AULA Nº 12
Infraestrutura Comp. Alto Desempenho e Sist. Distribuídos

Firewall

Julio Cezar Estrella
ICMC-USP - 2019

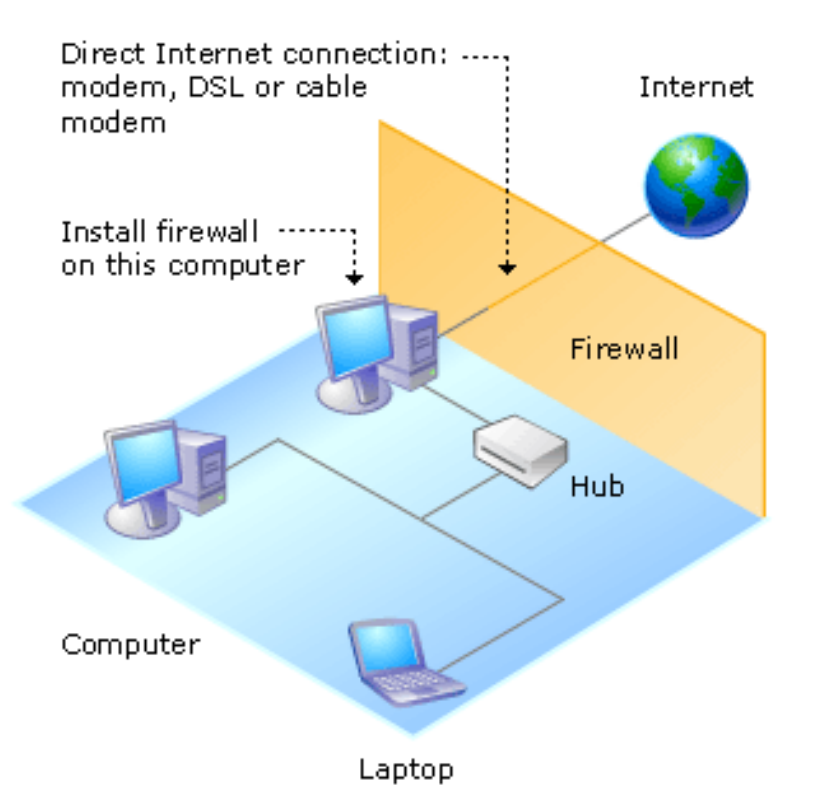
Introdução

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

O que é?

- Firewall significa Parede Corta Fogo
- Regula tráfego entre redes existentes
- Impede a propagação de dados nocivos

O que é?


Direct Internet connection: modem, DSL or cable modem
Internet
Install firewall on this computer
Firewall
Hub
Computer
Laptop

O que um Firewall 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 um Firewall não pode fazer?

- Proteger uma rede contra usuários internos
- Proteger uma rede contra conexões que não passam por ele
- Proteger contra ameaças completamente novas
- Proteger contra vírus

Principais Características

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

O Básico de Firewall

- **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 Firewall

- **Estratégias gerais:**
  - **Allow-All**
  - **Deny-All**
  -
  - **Uma boa opção é misturar ambas!**

