Připojení pobočkové sítě

AT-AR750S – univerzální směrovač určený pro malé a střední sítě

DAN VÁVRA

V stříc požadavkům menších a středních firem vychází společnost Allied Telesyn, jež se zabývá řešeními pro sítě IP a technologiemi pro Ethernet. Její novinka, směrovač s označením AT-AR750S, spojuje univerzální funkcionalitu s bezpečnostními mechanizmy, a je díky tomu vhodným síťovým prvkem pro spojení menších poboček či kanceláří s centrální sítí firemního sídla či jinou pobočkou. Na tomto produktu je zajímavá především cena, jež má při zohlednění technologické výbavy představovat výhodné řešení právě pro zajištění bezpečné konektivity se vzdálenými lokalitami, připojenými typicky jediným zařízením.

Mezi klíčové mechanizmy při zajištění bezpečnosti patří především podpora virtuálních privátních sítí (VPN) na bázi standardu IPSec. Díky hardwarové výbavě je směrovač schopen souběžně obsloužit až 250 aktivních připojení, avšak celkově je možné v konfigurační databázi předem definovat až 5 000 tunelů pro pozdější aktivaci. Dalším významným prvkem je plná podpora pro zajištění upřednostnění důležitého síťového provozu prostřednictvím technologií QoS. Právě tato výbava dává směrovači schopnost plně se začlenit do moderní infrastruktury, jež využívá pokročilé metody kombinovaného přenosu dat, hlasové komunikace a multimediálních přenosů. Směrovač navíc podporuje protokol IP verze 6.

Protože je směrovač AT-AR750S koncipován jako univerzální zařízení pro připojení celých poboček, nabízí kompletní nezbytnou funkcionalitu i pro ochranu jednotlivých segmentů. Vedle zmíněných možností je samozřejmostí služba překladu adres (NAT), a to včetně průchodu tunelů IPSec (NAT-T), dále stavový firewall pro ochranu síťové komunikace, systém detekce pokusů o průnik z externích síťových rozhraní a pokročilé záznamy událostí. Díky implementaci protokolu 802.1x je zajištěna dostatečně přizpůsobivá a široce použitelná technologie ověření uživatelů při různých způsobech přístupu, nechybí ani podpora souvisejících služeb podle standardů RADIUS a TACACS.

Allied Telesyn AT-AR750S

- ☺ minimální konfigurace
- ☹ pevný disk

Cena: 1 500 USD
K testu zapůjčila firma: VUMS Datacom, *www.datacom.cz*

Zařízení je koncipováno pro začlenění do síťové infrastruktury především na bázi ethernetové technologie. Proto nejen vnitřní (lokální) přepínané porty, ale též dvě rozhraní pro sítě WAN jsou osazena pro Ethernet o rychlostech 10 nebo 100 Mb/s. Celková šířka pásma až 300 Mb/s tak dostačuje pro pokrytí požadavků většiny společností.

Pořízením směrovače AT-AR750S získá uživatel především výkonné řešení, jež při zachování potřebné datové propustnosti sítí IP zajistí jak plnou bezpečnostní kontrolu, tak výkonné směrování náročných multimediálních přenosů. Zároveň se jedná o integrované zařízení, jež zajistí jak obsluhu klientů VPN, přistupujících do pracovní sítě přes zabezpečený přístupový server, tak propojení stabilním šifrovaným tunelem typu gateway-to-gateway mezi pobočkou a ústředím.

