Combatendo Spam com Greylisting no sistema de email @usp.br

André Gerhard
Thiago Alves Siqueira

GSeTI (CSIRT USP)
CCE-USP, São Paulo

Cenário

- **Sistema de e-mail com muitos usuários**
  - Em torno de 25 mil;
  - 840000 conexões/dia (entrada), 174000 envios/dia
- **Características heterogêneas: docentes, funcionários e alunos.**
- **Muitos usuários? Muitas reclamações!**
- **Razão?**

SPAM!!!

Soluções adotadas

- **Verificação em algumas blacklists na Internet**
- **Blacklist própria**
  - Chegou Spam? Bloqueado!
- **Amenizam o número de spams, mas ainda são muitos.**
- **O que fazer?**

Nova camada de proteção...

Greylisting (1/3)

...Greylisting!

- **Spammers raramente utilizam servidores legítimos.**
  - Consequência: raramente reenviam as mensagens.
- **Protocolo SMTP define que a mensagem deve ser reenviada (código 4XX).**
- **Enviou apenas uma vez? Ficará bloqueado!**
- **Reenviou? Assume que o e-mail é legítimo.**

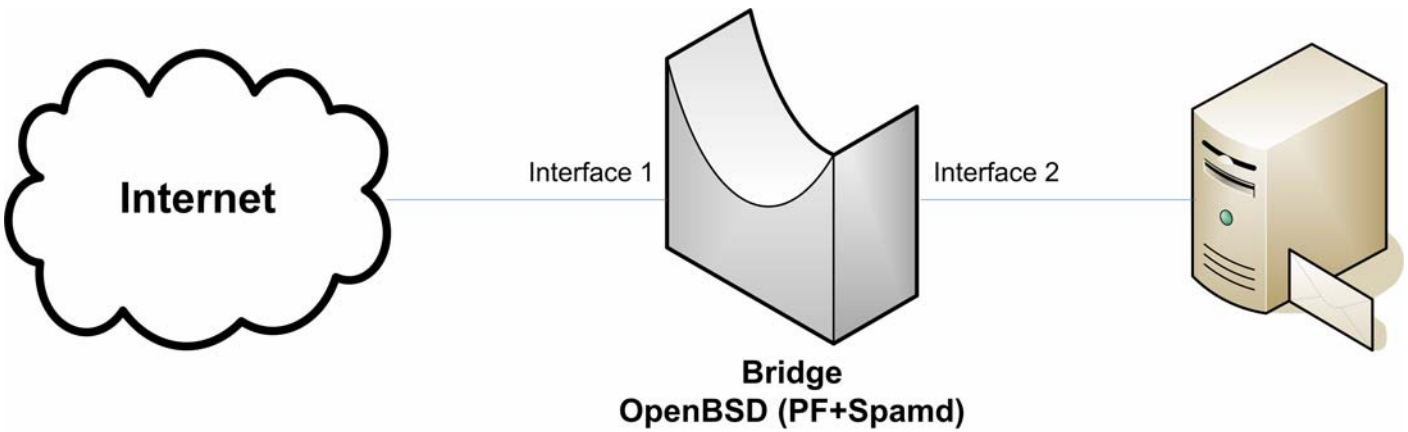
Greylisting (2/3)

- **Sou usuário legítimo.**
  - Utilizo meu servidor smtp e envio uma mensagem para *user*@usp.br;
  - O servidor @usp.br rejeita o e-mail temporariamente;
  - Conforme o protocolo manda, meu servidor smtp reenvia essa mensagem mais tarde;
  - O sistema da USP *lembra* que eu tentei enviar do meu servidor smtp, e que isso é um reenvio;
  - Então, a mensagem é entregue ao destinatário.

Greylisting (3/3)

- **Sou *spammer*!**
  - Envio milhares de spam para a USP;
  - A USP rejeita temporariamente os emails;
  - O software que utilizo para envio de mensagens em massa não reenvia as mensagens mais tarde;
  - Como não houve reenvio, mensagem não chegará no servidor de email.

