

# Sistema de feedback do SPFBL



<https://github.com/leonamp/SPFBL>

<http://spfbl.net/feedback>

**Leandro Carlos Rodrigues**

FEI - Bacharel em Ciência da Computação

SPFBL.net – fundador e desenvolvedor

# SPFBFL - O que é basicamente



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

# SPFBL explicado em detalhes



- Foi explicado em detalhes da GTER 42.
- A palestra pode ser assistida aqui:

<https://youtu.be/7OAL9uIMEy4>

# Problemas levantados

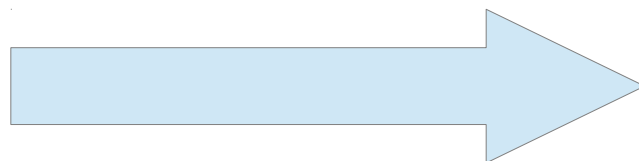


1. Como cerca de 5/6 de todo volume de e-mail é considerado SPAM, o serviço de recepção precisa de 6 vezes mais poder computacional que seria necessário se não houvesse SPAM algum.
2. O serviços de envio tem muita dificuldade em identificar quais de seus clientes estão cometendo abusos, fazendo com que seu IP seja listado em RBLs muito antes que ele possa tomar as providências necessárias.

# Detalhamento do problema 1



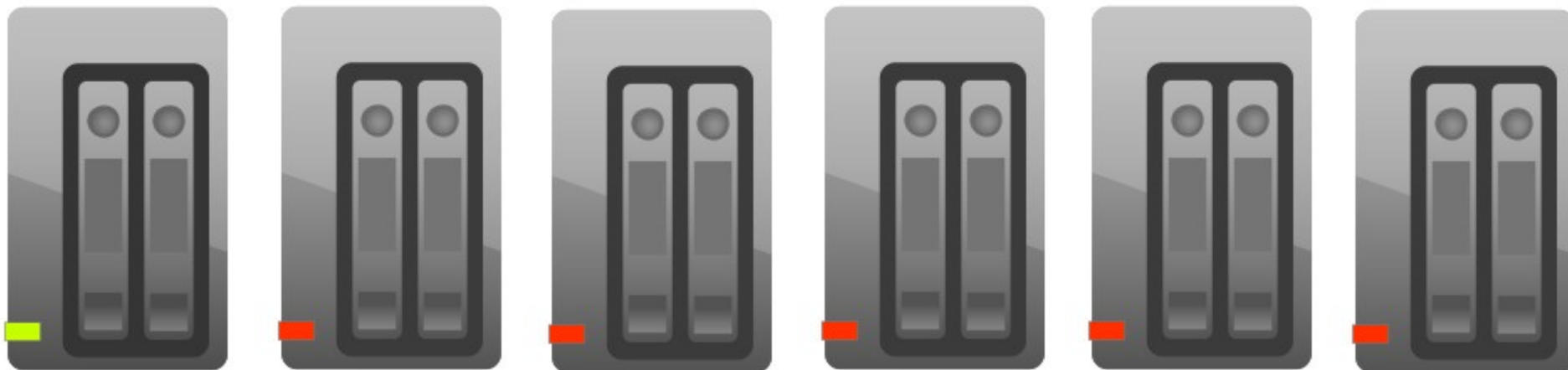
- Consideremos que 1 Unidade Recepção (UR) equivale a todos os recursos necessários para atender somente a recepção de e-mail desejável de todos os usuários.



