Firewall

Prof. Dr. João Carlos Lopes Fernandes
E-mail: joao.fernandes1@docente.unip.br

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

Características:

1. Bloqueia o recebimento de dados baseado em uma fonte ou destino
2. Bloqueia o acesso a dados baseado em uma fonte ou destino
3. Bloquear dados baseado em conteúdo
4. Permite conexões com uma rede interna
5. Reporta o tráfego na rede e as atividades do Firewall

Entendendo o Firewall

- O que é Firewall?
- Várias pessoas dirão coisas diferentes
- O básico é o mesmo
- Deve ter pelo menos as quatro funções básicas

1. Filtragem de pacotes
2. NAT (Network Address Translation)
3. Proxy de Aplicação
4. Monitoramento e registro

Estratégias Gerais:

1. Allow-All
2. Deny-All

Melhor opção: Misturar ambos

1. Deny network traffic on all IP ports.
2. Except, allow network traffic on port 80 (HTTP).
3. Except, from all HTTP traffic, deny HTTP video content.
4. Except, allow HTTP video content for members of the Trainers group.
5. Except, deny Trainers to download HTTP video content at night.

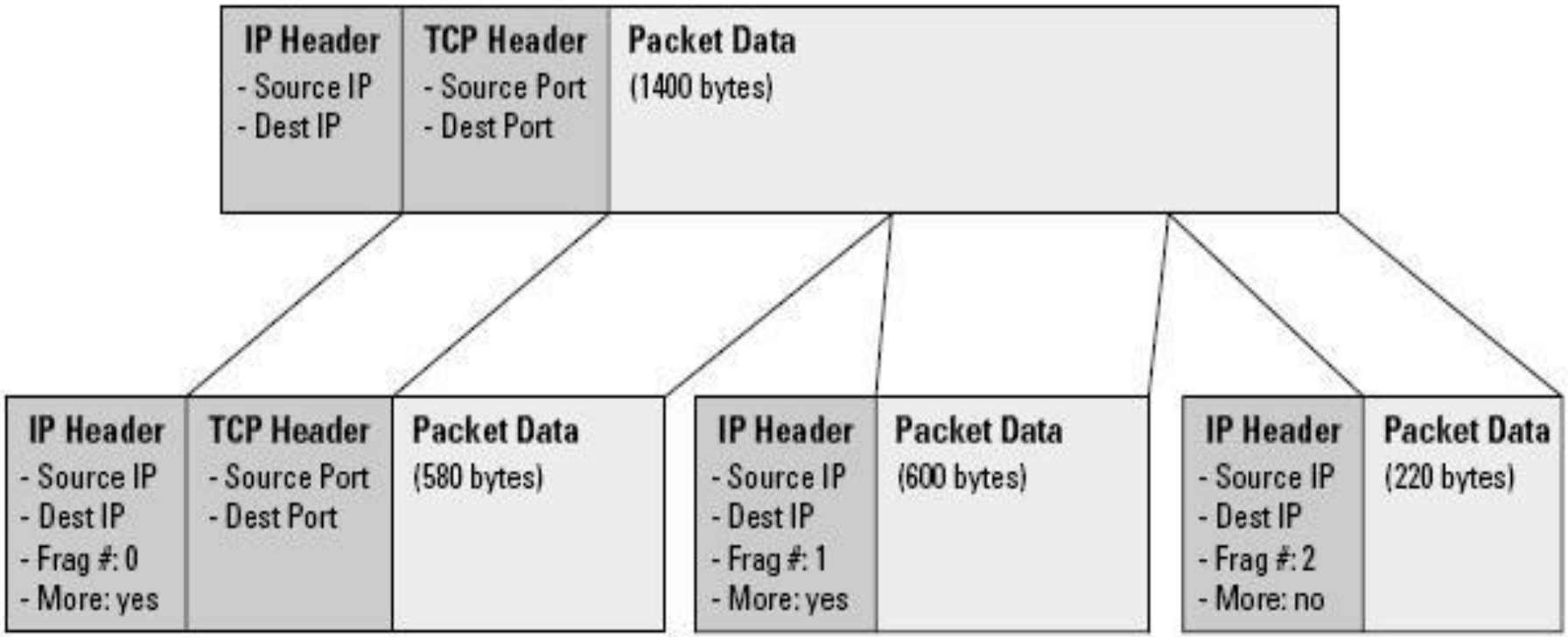
Filtro de Pacotes

Filtragem por Dados:

- IP de origem
- IP de destino
- ID de protocolo IP
- Numero de portas TCP e UDP
- Flags de Fragmentação
- Configuração das opções do IP

Filtro de Pacotes

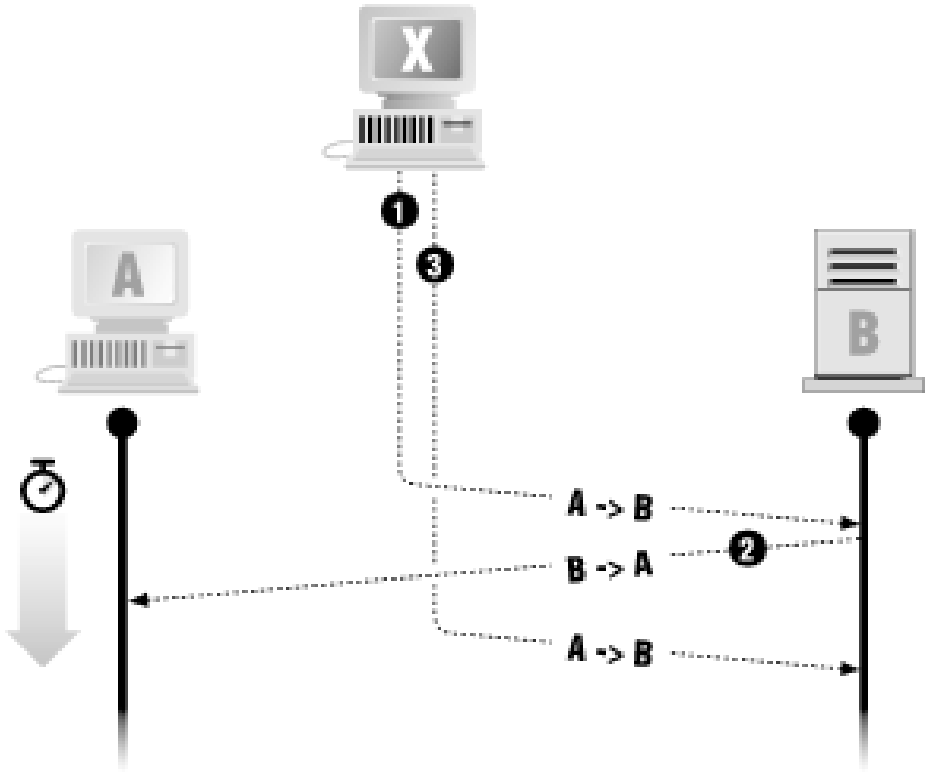
- ICMP
  - ❖Echo Request
  - ❖Echo Reply
  - ❖TTL Exceeded and Destination Unreachable


IP Header
- Source IP
- Dest IP
TCP Header
- Source Port
- Dest Port
Packet Data
(1400 bytes)
IP Header
- Source IP
- Dest IP
- Frag #: 0
- More: yes
TCP Header
- Source Port
- Dest Port
Packet Data
(580 bytes)
IP Header
- Source IP
- Dest IP
- Frag #: 1
- More: yes
Packet Data
(600 bytes)
IP Header
- Source IP
- Dest IP
- Frag #: 2
- More: no
Packet Data
(220 bytes)