Estrutura



OpenBSD

- **Implementação da bridge em OpenBSD**
- **Motivos:**
  - Suporte nativo a bridge;
  - Solução spamd integrada ao sistema;
  - Excelente desempenho do firewall pf (packet filter);
  - Sistema operacional desenvolvido pensando na segurança.
- **Receita desenvolvida pela “University of Texas-Pan American (UTPA.edu)”, mas aparentemente pouco disseminada.**

Bridge

- **Todas as mensagens para o servidor de e-mail passam por ela.**
- **É *transparente* para esse servidor, atuando na camada 2:**
  - Se o IP origem está *reenviando*, repassa a mensagem ao servidor;
  - Se o IP origem está *enviando pela primeira vez*, a bridge responde no lugar do servidor, com o IP do servidor.
- **Outros protocolos passam de forma transparente pela bridge.**

PF – Packet Filter

- **Firewall do OpenBSD**
  - Se o IP está liberado (consta nas tabelas mantidas pelo PF), redireciona pacote para o servidor SMTP.
  - Se não há informação sobre o IP, redireciona para o *spamd*.
- **IP's que podem conectar-se ao servidor SMTP atualizados automaticamente (greylisting).**

Spamd (1/2)

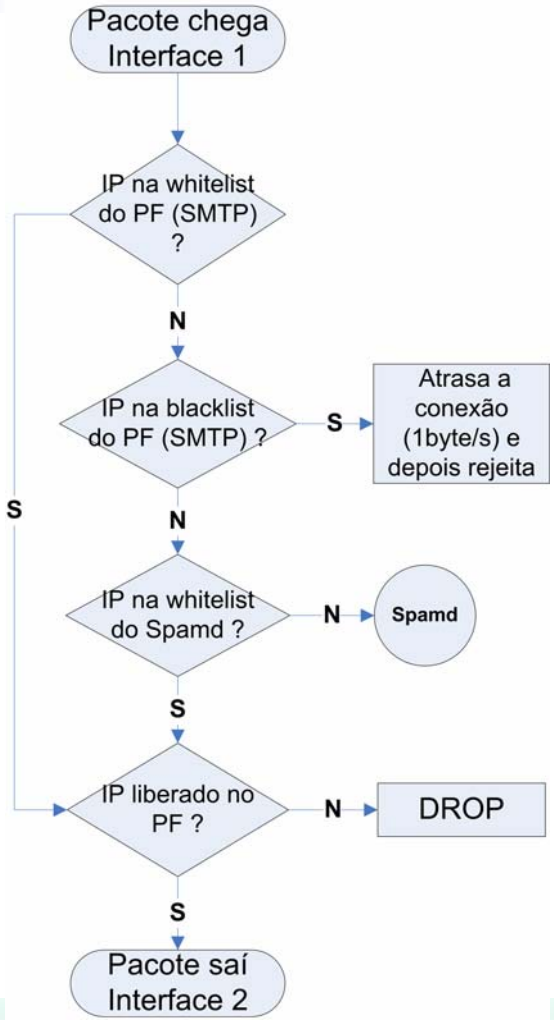
- **Daemon que implementa o *greylisting***
- **Trabalha em conjunto com o PF:**
  - Quando o PF não possui informação sobre o IP que está tentando enviar e-mail, ele pede para o *spamd* responder;
  - O *spamd* responde como sendo o servidor smtp.
- **Guarda as informações:**
  - IP de origem, e-mail de origem, e-mail de destino e horário que foi enviado o e-mail.

Spamd (2/2)

