SPFBL aplicação P2P para prevenção de SPAM

https://github.com/leonamp/SPFBL

Leandro Carlos Rodrigues
SPFBL.net – Founder, Developer

Gian Eboli
SPFBL Specialist - MTA Administrator

SPFBL - O que é basicamente

- Serviço TCP que processa SPF.
- Contorna alguns erros de SPF.
- Possibilita denuncias de SPAM.
- Rejeição SMTP por bloqueios manuais.
- Troca informação via P2P.
- Feedback para enviadores.

SPF formalizado pela RFC 7208

- O SPF é a definição de quais IPs podem enviar e-mails de um domínio.
- Essa definição é feita por um registro TXT na zona DNS do domínio.
- Se o IP de origem estiver mencionado neste registro TXT, então o remetente é válido.

Problemas comuns do SPF

- Alguns erros de sintaxe podem interromper a entrega de e-mails.
- Multiplos registros podem ser feitos por engano, fazendo com que o SPF considere apenas um e despreze os demais.
- Em alguns casos especiais, o registro SPF considera válidos todos os IPs existentes.

Problemas comuns do SPF

- O máximo de consultas DNS do SPF é dez.
- Se o limite for ultrapassado, a mensagem é rejeitada.
- O uso excessivo do mecanismo include aumenta a probabilidade de ultrapassar este limite.
- O responsável de cada domínio pode se ater ao seu limite individual mas não levar em conta o limite total.

Flexibilização do SPF

- Para estimular o uso do SPF é necessário fazer algumas mudanças que resolvam os problemas apontados.
- O objetivo é tornar o SPF respeitado e amplamente utilizado.
- O SPFBL foi implementado com esta ideia.

Flexibilização do SPF

- Dedução de mecanismos ip4 e ip6.
- Profissionais podem errar a sintaxe deste mecanismo, colocando como exemplo ipv4 ou ipv6.
- Ou então separam o mecanismo de seu valor.
- Se o registro tiver um IP ou um CIDR, deduz-se que o mecanismo seja ip4 ou ip6.

Flexibilização do SPF

- Merge de multiplos registros SPF como se fossem apenas um registro.
- O mecanismo all será sempre o último encontrado.
- Mecanismos permissivos demais passam a ser ignorados, como é o caso dos blocos contendo IPs reservados ou o caso do +all.

Flexibilização do SPF

- O SPFBL não tem limite de consultas DNS pois trabalha com cache local.
- Os includes visitados são marcados e ignorados na recorrência.
- O limite no SPFBL é dez includes consecutivos.
- Erros por limite de consultas DNS são extintos no SPFBL.

Domínios sem SPF

- O best-guess é o registro SPF padrão que maximiza a probabilidade de validar um remetente sem abrir demais a segurança.
- Sempre que o domínio não tiver registro SPF, será considerado o best-guess.

```
v=spf1 a/24 mx/24 ptr ?all
```

Método de consulta

- A consulta SPFBL é composta por: IP, remetente, HELO e destinatário.
- Com posse dos três primeiros parâmetros, é possível processar o SPF flexibilizado.
- É possível realizar filtros especificos para destinatários.
- O SPFBL diz ao MTA o que deve ser feito com a mensagem, por lógica própria ou determinada pelos usuários.

Sistema de reputação

- O sistema de reputação do SPFBL é composto pela distribuição binomial da quantidade total de e-mails legítmos (HAM) e da quantidade total de SPAM enviados no mesmo período de tempo cada cada identificador.

