Domácí firewally

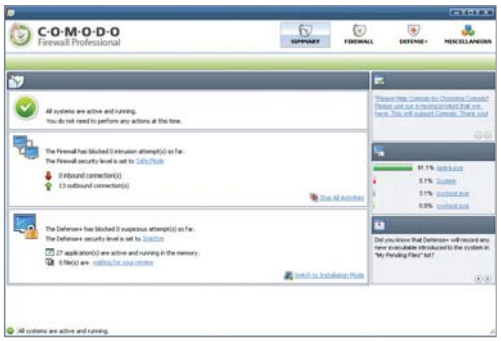
Ve světě plném virů, malwaru, hackerů a internetových červů patří **KVALITNÍ FIREWALL** k základním stavebním kamenům obrany vašeho počítače. Pojďme se podívat na kameny, za které neutratíte ani korunu…

PETR KRATOCHVÍL

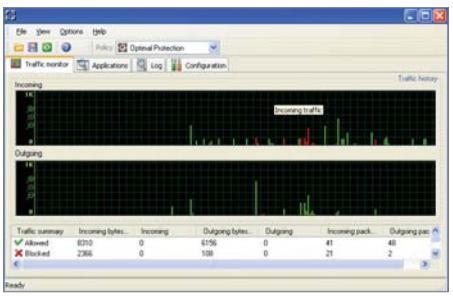
Seznamy aktivních červů a malwaru už dávno překonaly magickou hranici stovky položek a aktivity internetových mafií pasoucích po osobních údajích a číslech karet jsou stále častější. Ve světle těchto skutečností se stává osobní firewall nikoliv „výstřelkem" zvyšujícím bezpečnost, ale nutností pro každodenní bezproblémový chod počítače. A firewall ve Windows XP nebo Windows Vista? Je to lepší než nic, a pokud je váš počítač skryt za routerem s hardwarovým firewallem, je zbytečné hledat jinde. Pokud by ale měl být kterýkoliv ze zmiňovaných nástrojů jedinou bariérou mezi vámi a internetem, je lepší věnovat trochu času lepšímu zabezpečení.

Osobní volba

S železnou pravidelností vám v Chipu nabízíme přehled novinek v oblasti firewallů, a nejinak tomu bude i tentokrát. Pro většinu uživatelů bude výběr především osobní volbou založenou na konkrétních požadavcích, a to i proto, že mezi firewally poskytovanými zdarma nejsou příliš velké výkonnostní rozdíly. Základní útoky z „temné části" internetu blokují spolehlivě a obvykle nabídnou i kvalitní ochranu před náhodnými útoky červů. Rozdíly najdete především v oblasti funkcí, uživatelské přívětivosti a systémových nároků, a tak právě na tyto oblasti jsme se zaměřili. Pokud si nevyberete ani jeden z námi nabízených programů, máme pro vás pouze jedinou radu: Dříve než se pustíte do vybírání barevných skinů pro svůj zvolený firewall, zkontrolujte si jeho „spolehlivost". Stránek zabývajících se bezpečností programů najdete na internetu celou řadu, avšak server Secunia patří mezi absolutní špičku. Najdete na něm velké množství informací nejen o obyčejných programech a operačních systémech, ale i o zmiňovaných firewallech. Uživatelé hledající bezpečný firewall by měli zabrouzdat na adresu **http://secunia.com/product/**, kde mohou prověřit i jimi vybraný bezpečnostní nástroj. Nezapomeňte, že práce s „děravým" firewallem může být mnohem nebezpečnější než bez něj.



Comodo: Moderní program, určený i pro operační systém Vista, s poněkud drzým chováním.



Jetico: Efektní vzhled a překvapivě malé systémové nároky. Program určený spíše zkušenějším uživatelům.

Kvalitní a komplikovaný

Softwarové firmy vyvíjející firewall jsou v ošemetné situaci. Velká skupina uživatelů

NAJDETE NA CHIP DVD

Nejlepší firewally zdarma

Na DVD pod indexem Firewally najdete všechny testované programy. V závorce za názvem programu uvádíme podporované operační systémy.

Comodo firewall 3.0.25.3 ► (Win XP, Vista)

Jetico 1.0.1.61 ► (Win 2k, XP)

Outpost Firewall FREE ► (Win 9x/Me, NT, 2k, XP)

ZoneAlarm 7.0.470.0 Free ► (Win 2k, XP, Vista)

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **FIREWALLY**

JDE TO BEZ FIREWALLU?