O Básico de Firewall

- ***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 Firewall

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

Tipos de Firewalls

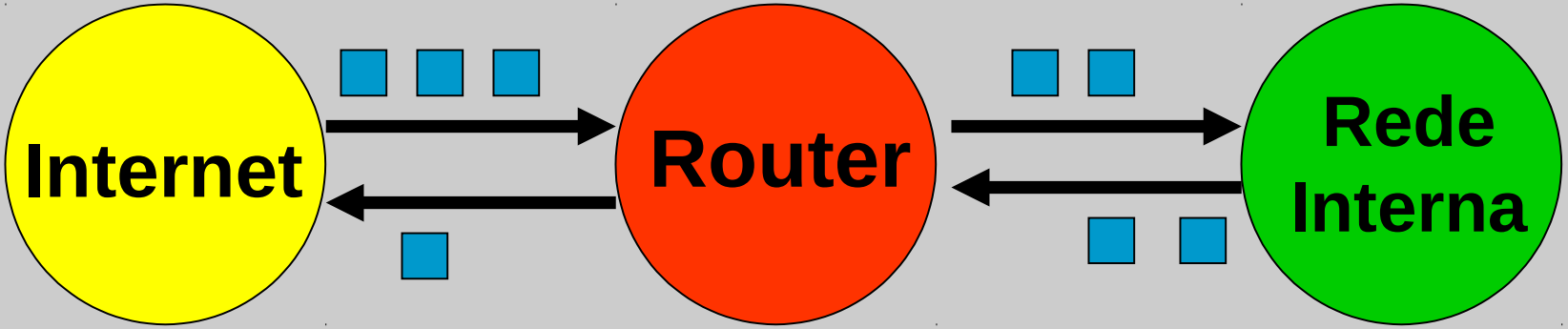
- **Filtro de Pacotes**
  - **Filtrar = peneirar, separar**
    - Controle do tráfego que entra e sai
    - Incrementa a segurança
    - Transparente aos usuários
    - Grande variedade no mercado

Tipos de Firewalls

- **Filtro de Pacotes**
  - **As regras dos filtros contém:**
    - 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

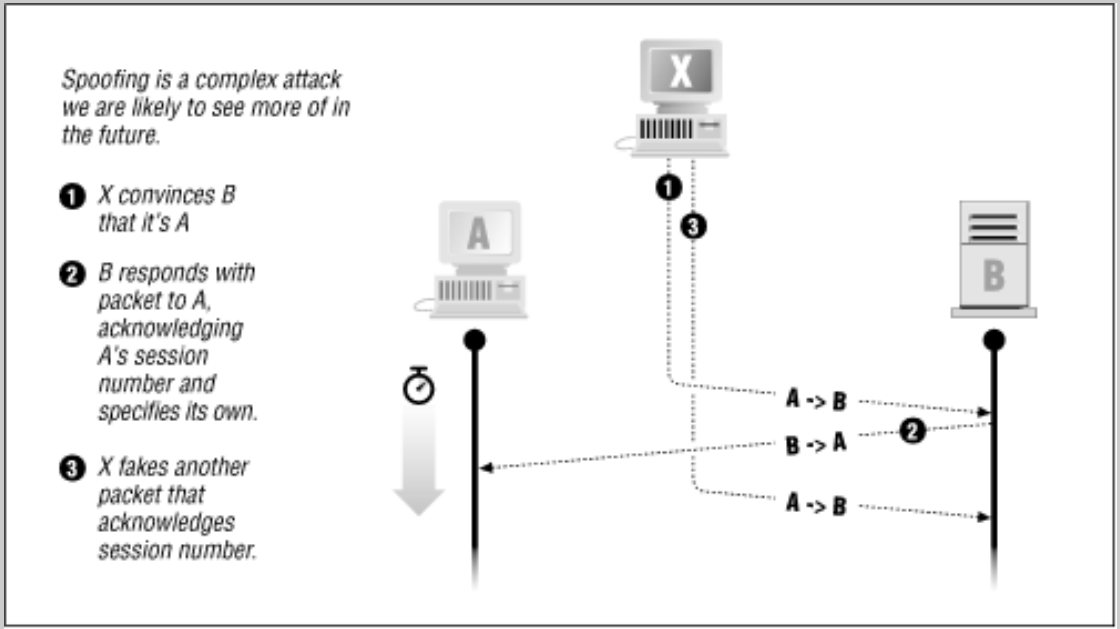
- **Filtro de Pacotes**
  - Filtragem por adapatador de rede – vantagem ao administrador
  - Principais problemas do filtro:
    - ***IP Spoofing***
    - **Serviço troca de porta**

