Segurança em redes de computadores

SEG786203 – CST em Análise e Desenvolvimento de Sistemas

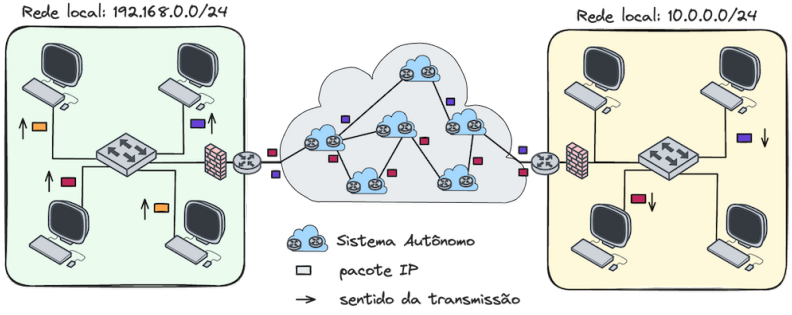
Prof. Emerson Ribeiro de Mello

mello@ifsc.edu.br

INSTITUTO FEDERAL
Santa Catarina
Campus São José

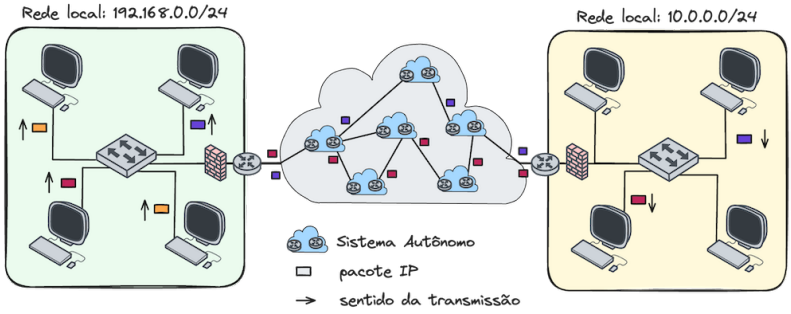
Licenciamento

Redes de computadores



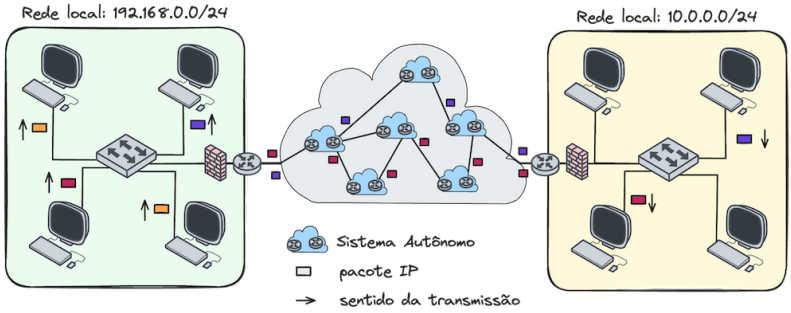
- Dispositivo Final
- Comutador
- Roteador
- *Firewall*

Redes de computadores



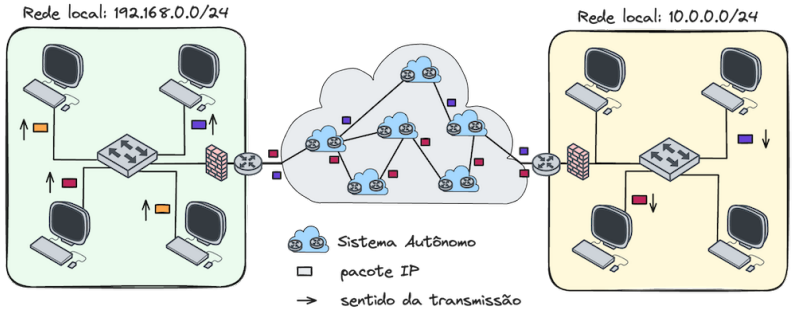
- O caminho do pacote de origem para o destino é chamado de **rota**
- A comunicação entre dois dispositivos é chamada de **sessão**
- Todos os pacotes de uma mesma sessão sempre seguirão a mesma rota?

Redes de computadores



- O pacote pode ser interceptado em qualquer ponto da rota
  - Na origem, na rede local, no roteador, na rede de destino, no destino
- Como garantir a confidencialidade, integridade e autenticidade dos dados?

Redes de computadores



- Processo servidor está associado a uma porta, protocolo e endereço IP
- É possível garantir que o servidor seja acessado somente por máquinas da rede local?
- É possível garantir que somente uma máquina local acesse o servidor?

Endereçamento I

- O **endereço MAC** é gravado na ROM da placa de rede pelo fabricante e é utilizado para identificar a placa de rede em uma rede local
- O **endereço IP** é associado a uma interface de rede e é utilizado para identificar um dispositivo em uma rede TCP/IP

