FIREWALLS

Trabalho Desenvolvido para a disciplina
Adminstração e Gerenciamento de Redes pelos alunos:

Ubiratan F. Soares
Paulo Ricardo Chagas Diniz
Ulisses F. Soares

São Carlos, 04 de dezembro de 2009

AGENDA

- Introdução
- Histórico e Evolução
- Classificação de Firewalls
- Estudo de Caso : IPFW
- Vantagens e Limitações
- Perspectivas Futuras
- Referências

O QUE É UM FIREWALL?

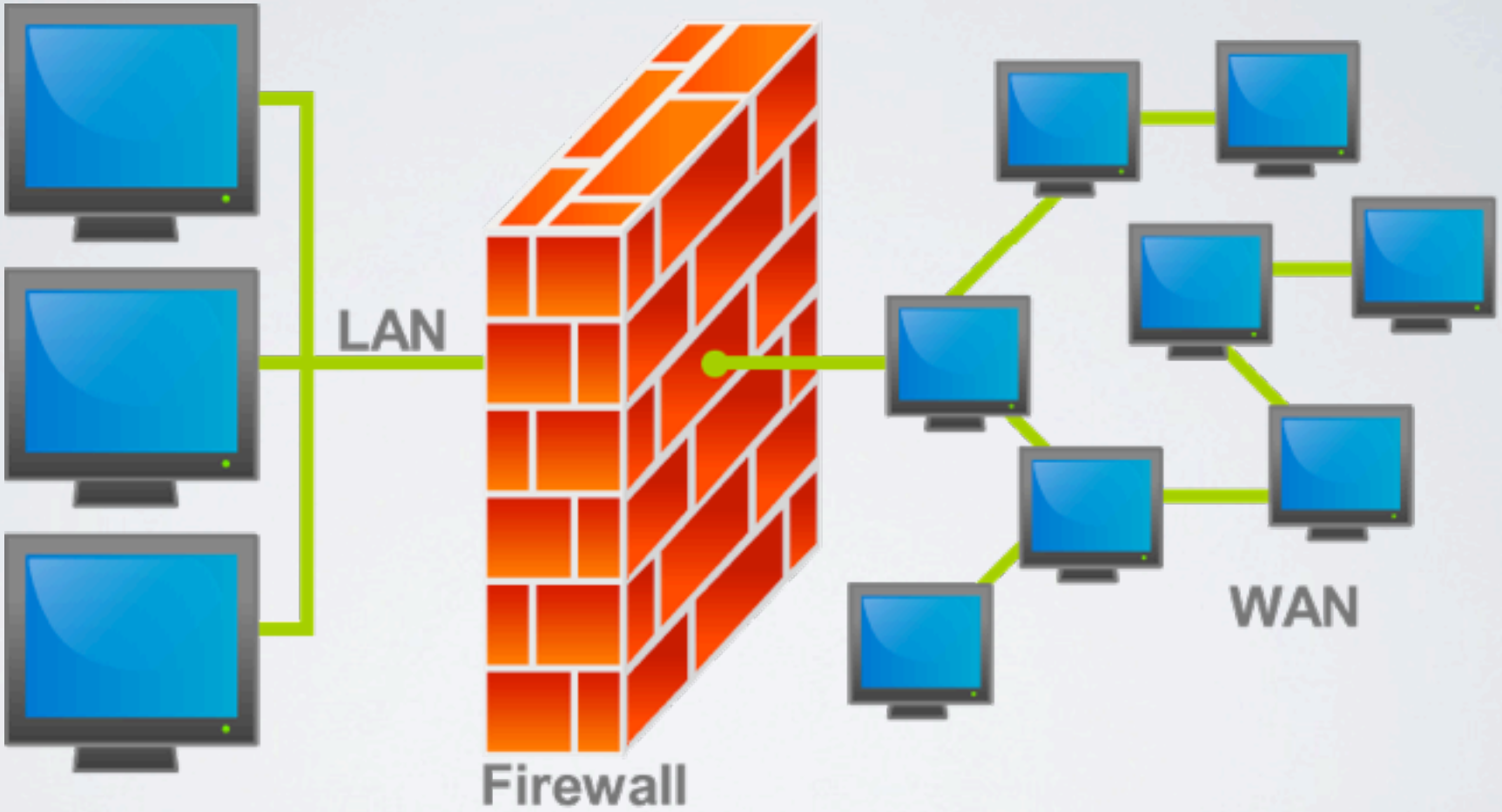
Um firewall[1] é uma parte de um sistema de computação ou de uma rede de computadores com duas finalidades bem definidas :

- ✓ Bloquear Acesso Não-Autorizado
- ✓ Permitir Comunicações Autorizadas observados certos Critérios de Controle

O QUE É UM FIREWALL?

