DOBRÉHO NESPÁLÍ

Test firewallů pro sítě do 150 uživatelů

Spravujete počítačovou síť a potřebujete ji zabezpečit? Chcete rozdělit firemní síť na nezávislé segmenty – zaměstnanecké počítače, veřejně přístupné služby, interní databáze – a stanovit pro ně odlišný způsob přístupu? Toužíte mít vše pod kontrolou, aniž byste se museli učit konfigurovat složité aplikace? Žádný problém – jsou tu hardwarové firewally.

Firewall je aktivní síťové zařízení, které slouží zejména ke kontrolování a filtrování datového toku. Obvykle má alespoň jedno vstupní a jedno výstupní síťové rozhraní. Firewall kontroluje procházející data podle definovaných pravidel. Pravidla se aplikují buď na jednotlivé pakety (tzv. paketový filtr) na základě směru toku (vstupní/výstupní), nebo IP adresy a portu (zdroje/cíle). Pokud se zaznamenává stav pro rychlejší zpracování paketů patřících do jednoho toku dat, jedná se o stavový filtr. V případě zpracování aplikačních protokolů jde o tzv. aplikační brány.

Dobře známé jsou softwarové firewally (např. ipfw), což jsou aplikace, které běží na serverech s více síťovými kartami a které kromě filtrování provádějí i překlad adres NAT. Obvykle je na serveru s firewallem také služba DHCP pro dynamické přidělování IP adres, případně DNS pro překlad doménových jmen na IP adresy. Softwarové řešení je levné a oblíbené – můžete využít volně dostupný software a přizpůsobit si ho podle svých požadavků. Nastavení však vyžaduje zkušeného administrátora. A také analýza přenosů nebývá jednoduchá.

Co přináší hardwarový firewall

Hardwarové firewally jsou specializovaná síťová zařízení, která na první pohled připomínají menší přepínače. Umějí však mnohem více. Kromě přepínání a filtrace paketů provádějí např. analýzu dat na aplikační úrovni (obsah WWW stránek, e-mailů). Kombinují funkce stavového i paketového filtru a přidávají kontrolu obsahu dat pomocí vyhledávání řetězců. Oproti softwarovému řešení jsou rychlejší, jednodušeji se konfigurují a spravují. Poskytují komplexní ochranu a monitorování bezpečnosti sítě. Konfigurovat je můžete pomocí grafického rozhraní (přes WWW) nebo textového CLI (Command Line Interface).

Z technického pohledu je hardwarový firewall vlastně specializovaný počítač, který obsahuje procesor, paměť a síťová rozhraní. Součástí mohou být i hardwarové akcelerátory postavené na technologiích ASIC nebo FPGA pro rychlý výpočet šifrovacích algoritmů u VPN či vyhledávání řetězců u systémů IDS (Intrusion Detection System). Např. u firewallu ZyWall 35 umožňuje přídavná PCMCIA karta prohledávání obsahu dat a antivirovou kontrolu. Operačním systémem těchto zařízení může být třeba Linux pro vestavěná zařízení, SnapGear SG565.

Jak postupovat při výběru firewallu

V našem testu jsme se dívali na zařízení určená pro menší organizace (max. 150 počítačů). Pro testování jsme měli k dispozici tři zařízení – SnapGear SG 565 (od firmy Secure Computing), DFL-800 (D-Link) a ZyWall 35 (ZyXEL). Všechna zařízení obsahovala několik portů pro připojení lokálních sítí LAN, obvykle dva WAN porty pro připojení k internetu a porty DMZ pro demilitarizovanou zónu. SnapGear a ZyWall obsahují navíc Wi-Fi rozhraní a mohou pracovat jako přístupový bod bezdrátové sítě (AP).