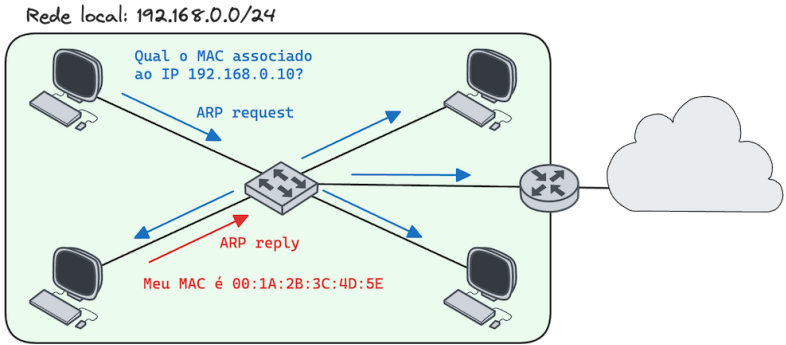
```
root@73436e94eae1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

Interface de rede
MAC
IPv4
IPv6

Endereçamento II

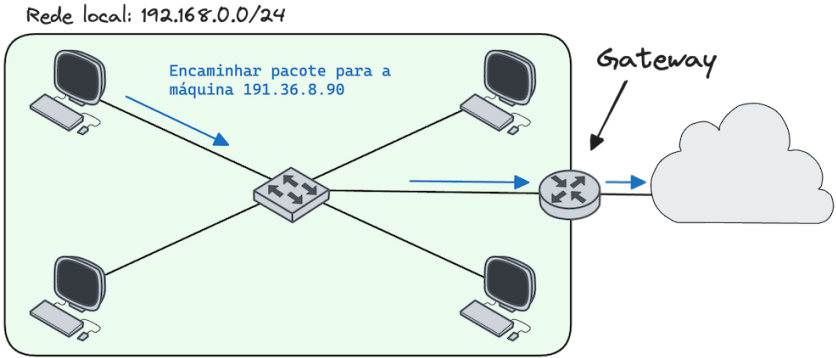
- Em um mesmo domínio de *broadcast* não podem existir dois dispositivos com o mesmo endereço MAC
- Em uma mesma rede TCP/IP não podem existir dois dispositivos com o mesmo endereço IP
- O endereço IP é utilizado para roteamento de pacotes, enquanto o endereço MAC é utilizado para entrega de pacotes na mesma rede
- Resolução de endereços IP para endereços MAC é feita pelo protocolo ARP (*Address Resolution Protocol*)
  - ARP mapeia um endereço de rede IPv4 para um endereço físico MAC

Endereçamento III



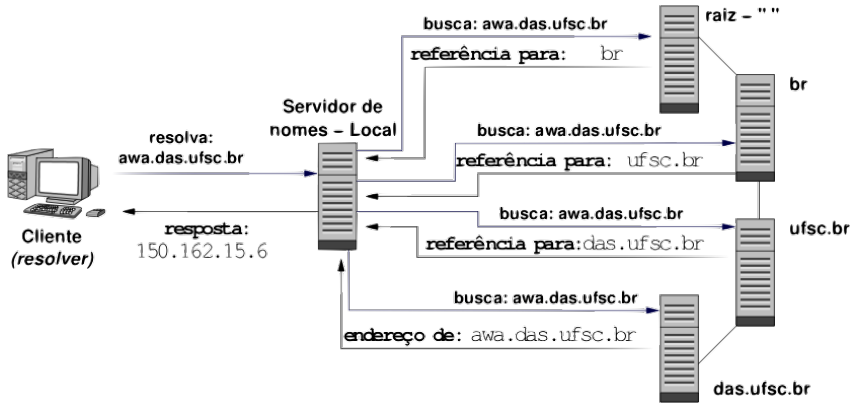
- Consulta feita em ***broadcast*** e o dispositivo com o endereço IP solicitado responde com seu endereço MAC (***unicast***)
- Os dispositivos mantém uma tabela ARP com os endereços IP e MAC dos dispositivos da rede (ARP *cache*)

Endereçamento IV



- O dispositivo de origem encaminha o pacote para o *gateway* padrão, uma vez que o destino não está na mesma rede
- E como o dispositivo de origem descobriu o endereço IP do destino?

Endereçamento V



- Serviço de nomes de domínio (DNS) é responsável por associar um nome de domínio a um endereço IP
- Resolução: recursiva e iterativa

Firewall

Definição convencional: Parede corta fogo

Dispositivo feito de material a prova de fogo para evitar que o fogo se espalhe de uma parte do edifício para outra

Firewall

Definição convencional: Parede corta fogo

Dispositivo feito de material a prova de fogo para evitar que o fogo se espalhe de uma parte do edifício para outra

Definição para sistemas computacionais

Ponto de controle que mantém acessos não autorizados fora do perímetro de segurança, ao mesmo tempo possibilita acesso aos sistemas externos

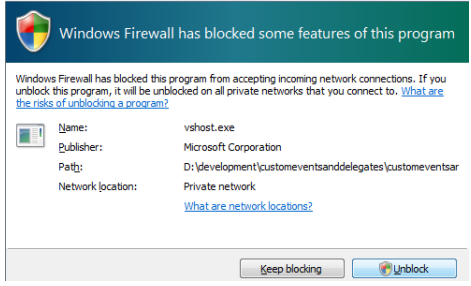
- Evita que potenciais vulnerabilidades de serviços sejam exploradas
  - Nenhum software complexo é 100% seguro

Firewall de máquina (ou Firewall pessoal)

- **Perímetro de segurança:** A própria máquina
- Analisa todo o tráfego entrante e sainte
  - Uma forma de proteção contra *spywares*, máquinas zumbis
- As regras podem seguir uma política de segurança da organização (mais seguro) ou o próprio usuário pode definir suas regras (menos seguro)
- **Exemplo:** Firewall do Microsoft Windows

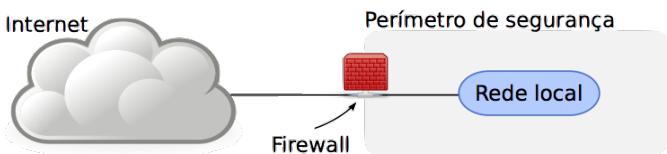
Firewall de máquina (ou Firewall pessoal)

- **Perímetro de segurança:** A própria máquina
