Título da aula

Redes Multimídia

Prof. Emerson Ribeiro de Mello

Instituto Federal de Santa Catarina – IFSC
campus São José
mello@ifsc.edu.br

janeiro de 2011

Conteúdo programático

1. Conceitos sobre segurança em redes
2. Conceitos sobre Firewall
3. Projetos de firewall
   - Perímetros de segurança
4. Códigos embutidos

Conteúdo programático

Propriedades básicas de segurança

A segurança está fundamentada sobre três propriedades básicas:

- **Confidencialidade** – A informação só deve ser revelada para usuários autorizados a acessá-la
- **Integridade** – A informação não poderá ser modificada, intencionalmente ou acidentalmente, por usuários que não possuam direito para tal
- **Disponibilidade** – O uso do sistema não poderá ser negado, de forma maliciosa, aos usuários autorizados

Vulnerabilidades, ameaças e ataques

- **Vulnerabilidades** – Um erro de programação, erro na configuração ou mesmo um erro de operação

Vulnerabilidades, ameaças e ataques

- **Vulnerabilidades** – Um erro de programação, erro na configuração ou mesmo um erro de operação
- **Ameaças** – possível ação que, se concretizada, poderá produzir efeitos indesejados ao sistema, comprometendo as propriedades básicas de segurança

Vulnerabilidades, ameaças e ataques

- **Vulnerabilidades** – Um erro de programação, erro na configuração ou mesmo um erro de operação
- **Ameaças** – possível ação que, se concretizada, poderá produzir efeitos indesejados ao sistema, comprometendo as propriedades básicas de segurança
- **Ataques** – é a concretização de uma **ameaça**, explorando alguma **vulnerabilidade** do sistema, executado por algum intruso, de forma maliciosa ou não

Medidas de segurança

- **Prevenção** – Significa que um ataque irá falhar.
  - Implica no uso de mecanismos de segurança que não podem ser ignorados – Ex: uso de senhas

Medidas de segurança

- **Prevenção** – Significa que um ataque irá falhar.
  - Implica no uso de mecanismos de segurança que não podem ser ignorados – Ex: uso de senhas
- **Detecção** – Quando um ataque não pode ser prevenido
  - informa que um ataque está em andamento ou que ocorreu
    - Ex: monitoramento das tentativas de logins, Sistema de detecção à Intrusão (*IDS*)

Medidas de segurança

- **Prevenção** – Significa que um ataque irá falhar.
  - Implica no uso de mecanismos de segurança que não podem ser ignorados – Ex: uso de senhas
- **Detecção** – Quando um ataque não pode ser prevenido
  - informa que um ataque está em andamento ou que ocorreu
    - Ex: monitoramento das tentativas de logins, Sistema de detecção à Intrusão (*IDS*)
- **Recuperação** – Existem duas formas
  - Interrompe o ataque e repara o dano
    - Ex: cópia de segurança de um arquivo que foi excluído
  - Repara o dano com o sistema em funcionamento e com o ataque em andamento
    - Ex: tolerância à falta

Conteúdo programático

Firewall

Definição convencional: Parede corta fogo

Dispositivo feito de material a prova de fogo para evitar que o fogo se espalhe de uma parte do edifício para outra

Firewall

Definição convencional: Parede corta fogo

Dispositivo feito de material a prova de fogo para evitar que o fogo se espalhe de uma parte do edifício para outra

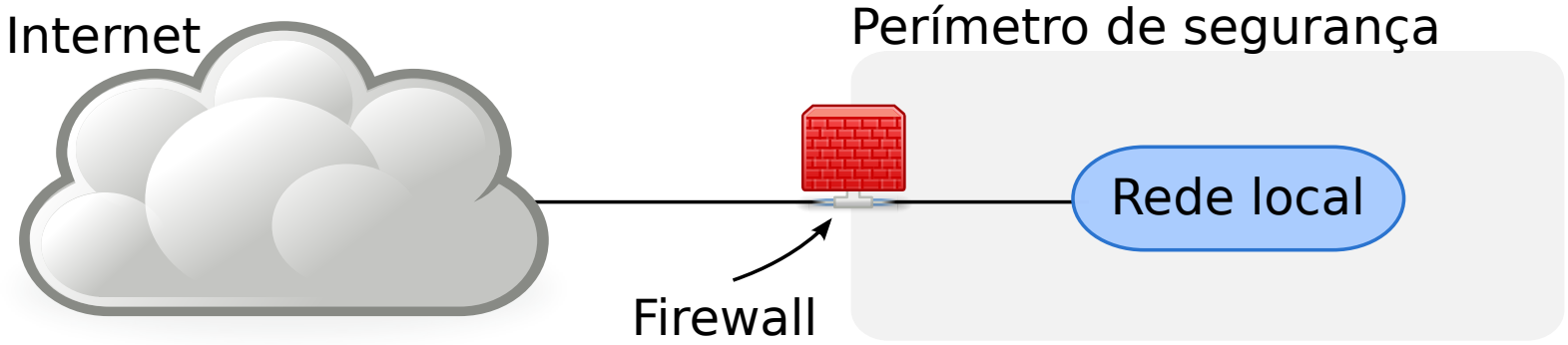
Definição para sistemas computacionais

Ponto de controle que mantém acessos não autorizados fora do perímetro de segurança, ao mesmo tempo possibilita acesso aos sistemas externos