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

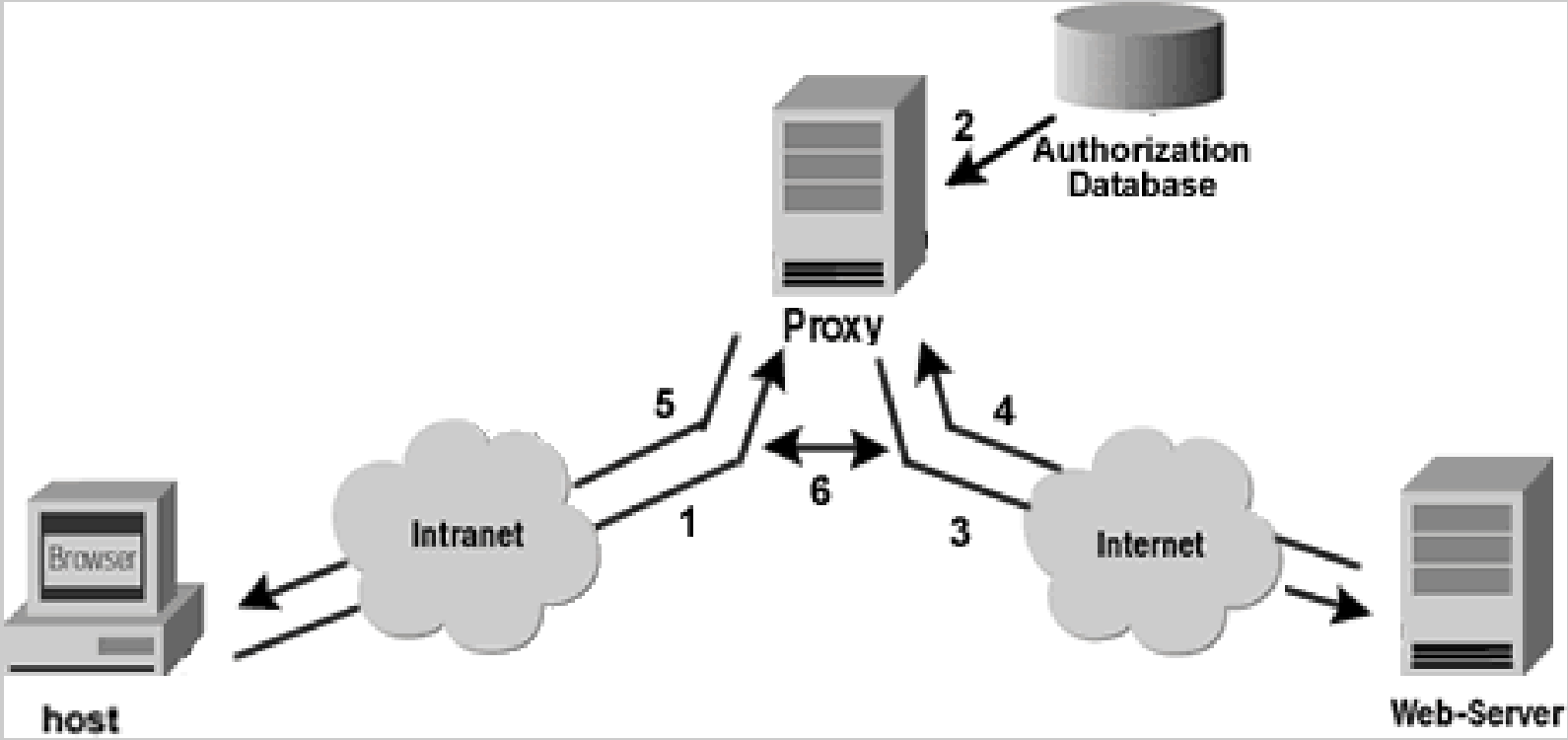
- **Filtro de Pacotes**
  - ***IP Spoofing***
    -



Servidores 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

Servidores Proxy



Servidores Proxy

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

Servidores 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**

Servidores 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**

Servidor Proxy x Filtro de Pacotes

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

Servidor Proxy x Filtro de Pacotes

- **Desempenho:**
  - **Filtro de pacotes possui uma vantagem por estar em nível mais baixo**
- **Auditoria:**
  - **Servidor proxy possui vantagem por permitir auditoria sobre o controle do tráfego**

