# Bezpečná brána do světa

# Staňte se experty na bezpečné připojení k internetu

#### MIROSLAV KNAPOVSKÝ

Bezpečnosti při připojení k internetu se věnuje v poslední době stále více pozornosti. Hackeři využívají slabin jak přenosových protokolů, tak i vlastních aplikací, takže musíme mít dokonalý přehled o tom, které aplikace, adresy či porty používáme, a které raději zakážeme. To nám zajišťují bezpečné brány, na nichž můžeme všechny potřebné parametry nastavit.

d podzimu loňského roku jsme měli k dispozici univerzální bránu 3Com OC Wireless 11g Cable/DSL Gateway, kterou lze připojit na libovolnou přípojku k internetu. U výrobků dalších producentů jsou postup při konfiguraci a funkčnost obdobné, takže jsme se rozhodli, popsat na ní celý postup při zabezpečeném připojení k internetu. Po přečtení tohoto článku by pro vás nemělo být žádným problémem připojit se bezpečně k internetu, a především nevynechat žádný důležitý krok, který je nutný pro zabezpečení přístupu zvenčí a k zajištění vlastní sítě LAN, především její bezdrátové části. Ta je vlastně prodloužením vaší domácí LAN sítě do volného prostoru, takže zabezpečení zvláště této části sítě není dobré podceňovat.

#### 3Com OC Wireless 11g Cable/DSL Gateway

Jedná se o bránu sloužící ke sdílení širokopásmového připojení k internetu pro více uživatelů současně. Kromě sdílení internetu je v zařízení integrován firewall s virtuální demilitarizovanou zónou, bezdrátový přístupový bod pracující dle IEEE standardu 802.11g rychlostí až 54 MB/s a čtyřportový přepínač 10/100 Ethernetu. Ačkoliv by se z názvu mohlo zdát, že je brána určena pouze pro připojení k ADSL či k internetu po kabelové televizi,



lze ji použít prakticky kdekoliv. Na "internetové straně" je tato brána vybavena 10/100 ethernetovým portem, takže ji lze připojit na libovolnou přípojku k internetu zakončenou právě Ethernetem. Zařízení se spravuje prostřednictvím webového rozhraní a vytvořenou konfiguraci lze zálohovat, a v případě potřeby obnovit v libovolné bráně stejného typu.

#### První kroky – využijte konfiguračního průvodce

Po rozbalení a zapojení napájení brána startuje přibližně 10 vteřin. Během startovacího procesu na předním panelu brány bliká kontrolka ALERT. Když natrvalo zhasne, zařízení je připraveno k základní instalaci. Ta se provádí z počítače vybaveného takřka libovolným operačním systémem (podporován je Linux, Windows i MAC OS) s podporou IP protokolu prostřednictvím webového prohlížeče. Dále v textu je postup konfigurace popsán pro operační systémy Windows, na jiných operačních systémech se jednotlivé kroky provádějí taktéž, ale syntaxe některých z nich může být mírně odlišná.

Počítač, ze kterého provádíte inicializační konfiguraci brány, připojte k bráně přes ethernetovou kartu přímým nebo kříženým kabelem (ano, je to jedno, zařízení podporuje automatické zjištění typu kabelu). Správnost za-

# Bezpečnost bezdrátových sítí

Komunikace v pásmu 2,4 GHz je jako většina rádiových přenosů všesměrová a všichni uživatelé obvykle sdílejí zvolený přenosový kanál tak, že pokud jeden uživatel přenáší data, ostatní naslouchají. Situace by se zjednodušeně dala přirovnat ke komunikaci prostřednictvím klasického ethernetového opakovače. Každý, kdo je v dosahu bezdrátového přístupového bodu a je vybaven příslušným bezdrátovým adaptérem, může přijímat stejný signál jako autorizovaný uživatel. Proto je více než jasné, že systémy bezdrátového přenosu musejí být vybaveny důkladnými bezpečnostními funkcemi, aby se bezdrátová komunikace dala považovat za bezpečnou. Systém zabezpečení bezdrátových sítí je obvykle kombinací ověření a šifrování. Podívejme se nyní, jak jednotlivé základní prvky bezpečnosti v bezdrátových sítích pracují a jaké jsou možnosti ověřování a zabezpečení přenosu dat.

