

# INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

## Firewalls e Web Proxies Parte 1

# ROTEIRO

- Introdução
- O que é?
- Principais características
- Funções do Firewall
- Tipos de Firewalls

# Introdução

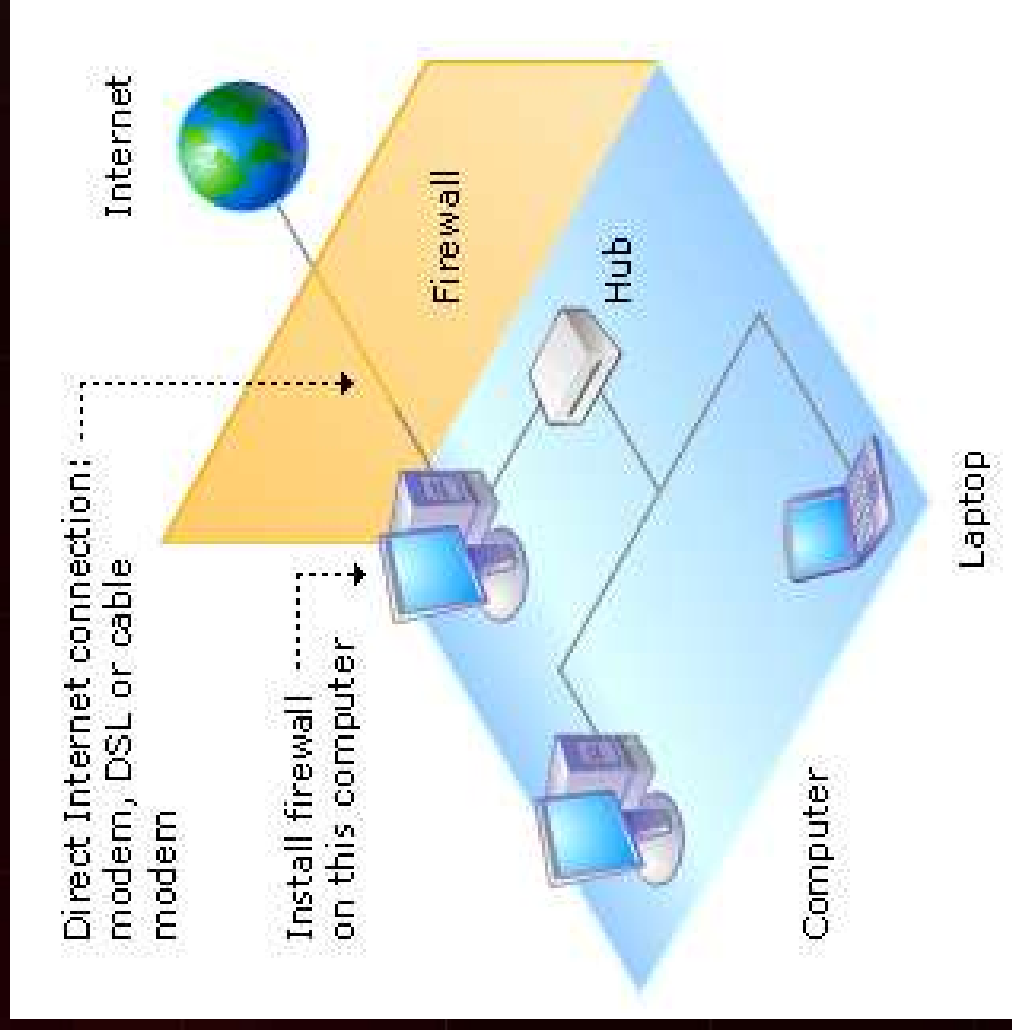
## Motivação

- Alto índice de ataques a redes
- Necessidade de controle de tráfego
- Garantir integridade aos serviços
- Alta demanda dos serviços da Internet

## Firewall significa Pareda **Corta Fogo**

- Regula tráfego entre redes existentes
- Impede a propagação de dados nocivos

# O que é?



# Principais Características

- Toda solicitação chega ao Firewall
- Somente tráfego autorizado passa pelo Firewall
- O próprio Firewall deve ser imune à penetração
- Bloqueia o recebimento de dados baseados em uma fonte ou destino
- Bloqueia o acesso a dados baseados em uma fonte ou destino
- Bloqueia dados baseados em conteúdo
- Permite conexões com uma rede interna
- Reporta o tráfego na rede e as atividades do Firewall