Tvrzení o zbytečnosti desktopového firewallu je dnes už zcela překonané. Ano, samozřejmě, zkušení hackeři dokážou osobní firewall „prolomit“. Jak ale platí i v ostatních oblastech, zločinci vždy sáhnou po nejsnáze dostupných obětech – což znamená, že ten, kdo si firewall nenainstaluje a neprovede ani jiná bezpečnostní opatření, jim v podstatě pošle pozvánku… Pro počítač bez firewallu ale nejsou největší hrozbou hackeří – tou pravou hrozbou jsou červi. Většina z nich se ani nesnaží překonávat cizí firewally, protože je k internetu stále připojeno dost počítačů bez nich. Podle našich zkušeností je počítač bez firewallu připojený k rychlému internetu napaden červem již v rozmezí 20 až 30 minut. A pak stačí jedna chybějící záplata u operačního systému a neštěstí je dokonáno…

(začátečníků a méně zkušených) chce po firewallu jednoduchost a přehlednost, zároveň však přibývá i těch zkušenějších uživatelů, kteří požadují program s širokými možnostmi nastavení. Řešení tohoto dilematu je poněkud obtížné a každý výrobce má v tomto případě svou cestu. Někteří z nich skrývají pokročilá nastavení do hloubi nabídek, jiní nabízejí dva „pracovní režimy“ (jednoduchý, a pro odborníky).

Jak jsme hodnotili

Každý firewall jsme nainstalovali na mírně podprůměrně výkonný počítač (Celeron 2,5 GHz, 512 RAM) s Windows XP SP3 a podrobili jsme ho zátěžovému testu. Zkoušeli jsme, jak moc firewall brzdí internetový provoz, jaké systémové požadavky pro svůj provoz potřebuje a jak se chová při extrémní zátěži. Důležité pro nás také bylo to, jak se nastavuje a ladí, zda dokáže „poradit“ méně zkušeným uživatelům a nakolik je jeho ovládání komplikované. Poslední sledovanou oblastí byla nabídka funkcí – hodnotili jsme, jaké služby firewall nabízí a v jaké kvalitě. A jak obstáli jednotliví kandidáti?

Comodo firewall

HODNOCENÍ:

+ ROZSÁHLÁ KONFIGUROVATELNOST PROGRAMU
+ MODERNÍ FIREWALL
- PONĚKUD VLEZLÉ CHOVÁNÍ

Na rozdíl od ostatních programů působí Comodo firewall už od počátku moderním dojmem. Na vzhledu i ovládání je znát, že program je určen i pro operační systém Vista. Silně nemoderní je ale jeho vlezlost – nejen že již při instalaci nabízí celou řadu dalších programů a ochran, ale i v dalších krocích se snaží uživateli vnutit „internetovou lištu“, nastavit firemní stránku jako homepage nebo se vnutit na místo implicitního vyhledávače. Pokoj nemáte ani po prvním spuštění – program doslova zaplaví obrazovku okny s dotazy, což může méně odolné uživatele vyděsit. Pokud se ale přes tyto počáteční obtíže „přenesete“, dostanete moderní firewall s rozumnými systémovými nároky (okolo 10 MB RAM).

Jetico

HODNOCENÍ:

+ ROZSÁHLÁ KONFIGUROVATELNOST PROGRAMU
+ NÍZKÉ SYSTÉMOVÉ NÁROKY
- CHYBÍ OFICIÁLNÍ I NEOFICIÁLNÍ ČEŠTINA

I v tomto případě byla instalace blesková, pouze před restartem počítače bylo nutné zodpovědět dvě „zákeřné“ otázky (secure zone, blocked zone). Začátky práce s firewallem

INFO

Jak správně nastavit firewall

Jedním z největších problémů klasických desktopových firewallů je jejich správné nastavení. Uživatelé, již od počátku zmateni zdánlivě komplikovanými požadavky, automaticky povolují vše, aniž by znali důsledky svého počínání. Jak tedy správně nastavit firewall?

Kvalitní firewall by měl základní porty (pro surfování nebo ftp) uvolnit sám, další „operace“ jsou už ve vašich rukou. Základní pravidlo zní: Pokud něčemu nerozumíte, nepovolujte to. Pokus o připojení dočasně zakažte, pak si například pomocí Googlu zjistěte podrobnosti, a teprve poté se rozhodněte, zda aplikaci komunikaci povolit.

Ideální postup je následující – po spuštění aplikace (která vás žádá o povolení spojení) spusťte „Process Explorer“ (najdete ho na **http://technet.microsoft.com/cs-cz/sysinternals/bb896653(en-us).aspx**) a vyhledejte proces dané aplikace. Na něj klikněte pravým tlačítkem myši, zvolte položku »Properties« a poté kartu TCP/IP. V ní najdete informaci, na kterých portech se zvolený program pokouší komunikovat. Ověřte si, zda je to tak správně, a pokud ano, porty ve svém firewallu uvolněte.

