Análise de Desempenho de Políticas de Segurança em Servidores de Correio Eletrônico

Gustavo Rodrigues Ramos

Thiago Alves Siqueira

Prof. Dr. Adriano Mauro Cansian

Coordenador

ACME! Computer Security Research Labs

UNESP - Universidade Estadual Paulista

Campus de São José do Rio Preto

Agenda

- Introdução
- Segurança dos servidores SMTP
- Política de segurança
- Implementação
  - Postfix, Amavis, Clamav e Spamassassin
- Testes e Resultados
- Conclusões

Introdução

Introdução

"Quase a **metade** de tudo que circula na internet é **lixo**. Trocando em miúdos: no Brasil e no mundo, os usuários da internet estão sendo inundados por uma onda de **spams, de vírus, de pornografia, de pedofilia, de propaganda nazista, de roubo de dados, de comercialização de produtos pirateados, de medicamentos falsos, de propostas mentirosas**, de endereços e remetentes apócrifos e oferecimentos semelhantes (...)."

Quinta-feira, 09 de setembro de 2004 - 09h37
http://www.estadao.com.br/tecnologia/coluna/ethevaldo/2004/set/09/30.htm

Introdução

- Os problemas envolvidos são:
  - Custo elevado para enviar e armazenar essas mensagens.
  - **Vírus:** atravessam *firewalls* e demais proteções atingindo diretamente o “elo mais fraco da corrente”.

Introdução

- **SPAM:** Existem dois tipos de spam:
  - **Ilegais:** São, por exemplo, aqueles que têm por objetivo a disseminação de pornografia infantil ou contêm mensagens de discriminação religiosa, racial ou sexual.
  - **Legalidade discutível:** Todas as demais mensagens não solicitadas que transmitem propagandas, correntes, ...

Introdução

- Necessidade de determinar regras para a utilização e configuração dos servidores SMTP.

Problema:

- Como determinar o desempenho de uma política de segurança?
- Quais regras podem ser implementadas com uma infra-estrutura?

Segurança dos servidores SMTP

Segurança dos Servidores SMTP

- O protocolo SMTP (RFC 821 – Agosto/1982):
  - Desenvolvimento voltado à conectividade, com poucas medidas de segurança.
- RFC 2505: *Anti-Spam Recommendations for SMTP MTAs* (fevereiro/1999).
- RFC 2821: *Simple Mail Tranfer Protocol* (Abril, 2001).
- RFC 3552: *Guidelines for Writing RFC Text on Security Considerations* (Julho, 2003).
- RFC 3865: *A No Soliciting Simple Mail Transfer Protocol (SMTP) Service Extension* (Setembro, 2004).

Recomendações do RFC 2505

- Bloquear o envio não autorizado durante o diálogo SMTP.
  - Este procedimento impede que a mensagem seja **armazenada** no servidor – poupando recursos.
  - Faz com que o cliente SMTP se responsabilize pelo tratamento do erro.
- Definição das informações confiáveis:
  - **IP de origem da conexão** (TCP).
  - **RCPT TO.**

Recomendações do RFC 2505

- Observações de segurança:
  - Implementar muitas regras de filtragem degradam o desempenho do servidor.
  - A checagem de domínio válido também pode causar *DoS* no servidor DNS do MTA.
  - Muitas das medidas de segurança que podem ser adotadas podem favorecer ataques de negação de serviço – aumento do tamnho dos arquivos de log ou aumento do número de requisições DNS.

Segurança dos Servidores SMTP

- Técnicas utilizadas no combate às mensagens não solicitadas:
  - Regras de checagem no MTA
  - Realtime Blackhole List
  - Sender Policy Framework (SPF)
  - Listas de bloqueio e permissão (*blacklist* e *whitelist*)
  - Filtro anti-spam
  - Anti-vírus