Po přečtení technických specifikací těchto zařízení vyplývá, že všechna obsahují téměř stejnou množinu funkcí. Mezi ty základní patří:

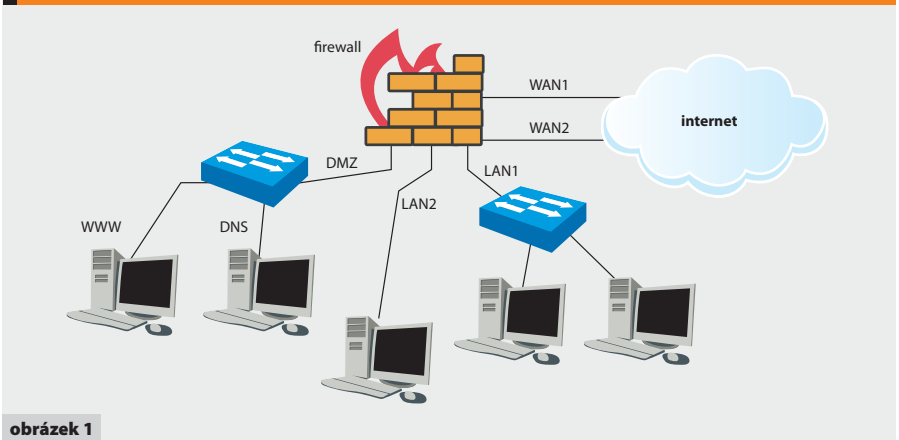
- síťové služby – dynamické přidělování adres DHCP, překlad adres a portů NAT/PAT, DNS proxy, řízení provozu (traffic shaping), rozložení zátěže (load balancing)
- management – správa přes webové/textové rozhraní, logování událostí, přehled navázaných spojení, vzdálená správa pomocí SNMP či syslog, zálohování konfigurace
- bezpečnostní funkce – stavové filtrování, podpora VPN, blokování aplikací, reakce na útoky, anti-spam, anti-virus, kontrola obsahu dat apod.

Některé funkce zkoumaných firewallů však málokterý administrátor využije. Pokud máte pouze jednu linku do internetu, bez dynamického směrování se určitě obejdete. Také podpora Wi-Fi je v podstatě zbytečná. Firewall bývá umístěn obvykle v místnosti serverů, kde Wi-Fi signál většinou nepotřebujete.

Kritický parametr – propustnost

Při testování jsme se zaměřili na propustnost. Ta je u firewallu zvláště důležitá, neboť přes něj tečou veškerá data z/do vaší sítě. Pro testování jsme použili obvyklé zapojení

Typické zapojení hardwarového firewallu



obrázek 1

AUTOR

Petr Matoušek

Autor je odborným asistentem na FIT VUT v Brně, kde se věnuje počítačovým sítím. Zabývá se verifikací časovaných systémů a validací protokolů.

zařízení – dvě interní LAN sítě s omezeným přístupem do internetu (WWW, ping, ssh), demilitarizovanou zónu (DMZ) s kontrolovaným přístupem z internetu a blokováním přístupu do vnitřní sítě LAN a internet (WAN síť) – viz obrázek č.1.

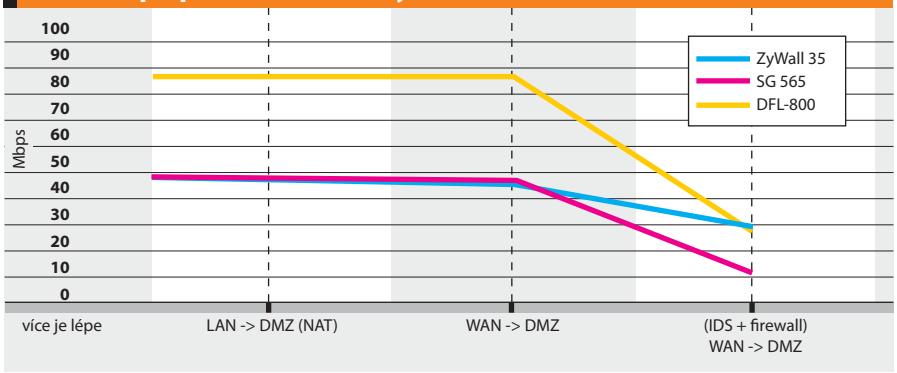
V testu jsme zjišťovali snadnost konfigurace tohoto zapojení a měřili rychlost přenosu souboru o velikosti 100 MB mezi jednotlivými stanicemi. Každé rozhraní firewallu bylo připojeno přes ethernet k dalším zařízením, vše na rychlosti 100 Mbps. Pro měření jsme použili program ttcp pod systémem FreeBSD. Naměřené hodnoty je potřeba brát jako relativní, neboť jsme nezohledňovali zpoždění na přepínačích v síti. Pro každý zkoumaný firewall bylo zapojení stejné. Výsledky měření jsou uvedeny v tabulce 1.

