BFW - Uma abordagem para Segurança baseada em Software Livre

Leonardo Garcia de Mello
Analista de Informática - MPF

São Paulo, abril de 2004

Objetivos - 1 de 3

- **Através de *firewalls*, aumentar a segurança para os sistemas computacionais em uso no ambiente de rede do MPF**
- **Implantar um sistema de detecção de intrusão do tipo *NIDS* em cada Unidade do MPF, visando a criação de um Banco de Dados Nacional para Incidentes de Segurança**

Objetivos - 2 de 3

- **Permitir que seja feita uma reserva na largura de banda para certas aplicações**
  - **Baseado em endereços IP e números de porta TCP/UDP**
- **Implementar o suporte a *transparent proxies*, segundo a RFC-3040**

Objetivos - 3 de 3

- **Redirecionar o tráfego SMTP, para**
  - **permitir a execução de antivírus, sem afetar a nenhum dos servidores de email já existentes;**
  - **aplicar regras diferenciadas para o roteamento de *emails* internos**
- **Disponibilizar analisadores de tráfego, que**
  - **facilitem o diagnóstico de problemas de rede; e**
  - **ajudem a encontrar possíveis gargalos de funcionamento**

Apresentação do problema - 1 de 6

- **A rede do MPF precisa estar conectada com a Internet para uso de recursos como *email* e *WWW***
  - **Isso nos torna alvo de *hackers* e outras ameaças**
- **Devido à extensão territorial de nossa WAN, torna-se bastante difícil obter informações centralizadas para detectar, diagnosticar e executar ações em resposta às tentativas de ataque**

Apresentação do problema - 2 de 6

- **Embora existam tipos diferentes de *hosts* no ambiente de rede em cada Unidade, a contratada não realiza nenhuma distinção entre eles**
  - **Exemplificando, um servidor de email (que deve estar acessível externamente) é tratado da mesma maneira que uma máquina de usuário final**

Apresentação do problema - 3 de 6

- Atualmente a contratada não oferece opções para tratamento diferenciado de tráfego.
- Por causa disso, não há como realizar nenhuma reserva de recursos (largura de banda) para aplicações específicas
  - Exemplificando, o download de arquivos por FTP concorre pelos recursos nas mesmas condições do que sistemas corporativos de bancos de dados

Apresentação do problema - 4 de 6

- Quanto à hierarquia de *proxies*
  - Não há como forçar com que a navegação Web seja feita através de *proxies*
  - Existe um esforço considerável para a configuração de browsers
  - Não há ferramentas automatizadas para ativar *proxies* de contingência
  - Existem aplicações que não suportam *proxies*

Apresentação do problema - 5 de 6

- A contratada não disponibiliza o acesso aos roteadores de cada Unidade
  - É difícil determinar se o serviço contratado pelo MPF está sendo prestado em níveis aceitáveis
- O diagnóstico de problemas torna-se complexo
  - Não existe um "ponto de controle" que seja único

Apresentação do problema - 6 de 6

- Existe um volume considerável de emails que poderiam trafegar diretamente entre as Unidades do MPF
  - Sem a necessidade de atravessar o nosso *relay*, que é a máquina mailgw.mpf.gov.br
- É preciso executar antivírus nas mensagens, mas de maneira que não exija nenhuma alteração nos servidores de email já existentes.

Solução proposta

- Um *firewall* baseado em software livre, que possa ser empregado em qualquer Unidade do Ministério Público Federal
- Dada a diversidade de cenários que podem ser encontrados em nossa WAN, esta solução deve poder ser implantada em cada Unidade da maneira menos "invasiva" possível

Descrição da solução proposta

- **Utilizar uma *bridge com firewall* para realizar as seguintes funções:**
  - **operação em nível 2 (*bridge)***
  - **filtro de pacotes *statefull* (iptables)**
  - **detecção de intrusão (snort)**
  - **análise de tráfego (ntop)**
  - **limitação da largura de banda (cbq)**
  - **Proxy transparente para HTTP (squid)**
  - **Redirecionamento de tráfego SMTP (iptables)**
  - **Uso do apt para atualizações automáticas**

