Segurança Lógica

Segurança lógica

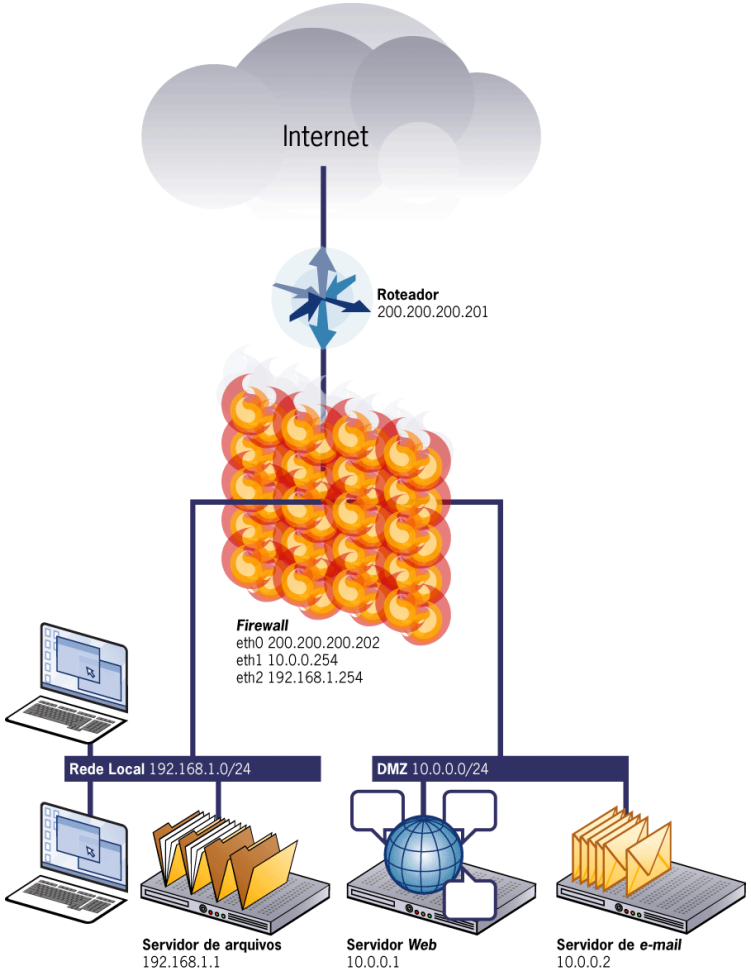
- Atenta contra ameaças ocasionadas por vírus, acessos remotos à rede, *backup* desatualizados, violação de senhas, etc.
- é a forma como um sistema é protegido no nível de sistema operacional e de aplicação.
- é considerada como proteção contra ataques, mas também significa proteção de sistemas contra erros não intencionais

Segurança lógica

- O controle de acesso lógico pode ser visualizado de dois modos diferentes:
  - A partir do recurso computacional que se pretende proteger.
  - A partir do usuário a quem se pretende dar privilégios e acesso aos recursos.

