Síť pro každý stůl

Síťová zařízení domů a do kanceláře
Přehled druhý

Patrik Malina

*****perex*****
V tomto článku bezprostředně navážeme na materiál, jejž jste nalezli v minulém čísle zhruba na tomto místě. Oproti prvnímu přehledu, v němž jsme si představili kolekci zařízení nabízející různé zajímavé možnosti „malého“ síťování, se v dnešním přehledu zaměříme na poměrně tradiční požadavek – zabezpečenou síťovou komunikaci.
*****perex*****

Ne že by jinak u malých routerů či ADSL integrovaných modemů hrála bezpečnost druhořadou roli – koneckonců, drtivá většina z nich již disponuje velmi slušně vybavenými ochrannými mechanismy, zahrnujícími paketové filtry, firewally na aplikační úrovni či jednoduché systémy pro boj s útoky s cílem znepřístupnit služby a prostředky (DoS). My jsme se však v tomto výběru zaměřili na další možnosti bezpečného síťování, a to sestavování šifrovaných síťových tunelů a tvorbu tzv. VPN, tedy virtuálních privátních sítí. Schopnosti různých zařízení jsou opět okomentovány v příslušných odstavcích.

Kam vede tunel?

Možnost sestavování virtuálních tunelovaných spojení je dnes již považována za poměrně běžnou záležitost a ochrana komunikace např. mezi různými firemními pobočkami či cestujícími uživateli a firemní sítí není ani v „domácích“ podmínkách žádným luxusem. V zásadě lze z koncepčního hlediska tato spojení rozdělit na dvě skupiny. První z nich můžeme též nazvat jako klasické tunelování a řadíme zde ta řešení, jejichž cílem je propojit dvě a více poboček – firemních či domácích sítí. Výsledkem takového postupu je vlastně sjednocená lokální síť, jež překlene dálkové linky právě v podobě chráněného virtuálního tunelu. Tento realizujeme pomocí plynule zasílaných šifrovaných paktů, a to především po internetu. V praxi pak situace vypadá tak, že na straně lokálního síťového segmentu, kde je nabízeno připojení pomocí Wi-Fi či ethernetových portů, probíhá normální provoz, a při snaze zaslat data na jinou pobočku provede brána šifrování a zapouzdření do tunelu, jenž je sestaven v prostředí ADSL či kabelové přípojky. Tyto spoje jsou též označovány jako brána-brána (gateway-gateway).
Druhou skupinou VPN jsou připojení vzdálených jednotlivých klientů a jejich bezpečně propuštění do lokálního síťového segmentu. Logika věci je zde v podstatě otočena: vzdálený uživatel s přenosným počítačem sestavuje po internetu tunel a „tluče na vrata“ naší brány zvenčí, tedy z ADSL či kabelové přípojky. Šifrovaný tunel je zde, na prahu lokální firemní či domácí sítě, ukončen a další komunikace pokračuje uvnitř sítě, pomocí Wi-Fi či některého ethernetového portu. Tato spojení bývají též označována jako vzdálený klientský přístup (remote access) či klient-brána. Oba popsané scénáře jsou dnes u hardwaru pro malé sítě běžně realizovatelné a řada zařízení podporuje paralelní provoz více tunelů obou druhů.

Jak vzniká VPN?

Aktuální vývoj v oblasti síťové bezpečnosti s sebou přinesl významnou skutečnost v podobě sjednocení používaných technologií, takže prakticky ve všech zařízeních jsme nalezli jednu ze tří nejpoužívanějších technologií pro sestavování VPN. Jednoznačně nejrozšířenější a de facto standardní implementací je ochrana pomocí šifrování síťových paketů s názvem IPSec. Přestože zde

představujeme hardware relativně levný, prakticky všude jsme nalezli slušné možnosti pro šifrování IPSecu: pro ochranu paketů před odposlechem jsou dostupné algoritmy DES či 3DES, v lepším případě též nejnovější AES, pro zajištění autenticity paketů („digitálního podpisu“) za účelem zabránění podvrhům či modifikacím na trase jsou nabízeny hashovací algoritmy MD5 či lepší SHA1. Na druhou stranu snaha o co nejsnazší implementaci v malých sítích se projevuje u jiné vlastnosti implementace IPSecu: prakticky všude se protistrany při sestavování tunelu navzájem ověřují pomocí tzv. preshared key (sdíleného klíče, tajemství), tedy vlastně hesla, jež administrátor zadá ručně. Pokročilejší řešení s digitálními certifikáty prakticky není u těchto zařízení k vidění. Krom čistých tunelů IPSec jsou k vidění další dvě technologie především pro připojování vzdálených uživatelů. Zatímco protokol PPTP je spíše určen pro starší klientské operační systémy, novější L2TP představuje, obzvláště ve spojení s IPSec šifrováním, novější generaci se světlou budoucností.