- Analisa todo o tráfego entrante e sainte
  - Uma forma de proteção contra *spywares*, máquinas zumbis
- As regras podem seguir uma política de segurança da organização (mais seguro) ou o próprio usuário pode definir suas regras (menos seguro)
- **Exemplo:** Firewall do Microsoft Windows



Firewall de rede

- **Perímetro de segurança:** rede local da organização
- Todo o tráfego de dentro para fora, e vice-versa, deverá passar pelo *Firewall*
- Somente o tráfego autorizado, definido pela política de segurança local, deverá ter permissão para passar
- O próprio *Firewall* deverá ser imune a invasões
  - Implica na utilização de um sistema confiável, com um sistema operacional seguro e rodando um conjunto mínimo de serviços



Características de um firewall de rede

- Ponto único de controle garante uma maior segurança da rede
  - Mesmo que máquinas de clientes não estejam plenamente seguras
- Um bom local para realizar Traduções de Endereços de Rede (NAT) e registro do tráfego
- **Não protege** contra ataques oriundos da rede interna
- **Não evita** que máquinas internas façam uso de modems (5G) e se conectem à rede externa

Características de um firewall de rede

- Ponto único de controle garante uma maior segurança da rede
  - Mesmo que máquinas de clientes não estejam plenamente seguras
- Um bom local para realizar Traduções de Endereços de Rede (NAT) e registro do tráfego
- **Não protege** contra ataques oriundos da rede interna
- **Não evita** que máquinas internas façam uso de modems (5G) e se conectem à rede externa

Firewall pessoal + Firewall rede

Se o firewall de rede protege contra ataques oriundos da rede externa, o firewall pessoal pode proteger contra ataques originados dentro da rede local

Tipos de Firewall

- **Filtro de pacotes** (camada de rede)
  - Se preocupa com endereço IP de origem/destino, porta de origem/destino, protocolo utilizado
  - Geralmente combinado com roteador
- **Inspeção de estado** (camada de transporte)
  - Não filtram pacotes individuais, o filtro é baseado em regras de sessões
- ***Gateway* no nível de aplicação**
  - O tráfego é analisado na camada de aplicação
- ***Web Application Firewall* (WAF)**
  - Inspeciona o tráfego HTTP

Filtro de pacotes

- Atua na camada de rede e não se preocupa com o conteúdo dos pacotes
- Analisa todo datagrama e decide se serão descartados ou encaminhados
  - Endereço IP de origem e de destino
  - Porta de origem e de destino
  - Interface de entrada e de saída
  - Protocolo TCP, UDP ou ICMP

