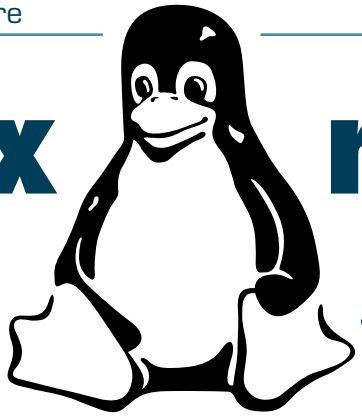
Linux na serveru

I. díl



Ivan Bíbr

Dnes se podíváme do oblasti, ve které je Linux neobyčejně silný a má zde velmi dobrou pozici. Jestliže při nasazení na desktop občas narazíme na problémy s dostupností aplikací, viz minulý díl seriálu, pak na serveru Linux pravděpodobně uspokojí většinu požadavků naprosto bez problémů. Linuxové servery jsou nejvíce rostoucí oblastí na serverovém trhu, a to ještě nikde není započítán fakt, že k provozu serveru nemusíte Linux v podstatě ani kupovat, a dost často se tak také děje. Tento díl jsem se rozhodl pojmout více prakticky než předchozí, teorií napěchované díly. Řekneme si, jak použít Linux pro připojení firemní sítě k internetu, a rovnou to i prakticky, s ukázkami krok po kroku, provedeme.

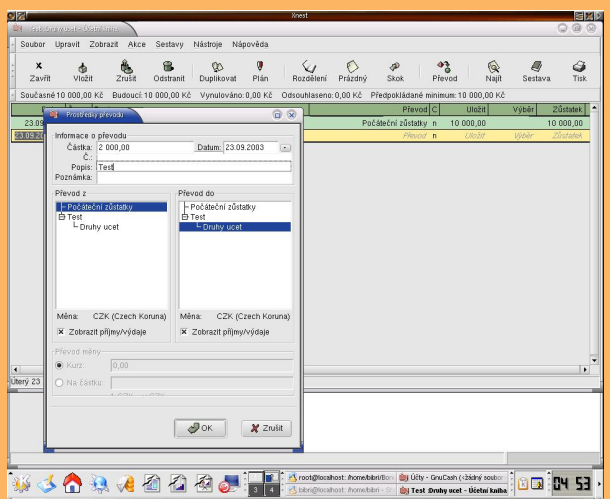
Podnikové aplikace – dodatek

Než se však do serverů pustím, musím vyřešit resty z minula. Ozval se mi aktivní čtenář s připomínkou, že jsem ve výčtu podnikových aplikací a účetních systémů na několik zajímavých projektů zapomněl. Omlouvám se tímto za opomenutí a pokusím se zjednat nápravu. První program, o kterém bych měl napsat, je GnuCash. GnuCash mohou použít ti z vás, kteří účtují v jednoduchém účetnictví, a lze pomocí něj snadno vést evidenci příjmů a výdajů. Obsažen je patrně v každé větší distribuci Linuxu, takže nemusíte nic stahovat. Ukázku vidíte na obr. 1.

Rozpracovaným „free“ projektem je MIS, podvojné účetnictví pro Linux. Celý projekt je napsán v PHP a běží přes webové rozhraní s napojením na databázový stroj PosgreSQL. Podle slov autora není doladěn, což se zdálo i mně. Dalším účetnictvím, tentokráte pro konzolu, je bohužel již delší dobu nevyvíjený Pub. Ani jeden zmíněný projekt není zařazen do žádné mně známé distribuce Linuxu, musíte si jej stáhnout a vyzkoušet sami, připojuji proto i odkazy. Zajímavým produktem slovenských kolegů je též podvojné účetnictví Tučniak vyvíjené pod licencí GPL. Koncem září by se měla objevit jeho první stabilní verze a očekávám, že si někdo dá práci s úpravou na české podmínky.