Kde hledat rozdíly?

Přestože mnohá zařízení disponují na první pohled stejnou výbavou, skutečnost je často komplikovanější, a proto je potřeba se před koupí a při testování zaměřit na některá důležitá hlediska. V první řadě si ověřte, zdali je možno provozovat vámi požadované typy VPN spojení, tedy buďto mezi pobočkami, nebo směrem ke vzdáleným uživatelům, případně oboje zároveň. Nenechte se zmást reklamními nápisy a otestujte, kolik paralelních tunelů lze skutečně provozovat, neboť často jsou zařízení různě omezena: obzvláště počet tunelů mezi pobočkami nebývá zbytečně vysoký. V neposlední řadě se zaměřte na hardwarovou výkonnost a skutečnou propustnost sestavených tunelů – šifrování IPSec je výpočetně velmi náročné a přestože konfigurační rozhraní dovoluje předem nastavit až desítky tunelů, reálně jich často může zároveň běžet méně než 10. Seriózní dodavatel či výrobce by vám tyto informace měl sdělit, neboť je bezpochyby zná, a mnohá zařízení mají přímo své zabudované limity.

D-Link Dl-804-HV
www.dlink.cz
Tento model v tuzemsku dobře známého výrobce představuje poměrně univerzální řešení pro hardwarové sdílení internetové linky spolu s širokou podporou pro virtuální privátní sítě. Pomocí ethernetového konektoru RJ-45 lze připojit jak kabelový, tak ADSL modem, neboť je podporováno připojení se statickou i dynamickou adresou a rovněž PPTP směrem k poskytovateli. Alternativou je sériové rozhraní (COM) pro dial-up variantu, škoda jen, že obě možnosti nelze použít zároveň. Obsluha LAN klientů je řešena DHCP serverem, jenž však nemůže rozdávat adresy mimo pevně daný adresní rozsah se síťovou maskou třídy C.
Po stránce VPN podpory je router vybaven velmi slušně. Dovoluje paralelně obsluhovat až 40 tunelů mezi vzdálenými branami, pro šifrování IP Sec je dostupný jako nejsilnější 3DES a klíče lze definovat jak ručně, tak vyměnit dynamicky. Míra bezpečnosti je jednoznačně dána faktem, že pro autentizaci IP Secu lze použít pouze sdílený (pre-shared) klíč. Router podporuje též funkci PPTP serveru. Z dalších vlastností je třeba zmínit dobře provedený firewall a podporu průchodu PPTP i L2TP VPN tunelů skrz filtry.

plusy: firewall, dial-up port
mínusy: pevné vymezení LAN IP adresace
Zapůjčila firma: D-Link, Česká republika
Cena vč. DPH: 3 060 Kč

Level One WBR-3402B

www.vanet.cz
Zařízení u nás nepříliš známé značky je výhradně určeno pro univerzální sdílení ADSL přípojky, neboť integruje jak ADSL modem, tak router, firewall a VPN bránu a Wi-Fi přípojný bod. Krom 4 ethernetových portů je tedy vybaven jedním konektorem RJ-11 pro připojení k ADSL splitteru, další možností je připojení síťové tiskárny pomocí jednoho portu USB a možnosti obsluhy lokální sítě posiluje Wi-Fi v obou tuzemských variantách 802.11b/g.
Výbava pro tvorbu VPN tunelů je standardního rozsahu. Podporován je IPSec, nejsilnějším algoritmem je zde 3DES, autentizace je prováděna metodou pre-shared key a předem je možno přichystat až 40 tunelových spojení, jejichž současný počet je možno omezit. Šifrovací klíče je možno vyměňovat dynamicky nebo nastavit napevno.
Bezdrátová výbava podporuje varianty b/g a možnosti zabezpečení jsou poměrně slušné: podporován je standard WPA i „domácí“ varianta WPA-PSK, dále klasický WEP a „holý“ 802.1x s WEPem. U WPA varianty, bohužel, není možno vybrat novější standard AES. Dobrou možností pro LAN připojení je možnost libovolně nastavit IP adresaci a přidělit serveru DHCP příslušný rozsah, avšak pouze v rozsahu třídy C. Dobré možnosti nabízí zabudovaný firewall.

