Faculdade de Computação

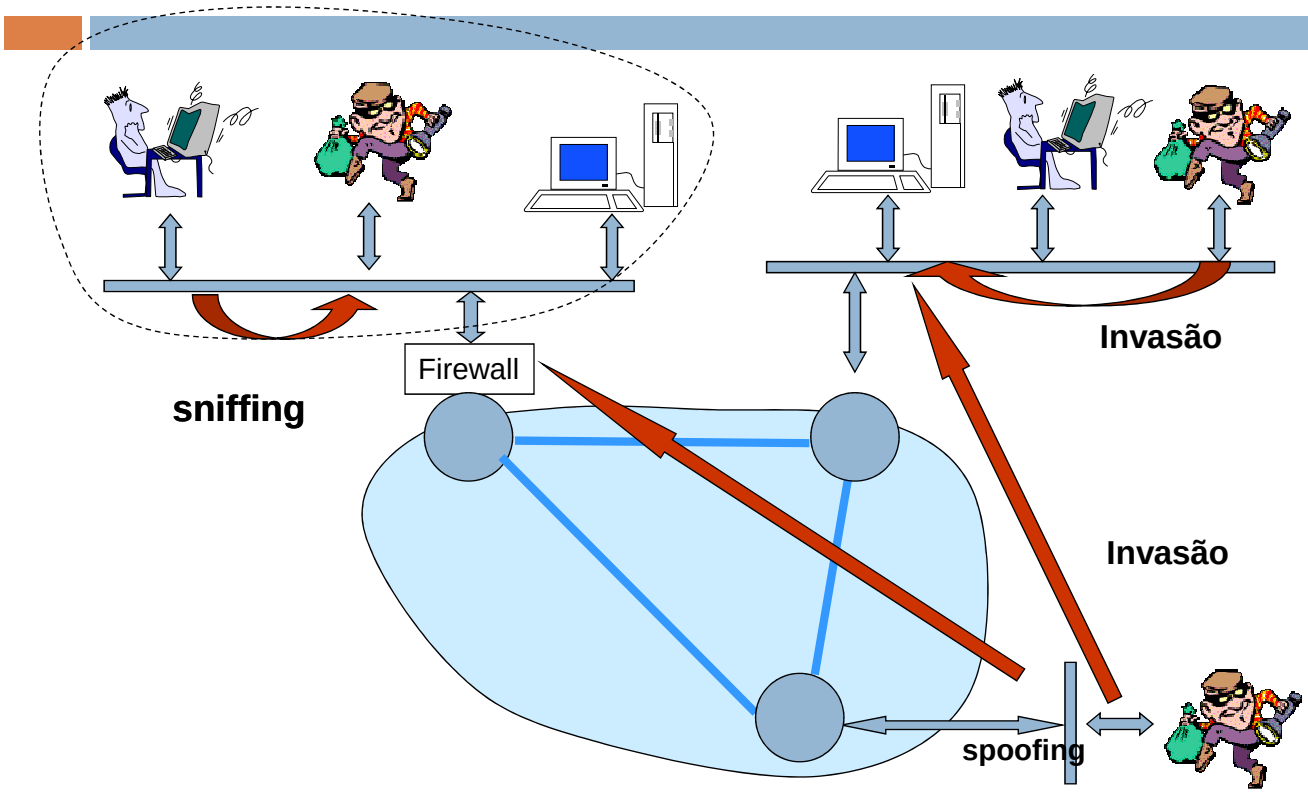
Redes de Computadores

LAB 11- FIREWALLS

Hana Karina S. Rubinsztejn

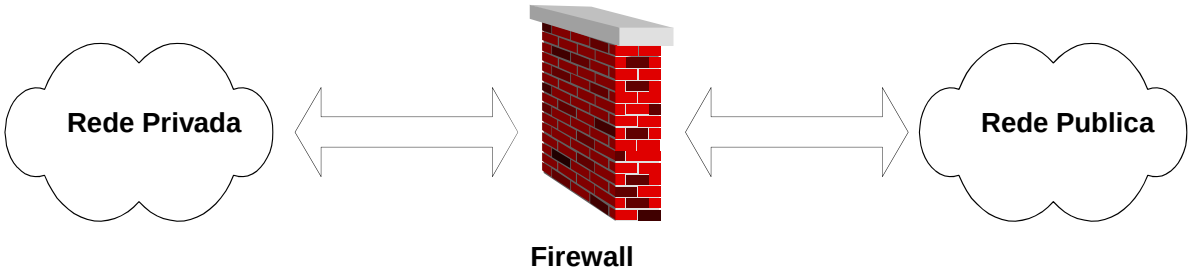
hana@facom.ufms.br

Riscos a Segurança de uma Rede



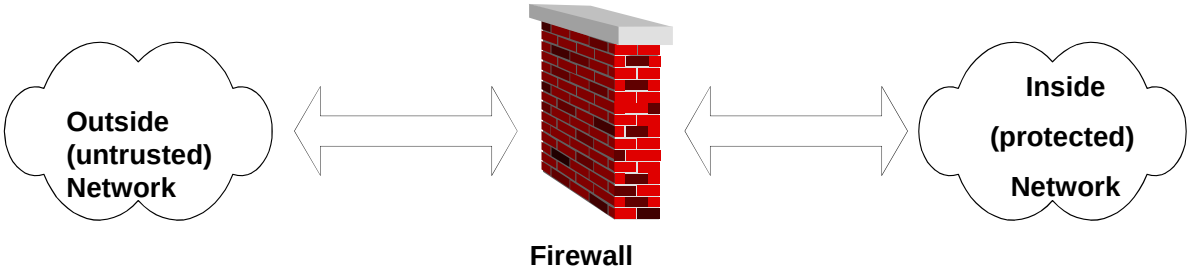
Firewall

- Firewalls são componentes de uma Política de Segurança que visam restringir ou controlar o fluxo de informação entre duas ou mais redes.



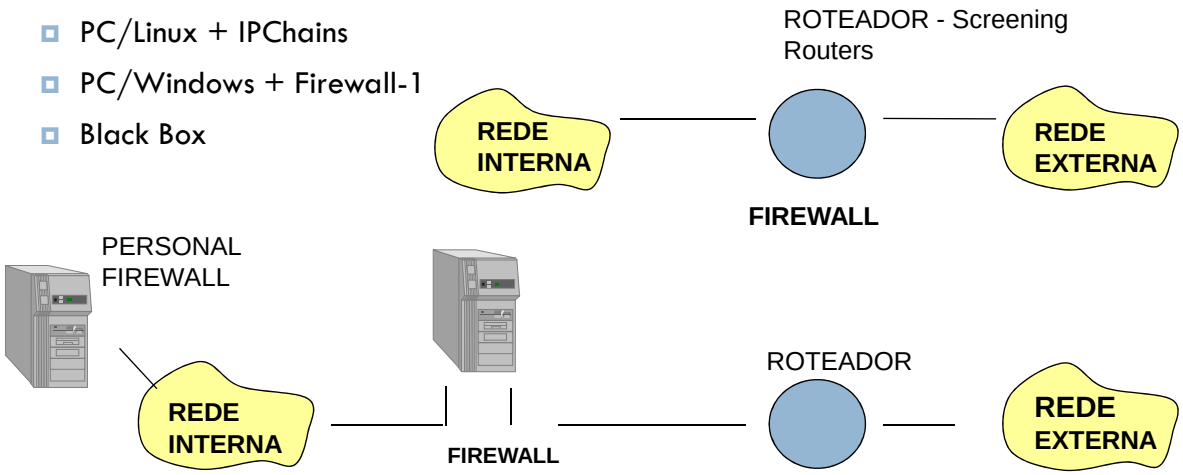
Ponto de Obstrução

- Força os intrusos a usar um canal estreito
- Facilita a monitoração e controle
- Um firewall é um ponto de obstrução
- Um ponto de obstrução é inútil se há caminhos alternativos de penetração
  - modems e outras conexões à Internet



Implementação Física do Firewall

- No software do Roteador
- No software de uma estação dedicada (um PC com duas placas de rede).
- Tipos de FW
  - Roteador CISCO
  - PC/Linux + IPChains
  - PC/Windows + Firewall-1
  - Black Box



Para que servem?