Tolik tedy z oblasti svobodného softwaru. Z komerčních produktů jsem zapomněl na dva významné projekty. Kdysi jsem četl na serveru Root o produktu firmy The Database Factory (TDF) jménem Economy. Economy je, nebo spíše má být, plnohodnotný a důsledně modulárně postavený informační systém pro podniky. Uvedení na trh mělo proběhnout počátkem roku 2003, ovšem nezaznamenal jsem jej a webové stránky TDF nejsou v době psaní článku dostupné. Možná až je zkusíte, dozvíte se více než já. Další firmou, tentokráte s fungujícím produktem, je Ortex a jeho informační systém Orsoft. Ten obsahuje kromě standardních účetních modulů také moduly pro řízení výroby, obchodu a lidských zdrojů. Multiplatformní klient systému napsaný v Javě běží i na Linuxu. Orsoft se může chlubit nasazením např. v Aero Vodochody nebo na Správě Pražského hradu.

Tímto bych téma podnikových aplikací ukončil.



Obr. 1: Systém pro vedení jednoduchého účetnictví GnuCash

Obr. 2: Sdílení připojení v Mandrake Linuxu – krok první, výběr zařízení připojeného k internetu

Linux a připojení k internetu

Linux je velmi často využíván jako vstupní brána do internetu. V případech, že máte jako firma k dispozici málo IP adres, často jen jednu, sdílejí všechny vaše počítače na interní sítí navenek právě tuto jednu adresu. Potřebujete k tomu buď specializovaný hardware, nebo jeden počítač, který má minimálně dvě síťová rozhraní a patřičnou funkcí disponuje alespoň softwarově. Český název „Sdílení připojení“ byl patrně odvozen od faktu, že daný počítač opravdu jakýmsi způsobem sdílí připojení k internetu ostatním počítačům v síti.

Původní označení v angličtině zní Network Address Translation (NAT), česky překlad adres, a jeví se mi přesnější. Systém totiž opravdu překládá adresy z vaší vnitřní sítě a naopak. Funkci překladu adres má v sobě zabudováno přímo linuxové jádro, takže v podstatě k připojení vnitřní sítě do internetu toho o mnoho více nepotřebujete. Záleží hodně na tom, jaký komfort při nastavení budete požadovat. Umíte-li nebo znáte někoho, kdo umí, nakonfigurovat NAT „ručně“ pomocí příkazu iptables, postačí vám pro ochranu menší sítě jakýkoliv vysloužilý počítač s procesorem Pentium. Možná i starším – zde záleží na výběru linuxové distribuce, některé novější distribuce vyžadují procesory i586 a vyšší.

Podíváme se teď, jak nastavit překlad adres trochu komfortněji. Chcete-li pracovat v grafickém rozhraní, doporučuji počítač s minimálně 64MB RAM, výkonově postačí jakékoliv Pentium. Možná si při konfiguraci chvíli počkáte, ale pro překlad bude stačit bohatě. Tedy, vzhledem k zaměření časopisu nepředpokládám extrémně velké sítě, tam by možná nestačil. Jako základ jsem použil instalaci Mandrake Linuxu, minimální instalaci s grafickým rozhraním, která vyžaduje 300 MB diskového prostoru. Počítač je Pentium II se 128 MB paměti, tedy žádný výkonný stroj. Instalaci jsme probírali v prvních dílech seriálu a nebudu se k ní již vracet.

Odkazy:
Gnucas: www.gnucash.org
MIS pro Linux: http://mis.webpark.cz
Pub: www.penguin.cz/~tycho
Tučniak: www.tucniak.sk
TDF: www.tdf.cz
Orsoft: www.orsoft.cz

Nyní již k samotnému postupu. Využil jsem všech výhod moderních distribucí a použil jsem jednoduchého „Průvodce sdílením připojení“ Mandrake Linuxu, který množství vaší práce redukuje na čtyři klepnutí myši. Na obr. 2 vidíte první krok – průvodce se zeptá, které síťové rozhraní je připojeno směrem ven. V následujícím kroku, viz obr. 3, zadáte, které rozhraní vede do vnitřní sítě. Tím je v podstatě vytvořen onen spojující most, který přenáší data z vnitřní sítě a naopak.

