

Filtre spam e vírus no servidor de email

Proteção na fonte

O melhor momento para eliminar emails suspeitos é antes de eles chegarem à sua caixa de entrada. O Amavisd-new é uma interface de código aberto para integrar filtros de spam e vírus com seu servidor de email.

POR LARKIN CUNNINGHAM

A pesar de ser possível a contaminação a partir de disquetes, CD-ROMs e mesmo por vermes e *root kits* que atacam diretamente vulnerabilidades do sistema, a probabilidade maior é de receber vírus por email.

Sem sombra de dúvida, é importante ter um antivírus atualizado no computador. Entretanto, a melhor tática é se proteger contra spam e vírus já no servidor de email, impedindo que mensagens indesejadas cheguem ao usuário, e mantendo os vírus do lado de fora de sua conta *POP3* ou *IMAP*. Filtrar no servidor reduz a carga no computador, a banda de Internet usada e diminui bastante a chance de mensagens comprometidas chegarem à sua estação de trabalho, além de reduzir o risco de um vírus passar despercebido, se houver um antivírus diferente no computador do usuário.

O *Amavisd-new* [1] é uma ferramenta de código aberto que serve como interface entre o servidor de email e outras formas de verificadores de conteúdo. Embora algumas ferramentas antivírus forneçam seus próprios mecanismos para filtrar mensagens no servidor, o *Amavisd-new* oferece vantagens em performance e garante um único ponto de configuração para gerenciar a filtragem tanto de vírus quanto de spam.

Alta performance

O *Amavisd-new* foi desenvolvido na linguagem *Perl*. Flexível e de alto desempenho, o aplicativo roda como um *daemon* que dispara um conjunto de processos (pai e filhos).

Ele se parece com um servidor SMTP, recebendo mensagens do seu servidor SMTP "real" (por exemplo, *Postfix*, *exim* ou *qmail*) e processando-as. Se estiver tudo bem, as mensagens são reenviadas e chegam de maneira transparente. Se estiverem infectadas, são rejeitadas.

O *Amavisd-new* suporta ferramentas antispam como o *SpamAssassin* [2] e uma grande variedade de antivírus comerciais ou de código aberto. O popular *ClamAV* [3] pode ser integrado de três maneiras: através do *daemon clamd* (melhor performance), o pacote *Perl Mail::ClamAV* (desempenho não muito bom) e a opção do comando *clamscan* (como uma ferramenta de prevenção no caso de o *clamd* não estar disponível). Muitos outros antivírus populares também são suportados, incluindo *F-Prot*, *Sophos*, *Grisoft AVG*, *KasperskyLab AVP*, *AntiVir*, *F-Secure*, *McAfee* e *Panda*.

No entanto, não se esqueça da licença do produto que você for usar. Obviamente, o *ClamAV* não possui nenhum custo de licença, mas outros programas terão

licenças para servidor SMTP significativamente mais caras que a versão desktop.

Você pode configurar o *Amavisd-new* para bloquear anexos com extensões perigosas, como *.exe*, *.bat* e *.vbs* (particularmente perigoso para clientes Windows® que estejam acessando o servidor). Também é possível especificar um grande intervalo de decoders ou descompactadores para examinar arquivos como *.cpio*, *.rpm*, *.deb*, *.zoo*, *.tar*, *.gz* e *.bz2*.

O *Amavisd-new* teoricamente suporta qualquer servidor SMTP, mas trabalha melhor com os mais famosos. Por exemplo, *Sendmail*, *exim* e *qmail*. Trabalha melhor ainda com o *Postfix* [4], no qual pode "reinjetar" mensagens no servidor depois da filtragem de conteúdo.

Requisitos de instalação

Para instalar o *Amavisd-new*, você precisa de um interpretador *Perl* instalado e funcionando. Recomenda-se a versão 5.8.2 ou superior. Apesar de instalações antigas funcionarem, as versões posteriores rodam melhor. Também é preciso instalar diversos pacotes de extensão do *Perl* (Tabela 1). Não se esqueça de atualizar para a última versão quaisquer pacotes que você já tenha instalados.

Obviamente, para que a filtragem de spam seja eficiente, a versão mais atu-



al do pacote *Mail::SpamAssassin* deve ser instalada. Spammers tentam estar sempre um passo à frente do SpamAssassin, por isso é necessário atualizá-lo assim que uma nova versão se tornar disponível.

Também é bom instalar alguns programas auxiliares para permitir a varredura do maior número de anexos em arquivos compactados. Entre esses programas adicionais temos *gzip*, *bzip2*, *arc*, *lha*, *rar*, *zoo*, *pax*, *cpio*, *freeze*, *ripole*, *cabextract* e muitos outros. Visite o site do Amavisd-new [1] para mais informações. Depois de configurar todos os programas auxiliares, a instalação é relativamente simples. Como o programa usa o interpretador Perl, não requer nenhuma compilação.