Firewall

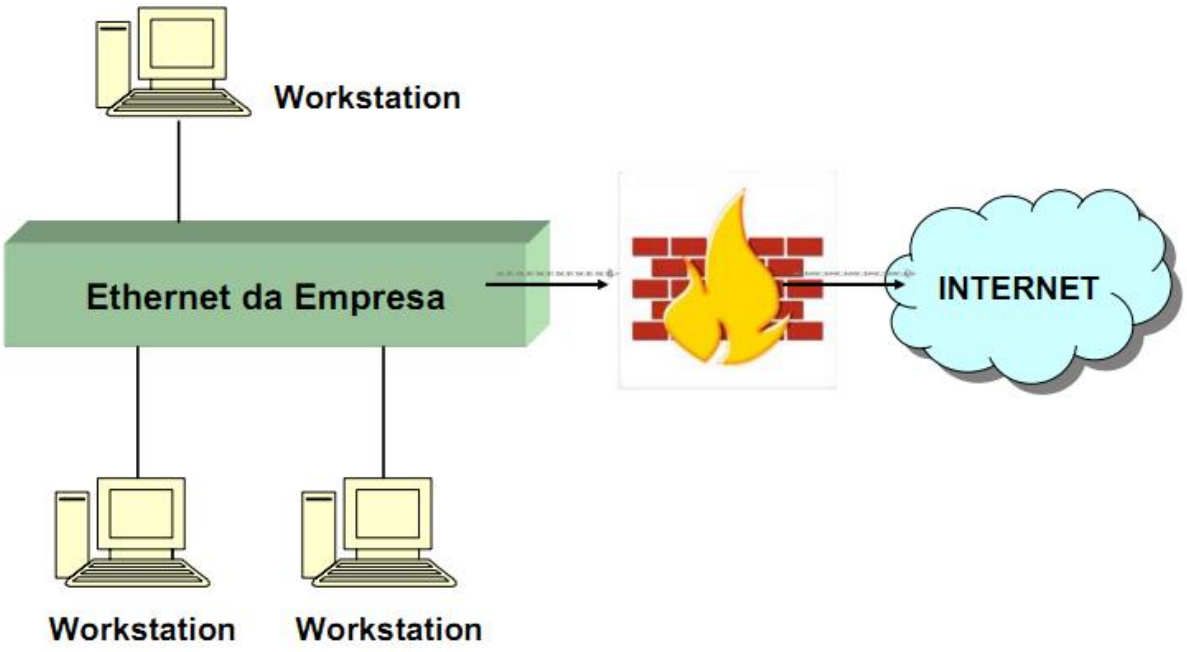
- Parede corta-fogo que protege a rede interna contra os perigos da internet
- Define o que pode e não pode entrar em seu computador ou rede.
- É diferente de antí-vírus.
- Serve a propósitos específicos:
  - Restringe a entrada a um único ponto controlado;
  - Previne que invasores cheguem perto de suas defesas mais internas;
  - Restringe a saída a um único ponto controlado.



Firewall

- Na Informática: previne que os perigos da Internet (ou de qualquer rede não confiável) se espalhem para dentro de sua rede interna
- Um firewall deve sempre ser instalado em um ponto de entrada/saída de sua rede interna
- Este ponto de entrada/saída deve ser único.
- O firewall é capaz de controlar todos os acessos de e para a sua rede.
- Pode estar em computadores, roteadores, configuração de redes, softwares específicos.

Firewall



O firewall ideal deve permitir a configuração das seguintes formas:

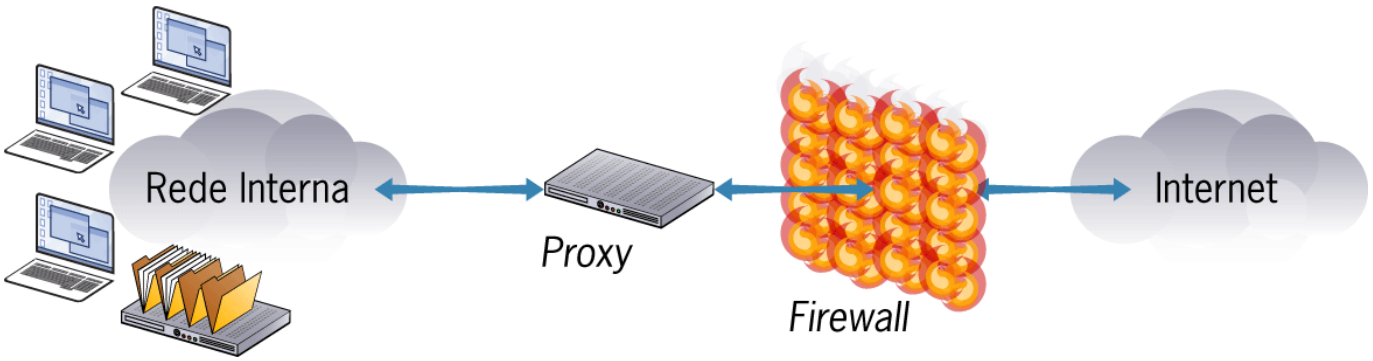
- controle de tráfego por portas.
- controle de tráfego por protocolo.
- controle de acesso por programa.