5 0410/BAM ❑

GPS pro mobilní telefon

Test GPS přijímače Nokia LD-1W ve spolupráci s komunikátorem Nokia 6670 a PDA

HYNEK VÁCHA

J e tomu již skoro rok, kdy jsme testovali přístroje GPS, které mohou být vítanými pomocníky při práci v terénu, jízdě automobilem nebo při turistice. Minule jsme měli k dispozici zařízení, jež nemají svoji vlastní zobrazovací jednotku a je tedy nutné jejich propojení s další jednotkou, která bude schopna přijaté informace zobrazit. Takovými univerzálními přístroji jsou notebooky a PDA. Tato kombinace přináší výhody hlavně vlastníkům PDA, kteří tak svého miláčka mohou velice snadno a hlavně levně rozšířit o navigační systém. GPS modul, který jsme měli k dispozici nyní, se od těch předchozích lišil hlavně způsobem připojení k zobrazovací jednotce. Zatímco v minulém testu se všechny moduly připojovaly napevno (kabelem nebo do komunikačního slotu), nyní vládnou bezdrátové přenosy. Toto řešení má nesporné výhody, kdy tou hlavní je, že se při používání navigace neustále nemotáme do kabelů ani nám nepřekáží GPS anténa trčící z PDA. Pojďme se ale podívat na vlastní testované zařízení.

Nokia, jejíž produktové portfolio přístrojů rozšířil, je známá spíše produkty pro mobilní telefonii – převážně vlastními mobilními telefony – a proto nás ani nepřekvapilo, že drobná krabička s nápisem Nokia zmátla každého, komu přišla na oči. Mnoho lidí se nechalo nápisem splést natolik, že se snažili do krabičky proniknout, aby našli displej a klávesnici. Teprve poté, co si poblíž všimli komunikátoru Nokia 6670, který jsme měli zapůjčený též, se nechali přesvědčit o tom, že jde skutečně o GPS. Zmiňovaný komunikátor doplňoval zapůjčené GPS jako náhrada za PDA. V porovnání s PDA se u komunikátorů obecně musíme spokojit s menším displejem a jinými drobnými omezeními, na druhou stranu však získáváme výhodu jednoho zařízení pro telefonování a spravování osobní agendy. My jsme GPSku vyzkoušeli jak s tímto komunikátorem, tak s PDA od DELLu a HP.

Vlastní GPS má velice jednoduché ovládání – jednodušší si lze představit pouze stěží. Vystačíme si totiž s jedním tlačítkem, kterým přístroj vypínáme a zapínáme. Pro kontrolu aktuální činnosti GPS jsou k dispozici tři LED diody. První indikuje, zda je přístroj zapnutý (zelené blikání), zda se nabíjí (zeleně svítí) nebo zda jsou již téměř vybité baterie (červené blikání). Druhá – modrá – svým blikáním upozorňuje na aktivní komunikaci GPS se zobrazovacím zařízením. Jak napovídá modrá barva diody, jedná se o komunikaci pomocí technologie Bluetooth, která je dnes dostupná ve většině mobilních zařízení. Poslední dioda upozorňuje bílým blikáním na komunikaci GPS se satelity. Nechybí zde samozřejmě ani napájecí konektor a pro případ potřeby je zde i konektor na externí anténu.

Většinu dalších funkcí pak zajišťuje zařízení, ke kterému GPS připojíme. Komunikace se zapůjčeným komunikátorem ani s PDA nečinila přístroji nejmenší obtíže. U PDA jsme GPSku pouze spárovali a poté stačilo její připojení a zapnutí programu s elektronickými mapami. Zde jsme navigaci vyzkoušeli pomocí PocketKiMu a SmartMaps. U obou zmiňovaných programů byla spolupráce naprosto bezproblémová a navigace probíhala více méně podle našich představ. Bližšímu popisu těchto programů bude věnován samostatný článek.

