

# DOST BYLO TUČŇÁKŮ, PŘICHÁZEJÍ ČERTI!

## Recenze operačního systému PC-BSD

**Máte raději teplo než zimu? Už vás nebaví okna a tučňáci? Máte raději klikání myši, než psaní příkazů? Máte rádi individualitu? Chcete, aby váš počítač byl výjimečný a vy s ním? Pokud jste na většinu těchto otázek odpověděli ano, tak je tento článek určen právě pro vás.**



Startovací obrazovka vypadá k světu.

**E**xistuje mnoho operačních systémů pro různé hardwarové platformy, ale neobjevíte jednotný názor na to, který z nich je lepší a proč. Každý z nás používá na svém počítači operační systém a vybral si jej na základě nějakých osobních sympatií k němu. Motivy, proč jste si vybrali právě „ten váš“ se mohou velice rozcházet s důvody jiných lidí. Existuje ale určitá skupinka uživatelů, kteří se chtějí lišit od většiny a zásadně nepoužívají masově rozšířené operační systémy. A pokud se do této skupiny lidí řadíte i vy mohl by vás zaujmout operační systém s názvem PC-BSD.

### Trocha historie

PC-BSD je operačním systémem, jehož snahou je vytvoření uživatelsky přívětivé desktopové distribuce založené na jádře FreeBSD, jež je obecně pokládáno ze velmi robustní a spolehlivou platformu. Zřejmě proto si tento systém našel mnoho příznivců mezi provozovateli velkých a známých serverů, jako je

například Yahoo!. V dnešním světě má však jednu velkou nevýhodu – klade vysoké nároky na znalosti uživatelů. A přesně na tenhle „nedostatek“ se zaměřuje projekt PC-BSD, jehož cílem je vytvoření distribuce, která by měla snadnost ovládnutí Microsoft Windows a byla postavena na základech BSD.

Trojice známých písmen BSD znamená „Berkeley Software Distribution“ a je odvozena od Unixu distribuovaného Kalifornskou univerzitou v Berkeley. Operační systém FreeBSD vznikl z původního UNIXu vyvíjeného v laboratořích společnosti AT&T, který byl v letech 1993 až 1995 kompletně přepsán, aby se předešlo soudním sporům o autorská práva. Jedná se tedy o jednu z větví UNIXu na rozdíl od GNU Linuxu, jehož jádro bylo napsáno jako úplně nový operační systém, který je kompatibilní s normou POSIX. Hlavním rozdílem mezi FreeBSD a Linuxem je v licenci a v tom, že FreeBSD je vyvíjeno jako kompletní operační systém jednou skupinou vývojářů. Oproti tomu jsou v Linuxu vyvíjeny podpůrné aplikace a kernel různými týmy.

### Začínáme instalovat

Dříve, než se pustíme do vlastní instalace, zkontrolujeme hardwarové nároky, které nejsou překvapivě vůbec velké. Vystačí se s kompatibilním procesorem řady 686, 128

MB operační paměti a 4 GB volného místa na pevném disku. Výhodou jsou čipsety od společnosti VIA a nVidia.

Celý systém je rozdělen na dvě CD. První obsahuje kompletní instalaci systému a na druhém nalezneme vše potřebné pro podporu jiných jazyků než anglického. Pokud tedy zatoužíte mít systém v češtině, budete potřebovat obě CD. Z domovských stránek projektu lze stáhnout obrazy obou disků.

Po naboování instalátoru nás mile překvapilo propracované grafické prostředí, které lze navíc přepnout do české lokalizace. Průvodce instalací je poměrně dobře zpracovaný a jednoduchý na ovládnutí, což činí celou akci snadnou i pro méně znalé uživatele. Během instalace jste tázáni, zda se jedná o novou kopii nebo upgrade, zda instalujete server nebo pracovní stanici, jak se má rozdělit disk, jak nastavit síť a můžete založit účty pro lokální uživatele.

### Pracujeme s PC-BSD

Po dokončení se provede restart a můžeme vesele začít pracovat s novým neotřelým systémem. Při nabíhání počítače se zobrazí efektní černá obrazovka ve stylu Windows XP, která je posléze vystřídána obrazovkou startujícího KDE. To je jistě dobrá zpráva pro ty, kteří KDE prostředí preferují. Ten kdo má raději GNOME a nechce se s KDE sžívat, může zkusit instalovat GNOME z FreeBSD portů, které jsou v PC-BSD podporovány. Není to však nic pro začátečníky.