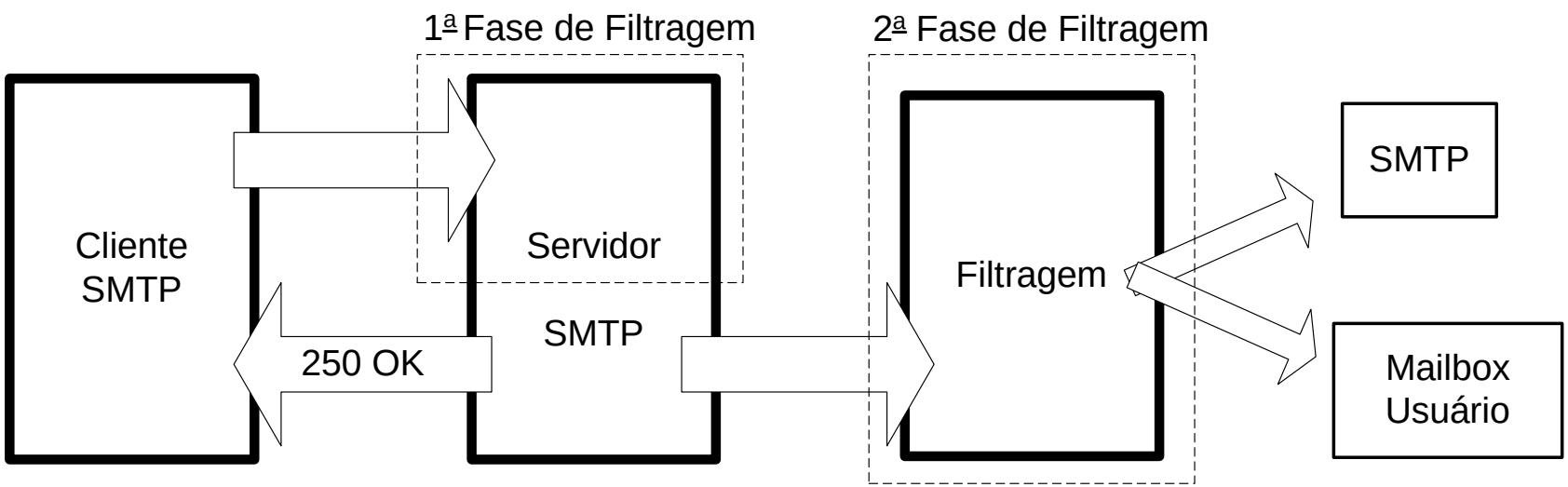
Política de Segurança

Política de Segurança

- Bloquear todas as mensagens com **vírus** e não permitir o envio de arquivos com extensão suspeita.
- Não receber mensagens de **domínios desconhecidos**.
- Não permitir o envio de mensagens que não estejam de acordo com o protocolo.
- Marcar os spams no cabeçalho e/ou o *subject* da mensagem.

Política de Segurança

- Duas fases de filtragem:



Política de Segurança

- 1ª fase:
  - Filtragem no **Postfix** de acordo com o RFC 2505.
  - Descarte das mensagens não permitidas antes de aceitar o envio.
- 2ª fase:
  - Filtragem através do **Amavisd-new**.
  - Descartar as mensagens que possuem vírus.
  - Marcar as mensagens que eram consideradas spam.

