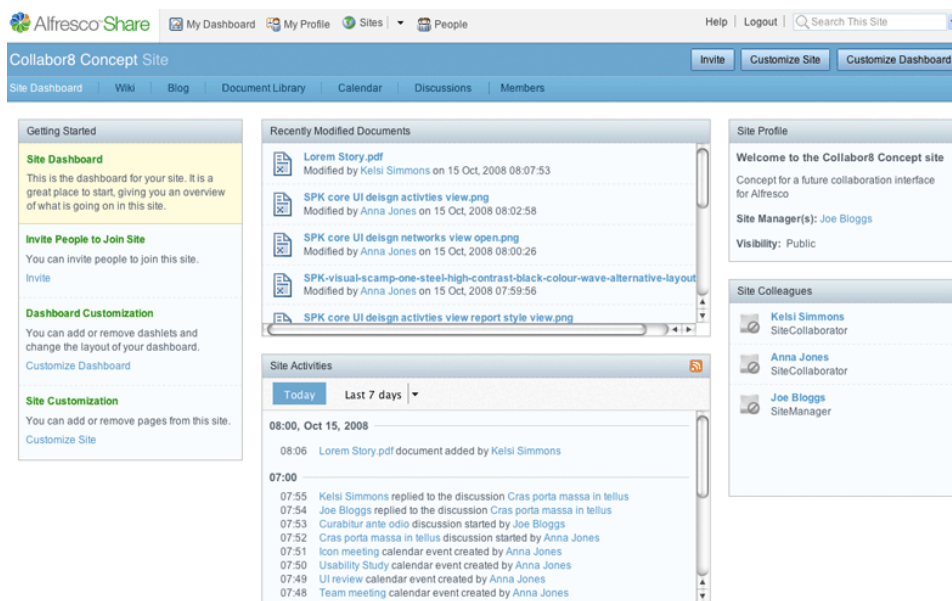
- **Document Management** - alebo správa dokumentov používa repository postavenú na štandarde JSR 170. Vyhľadávací stroj využíva Lucene indexáciu a umožňuje efektívne prehľadávať dátové priestory ako aj wiki, blogy a diskusie. Alfresco v dokumentovom sklade podporuje takzvanú funkciu SmartSpaces. Táto funkcia umožňuje priradiť každému zdieľanému dátovému priestoru (adresáru) určité pravidlá, napr. automatickú konverziu formátu alebo pridanie workflow daným súborom. Ďalšou funkcionalitou je napríklad verzovanie súborov, užívateľ si môže pozrieť, kto, kedy a čo menil v danom súbore, ďalej je to napríklad integrácia s MS Office alebo pridávanie tagov ku súborom, ktoré reprezentujú kategórie a s ich pomocou je neskôr možné efektívnejšie a rýchlejšie vyhľadávať. Repository je sprístupnená pomocou CIFS protokolu (a jeho jadra SMB, v unixovom svete známy pod menom SAMBA).



- **Web Content Management** - všetky funkcie popísané vyššie sú prístupné pomocou internetového prehliadača. Prezentačná vrstva je implementovaná pomocou JSF.



- Podpora spolupráce (Collaboration)** - pre podporu spolupráce Alfresco umožňuje vytvoriť užívateľské účty a každý užívateľ je schopný personalizovať si svoju domovskú stránku. Alfresco sa vlastne skladá z dvoch aplikácií. Prvou je Alfresco, ktoré slúži hlavne na správu dátovej repository - je v ňom možné vytvárať SmartSpaces a vykonávať akcie popísané vyššie. Druhou je Share, ktorá slúži ako domovská stránka každého užívateľa a je základnou platformou pre vytváranie užívateľských stránok pre spoluprácu. Každý užívateľ systému môže takúto stránku vytvoriť a povoliť buď verejný prístup, alebo určiť, ktorí užívatelia na ňu budú mať prístup. Na každej z týchto stránok sa nachádza wiki, blog, rozhranie pre prístup do skladu dokumentov (Document Library), kalendár, do ktorého je možné zapisovať udalosti a poznámky, ktoré vidia všetci užívatelia stránky. Na stránku je ďalej možné pridať linky na iné stránky, diskutovať o problémoch vo fóre alebo pridať RSS Feed zobrazujúci články. Toto všetko je rýchlo dosažiteľné pomocou dobre vyzerajúceho a intuitívneho webového rozhrania.