Další postup jsem si trochu „zkomplikoval“, abych vám mohl ukázat, jak bude síť nastavena. Kdybych nezvolil ruční konfiguraci, průvodce by sám nastavil IP adresu vnitřního rozhraní na 192.168.0.1 a nainstaloval a nastavil DHCP server pro připojované klienty. Já jsem se po volbě ruční konfigurace dostal k dialogům, které vidíte na obr. 4 a 5.V prvním jsem změnil nastavení IP adresy vnitřního rozhraní, druhý jsem ponechal tak, jak byl. Průvodce chvíli instaloval potřebné komponenty a pak oznámil, že vše je hotovo.

A opravdu bylo. Na vnitřní podsíti stačilo zapojit počítač a nakonfigurovat jej tak, aby získal konfiguraci sítě pomocí protokolu DHCP. Můj nový server přiřadil pomocí DHCP protokolu zapojenému počítači správné vnitřní IP, nastavil bránu a DNS a bylo to. Nelíbí-li se vám použití DHCP, můžete server samozřejmě vypnout, ale v takovém případě musíte mít správně nakonfigurovány klienty.

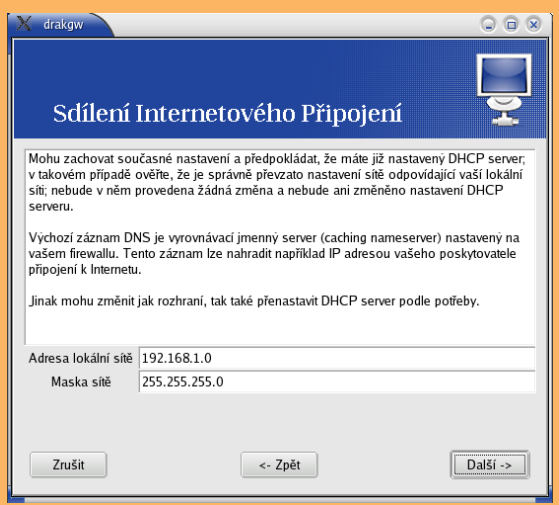
I s instalací zabrala tato část necelou půlhodinu. Dá se říci, že do třiceti minut od zahájení práce byla má pokusná lokální síť připojena k internetu.

Firewall

Firewall chránící síť před nebezpečím zvenčí je další z častých nasazení Linuxu. V běžných případech u menších sítí bývá instalován na stejném stroji, který provádí překlad adres popsaný v předchozí kapitole. Firewall má za úkol blokovat porty směrem dovnitř a případně i ven, zahazovat ze sítě ty pakety, které nepovažujete za vhodné, a minimalizovat riziko napadení.

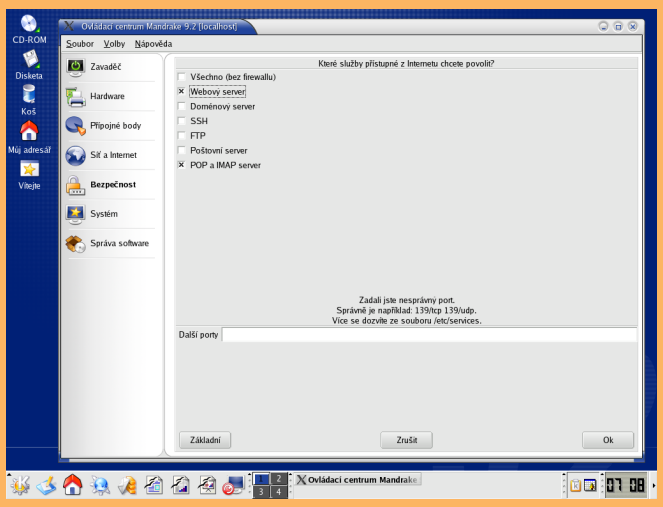
Ještě než se pustíme do jednoduché konfigurace, chtěl bych upozornit, že ani sebelepší operační systém vaši síť neochrání v případě, že na něj někdo nebude dohlížet. Pozor, platí to pro všechny systémy, ať už si reklama říká, co chce! Platí to i pro Windows anebo třeba pro OpenBSD, které se chlubí tím, že za posledních sedm let má pouze jednu (a to