Implementação

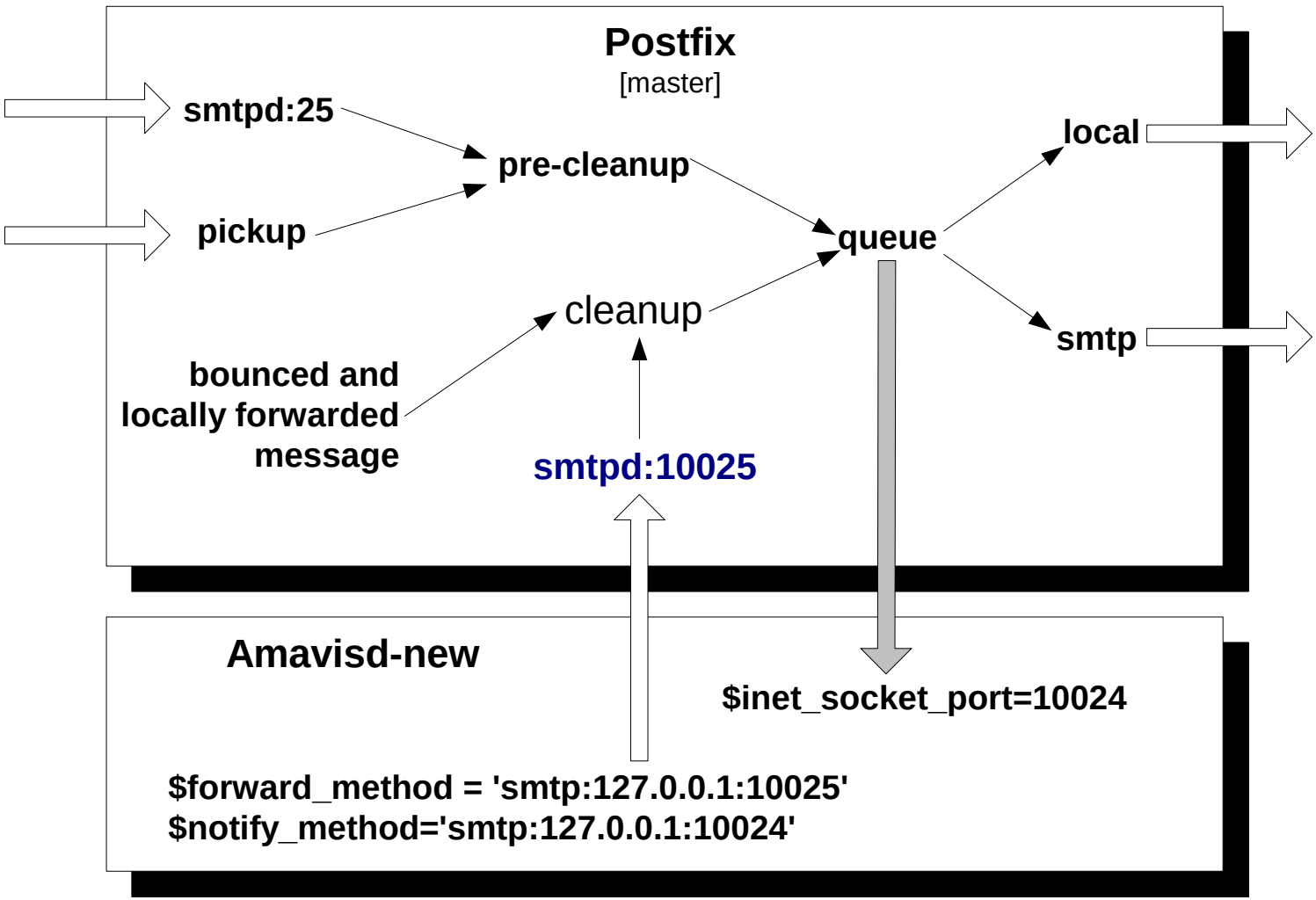
Implementação: **Postfix**

- Segurança e flexibilidade.
- Regras que podem ser aplicadas ao *smtpd* (main.cf):
  - smtpd_client_restrictions
  - smtpd_helo_restrictions
  - smtpd_sender_restrictions
  - smtpd_recipient_restrictions

Implementação: **Postfix**

- Filtragem de todos os arquivos com extensão suspeita.
  - mime_header_checks = regexp:/etc/postfix/maps/mime_checks
- HELO obrigatório.
  - smtpd_helo_required = yes
- Rejeitar mensagens cujo remetente não possui domínio válido.
  - smtpd_sender_restrictions = reject_non_fqdn_sender, reject_unknown_sender_domain
- Rejeitar mensagens que não seguem o protocolo.
  - strict_rfc821_envelopes = yes