IP Spoofing => Uso de IP falso

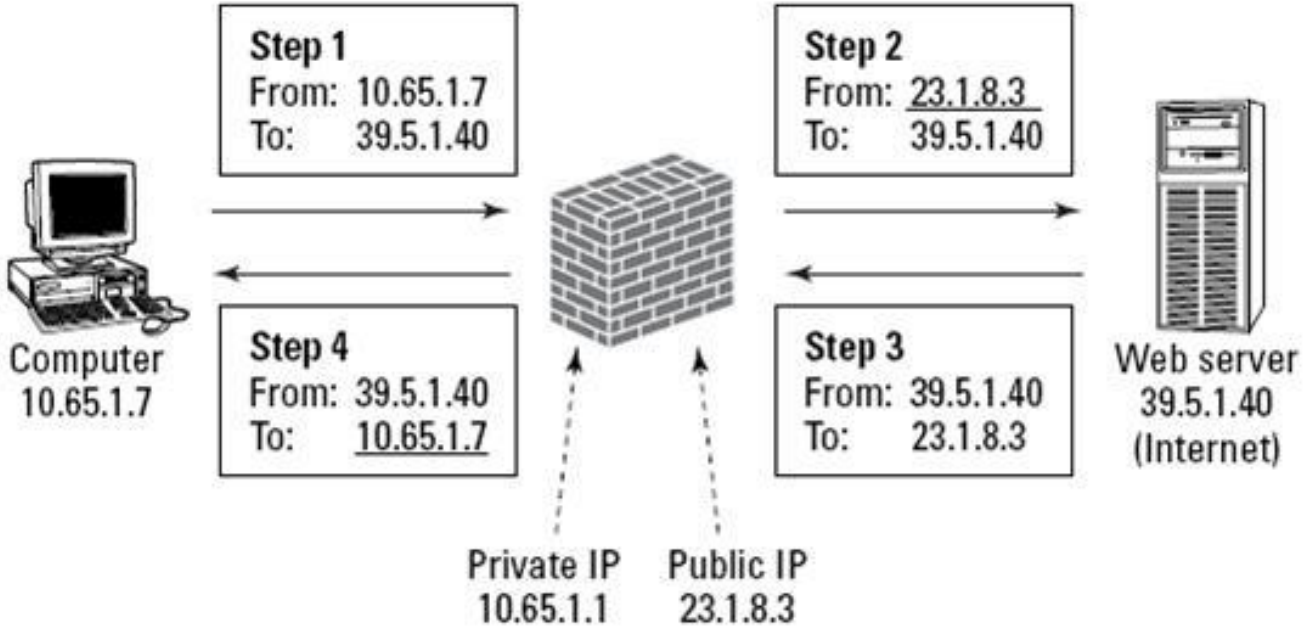
Spoofing is a complex attack we are likely to see more of in the future.

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 fakes another packet that acknowledges session number.*



Network Address Translation (NAT)

- IP => 32 bits! Maximo 4 bilhões de números.
- IP privado ⇔ IP publico



Proxy de aplicação

- Elaborada versão de Filtragem de pacotes
- Não inspeciona somente o cabeçalho, e sim uma parte de aplicação inteira de um pacote
- Gera novamente pacotes antes de enviar ao servidor de internet ou de responder ao computador remoto.

Proxy de aplicação

Difere de Filtragem de pacotes em 2 aspectos:

1. Inspeciona todos os dados de aplicação de um pacote
2. Não permite pacotes saírem ou chegarem. Cria novos pacotes a cada interação, restringindo a chegada de dados nocivos.