plusy: integrovaný ADSL modem s mnoha možnostmi
mínusy: limitace DHCP Serveru, chybí PPTP server
Zapůjčila firma: Vanet, s.r.o.
Cena vč. DPH: 5 900 Kč

Level One WBR-3403TX
www.vanet.cz
Tento router je mírně odlišnou variantou jiného zařízení, jež v našem přehledu najdete pod stejnou značkou také. Vyznačuje se především univerzálním ethernetovým WAN rozhraním, takže lze pro přístup použít jak ADSL či kabelový modem, tak jakékoliv jiné rozhraní s IP konektivitou. Rovněž zde nalezneme rozhraní pro síťové sdílení tiskárny, ovšem tentokráte v podobě klasického paralelního portu, pro jehož obsluhu lze doinstalovat software z přiloženého CD.
I tento model nabízí Wi-Fi připojení lokálních klientů, implementace je však zatížena několika nepříjemnostmi. V rozhraní jsme nenalezli možnost přepínat režimy 802.11b a 802.11g, a přestože WEP je k dispozici i pro dílku klíče 256 bitů, zcela zde chybí standard WPA, což je velká škoda. Protokol 802.1x je podporován pro dynamický WEP.
Výbava pro VPN je stejně slušná jako u zmíněného sourozence, autentizace pro IPSec je prováděna sdíleným klíčem a šifrovat lze pomocí algoritmů DES a 3DES a máme možnost definovat předem až 40 tunelů. Velmi solidní je opět firewall s možností publikovat nejdůležitější služby a dobře řídit filtraci nežádoucího provozu.

plusy: univerzální WAN rozhraní, tiskový port
mínusy: oslabení možností bezpečného Wi-Fi
Zapůjčila firma: Vanet, s.r.o.
Cena vč. DPH: 4 800 Kč

ZyXEL Prestige 334
www.mikenopa.cz
Zařízení tradičního výrobce je poměrně univerzálním řešením pro sdílení širokopásmového internetu. Připojení typu WAN je možno realizovat pomocí RJ-45 ethernetového rozhraní pomocí statické či dynamické IP adresy a k dispozici jsou též varianty PPPoE či PPTP, takže lze router nasadit k ADSL či kabelovému modemu stejně jako třeba k Wi-Fi internetovému připojení.
Pro obsluhu lokálních klientů jsou k dispozici 4 ethernetové porty a DHCP server je možno konfigurovat pro naprosto libovolnou IP adresaci. Nechybí funkce přesměrování lokálních DNS

dotazů, snadno lze vytvořit DHCP rezervaci a velmi slušné možnosti konfigurace najdete u služby překladu adres (NAT).
Poněkud skromnější výbavu najdeme u virtuálních privátních sítí. Přestože je možno nastavit IPSec do režimu tunelování i transportu v lokální síti a šifrování je podporováno pomocí algoritmů DES a 3DES, router dovoluje takto definovat pouze 2 spojení, což je opravdu málo. Autentizace je tradičně řešena sdíleným klíčem. Alespoň že IPSec je možno propustit skrze firewall. Velmi dobré možnosti jsou naopak v oblasti vzdálené administrace a nastavení logování událostí.

plusy: NAT, vzdálená správa, logování
mínusy: málo VPN spojení
Zapůjčila firma: MiKENOPA, a.s.
Cena vč. DPH: 1 800 Kč