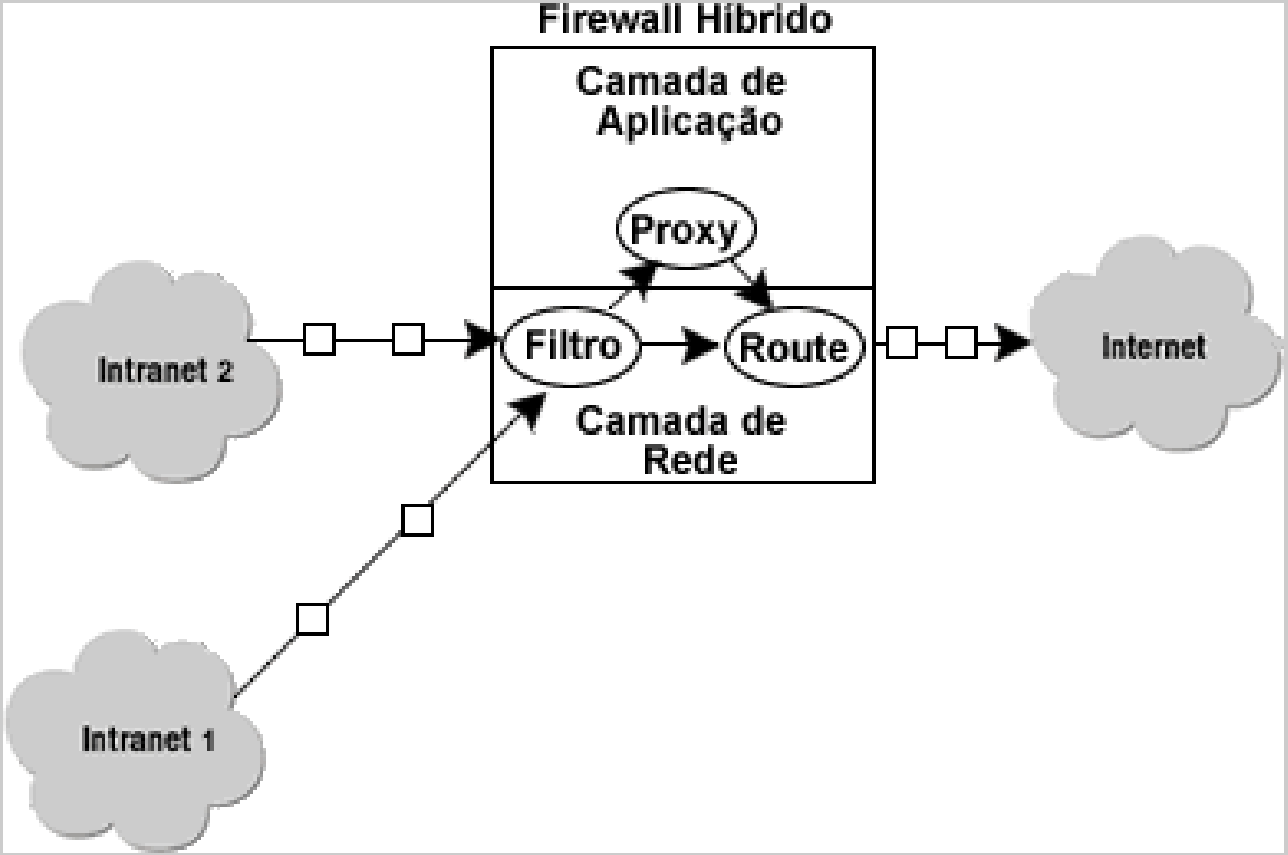
Outros Tipos de Firewalls

- **Há outros tipos de firewalls alternativos:**
  - ***Firewalls* Híbridos**
  - ***Firewalls Bastion Hosts***

Outros Tipos de Firewalls

- **Firewalls Híbridos**
  - **A maioria dos *firewalls* podem ser classificados como Filtro de Pacotes ou Servidores *Proxy***
  - **Outros tipos de *firewalls* oferecem uma combinação entre estes dois**