Obr. 3: Výběr zařízení určeného pro připojení vnitřní sítě



Obr. 4: Nastavení zařízení pro vnitřní síť

Obr. 5: Nastavení DHCP serveru pro připojované stanice



Obr. 6: Shorewall: firewall jednoduchý na konfiguraci

je výkon!) chybu ve standardní instalaci. Platí to pro specializovaný hardware (Cisco), ve kterém stejně běží operační systém. Především je důležité hlídat a včas aplikovat záplaty – opravy chyb. A to platí i pro Linux. Jakmile se vám někdo na počítač s firewallem dostane, vidí obvykle dále směrem do sítě a může začít zkoušet, kudy proniknout například k citlivým datům.

Zásada číslo jedna platná na všech systémech: čím méně softwaru bude na počítači přístupném z internetu nainstalováno, tím méně záplat budete muset aplikovat. Zároveň s tím bude menší riziko, že objevená bezpečnostní chyba v nějakém programu postihne právě vás a někdo ji stačí zneužít. A protože jsem chtěl použít stejný počítač pro funkci firewallu i překlad adres, provedl jsem v předchozím kroku opravdu minimální instalaci.

Zásada číslo dvě: konfiguraci je mnohem bezpečnější tvořit stylem „všechno zakázat, povolit, co je potřeba“. Opačný postup bude mít sice tu výhodu, že vše bude okamžitě fungovat, ale zároveň bude mít jednu zřejmou a velikou nevýhodu. Vše bude povoleno! A to může mít v některých situacích fatální následky.

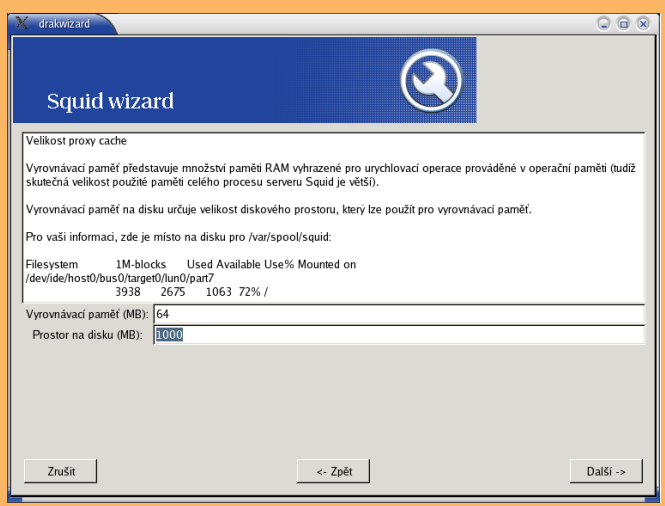
Funkce firewallu má Linux integrovány v jádře systému, stejně jako překlad adres. Pro jeho aktivaci a nastavení jsem opět použil průvodce. Ten je velmi jednoduchý, disponuje výběrem standardních portů (viz obr. 6).

Komu tyto porty nestačí, může zadat další. Po vybrání povolených portů a klepnutí na OK byl firewall nastaven.

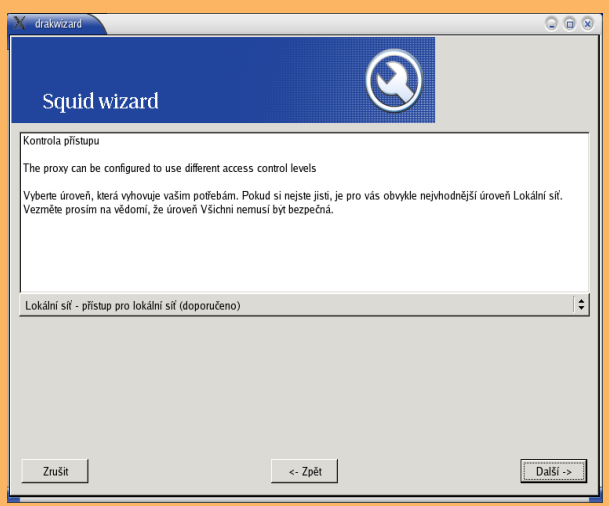
Celá operace trvala i s instalací balíčku potřebného ke zprovoznění tohoto jednoduchého firewallu asi pět minut. Protože Mandrake Linux používá na tyto funkce nástroj Shorewall, nic teoreticky nebrání odinstalaci průvodců a celého grafického rozhraní z počítače s tím, že nastavení je možno ovládat vzdáleně například pomocí nástroje Webmin. Ten má pro Shorewall příslušný modul, jak vidíte na obrázku č. 7. Chtělo by to ještě trochu práce s konfigurací, ale výsledek by stál za to. Kromě toho vždy zbývá možnost konfigurace z příkazové řádky...