Implementação: **Amavisd-new**



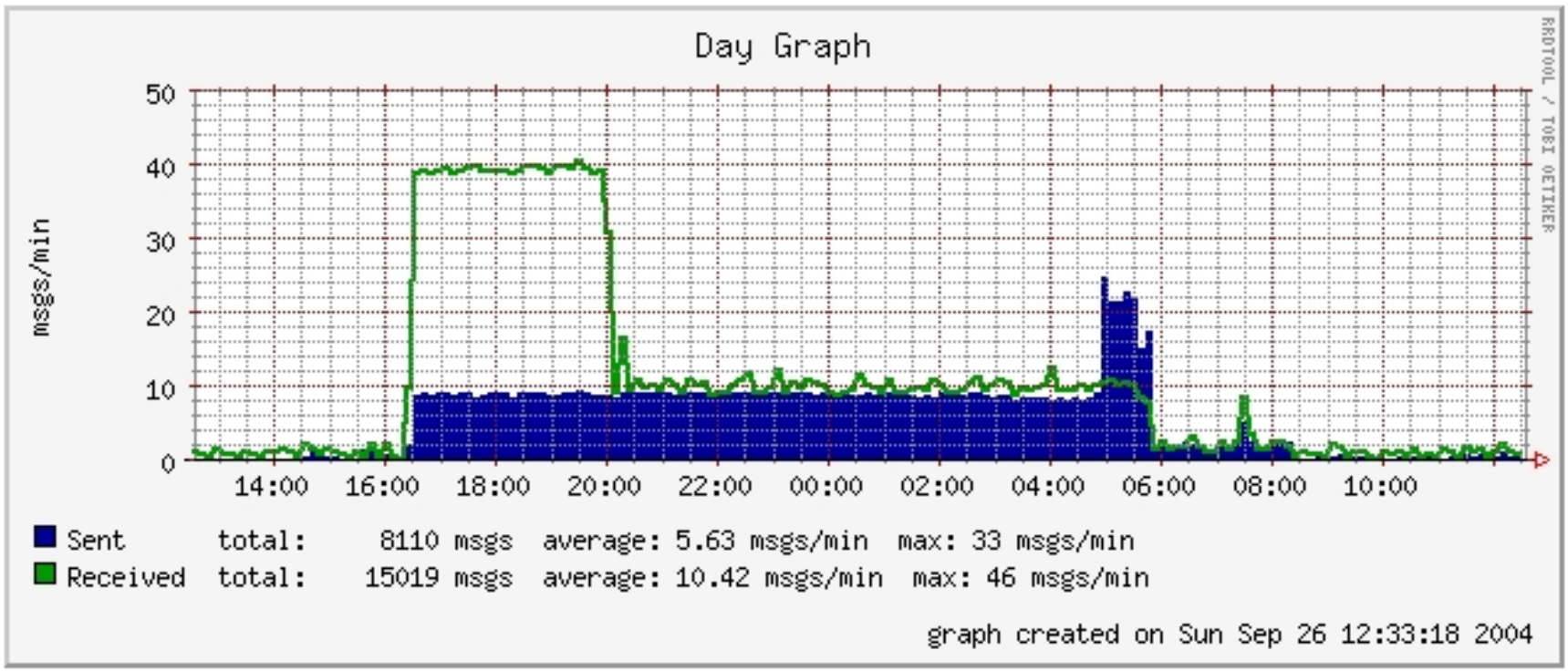
Implementação: **Amavisd-new**

- Responsável pela segunda filtragem das mensagens:
  - Encaminha as mensagens para o anti-vírus; possui suporte a vários anti-vírus.
  - Filtragem de spam com o *spamassassin*.
- Pode ser usado para distribuir a carga entre máquinas diferentes.

Implementação: **Amavisd-new**

- Anti-vírus
  - **Clamav**: distribuído sob licença GPL, nos testes apresentou um bom desempenho.
- Filtro de spam
  - **Spamassassin**: Com a atualização das regras aumentou o número de spams identificados com sucesso, porém diminuiu o desempenho do sistema – em um dos testes, observamos o máximo de 10 mensagens por minuto.

Implementação: Spamassassin



30 mensagens por minuto: Atraso máximo de 10 horas!!!

(Servidor Compaq Alpha DS20/600Mb de memória RAM)

Testes e Resultados

Testes e Resultados

- Os testes a seguir utilizaram:
  - Pentium III 800Mhz com 650 MB de memória RAM.
  - Sistema Operacional Debian GNU/Linux (Kernel 2.4.18).
  - Ferramenta **Postal** [1] para *benchmark* de servidores SMTP.

