Specifikace antivirového systému *AVirCheck*

soLNet, s.r.o.
info@solnet.cz

24. září 2003

Obsah

Část I

Popis produktu

1 Úvod

Následující text popisuje podrobně řešení a cenovou politiku antivirového systému AVirCheck.

2 Technická specifikace

Systém antivirového štítu AVirCheck zajišťuje automatickou kontrolu veškeré příchozí i odchozí pošty, která je zpracovávána místním poštovním serverem.

2.1 Vlastnosti

AVirCheck funguje v součinnosti se standardním poštovním systémem (např. Sendmail nebo Exim, viz 2.2). Ten spouští AVirCheck pro každou příchozí nebo odchozí zprávu a další zpracování zprávy je možné pouze po "schválení" od AVirChecku, který tímto způsobem blokuje buď zprávy s nepovolenou přílohou nebo zprávy, které obsahují virus. Zablokované zprávy jsou potom uloženy do karanténního adresáře a pošle se hlášení správci serveru a odesílateli (podle nastavení se může poslat hláška i příjemci).

Základní vlastnosti AVirChecku:

- vysoká konfigurovatelnost
- vyhledávání viru také v komprimovaných přílohách
- seznam zakázaných přípon příloh (zvyšuje účinnost systému proti novým virům, přitom ponechává možnost poslat spustitelné soubory jako komprimované přílohy)
- dopis, který obsahuje virus nebo blokovanou přílohu je stornován a je poslána varovná zpráva odesílateli dopisu i vybranému správci místní sítě
- hlášení o nedoručení dopisu s virem či blokovanou přílohou je možné zasílat i původnímu adresátovi dopisu
- kontrola na přítomnost virů může být prováděna současně několika volně šiřitelnými nebo komerčními antivirovými systémy
- systém obsahuje automatickou aktualizaci dat s popisem hledaných virů a tím umožňuje zachytit i nejnovější záškodníky

2.2 Platforma

Antivirový systém AVirCheck je určen pro servery s OS Linux. Vývoj AVirChecku probíhá na distribuci Debian GNU/Linux, je ale bezproblémově provozován i na serverech s distribucemi Red Hat Linux nebo SUSE Linux (AVirCheck se dodává jako DEB nebo RPM balík).

AVirCheck je nejčastěji provozován s velice kvalitním a bezpečným poštovním serverem Exim (`www.exim.org`), je však možná i spolupráce s dalšími nejběžnějšími poštovními servery jako je Sendmail nebo Qmail.

2.3 Použití antivirových systémů

Systém AVirCheck může spolupracovat s různými volně šiřitelnými i komerčními antivirovými systémy, z komerčních doporučujeme vysoce výkonný a velice často aktualizovaný (cca 20krát do měsíce) antivirový systém DrWeb (`www.drweb.ru`, angl. `www.sald.com`). O kvalitách antiviru DrWeb svědčí i to, že opakovaně obdržel cenu *Virus Bulletin 100 %* za antivir, který zachytí 100 % aktuálních virů. Tento antivir navíc díky OEM dohodě s distributorem DrWebu dodáváme za velice výhodnou cenu **v rámci AVirChecku**.

Kromě DrWebu umí ovšem systém pracovat i s dalšími antiviry, vyzkoušené jsou například:

- CAI InoculateIT
- KasperskyLab AVP
- Panda Antivirus
- F-Prot Antivirus
- McAfee Virus Scan 3.x
- NAI Virus Scan 4.x
- Dr. Solomon antivirus
- Sophos Sweep

V rámci AVirChecku je navíc možné násobit jistotu zachycení viru tím, že se zapojí do automatické detekce viru více antivirů.

2.4 Průtok a rychlost

Komplexnější testy rychlosti AVirCheck za účelem zjištění rychlosti ještě provedeny nebyly, ale referencí v tomto směru může být jeho bezproblémové nasazení na hostingovém serveru s několika stovkami aktivních domén.

Nasazovaný antivir DrWeb byl testován i v masívním provozu a autoři zveřejnili výsledné statistiky, kdy v průběhu 24 hodin prošlo tímto antivirem 5 miliónů zpráv s maximem cca 4 tisíce zpráv za minutu.

3 Cena

Současná cenová politika systému AVirCheck specifikuje licenci per server bez dodatečného omezení na počet domén či poštovních uživatelů. Součástí dodávaného balíku je i licencovaný antivir DrWeb.

Položka	Cena
První rok automatických aktualizací	3.000 Kč
další roky	1.500 Kč ročně

Ceny jsou uvedeny bez DPH.

Při odběru licencí na větší počet serverů je možné nabídnout množstevní slevy.

4 Způsob dodání a zkušební lhůta

AVirCheck je dodáván elektronickou poštou jako DEB nebo RPM balík, spolu s licencí nasazeného antiviru DrWeb, ssh klíči pro automatickou aktualizaci a návod na instalaci pro konkrétní poštovní systém.

Pokud to kupující požaduje, je možné dodat AVirCheck pro 7 denní testovací lhůtu bez licence antiviru DrWeb. V této lhůtě může kupující AVirCheck "vrátit" a nebude mu pak účtován žádný poplatek. V opačném případě po zaplacení zálohové faktury dostane kupující dodatečně i příslušnou licenci DrWebu.

