

# MODRÁ JE DOBRÁ

## Recenze hardwarového firewallu Cyberoam UTM CR25i

**Bezpečnostní brána Cyberoam – UTM Firewall – najde využití především v malých a středních firmách, a to díky komplexnosti ochrany v rámci jednoho zařízení a dostupné ceně. Cyberoam nabízí revoluční funkci řízení provozu založeného na identitě uživatele a volitelnou integraci s Active Directory.**

**P**roduktová řada výrobce obsahuje celkem 7 modelů UTM Firewallu, jsou určeny podle výkonnosti jak pro trh SOHO, tak SMB či Enterprise. UTM zařízení Cyberoam nabízí firewallové funkce s možností řízení provozu založeného na identitě uživatele a volitelnou integraci s Active Directory. Samozřejmostí je podpora VPN, řízení šířky pásma, URL filtrace včetně HTTPS, antiviru, antispanu, IPS, detekce IM a P2P. Chrání proti hrozbám, jako jsou spyware, spam, phishing, viry, trojani, DoS útoky a další. Nastavení pro jednotlivé uživatele snadno určí, jaké aplikace mohou spouštět, jaký obsah využívat, jakou šířku pásma mají přidělenou, nebo jaký objem dat mohou stáhnout či uploadovat. Český dovozce nabízí tři modely CR25i, CR50i a CR100i.

My jsme měli k dispozici základní model CR25i. Zařízení má na přední straně umístěné LED diody indikující činnost a rychlost 4 Ethernet portů, indikaci napájení a činnost vestavěného HDD. Zadní část obsahuje již zmíněné 4 Ethernet porty 10/100, dva porty USB, vstup pro externí napáječ, sériový COM port. Celé zařízení je umístěné v modré kovové krabici, slouží nejen k ochraně elektroniky a vestavěného 3,5 palcového HDD, ale i k lepšímu odvodu tepla.

### Nastavujeme

Konfigurace byla prováděna z Web Admin Console, která nás bude zajímat asi nejvíce, lze se připojit i do konsoly My Account a Reports. V IE 7.0, Firefox 3.0 a Opera 9.51 nebyl v zobrazení žádný rozdíl, vše fungovalo naprosto korektně. Vstup do zařízení je, jak jinak, chráněn uživatelským jménem a heslem, které jsou uvedeny v příložené příručce. Opravdu jen k základní konfigu-



raci slouží tzv. Wizard, kterým se nastavují následující položky.

- » Mód zařízení. Lze nastavit mód Gateway – brána a nebo mód Bridge – most. Častěji se bude zařízení používat jako brána.
- » Konfigurace portů. Každý Ethernet port lze nakonfigurovat pro různé použití (LAN, WAN, DMZ). Ve výchozím nastavení je port s označením A nastaven pro LAN.

Port s označením B je nastaven pro WAN a port s označením C je nastaven pro použití DMZ.

- » Konfigurace přístupu k internetu lze nastavit ve třech úrovních.

Pouze monitorování – bez jakékoliv blokace.

Hlavní politika – Blokování nežádoucích spojení. Scan HTTP portu a virů.

Striktní politika – Bez autentifikace nelze uskutečnit žádný přístup

### Ceny zařízení a podpory

Doporučená maloobchodní cena zařízení pro 10 uživatelů: 18 500 bez DPH; cena zařízení pro 25 uživatelů: 21 000 bez DPH, cena zařízení pro neomezený počet uživatelů: 25 700 bez DPH a cena zahrnuje:

Roční podporu 8x5, Firewall, VPN, Bandwidth Management, Multiple ISP Load Balancing & Failover and Reporting Module. Licence modulu Antivirus & Antispam na 1 rok. Licence modulu IDP na 1 rok. Licence modulu Web & Application Filter na 1 rok.

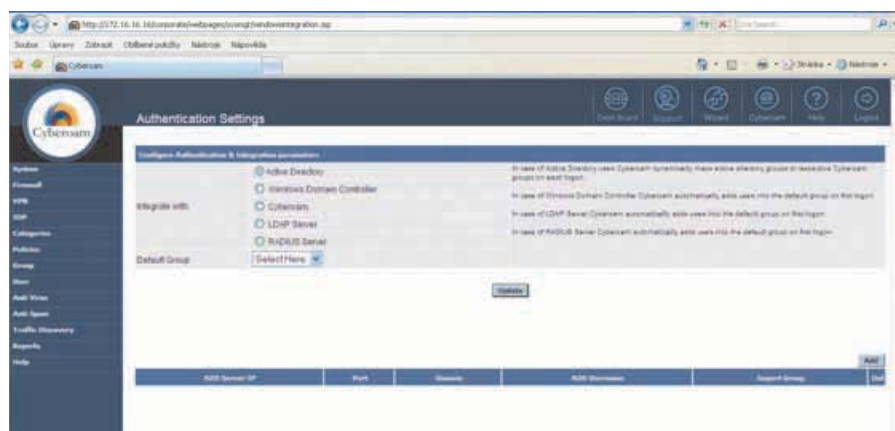
Za příplatek lze licence rozšířit na 2 a 3 roky a podporu na 24 x 7.