Podle očekávání klesla při zapnutí překladu adres (NAT) propustnost sítě o 40 až 50 %. Překvapením je výsledek u firewallu D-Link DFL-800, kde přenos s překladem adres neznamenal žádné zpomalení. Zdá se, že firma D-Link dobře využila své zkušenosti s vývojem přepínačů a směrovačů i v oblasti firewallů.

Jakmile jsme aktivovali filtrovací pravidla, zejména kontrolu obsahu dat (IDS), rychlost spadla až na 12 % normálního výkonu. Při použití šifrovaného kanálu VPN protokolem PPTP byl pokles rychlosti ještě dramatičtější. Zpomalení způsobuje především šifrování – u firewallu SnapGear dosahovalo vytížení procesoru 92 %, přestože rychlost přenosu se pohybovala kolem 1,5 Mbps. Při více souběžných spojeních klesá rychlost s počtem spojení. To se ukázalo u D-Linku, kde paralelní přenosy WAN->DMZ a LAN1->LAN2 způsobily pokles přenosové rychlosti na 13,6 Mbps, tj. téměř o polovinu. Při zapnutí IDS to bylo 11,2 Mbps.

Výsledné hodnoty nejsou příliš překvapující. Pokud chceme výkonnější zařízení, musíme sáhnout mnohem hlouběji do kapsy. Firewally pro gigabitové rychlosti se pohybují ve stovkách tisíc Kč. Obsahují hardwarové akcelerátory IDS a šifrování, rychlé přepínání paketů, větší paměť a specializované procesory. Nicméně pro malou podnikovou síť do maximálně 150 počítačů jsou testovaná zařízení dostačující.

Srovnání propustnosti testovaných firewallů



Porovnání propustnosti firewallů — **tabulka 1**

	LAN1->LAN2	LAN1->DMZ (NAT)	WAN->DMZ	WAN->DMZ (IDS+firewall)	WAN->DMZ (VPN PPTP)
ZyWall 35	88 MBPS	48,4 MBPS	45,6 MBPS	28,8 MBPS	–
SG 565	88 MBPS	47,2 MBPS	47,2 MBPS	10,4 MBPS	1,5 MBPS
DFL-800	88 MBPS	88 MBPS	88 MBPS	26,4 MBPS	19,2 MBPS

INZERCE ▼

ZyXEL ZyWall 35

Firewall od firmy ZyXEL vás zaujme na první pohled. Příjemný design, snadná a přehledná konfigurace. Obsahuje dvě rozhraní WAN a čtyři LAN, která lze nastavit také jako DMZ. Každé rozhraní DMZ může mít jinou adresu podsítě – firewall pracuje jako L3 přepínač. Druhé rozhraní WAN lze nastavit jako záložní. Při testování výpadku WAN1 ZyWall automaticky přesměroval provoz na WAN2 za cca 20 sekund. Také doba ukládání změn konfigurace byla rychlá – cca 5 sekund.

Při nastavování filtrovacích pravidel je velice užitečné přednastavené blokování spojení WAN->LAN, WAN1->WAN2, či DMZ->LAN. Při úpravě pravidel je potřeba dát si pozor na to, že implicitní pravidlo je permit. Pokud tedy nastavím povolení vstupu WAN->DMZ pro port 80, neznamená to, že ostatní služby jsou blokovány. Musíme je ještě implicitně zakázat. Pro IDP (Intrusion Detection Prevention) a antivirovou kontrolu je třeba zakoupit rozšířenou verzi ZyWall 35 UMT s PCMCIA kartou TurboCard, která provádí hardwarovou akceleraci a antivirovou kontrolu. Za tu si však připlatíme, stejně jako za antivirovou databázi a kontrolu spamů, které nejsou součástí základní verze.

Jako i ostatní testovaná zařízení obsahuje ZyWall DHCP server, překlady NAT/PAT, kontrolu šířky pásma, vytváření VPN sítí (pouze protokol IPSec), stavové filtrování či transparentní firewall (filtrace bez překladu adres, pouze jako přepínač). Implementace kontroly obsahu IDS je udělána velmi dobře – jako jediný firewall byl schopen správně filtrovat HTTP provoz při nastavení externího proxy serveru u WWW klientů.