#### Identifikátor obsluhované bezdrátové oblasti

Základním prvkem technologie bezdrátových sítí je informace o názvu obsluhované bezdrátové oblasti, ke které se uživatel připojuje (takzvaný Service Set Identifikátor – SSID). Tento identifikátor jednoznačně určuje, ke které bezdrátové síti se klient hodlá připojovat, a musí být totožný jak na přístupovém bodu bezdrátové sítě, tak u klienta této sítě. Jedná se o hexadecimální řetězec o délce až 32 znaků, jenž má zabezpečit komunikaci klienta s vyžádanou sítí. SSID však v současné době nemůžeme požadovat za platný bezpečnostní prvek, protože s rozvojem a zjednodušením technologie je většina bezdrátových karet schopna automaticky detekovat dostupné bezdrátové sítě a tuto informaci z okolního provozu jednoduše použít. V případě, že bezdrátový přístupový bod nevysílá veřejně svůj název SSID, lze jej z bezdrátové komunikace odposlechnout. I přesto, pokud to bezdrátový přístupový bod umožňuje, zablokujte veřejné vysílání názvu SSID.

#### Komunikace na základě povolených MAC adres

Dalším prvkem, který bychom mohli zahrnout do bezpečnostních vlastností bezdrátových sítí, by se mohla stát jednoznačná identifikace připojujících se uživatelů. Identifikace na základě jedinečné MAC adresy každé bezdrátové karty a jejího porovnání s tabulkou autorizovaných klientů v databázi přístupového bodu. Nicméně ani tato technologie bohužel neposkytuje byť jen základní bezpečnost. Z rádiové komunikace lze odposlechnout, které MAC adresy jsou na konkrétním přístupovém bodu autorizované, a jednoduchým zásahem do klientského systému lze MAC adresu upravit tak, aby odpovídala jakékoliv z autorizovaných. pojení zjistíte tak, že se rozsvítí příslušná kontrolka ethernetového portu. Pokud svítí žlutě, jste připojeni Ethernetem (10 Mb/s), svítí-li zeleně, jste připojeni Fast Ethernetem (100 Mb/s). Poblikávání stavové diody portu znamená, že daný port přenáší data.

Dalším krokem je nastavení počítače tak, aby získával IP adresu od DHCP serveru.

DHCP server je služba běžící na bráně, která na základě požadavku přidělí počítači dynamickou IP adresu, subnet masku a adresu brány tak, že odpovídá vnitřní adresaci sítě. To celý proces komunikace mezi bránou a počítači ve vnitřní části sítě urychluje a zjednodušuje. Na počítači s operačním systémem Windows 2000 nebo Windows XP zkontrolujete používání DHCP ve Vlastnostech síťové karty, protokol sítě internet (TPC/IP). Musí být nastaveno automatické získávání IP adresy i IP adresy DNS serveru. Dynamická IP adresa znamená, že si ji počítač z DHCP serveru pronajímá na omezenou dobu, po jejímž uplynutí může být tato IP adresa pronajata jiné stanici, pokud původní vlastník této IP adresy nezažádá o prodloužení nájmu. Může to znít složitě, ale celý proces je plně automatický a běží bez zásahu uživatele.

Správnost získání IP adresy lze velmi snadno ověřit tak, že v příkazové řádce napíšete příkaz "ipconfig". Tento příkaz zobrazí aktuální IP adresu počítače, a ta by v případě správného získání z DHCP serveru nenakonfigurované brány měla mít tvar 192.168.1.X, kde X se pohybuje v rozpětí od 2 do 254. Brána sama má v továrním nastavení IP adresu lokální sítě 192.168.1.1 s maskou 255.255.255.0. Pokud adresu od DHCP serveru brány nezískáte, zkontrolujte znova nastavení počítače a případně jej restartujte.

