Takový neobyčejný firewall

NetScreen 5XP – hardwarový firewall pro domácí kanceláře a malé pobočky

PATRIK MALINA

Produkty společnosti NetScreen patří na českém trhu v podstatě mezi novinky, neboť začaly být dodávány tuzemským distributorem v průběhu loňského roku. Ačkoliv se tedy jedná o u nás téměř neznámé řešení, ve světovém měřítku jde o špičkovou technologii pro zabezpečení síťového provozu, jež se vyznačuje především schopností zvládnout kontrolu silných datových toků. V návaznosti na obsah brožurky, kterou jste mohli najít v PC WORLDu č. 6/2003, bychom vám zde rádi představili řešení sloužící k bezpečnému připojení menší či střední firmy – v nabídce NetScreenu představuje tento model jakousi základní variantu, což ovšem rozhodně neznamená slabší funkcionalitu. Vzhledem k tomu, že základem je stejný OS a výkonný hardware jako u vyšších modelů, může uživatel za rozumnou cenu získat poměrně dobrou výkonnost. Jenom pro srovnání, v souvislostech již zmiňované brožurky je možno toto řešení zařadit do nejvyšší „výkonnostní" kategorie.

NetScreen 5XP Firewall/ /VPN/IDS appliance

- ☺ podpora VPN
- ☺ koncepce správy
- ☺ IDS
- ☺ vzdálená distribuce politik
- ☺ dokumentace
- ☹ na vnějším rozhraní neumí PPTP (nutné pro ADSL v Evropě)
- ☹ chybí konzolový kabel

K recenzi zapůjčila a distribuuje firma:
VUMS DataCom, s. r. o., Praha 8
www.datacom.cz
Cena: pro 10 uživatelů 645 USD
neomezená 1 300 USD

NetScreen 5XP je firewall typu appliance, tedy „černá skříňka" (v tomto případě tmavomodrá) se dvěma síťovými konektory typu RJ-45 pro běžnou ethernetovou kabeláž UTP kategorie 5, jež jsou označeny jako Trusted (důvěryhodný) pro vnitřní síť a Untrusted pro síť vnější. Pak už jsou k dispozici jen LED kontrolky indikující funkcionalitu, a všeho ostatního, čeho je zapotřebí, dosáhnete samozřejmě pomocí vzdálené správy. Metodou nejdostupnější pro většinu správců je zřejmě práce prostřednictvím webového prohlížeče a počáteční kroky jsou standardní – firewall očekává na vnitřní síti přihlášení na defaultní síťové adrese. Správa je rovněž dostupná pomocí textové konzole, a to buďto přes sériový port a konzolový kabel, nebo telnetem, a třetí možností je pokročilý administrativní nástroj NetScreen Global-Pro. My jsme prakticky vše zkoušeli pomocí prohlížeče. Pro úplnost dodejme, že v krabici obdržíte dva síťové UTP kabely (konzolový kupodivu chybí) a CD s dokumentací.

I v případě, že spravujete zařízení pomocí webového rozhraní, nemusí být vše ihned zřejmé. Je to dáno tím, že prakticky stejný OS slouží i pro nejvyšší modely, a proto zde je potřeba pochopit určité základní koncepty. Veškerá aktivita firewallu při ochraně síťového provozu je v podstatě řízena pomocí tzv. politik, jež pracují na principu spouště – nastanou-li definované podmínky, určitá politika se aplikuje, a výsledkem její činnosti může být stejně dobře zahození paketu jako sestavení šifrovaného VPN tunelu do žádoucí sítě. Dalším důležitým stupněm abstrakce jsou tzv. zóny, za nimiž se skrývají určité definované fyzické sítě, splňující stejné nároky na zabezpečení. Řízení provozu se poté provádí právě mezi zónami, což zajišťuje přehlednou a logickou správu. V neposlední řadě je

též potřeba pochopit tzv. mody síťových rozhraní, jež mohou pracovat v režimu transparentním (jako bridge), směrovacím (tedy jako router) a v modu překladu (se službou NAT). Klíčem k detailnímu využití možností NetScreenu jsou elementy jednotlivých politik, a proto nečekejte při správě instantní, prostá řešení. Počáteční investice do detailní konfigurace se vám však bohatě vyplatí.

Pojďme ke konkrétním možnostem. Při konfiguraci síťových rozhraní u tohoto základního modelu s úspěchem využijete na veřejném rozhraní možnost získat dynamickou adresu pomocí DHCP, zatímco do vnitřní sítě pomocí téže plně konfigurovatelné služby obsloužíte své klientské počítače. Síťová rozhraní mohou pracovat ve všech zmíněných modech a k dispozici máte až 100 různých politik, což dle našeho odhadu využijete jen výjimečně. Velmi zajímavé možnosti jsou k dispozici při ověřování klientů – lze sestavit interní databázi (zvládne 100 položek) či lépe využít populární externí služby typu RADIUS, RSA SecurID, LDAP (třeba MS Active Directory) či běžné ověření pomocí prohlížeče. Zajímavé je, že tyto možnosti jsou k dispozici v plné síle stejně, jako byste si pořídili nejdražší model, což platí i v oblasti šifrování tunelů VPN. Pro „hromadné" zpracování můžete zvolit algoritmy DES, 3DES či moderní AES, a omezení oproti vyšším kategoriím představuje počet současně sestavených tunelů, jenž je zde stanoven na 10, a to bez ohledu na typ (tunel mezi sítěmi či klient-brána). Pokud srovnáte posledně zmíněný fakt s vlastnostmi některých konkurenčních řešení, oceníte tento produkt. S uvedeným těsně souvisí též nekompromisní možnosti využití technologie IPSec, jež představuje integrální součást VPN protokolu L2TP, kde při ověřování můžete plně využít stávající infrastrukturu certifikátů či zajistit jejich automatické generování. Z mnoha drobností neopomeňme podporu přechodu IPSec komunikace skrze službu NAT. Zajímavě „rovnostářsky" přistupovali tvůrci k celé produktové řadě i u dalších funkcí, a proto zde u modelu 5XP najdete dosti bohatý IDS, výborné možnosti logování a monitorování činnosti či řízení datového provozu.

Jak jsme již zmínili, model 5XP je dimenzován pro použití v malých sítích či např. k připojení domácí kanceláře, čemuž odpovídají výkonnostní parametry. Rychlost obou hardwarových síťových rozhraní je 10 Mb/s a firewall dokáže v podstatě beze ztrát na rychlosti toto pásmo „ošetřit", a to i při provozu VPN tunelů (tedy např. šifrování algoritmem 3DES). Asi se shodneme, že při současných možnostech širokopásmového internetového přístupu je to pro připojení domácí kanceláře či malé pobočky více než dostačující kapacita.

Na závěr poznámka k licencování a ceně. NetScreen vás ani tady nechce stresovat či mást, takže máte dvě možnosti – licenci pro 10 uživatelů nebo neomezenou. 3 0479/FEL ❑