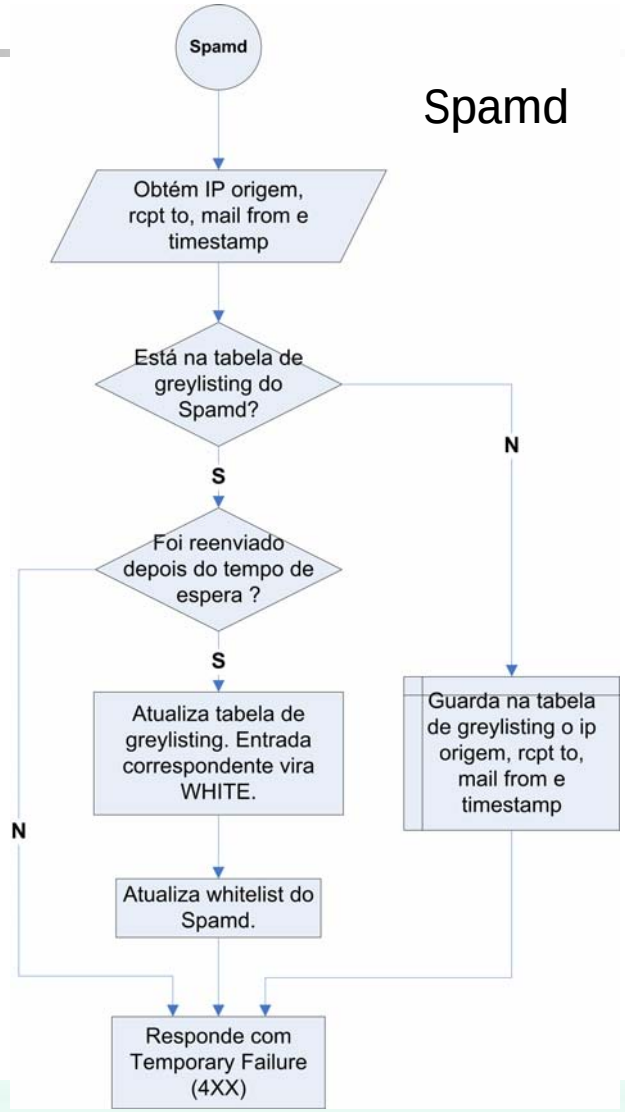
- Quando o servidor de origem reenvia a mensagem, e o tempo após o primeiro envio for maior que o tempo de espera (*passtime*) configurado no spamd, ele atualiza a tabela do PF, permitindo a conexão no servidor smtp verdadeiro.
- Entradas em GREY expiram após *greyexp* e em WHITE após *whiteexp*.
- -G *passtime:greyexp:whiteexp*
  - passtime: default 25 minutos
  - greyexp: default 4 horas
  - whiteexp: default 864 horas (36 dias)