- Um uso típico de Firewalls é regular o acesso entre uma rede de computadores local e a Internet
- O Firewall examina as mensagens que entram ou deixam a rede e bloqueia aquelas que não se encaixam nos critérios de segurança vigentes (regras)
- Implementação por Hardware ou Software
- Tipicamente, sistemas de Firewall estão embutidos nativamente no núcleo dos principais sistemas operacionais comerciais

ILUSTRANDO UM FIREWALL DE REDE



PRIMEIRA GERAÇÃO

- Filtros de Pacotes (*Stateless Packet Filters*)
- Inspeção básica nos **pacotes**, atentando para características básicas como:
  - ➡ Endereço de Origem
  - ➡ Endereço de Destino
  - ➡ Tipo de Protocolo
  - ➡ Número de Porta de Comunicação

PRIMEIRA GERAÇÃO

- Dependendo do conteúdo do pacote e do conjunto de regras, o firewall opta por:

  (1) Aceitar o pacote

  (2) Descartar o pacote ("*silent drop*")

  (3) Rejeitar o pacote (descarte com mensagem de erro)

- Esse tipo de firewall não é capaz de distinguir se um pacote faz parte de um fluxo de tráfego (*stateless*), mas pode ser efetivo para certos tipos de controle, em especial aos serviços de portas bem conhecidas. [6]

SEGUNDA GERAÇÃO

- Filtros de Pacotes com Registro do Estado de Conexão [2] (*Stateful Packet Filters* ou *Circuit-Level Firewalls*)

- Similar aos primeiros filtros de pacotes, mas com a característica adicional de manter um **registro de estado de cada conexão**, permitindo assim verificar se um pacote faz parte ou não de um fluxo de conexão;

- O estado da conexão passa a ser relevante e atua como *trigger* para **regras estabelecidas dinamicamente**

TERCEIRA GERAÇÃO

- Software na camada da aplicação (*application layer firewall*)[3]
- Esse tipo de firewall opera no topo da pilha TCP/IP e pode interceptar tráfego entre aplicações:

  (1) Web Browsers

  (2) Telnet

  (3) SSH, FTP, e outros

- Exemplo Clássico : bloquear qualquer conteúdo contendo a palavra "sexo" na porta 80 (http)

DESENVOLVIMENTOS POSTERIORES

- Refinamento de Tecnologias [4], como regras para MAC Adress, NAT, assinaturas digitais, dentre outros !

- Associação com outros recursos de segurança:

  ✓ **IDS** (Intrusion Detection System)

  ✓ **IPS** (Intrusion Prevent System)

  ✓ **DPI** (Deep Packet Inspection)

