

**Vysoká bezpečnost, nenáročné nastavování**

Astaro Security Gateway nabízí vysokou bezpečnost a uživatelskou přívětivost za rozumnou cenu. Check Point UTM1 je takřka dokonalý nástroj řízení obrany proti všem nástrahám, které se na sítích mohou objevit, posílený zázemím zkušeného dodavatele síťových produktů. A u Cyberoam CR15i zdůrazněme, že nenáročné nastavování není jeho jedinou předností.

**Modularita i práce s příkazovou řádkou**

Baví-li vás jemné nastavování, pak bude zřejmě Juniper SRX 100 vaší volbou. Je ideální pro přívržence práce s příkazovým řádkem. Kernun, český bohatýr boje proti hrozbám, pak nabízí rozsáhlé možnosti, výkonnou hardwarovou platformu i flexibilitu sestavy z řady modulů. A WatchGuard XTM 810, to je skutečný obrnělec pro velké sítě.

# Zařízení UTM ochrání vaši síť

**Problém bezpečnosti a jeho různorodost vede správce podnikových sítí i vedení podniků ke hledání efektivních způsobů obrany před možností napadení sítě nebo zcizení důležitých dat. Vývoj této činnosti vedl k definování jednotných principů obrany a její správy pod názvem Unified Threat Management, jednotné řízení bezpečnosti. Stále neexistuje přesná a všeobecně platná definice a zkratka UTM se používá mnohdy, v obecné rovině; její technický obsah zůstává trochu mlhavý.**



JIŘÍ ČEJKA

**J**ednotné řízení bezpečnosti zahrnuje tři velké oblasti. Bezpečnost síťového přístupu, bezpečné surfování po webu a bezpečné předávání elektronické pošty. Napříč přes tyto tři oblasti se táhne jiné možné dělení bezpečnostních problémů, a to podle typů možných útoků.

Mluvíme v této souvislosti o ochraně proti virům, proti nežádoucím e-mailovým zprávám (které nejen obtěžují, ale především mohou obsahovat potenciálně nebezpečné prvky), proti úmyslnému přetížení či případnému vyřazení z provozu sítí nebo serverů poskytujících služby a posledním, nikoli však nejméně důležitým bodem ochrany, je schopnost odolat různým pokusům o zcizení důvěrných dat.

Důležitou charakteristikou UTM je sjednocení fronty obrany proti všem vyjmenovaným hrozbám útoku do jednotného systému, soustředěného do jednoho místa a přehledně a pokud možno snadno ovladatelného jedním systematickým nástrojem. Přirozenými body, kde se dají tyto zásady realizovat, jsou místa, kudy proudí v největší hustotě síťový provoz – směrovače (routery) a firewally. Není proto divu, že přední výrobci těchto zařízení mají koncept UTM ve svých jednotkách již nějaký čas zabudován. Zajímalo nás, s jakou úspěšností se charakteristiky UTM podařilo různým dodavatelům posunout z komerční roviny do reálného fungování nabízených zařízení a systémů.

Přestože problém bezpečnosti asi nejvíc pálí velké firmy, rozhodli jsme se testovat spíše malé jednotky navržené pro použití v menších a střed-

ních podnicích. Vedly nás k tomu otázky praktické realizace testů a kromě toho i obava, že zařízení pro menší podniky nebudou mít všechny aspekty bezpečnosti tak dobře ošetřeny, jak se dá očekávat u drahých a propracovaných systémů a zařízení pro největší podnikové sítě.

Z nabízeného spektra jednotek a systémů jsme se soustředili hlavně na ty, které jsou u nás dostupné prostřednictvím českých zástupců nebo distributorů. Tím se výběr poněkud omezil, ale jak potom provedené testy ukázaly, je většina řešení UTM na vysoké úrovni a poskytuje téměř vše, co bychom od těchto zařízení očekávali.

Vlastní testování se provádělo tak, že jsme se postavili do role nového majitele zařízení či systému s nálepkou UTM a prováděli jsme nastavení a konfiguraci pokud možno všech důležitých prvků bezpečnosti tak, jak by to asi dělal typický uživatel, od samého začátku, kdy máme v ruce jednotku se základním nastavením z továrny a přizpůsobujeme ji svým požadavkům. Kde to bylo možné, zkoušeli jsme odolnost proti různým předpokládaným typům útoků simulováním skutečného napadení. Použili jsme pro to vzorky známých testovacích virů, typické e-mailové zprávy z kategorie spamu a pokusy o neautorizovaný přístup do sítí nebo podsystémů. Jak se dalo očekávat, všechny naše snahy o prolomení ochrany testované jednotky odrazily, což ale samozřejmě lze přičíst i na vrub použitých pokusů. Jako viry jsme použili testovací vzorky běžně dostupné pro tyto účely na webu; spamy jsme simulovali jednak