#### Vlastní konfigurace brány

Přístup ke konfiguračnímu rozhraní brány získáte tak, že ve webovém prohlížeči zadáte adresu http://192.168.1.1/ a stisknete Enter. V prohlížeči se načte úvodní stránka brány, ve které se ověřuje vaše heslo pro přístup k zařízení. Defaultní heslo je "admin", v konfiguraci dále jej doporučuji změnit. Po zadání hesla se načte další stránka, která po vás požaduje zvolit zemi, v jaké je zařízení využíváno. To je důležité z hlediska rádiové části brány, protože volbou země dojde ke správnému nastavení vysílacího výkonu integrovaného bezdrátového bodu a povolení kanálů, tak aby zařízení pracovalo v souladu s normami příslušné země. Nikdy proto nevolte jinou zemi, než tu, kde je zařízení užíváno. Po potvrzení volby země vyskočí nové samostatné okno prohlížeče, ve kterém se spustí konfigurační průvodce. Hned prvním krokem, který vám průvodce nabídne, je změna hesla. Dalším krokem je nastavení časové zóny, kde se zařízení nachází. Česká republika je v časovém pásmu GMT +1:00 a na této stránce zaškrtněte i využívání změny času. Brána totiž nemá vlastní hodiny, které by pracovaly i v případě vypnutí brány, ale informaci o čase si automaticky stahuje z internetu a upra-

# Počátky šifrování – Wired Equivalent Privacy (WEP)

Z výše uvedených vlastností bezdrátové sítě vyplývá potřeba celou komunikaci důsledně šifrovat. Proto byl do standardu 802.11 a jeho následníků 802.11b a 802.11g přidán systém, který měl zajistit úroveň bezpečnosti, jaká je dostupná na běžných, "drátových" sítích. Jedná se o šifrování veškeré bezdrátové komunikace pevným klíčem o délce 40 bitů (jsou využívány i delší klíče, ty ovšem nemají oporu ve standardu). Sdílený tajný klíč je používán k zašifrování paketů před odesláním bezdrátovou cestou a paket je také doplněn o kontrolní součet, který zajišťuje, že přenášený paket nebyl během cesty poškozen. WEP standard však nehovoří o způsobu, jakým je klíč generován, a tak většina stávajících řešení nabízí jen pevné nastavení klíče na obou stranách (jak v přístupovém bodu, tak u všech autorizovaných mobilních klientů). Pomineme-li veškerá bezpečnostní rizika spojená s vlastním nastavováním pevného sdíleného klíče, v poslední době se objevilo množství způsobů, jak bezdrátové sítě používající technologii WEP napadnout. Jedná se zeiména o pasivní odposlech, následné rozlomení šifry technologií srovnávání paketů a statistické predikce a výsledné získání používaného klíče. S běžně dostupnými prostředky (informace a programy volně dostupné na internetu) je hrozba prolomení WEP ochrany více než vážná. Kombinací SSID, tabulky MAC adres a šifrováním WEP tak lze dosáhnout jen omezené úrovně zabezpečení, ovšem pro domácí použití prozatím dostačující.

vuje na správnou hodnotu o rozdíl časového pásma a zda je letní či zimní čas. To je důležité pro přesnost časových údajů v protokolu o činnosti, který si brána vede.

#### Nastavené připojení k internetu

Dalším krokem v průvodci je nastavení připojení k internetu. Jak již bylo v úvodu zmíněno, brána na straně internetu vyžaduje přístupové zařízení s ethernetovým portem. Tím může být například router, ADSL modem, kabelový modem, bezdrátové pojítko či vlastní ethernetový rozvod internetu přímo od poskytovatele. Podívejme se, jak by se správně konfigurovalo zařízení ve třech různých typech připojení:

ADSL – Zvolte PPTP – pro připojení je třeba přepnout ADSL modem do režimu, ve kterém PPTP spojení neinicializuje modem, ale zařízení připojené až za modemem. Na bráně poté zvolíte způsob připojení PPTP a přepíšete do jednotlivých políček údaje dodané poskytovatelem ADSL. V dalším kroku nastavíte IP adresu brány, ze které se bude provádět inicializace PPTP tunelu. Pro správný údaj stačí stisknou tlačítko "Suggest", brána si vhodnou IP adresu nastaví sama. IP adresa uvedená jako PPTP server je adresou LAN portu vašeho ADSL modemu, nikoliv IP adresou, pod kterou bude vaše brána dostupná z internetu. Na ADSL jsou totiž IP adresy přidělovány dynamicky, a to i v případě, že vám poskytovatel garantuje pevnou internetovou adresu. Přidělenou internetovou IP adresu Ize zjistit v menu Status po dokončení konfiguračního průvodce.