Konfigurace přes textové rozhraní využívá místo příkazů textové menu a pro běžné použití je komplikovaná. Také záloha konfigurace ve formě binárního souboru není ideální. Ovládání zařízení přes webové rozhraní je velmi dobře vytvořené – je intuitivní a rychlé. Podrobné nastavení všech voleb je jasně a srozumitelně popsáno v přiloženém manuálu. Také sledování stavu zařízení, zobrazení logů a aktivních spojení je přehledné.

SnapGear SG 565

SG 565 je vlastně linuxový počítač s více rozhraními, který využívá standardní unixové služby pro implementaci firewallu – filtrování, překlad adres, služby DHCP, DNS, snort apod.

Jako jediný z testovaných firewallů není SnapGear uzpůsoben pro zapojení do racku. To se projeví zejména tehdy, když chceme sledovat aktivitu na ethernetovských rozhraních i LED diody na čelním panelu. Na rozdíl od ZyWallu obsahuje vyhledávání řetězců pomocí SNORT a podporu VPN nejen pro IPSec, ale i pro L2TP či PPTP (klienta i server). Obsahuje ClamAV verzi antivirové ochrany pro protokoly smtp, http, ftp, pop3, která je součástí zakoupeného řešení bez doplatku. Podporuje DHCP, NAT, DNS, nastavení šířky pásma a další služby. Pro sdílení souborů a tiskáren lze použít dva porty USB.

Výhodou je podpora virtuálních sítí VLAN (tagovaných i netagovaných, tzv. port-based VLAN), které rozšiřují možnosti kontroly přístupu do připojených podsítí. Při připojování VPN klientů umožňuje využít lokální databázi nebo služby RADIUS či TACACS+. Zprávy o provozu se zaznamenávají do unixového logovacího souboru, který není úplně čtivý a některé informace se tam velice špatně sledují – např. problémy s připojením VPN klienta. Také nastavení překladu adres NAT by mohlo být lépe řešeno – některé typy překladů (many-to-one) se nastavují komplikovaně. Zkušenější správce jistě ocení možnost připojit se přímo na linuxový server (přes ssh) a sledování nastavení klasickým způsobem.

Při testování propustnosti zaostává SnapGear výrazně za svými konkurenty. Důvodem je pravděpodobně linuxová architektura, která sice nabízí možnosti unixového systému a jeho rozšiřování, na druhou stranu degraduje hardwarový firewall na klasický softwarový. Zejména při filtrování provozu a kontrole obsahu dat došlo k výraznému poklesu rychlosti.

Srovnání testovaných firewallů — **tabulka 2**

	síťová rozhraní	rackové provedení	rychlost firewallu [Mbps]	rychlost VPN [Mbps]	konfigurace přes WWW	logování	záloha konfigurace	textová konfigurace	výrobce	cena v Kč bez DPH
ZyWall 35	2× WAN 4× LAN/DMZ	ano	70	30	přehledné, rychlé	přehledné	binární obraz paměti	textové menu přes ssh	ZyXEL www.zyxel.cz	14 401
SG 565	1× WAN, 4×LAN (VPN)	ne	120	7 (PPTP)	komplikovaná	unixový formát	binární i text. formát	ssh do Linuxu	Secure Computing (zapůjčila firma Skynet, www.skynet.cz)	19 996
DFL-800	2× WAN, 1× DMZ, 7× LAN	ano	120	60	pomalá aktivace změn, neintuitivní	přehledné	XML formát	CLI pouze přes sériové rozhraní	D-link www.dlink.cz	18 900

D-Link DFL-800

Posledním testovaným zařízením byl firewall od firmy D-Link. Konfigurace DFL-800 je celkem neintuitivní a přiložený manuál moc nepomůže. Pokus zprovoznit statický překlad adresy WWW serveru v DMZ zóně vyžadoval hlubší zkušenosti. Zapisování změněné konfigurace trvá 15 sekund, což je při úvodním nastavování firewallu nepříjemně mnoho, ale rekonfigurace se nedělá tak často, aby to bylo něco zásadního. Také některá základní nastavení jsou nejednotná – u rozhraní zapisujete podsíť ve formátu IP_adresa/24, u DHCP vypisujete 255.255.255.0. Nejen chyby nechtěně způsobené špatnou konfigurací lze snadno vysledovat v přehledných logových záznamech.