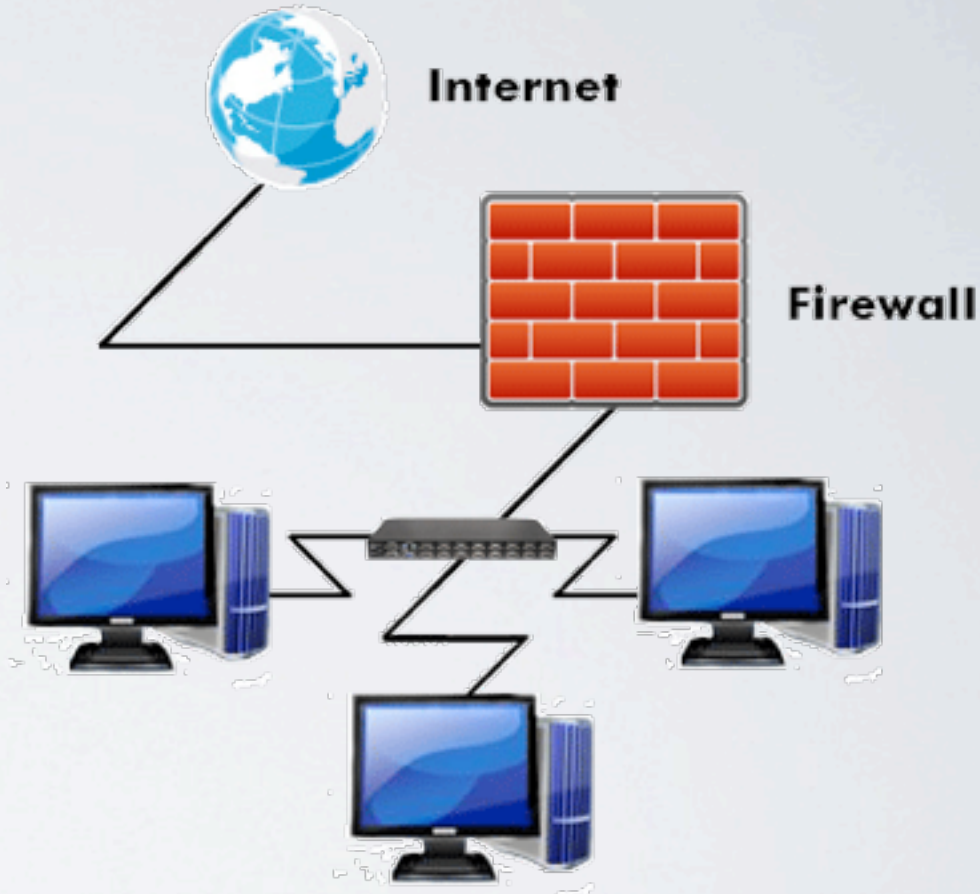
CLASSIFICANDO FIREWALLS

- Firewalls podem ser classificados segundo os seguintes critérios [6] :
  - Escopo de Utilização
  - Camada de Operação
  - Registro de Estado de Conexão

ESCOPO DE UTILIZAÇÃO

- Basicamente, dois tipos :

