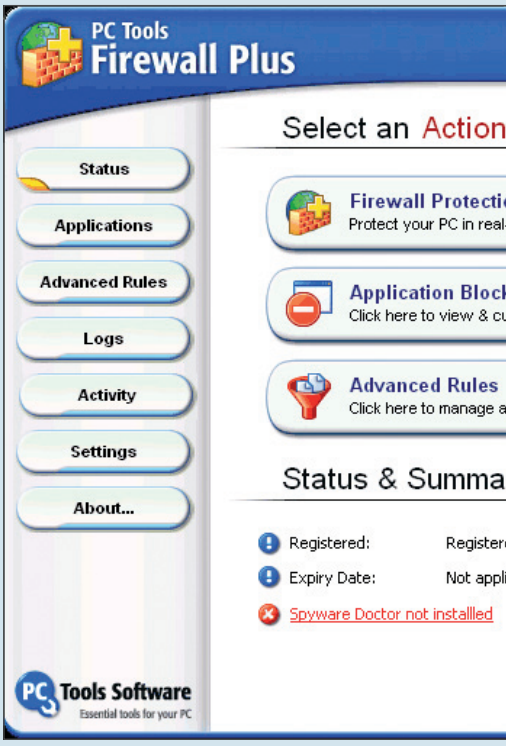
Bezplatné firewally

V jednom z předchozích Chipů jsme vám stručně představili nejoblíbenější bezplatné firewally. Nyní přišel čas **PODÍVAT SE JIM „NA ZUB“** důkladněji.

FABIAN VON KEUDELL



Firewall Plus: Přehledný firewall s celou řadou zajímavých funkcí bohužel nepatří k nejbezpečnějším v testu...

EXPRESNÍ TEST CHIPU

VŠECHNA FAKTA KRÁTCE A VÝSTIŽNĚ

Každým rokem se miliony uživatelů na celém světě stávají oběťmi počítačového zločinu – od už obyčejného zavirování počítače až po „hacknutí“ počítače a ukradení všech zpeněžitelných dat. Ve většině případů by škodám zabránil firewall, a proto mezi časté dotazy patří i kvalita firewallů. Který je ten nejlepší?

Abychom na tuto otázku dokázali alespoň zčásti odpovědět, vžili jsme se do role hackerů a s pomocí týmu Matousec (specializujícího se na bezpečnost) jsme firewally podrobili testům. Investice do bezpečnosti není nikdy zbytečná, v tomto případě však jde o výjimku potvrzující pravidlo: placené firewally toho často nenabízí o moc více než jejich bezplatní kolegové.

Bezpečnost: Jeden nástroj ochrání mnohé

V současnosti už firewall není jen obyčejným „strážcem dveří“. Musí kontrolovat nejen to, kdo (nebo co) chce dovnitř, ale i to, kdo (nebo co) se „dere“ ven – čili kontrolovat příchozí i odchozí spojení. Abychom zjistili bezpečnost firewallů, použili jsme sady tzv. „leak testů“, které zkouší, zda lze ochrannou bariéru překonat z vnitřku, když je již škůdce v počítači. Technika „leak testů“ je podobná té, kterou využívá malware (především trojské koně) ke kontaktu se serverem hackera. Výsledek je šokující: firewall ve Windows stejně jako Ashampoo identifikovaly pouhých šest procent útoků. Personal firewall „zvládl“ 18 procent útoků, a dokonce i poražený finalista odhalil jen nedostatečných 63 procent útoků. Pouze Comodo obstálo téměř bez „ztráty tváře“ s 95 procenty zvládnutých útoků.

Další testy měly prozradit, zda si firewally poradí alespoň se svou primární „náplní práce“. Nejprve jsme vyzkoušeli ochranu před útoky typu Denial-of-Service (DoS), které se snaží počítač ochromit tak, že ho bombardují dotazy „ping“, což obvykle také paralyzuje připojení k internetu. Potěšilo nás, že bez výjimky všechny firewally tento útok odrazily. Dalším předmětem testů byla ochrana proti skenování portů, a i v tomto případě všechny firewally obstály.