DrayTek Vigor2900G
www.attel.cz
Pod označením Vigor jsme již tradičně zvyklí nacházet zařízení s velmi širokými možnostmi a ani v tomto případě se nejedná o výjimku. Univerzální řešení pro sdílení širokopásmového internetu zahrnuje připojení pomocí WAN ethernetového portu, 4 ethernetové LAN porty s nepříliš často vídaným řízením šířky pásma, 802.11b/g přístupový bod a USB rozhraní pro sdílení síťové tiskárny. Podpora VPN je v tomto případě velmi dobrá. Lze definovat tunely jak mezi pobočkami (LAN sítěmi), tak pro obsluhu jednotlivých VPN klientů, šifrování IPSec nabízí krom algoritmů DES a 3DES také nejnovější AES a pro zpětnou kompatibilitu nechybí podpora PPTP, dokonce s možností volit sílu šifry MPPE.
Ani další funkce nezůstávají pozadu. Velmi široké možnosti nabízí firewall díky způsobu sestavování pravidel, samozřejmostí je konfigurovatelný překlad adres (NAT) a ne zcela běžnou výbavou je možnost řídit QoS, resp. šířku přerozděleného pásma. Rovněž možnosti zabezpečení Wi-Fi provozu jsou výborné, samozřejmě včetně plné varianty WPA se zapojením serveru RADIUS. Zajímavý je také základní systém detekce útoku (IDS), včetně LED indikace. Tento Vigor patří k nejlépe vybaveným zařízením svého druhu.

plusy: firewall, možnosti VPN, QoS, VLAN
mínusy: WPA prozatím bez AES
Zapůjčila firma: AtTEL Bohemia, s.r.o.
Cena vč. DPH: 10 100 Kč

ASUS SL500
www.joyce.cz
Firma ASUS není žádnou neznámou a i v minulém díle našeho přehledu jste mohli nalézt model s touto značkou. Toto zařízení je koncipováno jako univerzální router pro malé sítě s velkým důrazem na možnosti zabezpečení. Je vybaveno 4 porty pro lokální ethernet, stejným rozhraním pro WAN linku a RJ-45 konzolovým konektorem pro administraci prostřednictvím sériové linky. Přestože připojení k internetu je navrženo univerzálně, pro tuzemské ADSL bychom ocenili PPTP konektivitu, jež kupodivu chybí, takže váš předřazený ADSL modem musí toto umět vyřešit.
Opravdu výborně provedený je firewall, jenž nabízí pokročilou konfiguraci pomocí politik pro určité skupiny uživatelů a řada uživatelů bezesporu ocení širokou škálu aplikačních filtrů, např. pro služby SIP a H.323 v oblasti internetové telefonie. Koncepčně podobným, propracovaným způsobem jsou implementovány VPN, kde je opět možno definovat politiky pro jednotlivé uživatele či jejich skupiny.
Dostatečně flexibilní je také obsluha LAN klientů pomocí DHCP služby, dobře lze nastavit službu NAT a na dobré úrovni jsou možnosti logování činnosti jednotlivých komponent.

plusy: firewall, NAT, aplikační filtry, VPN
mínusy: chybí WAN pomocí PPTP
Zapůjčila firma: Joyce ČR, s.r.o.
Cena vč. DPH: 4 100 Kč

3COM OfficeConnect VPN Firewall 3CR870-95
www.3com.cz
Společnost 3COM patří mezi tradiční výrobce síťových prvků a zde představované řešení je již delší dobu standardní součástí nabídky v rámci řady OfficeConnect pro připojování domácností a malých kanceláří. Jde o univerzální router, jenž na WAN rozhraní pomocí ethernetu připojuje ADSL či kabelový modem nebo jakoukoliv statickou či dynamickou IP bránu a do lokálního segmentu poskytuje 4 ethernetové porty.
Hlavní předností je kvalitní implementace virtuálních privátních sítí. Router podporuje „čistý“ IPSec, L2TP nad IPSec i PPTP spojení a v případě IPSecu dovoluje šifrovat také novou technologií AES, což zatím není zcela běžné. Jednotlivá spojení jsou jednoznačně rozdělena na tunelovaná a klientská a dle potřeby jsou takto obsluhována. Autentizace IPSecu je prováděna dle sdíleného klíče.
Z dalších funkcí je zajímavou možností nastavení priorit pro přidělení šířky pásma různým službám, velmi slušně je navrženo filtrování nežádoucího obsahu a obsluha LAN klientů službou DHCP je bez omezení v IP adresaci. Samozřejmostí jsou virtuální demilitarizovaná zóna, publikování služeb a zajímavostí pak služba NAT v režimu one-to-one (1:1).