Necessidades em um *firewall*

- Capacidade para lidar com os desafios de gerência e controle de tráfego de rede, como:
  - Tratamento de TCP
  - Tratando pacotes UDP
  - Tratamento de ICMP
  - Ataques DOS de "*flood*" de pacotes
  - Aplicações P2P
  - Jogos na rede
  - Nat

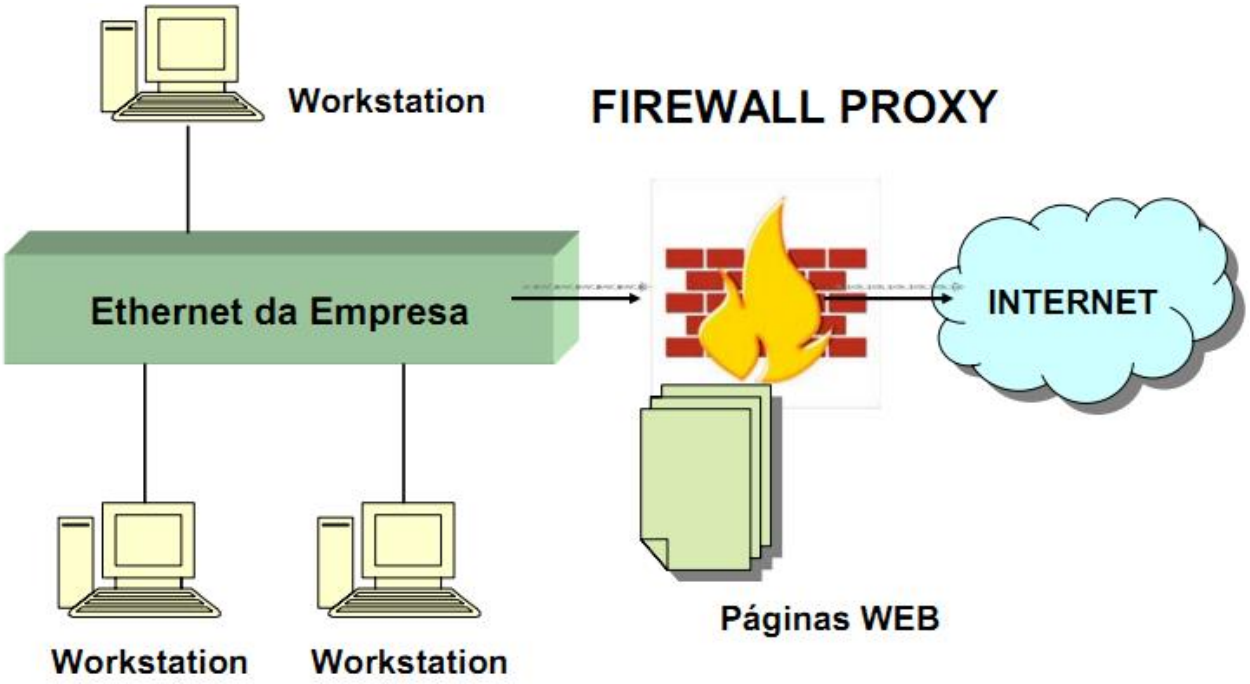
Application proxy (proxy de aplicação)

- Permite análise e filtragem até a camada de aplicação;
- Controla toda a comunicação de um serviço entre as máquinas internas e externas;
- Necessita de duas conexões: cliente → *proxy*, *proxy* → servidor remoto;
- Extranet: cliente externo → *proxy* interno, *proxy* interno → servidor interno;