Proxy de aplicação

Vantagens e desvantagens:

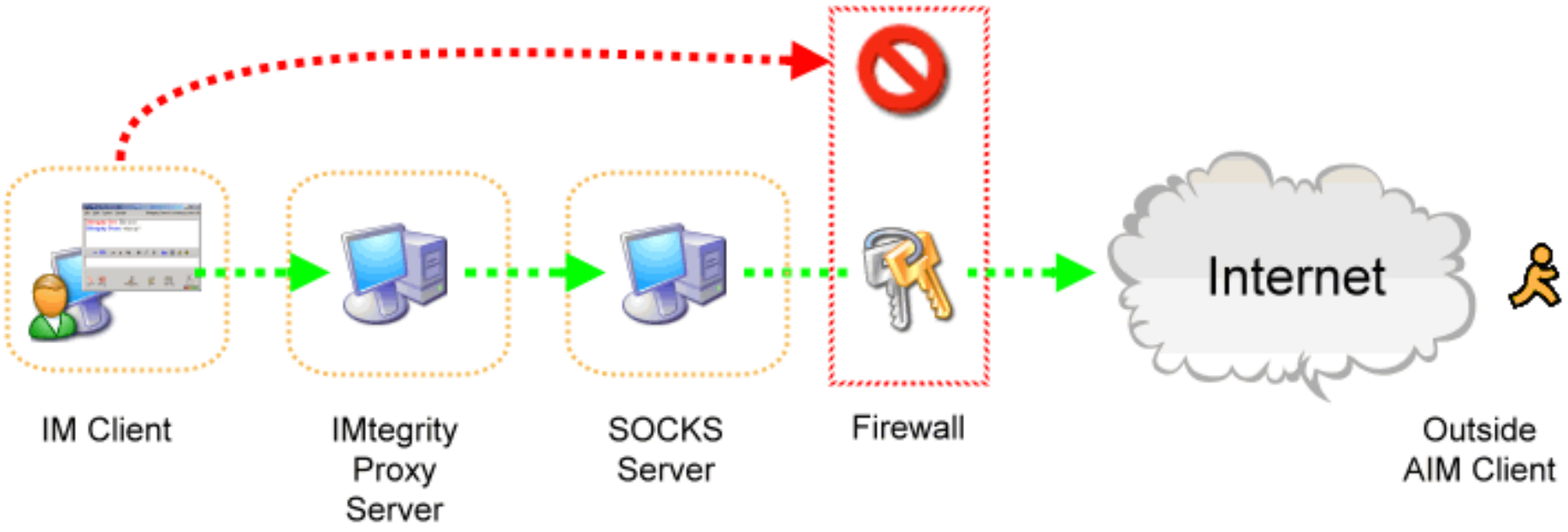
1. Inspeciona uma porção inteira da aplicação do pacote.
2. Registros mais detalhados
3. Impede uma conexão direta entre o computador remoto e o servidor de internet
4. Se o Firewall cair, não há riscos

Proxy de aplicação

Vantagens e desvantagens:

1. O Firewall deve ter um específico proxy de aplicação para cada aplicação
2. O computador da rede interna deve saber que está sob Proxy de aplicação.

Proxy de aplicação



Monitoramento e Registro

Reportar Uso

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

Pergunta

Qual a melhor estratégia ao se configurar um Firewall?

Resposta:

Misturar as estretégias “Allow-All” e “Deny-All”.

Pergunta:

O que significa o termo “IP Spoofing”?

Resposta:

A utilização de uma fonte IP falsa nos pacotes enviados ao Firewall

Pergunta:

Defina “NAT Mappings”:

Resposta:

É uma lista que o NAT de que endereços são trocados por cada endereço original

Pergunta:

Quais as duas diferenças mais importantes entre Filtragem de Pacotes e Proxy de Aplicação?

Resposta:

A filtragem de pacotes inspeciona apenas o cabeçalho do pacote, enquanto o Proxy de aplicação analisa todos os dados de aplicação de um pacote.

A filtragem de pacotes passa um pacote que foi permitido. O mesmo pacote viaja entre a internet e o computador da rede interna. Um proxy de aplicação gera novamente um pacote através de um pacote que foi permitido. Ele constrói um novo pacote e envia do firewall pro servidor da internet (ou pro computador remoto, dependendo do sentido).

Pergunta:

Como manter o Registro seguro?

Resposta:

Armazenando-o em um outro computador ou em um dispositivo de gravação única.