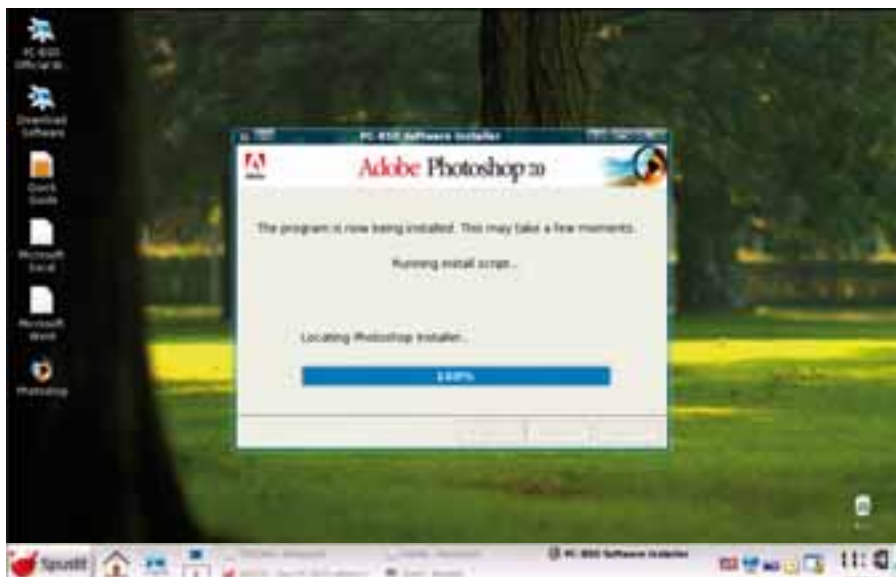
V základní instalaci PC-BSD není předinstalována spousta programů tak, jak jsme zvyklí z Linuxových distribucí. Najdete zde programy na správu systému, několik her a další běžný software jako je textový editor, prohlížeč PDF souborů a podobně. Pokud vám bude některá aplikace scházet, není nic jednoduššího, než si ji instalovat. A právě v tom tkví síla PC-BSD.

Pro distribuci aplikací a programů využívá PBI balíčků, které nápadně připomínají MSI balíky známé z platformy Microsoft Windows. Ze stránky [www.pbidir.com](http://www.pbidir.com) si stáhnete požadovanou aplikaci a dvojklikem na stažený soubor s příponou PBI spustíte její instalaci. PBI soubor v sobě obsahuje grafický instalátor, na který jsme zvyklí z aplikací pod Windows (instalace stylem „další, další a je instalováno“). Velkou výhodou tohoto způsobu distribuce aplikací je i to, že nemusíte řešit závislosti balíčků, pro-



**Marek Štaud**

Autor pracuje ve společnosti Outsourcing Solution jako správce serverů a softwarový auditor. Počítačová bezpečnost je jeho velkým koníčkem.



Žádné reklamní triky, Photoshop opravdu instalovat jde.

tože PBI balíček obsahuje všechny potřebné knihovny a podpůrné programy.

Na výběr máme slušný repertoár programů a aplikací, i když výběr je pochopitelně poněkud omezenější, než v ostatních distribucích s delší historií. Musíme však říct, že pro nás bylo velkým překvapením, když jsme mezi PBI balíčky objevili instalaci Microsoft Office 97 a Photoshop 7. Chvíli jsme byli na vázkách, zda-li nejde o vtip anebo nějakou chybu, ale po podrobnějším prozkoumání popisu zmiňovaných balíčků jsme zjistili, že jde o předpřipravené WINE, které je uzpůsobeno tak, aby umožňovalo bezproblémový běh těchto programů. Když spustíte instalační balíček pro Office 97, tak se instalují potřebné soubory WINE a vytvoří se spouštěcí ikony na ploše a v menu. Dále budete vyzváni k vložení originálního CD s Microsoft Office 97 a proběhne standardní instalace tohoto programu tak, jak jsme zvyklí z Windows. Po dokončení instalace můžete používat programy z Microsoft Office 97 přímo v prostředí PC-BSD tak, jako by šlo o program pro platformu BSD. Stejný postup platí i pro aplikaci Photoshop 7. Jen je třeba dodat, že musíte dodržet verzi programu, protože WINE je odladěno přesně pro tyto konkrétní aplikace.