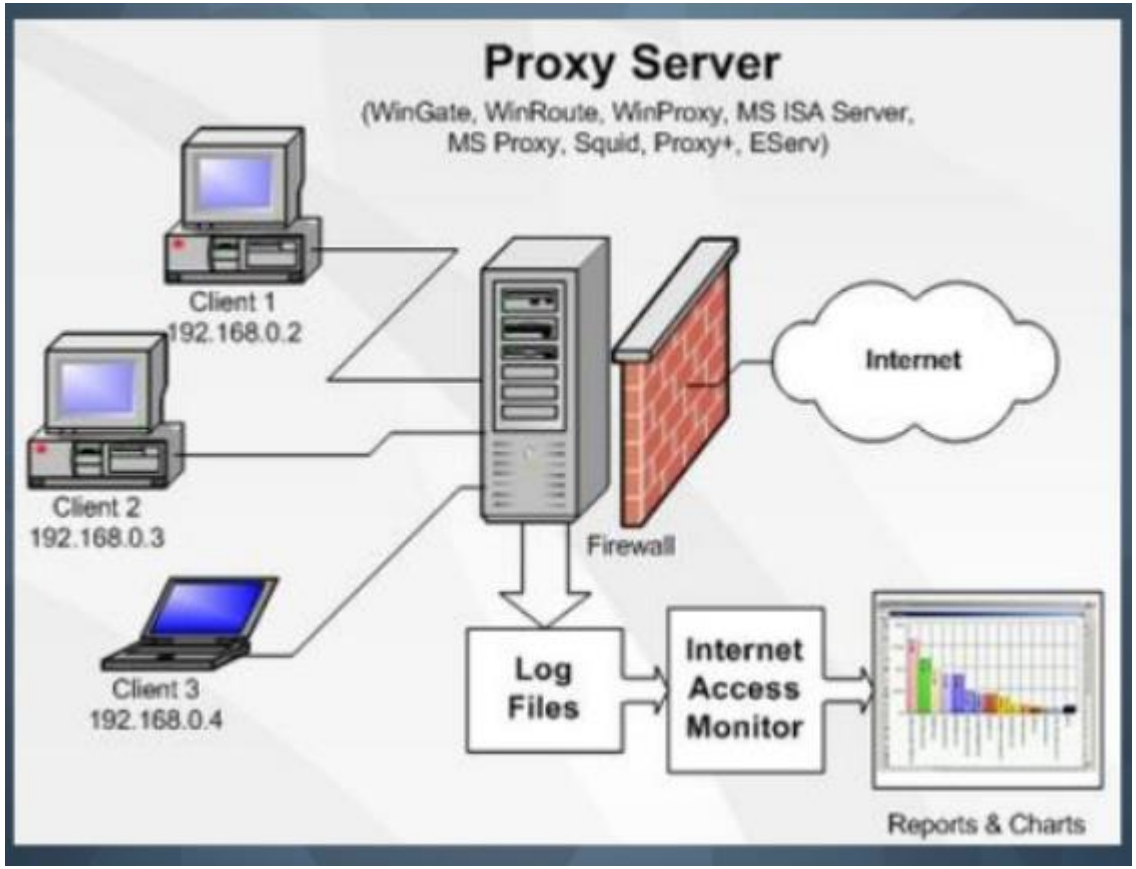


Application proxy (proxy de aplicação)

- Não há comunicação entre as máquinas internas e os servidores remotos;
- Pode agregar outros serviços.



Application proxy (proxy de aplicação)