[1] http://www.coker.com.au/postal

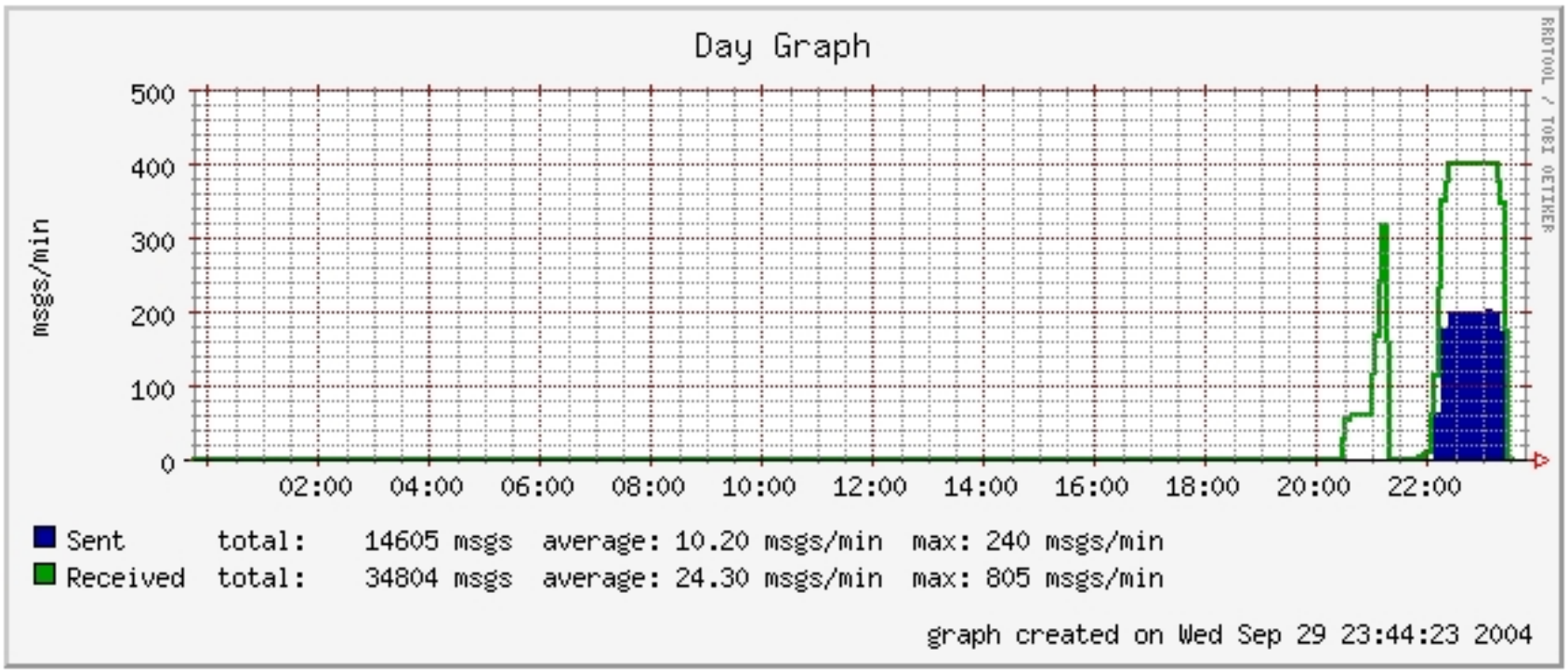
Testes e Resultados

- Testes **sem filtros**:
  - Mensagens de 10 KB.
  - 500 mensagens por minuto.
  - Sem atraso.