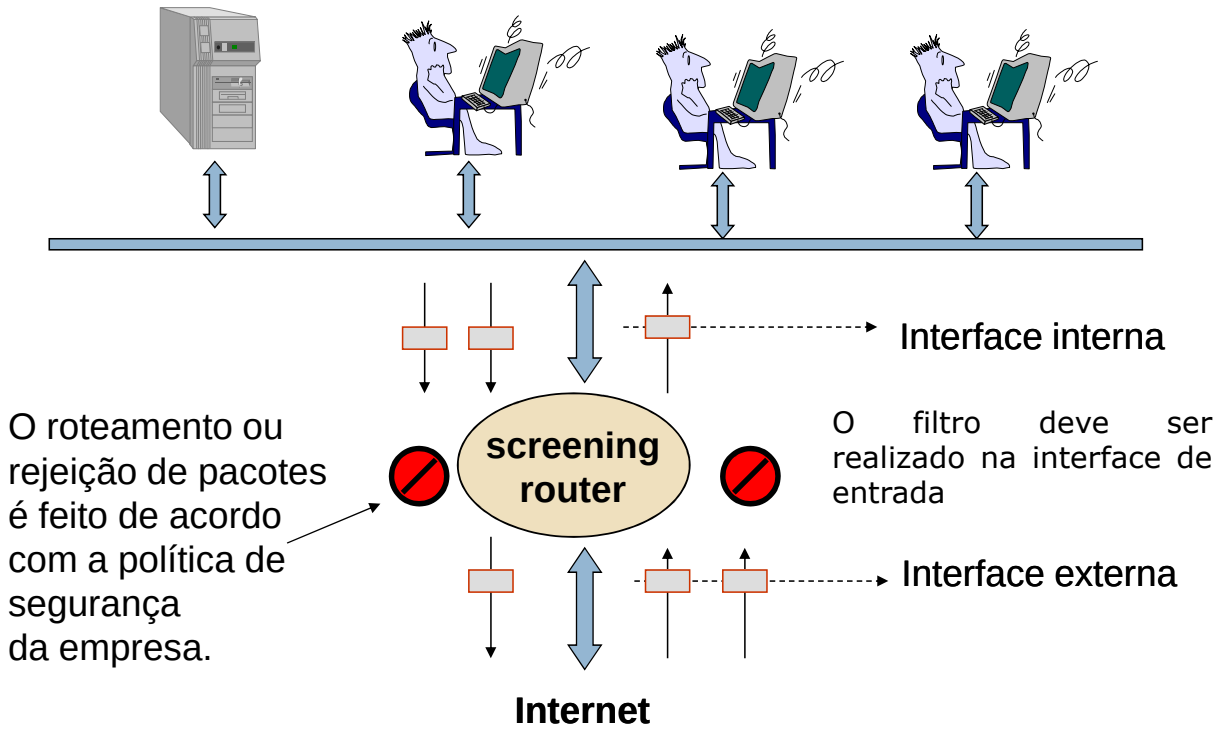
- Controlar os serviços a serem disponibilizados.
- Proteger uma rede de ataques externos/internos.
- Registrar a comunicação entre as máquinas internas e externas.
- Esconder máquinas internas.
- Traduzir/Converter endereços IP (NAT).
- Criptografar e autenticar tráfego de dados.

Para que não servem?

- Bloquear comunicação entre máquinas da mesma sub-rede.
- Impedir ataques de pessoas internas.
- Detalhes de acesso à aplicação
  - ex: usuário xyz pode conectar-se via telnet do exterior mas os outros usuários não
  - ex: somente os arquivos do diretório /public podem ser transferidos em sessões FTP
- Vírus na rede interna
- Cavalos de tróia
- Engenharia Social
- Ameaças físicas
- Configuração mal feita

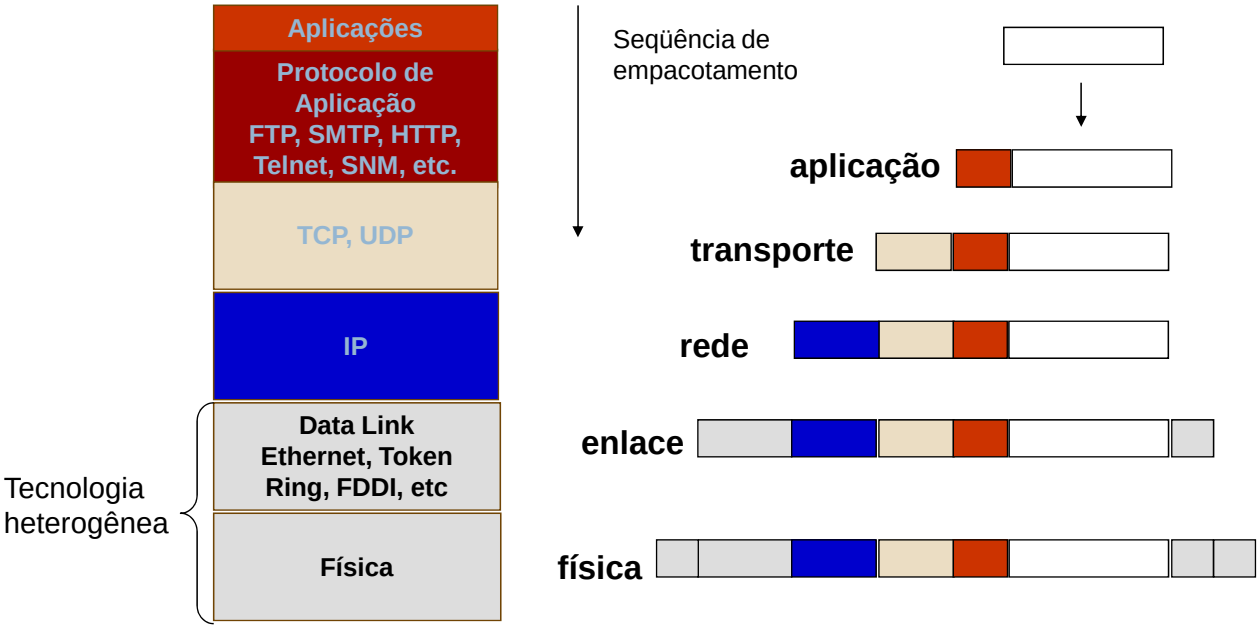
Filtros de pacotes por si só não garantem segurança, apenas limitam o espaço de ataque de um invasor.

