



**MEDIADIGITAL**  
NEW MEDIA SOLUTIONS



Alojamento  
Profissional  
em Servidores  
Linux



Alojamento  
Profissional  
em Servidores  
Windows



Suporte  
Profissional  
24/7/365

## Serviço SVS AntiVírus e Spam Killer Professional



## Novo Serviço SVS – AntiVírus e SPAM KILLER Profissional

A MEDIADIGITAL – new media solutions, vem por este meio informar os seus clientes de Alojamento Profissional em Servidores Windows que, no sentido de continuar a prestar um serviço de alojamento de elevada qualidade, procedeu à instalação de um novo e avançado serviço de filtragem de Vírus e SPAM em todos os seus servidores e que o disponibiliza de forma gratuita aos seus clientes dos planos Galaxy, Nemesis e Gold. Nos planos NetGo, Planet e Atlantis o serviço está disponível como opcional pelo valor de € 5,00/mês.

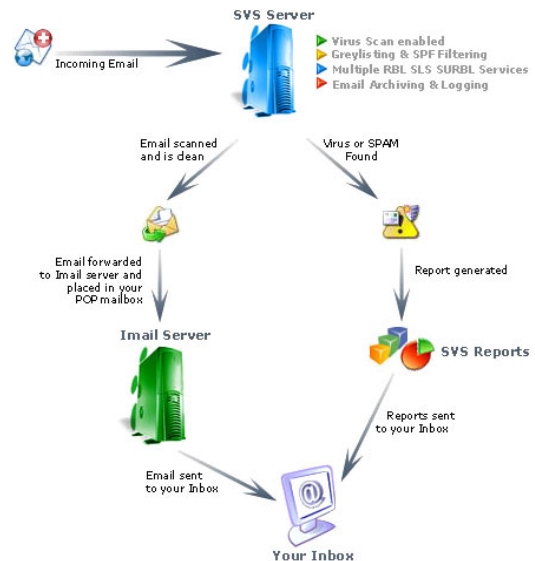
O novo serviço spam/virus está desenhado para libertar a sua caixa de correio de emails não solicitados e todo o tipo de vírus. Na MEDIADIGITAL compreendemos a importância do serviço de email e foi nesse sentido que, após algum tempo de estudo e de análise das soluções oferecidas no mercado, desenhámos uma solução que maximizará a protecção do sistema evitando perdas de emails e do seu precioso tempo "filtrando" na sua caixa de correio todo o tipo de "lixo" não solicitado que é cada vez mais hoje em dia uma infeliz realidade.

**Este serviço é uma solução completa e inclui as seguintes características:**

- Filtragem Spam Multi-camadas
- Tecnologia de Ponta na Filtragem de Spam
- Sistema totalmente redundante
- Prevenção de ataques (mailbombs, etc.)
- Filtragem de Vírus – Servidor de email secundário
- Relatórios Spam & Vírus

**Vantagens do Serviço SVS:**

- A sua implementação requer apenas uma simples alteração na configuração de DNS do domínio.
- Não é necessária qualquer formação para o cliente
- Latência não perceptível
- Um típico e-mail demora em média 1.5 segundos a processar
- Acabam-se as preocupações resultantes de que nem todos os utilizadores do domínio (caixas de correio) tenham actualizadas as soluções de vírus instaladas nos seus computadores pessoais.



O nosso sistema foi desenhado de modo a garantir a maior protecção possível e de forma redundante. A solução SVS foi desenvolvida utilizando as seguintes tecnologias:

**Xwall, Fprot e EsatInformer**

**Como funciona o Serviço?** Quando um email lhe é enviado, o servidor SVS apanha-o e analisa se o seu conteúdo e anexos constituem potenciais ameaças em termos de vírus e spam. Se um vírus ou spam é encontrado num email, o email será bloqueado e armazenado. Se o email for limpo, o email é então reenviado para o servidor IMail para distribuição. Todos os dias um relatório será compilado de todos os emails que foram, por algum motivo, bloqueados. Este relatório ser-lhe-á enviado e dar-lhe-á a possibilidade de fazer o download de qualquer email que tenha sido bloqueado.

**E se o Servidor SVS fica indisponível temporariamente?** Se, por qualquer motivo, o Servidor SVS estiver em baixo temporariamente, os emails serão automaticamente enviados para o Servidor IMail.

**E se o Servidor Imail fica indisponível temporariamente?** Se, por qualquer motivo, o Servidor Imail estiver em baixo temporariamente, os emails serão armazenados no Servidor SVS até que a entrega seja possível. Isto prevenirá qualquer perda de emails.

**Durante quanto tempo permanecem bloqueados os emails no Servidor SVS?** Os emails bloqueados permanecem armazenados no Servidor SVS e estarão disponíveis para download durante 7 dias.

Web Site: [www.mediadigital-nms.com](http://www.mediadigital-nms.com) | E-mail: [suporte@mediadigital-nms.com](mailto:suporte@mediadigital-nms.com)



## Descrição da Filtragem de SPAM do Serviço SVS

O Serviço SVS proporciona Filtragem Spam Multi-camadas. A primeira análise é efectuada no Servidor SVS utilizando a tecnologia Xwall.



As seguintes filtragens são efectuadas:

**-RBL Black lists scan:** Previne que emails de conhecidos utilizadores de spam lhe sejam enviados.

**-SURBLs scan:** SURBL diferem da maioria dos outros RBLs na medida em que são utilizados para detecções com base em hiper ligações (normalmente endereços de web sites) existentes no corpo da mensagem.