# Firewall

- O que ele pode fazer?
  - É um foco para a tomada de decisões
  - Pode ser usado como um ponto de partida para a política de segurança
  - Pode gravar requisições
  - Limita a exposição da rede
- O que ele não pode fazer?
  - Proteger uma rede contra usuários internos
  - Proteger uma rede contra conexões que não passam por ele
  - Proteger contra ameaças completamente novas

# O Básico de Firewalls

- Deve ter pelo menos as 4 funções a seguir:
- Filtragem de pacotes
- NAT (Network Address Translation)
- Proxy de Aplicação
- Monitoramento e registro

# O Básico de Firewalls

- Estratégias gerais:
  - Allow-All
  - Deny-All

Uma boa opção é misturar ambas!



## O Básico de Firewalls

*Deny network traffic on all IP ports.*

*Except, allow network traffic on port 80 (HTTP).*

*Except, from all HTTP traffic, deny HTTP video content.*

*Except, allow HTTP video content for members of the Trainers group.*

*Except, deny Trainers to download HTTP video content at night.*

# Tipos de Firewalls

- Há 2 tipos principais
  - Filtro de Pacotes
  - Servidores Proxy

# Tipos de Firewalls

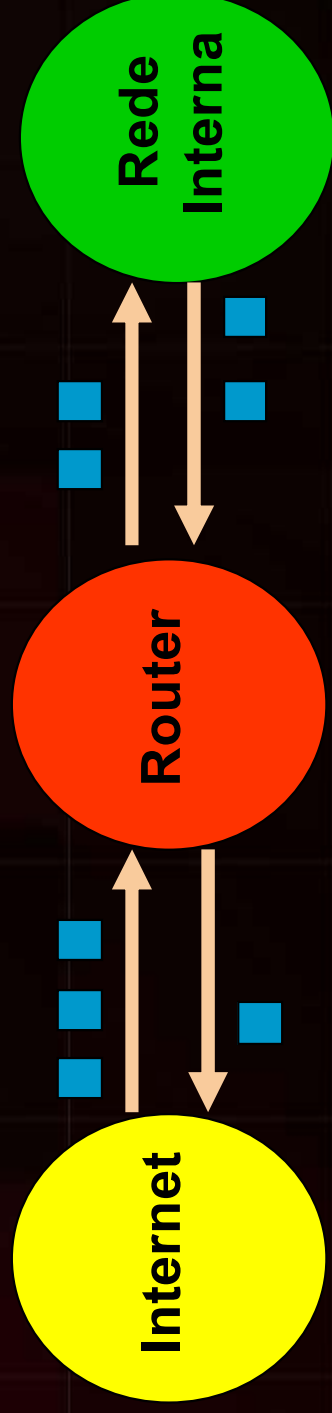
- **Filtro de Pacotes**
- **Filtrar = peneirar, separar**
  - Controle do tráfego que entra e sai
  - Incrementa a segurança
  - Transparente aos usuários
  - Grande variedade no mercado

# Tipos de Firewalls

- **Filtro de Pacotes**
- **As regras dos filtros contêm:**
  - Endereço IP de origem
  - Endereço IP de destino
  - Protocolos TCP, UDP, ICMP
  - Portas TCP ou UDP origem
  - Portas TCP ou UDP destino
  - Tipo de mensagem ICMP

# Tipos de Firewalls

- Filtro de Pacotes



Roteador com Filtro de Pacotes

# Tipos de Firewalls

- **Filtro de Pacotes**
  - Filtragem por adaptador de rede – vantagem ao administrar
- Principais problemas do filtro:
  - ***IP Spoofing***
  - **Serviço troca de porta**