Proxy server

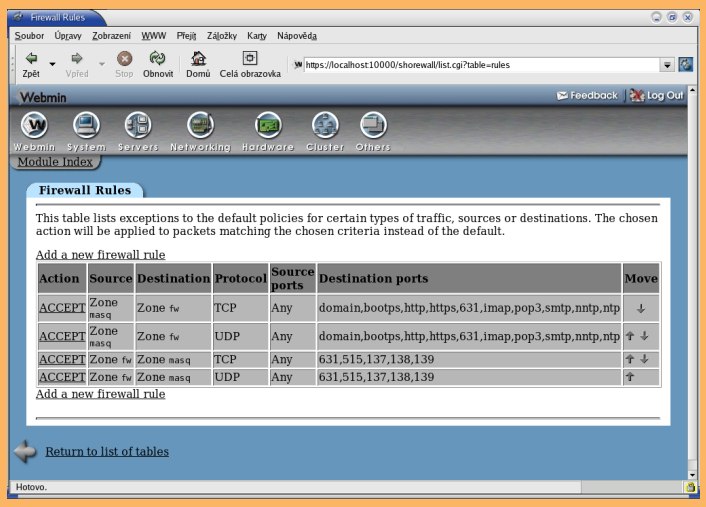
Dalším krokem při připojení mé testovací sítě bylo nastavení proxy serveru. I ten jsem instaloval na stejný počítač jako firewall a NAT. Proxy server sice není nezbytnou součástí, ale řekněme, že dokáže silně zpříjemnit práci s internetem, zvláště při slabém připojení. Proxy server, v mém případě www proxy Squid, uchovává u sebe již jednou přenesená data (např. webové



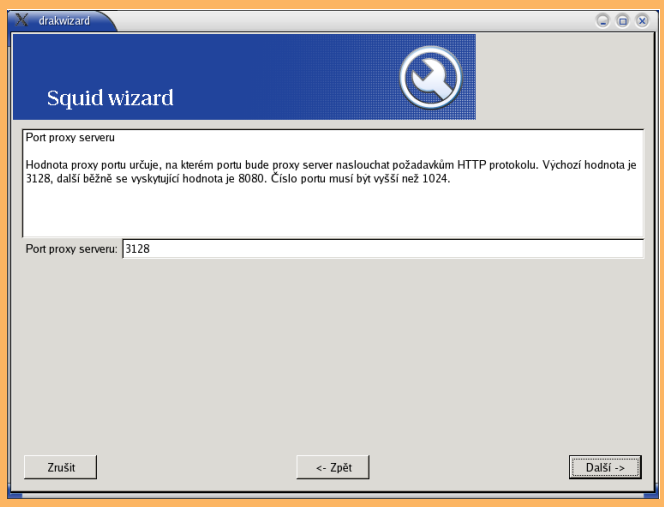
Obr. 9: Nastavení velikosti vyrovnávací paměti na serveru



Obr. 10: Přístup k proxy je povolen pouze lokálním počítačům



Obr. 7: Konfigurace shorewallu vzdáleně pomocí aplikace Webmin



Obr. 8: Zadáváme port proxy serveru Suid

stránky). Ty se pak při dalším přístupu nemusí stahovat až ze vzdáleného serveru, samozřejmě pokud se nezměnily.