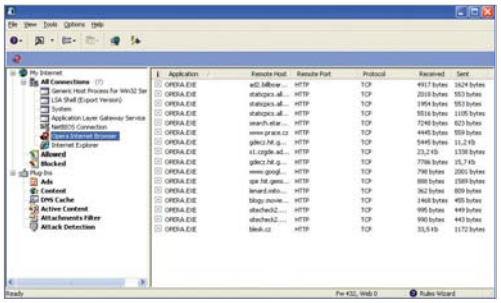
Na internetu najdete seznamy, v nichž je uvedeno, který protokol používá zvolený port. Je ale nutné si uvědomit, že jde o tzv. serverové porty, které udávají, jaké porty musí být otevřeny na straně webového serveru. Tak například webový server (HTTP) má číslo portu 80, FTP 21 a SSH port 22. Pro domácí firewall jsou tyto porty důležité pouze pro regulaci odchozích spojení.

POMALÉ STAHOVÁNÍ: ŘEŠENÍ KONFLIKTŮ PŘI SDÍLENÍ SOUBORŮ

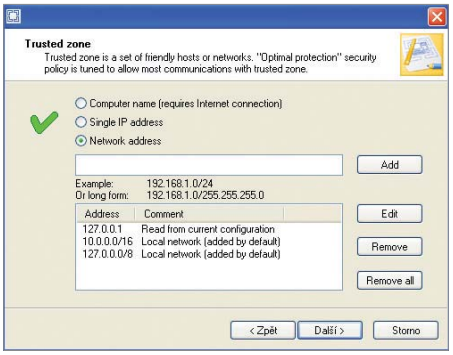
Poměrně problematické bývá soužití firewallů s P2P sítěmi. Máte na svém počítači BitTorrent nebo EMule a po aktivaci desktopového firewallu P2P aplikace nefungují? Stačí správně nastavit porty a můžete znovu „do akce“. Důležité je povolení následujících UDP portů:

DC++	411-413
BitTorrent	6881-6889, resp. 25819
Overnet/EDonkey	4661-4665
Gnutella (Bearshare, Limewire)	6345-6349

Pokud uvolnění odpovídajících portů úspěch nepřinese, mohlo by se jednat o záležitost vašeho směrovače – aktivujte pro něj proto „Port-Forwarding“.



Outopost: Jednoduché, přehledné a funkční. V programu překvapivě najdete také blokování reklam nebo DNS cache.



Konfigurace: Firewall Jetico předpokládá alespoň základní síťové znalosti. Bez nich budete zcela ztraceni...

lze bez nadsázky označit jako náročné – program se trpělivě ptá na každou aplikaci či proces snažící se komunikovat s okolím. Nic pro netrpělivé začátečníky. Také spíše efektnější vzhled programu naznačuje, že zde se více než na ergonomii hledělo na vzhled. Vzhledem k těmto výhradám nás překvapily systémové nároky – firewall počítač téměř nebrzdil a neřekl si o více než 8 MB paměti.

Outpost Firewall

HODNOCENÍ:

+ JEDNODUCHÉ A SROZUMITELNÉ OVLÁDÁNÍ
+ NÍZKÉ SYSTÉMOVÉ NÁROKY
- CHYBÍ OFICIÁLNÍ I NEOFICIÁLNÍ ČEŠTINA

V jednoduchosti je síla – to je s největší pravděpodobností heslo autorů programu Outpost Firewall. Jednoduchá instalace, snadné ovládání, přehledný design – zkrátka ideál každého uživatele. Na to, že je k dispozici zdarma, nabízí překvapivě i blokování reklam a nežádoucího obsahu a také DNS cache. Jeho hlavní výhodou jsou však systémové nároky – ani při největším provozu nezabral v paměti více než 10 MB (což je v dnešní době neuvěřitelné) a ani na našem pomalejším počítači nijak viditelně nebrzdil provoz (zatížení procesoru do 8 %). Pokud by se k tomuto programu našla „vhodná čeština", lze ho doporučit i naprostým začátečníkům.

