Resultados do uso dos protocolos SPF, Greylisting e DK

Danton Nunes, InterNexo Ltda.
danton.nunes@inexo.com.br

Rodrigo Botter, Telar Engenharia e Comércio
rodrigo.botter@telar.com.br

Estudos de caso:

1. e−mail corporativo, com sendmail + milters

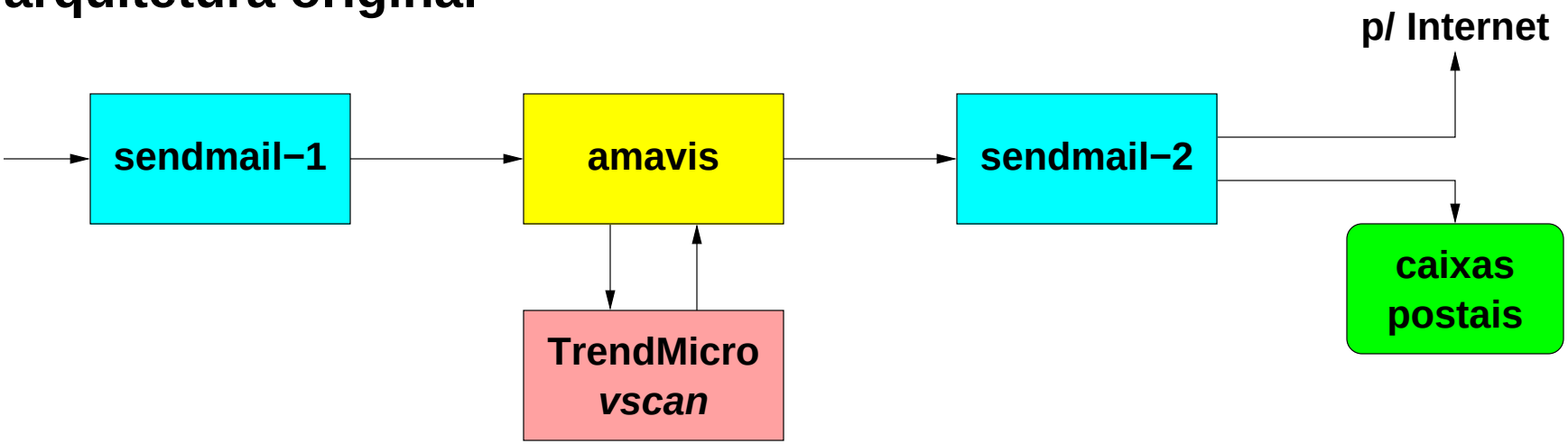
2. domínios virtuais, com qmail + patches

Tópicos

» arquitetura, instalação e políticas
» afinação de parâmetros
» comparativo antes−depois
» conclusões