- Atua como uma barreira de segurança entre a rede interna e o mundo exterior
- Evita que potenciais vulnerabilidades de serviços sejam exploradas
  - Nenhum software complexo é 100% seguro
- Pode ser classificado como firewall de **máquina** ou de **rede**

Firewall de rede

- **Perímetro de segurança:** rede local da organização
- Todo o tráfego de dentro para fora, e vice-versa, deverá passar pelo *Firewall*
- Somente o tráfego autorizado, definido pela política de segurança local, deverá ter permissão para passar
- O próprio *Firewall* deverá ser imune a invasões
  - Implica na utilização de um sistema confiável, com um sistema operacional seguro e rodando um conjunto mínimo de serviços

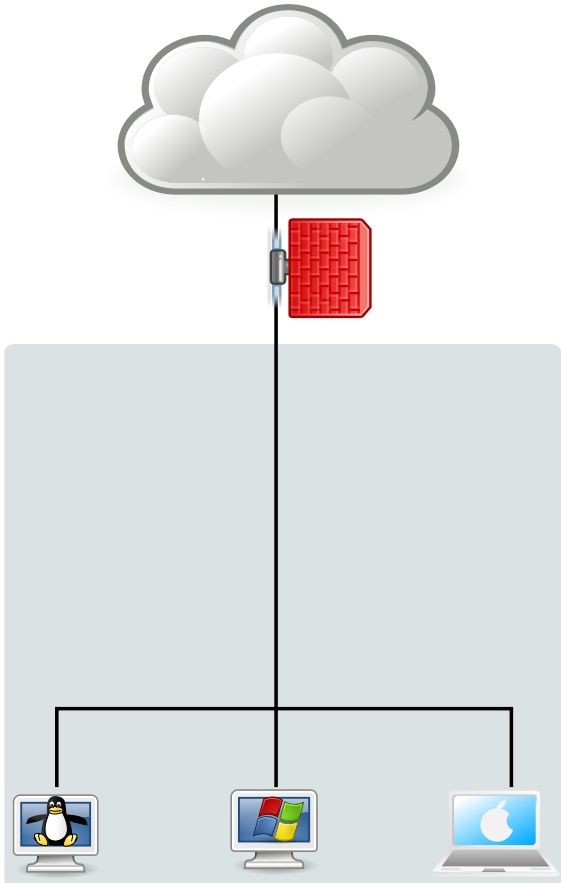


Conteúdo programático

1. Conceitos sobre segurança em redes
2. Conceitos sobre Firewall
3. Projetos de firewall
   - Perímetros de segurança
4. Códigos embutidos

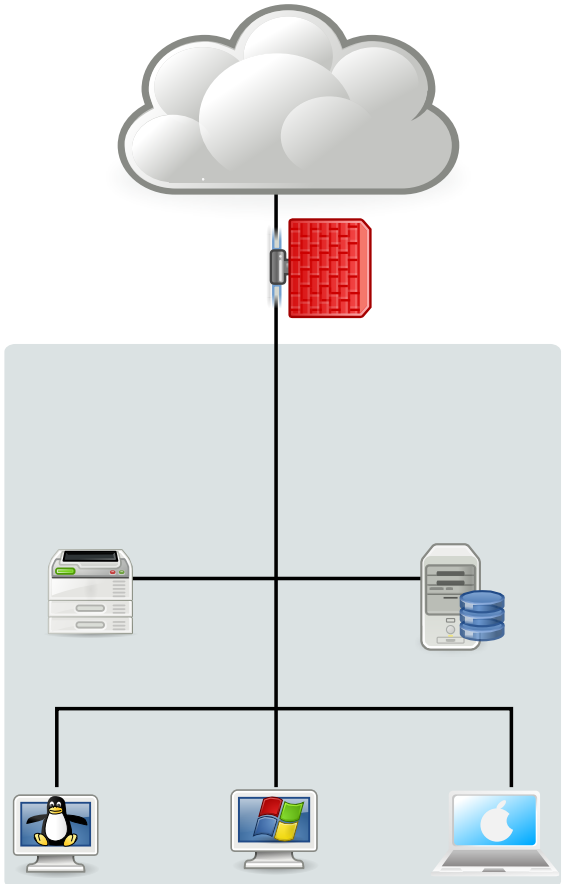
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas



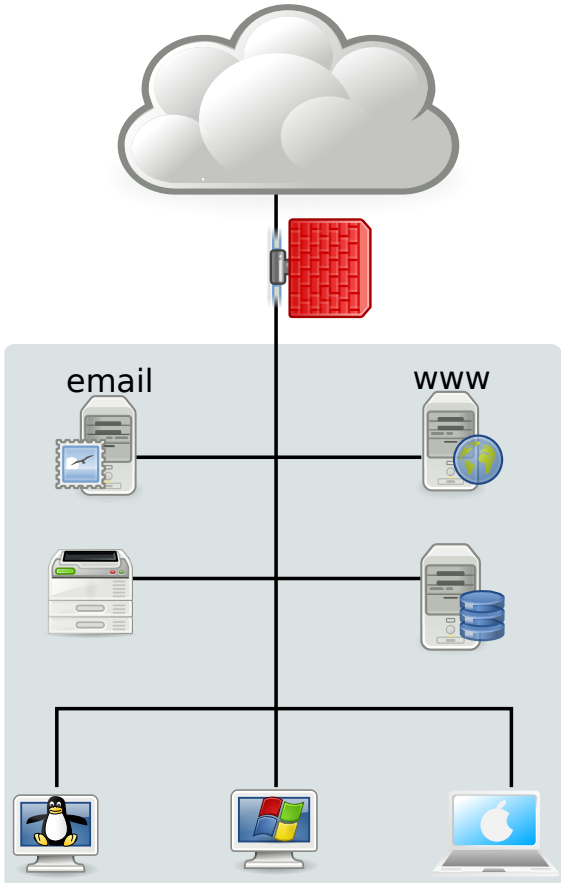
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.



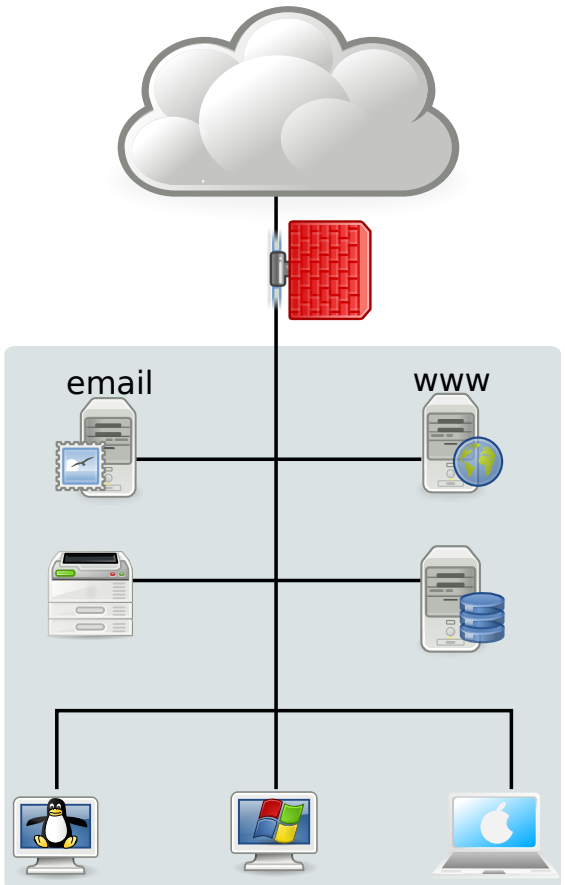
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.
3. **Estações, servidores internos e externos**
   - WWW, SMTP, DNS, POP, IMAP, etc.



Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.
3. **Estações, servidores internos e externos**
   - WWW, SMTP, DNS, POP, IMAP, etc.



Como oferecer serviços externos sem que isto resulte em ameaças para a rede interna?

Conteúdo programático

1. Conceitos sobre segurança em redes
2. Conceitos sobre Firewall
3. Projetos de firewall
   - Perímetros de segurança
4. Códigos embutidos

Código em Java

- Lembre-se de colocar a opção **fragile** no frame.

```
1  public class Ola{
2    public void olaMundo(){
3       System.out.println("Ola mundo!");
4    }
5  }
```

Código em Shell Script

- Lembre-se de colocar a opção **fragile** no frame.

```
6  echo "ola mundo"
```

Bibliografia


William Stallings
Network Security Essentials.
Prentice Hall, 2000.


Matt Bishop
Computer Security – Art and Science.
Addison Wesley, 2003.


Charles P. Pfleeger and Shari Lawrence Pfleeger
Security in Computing.
Prentice Hall, 2006.


B. Fraser
Site Security Handbook.
RFC 2196, 1997.