**i** Jednotná koncepce obrany proti útokům na síti (Unified Threat Management) není jen komerčním pojmem a náš test zařízení, nesoucích tuto nálepku, se vás o tom pokusí přesvědčit.

prakticky přijatými vzorky, klasifikovanými jako spam jinými prostředky, anebo pokusy poslat e-mailem zprávu s typickými slovy očekávanými ve zprávách kategorie spam. Z takto prověřené odolnosti samozřejmě nevyplývá, že testovaná zařízení či systémy jsou dokonalé, známou skutečností je neustálý předstih kybernetických zločinců před všemi způsoby ochrany, vyplývající z omezení, které obrana v této oblasti má. Přesto je naše zjištění pozitivním signálem, že boj proti kriminalitě na sítích je úspěšný.

sestav pro nastavení pestré škály jednotlivých vlastností zařízení. Od samého počátku konfigurace, kdy je možné použít průvodce konfigurací (pro méně zkušené uživatele) anebo nastavit všechny nebo jen některé parametry a vlastnosti ručně, je k dispozici detailní a zpracované zobrazení, s jehož pomocí lze navigovat po všech důležitých oblastech správy bezpečnosti.

Zařízení umožňuje nastavovat všechny základní i mnoho dalších bezpečnostních prvků velmi podrobným způsobem. Řadu detailů lze ihned kontrolovat na stavových

Astaro, úvodní obrazovka.

## Astaro

Řada Astaro Security Gateway má několik typů, které se liší především počtem připojitelných účastníků. Nejmenší typ 110/120 obsluhuje méně než 100 účastníků, typy 220 a 320 jsou pro větší sítě. Pro velké sítě se dodávají zařízení 425, 525 a 625, z nichž poslední obsluhují až 5 000 účastníků. Pro náš test jsme vybrali malou jednotku ASG 120.

Jednotka má kromě čtyř ethernetových portů i dva USB konektory, na které se může připojit např. USB klávesnice, a VGA port pro displej. Pro připojení konzole je tu sériový COM port. Připojený displej umožňuje kontrolu stavu zařízení, ale není z něj možné měnit konfiguraci.

Ovládání jednotky je přes webové rozhraní. Na počítači, připojeném k jednomu ethernetovému portu zařízení, se administrátorovi zobrazuje bohatá konfigurační stránka s mnoha desítkami dílčích

tabulkách a podrobných reportech, které zařízení poskytuje na požádání, anebo podle nastaveného plánu.

Prošli jsme podrobně řadu dostupných variant síťové bezpečnosti, bezpečnosti přenosu e-mailů, webové bezpečnosti i bezpečnosti webových aplikací. Ve všech oblastech a na všech úrovních granularita podává Astaro Security Gateway podrobnou, přehlednou a jasně pochopitelnou informaci o prováděných úpravách a nastavené bezpečnostní konfiguraci. Velmi užitečná je možnost konfiguraci zálohovat a při nečekaných událostech (např. výpadku napájení apod.) zazálohovanou konfiguraci použít k automatickému nastavení zařízení do předchozího stavu.

Stejně jako automatické zálohování konfigurace lze určit, i kdy a jak často se provádí automatická aktualizace virových a spamových

## INZERCE

vzorků. Zařízení sleduje i aktualizace firmwaru, ale ty jen automaticky stáhne a pak administrátora upozorní na nutnost instalace, která může vyžadovat restart, a proto se nemůže udělat v libovolném okamžiku.

Při procházení dílčích nastavení nás upoutalo nejen, jak rozsáhlé a podrobné lze různé možnosti nastavovat, ale především jak snadno to lze dělat a ve většině případů i okamžitě kontrolovat úspěšnost daného nastavení. Z tohoto hlediska lze Astaro Security Gateway považovat za zařízení velmi dobře připravené každodenní práci administrátora sítě.

Kdybychom chtěli vypsat všechny možnosti pro zabezpečení sítě, e-mailu a webového přístupu, zřejmě bychom překročili možnou velikost tohoto článku. Stačí jen říct, že nechyběl žádný prvek obvykle u těchto zařízení dostupný. Naopak některé podrobnosti značně přesáhly obvyklý rozsah konfiguračních možností.