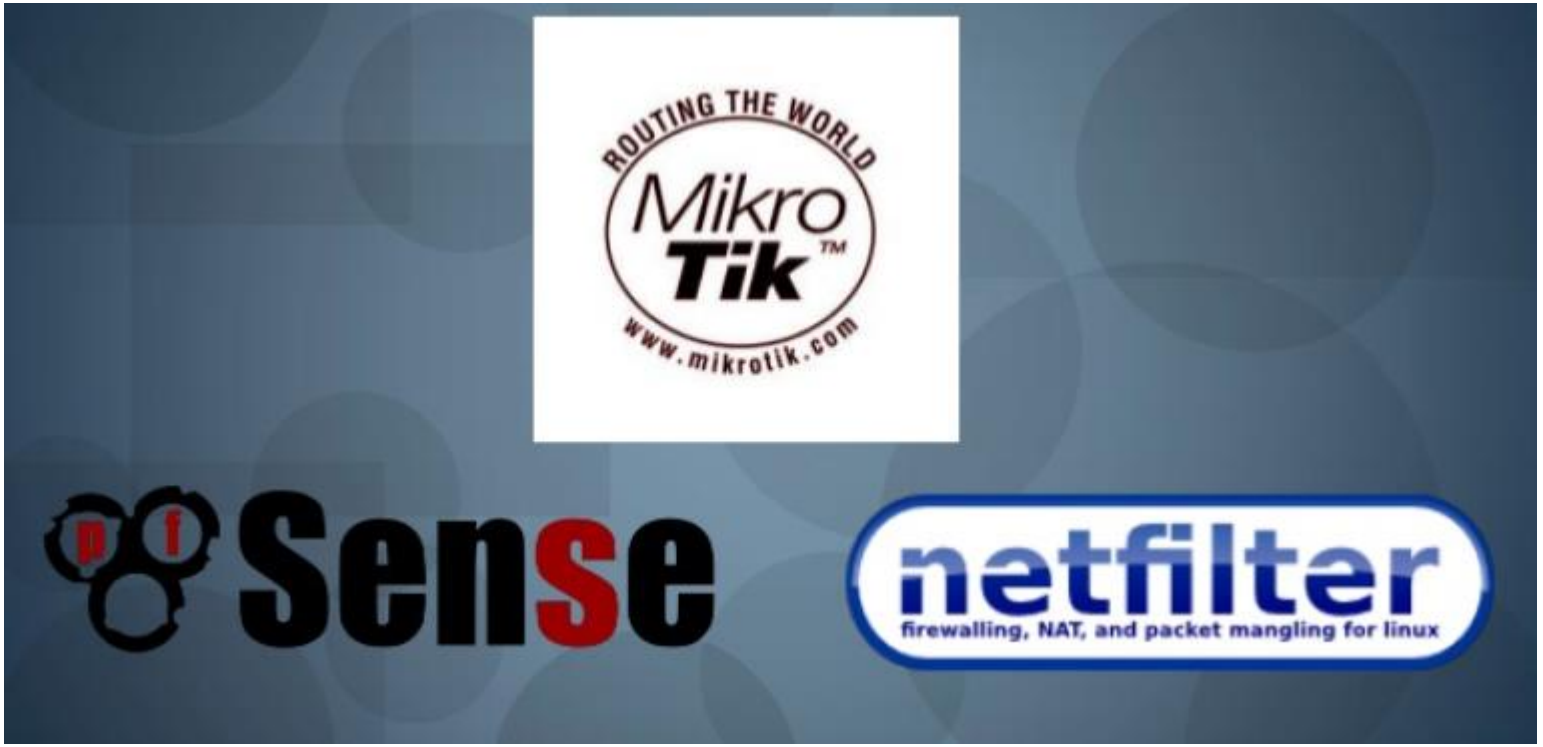
Exemplos de *firewalls*

- Linux Kernel 2.0.x:
  - IPF – Packet FilterB
- Linux Kernel 2.2.x:
  - IPchains – StateLess
- Linux Kernel 2.4.x / 2.6.x:
  - Iptables – Stateful Packet
- Outras soluções OpenSource:
  - IPFW (FreeBSD)
  - PF-sense
  - Edien-Firewall
- FireStarter

Firewall

Zone Alarm - *www.zonelabs.com*
BlackICE PC Protection - *http://blackice.iss.net/update_center/index.php*
Kerio Personal Firewall (atenção à porta 25) - *www.kerio.com/kerio.html*
Norton Personal Firewall - *www.symantec.com.br*
McAfee Personal Firewall - *http://br.mcafee.com*
Sygate Personal Firewall (insiste na versão paga) - *www.sygate.com*
Outpost Firewall - *www.agnitum.com/download/outpost1.html*
Tiny Personal Firewall - *www.tinysoftware.com*
Coyote Linux (roda até em um PC 486 sem HD e sem monitor, basta um drive de disquete) - *www.coyotelinux.com*
eTrust (da Computer Associates e vem com antivírus) - *www.my-etrust.com/microsoft/*

Firewall


ROUTING THE WORLD
MikroTik
www.mikrotik.com
pf Sense
netfilter
firewalling, NAT, and packet mangling for linux