Fluxo

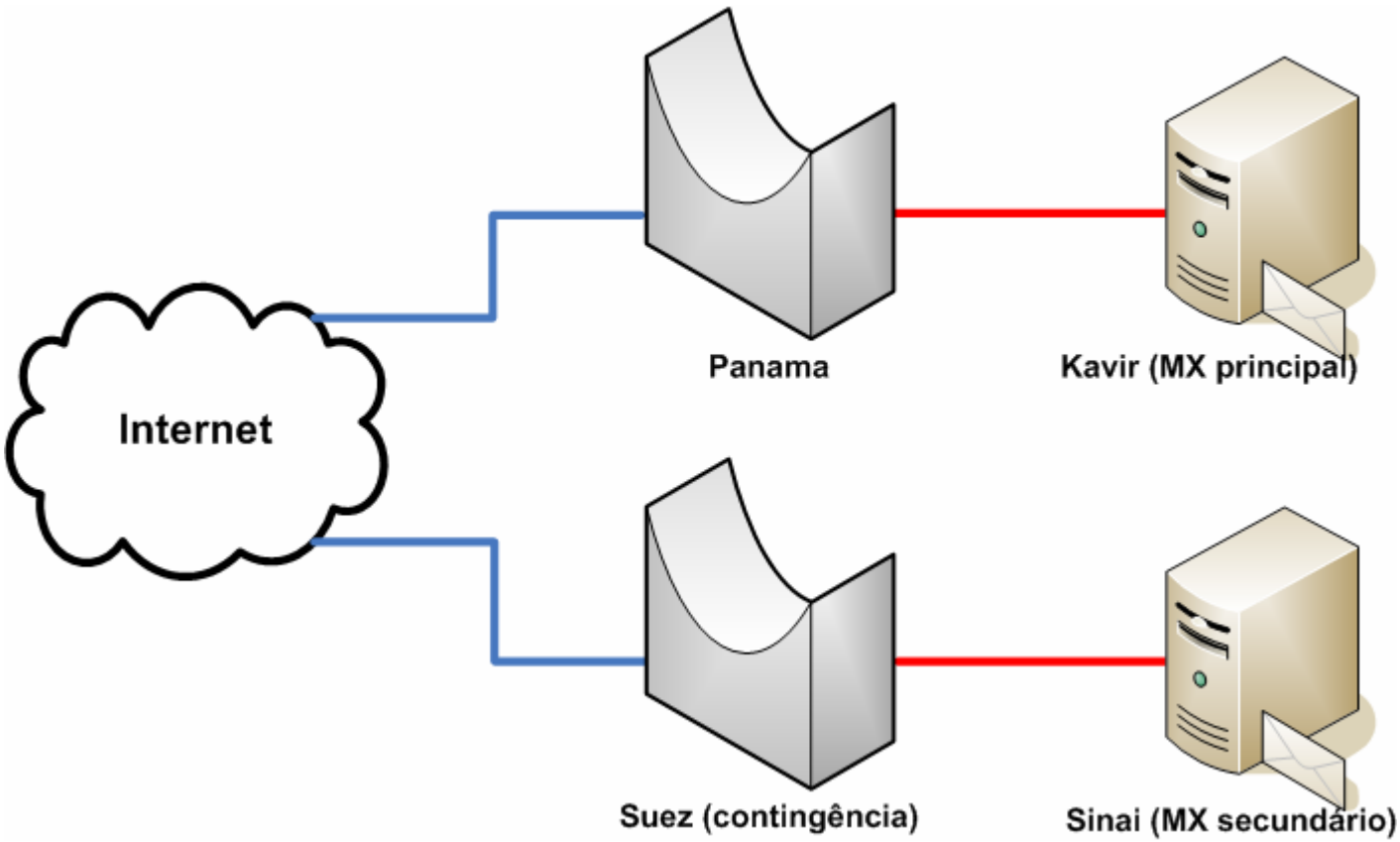
PF



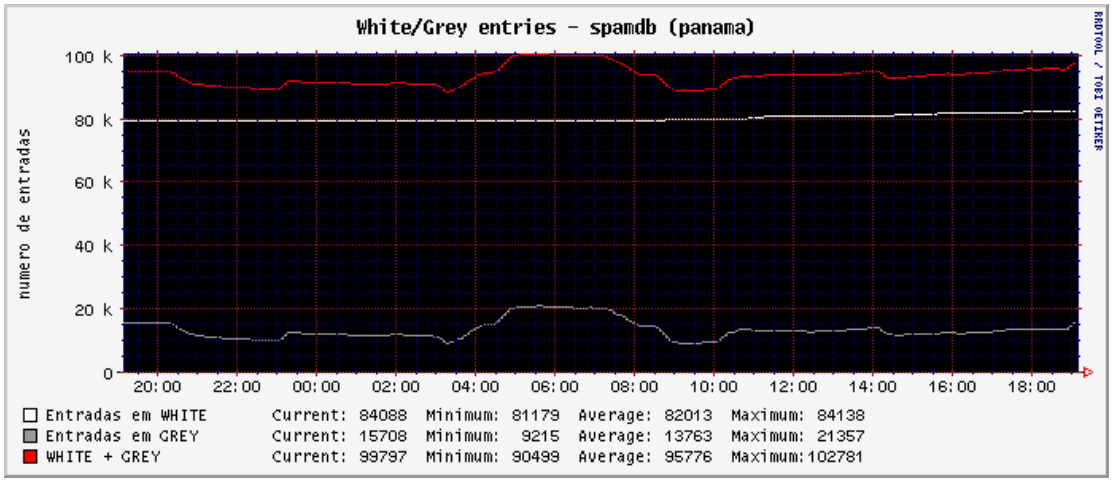
Spamd



Implementação

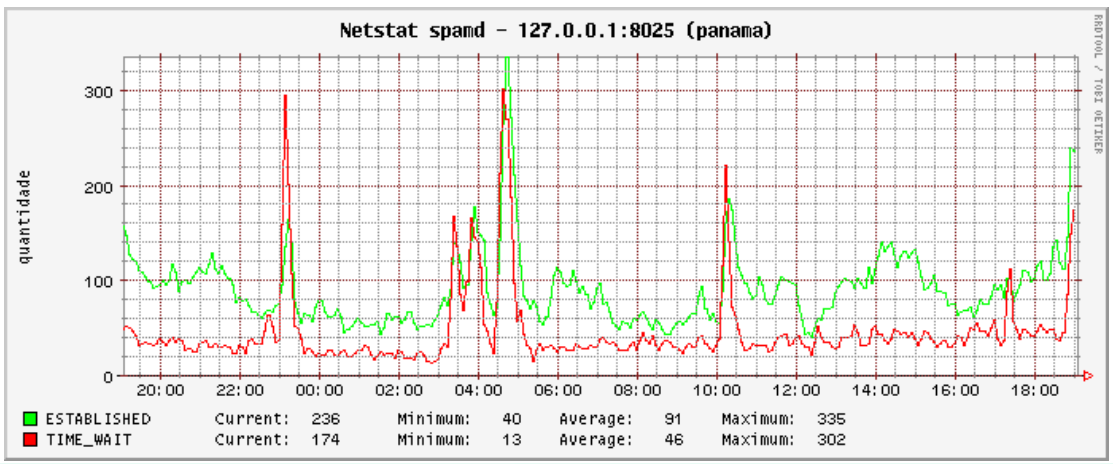


Implementação



Spamdb:
~100.000 entradas,
~55Mb

3 meses em produção



Implementação

Exemplo: algumas entradas na tabela de greylisting (comando *spamdb*)

WHITE|201.212.1.226|||1161913310|1161921266|1165031677|2|0
GREY|201.212.143.193|<Hartley@168city.com>|<pedro@usp.br>|1163012482|1163026882|1163026882|1|0
WHITE|201.212.148.89|||1162598182|1162600047|1165710467|2|0
WHITE|201.212.175.196|||1162245962|1162247755|1165358182|4|0
GREY|201.212.179.242|<33kendrick@stringerinc.com>|<miglugra@usp.br>|1163011262|1163025662|1163025662|1|0
WHITE|201.212.186.13|||1160434078|1160443643|1163554055|3|0
WHITE|201.212.187.13|||1162678680|1162690574|1165800989|2|0
GREY|201.212.36.187|<onlinesupport_id-056922401482804ams@amsouth.com>|<flamori@usp.br>|1163017832|1163032232|1163032232|1|0
WHITE|201.212.48.12|||1160174405|1160186755|1163297160|2|0