# Detalhamento do problema 1



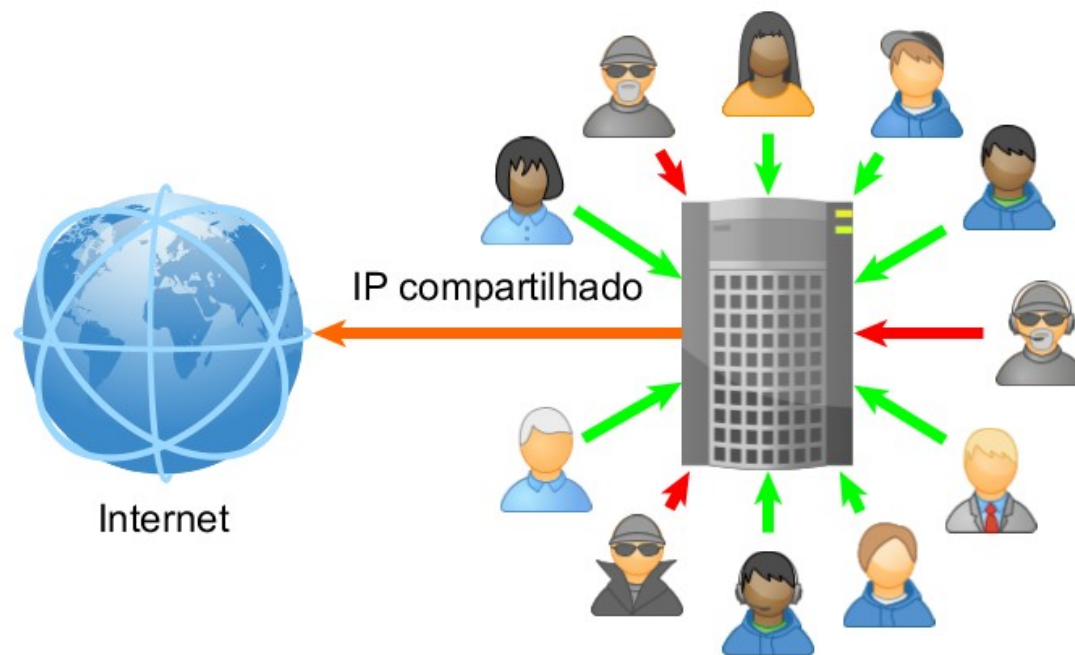
- Como 5/6 do fluxo é considerado indesejável, o serviço de recepção deverá manter 6 URs para atender plenamente todos os seus usuários.



# Detalhamento do problema 2



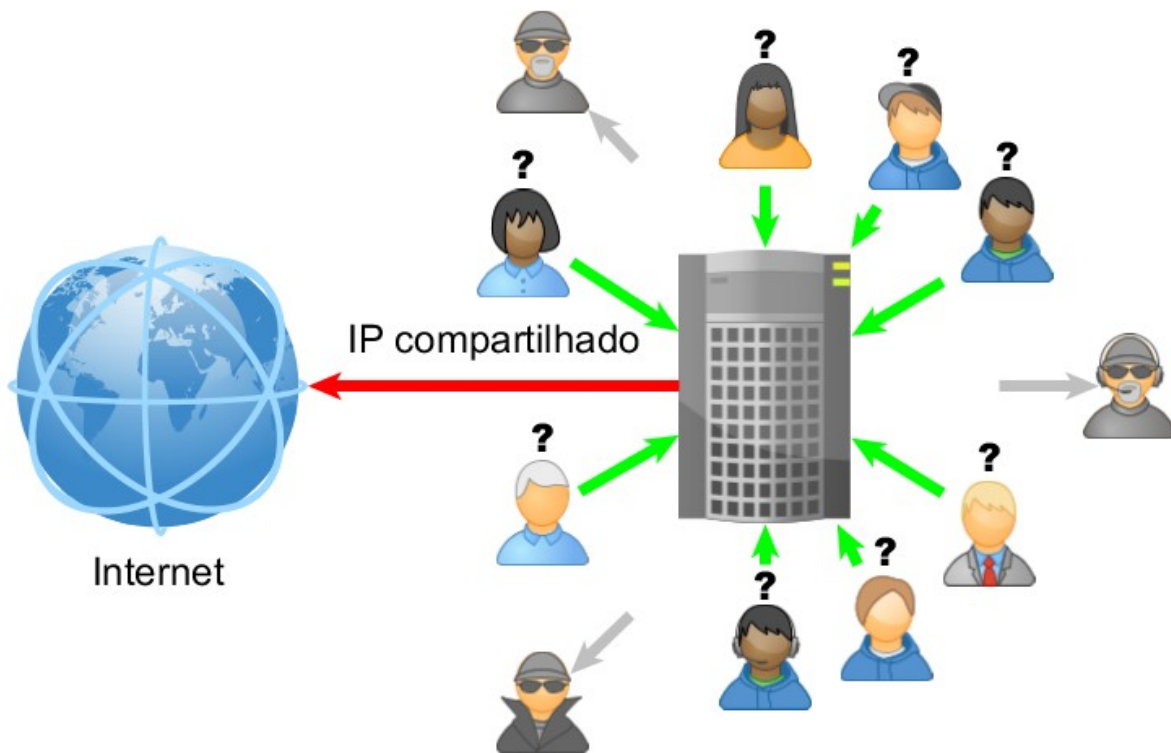
- O serviço de envio é frequentemente contratado por pessoas novas.
- É difícil saber as reais intenções destas pessoas a priori.



# Detalhamento do problema 2



- Os usuários mal intencionados se aproveitam da boa reputação do IP compartilhado.
- Os usuários bem intencionados são prejudicados com a listagem do IP compartilhado.