## Check Point

Firma Check Point je jednou z nejvíce zavedených na trhu zařízení pro správu bezpečnosti. Při prověření zařízení UTM 1-136, ačkoli

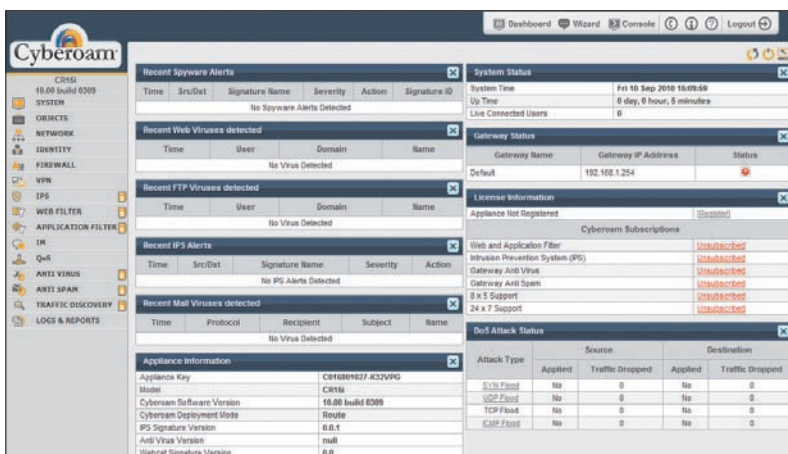
se jedná o nejmenší ve své kategorii, se tato reputace jen potvrdila. Od samého začátku testů bylo patrné, že jde o vysoce profesionálně vytvořené zařízení, jemuž předcházela dlouhá a úspěšná vývoj předchozích jednotek.

Nastavování a konfigurace sítě se dělá buď na úrovni příkazů konfiguračního jazyka, nebo pomocí grafické webové konzole, anebo konečně na lokální grafické aplikaci dostupné ke stažení pro několik různých platform. Každý z těchto tří způsobů je určen pro určité zákaznické prostředí a stupeň podrobnosti a přesnosti konfigurování.

Jednotka obsahuje několik modulů tzv. softwarových bládů. Jejich počet a struktura jsou do značné míry volitelné, což umožňuje velkou flexibilitu zákaznického uspořádání. Dodatečně je možné sestavu rozšířit podle rostoucích potřeb zákazníků. Pro ilustraci jména několika z těchto „software blades“: Firewall, IPSec VPN, IPS, Anti-Virus & Anti Malware, Anti-Spam and Email Security, URL Filtering.

Po prvním zapojení lze použít konfiguračního průvodce, který uživateli usnadní základní nastavení. Protože je firma orientována na větší sítě, nepřekvapí, že z jed-

Check Point a jeho přehledné výstupy.



Cyberoam, grafická konfigurace.

noho místa lze spravovat několik jednotek současně. Lze je spojovat do skupin s podobnými vlastnostmi a tyto skupiny je možné spravovat jako celek. Všechny prvky bezpečnosti, nejen antivir a antispam, dostávají automaticky podle nastavitelného plánu aktualizace vzorů.

Ochrana před nežádoucími útoky na bezpečnost se realizuje na tzv. Multi-Tier Threat Detection Engine, což je kombinovaný systém detekce

hrozby útoku s pomocí signatur, validace protokolu, detekce anomálií, behaviorální analýzy a dalších metod, jejichž efektivnost se díky několika použitým přístupům odhalení hrozby blíží ke stu procent úspěšnosti. Více než 90% procházejícího síťového provozu nevyžaduje hlubší analýzu, a zbývající síťová aktivita tak může být podrobně a přesně analyzována systémem IPS, aniž se nadměrně zvýší zatížení systému a následně sníží propustnost.

Antivirová a antispamová kontrola používá několik úrovní a přístupů pro co nejdokonalejší odhalení možné hrozby. Na prvním místě je hodnocení reputace IP adresy, ze které provoz pochází. Dynamicky aktualizovaná databáze umožňuje rychlé a účinné zablokování provozu již jen na základě IP adres příchozího datového toku. Další úroveň je filtrování podle obsahu, které zahrnuje nejen textové skenování, ale i filtrace podle vzorů, takže je možné zpracovat i obrázky a zprávy v cizích jazycích. Testování podle blacklistů (seznamů zakázaných zdrojů) a whitelistů (seznamů důvěryhodných zdrojů) umožní vytřídění dalších možných hrozeb. Následuje antivirové skenování včetně komprimovaných souborů a e-mailových příloh.

Systematickým sledováním výskytu spamu a škodlivého softwaru na celém internetu je možné zablokovat zprávy, pro které ještě nejsou k dispozici aktuální spamové nebo virové signatury.

Poslední vrstvou obrany je IPS, který chrání před útoky typu DoS

(Denial of Service) a přetečení, směřujícími dovnitř infrastruktury jednotky. Kombinací všech výše popsaných subsystémů ochrany lze dosáhnout vysokého stupně zabezpečení před všemi známými i dosud neznámými typy útoků na bezpečnost.

Nastavení konfigurace s grafickým rozhraním je snadné a přehledné. K dispozici je bohatá množina připravených variant nastavení jednotlivých prvků, do kterých se v některých případech jen doplní číselné nebo jiné konkrétní hodnoty, které administrátor chce pro nastavení použít. Kontrola a uvedení prvků nastavení do konfigurace jsou rychlé a nezdržují práci.