Personal Firewall



Network Firewall

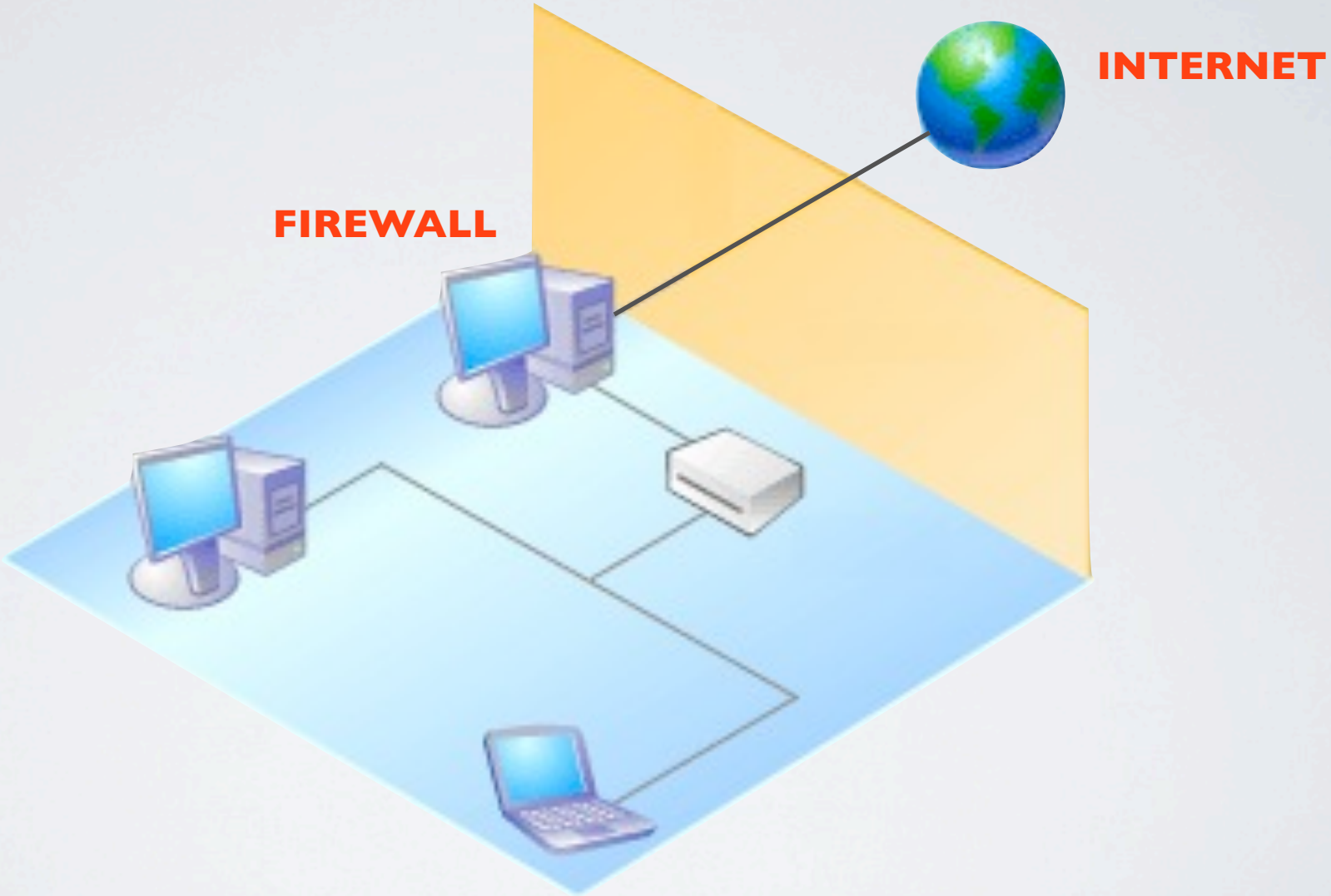
PERSONAL FIREWALL

- Restrito ao host final (*end-user*)
- Recursos interessantes[8] :
  - ✓ Informes sobre tentativas não autorizadas de conexão
  - ✓ Controle sobre programas que acessam a LAN ou a Internet
  - ✓ Bloqueio externo de tentativas de conexão
  - ✓ Monitorar aplicações que aguardam (*listening*) por conexões, dentre outros

NETWORK FIREWALL

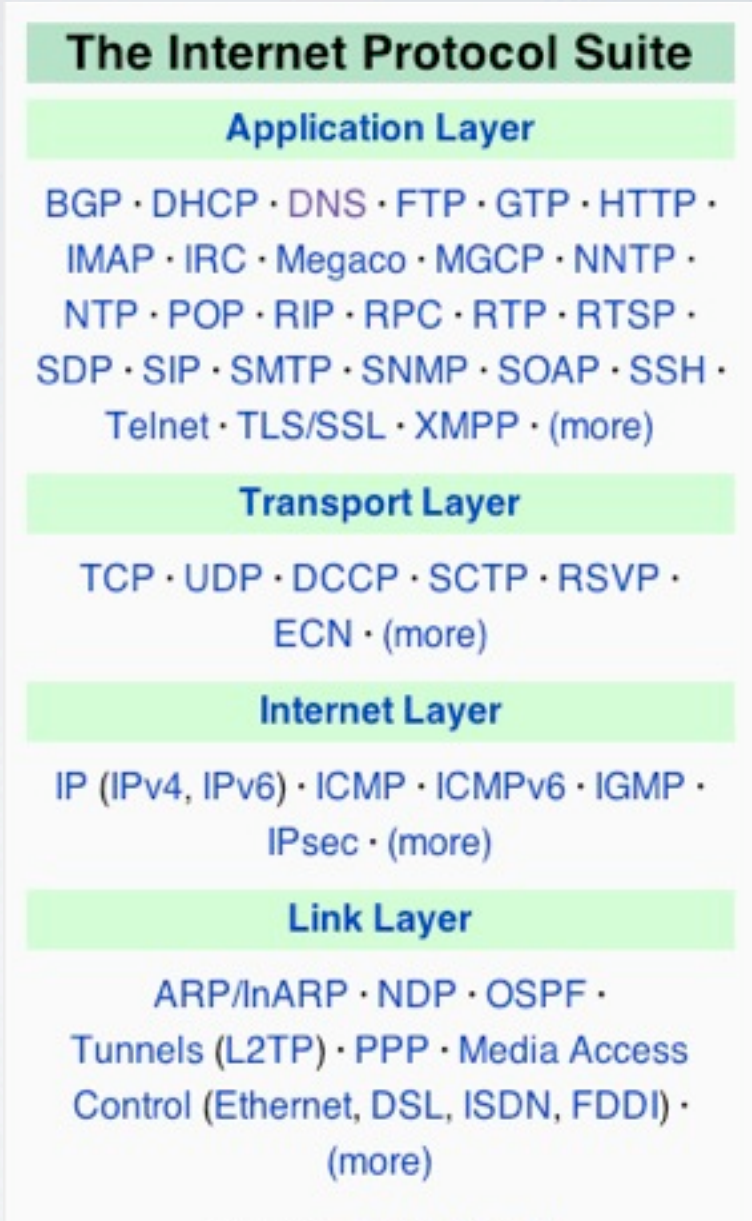
- Dispositivo dedicado ou máquina posicionada no limite de duas redes cujos níveis de confiança sejam díspares [1]:
- Uma rede intermediária entre dois cenários opostos é normalmente referenciada por Zona Desmilitarizada (DMZ) ou Rede Perimetral [1][6]
- Exemplo clássico de uso : conectar uma Intranet à Internet de maneira confiável !