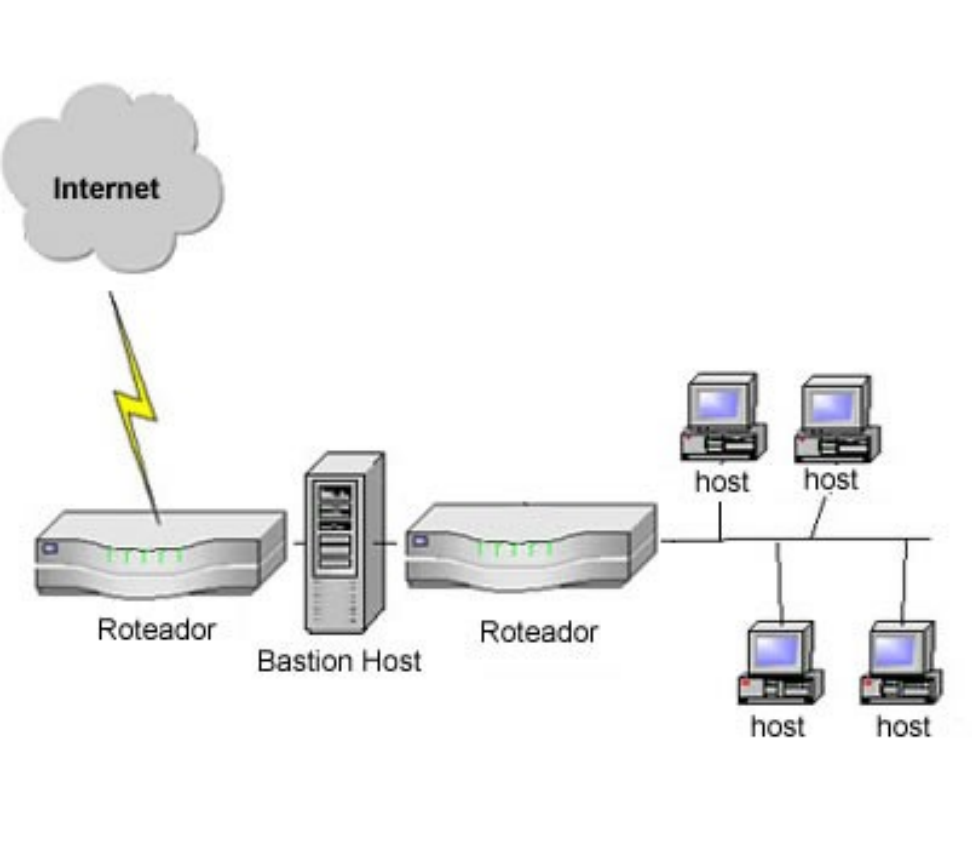
Outros Tipos de Firewalls



Outros Tipos de Firewalls

- **Bastion Host**
  - **Hosts fortemente protegidos**
  - **Único computador da rede que pode ser acessado pelo lado de fora do firewall**
  - **Pode ser projetado para ser um servidor Web, servidor FTP, dentre outros**

Outros Tipos de Firewalls



Outros Tipos de Firewalls

- **Bastion Host**
  - **Honey Pot**
    - **Chamariz para crackers**
    - **Função de coletar dados de tentativas de invasão**
    - **Ferramentas de registros de logs são matidas o mais seguro possível**