# Intersecção de objetivos



1. O serviço de recepção deseja ter uma redução do fluxo indesejado para conseguir aplicar uma redução de custo a seus usuários ou então conseguir aumentar a quantidade de usuários sem precisar investir em novas URs.
2. O serviço de envio quer ser capaz de identificar com rapidez os usuários mal intencionados para conseguir cortar o fluxo deles e evitar assim que seus usuários bem intencionados sejam prejudicados por listagem do IP compartilhado em alguma RBL.

# Solução usada atualmente



- A solução mais usada para estes problemas é o **Feedback Loop (FBL)**.
- Trata-se de um sistema onde o serviço de envio se cadastra no provedor de destino para receber informações sobre abusos.
- O destinatário denuncia um e-mail e o provedor dele envia a informação da denúncia ao serviço de envio, para que este último possa tomar as providências necessárias.

# Problemas do sistema FBL



- O enviador deve realizar um cadastro para cada provedor de destino, que são cerca de 2 mil só no Brasil, segundo a Anatel.
- As informações de denuncia não são padronizadas, forçando o serviço de envio a aplicar múltiplos modos de processamentos.
- É complexo implementar o FBL e por isso e pequenos provedores não implementam pelas severas restrições de recursos.
- A informação da denuncia é enviada muito tempo depois que a mensagem foi transmitida.
- Depende que serviço de e-mail cadastrado esteja disponível.

# Sistema de feedback do SPFBL



- Toda informação de feedback no SPFBL é passada pela camada SMTP e é compatível com a [RFC5248](#).
- Isso garante que o serviço de envio obtenha as informações sobre o abuso sem precisar de cadastro prévio do tipo FBL.
- Caso o MTA de origem obtenha um rejeição 5.7.1, significa houve pontuação negativa na rede SPFBL.