### Lokalizace nejen pro Čechy

PC-BCD je lokalizováno do mnoha jazyků a jedním z nich je i čeština. To přirozeně potěší každého, kdo nerad řeší neustálé problémy s českými fonty, klávesnicí a dalšími drobnostmi, které stěžují možnost použití daného systému pro plnohodnotnou práci. Nelze však počítat s tím, že všechny instalované programy budou plně lokalizovány do češtiny. Nás osobně například potěšilo to, že se mezi PBI balíčky objevily i české OpenOffice.

Licenční ujednání PC-BSD je velmi jednoduché a obsahuje pouze dvě klauzule,

kteří umožňují každému použít a redistribuovat PC-BSD podle potřeby. PC-BSD má nicméně zakomponovány programy, které podléhají i jiným licenčním ujednáním jako například GPL, LGPL, ISC a podobně. I na tyto licence je tedy třeba brát ohled při nakládání s tímto softwarem.

### Kompatibilita s Linuxem

PC-BSD poskytuje binární kompatibilitu s některými dalšími Unixovými operačními systémy včetně Linuxu. Má to hned několik praktických důvodů. Tím hlavním z nich je, že vám tato kompatibilita zajistí možnost provozování komerčních aplikací, které jsou dodávány jen v binární podobě pro Linux, takže není možnost je recompileovat pro BSD systémy. Je nutné dodat, že kompatibilita není stoprocentní, a tak se může stát, že se některá aplikace nebude chovat zcela korektně.

### Doporučujeme

Každému, kdo touží po změně operačního systému a nepřestává ve svém hledání, můžeme PC-BSD jen doporučit. Je to určitě zajímavý systém a nabízí mnoho možností jak pro znalé uživatele, tak pro úplně začátečníky. To lze demonstrovat na možnostech instalace aplikací. Začátečník může použít PBI balíčky, které mu při tom zajistí plný komfort. Znalý uživatel se nespokojí s omezeným výběrem PBI balíčků a jednoduchými instalátory a bude chtít více, například v podobě FreeBSD portů, v kterých lze nalézt nepřehledné množství programů. Tento systém má určitě budoucnost a to si jistě uvědomila i společnost iXsystems, která nedávno oznámila akvizici s PC-BSD, přislíbila větší přísun peněz a tím urychlení a zlepšení budoucího vývoje. □

Domovská stránka projektu [www.pcbbsd.org](http://www.pcbbsd.org)

## Neriskujte ztrátu dat

Automatická záloha se síťovým souborovým serverem

**ZyXEL**  
NSA-2400



Ideální řešení pro ukládání velkých objemů firemních dat, automatizovanou zálohu a obnovení ztracených či poškozených souborů.

### V čem je ZyXEL lepší?

- > jednoduchá instalace
- > přehledná správa zařízení
- > sofistikovaný záložní software
- > podpora rozhraní 4x SATA a 3x USB 2.0.
- > tvorba virtuálního diskového pole (RAID 0)
- > automatické zrcadlení (RAID 1 mirroring)
- > nejpokročilejšího zálohování (RAID5)

\*19.990 Kč

\* doporučená  
koncová  
cena  
bez DPH



**ZyXEL**

[www.zyxel.cz](http://www.zyxel.cz)

# ZABEZPEČTE SÍŤ JEDNOU PROVĚZDY

## Test Sidewinder Network Gateway Security Appliance

**Co to vlastně je appliance? Pojďme se na tuto problematiku podívat podrobněji. Sidewinder Network Gateway Security Appliance je zařízení, které spojuje všechny hlavní funkce pro zabezpečení internetového provozu do jednoho boxu.**



**S**polečnost Secure Computing se specializuje na bezpečnost podnikových sítí více než 20 let. K hlavním produktům patří UTM Firewall Sidewinder Network Gateway Security Appliance, jenž patří mezi nejbezpečnější řešení na trhu díky souboru technologií „Zero-hour Attack Protections“. Chrání před známými i neznámými hrozbami díky integrovaným ochranám proti narušení (IPS), proti virům, spywaru, spamu, phishingu a jiným zákeřným kódům. Sidewinder též ochraňuje organizace před riziky spojenými s využíváním internetu a bezpečně rozšiřuje možnosti vzdáleného přístupu přes VPN služby a řízený přístup. Součástí je napojení na globální inteligenci „TrustedSource“.

