

Ironmail – Filtrando emails indesejados

Leonard Bohrer Spencer, Guilherme Bertoni Machado

FATEC RS – Faculdade de Tecnologia Senac RS

lbohrer@terra.com.br , gb.machado@sinprors.org.br

Ironmail – Filtrando emails indesejados

- **O Problema:**

- Spam;
- Vírus;
- Consumo de banda;
- Consumo de espaço em disco;
- Consumo de memória;
- Tempo;

Ironmail – Filtrando emails indesejados

- Idéia
 - Ferramentas incompletas (difícil instalação e faltando alguns requisitos necessários para um bom controle sobre o servidor como, por exemplo, políticas por usuário para envio de emails)
 - Amavisd-new e Mailscanner

Ironmail – Filtrando emails indesejados

- O que é o Ironmail?
- Qual sua utilidade?
- A quem interessa?

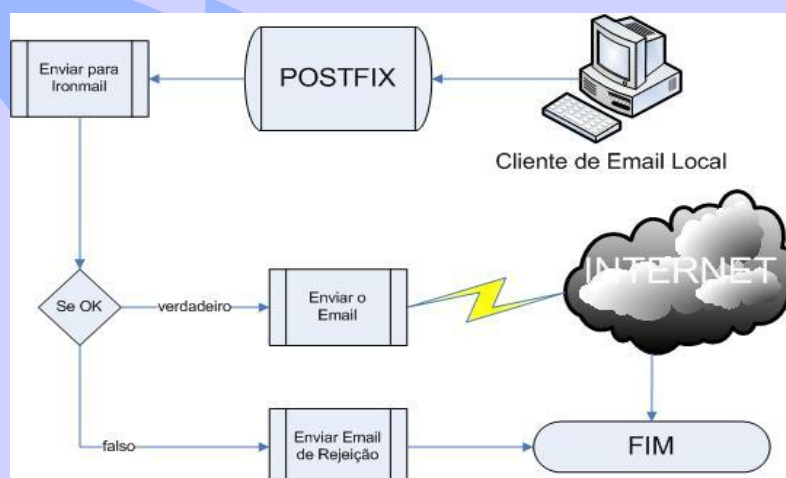
Ironmail – Filtrando emails indesejados

- Tecnologias utilizadas:

- Spamassassin;
- Clamav Antivirus;
- Perl;
- Mysql;
- Postfix.

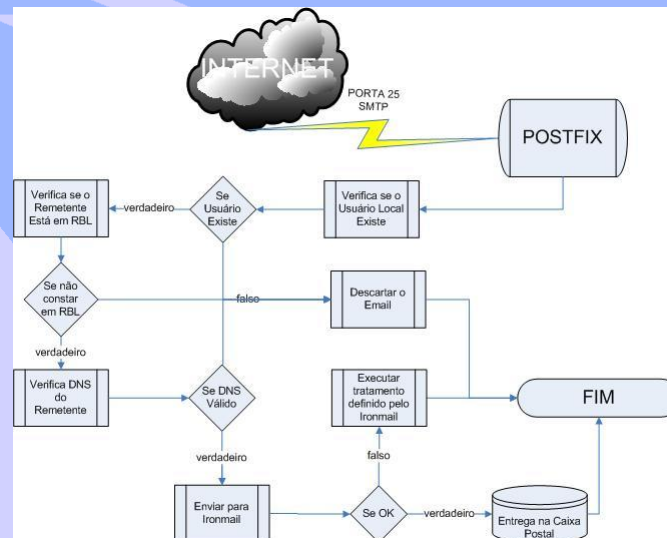
Ironmail – Filtrando emails indesejados

- Fluxo do email envio:



Ironmail – Filtrando emails indesejados

- Fluxo do email recepção:



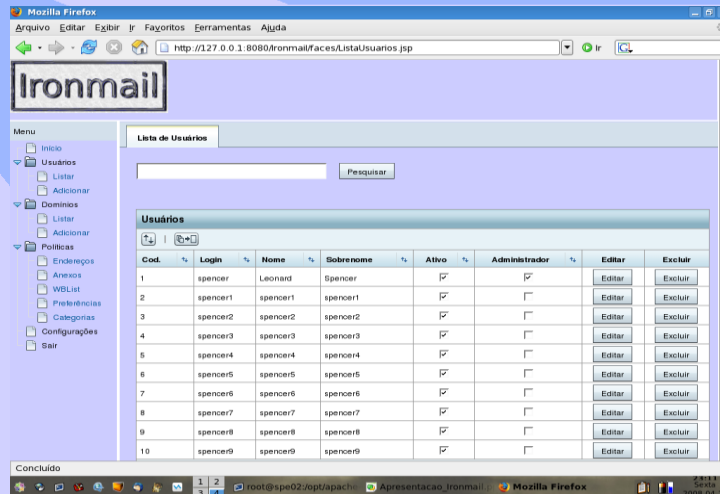
Ironmail – Filtrando emails indesejados

- Interface Gráfica:

- O Ironmail possui uma interface gráfica para facilitar o gerenciamento dos usuários e das políticas, definidas pelo administrador da rede.