• Kabelovým modemem – Zvolte via DHCP – i zde je IP adresa bráně obvykle přidělována poskytovatelem dynamicky, a to s možnou vazbou na jméno či MAC adresu koncové stanice, na kterou byla sepsána smlouva o připojení. Obojí lze samozřejmě v průvodci modifikovat. Pokud máte službu vázanou například na MAC adresu síťové karty vašeho počítače. Ize tuto MAC adresu vložit i do brány tak, že z pohledu poskytovatele nelze rozpoznat, zda se jedná o bránu či počítač. Obecně jsou k dispozici 3 možnosti: 1. nemodifikovat původní MAC adresu brány 2. zkopírovat MAC adresu počítače, ze kterého se provádí konfigurace (tuto volbu využijte v případě, že jste dříve měli ke kabelovému modemu přímo připojený právě tento počítač) 3. manuální změnu MAC adresy. Tuto volbu využijte v případě, že provádíte novou instalaci jak kabelového modemu, tak brány a poskytovateli jste již dříve dali MAC adresu, ze které se budete k internetu připojovat. • Čímkoliv ostatním s ethernetovým portem a pevnou IP adresu – Pokud vás poskytovatel připojení k internetu vybaví libovolným přístupovým zařízením a na předávacím protokolu je uvedena pevná IP adresace, kterou si do svého zařízení máte zadat, volte Static IP address. Dodané údaje vložte do následujícího menu průvodce.

#### Bezpečný přístup – Wi-Fi Protected Access (WPA)

Je novým Wi-Fi standardem, který znatelně vylepšuje bezpečnost dosažitelnou dříve používáním starších technologií, a prakticky tak eliminuje veškeré známé útoky, které se daly využít k prolomení sítě chráněné WEP technologií. WPA používá vylepšený šifrovací algoritmus s dynamickým klíčem, ověřování a kontrolní systém integrity paketů, který dokáže jednoznačně detekovat podvržené pakety. WPA technologie by u Wi-Fi certifikovaných zařízení neměla jít používat současně s WEP technologií, nicméně všechny prvky, které jsou certifikované Wi-Fi dle standardu 802.11g, by již technologii WPA měly mít obsaženou v základní výbavě. U produktů 802.11b to není podmínkou, ale u většiny modernějších zařízení solidní výrobci umožňují provést softwarový upgrade taktéž. U koncových zařízení je implementace WPA techniky záležitostí operačního systému, takže lze obecně říci, že karty s ovladači pro Windows 2000 a Windows XP mohou využívat WPA, protože podpora WPA byla v rámci opravných balíčků (Service Packu 4 u Windows 2000 a Service Packu 1 u Windows XP) do těchto systémů přidána.

#### Doporučení

Mají-li vaše zařízení Wi-Fi certifikát pro WPA, dejte přednost WPA před WEP. Nebudete se muset bát, že je ve vašem okolí hacker-začátečník, který si přečetl pár návodů na internetu a několik hodin nato získal přístup do vaší sítě.

to the Parks	U-faithers Laborat Read	DECENTY B	-	
anna lana	The Logical sets of the	a brittiana Pinana	Aught -	
and particular	Provident address Store 1988 Lat here	terrer T E BET 214 Jackson		

Nastavení IP adresace LAN, včetně možnosti vypnutí DHCP serveru. Systém podporuje i IP telefonii 3Com, takže v lokální části sítě lze využívat 3Com NBX IP telefonní ústřednu.



Potřebujete-li na internetu zveřejnit nějaké aplikace lokální sítě, snadno je přidáte do virtuální DMZ nastavením LAN IP adresy počítače, na kterém aplikace běží a volbou typu aplikace.

# Nastavení IP adresace lokální sítě

Po zadání způsobu připojení k internetu vás průvodce vyzve k nastavení IP adresace lokální sítě. Položky LAN IP address a DHCP server setup nemodifikujte, pokud to nevyžadují zvláštní okolnosti, jako například shodná IP adresace LAN a WAN sítě v případě, že i váš poskytovatel využívá překlad adres (NAT) a přiděluje IP adresy z "privátního prostoru".