Bezpečnosť systému

Autori vybavili Alfresco štandardnou funkcionalitou, čo sa týka zabezpečenia. Možno vytvárať používateľov, role a skupiny. Alfresco možno integrovať s LDAP / MSAD / NTLM, pričom v prípade posledne menovanej možnosti Internet Explorer vie vykonávať automatické prihlásenie (čo sa týka aj zdieľanie zložiek).

Vývojári nezapomenuli na nevyhnutný audit - teda veľmi podrobný log, čo sa s dokumentmi presne deje. Nasadením CMS systému vo firme odpadnú problémy, kedy nadriadený bude tvrdiť podriadenému, že dokument neschválil. Alebo ešte bežnejšie a obligátne vydania verzie dokumentu, ktorá nemala byť zverejnená. CMS systém týmto chybám nevie zabrániť. F firme ale dáva nástroj, ktorým je poverená osoba schopná vystopovať, ako to naozaj bolo (kto inkriminovaný dokument prepísal alebo schválil).

Vnútrofiremná VoIP komunikácia – Asterisk

VoIP je skratka pre „Voice over IP“, čiže prenos hlasu cez IP protokol. VoIP v podstate funguje tak, že telefonický hovor je skonvertovaný z analógového signálu do digitálneho formátu a potom sa prenáša prostredníctvom IP paketov. Hlavnou výhodou VoIP je možnosť smerovania cez Internet ako média, čím sa prakticky eliminujú nároky na budovanie prepojenia k pobočkovej ústredni alebo koncovému telefonickému aparátu ako v prípade pevných liniek.

SIP reprezentuje Session Initiation Protocol. SIP je pomerne jednoduchý protokol, ktorý má vlastnosti podobné HTTP a SMTP. Týmto vlastnosťami SIP dovoľuje aj pomerne jednoduché riešenie prípadných problémov. SIP požíva buď TCP alebo UDP, no väčšina poskytovateľov využíva UDP metódu. Vďaka jednoduchej konfigurácii a skutočnosti, že je vo všeobecnosti

považovaný za "ľahký protokol", prevažná väčšina poskytovateľov VoIP využíva SIP protokol pre svoje služby.



Asterisk je Open Source projekt pobočkovej ústredne (IP PBX) , ktorý je postavený na Linuxe, jeho možnosti sú praktický neobmedzené. Podporuje VoIP protokoly: SIP, H323 a IAX. Asterisk tiež podporuje širokú škálu hardware, ktorý vám umožní pripojiť vašu Asterisk ústredňu pevným okruhom telekomunikačných operátorov FXO, ISDN BRA, PRA, E1.

Nastavenie Asterisk server pre firemné použitie alebo pre domáce použitie je v podstate rovnaké a líši sa len počtom IP pobočiek a samozrejme pripojením VoIP a klasických operátorov. Veľkým problémom hlavne vo firemnom prostredí je používanie akýchkoľvek P2P aplikácií a sietí, čo spôsobuje starosti nejednému administrátorovi. Preto je potrebné počítať, že šírka dátového pásma nemusí byť stabilná a kvalita VoIP hovoru nebude postačujúca. Samozrejme mnoho v tomto ohľade je možné zmeniť, ako napr. zmeniť používateľské návyky (asi najzložitejší problém), správne konfigurovať firewall, použitie funkcií prioritizácie VoIP služieb QoS a UDP služieb.