plusy: IPSec s šifrou AES, NAT, QoS
mínusy: skromnější firewall
Zapůjčila firma: 3COM, pobočka Praha
Cena vč. DPH: 9 200 Kč

3COM OfficeConnect ADSL Wireless 11g Firewall Router 3CRWE754G72-B
www.3com.cz
Tento model z rodiny „kancelářského vybavení“ společnosti 3COM je zaměřen na sdílení internetové konektivity jak pomocí 4 portů tradičního ethernetu, tak prostřednictvím bezdrátového přípojného bodu Wi-Fi s rychlejší technologií dle normy 802.11g. Přestože má tento model přímo zabudován ADSL router k napojení splitteru a řadu variant připojení ADSL linky, dle našeho zkoumání mu chybí možnost připojení pomocí PPTP, což je v tuzemsku značná nevýhoda. Bezdrátové rozhraní je možno nasadit v sítích 802.11b/g s možností volby kompatibility a k dispozici je zabezpečení jak pomocí WEPu, tak formou WPA-PSK se sdíleným klíčem a WPA se serverem RADIUS. Novější standard AES k dispozici nebyl.
Oproti jiným modelům stejné řady je zde velmi dobře propracován firewall. Lze sestavovat složitější filtry, vázat je na konkrétní uživatele a také virtuální DMZ může pracovat na více počítačích. Samozřejmě zde nechybí filtrování dle MAC adres. Na druhou stranu nastavení DHCP serveru pro interní klienty je nešikovně omezeno na pevně daný síťový segment s určenou maskou třídy C.

plusy: možnosti firewallu
mínusy: chybí PPTP pro ADSL, omezení DHCP
Zapůjčila firma: 3COM, pobočka Praha
Cena vč. DPH: 5 100 Kč

3COM OfficeConnect Secure Router 3CR860-95
www.3com.cz
Tento model z nabídky společnosti 3COM představuje tradiční hardwarové řešení pro bezpečné sdílení internetového připojení s implementací virtuálních privátních sítí. Ethernetové WAN rozhraní je možno připojit ke kabelovému modemu, ADSL modemu včetně PPTP sestavení linky či jinému rozhraní se statickou či dynamicky přidělovanou IP adresou, do lokální sítě jsou k dispozici 4 ethernetové porty 10/100.
Podpora VPN je poměrně všestranná, takže je možno sestavovat jak IPSec tunely mezi pobočkami s různými LAN sítěmi, tak přímo připojovat klienty pomocí L2TP/IPSec nebo PPTP. Pro šifrování jsou k dispozici DES, 3DES i nejnovější AES, autentizace klientů IPSecu probíhá pomocí sdíleného klíče.
Poměrně dobré možnosti nabízí zabudovaný firewall, přesněji publikování služeb do internetu, propouštění specifických protokolů a hodně může také pomoci filtrování požadavků uživatelů z vnitřní sítě na základě klasifikace závažnosti obsahu. V případě dostatku WAN IP adres lze zprovoznit pro speciální účely službu NAT v režimu 1:1 a při obsluze LAN klientů pomocí DHCP služby nebudete ničím omezeni.

plusy: možnosti VPN, standard AES, aplikační filtry
mínusy: nic významného
Zapůjčila firma: 3COM, pobočka Praha
Cena vč. DPH: 3 700 Kč