1. e−mail corporativo, com sendmail + milters

arquitetura original

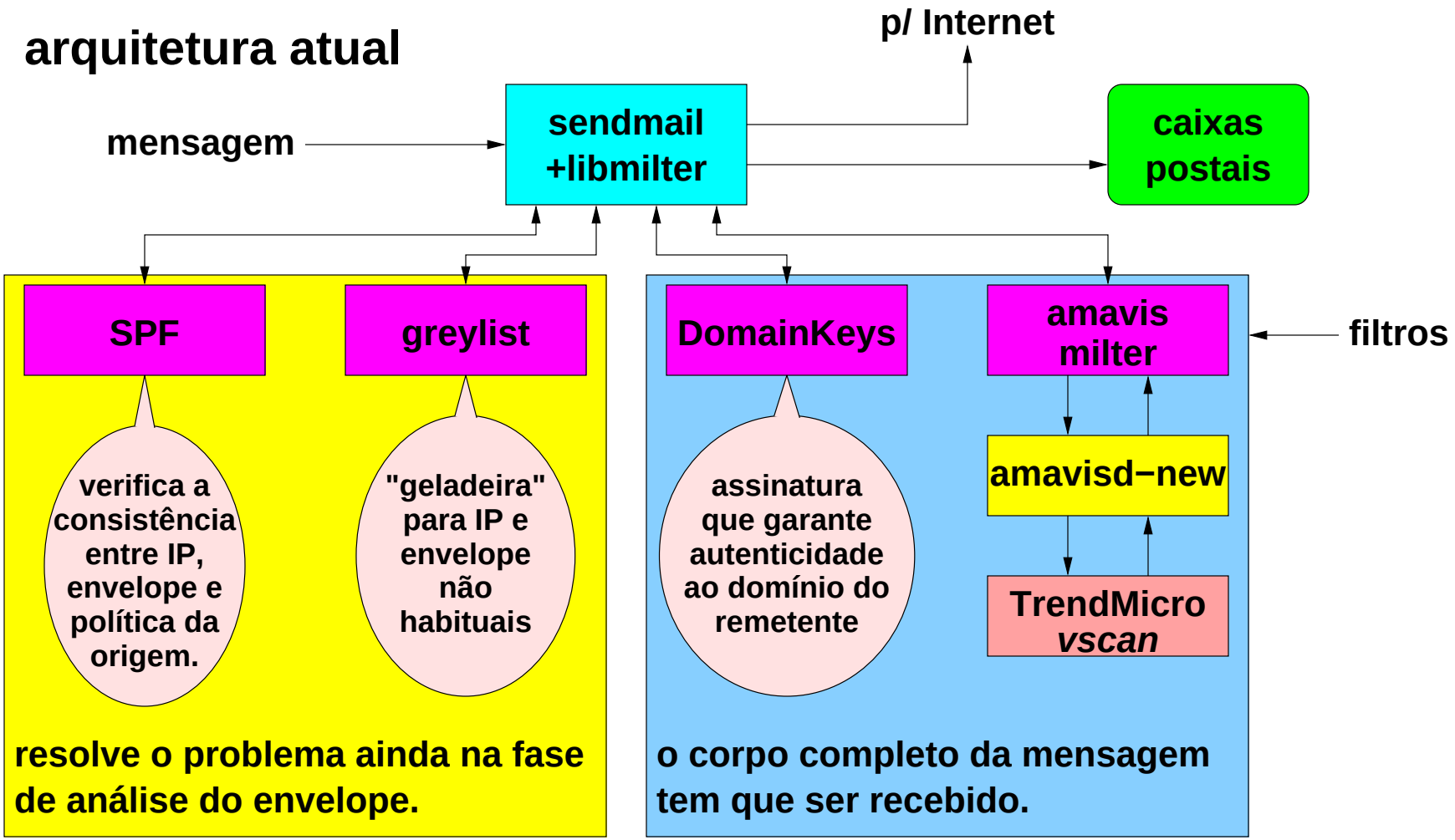


problemas

» sobrecarga de trabalho no servidor para testar vírus
» desperdício de banda
» entupimento de logs e quarentena
» entupimento de caixas postais com SPAM
» perda de tempo do administrador e dos usuários

1. e−mail corporativo, com sendmail + milters

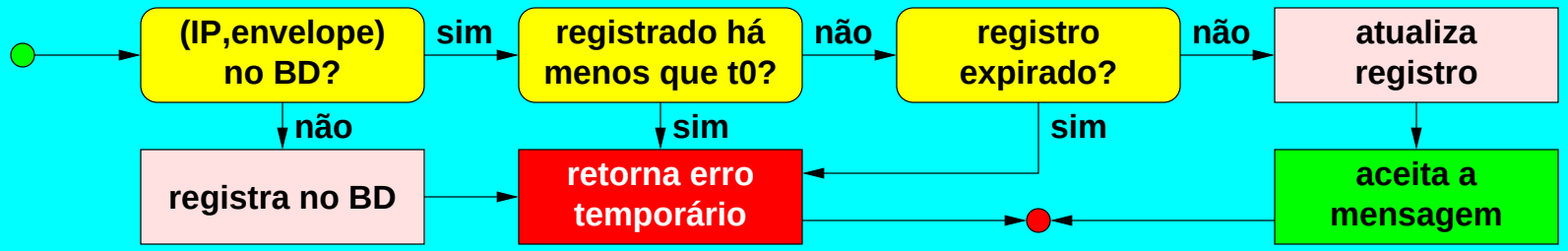
arquitetura atual



o que faz cada filtro

SPF verifica se o endereço IP do remetente pode enviar e−mail em nome do domínio, em função de política publicada pelo dono do domínio via DNS.
http://spf.pobox.com/

GL greylisting ou "geladeira"



