Aula 18:
Redes e Internet
(parte 2)

Prof. Sérgio Montazzolli Silva
smsilva@uel.br

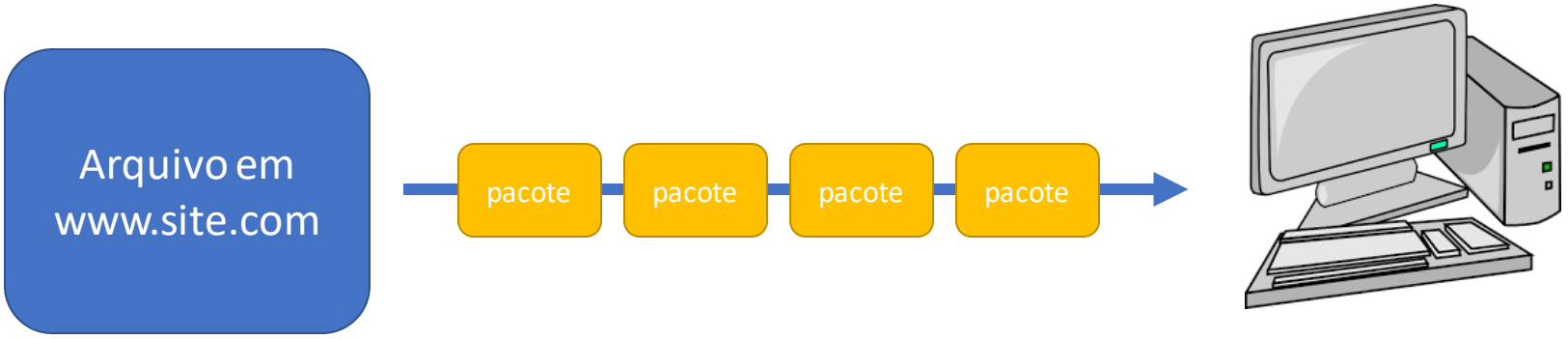
Nesta aula

- Trafego de Rede
- Ataques e soluções

Tráfego de Rede

Pacote de dados

- Usa-se o termo Pacote de Dados, ou simplesmente **pacote**, para designar pequenos volumes de dados que trafegam de um lugar a outro
- Por exemplo: ao baixar um arquivo, este vêm até o seu computador dividido em vários pacotes de dados

