

# Modrý ďábel pro bezpečnou síť

## PETR VELECKÝ

Mezi zajímavé UTM (Unified Threat Management) firewally v letošním roce na českém trhu přibýly také produkty společnosti Cyberoam, která je schopna uspokojit i náročné zákazníky, avšak její nabídka začíná u levného, ale dobře vybaveného a flexibilního modelu CR25i. Ten za velmi příznivou cenu nabízí celou škálu bezpečnostních funkcí včetně své unikátní vlastnosti, již je snadná integrace s Active Directory a definování/aplikace bezpečnostních politik na základě identity uživatelů.

Přední panel zařízení malých rozměrů obsahuje pouze sérii stavových LED, zatímco vzadu najdete COM port, dva USB a čtveřici 10/100Mb/s ethernetových portů – absence podpory gigabitového Ethernetu, který se už i v těch menších firmách stává samozřejmostí, nás sice nepotěšila, ale fakticky koresponduje s maximální propustností firewallu, která činí 100 Mb/s. Při spuštění dalších funkcí propustnost klesá a se všemi aktivními UTM funkcemi zařízení poskytuje výkon 25 Mb/s – to je dostatečná kapacita pro menší firmy. V rámci uvedených parametrů poskytoval Cyberoam stabilní výkon. Navíc každý ze čtveřice ethernetových portů si můžete libovolně nakonfigurovat jako WAN, LAN či DMZ,

což umožňuje vytvořit konfiguraci s podporou fail-overu a více internetových připojení pro vysokou dostupnost.

CR25i je coby nejmenší model dodáván jako komplexní balíček s plnou funkcionalitou (vyšší verze dovolují volbu funkčních bloků dle požadavků), která zahrnuje Stateful Inspection firewall, IPSec, L2TP, a PPTP VPN, antivirus/antispayware



Cyberoam CR25i

a antispam (pracují jako gateway), IPS (Intrusion Prevention System), filtrování aplikačního provozu a obsahu, řízení šířky pásma, správu více připojení a reporting.

Počáteční nastavení není úplně nejjednodušší (bereme-li v potaz orientaci na malé a střední firmy), nicméně tento fakt lze považovat za relativně malou daň za vysokou flexibilitu.

K nejzajímavějším vlastnostem patří zmíněná schopnost monitorovat a analyzovat provoz či události na základě identity uživatele (konvenční přístupy jsou založeny pouze na IP adresách). Samozřejmě to předpokládá, že využíváte (nebo hodláte využívat) síťové adresářové

služby Active Directory nebo LDAP/RADIUS databázi, s nimiž pak můžete zařízení integrovat. Privilegia či omezení tak můžete aplikovat na již existující skupiny uživatelů či jednotlivce a ověřování probíhá přes protokol LDAP. Chcete-li podle identity ověřovat uživatele (či systémy), kteří se v adresáři nenacházejí nebo se nejsou schopni identifikovat, nainstalujete na ně klientské agenty (ve verzi pro Windows nebo Linux), kteří autentizaci umožní. Účty a skupiny těchto uživatelů definujete přímo ve firewallu. Tento způsob aplikace bezpečnostních pravidel může poskytnout nejen dodatečnou úroveň ochrany, ale třeba také lepší možnosti sledování aktivit uživatelů. Kromě toho ale UTM dovoluje také běžnou kontrolu bez autentizace, tj. podle IP.

U antiviru Cyberoam sází na osvědčený engine Kaspersky, který podporuje protokoly HTTP, FTP, ale také SMTP, IMAP a POP3, a antispam využívá technologii Commtouch a dovoluje tvorbu white- i blacklistů. Podezřelé zprávy – spam i ty zavírované – se ukládají do karantény na vestavěný disk.

K silným stránkám produktu řadíme filtrování URL/obsahu a řízení šířky pásma – a to zejména díky možnostem aplikace pravidel podle uživatelů a skupin s vysokou mírou

pružnosti. Kategorie webových stránek jsou již předdefinovány a lze je dále podle potřeby dělit, třeba na „pracovní“, „nepracovní“ a „nežádoucí“ atd., a dle toho aplikovat příslušná omezení včetně časových parametrů, kdy například povolíte prohlížení „nepracovních“ webů na půl hodiny denně.

Také možnosti reportingu lze v této kategorii produktů označit za nadprůměrné – dovolují velmi detailně sledovat bezpečnostní incidenty i aktivitu uživatelů podle různých kritérií a nechybějí ani přehledné grafy.

Model CR25i může být díky své ceně a flexibilitě lákavou alternativou zejména pro menší firmy. Využíváte-li možnost autentizace uživatelů, pak výrobce uplatňuje licencování podle počtu (autentizovaných) uživatelů. Pokud možnosti autentizace nebudete využívat, můžete zařízení nasadit za základní cenu bez omezení počtu uživatelů.

(wep) 8 0510

### Cyberoam CR25i

- definice politik na základě identity uživatele, filtrování, podpora pro fail-over, cena
- ➖ konfigurace, externí napájecí adaptér

**Prodejce:** Comguard, [www.comguard.cz](http://www.comguard.cz)  
**Cena (bez DPH):** 18 500 Kč pro 10 současně autentizovaných uživatelů, 21 000 Kč pro 25 současně autentizovaných uživatelů, 25 000 Kč pro neomezený počet uživatelů (vše s licenci a podporou na 1 rok, v nabídce jsou balíčky na 1, 2 nebo 3 roky), 5 500 Kč obnova licence, podpory na HW a záruky na 1 rok

INZERCE

## ORACLE DEVELOP

Největší konference pro vývojáře ve střední Evropě

10. a 11. února 2009

Congress Hotel Clarion  
PRAHA

# D

# DEVELOP

[www.oracle.com/events/oracledevelop/prague](http://www.oracle.com/events/oracledevelop/prague)

JSF, SQL, PL/SQL, ASP and AJAX

Forms, SOA, .NET, XML, Security, BPEL, JSF, SQL, PL/SQL, ASP and AJAX  
 DBA, Java, EJB 3.0, JPA, Forms, SOA, .NET, XML, Security, B

SQL, PL/SQL, ASP, and AJAX

AJAX, ASP and  
 PL/SQL, ASP, and AJAX

XML, Security, BPEL, JSF, SQL, PL/SQL, ASP, and AJAX

BPEL, JSF, SQL, PL/SQL, ASP, and AJAX

EJB 3.0, JPA, Forms, SOA, .NET, XML, Security, BPEL, JSF, SQL,  
 SOA, .NET, XML, Security, BPEL, JSF, SQL, PL/SQL, ASP, and AJAX  
 Java, EJB 3.0, JPA, Forms, SOA, .NET, XML, Security, BPEL, JSF, SQL, PL/SQL, ASP, and AJAX

BPEL, JSF, SQL, PL/SQL, ASP, and AJAX

ORACLE®