**5.1.1 SPFBL <message>**

**5.7.1 SPFBL <message>**

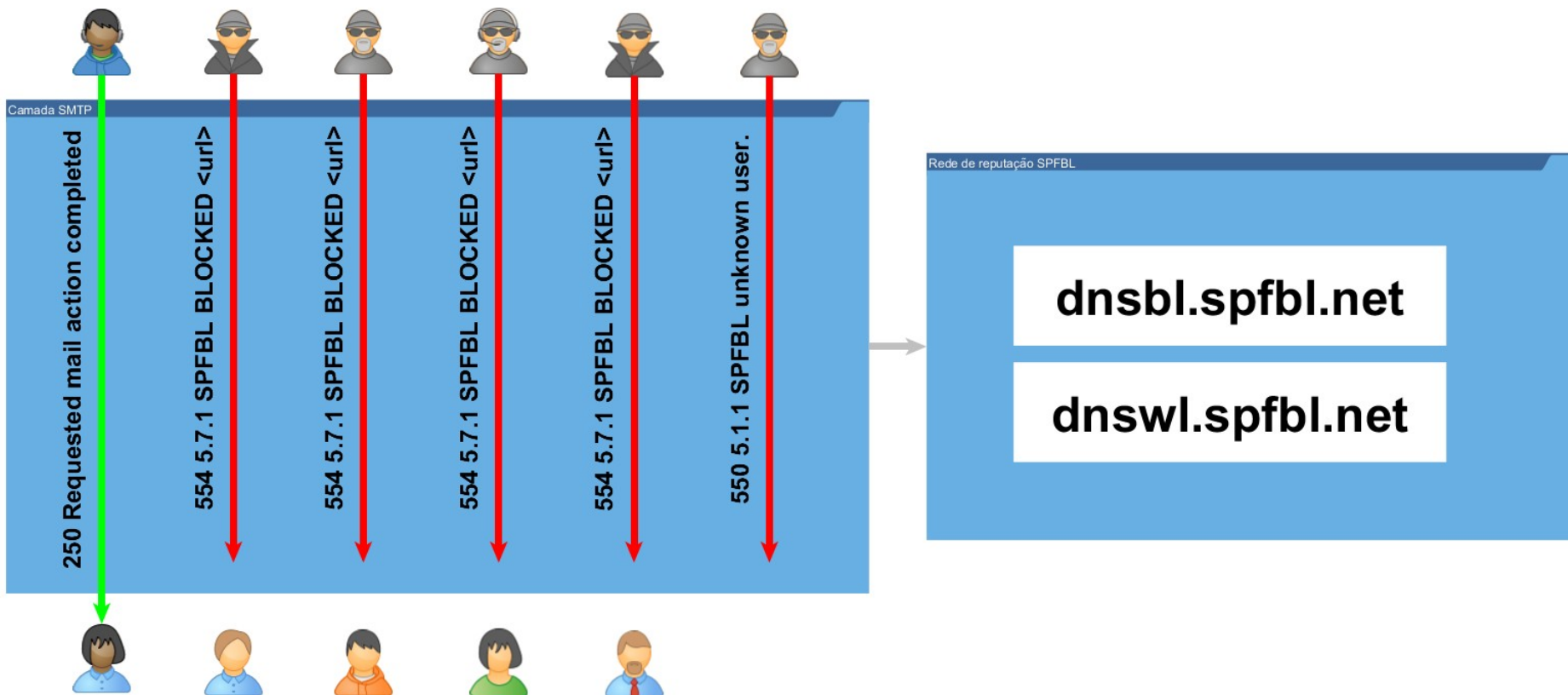
# Mecanismo de denúncia SPFBL



- Cada mensagem acompanha uma URL com o ticket da consulta.
- Este ticket é colocado no cabeçalho Received-SPFBL da mensagem.
- O destinatário pode acessar esta URL para formalizar a denúncia com a possibilidade mandar bloquear o remetente.

Received-SPFBL: PASS [http://matrix.spfbl.net/Y6g\\_GzIGITHC5Q...](http://matrix.spfbl.net/Y6g_GzIGITHC5Q...)

# Sistema de feedback do SPFBL

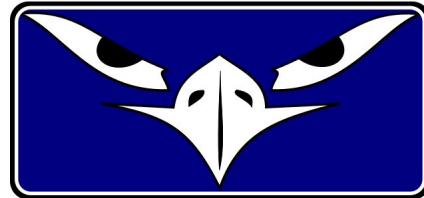


# Uso do sistema de feedback



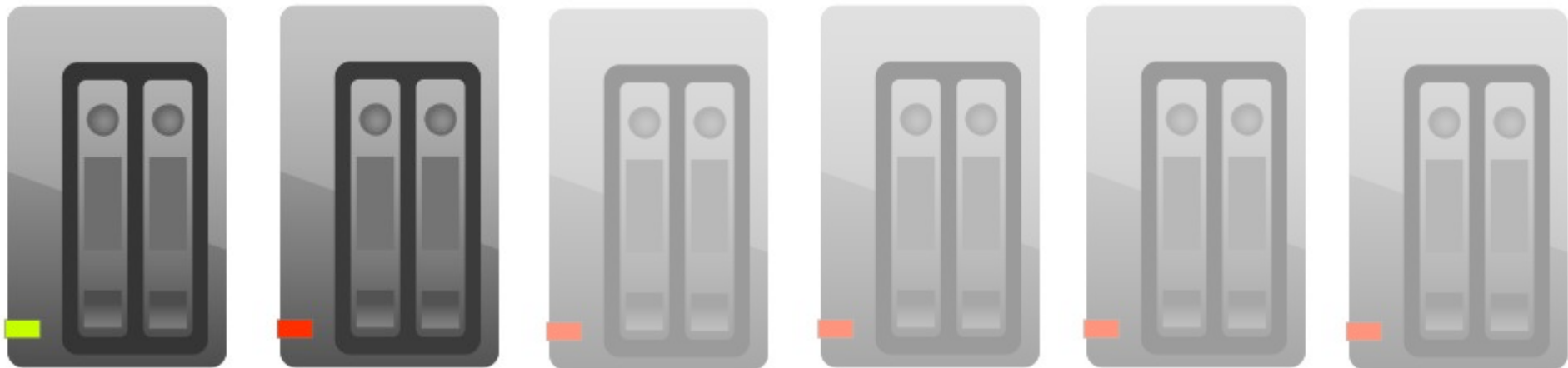
"Ferramentas de bloqueio que nos fornecem a maior quantidade de informações, nos ajudam a erradicar o spam desde sua origem. Seguindo essa lógica se os spammers não encontram lugares para realizarem seus envios, menos e-mails serão enviados e os dois lados ganham com isso.

As informações passadas pela SPFBL no momento da conexão SMTP nos dão agilidade e precisão já que com isso podemos identificar o remetente e agir imediatamente sobre a denúncia, evitando impactos maiores."



# Meta de redução do volume

- Estipulemos uma meta de proporção de 1/2 do volume indesejado para que a capacidade de escalar o serviço de recepção aumente 3 vezes sem necessidade de novos investimentos.
- Criação de sistemas de contenção para serviços de envio.





# Esclarecimento de dúvidas

Façam suas  
perguntas



# Links sobre o SPFBL



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

Site: <http://spfbl.net/>

Dúvidas: [leandro@spfbl.net](mailto:leandro@spfbl.net)

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

Camiseta: <https://www.montink.com.br/loja/spfbl>