$$D = (HAM, SPAM)$$

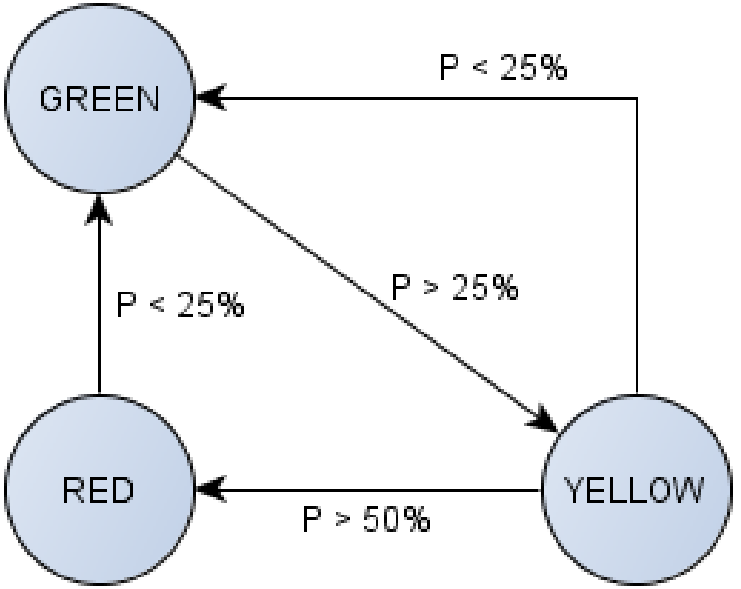
Sistema de reputação

- Cada consulta SPFBL incrementa o valor de HAM.
- Cada denuncia decrementa o valor de HAM e incrementa o valor de SPAM.
- A proporção de SPAM será a razão de SPAM pela soma de HAM e SPAM.

$$P = SPAM / (HAM + SPAM)$$

Sistema de reputação

- A reputação de remetentes é dividida em três cores: verde, amarela e vermelha.



Mecanismo de denúncia

- Cada mensagem acompanha uma URL com o ticket da consulta.
- Este ticket é colocado como cabeçalho da mensagem.
- O destinatário pode acessar esta URL para formalizar a denúncia.

```
Received-SPFBL: PASS http://matrix.spfbl.net/Y6g_GzIGITHC5Q...
```

Mecanismo de bloqueio

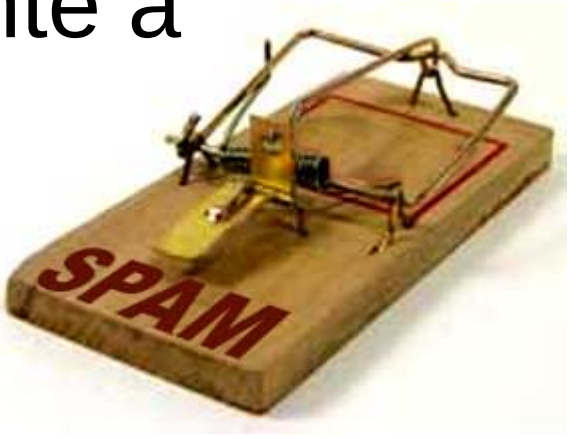
- É possível realizar diversos tipos de bloqueios.
- Toda vez que um remetente bloqueado envia uma mensagem, a mensagem é automaticamente denunciada e rejeitada.

Mecanismo de liberação

- Um liberação só será considerada pelo SPFBL de houver a validação.
- Se o remetente for liberado, o SPFBL manda o MTA aceitar imediatamente a mensagem e ignora qualquer outro processo.

Mecanismo de spamtrap

- Se um destinatário estiver registrado como spamtrap, o SPFBL realiza a denuncia automáticamente e manda o MTA descartar silenciosamente a mensagem.



Mecanismo de marcação

- Sempre que o SPFBL receber uma consulta e esta não resultar em bloqueio, liberação ou spamtrap, será verificada a reputação do remetente.
- Caso a reputação esteja RED, a mensagem é marcada como SPAM e redirecionada para a pasta Junk do destinatário

Mecanismo de atraso

- Caso a reputação esteja YELLOW, a mensagem é atrasada por greylisting.
- O greylisting também é acionado por anti-flood.