DrayTek Vigor2900
www.attel.cz
Model s označením 2900 je velmi podobný svému sourozenci, o němž si můžete rovněž přečíst v tomto našem přehledu, a liší se v zásadě jen absencí bezdrátové části pro obsluhu Wi-Fi klientů. Připojení internetové linky lze realizovat přes ethernetový WAN port mimo jiné jako PPTP spojení pro tuzemské ADSL, nechybí statická či dynamická IP adresa. Pro LAN jsou k dispozici 4 ethernetové porty a 1 USB rozhraní pro síťovou tiskárnu.
Tradičně výborné jsou bezpečnostní funkce. Velmi propracovaný je firewall a možnosti definování příslušných pravidel, jenž zahrnuje také filtr URL adres či základní modul pro obranu proti DoS útokům. Široké možnosti nabízí také implementace VPN, kde jsou k dispozici šifrovací algoritmy DES, 3DES a AES, krom IPSecu nechybí PPTP a odděleně je možno konfigurovat jak vzdálené klienty, tak tunely mezi pobočkami.
Mezi ne zcela běžnou výbavu určitě patří technologie virtuálních LAN sítí s možností vazby na vybrané porty a omezením šířky pásma a rovněž funkce QoS pro řízení využití WAN linky není úplnou samozřejmostí. Možnosti DHCP serveru jsou také velmi slušné a kvalitní je též diagnostické rozhraní.

plusy: univerzální VPN, QoS na WAN, VLAN, Radius klient
mínusy: nic významného
Zapůjčila firma: AtTEL Bohemia, s.r.o.
Cena vč. DPH: 6 600 Kč

SMC BR14VPN a BR18VPN
www.compexdata.cz
Zařízení pod značkou SMC patří mezi stálice nejen na tuzemském trhu a většinou se vyznačují

širokou škálou funkcí, což potvrzuje tento představovaný model. Jedná se o širokopásmový router s řadou variant internetového připojení, mezi nimiž najdeme PPTP pro tuzemské ADSL či klasické IP připojení třeba ke kabelovému modemu, což v obou případech zajistí standardní ethernetový port. Zajímavou možností je zde klasický sériový konektor pro dial-up či ISDN modem, což rozšiřuje variabilitu WAN spojení.
Výbava funkcí pro VPN je velmi slušná. Router může pracovat jako brána pro spojení s ostatními pobočkami, kde je použit tradiční IPSec s dobrými možnostmi šifrování, a vzdálené klienty lze obsloužit pomocí PPTP či L2TP tunelovaných připojení. Variabilita konfigurace IPSec tunelů je velmi vysoká a správce tak má prakticky vše bezpečně pod kontrolou, včetně možnosti zvolit šifru 3DES.
Router dále nabízí kvalitní zabudovaný firewall a variabilní nastavení služby NAT, obsluha LAN klientů DHCP serverem je však nepříjemně omezena na rozsah adres třídy C. Router je dodáván ve variantách se 4 či 8 ethernetovými porty pro připojení lokálních počítačů.

plusy: variabilita WAN spojení, možnosti VPN
mínusy: omezení DHCP služby
Zapůjčila firma: Compex Data Bohemia, s.r.o.
Ceny vč. DPH: 3 200 Kč a 4 400 Kč

Linksys WRV54GS a WRV54G
www.levi.cz
Zařízení se značkou Linksys bezesporu nejsou zajímavá jen svým lehce futuristickým designem, ale též skutečností, že patří do stáje jednoho z dirigentů vývoje síťových technologií, společnosti Cisco. K dispozici jsme měli dvě zařízení s výše uvedeným označením, jež představovala dva odlišné světy.
Druhé uvedené je klasickým routerem s širokými možnostmi při sestavování VPN spojení. Pomocí ethernetového portu lze připojit ADSL, kabelové či jiné WAN rozhraní a lokální síť může být sestavena jak pomocí ethernetu, tak prostřednictvím bezdrátového připojení 802.11b/g s výbornými možnostmi zabezpečení, včetně RADIUS služby a AES. Implementace VPN nabízí dobré možnosti pomocí IPSecu, na druhou stranu L2TP či PPTP server chybí. Velmi dobrý je pak firewall s filtrováním na aplikační úrovni.
Mírně odlišný je model s označením GS na konci. Je vybaven řešením SpeedBooster pro rychlejší bezdrátový přenos, což jsme mohli vyzkoušet pomocí klientské karty stejného dodavatele, avšak zcela mu chybí výbava pro VPN, což jej předurčuje pro odlišné nasazení. Ideální kombinací by bylo propojení schopností obou zařízení dohromady.

plusy: IPSec s RSA autentizací, dobré možnosti VPN, Wi-Fi bezpečnost, logování
mínusy: omezení DHCP služby a lokální adresace
Zapůjčila firma: Levi International
Ceny vč. DPH: WRV54GS nestanovena, WRV54G 6 500 Kč