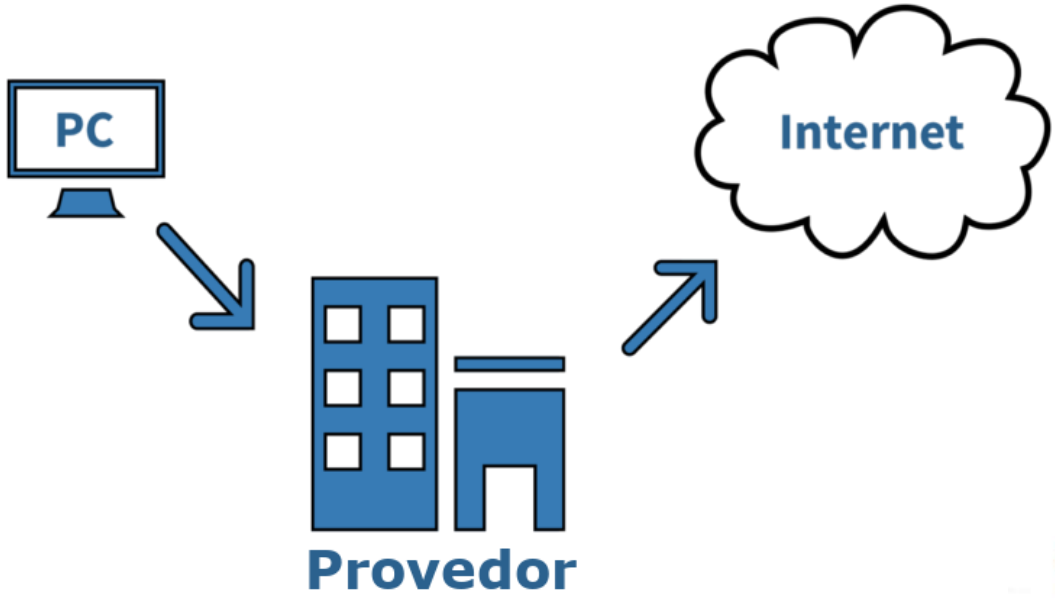


Trafego

- Tanto nas intranets quanto na internet, os pacotes trafegam de uma máquina a outra através de “vias” digitais
- Estas vias digitais são conexões ultra-rápidas entre regiões razoavelmente distantes
  - Podem conectar por exemplo Londrina à Curitiba, Curitiba à Nova Iourque (EUA), etc...
- Pode-se fazer uma analogia com o trânsito: os pacotes são carros que trafegam tanto em vias rápidas e super movimentadas (fibras óticas), como em vias lentas (wifi, cabo) para chegar ao seu destino final (máquina alvo)
  - Igualmente, se a via estiver muito movimentada, o transito fica lento; no caso, a transmissão

Provedor de Acesso a Internet

- Também chamado de ISP (*Internet Service Provider*), o **provedor** é o primeiro lugar para onde os seus pacotes, assim que saem da rede local (intranet), se dirigem
- Da mesma forma, pacotes que chegam endereçados a sua máquina, também passam pelo seu provedor
- *O provedor é a borda da sua conexão à Internet*



Backbones

- Do provedor, o pacote é direcionado a um *backbone*
- *Backbones*, assim com provedores, trabalham unicamente com tráfego de rede
- Cada *backbone* possui conexões com outros *backbones* ou provedores de acesso
- Ao receber um pacote em uma destas conexões, ele analisa o endereço IP do destinatário, e redireciona o pacote para a conexão de saída correta

Analogia: imagine que você está viajando até Curitiba, e se depara com uma bifurcação ou trevo, onde existem rotas possíveis para São Paulo, Foz do Iguaçu e Curitiba. Você obviamente escolhe Curitiba; Neste caso, você é o pacote, a estrada é o meio transmissão (e.g. cabo), e o trevo poderia ser o *backbone*.