Princip činnosti brány, privátní a veřejné IP adresy a jejich překlad: Činnost brány je založena na schopnosti zařízení využít jednu veřejnou IP adresu a jejím prostřednictvím umožnit komunikaci všech stanic vnitřní sítě do internetu. Rozdíl mezi privátní a veřeinou IP adresou spočívá v tom, že veřeiná IP adresa je na světě unikátní, a pokud není specificky omezeno, je zařízení s veřejnou IP adresou dostupné z celého internetu. Oproti tomu privátní adresace využívá adresných prostorů vyhrazených mezinárodní autoritou pro přidělování IP adres (IANA) pro použití v sítích, kde není nutná trvalá dostupnost zařízení z internetu. K systému využívání privátních adres se začalo přecházet v první polovině devadesátých let ruku v ruce s prudkým rozvojem internetu. Bylo jasné, že počet veřejných IP adres je pouze limitovaný a při tehdejším nehospodárném přidělování by se brzy vyčerpal. Dokumentem RFC1597 jsou privátní adresné prostory specifikované v následujících rozsazích: 10.0.0.1-10.255.255.255, 172.16.0.0-172.31.255.255 a 192.168.0.0-192.168.255.255, proto pokud budete modifikovat IP adresaci lokální sítě, volte z těchto vyhrazených rozsahů. Překlad adres brána provádí tak, že požadavky komunikace z vnitřní sítě na internet přebírá a vysílá do internetu s pozměněnou zdroiovou IP adresou. Na místo původní IP adresv odesilatele, která je z privátního adresného prostoru, použije veřejnou IP adresu přidělenou bráně. U všech navázaných spojení si pamatuje iniciální adresu stanice z vnitřní části sítě, a když obdrží odpověď, přepošle ji na původního tazatele. Technika překladu adres umožňuje bráně realizovat i funkci virtuální demilitarizované zóny. Tuto funkci využijete v případě, že hodláte zveřejnit nějakou službu na internet. Například, pokud byste chtěli zveřejnit interní webový server na internet a využíváte tuto bránu, stačí bráně sdělit IP adresu tohoto serveru a tvp aplikace, který hodláte publikovat. Limitem virtuální demilitarizované zóny je, že pro každou aplikaci lze publikovat pouze jeden server. V bráně jsou nejčastěji využívané aplikace již zadané. Pokud hodláte publikovat zde nedefinovanou aplikaci, musíte si dopředu zjistit UDP/TCP číslo portu, kterým se s aplikací navazuje spojení.



Nastavení základních parametrů bezdrátové sítě v jednom okně. Zde volíte kanál, na kterém bude přístupový bod pracovat, modifikujete název bezdrátové oblasti SSID a můžete zablokovat broadcast názvu SSID.



K volbě šifrování máte 40- a 128bitový WEP, příp. WPA s možností předsdíleného klíče nebo ověřováním na RADIUS serveru.



Nastavení profilu připojení k bezdrátové síti lze uložit do souboru a přenést do mobilního klienta. Při používání bezdrátových síťových karet 3Com si tak můžete ušetřit práci s manuální konfigurací klientů.

#### Nastavení bezdrátové části

Brána je vybavena bezdrátovým přístupovým bodem s teoretickým dosahem až 100 metrů v otevřeném prostranství. Dosah v zastavěném prostoru či uvnitř budov je velmi proměnný v závislosti na prostředí. V průvodci nastavením jste v prvním kroku dotázáni, jaký kanál si přejete bráně přidělit a jak se má imenovat vaše bezdrátová síť (SSID). Optimální volbou v případě kanálu je Clear Channel Select, což znamená, že brána po zapnutí poslouchá chvíli na všech 13 kanálech a automaticky zvolí kanál, na kterém detekuje nejmenší rušení. Stejný proces použije po každém restartu, takže se využívaný kanál může časem změnit. Název sítě je taktéž vhodné modifikovat, tentokrát však ne z praktických, ale spíše bezpečnostních důvodů. Je vhodné, aby název SSID nebylo možné spojovat jak s typem zařízení, tak s jeho majitelem. Tím končí zjednodušené nastavení brány pomocí konfiguračního průvodce. Po posledním odkliknutí se vložená nastavení hromadně vykonají a brána bez nutnosti restartu začne pracovat s novou konfigurací. Pokud jste prováděli změnu IP adresace využívané v lokální síti, je třeba obnovit IP adresu z DHCP serveru brány. To provedete příkazem "ipconfig/renew" v příkazové řádce.