### Propustnost Cyberoam CR25i

Propustnost firewallu	100 Mbit/s
168 bit Triple DES/AES	30/75 Mbit/s
Propustnost antiviru	30 Mbit/s
Propustnost IPS	60 Mbit/s
Propustnost UTM	25 Mbit/s

- » Nastavení emailu – Slouží pro zaslání zpráv správci systému, zadá se emailová adresa, port a IP adresa emailového serveru.
- » Čas, datum a časová zóna

Zařízení lze konfigurovat přes jednotlivé menu a podmenu na levé straně obrazovky. Spočítali jsme, že zařízení obsahuje zhruba 150 menu a podmenu, je tedy opravdu co konfigurovat. Lze konstatovat, že je administrace velmi jednoduchá a přehledná a odpo-



Integrace s Active Directory zvyšuje komplexnost zařízení.

- + integrace s AD
- + silný reporting, monitoring, statistiky
- + dostupná cena
- absence 1Gb Ethernet portů
- omezení pouze na antivirus Kaspersky



#### Jiří Vrchota

Pracuje jako IT Manager ve společnosti Piccolo. Informačním technologiím se profesionálně věnuje již od roku 1993.



URL filtrace poskytuje 68 kategorií, které lze „brouzdajícím“ uživatelům zakázat.

vidá dnešnímu standardu. Pokud je administrátor delší dobu neaktivní, bude automaticky odpojen. V administraci lze plně konfigurovat např. DNS, DDNS, DHCP, Proxy, NAT, VPN, IPS, IDP, VLAN, GRE Antivirus, Antispam, Uživatelé, Skupiny, Politiky, QoS atd.

### Připraven na vše

Co vše vlastně UTM CR25i obsahuje a umí? Je to stavový firewall, který chrání protokoly síťové vrstvy a služby. Lze definovat bezpečnostní zóny a pravidla dle identit uživatelů nebo IP. Dále komponenta pro prevenci průniku (Intrusion Prevention System, IPS) schopná odhalit útoky známé i neznámé. Dnes je i u HW řešení nezbytností integrovat antivirový a antispamový program, v tomto případě je to systém Kaspersky, který skenuje elektronickou poštu (protokoly POP3, SMTP, IMAP), přenos souborů (FTP) i webový provoz (HTTP). Anti-Spam je zabezpečen systémem Commtouch s filtrem obrázkového spamu.

Filtrování webového provozu vychází z vlastní vestavěné databáze web kategorií, je prováděno blokování URL, blokační na základě klíčových slov a typu souborů.

Samozřejmě nesmíme zapomenout na komponentu VPN, která zajišťuje bezpečnou komunikaci v internetu vytvořením šifrovaných datových tunelů mezi jednotlivými lokalitami. Ta neslouží jen k propojování lokalit, ale umožňuje i vzdálený přístup (IPSec, Integrity SecureClient) nebo L2TP, PPTP.

K řízení šířky pásma využívá zařízení funkce QoS (Quality of Service), která umožňuje nastavit minimální a maximální šířku pásma datového toku. Lze přitom definovat větší množství pravidel. Zařízení má silně zastoupený reporting, monitoring, statistiky a logování.

Např. monitoring aktuálně procházejícího provozu na jednotlivého uživatele se zobrazením download a upload dat a celkového počtu stažených dat, MRTG (The Multi Router Traffic Grapher) grafy se statistikami o objemu a chybovosti provozu a zátěži zařízení. Revolučním řešením v oblasti řízení firemní bezpečnosti je jednoduchá integrace s Active Directory nebo jinou adresářovou strukturou uživatelů. Politiky se pak určují na uživatele. Např. jaké aplikace může spouštět, jaký obsah využívat, kdy se může připojovat vzdáleně, jakou šířku pásma může využít nebo jaký objem dat může stáhnout. Pokud nemáte Active Directory či jinou adresářovou strukturu, Cyberoam poskytuje stejné funkce jako jiný firewall pro běžné nastavení pravidel provozu.

### Pro koho?

Tento firewall, který není v podstatě čistokrevným firewallem, ale víceúčelovým zařízením, najde využití především v malých a středních firmách, a to díky komplexnosti ochrany v rámci jednoho boxu a dostupné ceně. Revolučním řešením je pokročilá, a přesto jednoduchá integrace s Active Directory nebo jinou adresářovou strukturou uživatelů. □

inzerce ▼

Chcete si připadat  
SKUTEČNĚ ZABEZPEČENÍ?  
Pořídte si...

**secure**  
computing®

**Webwasher®**  
Web Gateway Security

#### » Secure Web 2.0

Ochrání Vás před hrozbami webového provozu v prostředí Web 2.0 a zneužívání Internetu zaměstnanci.

#### » Komplexní řešení: SecureWeb Cache, URL Filtrace SmartFilter, AntiMalware, kontrola SSL a Antispam.

Unikátní sada ochran s napojením na TrustedSource.org

#### » Gartner Magic kvadrant leader.

**SecureCache™**  
Webwasher Gateway

» **Revoluční technologie** šetří až 50% konektivity i v dnešním dynamickém prostředí WEB 2.0 a podrobuje „skladované“ objekty proaktivní kontrole a testům reputace.

» **Nativní provázanost** s ostatními moduly Webwasher.

**IronMail®**  
Messaging Gateway Security

» Přesná a efektivní detekce spamu a virů.

» **Nejkomplexnější řešení** s ochranou proti úniku dat, IPS pro mail servery a web mail, šifrování, uživatelské účty, LDAP.

» Gartner Magic kvadrant leader.

**SmartFilter®**  
Web Gateway Security

» Řízení přístupu k internetu.  
» Zvýšení produktivity práce.



**Sidewinder®**  
Network Gateway Security

» Aplikační proxy firewall.  
» IPS, Antivirus, Antispam, URL filtrace.

Distributor pro ČR a SR  
www.comguard.cz; info@comguard.cz

**COMGUARD**  
communication security