## Cyberoam

Jednotka Cyberoam CR15i spadá do kategorie malých systémů pro nepřehledné rozsáhlé sítě, určených pro malé a střední podniky, SOHO (Small Office – Home Office) a ROBO (Remote Office Branch Office). Je částí koncepce Extensible Security Architecture (ESA), díky níž se v budoucnu může jednotka rozšiřovat

INZERCE

# Kernun Clear Web – chytré české řešení, které je efektivnější

Webové filtry jsou na výsluní – jsou stále častěji používány, už dávno nejsou doménou velkých nadnárodních korporací a své nepostradatelné místo nachází i v organizacích střední velikosti. Hned ze dvou důvodů. První je zvýšená produktivita zaměstnanců – webové filtry poskytnou pouze takový obsah internetových serverů, které zaměstnanci ke své práci potřebují. Druhý důvod je ryze bezpečnostní – webové filtry dokáží zabránit přístupům na kontroverzní portály, které poskytují problematický obsah anebo jsou využívány pro vylákání citlivých údajů. Při dnešní rychlosti, s jakou se mění obsahy milionů webových stránek na celém světě, je ale úspěch či neúspěch webového filtru závislý především na kvalitě databáze, se kterou pracuje.

Studie provedená společností TNS ukazuje, že organizace o 600 zaměstnancích dokáže navštívit až 85 tisíc webových stránek. Průměrný zaměstnanec si stáhne do svého webového prohlížeče 142 stránek. Tyto patří průměrně do 2 400 různých domén druhého řádu (např. seznam.cz, ceskatelevize.cz, atd.). Na jednu doménu tedy připadá průměrně 35 kliknutí. Ze studie dále vyplynulo, že až 75 procent domén patří doméně prvního řádu .cz, 21 procent patří k mezinárodní doméně .com a pouze 4 procenta k jiným doménám. Je tedy zřejmé, že absolutní počet kategori-

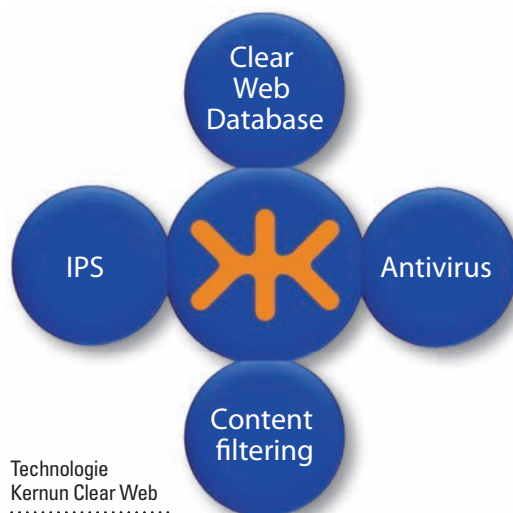
zovaných domén není důležitý. Místní surfeři se zajímají zejména o webové stránky v českém jazyce a je proto nutné zaměřit se při výběru filtru na kvalitu kategorizace zejména lokálního obsahu.

Porovnali jsme proto výsledky reálného nasazení zahraničního web filtru a českého produktu Kernun Clear Web. Šlo o konkrétní nasazení těchto dvou řešení v počítačové síti krajského úřadu. Původní řešení poskytovalo jednu z nej-

větších databází s desítkami milionů kategorizovaných stránek. Výrobce v honbě za co největší databázi používá automatickou kategorizaci pomocí „umělé inteligence“ a vůbec nezohledňuje požadavky konkrétního nasazení. Kolik českých uživatelů se podívalo na stránku <http://www.troy.ao?> Naproti tomu české řešení Kernun Clear Web klade důraz na úspěšnost databáze a její kvalitu. Pracuje s konkrétními www stránkami, které uživatelé sítě skutečně používají a jejich zařazení do kategorií je kontrolováno operátory. Tak je dosahováno nejen vysoké kvality, ale i úspěšnosti databáze.

V popisovaném testu se zvýšila úspěšnost webového filtru ze 45 procent na 95 procent u domén „.cz“ a z 85 procent na 92 procent u domény „.com“. Navíc měli uživatelé k dispozici české webové rozhraní oznamující důvod zablokování přístupu, mnohem preciznější zařazení nejnavštěvovanějších stránek ([seznam.cz](http://seznam.cz), [email.cz](http://email.cz)), lepší kategorizaci nebezpečných stránek a administrátoři detailní statistiky využívání internetu jednotlivými zaměstnanci.