Amavisd-new com SQL

Há diversas maneiras de configurar o Amavisd-new. É possível definir a configuração usando o arquivo *amavisd.conf*, arquivos de listas, arquivos *hash*, expressões regulares e buscas *LDAP* ou *SQL*.

A solução SQL fornece a melhor oportunidade para construir um *front-end* de configuração usando uma linguagem

de scripts como o *PHP*. Você pode usar qualquer banco de dados que siga o padrão SQL e que seja compatível com as bibliotecas Perl DBD/DBI. O *SQL DDL* (Data Definition Language) é fornecido no arquivo *README.sql* para criar tabelas, índices e dados de exemplo.

Na documentação do Amavisd-new, há recomendações específicas para *MySQL*, *PostgreSQL* e *SQLite*. Muitos outros bancos de dados também podem ser empregados, incluindo *Oracle* e *DB2*. Note que muitas das tabelas possuem chaves primárias seqüenciais e seriais. Dessa forma, para Oracle, você vai precisar de diversas seqüências e gatilhos (*triggers*), além das tabelas.

Você deve especificar dois DSNs (*Data Source Names*). Um DSN se refere às buscas (leia em **Políticas**, a seguir) e o outro ao armazenamento (*logging*). Você pode otimizar a performance usando um banco de dados que seja rápido no acesso somente leitura (para fazer buscas) e um banco de dados rápido na gravação (para o armazenamento). O Amavisd-new também permite especificar múltiplos DSNs para habilitar o *failover* (mudança de máquinas no caso de falhas).

Políticas

Uma política de firewall é um conjunto de instruções especificando o que o firewall deve fazer com certos tipos de tráfego. Por exemplo, uma política pode especificar se bloqueia tráfego de certa porta ou se redireciona o tráfego de uma porta para outra.

Uma política do Amavisd-new é similar. Cada uma diz ao programa para, por exemplo, ignorar a verificação de vírus e spam, ser mais duro ou permissivo, marcar o assunto do email com um palavra-chave (por exemplo, "Spam?") ou redirecionar todo spam para uma conta específica.

Cada domínio ou usuário de email pode ter sua própria política. Você pode especificar uma política para cobrir todas as contas de email dentro de um domínio; também pode delimitar políticas adicionais por cada conta individual de email dentro desse mesmo domínio. Por exemplo, é possível criar uma política padrão para todos os usuários de um certo domínio, mas talvez a conta de "Fulano" esteja sendo inundada de spam. Uma política individual para essa conta

Tabela 1: Pacotes Perl necessários

Archive::Tar
Archive::Zip
Compress::Zlib
Convert::TNEF
Convert::UUlib
MIME::Base64
MIME::Parser
Mail::Internet
Net::Server
Net::SMTP
Digest::MD5
IO::Stringy
Time::HiRes
Unix::Syslog
BerkeleyDB

Tabela 2: Principais opções da tabela de políticas

virus_lover	Aceita email mesmo se contaminado por vírus
spam_lover	Aceita mesmo se identificado como spam
<i>OBS: As opções do tipo <code>_lover</code> não cancelam o checagem, apenas ignoram seus resultados.</i>	
bypass_virus_checks	Não verifica se o email está infectado por vírus
bypass_spam_checks	Não procura por spam e não adiciona o cabeçalho X-Spam
spam_modifies_subj	Acrescenta uma marca de texto (<i>tag</i>) ao início do assunto, caso seja identificado como spam
virus_quarantine_to	Conta de email para enviar mensagens infectadas
spam_quarantine_to	Conta de email para enviar mensagens identificadas como spam
spam_tag_level	Pontuação do SpamAssassin acima da qual mensagens ganham um cabeçalho X-Spam
spam_tag2_level	Pontuação do SpamAssassin acima da qual mensagens ganham uma marca no assunto
spam_kill_level	Pontuação do SpamAssassin acima da qual uma "ação" precisa ser tomada, determinada pela variável <code>\$final_spam_destiny</code> no arquivo de configuração (o default é descartar o email, isto é, mandá-lo para um "buraco negro").
spam_subject_tag	Texto para ser usado na tag de spam (ver spam_modifies_subj)
spam_subject_tag2	Texto para ser usado na tag de spam com pontuação alta

Logs e a lei

Um assunto quente para todos os provedores de Internet do mundo no momento é a possibilidade de que seja obrigatório o arquivamento de emails por até três anos, como uma resposta de alguns governos à ameaça terrorista.

Está sendo cogitada, inclusive, a possibilidade de que agências policiais tenham acesso a essas informações para monitorar atividades ilegais – em adição aos registros de chamadas telefônicas e mensagens SMS. Enquanto o armazenamento do conteúdo dos emails inevitavelmente traria um peso enorme para os provedores, o arquivamento dos logs do *Amavisd-new* poderia cobrir muitos dos possíveis futuros requerimentos (esse é um tema que está sendo bastante debatido na Europa e nos EUA).

pode ter uma tolerância menor. A **tabela 2** detalha algumas das opções.