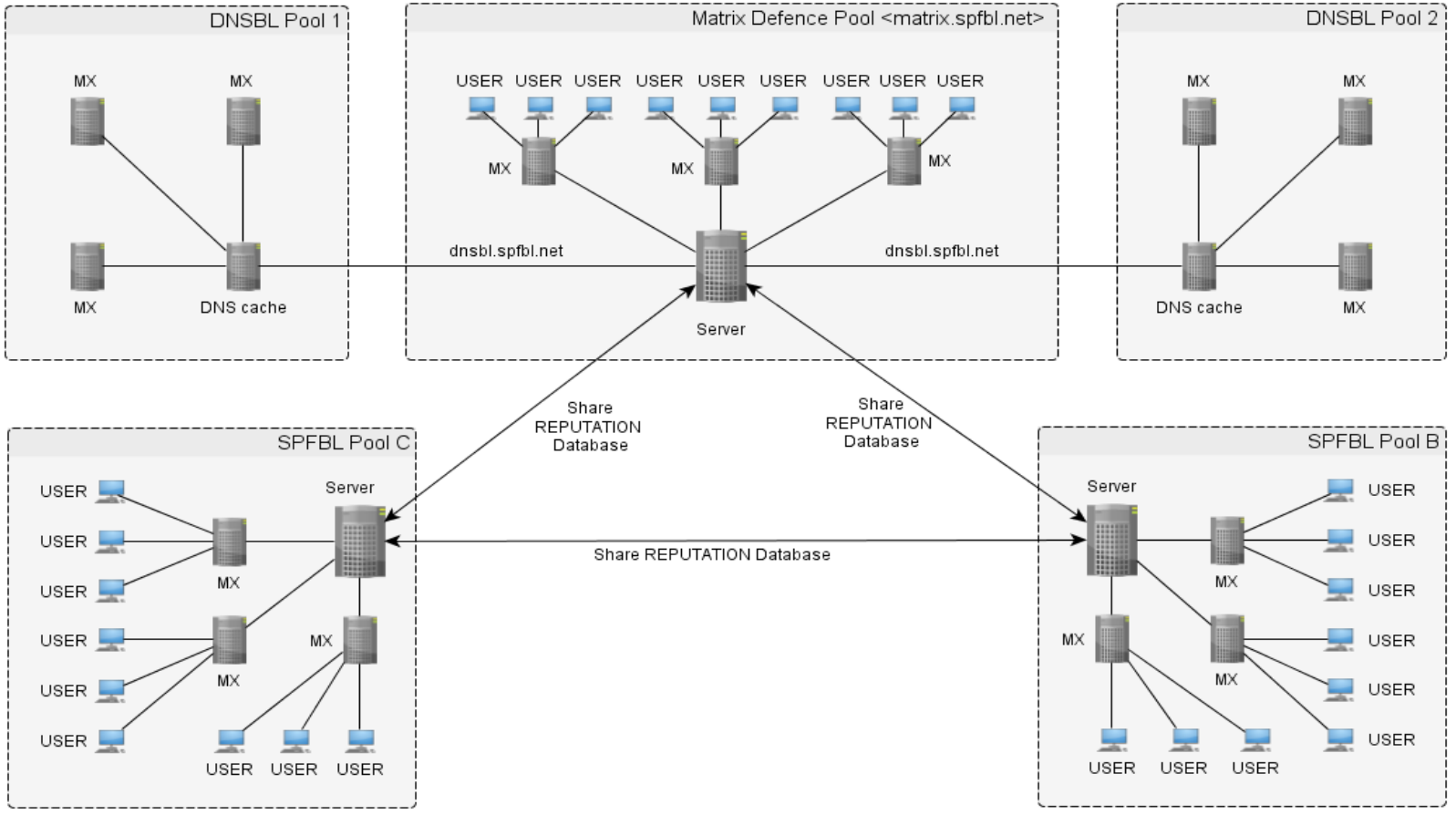
DNSBL paralelo

- O SPFBL pode ser configurado para abrir um serviço DNSBL paralelo para publicar lista de IPs bloqueados ou com reputação ruim.

Rede P2P de reputação

- O SPFBL pode ser organizado como uma rede, onde as distribuições binomiais são somadas às respectivas distribuições do seu par.
- Se o destinatário for denunciado em um provedor, essa denuncia será considerada por todos os provedores pares.

Rede P2P de reputação




```
.smtp4.fuscapreto.com.br 0 114

84.200.90.95 0 114

89.36.221.55 18 345

.host17.melhor-desconto.com 0 15

.melhor-desconto.com 0 1023

212.129.63.99 0 15

.mm25-143.viptop.com.br 0 459

131.100.25.143 0 459

.mdzz10.negociobom.site 2 45

45.58.119.12 2 45

.vennus.com.br 0 432

.mercadoprecos.com.br 1 1023

40.114.80.125 0 0

.spcr-1.arsmkt.com.br 0 0

186.195.241.219 0 102
```

Sistema de feedback

- Toda informação de feedback no SPFBL é passada pela camada SMTP.
- Isso garante que o administrador do MTA de origem obtenha as informações sobre a sua reputação sem precisar de cadastro prévio.
- Caso o MTA de origem obtenha um rejeição desta, houve denúncia na rede SPFBL.

```
5.7.1 SPFBL <message>
```

Esclarecimento de dúvidas

Façam suas perguntas

Links sobre o SPFBL

Projeto: https://github.com/leonamp/SPFBL

Site: http://spfbl.net/

Dúvidas: leandro@spfbl.net

Forum: https://groups.google.com/forum/#!forum/spfbl