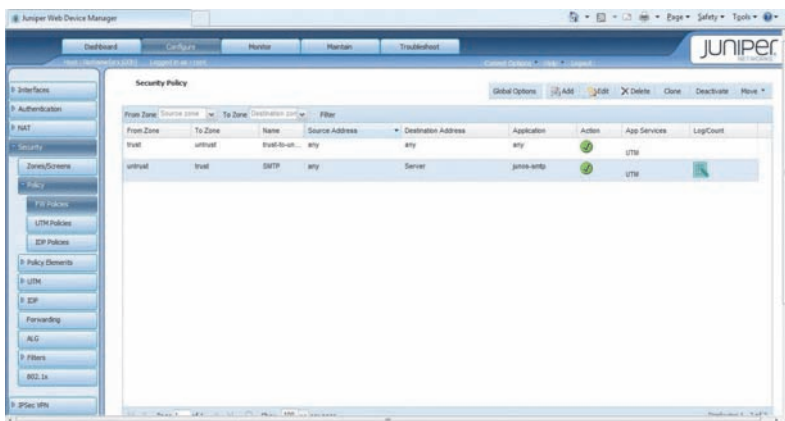
České řešení Kernun Clear Web je chytré. Nesnaží se o maximální databázi, protože o ni nikdo nestojí. Místo toho dosahuje dvojnásobné úspěšnosti v konkrétním nasazení s mnohem vyšší kvalitou databáze.



## Přehledová tabulka

Výrobce	typ	instalace, konfigurace	síťová bezpečnost	e-mailová bezpečnost	webová bezpečnost	další vlastnosti	lokalizace	dodavatel	Cena bez DPH
Astaro	Security Gateway 120	snadná a přehledná, bohaté dílčí možnosti	firewall, VPN, autentizace, ochrana proti DoS, IPS a další	dvojitý antivir, antispam, šifrování a další	proxy, dvojitý antivir, URL a obsahová filtrace, ochrana proti spywaru, filtrace IM a P2P, skenování HTTPS	ochrana webových aplikací, HA*	částečná	Annex NET	HW 15 000 Kč, licence FullGuard 16 250 Kč ročně
Check Point	UTM1-136	velmi podrobná konfigurace, webová, z příkazového řádku nebo lokální GUI aplikací	firewall, VPN, autentizace, paketová filtrace, IPS, ochrana před DoS, ochrana VoIP a další firemní nadstavby	antispam, antivir, antispoofing a další	proxy, antivir, URL a obsahová filtrace, hash filtrace podle neobvyklé statistiky výskytu a reputace a další	HA*	ne	Check Point Software Technologies	HW a roční licence 96 000 Kč
Cyberoam	CR15i	podrobná konfigurace pomocí webového rozhraní a průvodce, možnost příkazového řádku	firewall, IPS, autentizace, obsahová filtrace, filtrace IM a P2P, ochrana před DoS a DDoS	antivir, antispam, filtrace podle MIME hlavičky	webfilter včetně HTTPS, proxy, obsahová filtrace, URL filtrace (blacklist), filtrace podle IP reputace	HA*, ochrana webových aplikací, aplikační kategorie	ne	Comguard	13 900 Kč včetně licence
Juniper	SRX 100	méně uživatelsky příjemná, ale přehledná	firewall, VPN, autentizace, ochrana před DoS, IPS, UAC	antivir, antispam a další	proxy, antivir, URL a obsahová filtrace		ne	DNS	HW a roční licence 70 200 Kč
TNS	Kernun	velmi podrobná konfigurace, kombinace GUI a příkazů ve vlastním jazyce	paketová inspekce, VPN, autentizace a ochrana před DoS, IPS/IDS a další	antivir, antispam a další	webový filtr, URL a obsahová filtrace, ochrana proti spywaru a další	HA*	částečná	TNS	bez hardwaru od 50 000 Kč, s HW od 80 000 Kč
WatchGuard	XTM 810	podrobná konfigurace pomocí webového rozhraní nebo lokálního System Manageru, možnost použít průvodce konfigurací	firewall, VPN, filtrování obsahu v aplikační vrstvě, autentizace, ochrana proxy pro většinu protokolů, IPS, ochrana před DoS, DDoS a PAD, LiveSecurity@Service	Gateway Antivir/IPS s Virus Quarantine, antispoofing, SpamBlocker s Virus Outbreak Detection	WebBlocker s HTTPS URL filtrováním	HA*, správa provozu (QoS), přepnutí WAN, vyvážení zátěže serveru	ne	Permanence	od 208 000 Kč včetně roční podpory

\* High Availability



Juniper, nastavení politik.

o dodatečné funkce a schopnosti. Podle výrobce je „IPv6 Ready“, tedy připravena pro integraci nové verze IP adres v budoucnosti.

Nastavování a konfigurace se provádějí přes webové rozhraní a průvodce, vyspělí uživatelé mohou rovnou konfigurovat jednot-

livé prvky bezpečnosti, a pokud chtějí, mohou použít i konfiguraci prostřednictvím příkazového řádku. Odezva systému u námi testované jednotky byla rychlá a možnosti přehledně uspořádané, což práci administrátora usnadní a urychlí.