Na aplikaci Wayfinder se ovšem podíváme podrobněji již nyní. Ta totiž využívá odlišný způsob správy mapových podkladů, než je u většiny aplikací běžné. Standardně jsou všechny mapové podklady uloženy na paměťové kartě a odtud pak zobrazovány. Tento způsob má své výhody, ale i nevýhody. Výhodou je rychlý a jednoduchý přístup do takovéto interní paměti, nevýhodou je komplikovanější řešení updatů. Wayfinder funguje na jiném principu. V paměti komunikátoru nejsou uloženy všechny mapy, čímž se ušetří místo v paměti. Potřebné mapové podklady se do komunikátoru zasílají pouze na vyžádání – po zjištění aktuální polohy. Pro přenos map se používá mobilní síť, respektive technologie GPRS. S tímto je nutné počítat, protože při využívání s tarifem, který nemá GPRS přenosy placené paušálem, vznikají další náklady. Zajímavé je, že přístup k mapám je možný nejen pomocí vlastního Wayfinderu, ale i prostřednictvím webových stránek. Odtud je možné provádět většinu úkonů, jako je plánování tras nebo správa cílových bodů. Všechny změny, které na webu provedeme, se nám přenesou do komunikátoru a stejně tak i obráceně. Webová databáze umí spolupracovat i s kontakty uloženými v Outlooku, což dále usnadňuje práci s cílovými body a tím i vytváření tras. Tento přístup k mapovým datům má svá pro i proti. Na jedné straně jistě potěší menší kapacita zabraná programem a aktuálnost stahovaných mapových podkladů, naopak méně příjemná je již nutnost přenášení dat – to může zvýšit částku za používání systému, což je zvláště patrné v zahraničí při GPRS roamingu.

Nokia LD-1W

- ☺ snadná obsluha GPS
- ☺ Bluetooth pro připojení
- ☺ nízké nároky aplikace Wayfinder na paměť
- ☺ stále aktuální mapové podklady
- ☹ nutnost přenášení GPRS dat
- ☹ dlouhé odezvy Nokie 6670

Cena vč. DPH: 4 190 Kč
K testu zapůjčila firma: Nokia, *www.nokia.cz*

Celkově jsme byli s funkčností GPS značně spokojeni. Její obsluha je velmi jednoduchá a výhodou je Bluetooth technologie, která zajišťuje propojení s výkonnou jednotkou. Tím se rozšiřuje počet zařízení, s nimiž je možné GPS provozovat. Již méně nás nadchl komunikátor 6670, jehož odezva na požadované akce byla v některých případech neúměrně dlouhá.

5 0408/BAM ❑

Osobní strážce

ZyXEL ZyWALL P1 – kapesní ochrana pro notebooky i PC

MARTIN KYBAL

B ezpečnost je dnes stále častěji skloňovaným pojmem. Zejména při připojení k internetu je riziko napadení, zavirování či poškození dat velmi vysoké. Proto přišla firma ZyXEL s řešením, které využijí zejména majitelé notebooků, jež se často připojují do neprověřených sítí.

Toto řešení se jmenuje ZyWALL P1 a jedná se o personální hardwarový firewall. Personální proto, že je velmi skladný a kompaktní a je tak vhodný pro použití na cestách. Je koncipován jako plnohodnotný firewall s velkým množstvím funkcí a rozhodně se nejedná o okleštěnou verzi stolního řešení. Podívejme se blíže, co nám P1 přináší.

Zařízení o velikosti 12 × 8 × 2 cm je vybaveno čtyřmi konektory. Jeden je určen pro připojení do sítě WAN, což je označení pro vnější síť, do které se uživatel připojuje, další již představuje chráněnou vnitřní síť. Zbylé dva jsou určeny pro napájení, a to buď z externího adaptéru, nebo přes USB rozhraní. Pro opravdové cestovatele je P1 vybaveno elegantním pouzdrem, které jej chrání před možným poškozením.

ZyWALL P1 je uzpůsoben pro filtraci procházejícího provozu a zároveň může sloužit jako VPN klient pro vytvoření bezpečného tunelu například do firemní sítě. Oproti softwarovému řešení má P1 výhodu v tom, že šifrování dat nezatěžuje procesor počítače. VPN klient je typu IPSec se šifrováním DES/3DES a AES. Firewall pak zajišťuje standardní funkce ochrany před DOS a DDOS útoky, stejně jako blokování vybraných portů a adres podle nastavených pravidel. Pravidla určují, jaká aplikace a na jakých portech může s vnější sítí WAN komunikovat a naopak. Nastavení pravidel je možné buď v prostředí internetového prohlížeče, nebo pomocí SSH klienta. V prostředí prohlížeče je administrace velmi přehledná a srozumitelná. Pravidla se nastavují v jednotlivých formulářích, kde se vyplní připravené položky, a vše je hotovo. Musíme zmínit velmi dobře zpracovanou dokumentaci, která seznámí uživatele nejen s funkcemi a možnostmi zařízení, ale poskytne vysvětlení základních principů síťové bezpečnosti a vybraných pojmů. To spolu s provedením a poskytovanými funkcemi činí z P1 velmi užitečný nástroj pro zabezpečení mobilních uživatelů.

