Protótipo de aplicação web para gerenciamento de Firewall Linux

Acadêmico: Régis Maciel Borscheid
Orientador: Francisco Adell Péricas

Roteiro da apresentação

- Introdução
- Segurança de redes de computadores
- Firewall
- Iptables
- Contexto atual
- Desenvolvimento (requisito, especificação, implementação, validação)
- Conclusão e extensões

Introdução

- Proteção dos recursos da rede
- Manutenção constante das configurações de segurança das redes

Objetivo do trabalho

O objetivo do trabalho é criar um protótipo web para administração de Firewall Linux, facilitando assim a manipulação das regras de Firewall baseadas no Iptables.

Segurança de redes

- Objetivo de proteger as informações
- Garantir a consistência e confiabilidade
- Confidencialidade e isolamento
- Disponibilidade

Política segurança

- Conjunto formal de regras
- Definir o que vai ser protegido
- Eleger conjunto de pessoas responsáveis pela segurança
- Procedimentos pós violação
- Plano de continuidade de negócio

Firewall

- Sistema que impõe uma política de controle de acesso
- Principais tipos de Firewalls:

  - Filtros de pacotes

  - Filtros de pacotes com base no estado da conexão

  - Filtro de pacotes na camada de aplicação

Iptables

- Compões a quarta geração de sistemas de Firewall do Linux
- Incorporada a partir do kernel 2.4
- Ferramenta Front-End para o Netfilter
- Netfilter módulo agregado ao kernel
- Grande flexibilidade na configuração