### Seznamte se bez podání ruky

Po zapojení se spustí jednoduchý inicializační proces, ve kterém odsouhlasíme licenční ujednání a vyplníme několik dotazů (seriové číslo, IP adresu externí a interní síťové karty, či údaje o firmě). Závěrem nastavíme uživatelské jméno a heslo. Po té odsouhlasíme, zda chceme provedené změny uložit a následně se provede automatický restart a zařízení je připraveno ke konfiguraci.

Pro ty z vás, kteří potřebují vědět trochu více, je základem integrovaný operační systém SecureOS chráněný technologií „Type Enforcement“, což je mechanismus povinné kontroly přístupu. V zásadě jde o striktní uplatnění „mandatory access control“, tedy aplikace

běžící v systému mají striktně definovaný přístup ke konkrétním zdrojům v systému bez ohledu na běžná unixová oprávnění, a zda-li je vlastníkem superuživatel (root) či nikoli. Ty chrání řízení periferních jednotek, jádro a operační systém jako takový a co je nejdůležitější, zabrání i splnění hackerských snů: nepovolenému přístupu ke zdrojům (root access). Tím nedovolí útočnickovi zneužít jednu službu k pokolení další, zabraňuje instalaci „zlo-myslného“ softwaru či spuštění útoku, jehož výsledkem je přeplnění vyrovnávací paměti nebo převzetí a vyřazení systému díky vniknutí do základního přístupu.

Nástavbou je kontrola přes aplikační proxy i stavová inspekce – filtrování obsahu od vrstvy 3 do vrstvy 7 OSI modelu.

### Vítej v síti a pracuj

Instalace jako taková je bezobslužná, necháme-li instalační CD v mechanice, provede se reinstalace. Tím narážíme na podporu „disaster recovery“. To znamená, že dojde-li k závažné poruše anebo jinému druhu poškození (krádež, požár, ...), máte při opětovné reinstalaci možnost, obnovit již nakonfigurované soubory ze zálohy a tím minimalizovat dobu výpadku. Samotná obnova je pak záležitostí doslova několika minut (asi 20 minut).

Další výhodou Sidewinderu je, že můžete mít k dispozici všechny služby, které výrobce poskytuje – jednotlivé modely se tak liší pouze výkonem, nikoli funkčně. Samotná aktivace služby se provádí pouze zadáním patřičné licence.

Pro konfiguraci nám poslouží administrátorská konzole, kterou lze instalovat prakticky na libovolný počítač zapojený do firemní LAN.

Jen ve stručnosti si dále vysvětlíme základní pojmy. Pracujeme se sítěmi, tudíž nás moc nezajímá fyzické zapojení, ale jak máme jednotlivé segmenty pojmenovány. Připojení do internetu je zde pojmenované jako „external“, lokální komunikace LAN je uvedena jako „internal“ připojení. Můžeme zde mít i připojení do DMZ VPN, LAN2 a podobně. To je důležité pro pochopení, jak budeme dále konfigurovat pravidla. Naskytá se otázka: „Proč je to takhle nastaveno?“ Důvod je zcela prostý, při definování pravidel říkáme, jaký provoz z jedné sítě může jít na jinou síť. To si ukážeme dále při definici pravidel.

Dále zde konfiguruje DNS server, který může být transparentní (dotazy se předávají na jiný DNS server), anebo můžeme vytvořit tzv. „Sidewinder Hosted DNS server“. V tom to případě bude náš stroj fungovat i jako plnohodnotný DNS server. Jak již bývá u sítí zvykem, můžeme zde i definovat routovací pravidla, tj. vlastně to, kam má ta která síť přístup. Jako správný firewall má jedno důležité pravidlo: zakazuje veškerou komunikaci směrem do internetu.

### Pravidla se musejí dodržovat

Po definici sítí přejdeme k upřesnění pravidel, což je základ. Ukážeme si, jakým způsobem se pravidla nastavují a z čeho se skládají. Základním stavebním kamenem jsou zde „Rule Elements“ (základní prvky pravidel), jež tvoří služby (Services), síťové objekty (Network objects), autorizace (Authentications) a časový plán (Time periods).