GREY|201.212.57.123|<albuquerquecirculant@roykestopp.com>|<angelofe@usp.br>|1163020112|1163034512|1163034512|1|0
GREY|201.212.57.123|<alightbasso@royhelgeringrescue.nl>|<acossedxpf@usp.br>|1163019943|1163034343|1163034343|1|0
GREY|201.212.57.123|<alliteratebesetting@rowmedia.com>|<acasa@usp.br>|1163019971|1163034371|1163034371|1|0
GREY|201.212.57.123|<ambulatebaku@royaltef.com>|<bhenrique@usp.br>|1163020046|1163034446|1163034446|1|0
GREY|201.212.57.123|<anglicancambric@roydmercer.com>|<angelofe@usp.br>|1163019998|1163034398|1163034398|1|0
GREY|201.212.57.123|<anteroomadministrate@rottweilerklubbenskane.com>|<bcezar@usp.br>|1163020030|1163034430|1163034430|1|0
GREY|201.212.57.123|<antitheticcommitteewomen@rossmoorrealty.com>|<bhenrique@usp.br>|1163019953|1163034353|1163034353|1|0
GREY|201.212.57.123|<aperturecatkin@rossi-gioielleria.it>|<acasa@usp.br>|1163020016|1163034416|1163034416|1|0
GREY|201.212.57.123|<apologyconvertible@royalline-sy.com>|<acasa@usp.br>|1163020125|1163034525|1163034525|1|0