Testes e Resultados

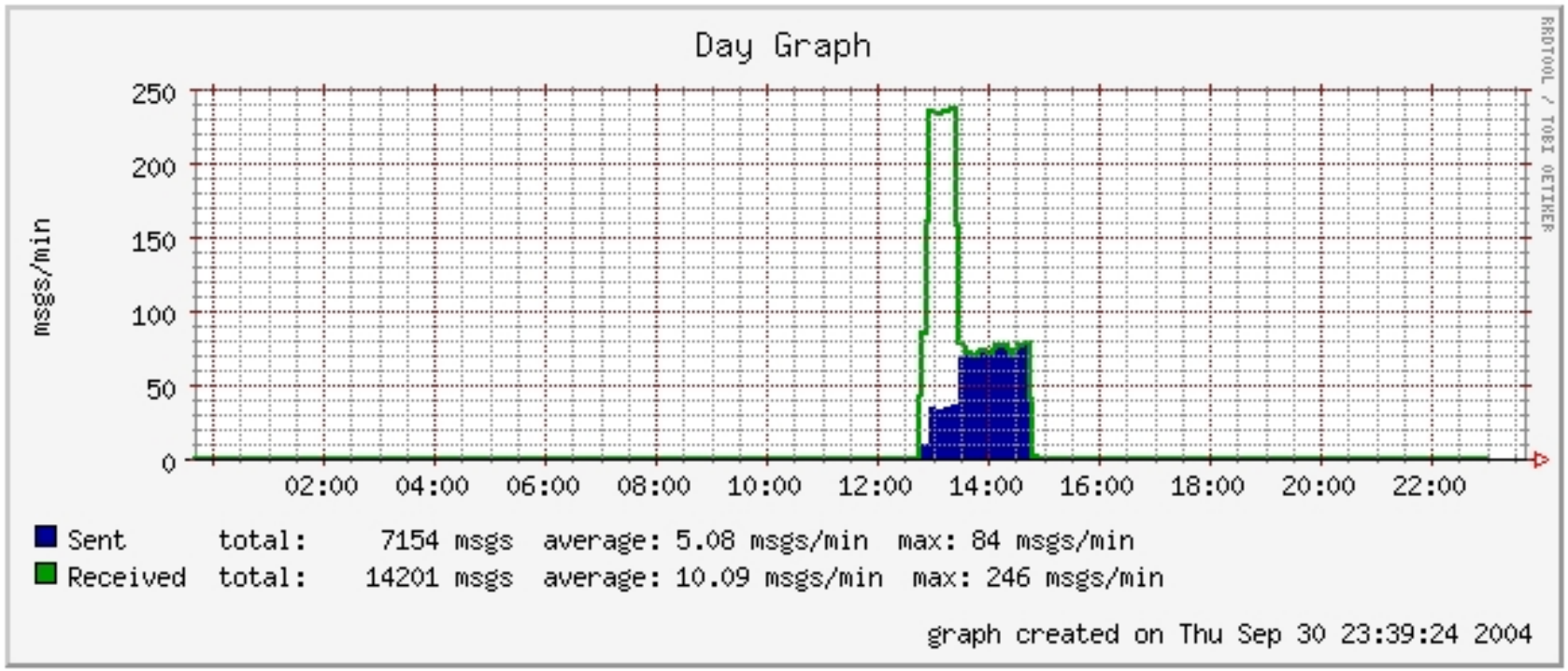
- Testes **com anti-vírus**:
  - Mensagens de 10 KB.
  - Máximo 250 mensagens por minuto.
  - Sem atraso.
- Testes **com anti-vírus**:
  - Mensagens de 500 KB.
  - Máximo de 40 mensagens por minuto.
  - Sem atraso.

Testes e Resultados



Com anti-vírus: 200 mensagens (10 KB) por minuto com atraso mínimo.