Funkčnost: Vše zcela automaticky

Aby firewall dobře chránil, musí být bezpečnostní pravidla dobře nastavena. Pokud jsou pravidla příliš „přísná“, na internet se nedostanou žádné programy (ani ty, které by se na něj dostat měly). Pokud jsou naopak pravidla příliš „volná“, může být počítač přístupný i pro útočníky.

Problém má jméno konfigurace – většina uživatelů totiž rychle uteče od nástroje vyžadujícího zadávání blokovaných portů nebo rozsahu IP adres. V ideálním případě by tato pravidla měl vytvořit sám firewall, s možností jejich případné úpravy uživate-

SHRNUTÍ TESTU

Náš vítěz testu Comodo nabízí téměř dokonalou ochranu a i jeho systémové nároky jsou přijatelné. Všechny zbývající firewally propadly v námi nejvíce testované oblasti – bezpečnosti. Ani výborné ovládání, které nabízí například Firewall Plus od PC Tools, nenahradí nedostatky v jiných, pro nás důležitějších oblastech...

VÍTĚZ TESTU 11/2008

PŘEHLED	1. MÍSTO
Produkt	**Comodo Firewall Pro**
Verze	3.0.25
Výrobce	Comodo
Web	www.comodo.com
Cena	freeware
Celkové hodnocení	86 bodů
Bezpečnost (50 %)	98
Funkce (25 %)	85
Ergonomie (25 %)	61
Bezpečnost	
Bezpečnostní testy (např. Leaktest, Portscans): Úroveň ochrany (0-10)	95% úspěšnost, úroveň ochrany: 10
Ochrana před DoS-útoky	●
Blokování skenu portů	●
Funkce	
Implicitní bezpečnostní úrovně	2 úrovně
Ukládání logu	●, včetně archivace
Automatická pravidla	●
Automatické updaty	●
Zjištění útočníka	–
Uvolnění jednotlivého portu	●
Uvolnění jednotlivého programu	●
Zjištění LAN	●
Ergonomie	
Varovná hlášení	mnoho informací, většinou však pouze pro odborníky
Nápověda	detailní nápověda, vždy ke zvolenému tématu
Průvodce	–
Zabraná paměť (MB)	5,4
Místo na disku (MB)	57,6
Rozhraní	nepřehledné, bez textové nápovědy
Jazyk	anglický

► **NA DVD:** Všechny testované nástroje najdete na našem DVD pod indexem **FIREWALLY**.

Zbytečná: Hlášení firewallu Windows jsou téměř zbytečná - nezjistíte z nich téměř nic...

lem. V této oblasti boduje většina námi testovaných firewallů, protože až na nástroj od firmy Ashampoo dokážou všechny automaticky vytvořit základní pravidla. Všichni kandidáti navíc vytváří záznam, ze kterého může uživatel později zjistit, které programy komunikují s „internetem“, jakým způsobem a kdy. Některé firewally (v našem případě Comodo, ZoneAlarm a PC Tools) jsou vybaveny funkcí, která umožňuje tyto záznamy archivovat. Více než kdekoliv jinde platí u firewallů pravidlo, že aby byl program opravdu bezpečný, musí být aktuální, a proto jsou všechny námi testované nástroje vybaveny i funkcí automatické aktualizace.

Ergonomie: Jeden program jako záchrana počítače

Pokud automatická pravidla nestačí, musí program varovat uživatele. Ten musí rozhodnout, zda aplikaci přístup k internetu povolit, či nikoliv. Pro toto rozhodnutí potřebujte znát důležité informace typu „který program se o připojení pokouší a přes který port“. V tomto případě nabízí nejlepší informace ZoneAlarm, který zobrazuje vše důležité v jediném okně. Navíc může uživatel obdržet další informace (týkající se varovného hlášení) přímo z webu ZoneAlarmu. Hlášení firewallu Windows je zdaleka nejhorší – nabízí totiž jen základní informace. Firewall by měl sice především chránit, neméně důležitou podmínkou je ale také co nejmenší spotřeba „systémových prostředků“. Proto jsme se podívali i na paměťové nároky všech kandidátů. A výsledek? Žádný z firewallů nezabral v paměti více než 50 MB, a vítěz testu se spokojil dokonce s pouhými 5 MB...