#### Pokročilá konfigurace brány

Konfigurační průvodce brány umožní provést pouze základní nastavení. Z bezpečnostních důvodů je vhodné, abyste v konfiguraci pokračovali alespoň změnami v bezdrátové části brány a případně, pokud hodláte bránu spravovat na dálku přes internet, abyste v menu Firewall/Security specifikovali adresný prostor, ze kterého lze bránu vzdáleně spravovat.



**b** Ve statusu zařízení zjistíte aktuální revizi firmwaru brány, IP adresaci na LAN i WAN straně, nastavení bezdrátové sítě a rychlosti na jednotlivých portech brány.

	Long The		1 A
an being an being an being at at Tak		1. 4440 1. 4447 1. 4447 1. 4447 1. 4447 1. 4445 1. 4445 1. 4445 1. 4445 1. 4445 1. 4445 1. 4445 1. 4445 1.	ana Anna Anna
	Statut Inc.	man man (in 12 with 18 miles	

V logu brány najdete informace o činnosti zařízení a práci integrovaného firewallu. Log používá přesný čas získaný z internetu, modifikovaný o vámi nastavené časové pásmo. Je stručný, ale pro domácího uživatele velmi přehledný.

# Teorie integrovaného bezdrátového přístupového bodu

Na počátku je potřeba si uvědomit, že bezdrátová síť u této brány není úplnou náhradou konvenční LAN sítě, ale je jejím efektivním rozšířením. Dává mobilnímu uživateli svobodu pohybovat se po budově nebo po areálu pokrytém bezdrátovým signálem a přitom být stále připojený, mít přístup k aplikacím na lokálním serveru či k internetu, přijímat a odesílat elektronickou poštu a tisknout dokumenty. Slabší stránkou bezdrátových sítí pracujících dle standardu 802.11 je to, že se jedná o sdílené médium, jehož reálné přenosové rychlosti isou daleko vzadu za rychlostmi, které isou těmto standardům přiřazovány. Pojďme se podívat na základní pojmy z oblasti bezdrátových sítí. Určitě jste již slyšeli o takzvaném Wi-Fi, což bývá používáno jako synonymum pro zařízení bezdrátových sítí pracující dle standardu 802.11b až do rychlosti 11 Mb/s (teoretická rychlost) v nezpoplatněném rozprostřeném pásmu 2 400–2 483,5 MHz. Pro svoji komunikaci využívají 13 přenosových kanálů (pozor, kanály se překrývají a některé mohou být zarušené, proto raději volte funkci Clear Channel Select). Wi-Fi označení znamená, že se jedná o zařízení pracující přesně dle daného bezdrátového standardu a je plně interoperabilní s ostatními zařízeními s certifikátem Wi-Fi pro daný standard. Od konce léta loňského roku existuje i nový standard 802.11g, který je zpětně kompatibilní s 802.11b, tudíž i pracuje ve stejném pásmu. Nabízí však skoro 5násobně lepší rychlost (teoreticky 54 Mb/s), takže pokud se dnes budete rozhodovat také pro nákup koncového zařízení (PCMCIA, PCI nebo USB bezdrátové karty), bude již lépe volit některé z Wi-Fi certifikovaných 802.11g zařízení. Reálné přenosové rychlosti na bezdrátové části této brány se při nejlepší kvalitě signálu pohybují u klienta pracujícího dle staršího standardu 802.11b kolem 6 Mb/s a u klienta s kartou 802.11g je to pak kolem 23 Mb/s. Abyste nenabyli dojmu, že se zařízením není něco v pořádku, reálné přenosové rychlosti jsou u zařízení pracujících dle těchto standardů opravdu asi poloviční, než je jejich teoreticky udávaná rychlost. Daleko horší zprávou je, že pokud do sítě přidáte další mobilní klienty, kumulovaná přenosová rychlost ještě více klesá. Speciálně pak u přístupových bodů 802.11g, pokud se mezi uživateli vyskytují i klienti s kartou pracující dle 802.11b. Z toho vychází jasná rada, že pokud máte zájem, aby vaše 802.11g bezdrátová síť byla spolehlivá a co nejrychlejší, používejte pouze Wi-Fi certifikované karty pracující dle novějšího standardu. Seznam aktuálně certifikovaných zařízení všech výrobců naleznete na stránkách *www.wi-fi.org*.