Asi tušíte, že pro instalaci jsem opět použil průvodce. Instalace balíčků s proxy serverem Squid a patřičným průvodcem zabralo opět několik málo minut. Nastavení proběhlo v několika krocích. Nejdříve proběhlo nastavení portu pro přístup k proxy serveru (viz obr. 8), kde jsem nechal standardní port 3128. Pak se průvodce zeptal na velikosti vyrovnávací paměti na serveru (obr. 9). V dalším kroku jsem zadal, že proxy mohou využívat jen počítače z lokální sítě (obr. 10), a jako poslední jsem pouze zkontroloval nastavení.

Všechny parametry proxy serveru vidíte pohromadě na obr. 11.

Nastavení www proxy zabralo maximálně deset minut i s nastavením klienta na lokální síti.

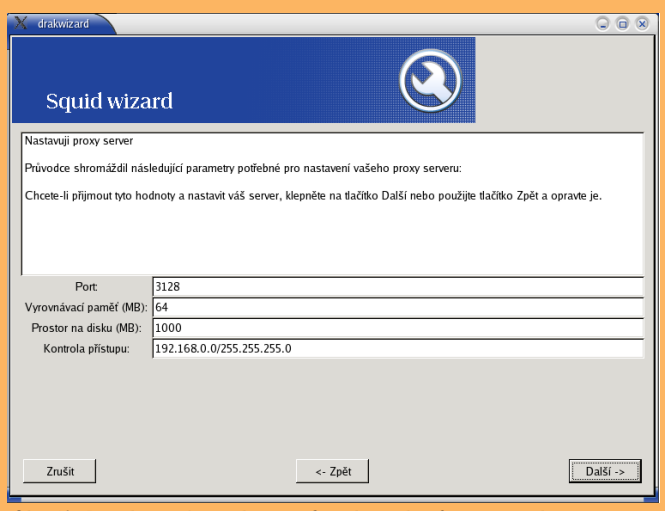
Diskuze řešení

Pokusím se nyní shrnout celý provedený postup a poukázat na jeho výhody či nevýhody. Prezentoval jsem řešení na distribuci, kterou znám nejlépe, s využitím dostupných průvodců, a tak by se mohlo zdát, že jde o specifický a jinde nepoužitelný způsob. Není tomu tak. Na podobných „user-friendly“ distribucích, jako je SuSE nebo RedHat, najdete nástroje podobné. A pokud ne, lze s úspěchem použít nástroje obecné jako například prezentovaný Webmin nebo třeba KMyFirewall na nastavení firewallu.

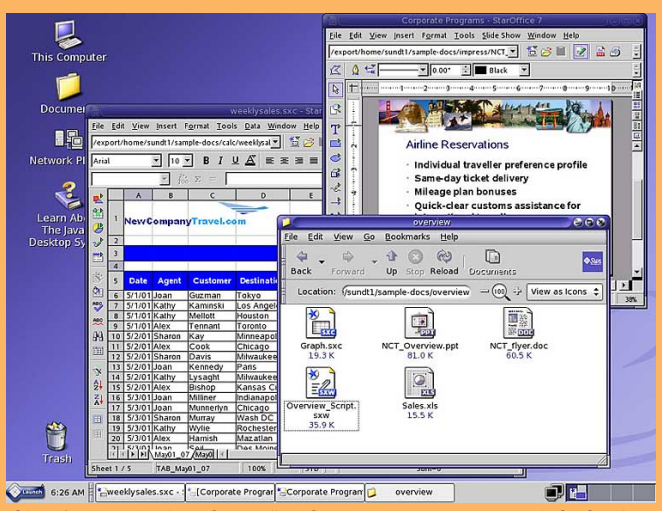
Finanční nároky jsou nevelké, spíše malé. Starý počítač třídy Pentium nebo v lepším případě Pentium II zvládne připojení menší sítě do internetu se všemi výše zprovozněnými funkcemi bez potíží. Určitě nebude problém někde takový odložený stroj najít, vybavit dvěma síťovými kartami a využít tímto způsobem. Software můžete koupit, ale nemusíte, v podstatě vám stačí vypálená média od přítele nebo speciální verze z časopisu. Chcete-li podporu a pomoc například při instalaci, můžete sáhnout po nějaké linuxové krabici, cenově v řádu tisícikorun. Prezentované řešení není nijak licenčně závislé.