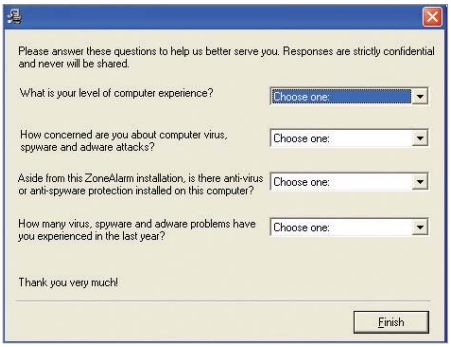
ZoneAlarm

HODNOCENÍ:

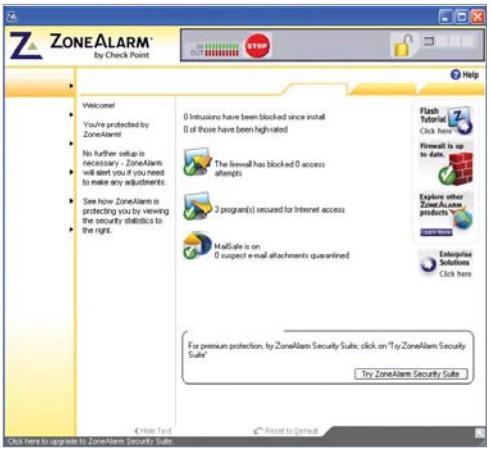
+ JEDNODUCHÁ INSTALACE
- PRO MÉNĚ ZKUŠENÉ UŽIVATELE KOMPLIKOVANÉ OVLÁDÁNÍ
- PROBLÉMY PŘI NASTAVOVÁNÍ FIREWALLU

ZoneAlarm patří do staré gardy programů, které najdete na počítačích už hodně dlouho. To je bohužel znát na celé řadě věcí. Při instalaci doporučujeme zrušit zatržítko u lišty Spyblocker, která by měla varovat před podvodnými weby a spywarem. Ve srovnání s moderními prostředky v browserech a antivirových programech by lišta jen zbytečně zabírala místo. Instalace je sice záležitostí jen několika kliknutí, o to více však zamrzí „dotazník" na jejím konci. Ačkoliv zjišťuje vaše znalosti (a situaci na PC), firewall tomu zdaleka nepřizpůsobí. Ačkoliv jsme na počátku zadali, že jsme „začátečníci", program po nás i nadále vyžadoval potvrzení i u obyčejného browseru. Navíc se nám některé programy komunikující s internetem nepodařilo ani zprovoznit. Podle našeho názoru lze ZoneAlarm doporučit spíše zkušenějším uživatelům, kteří jsou zvyklí na komplikovanější ovládání a kterým nevadí obtížnější konfigurace.

PETR.KRATOCHVÍL@CHIP.CZ



Zbytečné: Úvodní dotazník u programu ZoneAlarm se v chování firewallu nijak výrazně neprojeví...



ZoneAlarm: Na první pohled uživatelsky přívětivé ovládání, ve skutečnosti však spíše chaos a zmatek...

INFO

Když se firewall zeptá

Pokud se firewall zeptá na komunikaci běžného programu, lze bez problémů situaci vyřešit. Mnohem záhadnější bývají požadavky systémových procesů, kterým s přehledem vévodí Svchost. Chcete vědět, co za těmito zprávami skrývá?

Takovéto hlášení se často vztahuje k procesu „svchost.exe" (Service Host), pod který spadá několik služeb Windows. Ty jsou pak prováděny za pomoci různých DLL souborů. Zmíněné služby jsou nezbytné například pro automatický update, rozpoznání USB zařízení nebo také pro tisk. Kdykoli systém potřebuje některou z těchto služeb, Windows spouštějí proces Svchost, a zároveň toto spuštění aktivuje hlášení firewallu. Pokud chcete zjistit, zda se skutečně jedná o korektní spojení, podívejte se nejprve na cestu k souboru a na vzdálenou adresu, s níž se služba pokouší spojit. Soubor „svchost.exe" musí být umístěn ve složce C:\Windows\System32. Důležité je také zkontrolovat přesný zápis názvu. Mnoho trojských koní se totiž pokouší schovat za podobně vypadajícím názvem, jako třeba „svhost.exe", „svchosts.exe" nebo „sychost.exe".
Pokud chcete vědět, které podprocesy a s nimi svázané služby Windows váš program používá, opět spusťte již zmiňovaný freewarový „Process Explorer". Nástroj vám pak všechny běžící procesy vypíše. Vyberte proces „svchost.exe". V detailním okně pak najdete všechny soubory, adresáře a položky systémového registru, které jsou s ním propojeny. Po kliknutí na »Properties« se dozvíte další podrobnosti. Mezi nimi je také IP adresa a port, s nímž se program spojuje. Obvykle se „svchost.exe" spojuje jen s lokálními adresami jako „127.0.0.1" nebo „192.168...". U všech jiných adres je třeba mít se na pozoru.