# Tipos de Firewalls

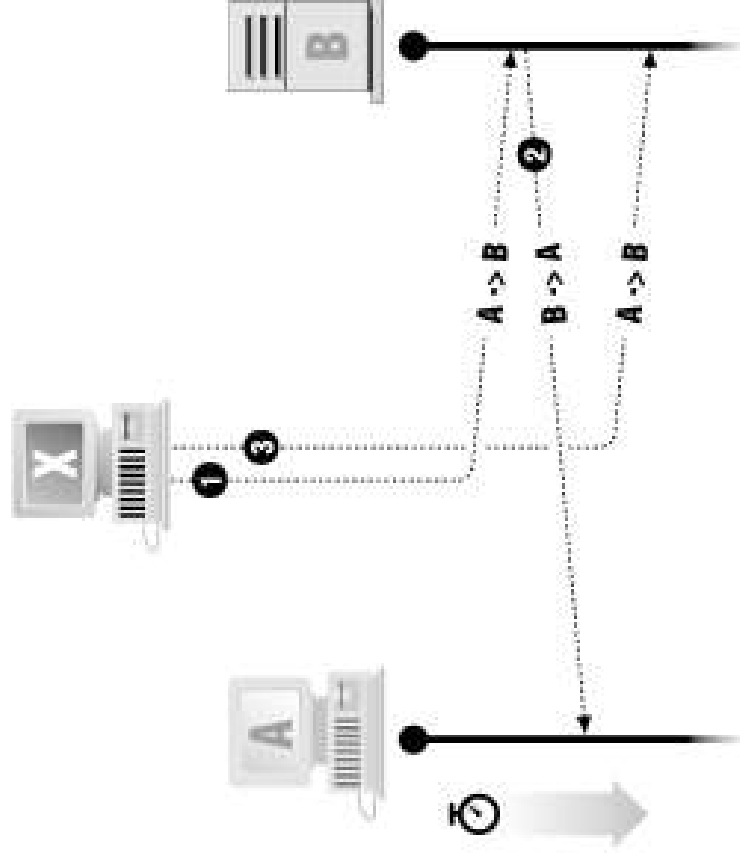
- **Filtro de Pacotes**
  - Não tratam protocolos da camada de aplicação
  - Não são uma solução única – é um complemento
  - Causam atraso no roteamento

# Tipos de Firewalls

- Filtro de Pacotes
- Problemas
- IP Spoofing

*Spoofing is a complex attack we are likely to see more of in the future.*

- 1 X convinces B that it's A
- 2 B responds with packet to A, acknowledging A's session number and specifies its own.
- 3 X takes another packet that acknowledges session number.