Filtro de pacotes

Exemplo de política vs configuração

Política

Configuração do firewall

Filtro de pacotes

Exemplo de política vs configuração

Política

- Máquinas de usuários não podem gerar SPAM

Configuração do firewall

- Descarte todos pacotes saintes com destino a porta 25

Filtro de pacotes

Exemplo de política vs configuração

Política

- Máquinas de usuários não podem gerar SPAM
- Máquinas internas não podem ser acessadas remotamente

Configuração do firewall

- Descarte todos pacotes saintes com destino a porta 25
- Descarte pacotes destinados as portas do SSH, VNC, RDesktop

Filtro de pacotes

Exemplo de política vs configuração

Política

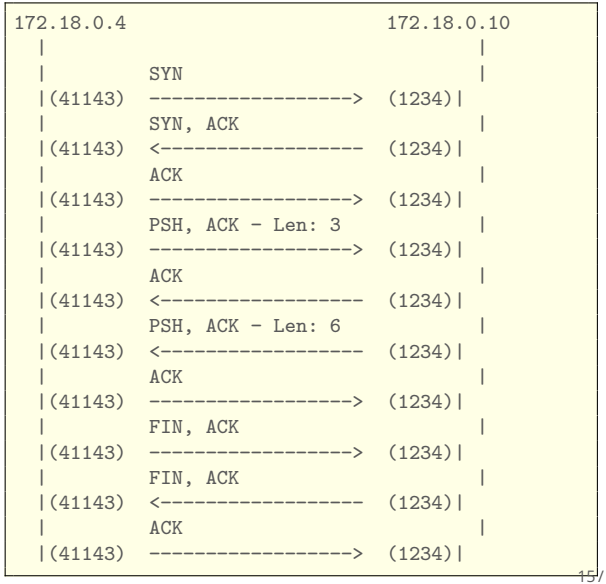
- Máquinas de usuários não podem gerar SPAM
- Máquinas internas não podem ser acessadas remotamente
- Usuários podem navegar na web

Configuração do firewall

- Descarte todos pacotes saintes com destino a porta 25
- Descarte pacotes destinados as portas do SSH, VNC, RDesktop
- Permita o tráfego sainte para as portas 80 e 443

Inspeção de estado

- Atua na camada de transporte (camada 4)
- Não analisa pacotes individuais
- Mantém estado de todas as conexões que passam por este
- Consegue determinar se um pacote faz parte de uma conexão existente ou de uma nova conexão
  - TCP *Flags*: SYN, ACK…



Gateway no nível de aplicação

Examina conteúdo dos pacotes - camada 7

- Permite um controle mais granular que aquele presente nos filtros de pacotes e de sessões
  - Ex: Aos usuários internos não é permitido baixar arquivos .EXE
  - Pode ser combinado com antivírus
- Consome uma carga maior de processamento se comparado a outros filtros
- A conexão entre clientes e servidores é sempre intermediada
  1. Pacotes originados pelos clientes param no *gateway*, onde são analisados
  2. Se estiverem de acordo, o *gateway* inicia uma conexão com o servidor externo

Web Application Firewall (WAF)

- *Gateway* de aplicação especializado em proteger aplicações *web*
- Proteção contra ataques *SQL Injection*, *Cross-Site Scripting* (XSS), *Cross-Site Request Forgery* (CSRF) e mitiga ataques de negação de serviço (DoS)
- Redes de distribuição de conteúdo (CDN) como Akamai e Cloudflare oferecem *WAF* como serviço
  - Possuem regras pré-definidas e atualizadas constantemente com base em ameaças conhecidas e vulnerabilidades de dia zero
  - Detecta vazamento de informações sensíveis ou uso de credenciais roubadas

Comparativo entre os tipos de firewall

- Filtro de pacotes
- Inspeção de estados
- Gateway de aplicação