Rotas

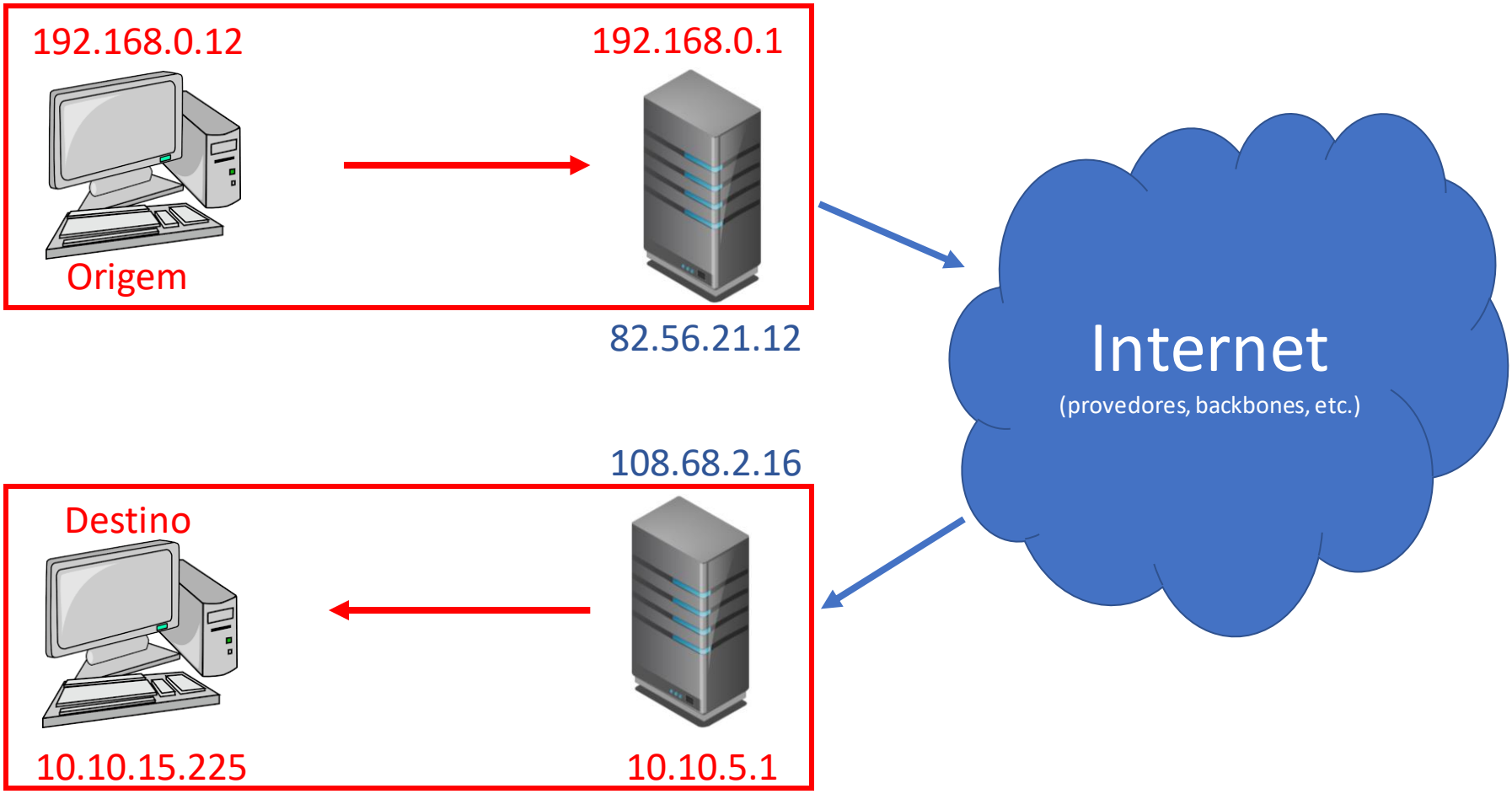
- Rotas são os caminhos que um pacote toma para chegar ao seu destino
- Normalmente uma rota é algo como:

1. Switch ou roteador local 2. Gateway	Intranet
3. Provedor 4. Backbone 1 5. Backbone 2 6. … 7. Backbone N 8. Provedor do destinatário	Internet
9. Gateway do destinatário 10. Switch ou roteador local do destinatário 11. Destinatário	Intranet

Endereçamento

- Cada máquina em uma intranet possui seu próprio IP
- Uma Intranet é representada na Internet através do seu gateway. Dessa forma o IP do gateway representa todas as máquinas da Intranet
- Existem basicamente 4 endereços IP em uma comunicação:
  - Endereço IP da máquina de origem
  - Enredeço IP de internet do gateway
  - Enredeço IP de internet do gateway do destinatário
  - Endereço IP local do destinatário

Endereçamento



Endereçamento

- Como o gateway é quem representa nossa intranet na Internet, podemos facilmente descobrir seu IP através de sites como:
  - https://www.meuip.com.br/
  - https://e-meuip.com/
  - https://www.meuenderecoip.com/
  - Etc...
- Basta procurar por “Meu IP” no Google
- Note que o IP que aparece nestes sites não é o mesmo que é mostrado pela ferramenta ***ipconfig***