Comodo nás skutečně překvapilo – opravdu funguje: tento bezplatný firewall nabízí výbornou ochranu s malými nároky na systémové zdroje. Snad se brzy dočkáme i jeho oficiální české verze. Pokud ho chcete vyzkoušet a vaše znalost angličtiny není nejlepší, doporučujeme vám přečíst si nejprve praktický návod na serveru Viry.cz **(http://viry.cz/forum/viewtopic.php?t=53347)**.

AUTOR@CHIP.CZ

	2. MÍSTO	3. MÍSTO	4. MÍSTO	5. MÍSTO	6. MÍSTO
	ZoneAlarm	Personal Firewall	PC Tools Firewall Plus	Windows-Firewall	Ashampoo FireWall
	7.1.248	4.6	4.0.0.40	-	1.2
	Check Point	Sunbelt Software	PC Tools	Microsoft	Ashampoo
	www.zonealarm.com	www.sunbeltsoftware.com	www.pctools.com	www.microsoft.com	www.ashampoo.com
	freeware	freeware	freeware	freeware	freeware
	78 bodů	55 bodů	53 bodů	52 bodů	45 bodů
	75	60	37	36	36
	90	48	68	83	38
	72	50	68	51	70
	63% úspěšnost, úroveň ochrany: 7	18% úspěšnost, úroveň ochrany: 3	6% úspěšnost, úroveň ochrany: 1	**5% úspěšnost, úroveň ochrany: 1**	**5% úspěšnost. úroveň ochrany: 1**
	●	●	●	●	●
	●	●	●	●	●
	1 úroveň	1 úroveň	1 úroveň	1 úroveň	1 úroveň
	●, včetně archivace	●	●, včetně archivace	●	●
	●	●	●	●	–
	●	●	●	●, přes Windows-Update	●
	–	–	–	–	–
	–	–	●	●	–
	●	●	●	●	●
	●	–	–	●	–
	málo informací, odkaz na web výrobce	všechny důležité informace přehledně zobrazeny	všechny důležité informace přehledně zobrazeny	málo informací a žádná dodatečná pomoc	všechny důležité informace přehledně zobrazeny
	detailní nápověda a průvodce na webu výrobce	stručné informace, často poněkud zmatené	jednoduchý průvodce po spuštění, žádná další nápověda	detailní nápověda na webu výrobce	stručná nápověda přímo v programu
	–	–	–	–	–
	15,4	**50**	18,5	35,5	21,3
	34,6	15,7	18,3	integrován ve Windows	13
	přehledné, s drobnou nápovědou	nepřehledné, textové informace pouze pro odborníky	přehledné rozhraní s praktickou nápovědou	jednoduché, bez dodatečných informací	přehledné, s drobnou nápovědou
	anglický	anglický	anglický	anglický	anglický

● Špičková třída (100–90) ● Vyšší třída (89–75)
● Střední třída (74–45) ● Nelze doporučit (44–0)
Všechna hodnocení v bodech (max. 100)

● ano – ne
údaj nejlepší údaj
údaj nejhorší údaj

INFO

Metody testování

Kolem firewallů a metod jejich testování probíhají v internetových diskusích stejně líté boje jako na poli Windows versus Linux. Část uživatelů totiž považuje „leak testy“ za zbytečné – ve stručnosti lze říci, že jde o testy propustnosti – neboli o situaci, kdy už je počítač kompromitován (zavirován) a škůdce se pokouší o kontakt ven z počítače. Odpůrci testů argumentují tím, že se správným firewallem by nemělo ke kompromitaci vůbec dojít a prvořadou funkcí firewallu by měla být filtrace odchozí a příchozí komunikace. Podle našeho názoru je ale pravda někde „mezi“. Správný firewall by měl nabízet jednoduchou filtraci a zároveň odolat útokům z internetu na chráněný počítač – což lze otestovat na celé řadě serverů. Lze doporučit například tyto:

- **www.paranoia.cz/test;**
- **www.hackerwatch.org/probe/;**
- **www.pcflank.com/advanced.htm.**

Zavrhnout však nelze ani zmiňované „leak testy“, které prověřují bezpečnost systému v případě jeho napadení malwarem (ke kterému může dojít jiným způsobem než „přes firewall“). S těmito testy tedy mohou mít problémy i firewally renomovaných firem, které jsou primárně určené především k filtrování komunikace.