5 Výhody proti konkurenčním řešením

Mezi hlavní výhody AVirChecku patří:

- bezkonkurenční cena serverového řešení
- vysoká konfigurovatelnost
- blokování nebezpečných přípon (nejlepší prevence proti novým virům)
- díky vysoké modulárnosti snadná možnost nasazení více antivirů
- možnost dalšího využití AVirChecku na daném serveru v dalších nástavbových produktech:
  - *WWWAVirCheck* – skenování veškerého HTTP a FTP toku
  - *FileAVirCheck* – periodické skenování souborů v určené adresářové struktuře na serveru
  - komplexní poštovní systém *soLNet mailbox* – příjem a odesílání pošty, sdílené kontakty, sdílené schránky, kompletní správa přes WWW rozhraní, neomezené množství domén, práva uživatelů, ...
  - hostingový systém *soLNet hosting server* – soLNet mailbox plus DNS, Apache, FTP, ...

6 Kontakt

V případě speciálních požadavků je samozřejmě možné upravit AVirCheck pro potřeby systému zákazníka. Pro podrobnosti nás prosím kontaktujte:

soLNet, s.r.o.
Šumavská 31
612 54 Brno
telefon: +420–549 131 233
mobil: +420–737 743 587
e-mail: info@solnet.cz
www.solnet.cz

Část II

Přílohy

1 Kompletní nabídka služeb

Námi dodávané servery mohou nabízet velice rozsáhlý výběr služeb. Konkrétní služby serveru a jejich nastavení se sjednávají vždy individuálně podle potřeb zákazníka a jeho místní sítě. Kompletní nabídku služeb tvoří:

- Transparentní připojení lokálních sítí do Internetu, realizované překladem vnitřních adres na adresy Internetu (NAT, masquerade). Klienti vnitřní sítě mohou navazovat spojení se servery na Internetu, jako kdyby byli připojeni přímo k Internetu.
- Ochrana lokálních sítí i serveru samotného proti útokům z Internetu pomocí firewallu.
- Komplexní řešení pošty pomocí poštovního serveru Exim. Umožňuje libovolný počet poštovních schránek, virtuálních adres, přeposílání mailů (i na SMS), budování vlastní černé listiny odesílatelů, archivaci veškeré příchozí a odchozí pošty.
- Výběr pošty klientskými stanicemi probíhá pomocí protokolu POP3 nebo IMAP (případně jejich bezpečnými variantami POP3S, resp. IMAPS), který podporuje naprostá většina poštovních klientů (MS Outlook, . . .).
- DNS cache (překlad jmen) pro urychlení přístupu na Internet — IP adresy přeložené z doménových jmen se uchovávají v paměti brány a zmenšuje se tím režie přístupu klientských stanic k Internetovým DNS serverům.
- HTTP a FTP proxy cache pro urychlení přístupu na Internet (program Squid) — stránky a soubory stažené z Internetu se ukládají do cache na disku brány a při opětovném přístupu ke stejnému prostředku se použijí, čímž se významně omezí objem dat přenesených z Internetu. Z logů proxy cache je každý měsíc možné vytvořit statistiky přístupů k jednotlivým stránkám a doménám.
- File server, který umožňuje využít zbylou kapacitu disků jako sdílené datové adresáře, případně umožňuje využití serveru jako přípojného bodu sdílených tiskáren.
- Antispamová ochrana vnitřní sítě — heuristická analýza obsahu zprávy a/nebo kontrola IP adresy odesílatele ve veřejné databázi spammerů.
- Antivirová ochrana vnitřní sítě — kontrola příchozí a odchozí pošty na přítomnost virů a blokování přenosu virů prostřednictvím pošty, kontrola dat stažených z Internetu přes HTTP proxy server.
- Možnost využití moderní výměny informací uvnitř firmy pomocí sdílených kontaktů, sdílených poštovních schránek a přístupu k poště přes WWW rozhraní odkudkoliv z Internetu (WebMail).
- Služba QoS (Quality of Service) — omezování šířky pásma a nastavení kvality služeb.
- Virtuální privátní síť (VPN) pro vybudování šifrovaného spojení mezi pobočkami, pomocí které budou pobočky přístupné, jako kdyby byly umístěny na lokální síti.
- Pošta pro VPN — umožňuje centrální správu několika poštovních serverů pomocí automatických replikací databáze LDAP.

- WWW server (Apache) zajišťující vystavení Vašich webových stránek a aplikací na Internetu a intranetu. Apache podporuje statické i dynamické stránky, virtuální servery, omezování přístupu, vícejazyčné stránky, šifrované spojení (HTTPS).
- DNS server — poskytuje Internetu překlad adres například při provozování více domén (virtuální servery — web, mail, ...).
- FTP server pro přenos/předávání velkých souborů v rámci Internetu (anonymní i autentizovaný přístup).
- FAX server — odesílání a příjem faxů. Možnost emulace tiskárny ve Windows.
- Databázový server — SQL server je vyžadován pro některé webové aplikace (MySQL, PostgreSQL, Interbase, Oracle, ...).
- Účtování přenesených dat umožňuje online přehled provozu na lince pro jednotlivé počítače nebo podsítě. Přes WWW rozhraní je možné zobrazovat grafy průtoků a součty za jednotlivá období.
- WWW rozhraní pro administraci domén a virtuálních WWW/mail serverů.
- WWW rozhraní pro práci s poštovní schránkou uživatele. Přístup k nové poště z vnitřní sítě i z Internetu bez nutnosti konfigurovat poštovního klienta.
- Tvorba WWW stránek a aplikací — firemních prezentací i intranetových portálů.
- Servis a správa serverů i celých sítí.