Comparativo entre os tipos de firewall

- **Filtro de pacotes**
  - **Vantagens:** Com regras simples é possível se proteger da maioria das ameaças de segurança
  - **Desvantagens:** Segurança *vs* facilidade para usuários
- **Inspeção de estados**
- **Gateway de aplicação**

Comparativo entre os tipos de firewall

- **Filtro de pacotes**
  - **Vantagens:** Com regras simples é possível se proteger da maioria das ameaças de segurança
  - **Desvantagens:** Segurança *vs* facilidade para usuários
- **Inspeção de estados**
  - **Vantagens:** Evita ataques mais elaborados; facilidade para usuários
  - **Desvantagens:** Aplicações UDP não são atendidas
- **Gateway de aplicação**

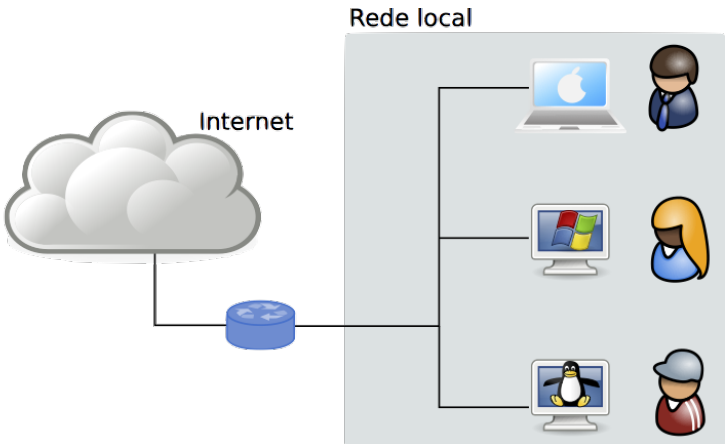
Comparativo entre os tipos de firewall

- **Filtro de pacotes**
  - **Vantagens:** Com regras simples é possível se proteger da maioria das ameaças de segurança
  - **Desvantagens:** Segurança *vs* facilidade para usuários
- **Inspeção de estados**
  - **Vantagens:** Evita ataques mais elaborados; facilidade para usuários
  - **Desvantagens:** Aplicações UDP não são atendidas
- **Gateway de aplicação**
  - **Vantagens:** Filtro granular baseado em conteúdo
  - **Desvantagens:** Não é adequado para aplicações que necessitam de baixa latência

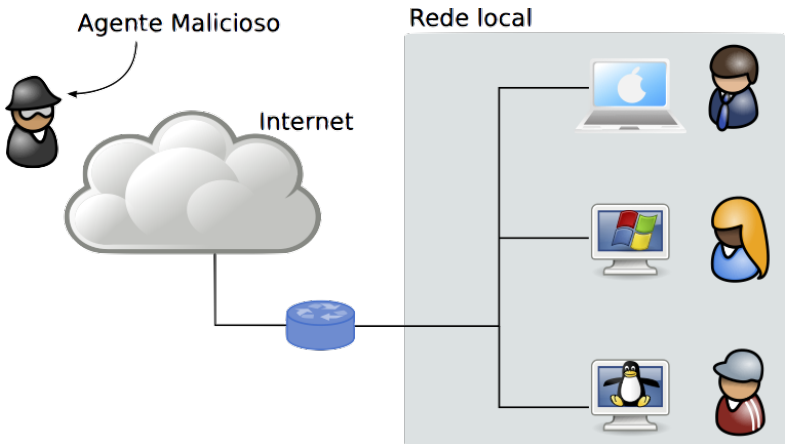
Estratégias de implementação de firewall

Estratégia	Descrição
Local	Instalado em cada máquina individual
Roteador/Firewall	Uma única máquina para roteamento e filtragem de pacotes
***Firewall* com 2 interfaces**	Intermedia a conexão entre a LAN e o roteador
Firewall com subredes	Máquinas da rede interna são alocadas em diferentes subredes
2 Firewalls com subredes	Separação de tarefas por 2 firewalls

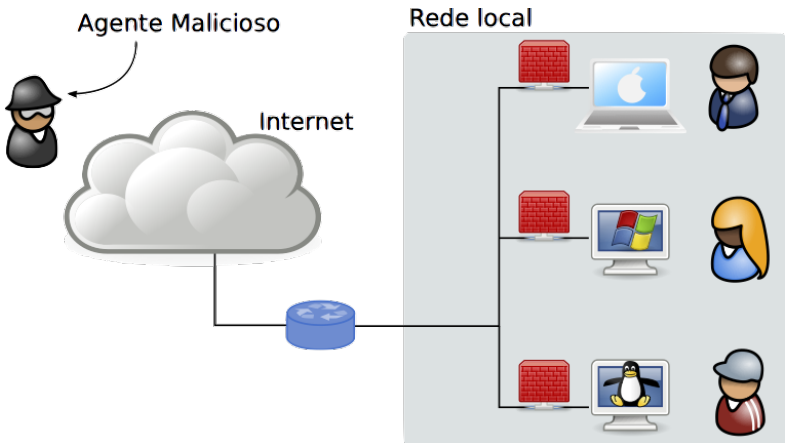
Estratégia: Local



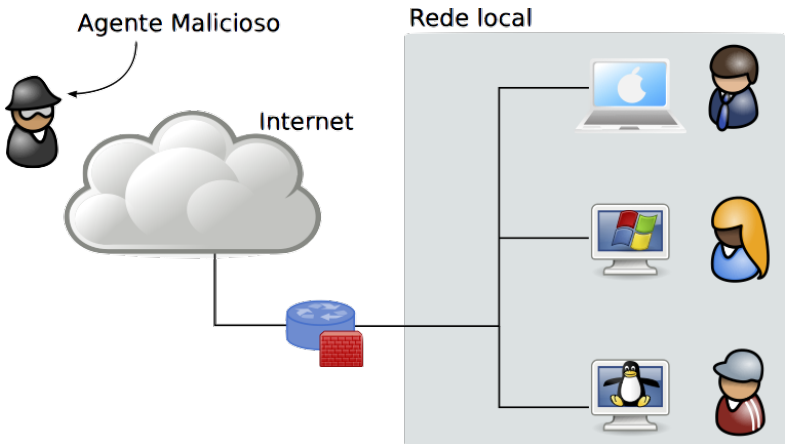
Estratégia: Local



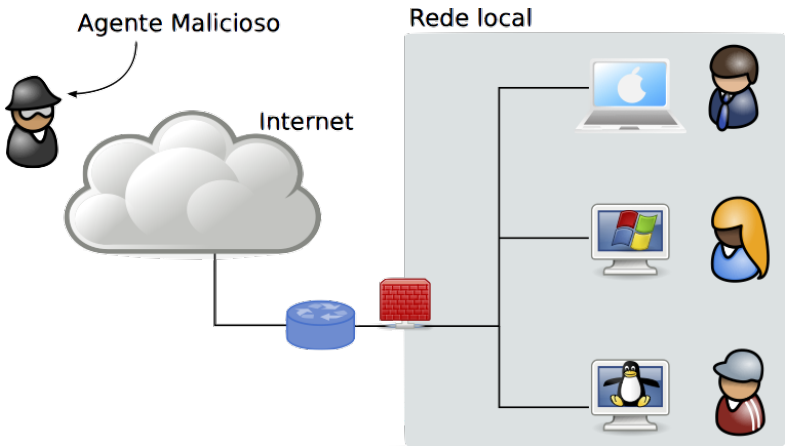
Estratégia: Local



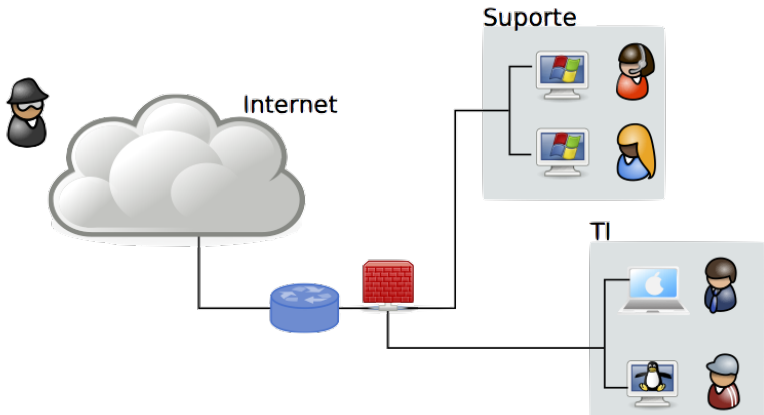
Estratégia: Roteador/Firewall



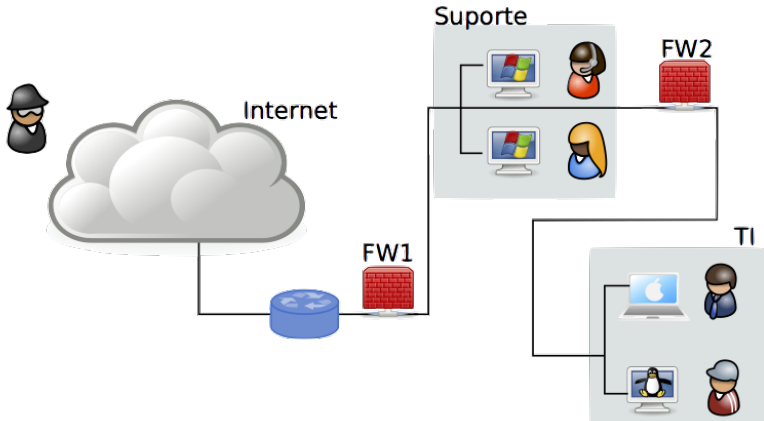
Estratégia: *Firewall* com 2 interfaces



Estratégia: Firewall com subredes



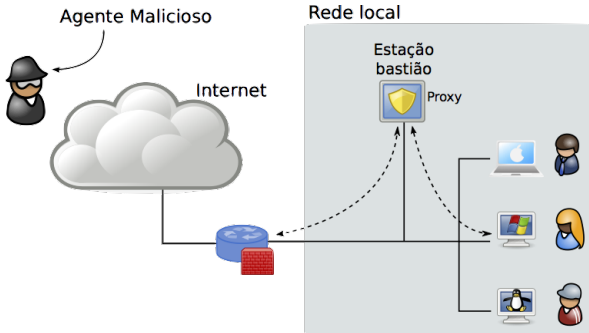
Estratégia: 2 Firewalls com subredes



Estação bastião

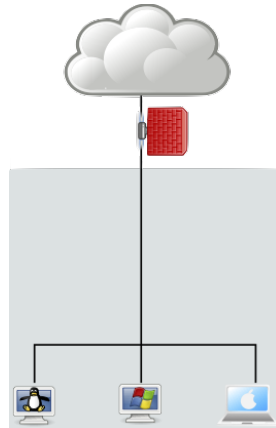
Bastion host

- Máquina com poucas aplicações em execução, projetada e configurada para resistir a ataques
  - Servidores proxy (SOCKS, HTTP, RTP, etc.)
- Somente pacotes oriundos e destinados a esta máquina podem passar pelo firewall



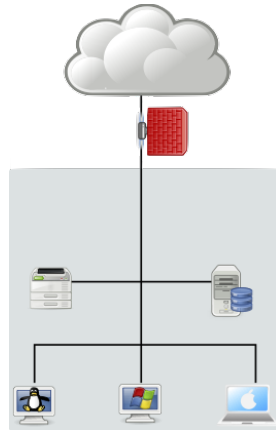