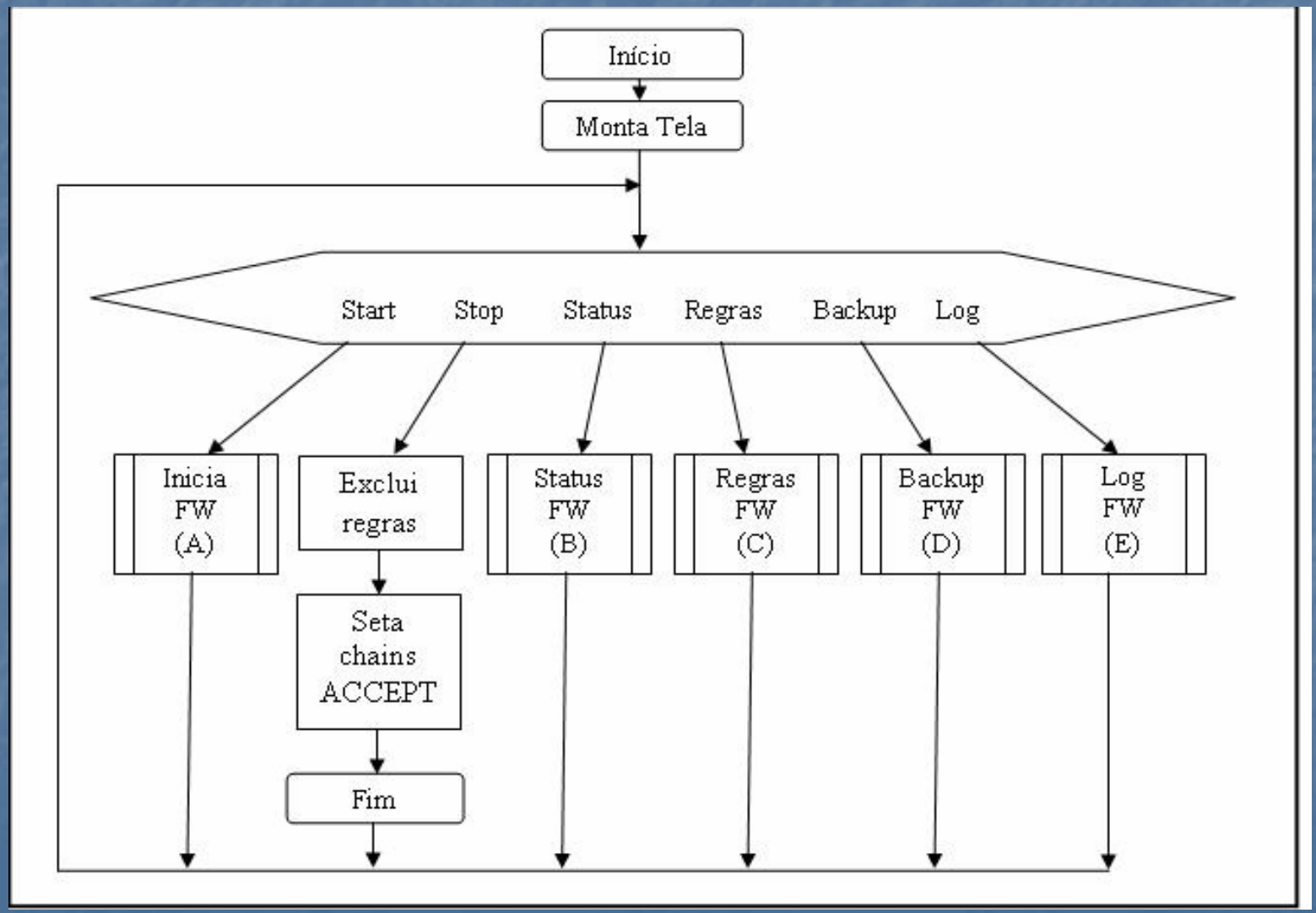
Contexto atual do tema

- Trabalhos correlatos:
  - Guarddog (hosts)
  - StarLink Xfwall (servidores)