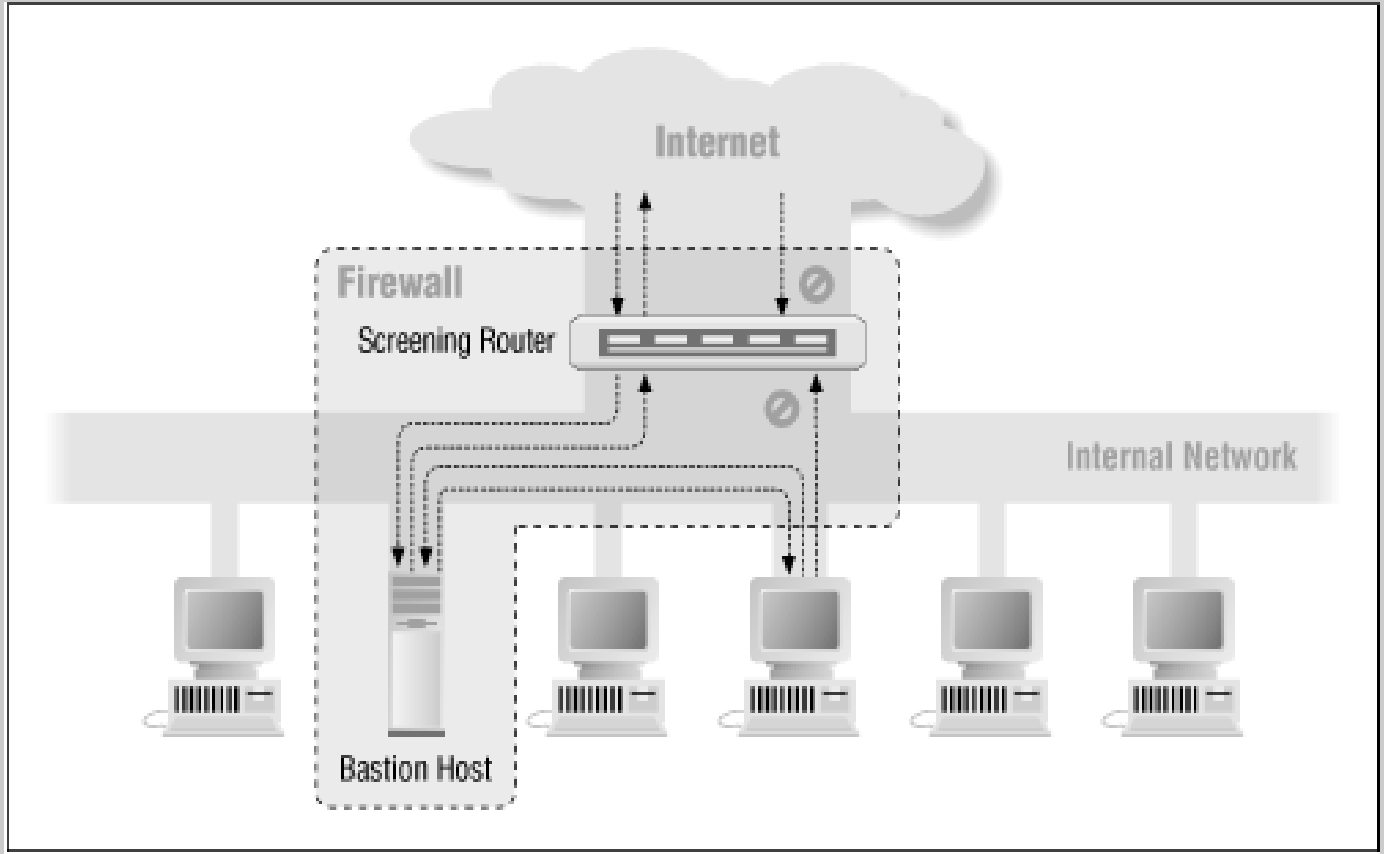
Arquiteturas de Firewalls

- **Principais:**
  - ***Screened host***
  - ***Screened subnet***
- ***Screened* = proteger, peneirar, investigar**

Arquiteturas de Firewalls

- **Screened Host**
  - **Sem sub-rede de proteção**
  - **Elementos = 1 roteador e 1 *bastion host***
  - **Rede protegida sem acesso direto ao "mundo"**
  - ***Bastion host* realiza o papel de procurador – só ele passa pelo roteador**