Inovação e ineditismo

- De um modo geral, *firewalls* podem ser implementados operando em diferentes níveis de abstração
  - Em *layer* 3 (rede), como roteador
    - O endereço IP do firewall é indicado como *gateway default*
  - Em *layer* 2 (enlace), como *bridge/switch*
    - As interfaces funcionam em modo promíscuo, fazendo o repasse de tráfego entre diferentes domínios de colisão com base nos endereços MAC

Análise das abordagem nível 3

- ***Firewalls*** **implementados como roteador tem como características**
  - **Vantagens**
    - **é possível oferecer contingência através de protocolos como HSRP ou VRRP**
  - **Desvantagens**
    - **é necessário fazer ajustes em <u>todos os clientes</u> para fazê-los usar o endereço IP do *firewall* como *gateway default***
    - **podem ser detectados facilmente**
      - **Através de comandos como o *traceroute***

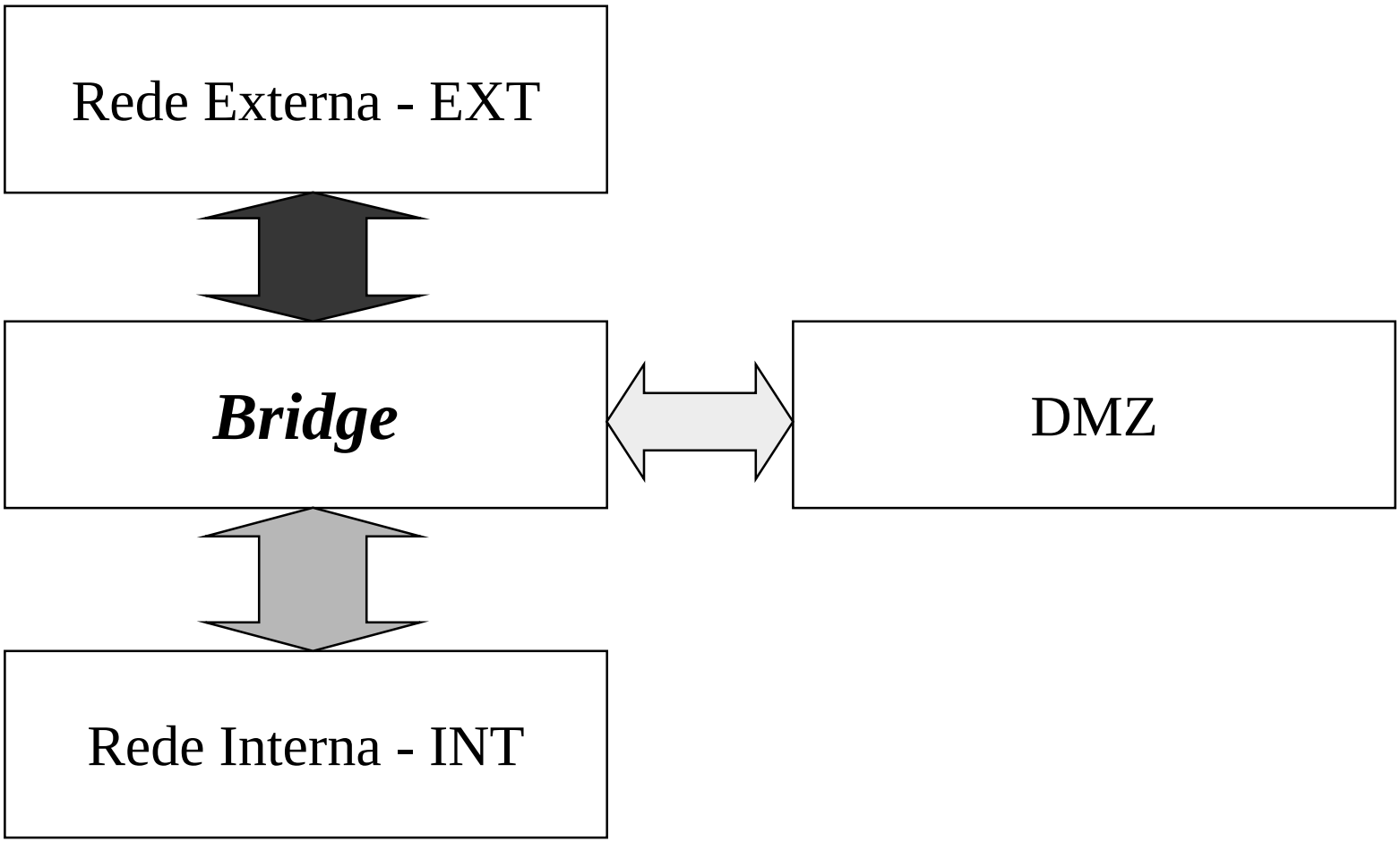
Análise das abordagem nível 2

- ***Firewalls*** **implementados com uma** ***bridge*** **apresentam as seguintes características:**
  - **são "invisíveis";**
  - **havendo problemas com a** ***bridge*****, é possível oferecer contingência através de** ***failover*** **por uma outra unidade, ou removendo-a da topologia**
  - **a sua implantação é extremamente simples, do tipo "caixa-preta"**

Proposta de arquitetura de *firewall*

- Através da *bridge* é possível dividir o ambiente de rede, em cada Unidade, da seguinte maneira:
  - Rede Externa (EXT) - representa todas as máquinas que não sejam desta Unidade
  - DMZ (DMZ) - máquinas da Unidade que precisam estar acessíveis pela Internet - tais como servidores de *email*
  - Rede Interna (INT) - máquinas da Unidade que não devem estar acessíveis externamente

Esquema para arquitetura de firewall



Filtro de pacotes *statefull*

- **Com base nesta organização, é possível controlar o fluxo através da *bridge* em cada um dos sentidos indicados:**

EXT → DMZ
permitir alguns serviços

EXT → INT
não permitir nada

INT → EXT
permitir alguns serviços

INT → DMZ
permitir alguns

DMZ → INT - não permitir nada

DMZ → EXT - permitir alguns serviços

Detecção de intrusão

- A *bridge* é capaz de detectar tentativas de ataque por *hackers* através do *Snort*, uma ferramenta do tipo *NIDS (Network Intrusion Detection System)*
- Através dele, é possível configurar eventos que executem uma ou mais das seguintes ações:
  - registro em um banco de dados
  - envio de mensagens de *email*
  - envio de *traps* SNMP
  - geração de mensagens no *syslog*

Analisador de tráfego - ntop

- Auxilia o diagnóstico de problemas na rede, permitindo fazer uma identificação de possíveis gargalos no funcionamento
- Através do ntop, podemos identificar
  - Serviços mais utilizados (TCP e UDP)
  - Hosts que mais utilizam a rede
  - Tamanho médio de pacotes