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas



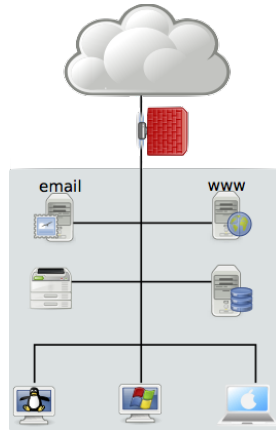
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.



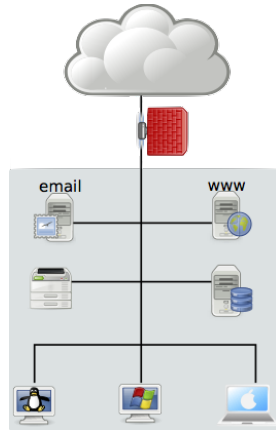
Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.
3. **Estações, servidores internos e externos**
   - WWW, SMTP, DNS, POP, IMAP, etc.



Organização da rede

1. **Somente com estações de trabalho**
   - Residencias e pequenas empresas
2. **Estações e servidores internos**
   - Servidor de impressão, arquivos, etc.
3. **Estações, servidores internos e externos**
   - WWW, SMTP, DNS, POP, IMAP, etc.



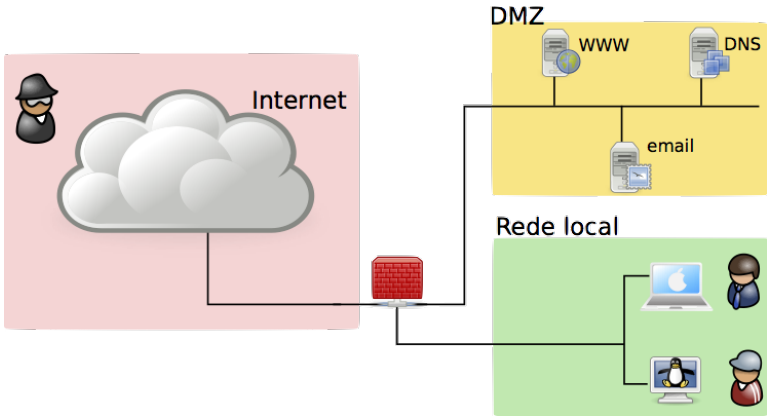
Como oferecer serviços externos sem que isto resulte em ameaças para a rede interna?

Zona desmilitarizada

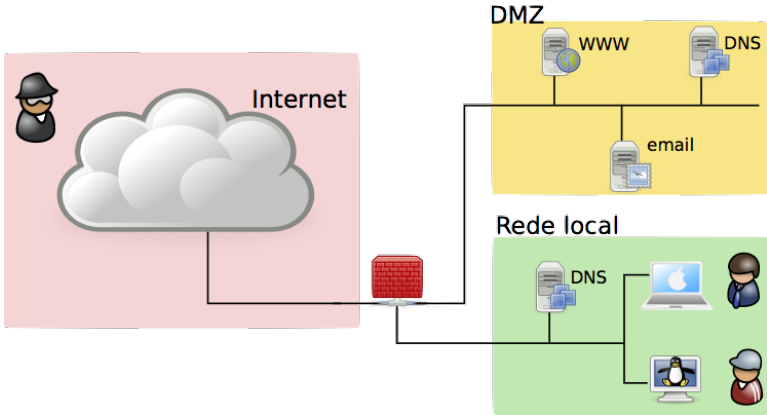
***Demilitarized Zone* (DMZ)**

- Segmento de rede tratado como **zona neutra** entre faixas em conflito (rede local e Internet)
  - Protege a rede interna contra ataques oriundos dos servidores externos, caso estes sejam comprometidos
- Local ideal para disponibilizar serviços que podem ser acessados tanto por máquinas da rede local como da rede externa (Internet)
  - Exemplo: DNS, WWW, SMTP
- Assume que as máquinas na DMZ seguem à risca a política de segurança e estão sempre com as últimas atualizações de segurança

Zona desmilitarizada



Replicar serviços pela DMZ e rede local



- Replicar serviços pela rede local e DMZ garante que se o servidor na DMZ for comprometido, isto não irá afetar os usuários da rede local
- Exemplo: Servidor de DNS apontando para máquinas maliciosas

Ataques

- Intercepção de tráfego
  - Sniffing
  - Spoofing
  - DNS spoofing ou cache poisoning
  - BGP hijacking
- Ataques de negação de serviço (DoS)
  - IP spoofing (camada de rede)
  - SYN flood (camada de transporte)
  - Slow loris (camada de aplicação)

Intercepção de tráfego

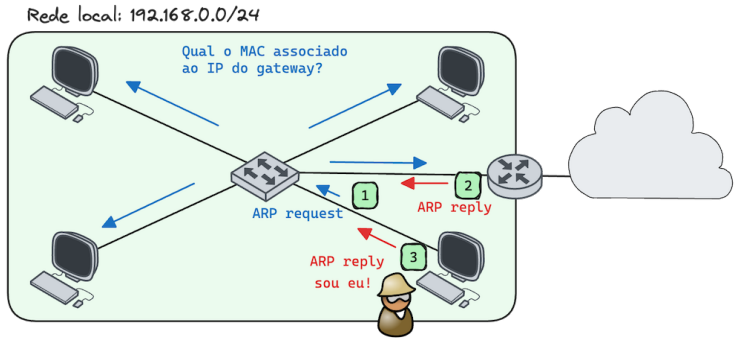
Packet Sniffing

- *Sniffing* é uma técnica de ataque usada para interceptar, capturar e analisar dados transmitidos em uma rede
  - Ethernet, Wi-Fi, Bluetooth, etc.
- O atacante precisa estar na mesma rede que a vítima, ou ter controle sobre um roteador intermediário
  - Em alguns casos de redes sem fio, é possível capturar pacotes mesmo sem estar conectado à rede
- Por ser um **ataque passivo** é difícil de ser detectado, porém é possível se proteger por meio da criptografia
  - VPN, HTTPS, SSH, criptografia ponta a ponta (E2EE)
- Faz uso de ferramentas como Wireshark, tcpdump, Ettercap e Kismet