NETWORK FIREWALL



CAMADA DE OPERAÇÃO

- Camada de Rede
- Camada de Transporte
- Camada de Aplicação

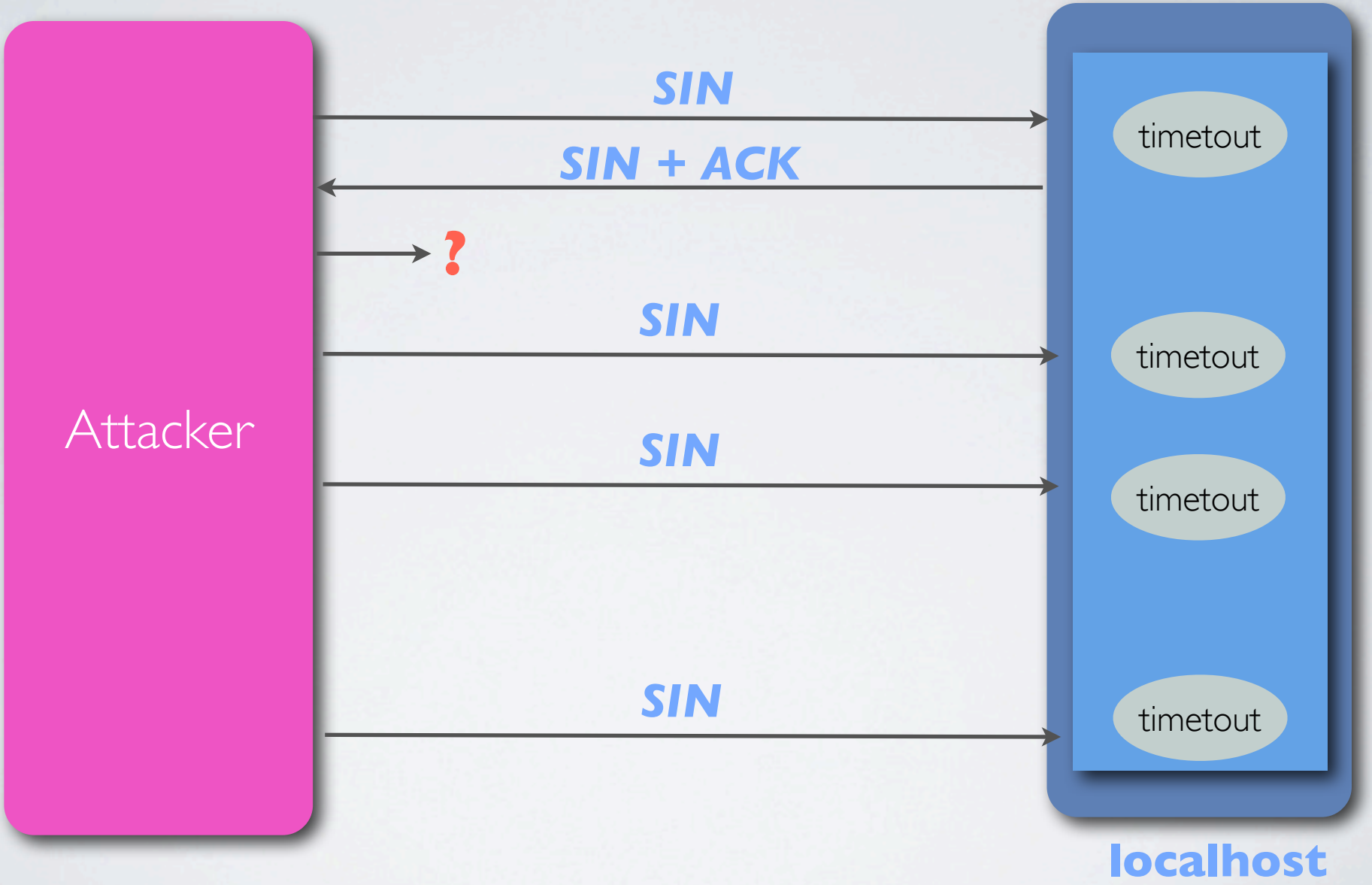