Testes e Resultados

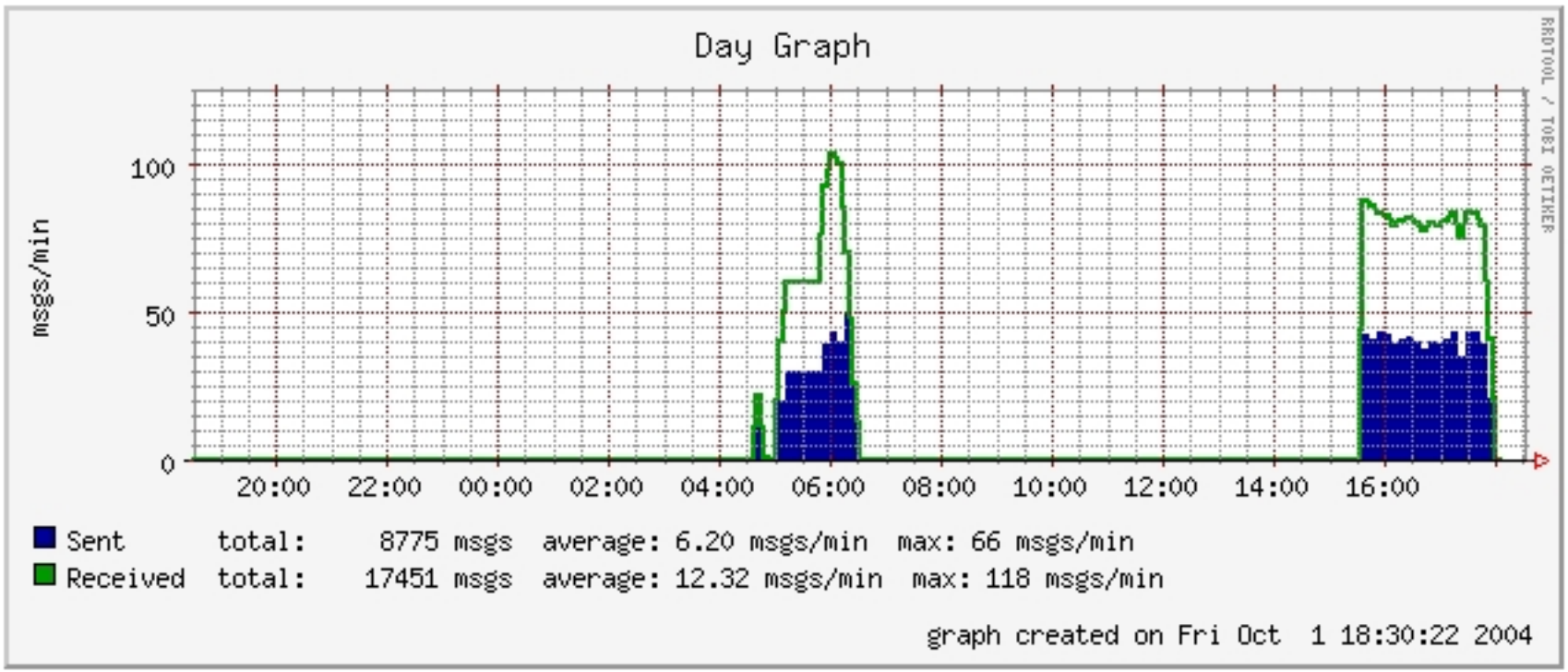


Com anti-vírus: 40 mensagens (500 KB) por minuto com atraso mínimo.

Testes e Resultados

- Testes **com filtro de spam e anti-vírus**:
  - Mensagens de 10 KB.
  - Máximo 45 mensagens por minuto.
  - Com atraso de 20 a 30 segundos para a entrega das mensagens.

Testes e Resultados



Filtragem de vírus e spam: 40 mensagens (10 KB) por minuto com atraso menor que 1 minuto.

Conclusões

Conclusões

- As ferramentas escolhidas são facilmente adaptáveis às diversas políticas de segurança, infra-estrutura e necessidades de desempenho.
- Implementar TODOS os tipos de filtragem é inviável. No entanto pode-se **equilibrar** e **testar** a implementação antes de colocá-la em produção.
- Monitorar, monitorar...

Referências

- CERT/CC – **Email bombing and spamming**.
  http://www.cert.org/tech_tips/email_bombing_spamming.html
- GRC/AI/UNESP – **Spamassassin – Testes Iniciais**
  http://grc.unesp.br/modules.php?op=modload&name=News&file=article&sid=16&mode=thread&order=0&thold=0
- Postfix – **Postfix Documentation.**
  http://www.postfix.org/documentation.html
- RFC 2505: **Anti-Spam Recommendations for SMTP MTAs.**
  http://www.faqs.org/rfcs/rfc2505.html
- SANS Institute – **Security Policy Project.**
  http://www.sans.org/resources/policies/
- Security Sage – **Anti-spam Guide.**
  http://www.securitysage.org/antispam

Dúvidas, sugestões, idéias, ...

Para entrar em contato:

gustavo@acmesecurity.org Key ID: 0x797950D6

thiago@acmesecurity.org Key ID: 0x11ED1273

adriano@acmesecurity.org Key ID: 0x3893CD28

http://www.acmesecurity.org

ACME! Computer Security Reseach Labs

UNESP – IBILCE

São José do Rio Preto - Brasil