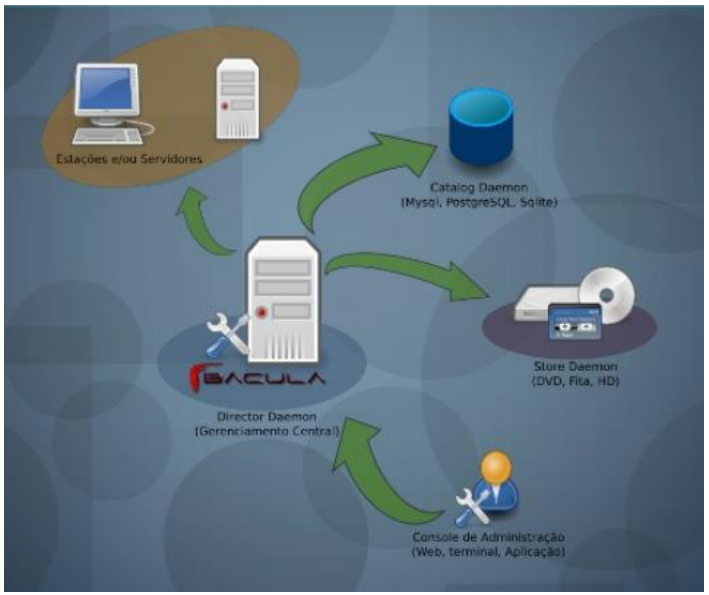
Antivírus

- Softwares elaborados para prevenção, detecção e eliminação de vírus de computador.
- Formas de detecção:
  - Escaneamento de vírus conhecidos
    - Base de dados de assinaturas.
  - Análise Heurística
    - Indícios em programas executados.
  - Busca Algorítmica
    - Extensão de arquivos, Tamanho, Strings.
  - Checagem de Integridade
    - Ids registradores.

- Vídeo...

Backup

- Backup pode ser também classificado como segurança lógica (Softwares de Backup)



Backup

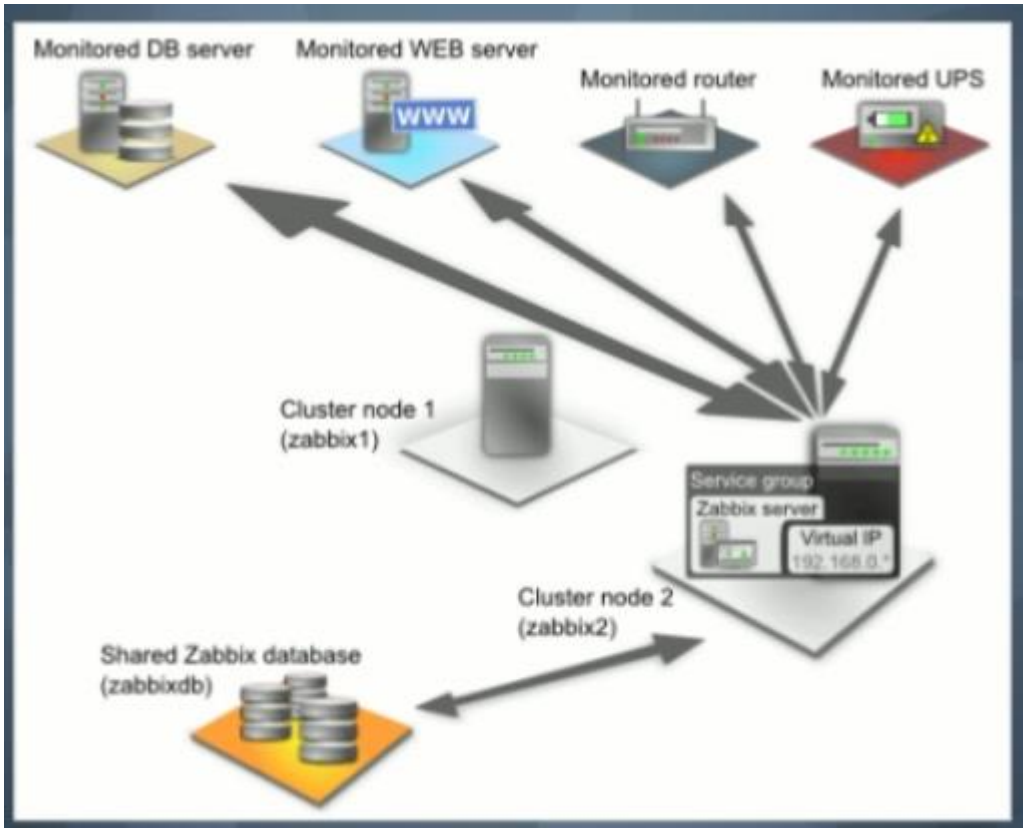
Monitoramento

Monitoramento

Definição

- Utilização de alguma plataforma/software para prover informações sobre a utilização da rede e de seus recursos.
- Motivos:
- Identificar e corrigir problemas.
- Analisar e medir disponibilidade e performance.
- Descentralizada