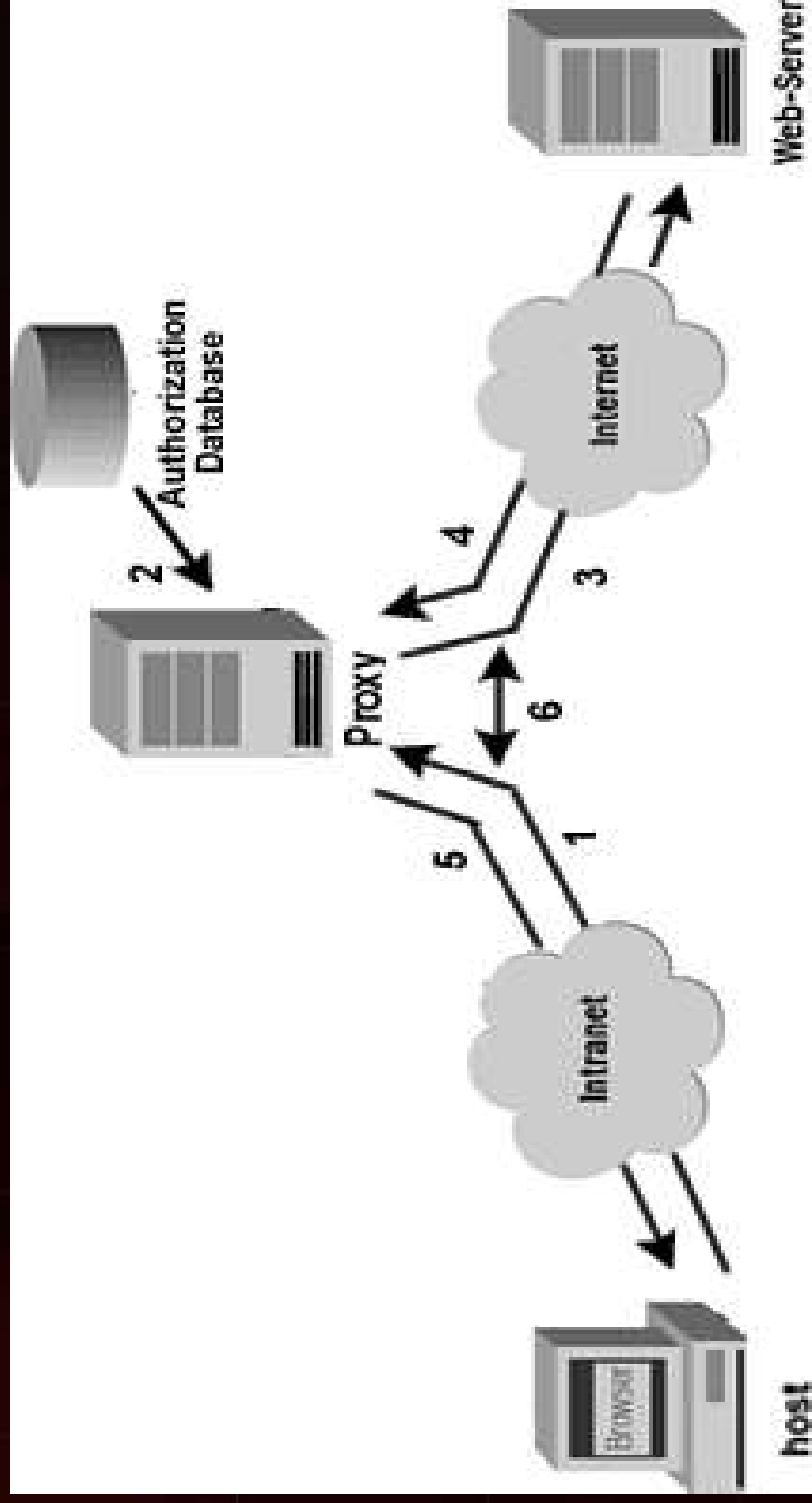
# Tipos de Firewalls

- **Proxy**

- Assumem requisições de usuários de uma rede
- Atuam em nome do cliente de uma forma transparente
- Não permitem que pacotes passem diretamente entre cliente e servidor

# Tipos de Firewalls

- Proxy



# Tipos de Firewalls

- Proxy
  - Métodos de utilização:
    - Método da Conexão Direta
    - Método do Cliente Modificado
    - Método do Proxy Invisível

# Tipos de Firewalls

- Proxy

- Vantagens de utilização do proxy:

- Permite ao usuário acesso direto aos serviços na Internet
    - Possui bons mecanismos de log
    - Provê uma ótima separação entre as redes

# Tipos de Firewalls

- **Proxy**
- Desvantagens do proxy:
  - Cada serviço possui o seu servidor proxy
  - Deve ser desenvolvida uma nova aplicação para cada novo serviço
- Existem alguns serviços inviáveis

# Tipos de Firewalls

- **Firewalls x Proxy**
- Tomada de decisões:
  - Servidor proxy toma decisões baseado em informações fornecidas pelo serviço
  - Filtro de pacotes utiliza o cabeçalho do pacote.

# Tipos de Firewalls

## • Firewalls x Proxy

- Tomada de decisões:
  - Servidor proxy toma decisões baseado em informações fornecidas pelo serviço
  - Filtro de pacotes utiliza o cabeçalho do pacote.
- Desempenho:
  - Filtro de pacotes possui uma vantagem por estar em nível mais baixo
- Auditoria:
  - Servidor proxy possui vantagem por permitir auditoria sobre controle do tráfego

# REFERÊNCIAS

Zwicky, E; Cooper, Simon – Construindo Firewalls para a Internet  
O'Reilly, 2000

Internet Firewalls – UFRGS -  
<http://penta.ufrgs.br/redes296/firewall/fire.html>



# INFRAESTRUTURA PARA SISTEMAS DE SOFTWARE

## Firewalls e Web Proxies Parte 1