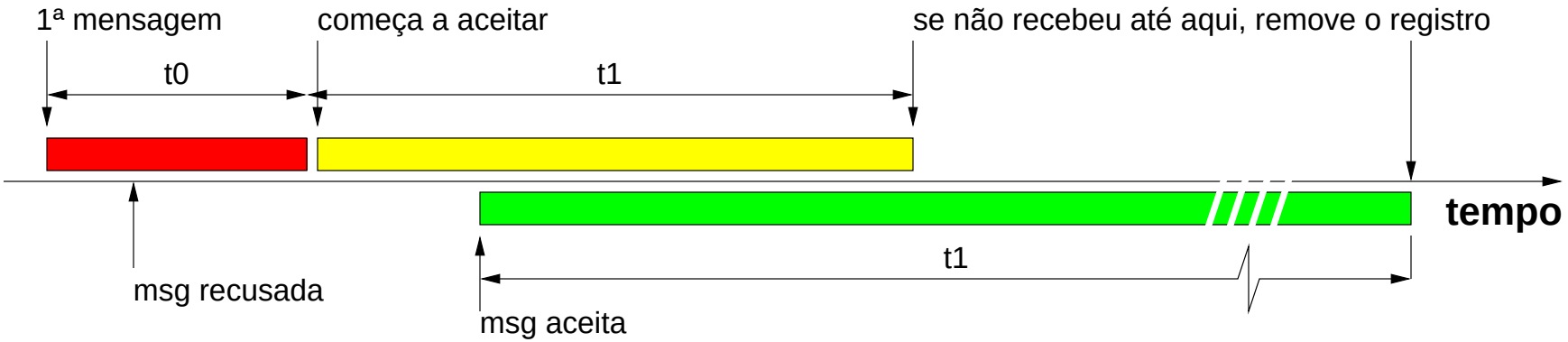
a idéia é barrar mensagens que não venham de MTAs de verdade, p.ex. spam−zombies e vetores de vírus.

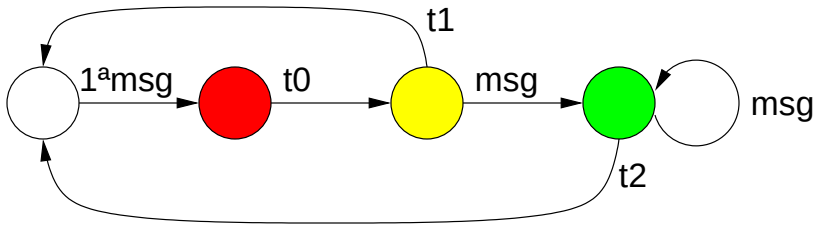
DK DomainKeys: assina mensagens que saem e verifica mensagens que chegam, validando o domínio do remetente que figura no cabeçalho por meio de chave pública distribuida por DNS. Somente marcação.
http://antispam.yahoo.com/domainkeys

afinação da geladeira

O GL tem parâmetros arbitrários de tempo cuja escolha pode ser impactante no funcionamento do sistema de correio eletrônico.

» tempo entre inserção no BD e começar a aceitar mensagens (t0)
» tempo de expiração de registro no BD (t1)
» tempo de expiração de registro no BD após ter aceito uma mensagem (t2)





afinação da geladeira

» o desempenho do bloqueio não é muito afetado por t0, mas a demora na entrega de mensagens válidas é, porisso é bom que esse tempo seja curto.

» se t1 for muito longo estaremos dando uma "segunda chance" para o spammer, se for muito curto, pode não ser suficiente para que mensagens válidas consigam entrar.

» t2 deve ser maior que o intervalo médio entre mensagens normalmente recebidas para evitar que mensagens "boas" voltem sem necessidade à geladeira, mas não muito maior, para evitar que o BD cresça demais.

valores que usamos atualmente (experimentais):

t0 = 5 minutos
t1 = 8h20’ (500 minutos)
t2 = 10 dias

é necessário um estudo mais cuidadoso para se obter critérios racionais.

alguns resultados práticos

médias diárias	antes(%)	depois(%)
conexões de SMTP (total)	2115 (100)	2517 (100)
mensagens enviadas para a Internet	220 (10.4)	164 (6.5)
mensagens bloqueadas no SMTP por qq. motivo	1026 (48.5)	1812 (72.0)
mensagens processadas pelo anti−vírus (amavis)	1089 (51.5)	240 (9.5)
mensagens carregando vírus bloqueadas	65 (3.1)	25 (1.0)
mensagens com bloqueadas por SPF fail		65 (2.5)
mensagens identificadas com SPF softfail		10 (0.4)
mensagens identificadas sem SPF		154 (6.1)
mensagens com SPF pass		61 (2.4)
mensagens com DK incorreto		10 (0.4)
conexões retidas na "geladeira"		551 (21.8)

Nota: o sendmail rejeita naturalmente ’mail from’ com domínio inválido

É notável a redução do número de mensagens que chegam ao estágio mais pesado do processamento (anti−vírus), de 51.5% para 9.5%!

A maioria dos vetores de vírus foram barrados por SPF (por terem envelope falso) e por GL (por não sairem de um MTA com fila).