Pod „síťovými objekty“ si představme skupinu IP adres (třeba IP adresy serverů) či běžnou stanicí. U autorizace máme na výběr všechny běžně používané metody. Časový plán zase definuje, kdy se mají jednotlivá pravidla aplikovat – nastavujeme hodiny i dny v týdnu.

Nyní, kdy již máme alespoň stručný přehled, z čeho se budou jednotlivá pravidla skládat, přistoupíme k jejich definicím. Jak jsme se již zmínili v úvodu článku, poslední pravidlo je tím nejdůležitějším – zakazuje veškerou komunikaci. Podívejme se, jak se takové pravidlo sestavuje a co všechno tu můžeme nastavit.

Při jeho vytváření definujeme název a popis pro snadnější orientaci

#### Lubomír Papp

Pracuje ve firmě Outsourcing Solution jako technický konzultant. Je specialistou na HP servery, zálohování, síťovou bezpečnost a Symantec Security.

v pravidlech. Pak určujeme, zda-li pravidlo danou akci povoluje, zakazuje, či dokonce zahazuje. Dále definujeme „service a time period“. Volíme, která síť je výchozí a která cílová, jestli budeme používat NAT, nebo budeme provádět redirekci (přesměrování). Nastavíme autorizaci a případně IPS. Velmi vhodné při zavádění pravidel je zapínat auditování. V případě, když se nám nedaří, jak bychom chtěli, lze přejít ze standardního na „upovídaný“ režim, kde se nám do logovacího souboru budou psát všechny záznamy. To na druhou stranu celý systém poměrně citelně zatíží, proto tento mód doporučujeme zapínat jen v případě řešení problému.

## Opatřete aplikace ochrany

Po nastavení základních pravidel se pustíme do konfigurace aplikačních ochrany. Jednou z nejrozšířenějších je ochrana HTTP. Zde již kontrolujeme, co přesně se nám děje na portu 80, a tak můžeme důkladněji monitorovat celou komunikaci. Samozřejmě lze definovat zakázané webové stránky a třeba i to, povolíme-li Javu, prvky typu „Active X“, skriptování a další.

Pro kvalitnější kontrolu nad přístupem na internetové stránky je možné provést integraci URL filtrace s technologií „SmartFilter“, jejíž engine je přímo integrován v http proxy Sidewinderu. Všechny požadavky na webové stránky tak nejprve projdou kontrolou dle webových zásad organizace s použitím denně aktualizovaného kontrolního seznamu (tj. lze např. zakázat kategorie chat, internetová rádia, pornografie, spyware, násilí, ...) a následně jsou tyto požadavky buďto povoleny, odepřeny, pozdrženy nebo řízeny.

## TrustedSource – globální inteligence vás ochraňuje

Technologie klasických, na signaturách založených, IPS nebo antispamových řešení využívajících „bayesovské filtry“ byly ještě

nedávno efektivní, ale útočníci a spammeři našli nové cesty, jak obcházet dokonce tyto robustní ochrany. „TrustedSource Reputation Service“ je zcela nový způsob boje proti hrozbám, kdy je upřednostňován systém globálních informací o důvěryhodnosti odesílatelů před lokálním řešením v tradičním duchu heuristických a jiných analýz, které přestávají mít požadovanou účinnost. „TrustedSource“ používá ohodnocení reputace systémů, které přistupují, komunikují či mailují se zdroji v naší síti a dokáže tak odchytil i neznámé útoky.

## Další funkce a schopnosti firewallu

Sidewinder dále nabízí ochranu VoIP provozu aplikačními proxy pro SIP a H.323, split server ochrany přímo na firewallu, jako je „Secure MAIL“. Stejně jako u HTTP, tak u SMTP komunikace lze pak provést i integraci s „TrustedSource“.

Posledním „pánem na holení“ je skupina „Maintenance“. Zde nastavujeme administrátorské účty a vytváříme certifikáty pro bezpečnou komunikaci. Důležitou položkou je konfigurace zálohy (Configuration backup), kam by měl zavítat každý správce tohoto systému a vytvořit si tu již výše popsany „disaster recovery backup“ a následně pravidelně běžné zálohy systému. Dále tu nastavujeme časové pásmo, licence, konfiguraci DNS serveru a mail serveru. Instalaci aktualizací, vypnutí systému a nastavení UPS.