Můžete je použít z jedněch instalačních médií ve třiceti pobočkách na třiceti počítačích. Pozor, toto se liší od distribuce – můžete narazit na některé speciální licenční podmínky, které zavedlo v poslední době například SuSE. Použitým programům je naprosto jedno, připojuje-li se přes ně deset nebo deset tisíc uživatelů. Při zvýšení počtu uživatelů tak zůstane otázkou pouze výkon hardwaru, ale při desítkách uživatelů nebudete muset toto řešit.

Bezpečnost – ožehavá otázka. Již při instalaci jsem měl možnost využít dostupných aktualizací a radím vám, udělejte to



Obr. 10: Ještě kontrola a je hotovo, Squid je nakonfigurován a běží



Obr. 12: „Java Desktop System“ od SUNu, založený na prostředí GNOME

také. Na ukázkovém serveru běží několik komponent, jejichž opravy se vyplatí sledovat. V první řadě je to jádro, které obstarává překlad adres, a firewall. Jádro může být cílem útoku zvenčí. Moderní distribuce zpravidla nabízí kromě normálního jádra i jistým způsobem ošetřenou a k některým útokům méně náchylnou tzv. „secure“ verzi.

Odkazy:
Linux NAT Howto: www.netfilter.org/unreliable-guides/NAT-HOWTO/NAT-HOWTO.linuxdoc.html
Shorewall: www.shorewall.net
Squid: www.squid-cache.org
Mandrake Linux: www.mandrake.cz

Nebojte se ji použít. Další balíčky, jejichž aktualizaci musíte sledovat, jsou proxy server Suid a DHCP server (útok může přijít i zevnitř!). Za určitých okolností mohou být potenciálně zneužitelné i chyby v základních komponentách, jako je například knihovna Glibc. Ale to spíše výjimečně.

Každá rozumná linuxová distribuce má informační kanál o dostupných opravách, který se vyplatí sledovat. Opravy jsou vydávány během maximálně dnů, například nedávné opravy OpenSSh vyšly během několika hodin od zveřejnění!

Nároky na čas a odbornost obsluhy jsou srovnatelné se stejným řešením na platformě Windows. Kdo problematice rozumí, nastaví si vše po svém, ostatní sáhnou do manuálu nebo ponechají standardní nastavení. Ukázkové obrázky ale myslím hovoří jasným jazykem. Celou proceduru jsem absolvoval asi za hodinu, počítaje v to i montáž síťové karty.

Stejnou instalaci jsem prováděl před rokem a půl při zprovoznění vlastního bezdrátového připojení. Na bazarovém počítači Pentium 200 s 32MB RAM a 2GB diskem jsem použil instalaci v textovém režimu, dále jsem pomocí podobných nástrojů, jako jste viděli dnes, ale v textovém režimu, nakonfiguroval bezdrátovou kartu, překlad adres, firewall a proxy server. Od té doby o počítači nevím a provádím na něm vzdáleně, v případě nutnosti, pouze aktualizace softwaru.

Linuxové aktuality

Patrně nejzajímavější událostí, kterou jsem zaznamenal, bylo uvedení desktopového prostředí GNOME 2.4. GNOME desktop udělal obrovský krok kupředu jak v oblasti použitelnosti, tak v oblasti spolupráce s ostatními prostředími. Možná je to jeden z důvodů, proč na GNOME postavil SUN svůj nedávno představený „Java Desktop System“. V podání Sunu jde o upravené GNOME 2.2 v kombinaci s Evolution, Mozillou a kancelářským balíkem StarOffice 7, viz obr. 12. Produkt je doplňuje na straně serveru „Java Enterprise System“ a celé řešení směřuje především do podnikové sféry. Protože vypadá velmi zajímavě, předpokládám, že se tam uchytí. Více informací naleznete na stránkách SUNu: www.sun.com/software/javadesktopsystem.