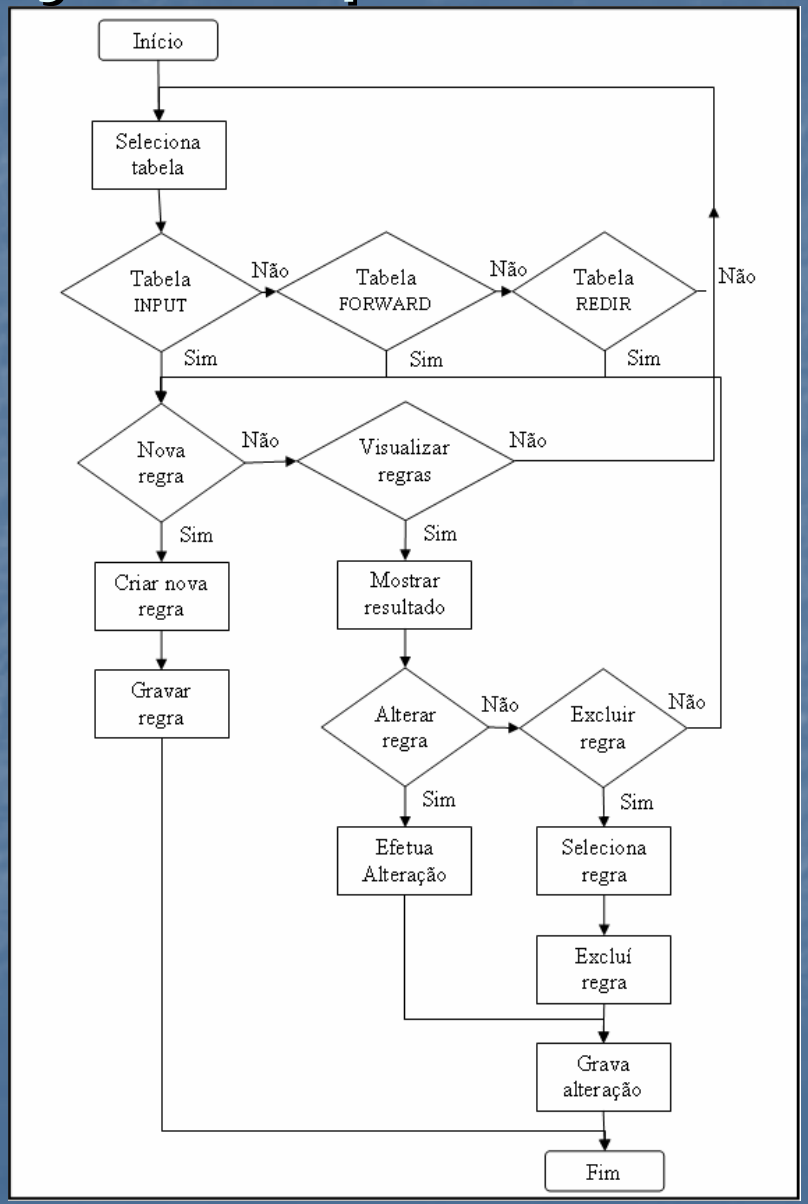
Requisitos principais

- Disponibilizar mecanismo para autenticação de usuários;
- Interface amigável, com exemplos de regras de Firewall;
- Permitir criar, alterar e excluir regras de Firewall
- Analise de logs
- Backup e restauração de regras