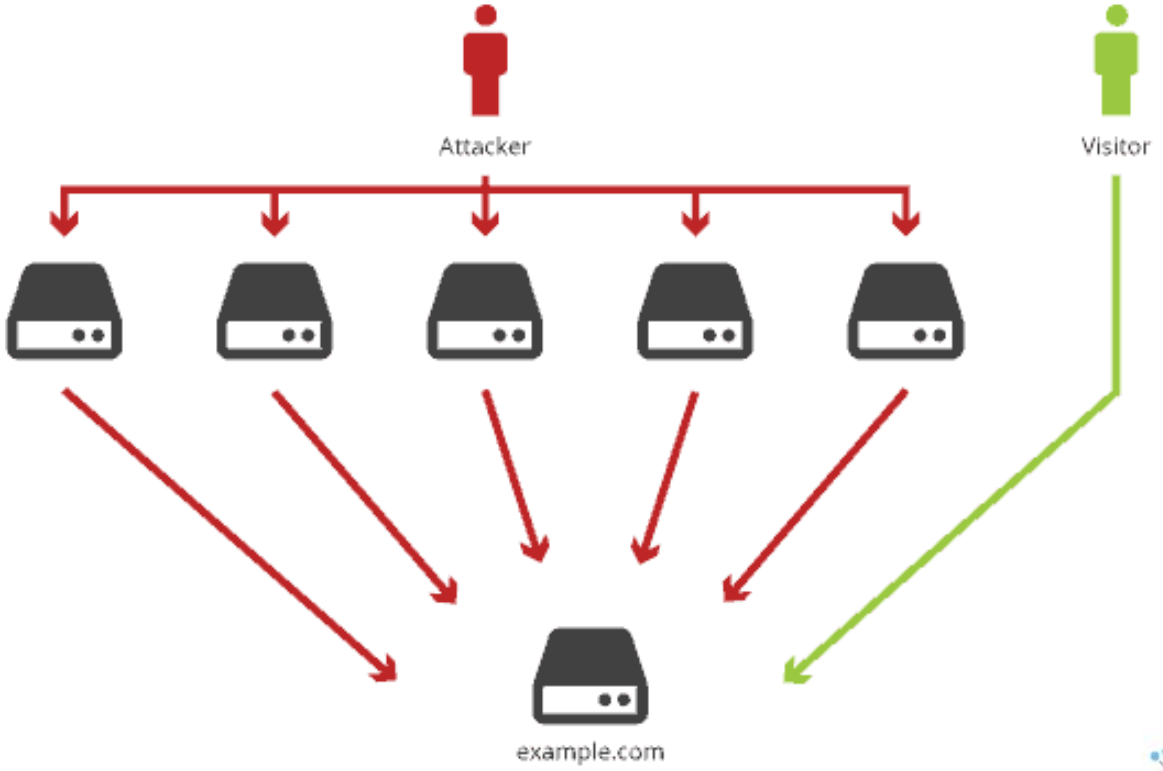
Segurança

Ataques – DOS

- Um tipo comum de ataque chama-se *Denial of Service* (DoS) ou Negação de Serviço
- Aqui um operador malicioso utiliza centenas a milhares de máquinas infectadas para realizar requisições a um servidor alvo (vítima)
- Como servidores tem uma capacidade limitada, excessivas requisições podem fazer com que ele pare de funcionar, ou, passe a "negar o serviço"
- Exemplo: apesar de não ser um ataque, quando resultados de concursos (como o vestibular) são publicados, eles costumam gerar volumes atípicos de acesso a determinados sites, muitas vezes tirando estes sites do ar