**Praxe integrovaného bezdrátového přístupového bodu** Po nastavení konfiguračním průvodcem je v bezdrátové části brány umožněn přístup do lokální části sítě i internetu komukoliv bez omezení. Pro dokonalé zabezpečení bezdrátové sítě je třeba provést následující kroky:

 Zakázat vysílání názvu bezdrátové obsluhované oblasti. V menu Configuration by mělo zůstat prázdné políčko Enable broadcast SSID. Tím zabezpečíte, že název vaší sítě nebude volně viditelný pro mobilní klienty, a bez zadání správného SSID se klient nedokáže připojit.

2. Zvolit vhodné šifrování. V menu Encryption, pokud máte všechna koncová zařízení s podporou WPA, nejlépe i s Wi-Fi certifikací pro WPA, zadejte šifrování WPA. Pamatujte, že všichni bezdrátoví klienti připojující se k braně musí mít stejně nastavený šifrovací algoritmus a předsdílený klíč, jinak nebudou moci komunikovat. Jak u WPA, tak i u WEP šifrování můžete vložit klíč manuálně nebo pomocí parafráze, ze které se klíč automaticky vygeneruje. Parafrázi používejte pouze v případě, že klientské karty jsou od firmy 3Com; protože se jedná o nestandardizovaný postup, zařízení jiných výrobců nemusejí využívat shodný postup generování klíče z parafráze.

3. Řídit připojování bezdrátových stanic. V menu Connection control zvolte "only authorised Wireless…" a do nově otevřeného okna vložte MAC adresy bezdrátových síťových karet, kterým chcete povolit přístup do lokální sítě a k internetu prostřednictvím vaší brány. Všechny ostatní bezdrátové karty nebudou moci s vaší bránou komunikovat.

Na straně bezdrátového klienta pro jeho úspěšné připojení k bráně musíte nastavit následující parametry:

1. Kartu nastavit do infrastrukturního modu

Mít nastavený shodný název bezdrátové oblasti (SSID) jako brána
 Používat automatickou volbu kanálu (dnes běžná funkce u všech bezdrátových klientů, nicméně pokud to mobilní klient neumožňuje, budete na bráně muset nastavit některý z kanálů napevno a stejné číslo kanálu následně vložit i do klienta)

4. Používat stejný typ šifrování a šifrovacího klíče

**5.** Zkontrolovat, zda je správně zadaná MAC adresa bezdrátové síťové karty v seznamu povolených klientů

Pokud dodržíte tento postup, bezdrátová část vaší brány bude optimálně zabezpečena proti odposlechu a neoprávněnému vniknutí do lokální sítě či zneužívání vašeho internetového připojení.

# Něco je špatně? Pár dobrých rad nakonec Ztráta hesla či IP adresy brány

Pokud se vám náhodou stane, že zapomenete přístupové heslo na bránu, či si omylem vypnete DHCP server a zapomenete IP adresu brány, lze ji snadno uvést do továrního nastavení. Stačí bránu vypnout a jedním kabelem, který jste doposud využívali na propojení brány s počítačem, propojte LAN a WAN port brány. Bránu zapněte, a asi po 30 vteřinách zase vypněte. Rozpojte smyčku, a po dalším zapnutí brány již bude nastavena v továrním nastavení. (Vraťte se na začátek tohoto návodu a konfiguraci si zopakujte :-)

# Aktualizace firmwaru

Brána je něco jako počítač; operační systém se vyvíjí a upgradem operačního systému brány (firmwaru) můžete získat nové funkce či odstranit problém, se kterým jste si dosud nevěděli rady. Proto se občas podívejte na webové stránky společnosti 3Com, zda se pro zařízení neobjevil nový firmware. Pokud ano, stáhněte si jej na lokální počítač a zazipovaný soubor rozbalte. Bude obsahovat popis vylepšení pro bránu a firmware, který prostřednictvím webového rozhraní do brány za několik vteřin nahrajete. Nahrání nového firmwaru se inicializuje v menu System Tools/Upgrade. Po nahrání nového firmwaru a restartu není třeba bránu znova konfigurovat, ponechá si původní nastavení.