Uma tabela de usuários permite associar políticas a domínios específicos ou contas individuais de email. O campo email determina se várias ou apenas uma conta serão afetadas pela política. Por exemplo, “@domain.com” se refere a todas as contas no domínio domain.com. Já “fulano@domain.com” se refere a um único endereço. Se tanto “@domain.com” e “fulano@domain.com” estiverem na tabela de usuários, a prioridade é dada para o endereço individual.

Lista negra e “lista branca”

Quando emails importantes são repetidamente bloqueados por estar sendo identificados como spam, você pode garantir que o remetente é uma exceção

na checagem de spam adicionando-o à “lista branca”. Inversamente, se continuar recebendo spam de alguém que você tem certeza se tratar de um spammer, pode adicionar esse endereço à lista negra.

Essas listas funcionam através da referência cruzada entre a tabela `mailaddr` (endereços de email), a tabela de usuários e a `wblist` (listas negra e branca). Emails listados na lista negra e branca são adicionados à tabela `mailaddr` com um identificador único. As linhas na tabela `wblist` especificam endereços de email e usuários aos quais a regra se aplica.

Registro de incidentes

Um dos novos recursos do *Amavisd-new* é a habilidade de registrar toda atividade envolvendo correio eletrônico. Os logs são abrangentes e incluem informações como remetentes, destinatários, horas, datas, assuntos e pontuação de spam ou vírus.

Esse registro ajuda a reunir dados para fazer estatísticas sobre o nível de mensagens limpas, com spam ou vírus. É possível classificar os dados por usuário, facultando ao administrador verificar onde os recursos de filtragem são mais necessários. Um provedor de Internet poderia usar esses dados para o cálculo da tarifa cobrada dos assinantes, levando em conta a banda usada, o tempo de processamento, o número de mensagens processadas ou o número de spam e vírus processados.

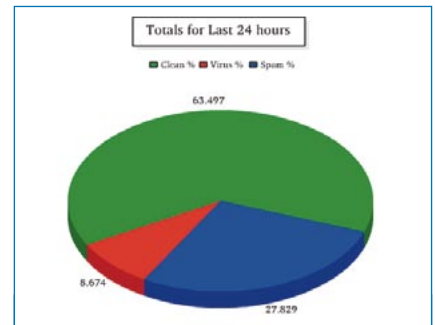


Figura 1: O *Amavisd-new* fornece dados detalhados que permitem a criação de gráficos.

Conclusão

Para quem está considerando a construção de um sistema robusto e escalonável de combate a spam e vírus, a combinação Postfix/*Amavisd-new* pode ser uma boa pedida. Hoje, fornecer filtros contra vírus e spam a seus clientes é, praticamente, uma obrigação dos provedores de acesso à Internet, mesmo que seja um serviço cobrado à parte.

Níveis crescentes de spam e vírus, além do número crescente de clientes, estão sobrecarregando a infra-estrutura de vários provedores. Essa combinação pode usar MySQL, PostgreSQL ou Oracle para o banco de dados – é possível, inclusive, empregar um banco de dados central, acessado por diversos servidores Postfix/*Amavisd-new*. Como se não bastasse, bancos de dados redundantes permitiriam maior tolerância a falhas. Usando algumas técnicas de failover, incluindo a configuração de registros DNS, é possível construir uma infra-estrutura escalonável, 100% tolerante a falhas e com carga balanceada.

Administração e números de maneira fácil

Usar um banco de dados ao invés de arquivos de configuração permite uma fácil administração. Essa opção também permite a atualização dinâmica de dados de configuração sem a necessidade de reiniciar os daemons do *Amavisd-new*. O mesmo vale se você optar por configurar seus usuários e domínios do *Postfix* em um banco de dados SQL.

Fazer consultas SQL é uma maneira útil de reunir estatísticas sobre spam e vírus. Isso pode ser feito via *phpMyAdmin*, por exemplo, se o MySQL for o banco de dados escolhido.

Um provedor com um grande número de clientes poderia desenvolver uma interface que permita aos usuários configurar suas próprias políticas contra spam e vírus. Isso poderia mostrar também aos clientes as estatísticas de emails limpos, infectados e de spam. Esse tipo de estatística pode ajudar na educação de muitos usuários de email. A **figura 1** mostra um exemplo de um gráfico que pode ser facilmente gerado para clientes. O exemplo foi feito com *ColdFusion MX 7*, mas é possível usar *PHP* em conjunto com o *jpGraph*.

INFORMAÇÕES

- [1] *Amavisd-new*: <http://www.ijs.si/software/amavisd/>
- [2] SpamAssassin: <http://spamassassin.apache.org>
- [3] Clam Antivirus: <http://www.clamav.net>
- [4] Servidor SMTP Postfix: <http://www.postfix.org>