V době, kdy budete číst tento článek, budou na světě pravděpodobně nové verze distribucí. Mandrake 9.2 by měl být dostupný koncem září a pravděpodobně jsem jej nestihl jen těsně – o dojmy se s vámi podělím příště. Také RedHat oznámil novou verzi, a to na začátek října, a SuSE, tedy vlastně čerstvě přejmenované SUSE, vydá novou verzi v přibližně stejnou dobu. Předpokládám, že tyto nové verze linuxových distribucí budou k vidění již na Invexu, za sebe mohu prohlásit, že Mandrake určitě.

Když jsme u toho Invexu, letos proběhne v rámci Invexu pátý ročník odborné konference LinuxHall, tentokrát s podtitulem „Open source ve státní správě a samosprávě“. LinuxHall bude probíhat 7. a 8. října, v prostorách sálu Morava, pavilon A3. Oba dva dny jsou plné přednášek se zajímavými tématy, poslechnout si můžete například o detailech nasazení Linuxu u Bati nebo jak provozují informační systémy na Linuxu na městském úřadě v Domažlicích nebo Ostravě.

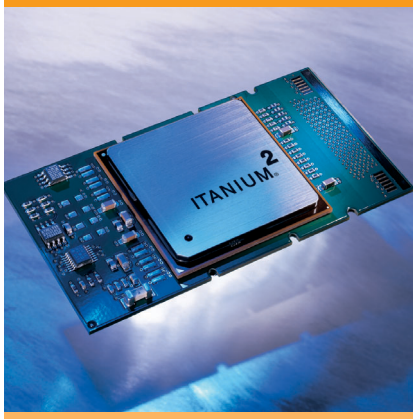
Závěrem aktualit zmíním, že hlasování o softwarových patentech v Evropské unii, o kterém jsem informoval minule, bylo odloženo. Doufejme, že zákonodárci budou mít dost času na nastudování problému a důsledků, které by zavedení softwarových patentů přineslo. Příští díl seriálu bude opět o serverových aplikacích pro Linux.

Chtěl bych se také blíže podívat na již několikrát zmíněného Webmina – aplikaci určenou pro vzdálenou správu Linuxu pomocí webového rozhraní. Máte-li k navrženým tématům připomínky nebo podnětné návrhy, neváhejte mě kontaktovat na uvedené adrese.

e-mail: ivan.bibr@autori.ccb.cz
www.otoffice.cz

Autor článku, Mgr. Ivan Bíbr, pracuje pro místní zastoupení distribuce Mandrake Linux.

Nové procesory Intel Itanium 2



Společnost Intel uvedla 9. září dva procesory Intel Itanium 2, optimalizované pro dvouprocesorové systémy. Tyto novinky rozšiřují možnosti nasazení procesorů řady Itanium do cenově dostupnějších systémů s nižší spotřebou, určených pro technické výpočty a podnikové aplikace.
Procesor Intel Itanium 2 s taktem 1,40 GHz a 1,5 MB vyrovnávací paměti 3. úrovně (L3 cache) poskytuje výborný poměr cena/výkon pro technické výpočty. Nízkonapěťový procesor (Low Voltage) Intel Itanium 2 s taktem 1,0 GHz s a 1,5 MB vyrovnávací paměti 3. úrovně (L3 cache) pracuje oproti stávajícím procesorům Itanium 2 se zhruba poloviční příkonem.
Pro produktovou řadu procesorů Intel Itanium jsou optimalizovány stovky aplikací a nástrojů, operační systémy s podporou procesorů Intel Itanium zahrnují Microsoft Windows Server 2003; Linux* od Red Hat, SuSE, TurboLinux, a UnitedLinux a HP-UX od HP.

Procesor Intel Itanium 2 s taktem 1,40 GHz a 1,5 MB vyrovnávací paměti a nízkonapěťový procesor Intel Itanium 2 s taktem 1,0 GHz a 1,5 MB vyrovnávací paměti jsou celosvětově dostupné za cenu 1 172, resp. 744 USD při odběru 1 000 kusů.