Grafické rozhraní obsahuje velké množství dílčích kategorií bezpečnosti a většina z nich má ještě pod sebou další bohaté možnosti nastavení nebo dílčích složek. Je tak možno dosáhnout optimálně vyvážení nastavení podle požadavků uživatele a charakteristik používaných sítí.

Antivir pracuje s jádrem Kaspersky, pravidelně aktualizovaným podle nastaveného plánu. Filtrace spamů používá nejnovější způsob,

RPD (Recurring Pattern Detection), který sleduje výskyt typických spamových zpráv na internetu a blokuje přenos přes jednotku dříve, než je samotný spam detekovatelný na použité jednotce svou signaturou. Navíc se tak získá nezávislost na konkrétním jazyce, ve kterém je spam šířen. Pro dokonalé fungování je ovšem třeba rozsáhlé sítě sledovacích robotů, kteří neustále monitorují tok zpráv a webových stránek a v případě potvrzeného výskytu informují všechny jednotky Cyberoam.

WEBCAT je nástroj pro filtrování založený na kategorii webové stránky, ne na jejím obsahu. Obsahuje víc než 80 kategorií a přes 40 milionů URL v databázi. Je tak možno efektivně blokovat přístup

INZERCE

NOVÁSPOJENÍ.DNS.CZ



Juniper Networks - routery, switche, WAN, datová centra, IT bezpečnost - špičkové systémy, které svými parametry poskytují maximální užitečnou hodnotu.

Zařízení jsou známa svou vysokou mírou spolehlivosti, stabilitou a odolností. Produkty Juniper zajistí všem uživatelům otevřené a flexibilní síťové služby s vysokou mírou zabezpečení. Zcela bezkonkurenční je dosažený poměr ceny a výkonu. Více na [novaspojeni.dns.cz](http://novaspojeni.dns.cz).

JUNIPER NETWORKS

**30 USD** za každý port Vašeho starého switchu: [novaspojeni.dns.cz/30usd](http://novaspojeni.dns.cz/30usd)

# VÁŽENÝ PANE VYBARVENÝ, S NÁMI SI MŮŽETE DOPŘÁT BAREVNÝ TISK I VE VAŠÍ KANCELÁŘI.

Nové barevné tiskárny KYOCERA Vám pomohou vylepšit dojem ze všech dokumentů, které opustí Vaši kancelář. Propadněte brilantní tiskové kvalitě ve spojení s nešední výbavou, spolehlivostí a obzvláště nízkými náklady na vytištěnou stranu. Více naleznete na [www.kyocera.cz](http://www.kyocera.cz)

- ▶ Duplexní jednotka pro automatický oboustranný tisk **ZDARMA**
- ▶ Síťová karta s pokročilými bezpečnostními funkcemi **ZDARMA**
- ▶ Vícenásobný podavač obálek, etiket a zvláštních formátů **ZDARMA**
- ▶ Patentovaná technologie zaručující nejnižší náklady na tisk ve své třídě
- ▶ Rychlost až 21, resp. 26 stran A4 za minutu černobíle i barevně

**KYOCERA. POČÍTEJTE S NÁMI.**

#### Kontaktujte nás prosím:

Distributor pro ČR: JANUS, spol. s r.o. – Tel.: (+420) 222 562 246 – [www.kyocera.cz](http://www.kyocera.cz)  
KYOCERA MITA Corporation – [www.kyoceramita.com](http://www.kyoceramita.com)  
KYOCERA MITA Europe B.V. – [www.kyoceramita.eu](http://www.kyoceramita.eu)



Ilustrační foto včetně volitelných součástí.

na stránky, na kterých je nevhodný obsah maskován např. do obrázků a podobně.

Zařízení umožňuje řídit šířku pásma, vyhrazenou jednotlivým službám. Tak se efektivně dosahuje QoS – řízení kvality přenosu. Služby s vyšší prioritou mají přiřazenou zaručenou propustnost a při větším zatížení jednotka aktivně omezuje přenos služeb s nižší prioritou, aby tak prioritní služby běžely se zaručenou šířkou pásma.

## Juniper

V nabídce firmy Juniper je několik směrovačů, které mají i řadu UTM vlastností. V řadě SRX je nejmenší typ SRX100 s průchodností firewallu 650 Mb/s, vhodný pro menší firmy, zatímco největší SRX5800 pro datová centra velkých podniků nabízí firewall s průchodností 120 Gb/s.

Test jsme uskutečnili s nejmenší jednotkou SRX100. Má osm ethernetových portů a jeden USB konektor. Jeden ethernetový port se typicky používá pro připojení k externí síti (untrusted) a zbylých sedm je pro vnitřní síť (trusted).