  entre várias outras informações

Limitação na largura de banda

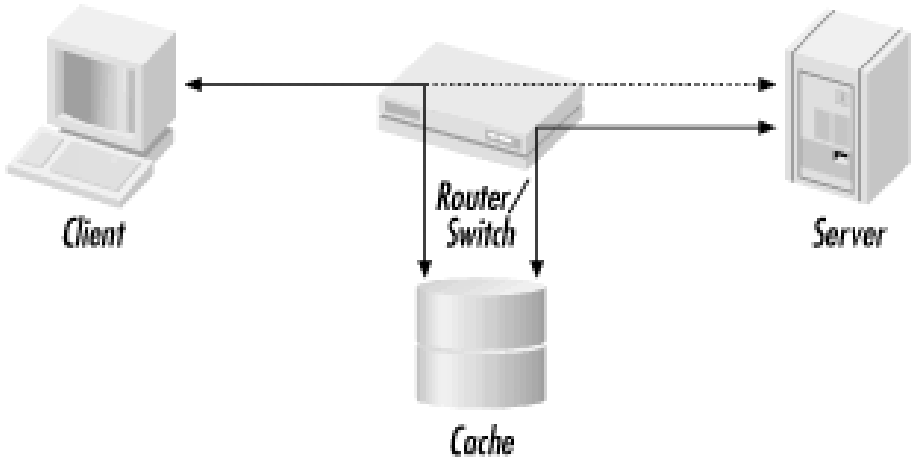
- Alterando-se a disciplina de filas empregada no Linux de FIFO para CBQ, é possível aplicar um tratamento diferenciado para certos tipos de tráfego
- Utilizando endereços IP e números de porta TCP/UDP, limitações podem ser impostas de maneira totalmente transparente para usuários finais

Limitação na largura de banda

- É possível fazer uma divisão que priorize determinadas aplicações
  - Para um link de 256 kbps, por exemplo
    - Navegação www - 150 kbps
    - DNS - 2 Kbps
    - Email - 50 Kbps
    - Oracle - 40 Kbps
    - Demais - 14 kbps
- Havendo ociosidade, a largura de banda excedente em uma dessas classes pode ou não ser compartilhadas com as demais

Proxy transparente

- A bridge pode ser configurada para redirecionar o tráfego HTTP para um *proxy* SQUID, de forma transparente
- A bridge opera como um *interception proxy* (RFC-3040)



Redirecionamento SMTP

- Através da *bridge*, é possível fazer um DNAT e direcionar todo o tráfego de emails para uma máquina do tipo *mail relay*
- No mailrelay, são executadas as seguintes funções:
  - Execução de software antivírus
  - Otimização no roteamento das mensagens que forem direcionadas para Unidades do MPF
    - Sem a necessidade de atravessar a máquina mailgw.mpf.gov.br

Relevância para o interesse público

- Solução extremamente barata, pois baseia-se em Software Livre
- Garante um alto nível de Segurança, necessário devido à demanda de sigilo e confiabilidade das informações jurídicas e administrativas que trafegam na rede do Ministério Público Federal
- Permite a execução de antivírus nos emails recebidos

Efetividade

- Milhares de emails com vírus foram impedidos de ingressar em nossa rede pelo mailrelay com antivírus
- Milhares de situações anômalas foram detectadas pelo Snort
- Milhões de tentativas de conexão com a rede interna das Unidades foram impedidas
- Uso mais eficiente da largura de banda, graças à disciplina de filas CBQ
- Maior segurança na conexão com a Internet, graças ao firewall

Facilidade de reprodução

- A solução pode ser implementada em qualquer distribuição Linux baseada em RPMS.
- O apt pode ser usado para fazer a gerência de configuração, através de pacotes RPM

Recursos necessários

- Hardware
  - Para a bridge com firewall
    - Computador PC compatível
      - 3 placas-de-rede, memória RAM mínima de 64 Mb, (recomendável 128 Mb), unidade de disco com pelo menos 650 Mb
  - Para o mail-relay com antivírus
    - Computador PC compatível, com placa-de-rede
- Software
  - Sistema operacional Linux
  - Software antivírus (Viruscan da McAfee)

Trabalhos futuros

- Este trabalho pode vir a ser estendido quanto aos seguintes aspectos:
  - Empregar outras soluções de software livre (tais como OpenBSD e FreeBSD)
  - Utilizar diferentes distribuições Linux (a versão atual baseia-se no Conectiva Linux)
  - No mailrelay, combater o envio de *spam*
    - Já estão sendo feitos estudos com o SpamAssassin

Grato pela atenção!!!

- Espaço aberto para perguntas
- Maiores informações podem ser obtidas com
  - Leonardo Garcia de Mello
    - Analista de Informática
    - Ministério Público Federal
    - Email lmello@prr4.mpf.gov.br