Arquiteturas de Firewalls



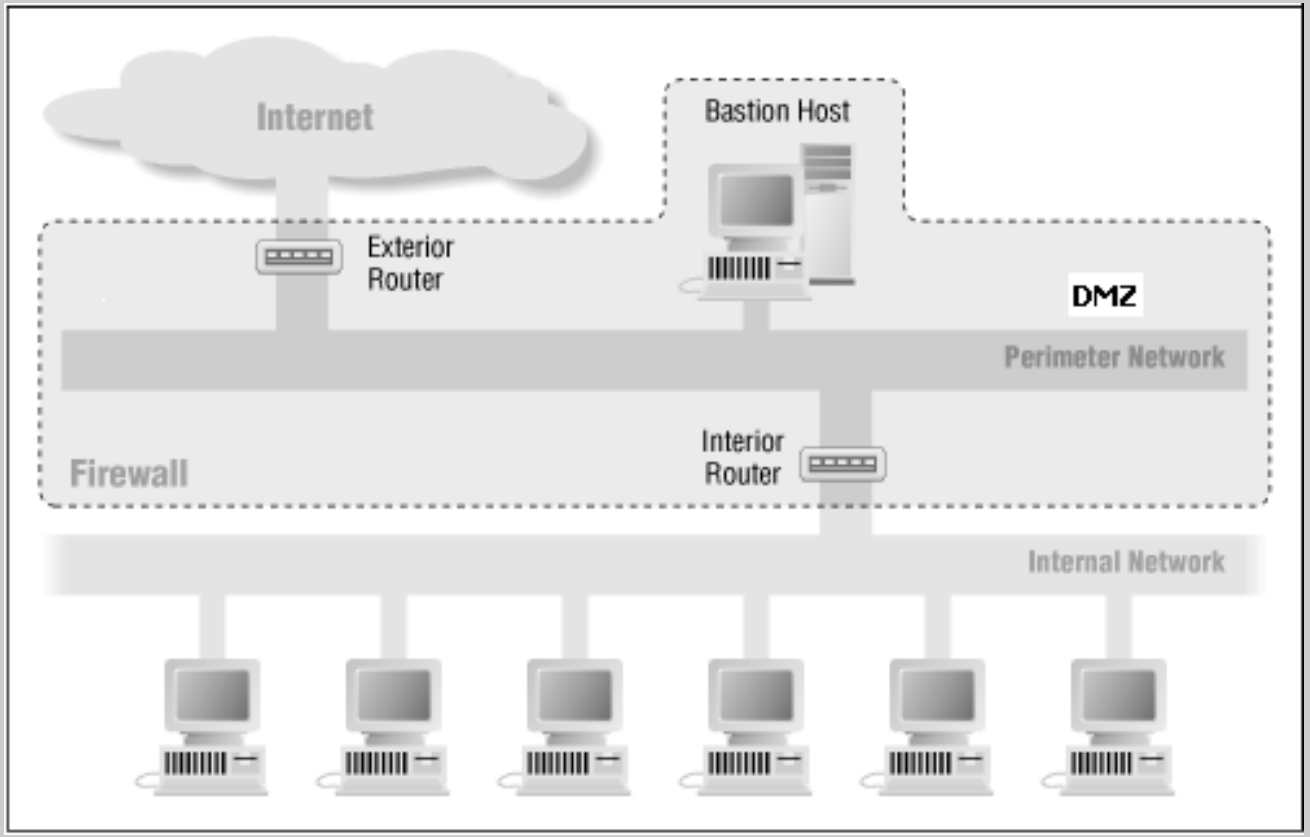
Arquiteturas de Firewalls

- **Screened Subnet**
  - **Apresenta múltiplos níveis de redundância**
  - **É a mais segura**
- **Componentes:**
  - **Roteador externo**
  - **Subrede intermediária (DMZ)**
  - **Bastion Host**
  - **Roteador Interno**

Arquiteturas de Firewalls

- **Screened Subnet**
- **O que é a DMZ (De Militarized Zone)?**
  - **Sub-rede entre a rede externa e a protegida. Proporciona segurança.**
- **Rede interna somente têm acesso ao *Bastion Host***
- **Somente a subrede DMZ é conhecida pela Internet**