Intercepção de tráfego por *Spoofing* I

- *Spoofing* é uma técnica de falsificação de identidade usada para enganar dispositivos ou usuários em uma rede
- Tipos comuns de *Spoofing*:
  - **ARP Spoofing:** Manipula o protocolo ARP para redirecionar tráfego
  - **IP Spoofing:** Falsifica endereços IP para mascarar o atacante
- Trata-se de um ataque **ativo**, onde o atacante pode interceptar, modificar e até mesmo injetar pacotes na rede

Intercepção de tráfego por *Spoofing* II



- Atacante faz *broadcast* para descobrir o endereço MAC do *gateway* (e da vítima) e quando o ARP cache for atualizado, envia um ARP *reply* (defasado) para sobrepor o endereço MAC do *gateway* (e da vítima)

Intercepção de tráfego por *Spoofing* III

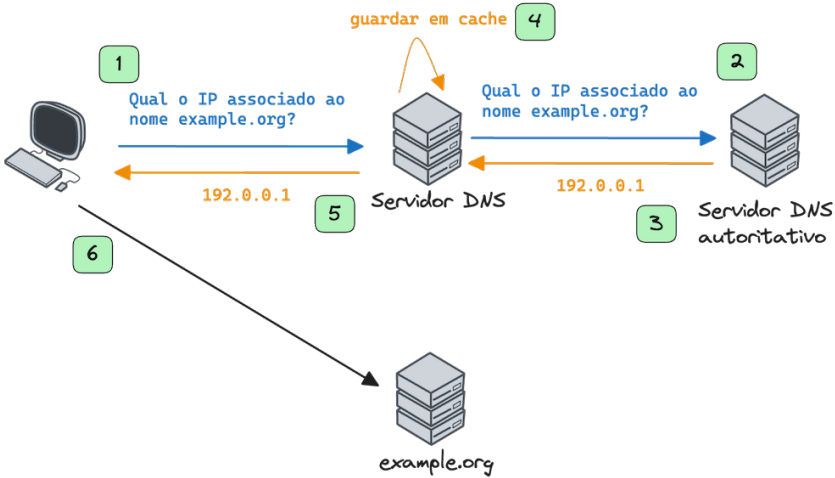
- **IP spoofing**, com atacante e vítima na mesma rede local (LAN) é algo simples de ser feito
  - Se a máquina que teve seu IP forjado estiver desligada, o atacante pode assumir seu IP e interceptar o tráfego destinado a ela
  - Se a máquina estiver ligada, poderá gerar conflitos de IP na rede e causar instabilidade
- Se atacante e vítima estiverem em redes diferentes, o atacante precisa ter controle sobre um roteador intermediário

Intercepção de tráfego por *DNS poisoning*

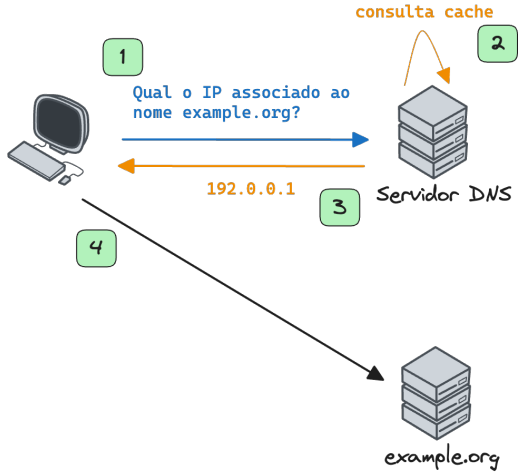
- *DNS poisoning* é um ataque que consiste em corromper a tabela de resolução de nomes de um servidor DNS, colocando informações falsas em seu *cache*
  - O atacante pode redirecionar o tráfego para um servidor malicioso, onde pode interceptar, modificar ou bloquear o tráfego
- O DNSSEC, extensão do protocolo DNS, usa criptografia de chave pública para garantir a autenticidade e integridade dos registros DNS
  - Proposta em 2005, ainda não é amplamente adotada

> **! Importante**
>
> Alguns softwares maliciosos alteram o arquivo `hosts` do sistema operacional, já outros alteram as configurações de DNS do roteador

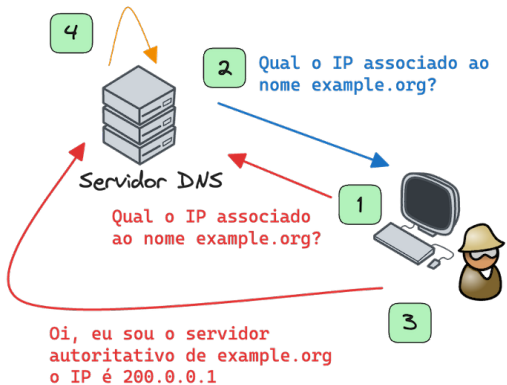
DNS poisoning



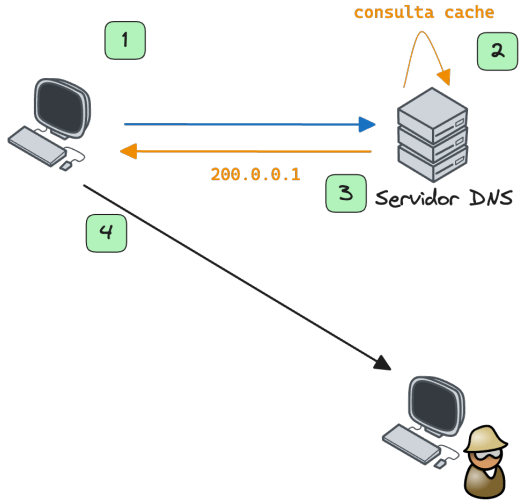
DNS poisoning



DNS poisoning



DNS poisoning



Sequestro de BGP

BGP hijacking

- *Border Gateway Protocol* (BGP) é um protocolo de roteamento usado para trocar informações de roteamento entre sistemas autônomos (AS)
- O ataque consiste em anunciar rotas falsas para um prefixo de IP, podendo redirecionar o tráfego para um servidor malicioso

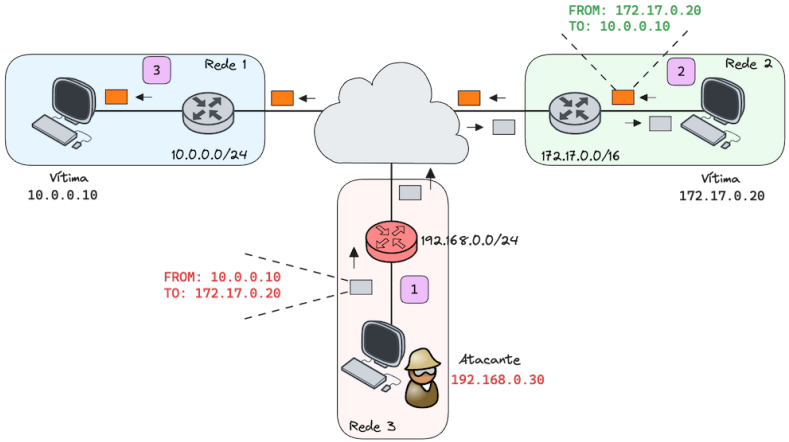
Border Gateway Protocol (BGP)

- 2010, China anunciou rotas para 15% do tráfego da Internet por 18 minutos