Monitoramento



Detectores de Intrusos

- IDS é a sigla de *Intrusion Detection Systems* (Sistemas de Detecção de Intrusão).
- Analisa o comportamento da rede ou do sistema, em busca de tentativa de invasão
- Utiliza dois métodos distintos
  - Detecção por assinatura
  - Detecção por comportamento
- Usa sensores espalhados pela rede ou pelo *host*

Detectores de Intrusos

- Detecção por assinaturas:
  - semelhante às assinaturas de antivírus
  - associam um ataque a um determinado conjunto de pacotes ou chamadas de sistema
  - não só detecta o ataque como também o identifica
  - exige atualizações frequentes do fabricante
- Detecção por comportamento:
  - observa o comportamento da rede em um período normal, e o compara com o comportamento atual da rede

IDS Snort

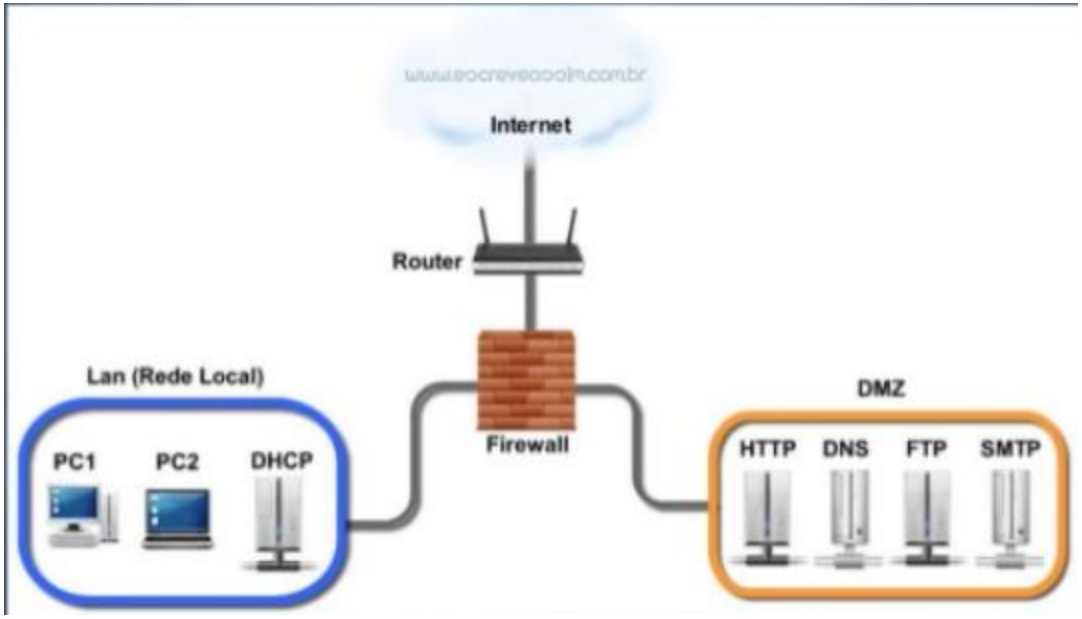
- Ferramenta de detecção de invasão NIDS *open source* (Linux); popular, rápida, confiável, exigindo poucos recursos do sistema:
  - Flexível nas configurações de regras
  - Possui grande cadastro de assinaturas
  - Atualizada constantemente frente às novas ferramentas de invasão

Segregação de Redes

Segregação de Redes

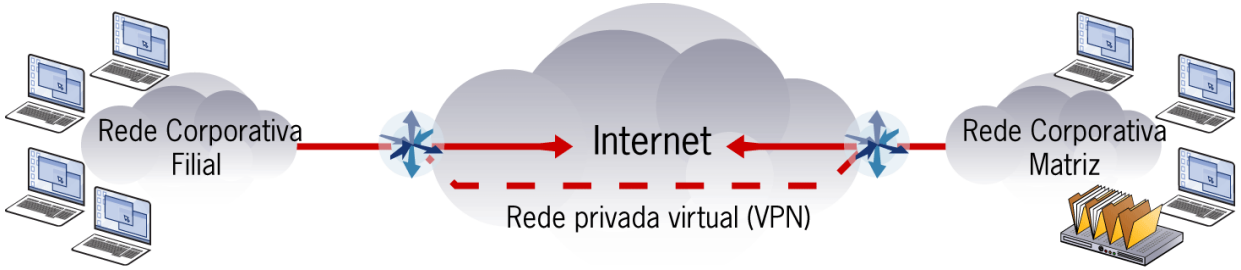
- **Definição**
  - Separação física ou lógica de uma sub-rede que compartilhará serviços entre uma LAN e outra rede externa.
  - DMZ (DesMilitarized Zone)
  - Interligada a LAN por Firewall
  - Separação Física (sempre que possível).