5 0407/BAM ❑

ZyXELL ZyWALL P1

- ☺ rozměry
- ☹ vyšší cena

Cena vč. DPH: 5 800 Kč
K testu zapůjčila firma: ZyXEL, *www.zyxel.cz*

Šikovný firewall

Juniper NetScreen 5-GT – přišel z lepší společnosti

JAROSLAV HRUBÝ

Na první pohled vypadá NetScreen 5-GT jako další z řady firewallů, určených pro SOHO, ale může nabídnout řadu nadstandardních funkcí. Primárně se jedná o stavový firewall s podporou řízení síťového provozu (traffic shapping) a kvality služeb (QoS), doplněný o podporu VPN (IPsec, L2TP), ochranu proti útokům typu DoS a volitelnou možnost AV ochrany a filtrování obsahu.

Balení obsahuje mimo firewallu napájecí zdroj, sériový kabel pro připojení konzole, dva přímé kabely RJ-45, instalační příručku a CD s manuálem. Samotný NetScreen 5-GT je modrá krabička o rozměrech 20 × 13 × 3 cm. Na přední straně nalezneme diody indikující stav zařízení i jednotlivých portů. Vzadu je kromě konektoru napájení ještě resetovací tlačítko, dvě sériová rozhraní RS-232 a pět rozhraní RJ-45. Jedno sériové rozhraní slouží pro připojení konzole a druhé pro modem. Čtyři rozhraní RJ-45 slouží k připojení lokální sítě (ať už přímo počítačů nebo rozbočovačů či přepínačů). Rozhraní „Untrusted" je určeno k připojení k xDSL modemu/kabelovému modemu či jinému širokopásmovému typu připojení. Existuje i provedení NS-5GT přímo s integrovaným ADSL modemem.

Hardwarovým srdcem NetSreenu 5-GT jsou integrované obvody ASIC, které spolu s 128 MB RAM dodávají firewallu dostatečný výkon. Udávaná propustnost činí 75 Mb/s, propustnost VPN spojení šifrovaného algoritmem 3DES je 20 Mb/s. Firewall by měl zvládnout (ač k tomu není určen) obsloužit i síť s více než padesáti koncovými stanicemi.

NetScreen 5-GT je možné konfigurovat jednak pomocí příkazové řádky CLI, dále přes webové grafické rozhraní, případně přes centrální management NSM. Webové rozhraní lze provozovat jak v nezabezpečené formě, tak přes šifrované HTTPS, přístup ke správě lze omezit na předem zvolené adresy. Po přihlášení do grafického menu spatříme souhrnný přehled nejdůležitějších informací, data o aktuálním vytížení procesoru, paměti, počet aktuálních sessions, logy a stav síťových rozhraní.

NetScreen 5-GT může pracovat ve dvou základních režimech, označovaných jako transparentní a routovací. V transparentním režimu se chová jako L2 bridge, tzn. na úrovni síťové vrstvy není vůbec „vidět". Všechny jeho filtrovací a bezpečnostní schopnosti jsou samozřejmě zachovány. V routovacím režimu se chová jako standardní L3 router. Jednotlivá rozhraní mají IP adresy, je možné používat NAT, PAT a mapování portů. Aby bylo možné mít za firewallem více sítí, podporuje NetScreen 5-GT jednak statické směrování a dále i dynamické směrovací protokoly RIPv2, OSPF i BGP.