Zařízení je primárně firewallem. Pro zvýšení stability a spolehlivosti je použit proprietární operační systém JUNOS a z toho vyplývají i logika a způsob ovládání a konfigurování sítě a bezpečnostních parametrů. Skalní přívrženci Unixu a programování z příkazového řádku si tu přijdou na své. Kromě přímé konfigurace na úrovni JUNOSU je možné použít i webové rozhraní, ale pro jeho použití u jednotky čerstvě dodané z továrny je nejdříve potřeba několik detailů nastavit na nižší úrovni příkazového řádku. Při procházení podrobností konfigurace jsme měli dojem, že konfigurovatelnost jednotky, i když dostatečně pestrá a obsahově bohatá, je méně „uživatelsky přívětivá“, než by průměrný uživatel očekával. Dodavatel nabízí pro usnadnění správy jednodenní školení na JUNOS zdarma.

Zajímavým jevem, který jsme neviděli u jiných výrobců, je vzájemné provázání některých parametrů konfigurace. Proto je nastavení konfigurace v každém kroku dvoufázové, nejprve systém prověří správnost prováděné změny, a pokud kontrola dopadne dobře, vyzve administrátora k potvrzení změny příkazem Commit.

THE NEW VALUE FRONTIER



U systému lze nastavit celou řadu konfigurací sítě, pro některé z nich je třeba restart jednotky. V menu grafického webového rozhraní jsou v levé části záložky pro jednotlivé oblasti konfigurace a po jejich otevření se objeví dílčí podoblasti pro konfiguraci, případně u některých i další nižší úroveň konfigurační struktury. Jak už bylo uvedeno, prakticky všechny změny musí být nejprve ověřeny a pak potvrzeny, což při větším množství změn poněkud zdržuje.

V konfiguraci je množství prvků typických pro nastavení a ovládání síťového přístupu. Pro nás bylo zajímavější nastavení bezpečnostních prvků a tam najdeme všechno, co bychom od jednotky UTM očekávali. Lze konfigurovat antivir (Juniper používá antivirové jádro Kaspersky), ochranu proti spamu, filtrování podle URL i podle obsahu a některé další aspekty. Celkově jsme měli dojem, že i když počet jednotlivých variant je velký, přece jen možnosti v jednotlivých podrobnostech jsou pouze základní, ale samozřejmě tu skoro vždy nechybí možnost přidání nového, zákaznický definovaného nastavení.

Neměli jsme možnost ověřovat průchodnost jednotky, ale odezva na většinu konfiguračních zásahů, ať už prováděných z příkazového řádku anebo z webového rozhraní, byla v řádu sekund. Občas se objevily drobné nestability grafického rozhraní, bylo třeba vyčkat neobvykle dlouho na další krok konfigurace a podobně.

## Kernun

Společnost Trusted Network Solutions je jediným výrobcem z České republiky v tomto přehledu zařízení UTM. Její produkt Kernun byl původně dodáván jako čistě softwarové řešení. Protože jeho instalace na nevyhovujícím hardwaru uživatele vedla někdy ke snížení kvality implementace, rozhodla se firma systém dodávat včetně hardwaru. Používají se serverové jednotky Dell ve čtyřech možných velikostech podle předpokládaného rozsahu sítě a datových toků.

Hardware používá operační systém KernunOS, vyvinutý z FreeBSD. Nastavení a konfiguraci lze provádět na konzoli pro Windows, Linux a BSD a používá se při ní vlastní konfigurační jazyk umožňující neomezeně variabilní sestavu

použitých pravidel a filtrů. Pro zjednodušení byl vyvinut konfigurator, který uživatele vede k napsání správné konfigurace pomocí kontroly syntaxe v reálném čase.

Dalším prostředkem pro zjednodušení a usnadnění práce je gra-



Kernun, modulární architektura.

fická konzole, na které se buď interpretují příkazy konfiguračního jazyka jako graficky ovládané prvky (s rozbalovacím menu a podobně), anebo se prvky systému graficky zobrazují formou detailních seznamů, popřípadě různých typů grafů (sloupcových, pásových, koláčových atd.).

Zvláštní charakteristikou systému Kernun je jeho modularita. Sestavu pro konkrétního zákazníka lze složit z několika nezávislých modulů věnovaných dílčím oblastem bezpečnosti. Modulů je celkem 15 a v nedávné době byly doplněny dvěma moduly pro IPv6. Tímto způsobem lze snadno pro každého zákazníka vytvořit přesně „na míru“ sestavený komplet odpovídající jeho požadavkům.