Apresentação da especificação



Especificação do processo "Regras" C



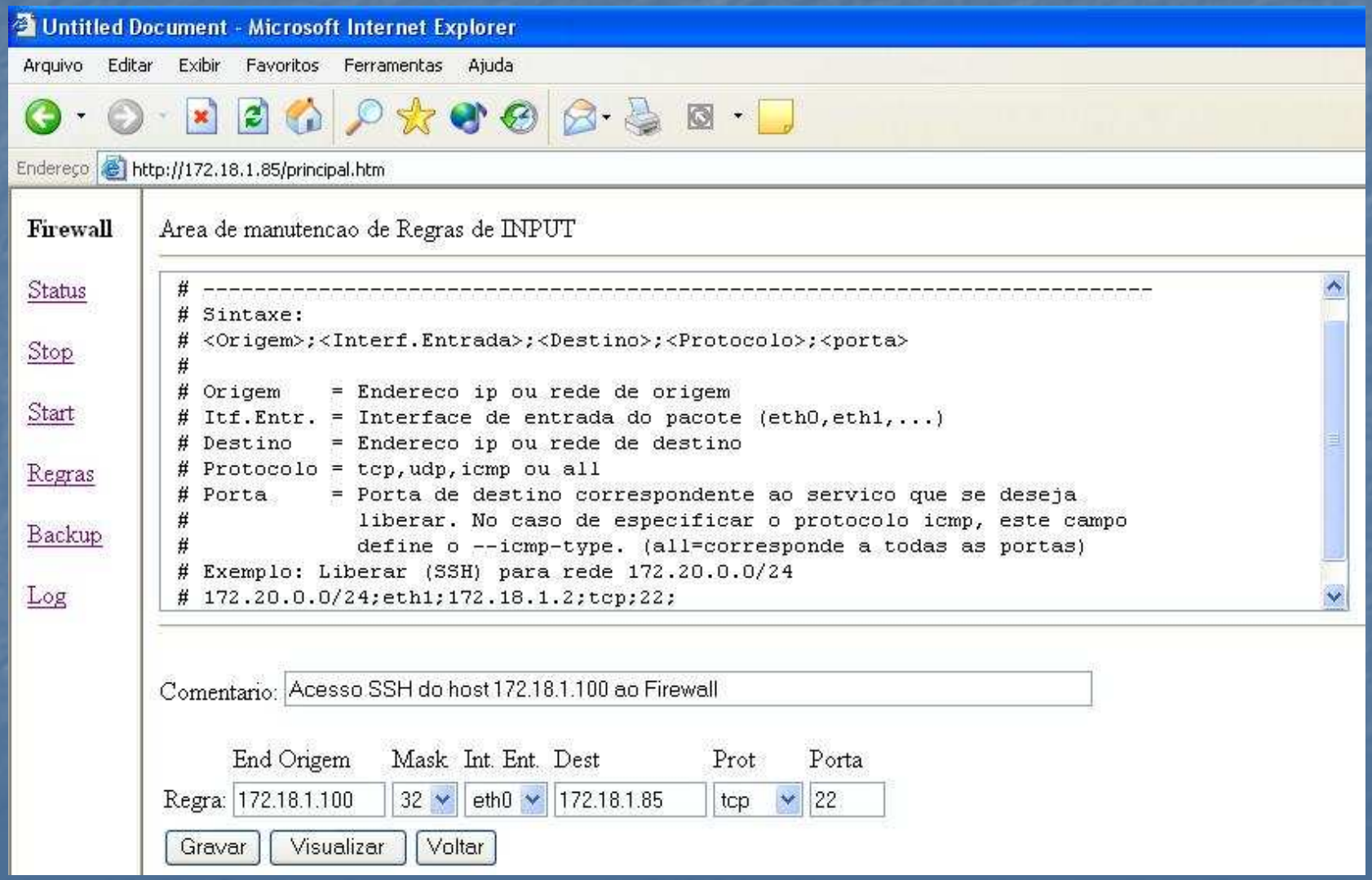
Implementação

- Programação estruturada, utilizando Perl-CGI, Shell Script
- Configuração servidor linux e web
- Autenticação dos usuários MD5 dos servidor Apache

Operacionalidade da implementação

- Aplicação deverá ser instalado em diretório onde somente o super-usuário tem permissão de acesso
- No servidor apache deverá ser feita a configuração do diretório dos Perl-CGI
- Configurado o modo de autenticação no servidor apache

Interface web manutenção regras



Caso de uso criação de regra

- Parâmetros passados pelo administrador

  #liberar ssh para rede 172.18.0.0

  172.18.0.0/16 ; eth0 ; 172.18.1.100 ; tcp ; 22

- Regra Gerada

  /sbin/iptables -A INPUT -s 172.18.0.0/16 -i eth0 -d 172.18.1.100 -p tcp --dport 22 -j ACCEPT

  /sbin/iptables -A OUTPUT -d 172.18.0.0/16 -o eth0 -s 172.18.1.100 -p tcp --sport 22 -j ACCEPT

Trecho de código caso uso apresentado

```
cmd_input="$bin -A INPUT -s $orig"
cmd_output="$bin -A OUTPUT -d $orig"

if [ "$itin" != "any" ]; then
  cmd_input=$cmd_input" -i $itin -d $dest"
  cmd_output=$cmd_output" -o $itin -s $dest"
else
  cmd_input=$cmd_input" -d $dest"
  cmd_output=$cmd_output" -s $dest"
fi
if [ "$prot" != "all" ]; then
 if [ "$prot" = "icmp" ]; then
   cmd_input=$cmd_input" -p icmp"
   cmd_output=$cmd_output" -p icmp"
 elif [ "$port" = "all" ]; then
     cmd_input=$cmd_input" -p $prot"
     cmd_output=$cmd_output" -p $prot"
  else
     cmd_input=$cmd_input" -p $prot --dport $port"
     cmd_output=$cmd_output" -p $prot --sport $port"
 fi
fi
```

Conclusão

- Com o planejamento das etapas do trabalho, definição do cronograma e ferramentas que seriam utilizadas, a conclusão do trabalho foi conseqüência do cumprimento destas atividades
- Monitoração e configuração de regras Firewall Iptables tornou-se simples e sem erros
- Pontos decisivos: especificação, método autenticação, estrutura dos script de Firewall

Extensões

- Desenvolvimento de um módulo de bloqueio de ameaças e ataques
- Desenvolvimento de módulo para integração com uma ferramenta de IDS