ESTADO DE CONEXÃO

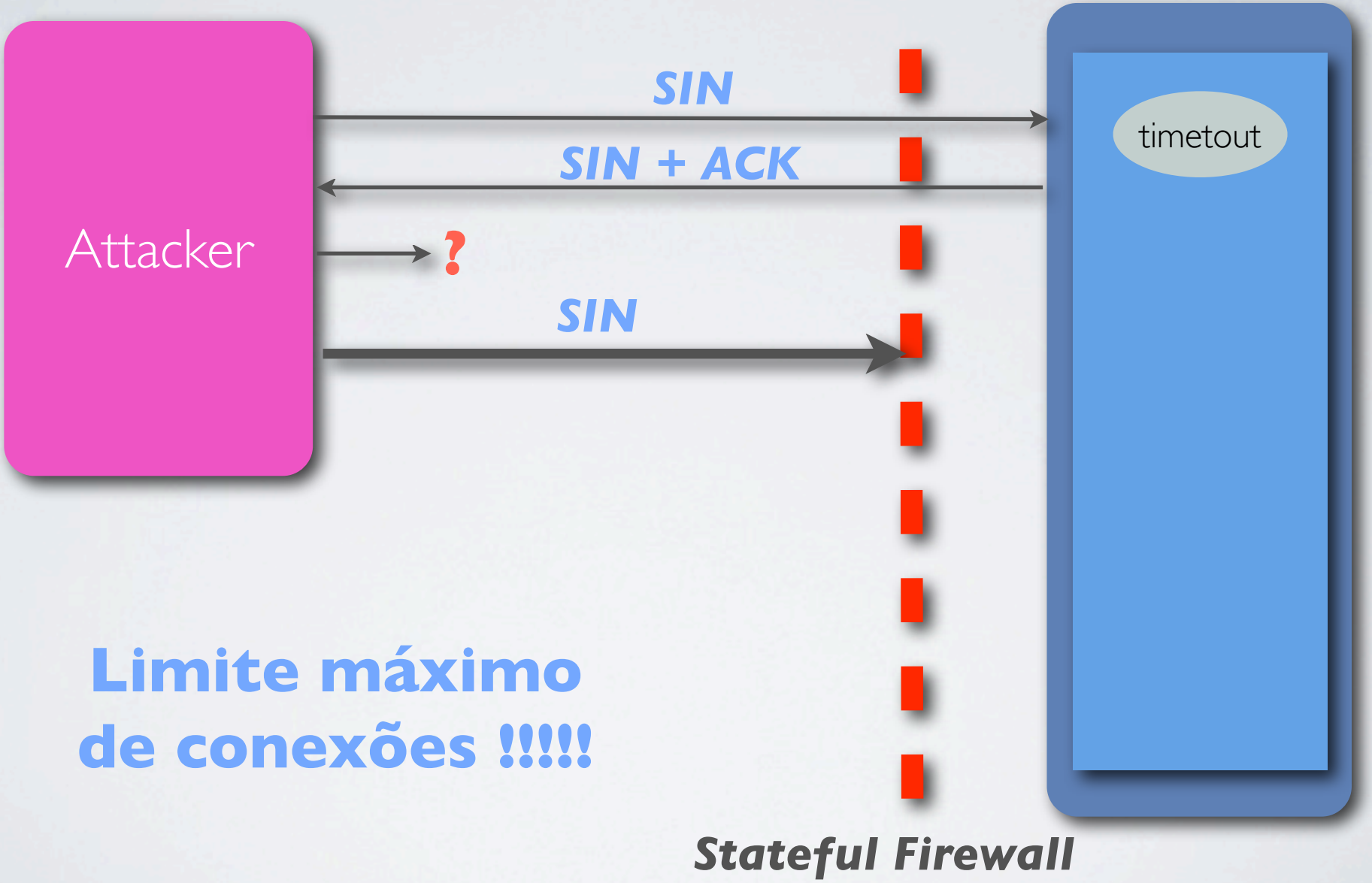
- **Stateless** : Não mantém registro das conexões TCP ou comunicações UDP