Implementação

Trecho do /var/log/spamd

```
Nov  8 20:02:52 panama spamd[4210]: 218.12.185.61: disconnected after 5 seconds.
Nov  8 20:02:52 panama spamd[4210]: 194.25.134.85: connected (67/0)
Nov  8 20:02:52 panama spamd[4210]: (GREY) 201.12.40.91: <elearning@elearningparatodos.com.br> ->
    <edsonbrt@usp.br>
Nov  8 20:02:52 panama spamd[4210]: 201.12.40.91: disconnected after 11 seconds.
Nov  8 20:02:52 panama spamd[4210]: 162.84.144.90: connected (67/0)
Nov  8 20:02:52 panama spamd[4210]: (GREY) 200.157.211.80: <adm@patrianiee.com.br> -> <luisalme@usp.br>
Nov  8 20:02:52 panama spamd[4210]: 200.157.211.80: disconnected after 11 seconds.
Nov  8 20:02:52 panama spamd[4210]: (GREY) 200.38.71.210: <natalino@usp.br> -> <natalino@usp.br>
Nov  8 20:02:52 panama spamd[4210]: 200.38.71.210: disconnected after 11 seconds.
Nov  8 20:02:53 panama spamd[4210]: (GREY) 82.42.162.84: <odloak@usp.br> -> <odloak@usp.br>
Nov  8 20:02:53 panama spamd[4210]: 81.50.86.42: disconnected after 411 seconds.
Nov  8 20:02:53 panama spamd[4210]: 141.158.137.205: disconnected after 411 seconds.
Nov  8 20:02:53 panama spamd[4210]: 200.171.87.101: disconnected after 10 seconds.
Nov  8 20:02:53 panama spamd[4210]: 74.135.74.244: disconnected after 3 seconds.
Nov  8 20:02:53 panama spamd[4210]: 200.171.87.101: disconnected after 3 seconds.
Nov  8 20:02:53 panama spamd[4210]: 200.143.24.122: disconnected after 6 seconds.
Nov  8 20:02:53 panama spamd[4210]: 82.42.162.84: disconnected after 12 seconds.
Nov  8 20:02:53 panama spamd[4210]: 71.251.137.92: disconnected after 11 seconds.
Nov  8 20:02:53 panama spamd[4210]: (GREY) 81.195.10.34: <wenputbenocxje@babydoll.ca> -> <anacampa@usp.br>
Nov  8 20:02:53 panama spamd[4210]: 81.195.10.34: disconnected after 13 seconds.
Nov  8 20:02:53 panama spamd[4210]: 201.18.63.170: connected (57/0)
```

Implementação

- 840000 emails/dia, 375000 chegam ao MX
  - ∴ **~55% barrados pelo greylisting**
- Dos 375000, 150000 passam pela RBL
  - ∴ **~60% barrados pela RBL**
- Total (greylisting+RBL): ~82% bloqueado

- Endereços de origem de spam que eventualmente passarem podem ser adicionados a uma BL (na própria bridge ou no servidor de email).
- Endereços de servidores legítimos (detectados pela bridge) podem ser adicionados a uma whitelist.

Problemas observados

- Na verdade, existem **3 estados** para uma email legítimo que chega ao sistema pela primeira vez: primeiro a entrada entra em GREY (retornando 4xx), depois em WHITE (ainda retornando 4xx) e só na tentativa seguinte ela é repassada ao servidor de email.

- Configuração PF, normalização de pacotes (scrub)

- Servidores com Callback – checagem de usuários

Conclusão

- **Solução de fácil configuração e utilização;**
- **Independente do servidor de correio eletrônico;**
- **Flexível, funciona como appliance na rede;**
- **Pode proteger mais de um servidor na rede.**
- **Custo: uma máquina**

Referências

http://wiki.utpa.edu/InfoSec/GreyListingInstall/

http://www.openbsd.org/papers/bsdcan05-spamd/

http://www.openbsd.org/

http://www.antispam.br/

Contato

- **GseTI (CSIRT USP)**
  - security@usp.br
- **SCSERED - CCE**
  - soc@usp.br

Obrigado!

Dúvidas? Sugestões?