Ve výchozí konfiguraci je zakázán veškerý provoz ve všech směrech. Pomocí průvodce (nebo ručně) je nutné generovat sadu pravidel. NetScreen 5-GT podporuje jednoduché řízení kvality služeb – QoS. U každého pravidla lze specifikovat minimální garantovanou rychlost, maximální přenosovou rychlost a stupeň priority daného provozu. U pravidel lze zapnout podrobné statistiky využití, včetně reakcí na překročení stanovených limitů. Poplachové zprávy lze doručit pomocí e-mailu nebo SMNP. V případě doručování zpráv pomocí e-mailu však nelze nastavit autentizaci vůči poštovnímu serveru a ani se nepředpokládá, že by SMTP server běžel na jiném portu než 25. Naproti tomu u nastavení syslog serveru možnost nastavit konkrétní port nechybí. Co se týče podpory SMNP, jsou podporovány pouze starší a z bezpečnostního hlediska nevhodné verze 1 a 2c. Poslední verze 3, která podporuje zprávy, jež mohou být současně šifrované i autentizované, bohužel není podporována.

Podporovány jsou VPN na bázi IPSec a L2TP a L2TP-over-IPSec. Lze vytvářet jak VPN typu klient/LAN, tak i LAN/LAN. Správu klíčů je možné realizovat ručně i automaticky pomocí protokolu IKE. Při použití IKE máme na výběr tzv. předsdílené klíče a variantu s certifikáty (X.509). Pakety přenášené ve VPN mohou být šifrovány algoritmy DES (klíč délky 56 bitů), 3-DES (klíč délky 168 bitů) nebo AES (klíč délky 128,192 nebo 256 bitů). Zabezpečení proti modifikaci nebo poškození dat se děje pomocí hashovacích funkcí MD-5 či SHA-1. Vzhledem k posledním poznatkům kryptologů o (ne)bezpečnosti MD-5 je rozhodně lepší používat pouze algoritmus SHA-1.

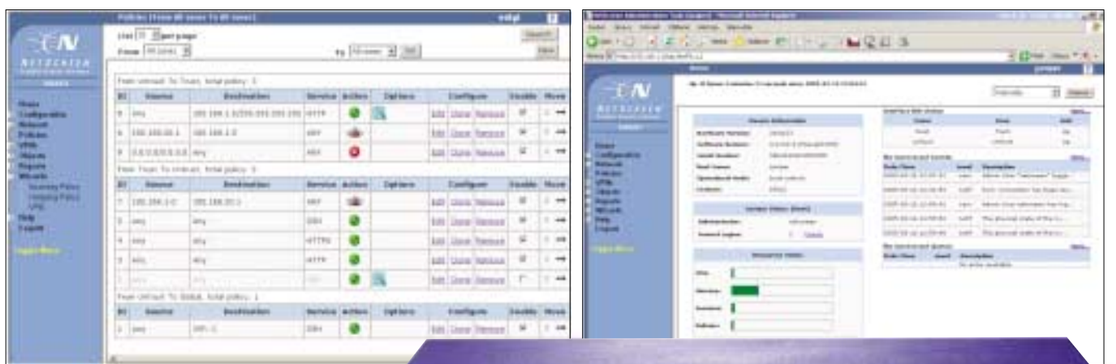
Instalace firewallu NetScreen 5-GT je jednoduchá a intuitivní. Za pomoci průvodců lze konfigurovat celé zařízení do provozuschopného stavu během několika minut. Ačkoliv by se našlo několik drobností, které výsledný dojem trochu kazí (např. v prohlížečích založených na jádře Gecko jsou některé grafické prvky vykresleny chybně), jedná se o věci, které by mohly být v příští verzi firmwaru odstraněny.

5 0409/BAM ❑

Juniper NetScreen 5-GT

- ☺ výkon
- ☺ pokročilé možnosti konfigurace
- ☹ chybné zobrazování GUI rozhraní v prohlížečích s jádrem Gecko
- ☹ nepodporuje SMTPv3

C testu zapůjčila firma:
VUMS DataCom
Cena vč. DPH: cca 14 000 Kč



▲ **Průvodce vytvářením pravidel.**

▶▶ **Okno, v němž lze podrobně nastavovat parametry pro Traffic shaping.**