2. domínios virtuais, com qmail + patches

» servidor pequeno (50 domínios, 300 usuários)
» qmail com remendos:
  » verificação de destinatário
  » autenticação de SMTP/submission

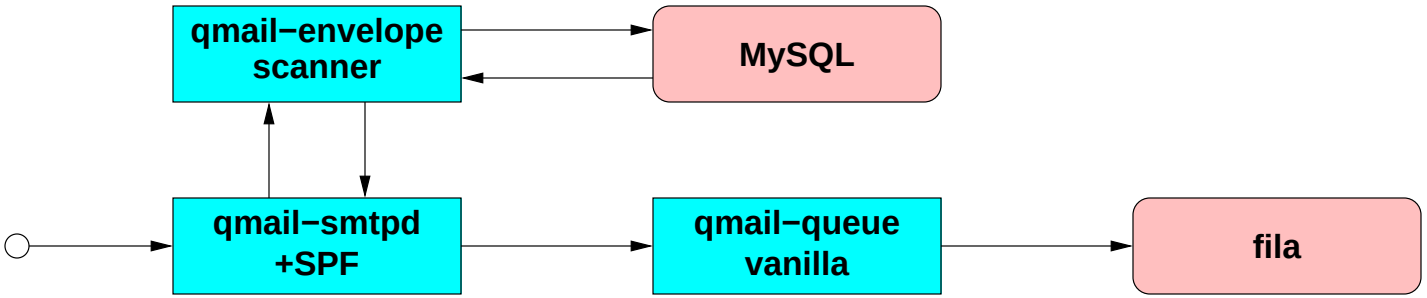
Antes

  » listas negras baseadas em IP e reverso

Depois

  » SPF incorporado ao qmail−smtpd
  » greylisting como um processo separado
  » sem verificação de conteúdo

eterna fonte de dor de cabeça:
» listas desatualizadas
» falsos positivos
» grande mobilidade dos spammers, especial−mente com zombies.



2. domínios virtuais, com qmail + patches

Regras

» (quase) todos os domínios hospedados publicam registros SPF

» os usuários transmitem e−mail somente por SMTP autenticado pelas portas 25/tcp, 465/tcp (sob SSL) e 587/tcp.

» autenticação dispensa do greylisting, enviando imediatamente.

Observações

» apesar de não usarmos qualquer filtro de conteúdo, a quantidade de spam e de vetores de vírus é muito pequena, de fato menor do que quando a defesa era baseada em listas negras.

» o remendo no qmail−smtpd que rejeita mensagens para destinatá−rios inexistentes protege o sistema de toneladas de ’bounces’, poupando banda e espaço em disco.

Algumas conclusões e observações

» quanto a SPF

- » apesar de relativamente poucos domínios publicarem registros SPF, o mecanismo funciona, já que grandes provedores de serviços aderiram.
- » é particularmente efetivo contra spam−zombies e propagadores de vírus.
- » muito fácil de configurar e manter. não requer prática ou habilidade.
- » é bom publicar registros SPF para evitar que mensagens falsas sejam enviadas em nosso nome.

» quanto a greylisting

- » é um tanto complicado por ter que armazenar estados, mas vale a pena.
- » longe de ser infalível, pois spammers muito teimosos (que repetem a transmissão de seu lixo) acabam passando.
- » falta uma certa dose de "ciência" para o ajuste ótimo de tempos.
- » nossa experiência mostra que o tempo de rejeição pode ser pequeno, praticamente nulo, sem afetar a capacidade de rejeição de lixo.
- » as pessoas precisam se acostumar com a idéia de que e−mail não é instantâneo.
- » deve ser combinado com SPF e outros métodos de validação.

Algumas conclusões e observações

» quanto a DK

» pouco difundido, mas é relativamente simples, e não requer "babysitting".

» como a assinatura é do domínio e não do indivíduo remetente, não há necessidade de senhas.

» encontramos algumas mensagens com DK inválido. pelo menos duas delas eram simulacros de mensagens provenientes do Yahoo, em que provavelmente o spammer recortou e colou cabeçalhos sem se preocupar com que se tratavam. claro que a assinatura não batia!

» ainda é cedo para bloquear mensagens com base no DK.

» listas negras?

» se tornam desnecessárias com estas novas tecnologias.

» finalmente

» temos técnicas de combate ao spam (SPF e DK) que se baseiam em informações prestadas pelo dono do domínio do remetente presumido.

» não demandam processamento pesado como análise de conteúdo.

TEM TUDO PARA DAR CERTO!