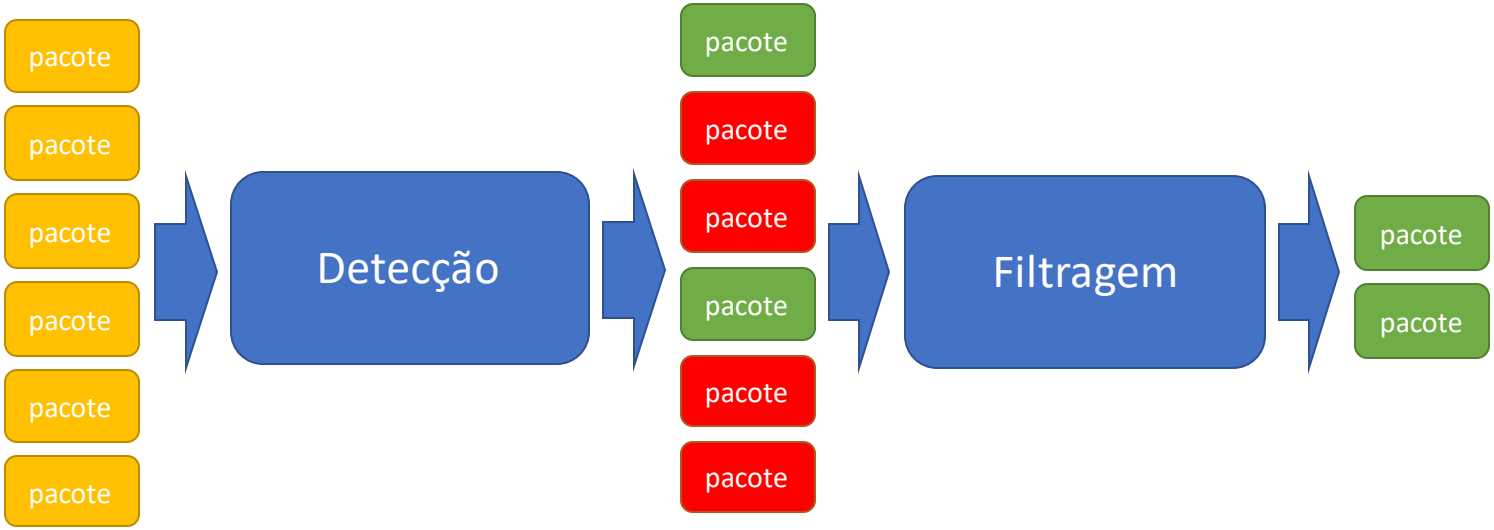
Ataques – DOS

- A idéia do DoS é justamente gerar este grande volume de acessos através de máquinas infectadas por algum tipo de vírus



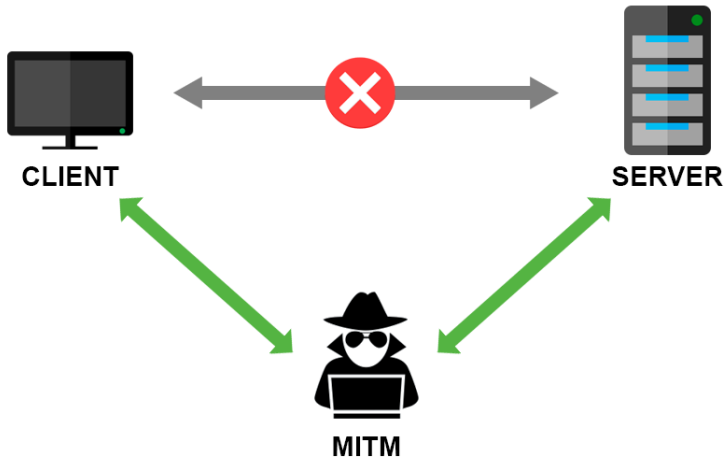
Ataques – DOS – Prevenção

- Prevenção:
  - Feita através de softwares ou equipamentos de segurança normalemente instalados no gateway ou servidores conectados diretamente a internet
  - Eles identificam e bloqueiam volumes de conexão suspeitos



Ataques – MITM

- Outro tipo comum de ataque a transmissão de dados chama-se “Man in the Middle” (homem no meio)
- Neste tipo de ataque, um operador malicioso se dispõe a ouvir o que está sendo transmitido entre duas máquinas
  - Ele intercepta os pacotes, analisa-os, e os recoloca novamente na rota de transmissão



Ataques – MITM

- Ao escutar transmissões, é possível identificar e roubar:
  - Dados pessoais
  - Senhas
  - Números de cartão de crédito
  - Conteúdo de e-mails
  - Conversas por chat
  - Etc...

- Como prevenir?
  - **Criptografia!**