## Zaznamenejte si události

Až na úplný konec jsme si schválně nechali otázku monitoringu. Nemáme-li totiž kontrolu, jak se systém chová a co dělá, stáváme se tak trochu bezzubými. A zde máme k dispozici jen základní kontrolu stavu systému sledující vytížení CPU, disků, paměti, kolik je otevřených spojení, jaký je stav sítí a aktuální „narušení“ podle protokolu nebo závažnosti. Z příkazo-

vého řádku přímo na stanici pak můžeme pomocí různých předdefinovaných filtrů vyčíst daleko více informací i o historii provozu. Výrobce ale slibuje integraci do GUI v nejbližší softwarové aktualizaci, což sledáváme jako krok kupředu.

Rozšiřujícím řešením, jež se doslova nabízí, je možnost obohatit Sidewinder o modul „SecurityReporter“ vycházející z „EIQ Network Security Analyzeru“, který nabízí bezpečnostním odborníkům nepostradatelnou službu sjednocení stovek hlášení a logů z mnoha systémů do jednoho, a to v reálném čase. To jim bezesporu usnadní identifikaci činnosti hackerů, virů či spamu a s tím spojeného narušení bezpečnosti.

## Kvalitní podpora

Vzhledem k možnostem, které toto zařízení skýtá, i rozumné cenové politice se Sidewinder stává ideálním řešením pro střední i větší společnosti. Zvláště jsme ocenili kvalitu technické podpory, která naše postřehy a dotazy obratem řeší.

Jak již bylo zmíněno, zařízení se dodává instalované jako „appliance“. Cena nejmenšího modelu se vším všudy se pohybuje okolo 50 000 Kč bez DPH a licenčně dokáže chránit neomezený počet uživatelů. Všechny typy disponují ochranami pro SMTP a DNS integrovanými vlastními „split servery“ a to v základní ceně. Všechny modely mohou být nasazeny ve „fail over clusteru“ pro dosažení vysoké dostupnosti služeb (SLA) a lze je též doplnit o přídatné moduly antivirus a antispyware, antispam a antiphishing, IPS modul, URL Filtering, TrustedSource a SSL šifrování. Jednotlivé konfigurace se tak liší pouze výkonem, nikoli funkčně, což je velmi férový přístup. Záruka obsažená v základní ceně zařízení je 3 roky, standardní servis je následující pracovní den. Lze si však připlatit za opravu do 4 hodin u zákazníka, případně prodloužit záruku na 5 let. □

## Modelová řada Sidewinder „D“ verze 7

Model	110D mini 1U	210D mini 1U	410D small 1U	510D small 1U	1100D enterprise 1U	2150D 2U
Ethernet rozhraní základ/max/ (opt)	4-10/100	4-10/100	4/6-10/100 (4)	4/6 Gigabit (4)	8/14 Gigabit (4)	8/20 Gigabit (6)
Počet uživatelů	Neomezen	Neomezen	Neomezen	Neomezen	Neomezen	Neomezen
Doporučený počet uživatelů	Menší firma do 75 uživatelů	Menší firma do 150 uživatelů	Střední firma do 300 uživatelů	Střední firma do 600 uživatelů	Střední/velká společnost	Velká společnost
Maximum odchozích IP adres	100	200	400	700	Neomezeno	Neomezeno
Počet modulů aplikačních ochrany	1 (max. 3)	2 (max. 3)	1 (max. 3)	2 (max. 3)	2 (max. 4)	2 (max. 4)
HW upgrady	2 možnosti	1 možnost	2 možnosti	1 možnost	1 možnost	1 možnost
RAID	-	-	-	-	RAID 1	RAID 5
Napájecí zdroj	jeden	jeden	jeden	jeden	jeden/volitelně i redundantní	redundantní
Propustnost pro paketovou filtraci (TCP)	150 Mb/s	180 Mb/s	275 Mb/s	650 Mb/s	1,6 Gb/s	2,6 Gb/s
Současná spojení	10 000 +	50	100	500	1 000 000	1 600 000
Propustnost při aplikační kontrole	100 Mb/s	140 Mb/s	230 Mb/s	250 Mb/s	1,2 Gb/s	1,8 Gb/s
IPSec AES propustnost • spojení	60 Mb/s • 75	80 Mb/s • 125	160 Mb/s • 200	160 Mb/s • 250	240 Mb/s • 350	350 Mb/s • 500