Segregação de Redes



Redes virtuais privadas - VPN

- *Virtual Private Network* (VPN) interliga duas redes privadas usando a internet como meio de interligação (rede pública)
- Usa normalmente canal de criptografia:
  - Rápida, para não comprometer o desempenho;
  - Segura, para impedir ataques;
  - Substitui linhas dedicadas a um custo reduzido;
  - Sujeita a congestionamento e interrupções na internet.
- Tipos:
  - Entre redes
  - Discada



Redes virtuais privadas - VPN

- Pense em uma empresa que precisa interligar duas de suas filiais. Existem algumas alternativas para solucionar o problema:

- Comprar equipamentos wireless e conectar as filiais por meio de um link de rádio.
- Conectar as duas por meio de um cabo de rede, o que pode ser totalmente inviável dependendo da distância entre estas.

- Pagar uma linha privada (LP) para que as filiais possam se comunicar.

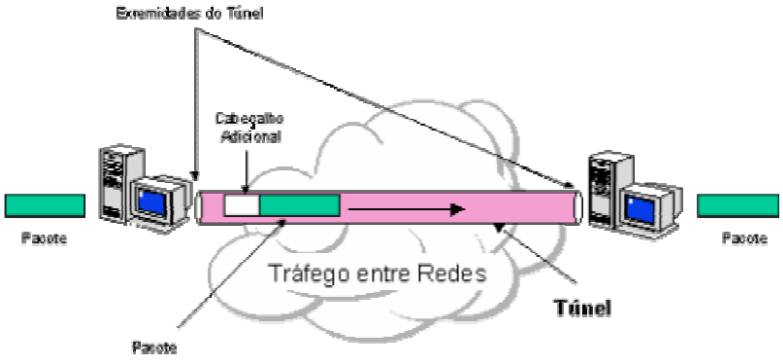
- Utilizar uma VPN.

Redes virtuais privadas - VPN

- Vantagens:
  - substituição de linhas dedicadas a custo baixo
  - uso de infra-estrutura já existente
- Desvantagens:
  - dados sensíveis trafegando em rede pública
  - sensível aos congestionamentos e interrupções que ocorrem na Internet
- As redes VPN são muito utilizadas por grandes empresas.

Redes virtuais privadas - VPN

- **Tunelamento:**
  - As redes virtuais privadas baseiam-se na tecnologia de tunelamento cuja existência é anterior as VPNs
  - pode ser definido como processo de encapsular um protocolo dentro de outro
  - antes de encapsular o pacote que será transportado, este é criptografado de forma a ficar ilegível caso seja interceptado durante o seu transporte.



Segurança de Software

- Auditoria
  - A auditoria implica em: quem fez o quê, quando, aonde?
  - Os registros de eventos (*logs*) são os primeiros objetos a serem consultados em uma auditoria.
  - Através dos log's você pode:
    - Detectar uso indevido do seu computador,
    - Detectar um ataque,
    - Auditar ações, como um programa utilizado,
    - Detectar problemas de hardware ou software

Auditoria – Logs

Cuidados:

- Mantenha o seu computador com o horário correto.
- verifique o espaço em disco livre em seu computador.
- Fique atento e desconfie caso perceba que os logs do seu computador foram apagados.
- Restrinja o acesso aos arquivos de logs.

Segurança de Software
Proteção contra infecção

- **Proteção contra infecção**
- Essa segurança inclui, principalmente, segurança contra vírus, worm, cavalo de tróia e controle de software instalados
- impedir que nenhum software não autorizado pelo administrador seja instalado nas máquinas de trabalho ou que seja instalado um software pirata.
- Garantem que os sistemas e os recursos de informação neles contidos não sejam contaminados
  - **antivírus e filtros de conteúdo**: incluindo trojans, worms,

    spyware e adware
  - **vulnerability scanners**: varredura nos sistemas em busca de falhas de segurança, a partir de uma base de conhecimento de vulnerabilidades existentes em elementos de rede