**-Heuristic scan:** A Filtragem Heuristic utiliza regras de cruzamento de características, desenvolvidas através de experiência, para identificar spam. Através de uma análise detalhada do email baseada em regras cuidadosamente desenhadas de emails entrando no sistema, a filtragem heuristic atribui um valor numérico ou uma pontuação a cada mensagem. Esta pontuação é usada para determinar o grau de probabilidade de uma mensagem ser ou não spam. Através de anos de "aprendizagem" sobre a aparência típica de mensagens que são ou não spam, o conjunto de regras padrão - e paralelamente a pontuação atribuída a essas mensagens - tornaram-se bastante fiáveis e eficientes na detecção do que é ou não spam.

**- Filtragem de Anexos Perigosos**

**- Filtragem de Conteúdo:** analisará o título e o corpo da mensagem na procura e identificação de frases tipicamente utilizadas em spam e bloqueará esses emails.

**-Filtragem Bayesian:** Este filtro aprende com o Spam que os outros filtros encontram. Uma vez suficientemente educado conseguirá encontrar SPAM por si próprio.

**- Definições Padrão:** Regras-padrão podem ser definidas no Servidor SVS de modo a que permitam que defina se quer receber ou bloquear determinados emails. Estas regras incluem a possibilidade de bloquear endereços de email e a definição de domínios/emails permitidos.

A Filtragem realizada no servidor IMAil é reduzida. Esta filtragem é definida para "apanhar" os emails enviados por spammers mas suficientemente reduzida para não bloquear todos os emails que não se classificam como spam.

Os nossos Servidores de Email são também protegidos contra *relay attacks*, o que assegura que os endereços no nosso servidor de email não serão adicionados a listas de Spam. As Restrições incluídas: autenticação SMTP, não permissão de *relaying* e outras...

### Filtragem de SPAM realizada no Servidor SVS

- » Realtime Black Lists enabled (RBL): ORDB.org, SpamHaus.org, SpamCop.net
- » SURBL service enabled
- » Heuristic (a.k.a. spamassasin) filter enabled
- » Dangerous attachments blocked (e.g.: .exe, .vbs, .com, .bat)
- » Content Filtering (body, subject checks)
- » Custom blocking of email addresses available on demand
- » Bayesian filter - Xwall learns from your blocked SPAM examples.
- » Filter out HTML and block strings
- » Custom White listing - allow messages to and/or from specified addresses to pass - Available on demand.

### Filtragem de SPAM realizada no Servidor IMAil

- » Realtime Black Lists enabled (RBL): ORDB.org, SpamHaus.org, SpamCop.net
- » SURBL service enabled
- » Dangerous attachments blocked (e.g.: .exe, .vbs, .com, .bat)

Web Site: [www.mediadigital-nms.com](http://www.mediadigital-nms.com) | E-mail: [suporte@mediadigital-nms.com](mailto:suporte@mediadigital-nms.com)



## Descrição da Filtragem de Vírus do Serviço SVS



Uma vez activado o serviço, todos os emails serão filtrados com base em todos os ataques de vírus listados e outros.

A MEDIADIGITAL elegeu a tecnologia F-Prot como a principal solução anti-vírus para os seus servidores de email. Esta solução foi desenhada para trabalhar eficientemente com o componente principal do nosso serviço de SVS, a tecnologia Xwal.

F-Prot Antivirus detecta mais de 100,000 diferentes ameaças e é diariamente actualizado. As capacidades inovadoras de detecção heurística do F-PROT's proporciona protecção contra todas as ameaças conhecidas e funciona como escudo para vírus desconhecidos ou ainda não lançados.

A gestão da protecção Anti-Vírus F-Prot, é efectuada por especialistas em tecnologia anti-vírus que trabalham a tempo inteiro na monitorização de novo surtos de vírus e na reacção aos mesmos no mais curto espaço de tempo possível. As actualizações de Assinaturas de Vírus são realizadas automaticamente no servidor duas vezes por dia, garantindo a sua paz de espírito de que está completamente seguro. Quando o relatório SVS é gerado, os emails bloqueados devido a infecção de vírus serão marcados como tal, pelo que não terá de se preocupar em fazer o download de um email infectado.

### Protecção contra os seguintes ataques de vírus:

- » Viruses within base64 encoding » Viruses without quotes around the filename
- » Viruses within binary encoding » Viruses within HTML segments
- » Viruses within quoted-printable » CR Vulnerability encoding
- » Viruses within uuencoding » Space Gap Vulnerability
- » Viruses within BinHex encoding » Blank Folding Vulnerability
- » Viruses embedded within another MIME segment » MIME Boundary Space Gap Vulnerability
- » Viruses within uuencoding within a MIME segment » Long MIME Boundary Vulnerability
- » Viruses within BinHex encoding within a MIME segment » MIME Continuation Vulnerability
- » Viruses within inline attachments » Empty MIME Boundary Vulnerability
- » Viruses embedded within an RFC822 message » Partial (Fragmented) Vulnerability
- » Viruses within a ZIP file » Attachment with a CLSID extension which may hide the real file extension.
- » Viruses sent from Pegasus » Viruses within a double ZIP file (i.e. a zip within a zip).
- » Viruses sent in a Microsoft TNEF file (winmail.dat) » Viruses within a ZIP file that has been manipulated to evade detection by some anti-virus software by changing the uncompressed size to zero within the ZIP file headers.

Web Site: [www.mediadigital-nms.com](http://www.mediadigital-nms.com) | E-mail: [suporte@mediadigital-nms.com](mailto:suporte@mediadigital-nms.com)