- **Stateful** : Monitoramento SPI (*Stateful Packet Inspection*) que mantém registro de streams TCP ou comunicações UDP, de maneira que somente pacotes que correspondam a transmissões com estados válidos serão permitidos

EXEMPLO DE USO - DOS



EXEMPLO DE USO - DOS



ESTUDO DE CASO

- Firewall nativo para plataforma BSD

- Principais Características

  - Processador de regras built-in nos kernels BSD

  - Implementação embutida para NAT

  - Comportamento completamente Stateful com número limitados de conexões

  - Suporte a IPv6, dentre outros

VANTAGENS DO USO DE FIREWALLS

- Controle de Acesso à Rede de maneira bidirecional
- Administrador é capaz de controle fino sobre aplicações (HTTP, FTP, SSH, Telnet, SNMP, dentre outros)
- Mecanismos para anti-spoofing, anti-spam, dentre outros;
- Associação com outros sistemas de segurança (detecção e prevenção de intrusão)
- Mecanismo alternativo para implementação de NAT

LIMITAÇÕES DOS FIREWALLS

- A maior parte dos ataques parte de dentro da própria organização[6]
- Filtros de palavras e outros mecanismos não podem lidar com esteganografia de dados[6]
- Firewalls representam gargalo de rede e acarretam queda no desempenho (firewalls de aplicação)

FUTURO

- Firewalls tendem a ganhar importância maior segundo a inevitável adoção do IPv6 nos próximos anos, a configuração dos mesmos nesse cenário segue as características da nova pilha (exemplo, ICMP)

- Personal Firewalls tendem a ser componentes de dispositivos móveis em um futuro próximo (Internet 3G), de acordo com as necessidades desse tipo de sistema, em versões full ou dedicadas

REFERÊNCIAS

1. *Firewall*. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Firewall
2. *Stateful Firewall*. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Stateful_firewall
3. *Application Layer Firewall*. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Application_layer_firewall
4. *Deep Packet Inspection*. Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/Deep_packet_inspection
5. *Firewalls*. Notas de Aula, Dr. Talal Alkharobi, 2007.

REFERÊNCIAS

6. *Computer Networks, Fourth Edition*. Tanenbaum, A. S. PrenticeHall, 2003.
7. *Computer Networks and the Internet : a Top-down Approach, 5th Edition*. Kurose, J.F. ; Ross, K.W - Pearson, *2004*
8. *Personal Firewall*. Wikipedia, The Free Encyclopedia http://en.wikipedia.org/wiki/Personal_firewall
9. *IPFirewall*. Wikipedia, The Free Encyclopedia http://en.wikipedia.org/wiki/Ipfirewall
10. *FreeBSD Handbook*. The FreeBSD Foundation, 2009

REFERÊNCIAS

11. *Exploring Mac OSX Firewall*. Hickman, Peter, O'Reilly Media, 2005.

12. *Network Administration with FreeBSD 7*. Farrokhi, B. - Packt Publishing, 2008