Zařízení obsahuje dvě rozhraní WAN, jedno DMZ a sedm portů LAN, na kterých lze nastavit VLAN podsítě. D-Link implementuje většinu služeb jako ostatní zařízení – DHCP, NAT, DNS, firewall, dále různé typy VPN (IPSec, PPTP, L2TP) či tunelování přes SSL. Pro prohledávání obsahu nemusíte kupovat žádné rozšíření – databáze je součástí běžné verze. Pouze za aktualizaci virové databáze si musíte připlatit.

Zajímavou funkcí je Zone Defence sloužící k odpojení zavirovaných nebo jinak podezřelých počítačů od sítě. Firewall spolupracuje s přepínači (zatím pouze od firmy D-Link), které zablokují port s infikovaným počítačem a zamezí mu komunikovat s dalšími stanicemi v lokální síti. Jde o velmi pokročilou a užitečnou funkci, která sleduje současný trend. Troufáme si tvrdit, že v blízké budoucnosti obdobné „karanténní“ funkce nebudou chybět na žádném firewallu či bezpečnostní bráně.

Nejzajímavější na firewallu D-Link jsou potom přenosové rychlosti. V našich testech byl suverénně nejrychlejší – překlad adres neměl žádný vliv na rychlost komunikace a také šifrovaný přenos VPN byl překvapivě rychlý. Bohužel způsob konfigurace a bezobsažný manuál patří k jeho velkým slabinám, které však zaskočí zejména méně zkušené administrátory.

Celkové srovnání zkoumaných parametrů testovaných zařízení je uvedeno v tabulce č. 2. Ve sloupci rychlosti firewallu a VPN jsou uvedeny hodnoty získané z materiálů výrobce.

Rychlost, obsluha nebo rozšiřitelnost?

V tomto článku jsme se podívali na několik firewallů, které jsou dostupné na našem trhu. Jsou to šikovná zařízení, která lze doporučit pro zabezpečení menších firemních sítí. Cenově se příliš neliší od spravovatelných přepínačů a mohou hodně usnadnit práci administrátorům sítě. Kdo chce velký výkon za přijatelnou cenu, sáhne po zařízení D-Link. Musí však být vybaven hlubšími znalostmi konfigurace v novém GUI rozhraní. Rozumný poměr výkon/cena/snadnost konfigurace nabízí ZyWall 35 od ZyXELu. Tento firewall nastavíte za chviličku a obsahuje téměř vše, co ostatní zařízení. SnapGear od CyberGuard je variantou softwarového firewallu s jednotným ovládáním. Obsahuje utility a možnosti rozšíření, které ostatní zařízení postrádají, jako jsou snort, antivir či data capturing. Platíte však za to sníženým výkonem a také cena je o něco málo vyšší.

Kdo sní o filtrování na rychlostech 100 Mbps či dokonce 1 Gbps, musí se poohlédnout po jiné kategorii výrobků. Ceny však rostou s rychlostí a počtem uživatelů a pohybují se ve stotisících.

Při použití firewallů je potřeba si uvědomit, že to nejsou zařízení všemocná a rozhodně je nelze brát jako náhradu za antivirové programy či anti-spyware. Pokud je firemní síť připojena k internetu více způsoby (pevná linka + záložní spojení ADSL), je nutné zabezpečit všechny přípojky. A jestliže máte nezabezpečenou Wi-Fi síť s dosahem mimo areál firmy, samotný firewall toho také moc nevyřeší. Je potřeba jasně stanovit, co a za jakých podmínek chcete chránit, a pak důsledně dodržovat bezpečnostní politiku. Hardwarové firewally vám v tom mohou významně pomoci. ❑

INZERCE ▶

JIŽ 15 LET VÁM
POMÁHÁME
CHRÁNIT DATA

AEC
DATA SECURITY COMPANY

Podrobnosti o historii AEC, spol. s r.o. a akcích k patnáctému výročí hledejte na www.aec.cz

Brno: AEC, spol. s r. o., Bayerova 799/30, 602 00 Brno
tel.: +420 541 235 466-7, e-mail: info@aec.cz
Praha: AEC, spol. s r. o., Vinohradská 184, 130 52 Praha
tel.: +420 267 311 402, e-mail: praha@aec.cz
Bratislava: AEC Bratislava, s.r.o., Kutlíkova 17
852 50 Bratislava, SK, tel.: +421 2 6828 6755
e-mail: bratislava@aec.sk, www.aec.sk