- 2017, Rússia fez anúncios para 7% do tráfego da Internet por 8 minutos
- Graças a Edward Snowden, sabemos que a NSA abusa da insegurança da rede para interceptar tráfego

Ataque de negação de serviço (DoS)

- **IP spoofing** é mais comum em ataques de negação de serviço (DoS), onde o atacante forja o IP de origem para dificultar a identificação do atacante
- Só são possíveis porque as redes permitem *spoofing*
  - http://bcp.nic.br/antispoofing

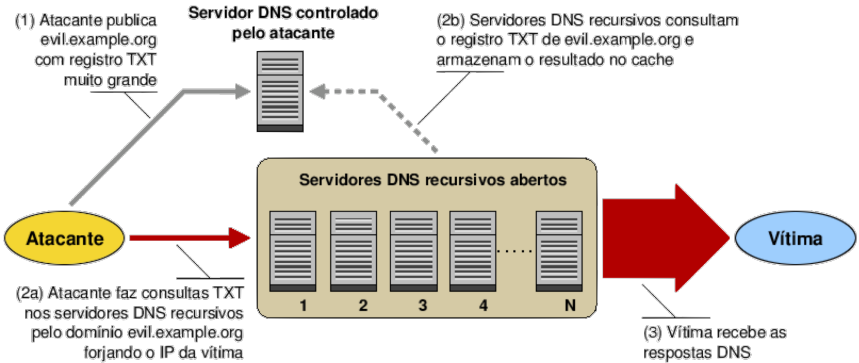
Ataque de negação de serviço (DoS) com IP *spoofing*



- Sobrecarrega um servidor com uma grande quantidade de tráfego (assemetria de tráfego, quando o tráfego de saída é maior que o de entrada)

DrDoS - Amplificação de DNS

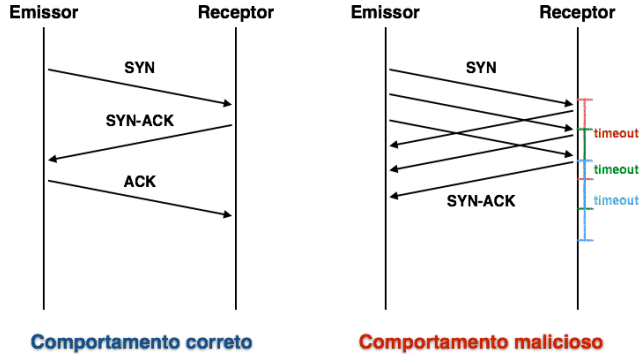
Por meio de servidores DNS recursivos abertos e IP *spoofing*



Fonte: http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Ataque SYN flood

Ataque de negação de serviço (DoS) na camada de transporte



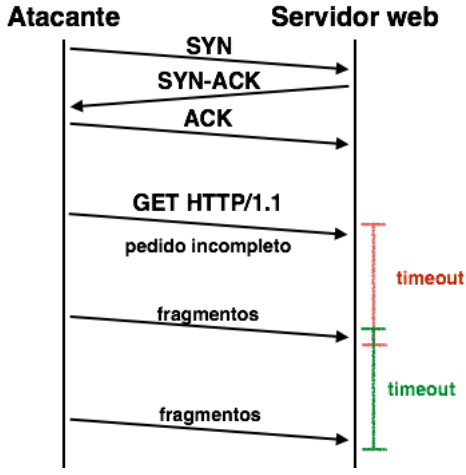
- Não responde SYN-ACK com o ACK
- IP de origem forjado (IP spoofing)

- Vítima mantém conexões abertas até o *timeout*
- Trata-se de um ataque volumétrico

Slowloris

Ataque de negação de serviço (DoS) na camada de aplicação

- Alvo: servidor web baseado em conexões, p.e. Apache HTTP
- Atacante não precisa de muito recurso (rede e processamento)



Rede Virtual Privada

***Virtual Private Network* (VPN)**

- VPN é uma rede privada virtual que estende uma rede privada sobre uma rede pública
- Utiliza criptografia para garantir a confidencialidade e integridade dos dados
- Pode ser do tipo
  - **VPN de acesso remoto** – usuário se conecta à rede corporativa
  - **VPN de site a site** – interconexão de redes (e.g. filiais de uma empresa)
  - **VPN pessoal** – foco na privacidade do usuário ao navegar na Internet

Rede Virtual Privada

VPN de acesso remoto

- Permite ao usuário acessar todos os recursos da rede corporativa, mesmo de servidores que não estejam acessíveis pela Internet

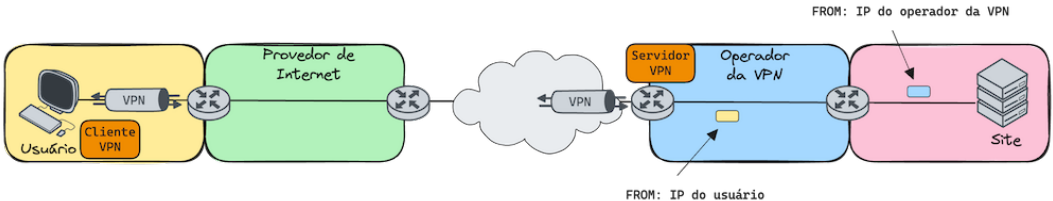
Rede Virtual Privada

VPN de site a site

- Todos os computadores de uma filial poderão atingir os computadores da outra filial, como se estivessem na mesma rede
- Traz segurança e privacidade para a comunicação entre as filiais

Rede Virtual Privada

VPN pessoal



- É importante escolher um provedor confiável, pois ele será capaz de:
  - Monitorar o tráfego e registrar os sites visitados
  - Bloquear o acesso a sites específicos
  - Injetar anúncios
- Em alguns casos pode haver redução de velocidade