Počáteční nastavení systému je podřízeno zásadě „co není výslovně povoleno, je zakázáno“. Proto musí být do nastavení zařazeno mnoho filtrů zajišťujících požadovanou bezpečnostní funkcionalitu systému. Při testování nám bylo jasné, že sestavování a ladění konfigurace je práce pro opravdové odborníky na síťovou bezpečnost. Pokud uživatel nepostupuje zmíněnou cestou konfigurator – průvodce, je počáteční nastavení vyloženě netriviální postup. Firma TNS pro tento účel nabízí systém jako službu, při které konfiguraci a péči o chod systému přebírá firemní specialista.

Při konfigurování pomocí grafického rozhraní jsme viděli velké

množství připravených variant pro všechny prvky bezpečnosti, dovolující pouhým klikáním sestavit velmi podrobně granulovanou bezpečnostní strukturu. Pokud tedy administrátor přesně ví, čeho chce dosáhnout, vychází mu grafické rozhraní daleko vstříc.

Anitvir a antispam, používající jádra volitelných třetích stran, mají nastavitelnou automatickou aktualizaci.

## WatchGuard

Původně jsme pro tento test chtěli použít malou jednotku WatchGuard XTM 2, ale protože nebyla momentálně dostupná, otestovali jsme větší zařízení, WatchGuard XTM 810. Tato jednotka je určena pro střední a větší podniky, se svými deseti 1GB porty umožňuje firewallovou propustnost až 5 GB/s.

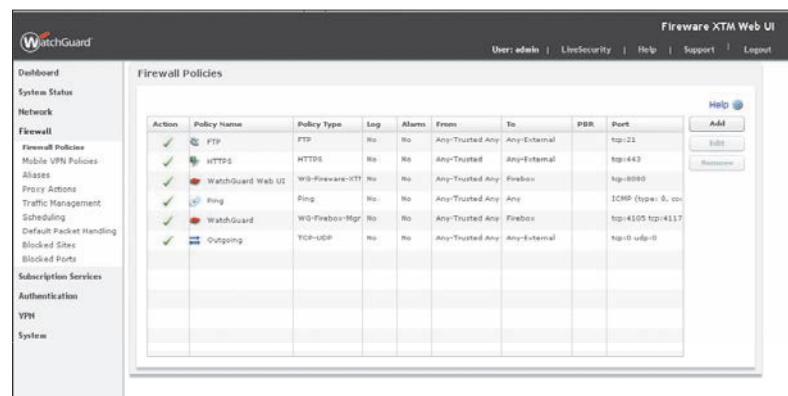
Zařízení má kromě deseti ethernetových portů na předním panelu i třířádkový LCD displej a čtyři kurzorová tlačítka, umožňující základní sledování a nastavení provozu jednotky. Nastavování a konfigurace se provádějí buď pomocí webového rozhraní s možností průvodce, nebo pomocí aplikace System Manager pro Windows, lokálně běžící na počítači administrátora. Protože je základní nastavování v režimu DHCP, jsou právě započaté kroky takřka automatické.

Počáteční menu obsahuje v levém sloupci jen několik kategorií, Dashboard, System Status, Net-

kromě údajů o jednotce (model, verze atd.) poskytuje i přehledně informace o všech licencích pro jednotlivé složky subskripce včetně doby platnosti (zbývající dny) a o všech připojených portech. Navíc formou časových grafů ilustruje zatížení procesoru a využití paměti.

Nejdůležitější pro nastavení bezpečnostních prvků jsou záložky Firewall, Subscription Services a Authentication. Každá vede na řadu dílčích kategorií s množstvím připravených voleb pro nastavení a samozřejmě i možností přidávání dalších uživatelských nastavení. Na rozdíl od většiny ostatních výrobců neposkytuje WatchGuard licenci na celkovou funkcionalitu jednotky, ale nabízí několik dílčích možností subskripce, licencovaných samostatně. To dává uživateli možnost konfigurovat svou sestavu na míru svým požadavkům, a vyhnout se tak placení zbytečných nákladů za služby, které by pro něj nemusely být důležité.

Obdobnou funkcionalitu pro konfigurování nabízí lokální System Manager. Přestože jde o lokální aplikaci, je možné s její pomocí spravovat i vzdálené jednotky; na začátku práce se uživatel svým jménem a heslem přihlásí buď k určitému zařízení, nebo serveru a ten pak v dalších krocích může sledovat nebo spravovat. System Manager grafickou formou umožňuje vybrat z připravených možností dílčí prvky konfigurace anebo přidávat nové



WatchGuard, firewall.

work, Firewall, Subscription Services, Authentication, VPN a System, ale každá z nich pod sebou nabízí dostatečně bohaté možnosti pro nastavení požadovaných bezpečnostních vlastností. Celkový stav zařízení popisuje první položka Dashboard, která v pravém panelu

hodnoty obdobně jako při práci s webovým rozhraním, navíc ale poskytuje grafy nastavení a využití pro celou řadu parametrů síťové a bezpečnostní konfigurace jednotky, ke které se administrátor předtím přihlásil.