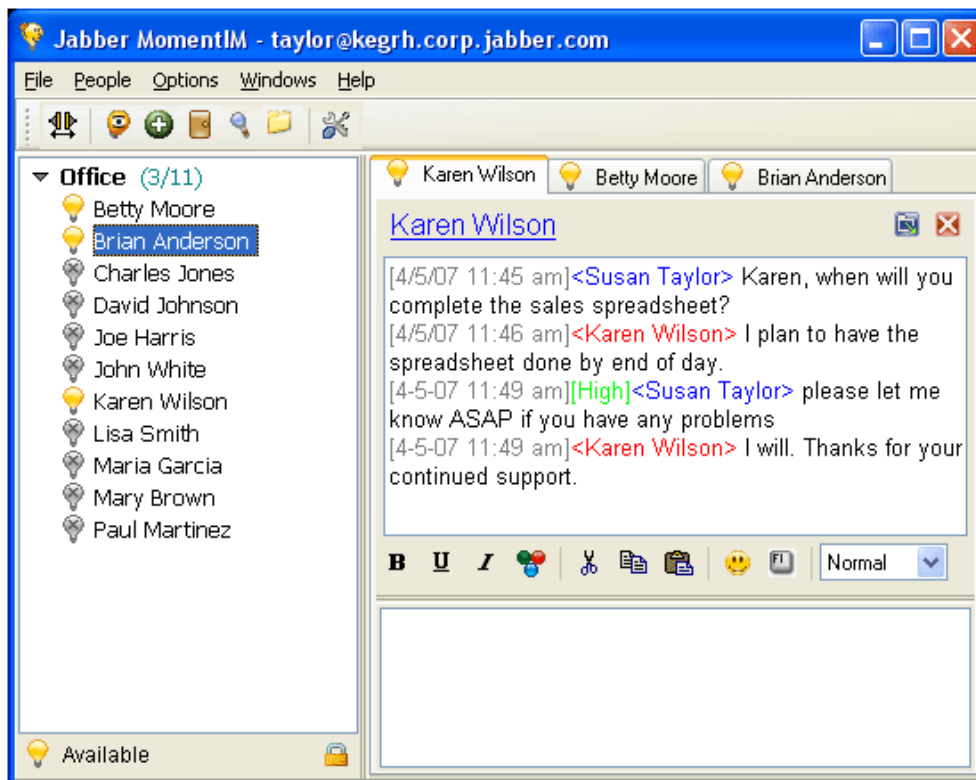
Instant messaging – Jabber



Jabber je otvorená technológia pre posielanie krátkych textových správ (IM - instant messaging), ponúka alternatívu k proprietárnym IM technológiám ako ICQ, AIM, MSN a ďalším. Zároveň nám však poskytuje možnosť využívať vaše kontá týchto IM služieb v rámci Jabber-u prostredníctvom 'konektorov/transportov'.

Ďalšie výhody jabberu:

- Zoznam vašich kontaktov je uložený na serveri.
- Jabber je bezpečný. Konto je chránené heslom. So serverom sa dá spojiť pomocou bezpečného protokolu SSL a používať šifrovanie a digitálny podpis PGP.
- Jabber je dostupný pre operačné systémy: GNU/Linux, UNIX, MacOS, Windows 95/98/ME, Windows NT/2000/XP/Vista, ako aj pre mobilné a iné zariadenia (multiplatformovo): Java, Mozilla, Newton, Windows CE, a iné.



Použitá literatúra

<http://wiki.alfresco.com/>

<http://www.linuxos.sk/clanok/324/index.html>

<http://weblog.morosystems.cz/ostatni/alfresco-nahrada-za-sharepoint>

<http://www.linuxexpres.cz/business/alfresco-cms>

<http://www.root.cz/clanky/voip-uz-nie-je-alternativa-ale-buducnost/>

<http://www.jabber.sk/>