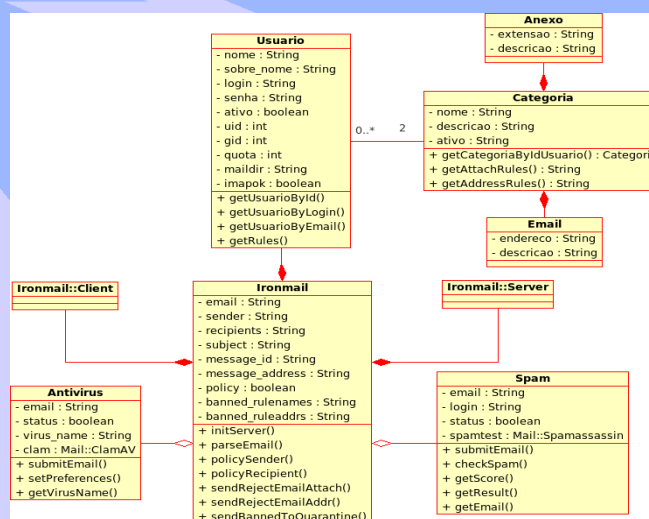
Ironmail – Filtrando emails indesejados

- Interface Gráfica:



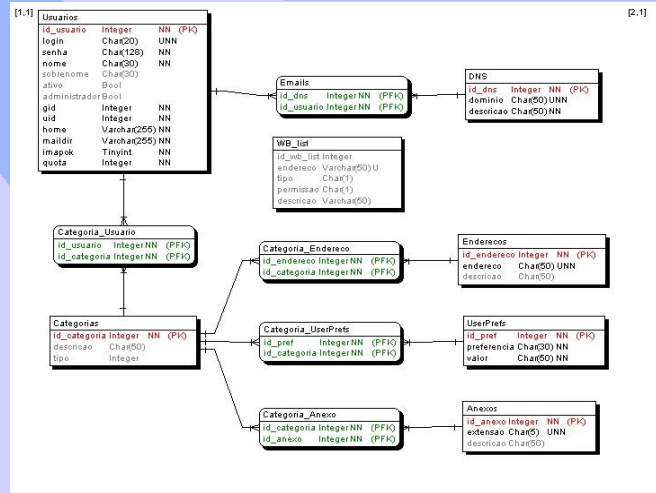
Ironmail – Filtrando emails indesejados

- Diagrama de Classes:



Ironmail – Filtrando emails indesejados

- Diagrama ER:



Ironmail – Filtrando emails indesejados

- Testes executados:

- Envio:

- Envio de email, para endereço externo, não permitido E permitido para o usuário local utilizado
 - Envio de email, para endereço externo, com anexo com extensão não permitida E permitida para envio do usuário local utilizado
 - Envio de emails classificados como *spam* por outros filtros de email contra o servidor de emails configurado para utilizar o Ironmail como filtro
 - Envio de email com arquivo Eicar (EICAR, 2008) anexo contra o servidor de emails configurado para utilizar o Ironmail como filtro. O Eicar foi criado para efetuar testes em ferramentas de antivírus.

Ironmail – Filtrando emails indesejados

- Testes executados:

- Recepção:

- Recepção de email, de endereço externo, não permitido para o usuário local utilizado
 - Recepção de email, de endereço externo, com anexo com extensão não permitida para recepção do usuário local utilizado
 - Recepção de email de endereço externo bloqueado, para o usuário local cadastrado
 - Recepção de email de endereço externo bloqueado, com anexo e com extensão permitida para recepção do usuário local cadastrado.

Ironmail – Filtrando emails indesejados

- Conclusão:

- Este trabalho permitiu constatar vários dos complexos problemas enfrentados pelos gestores da área de tecnologia e, em particular, os problemas associados ao envio e recepção de *emails*. Estes problemas podem ser solucionados a partir da utilização de políticas adequadas e bem definidas sobre os usuários do domínio.

Ironmail – Filtrando emails indesejados

- Trabalhos futuros:

- Armazenamento de dados sobre os emails, como: remetente, destinatários, assunto e tamanho da mensagem, para geração de relatórios e gráficos sobre os emails enviados e recebidos;
- Reescrever o ironmaild utilizando a linguagem de programação Java com o intuito de ter um melhor desempenho da aplicação;
- Autenticação de usuários por catálogo LDAP;
- Possibilidade de utilizar caixas postais de quarentena por usuário;

Ironmail – Filtrando emails indesejados

- Trabalhos futuros:

- Possibilidade de utilizar outros sistemas gerenciadores de banco de dados além do MySQL;
- Desenvolvimento de interface web para administração remota;
- Manipulação de regras para o Spamassassin para controle sobre palavras. Pode-se manipular o score de acordo com palavras encontradas no email;
- Remodelagem do algoritmo para facilitar a utilização de plugins

Ironmail – Filtrando emails indesejados

• Perguntas?

Leonard Bohrer Spencer, Guilherme Bertoni Machado

FATEC RS – Faculdade de Tecnologia Senac RS

lbohrer@terra.com.br , gb.machado@sinprors.org.br