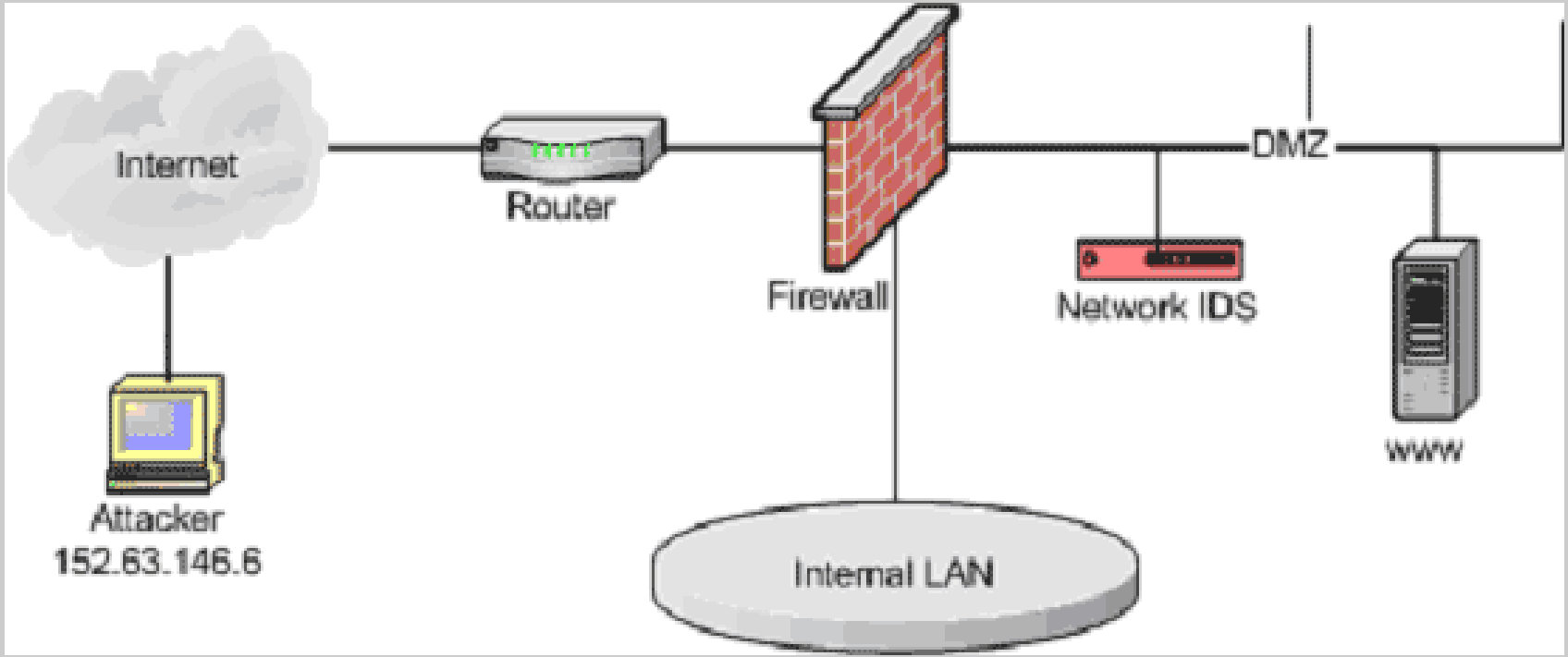
Arquiteturas de Firewalls



Sistema de Detecção de Intrusão

- **Solução complementar ao firewall**
- **Softwares capazes de detectar atividades suspeitas**
- **Utiliza-se de padrões conhecidos de comportamento de intrusos**
- **Podem analisar o tráfego interno, externo e entre eles**
- **Tipos de análise de tráfego**
  - **Detecção de assinaturas**
  - **Detecção Comportamento**
  - **Detecção de anomalias de protocolo**

Sistema de Detecção de Intrusão



Sistema de Detecção de Intrusão

- Detecção de assinaturas
  - procura de padrões específicos
  - desvantagem : necessidade de conhecimento prévio do padrão
- Detecção Comportamento
  - Cada rede tem determinada característica (estatística)
  - Procura alterações nestas característica (pico)
  - Desvantagem - método não muito eficaz
- Detecção de anomalias de protocolo
  - Análise do pacote com seu padrão

Monitoramento e Registro

- **Reportar Uso**
- **Detecção de intruso**
- **Descobrir método de ataque**
- **Evidências Legais**
- **Armazenar em outro PC ou em dispositivo de gravação única**

Conclusão

- **Importante ferramenta na proteção**
- ***Firewall* não deve ser o único componente da política de segurança**

Atividade

- **Disponível no Moodle conforme consta no cronograma da disciplina**

Referências

- **Zwicky, E; Cooper, Simon – Contruindo Firewalls para a Internet.** O´Reilly, 2000
- **Internet Firewalls – UFRGS -** http://penta.ufrgs.br/redes296/firewall/fire.html

Próxima Aula

- VPN