Filtragem de Pacotes

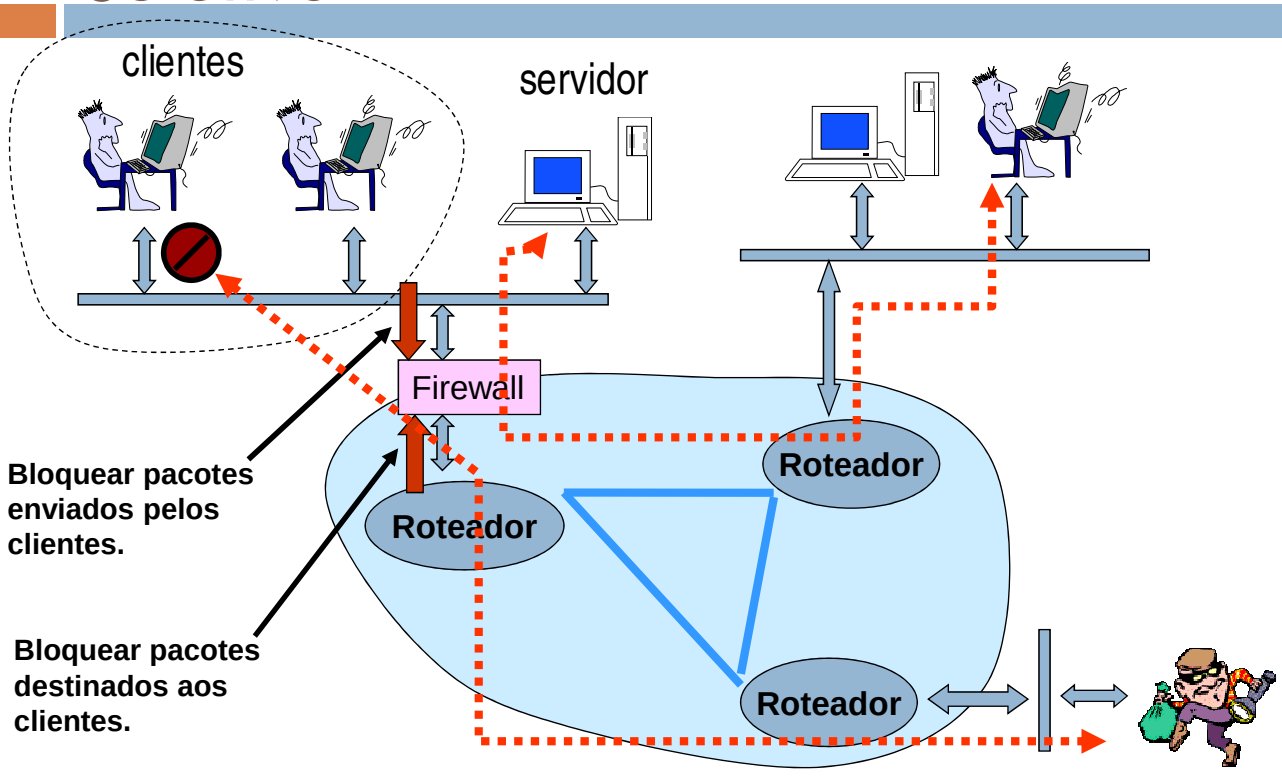


Filtragem de Pacotes

- A filtragem de pacotes é feita com base nas informações contidas no cabeçalho dos protocolos.



Camada de Rede → Roteamento Seletivo



Níveis de Filtragem

- Aplicação (FTP, Telnet, HTTP, HTTPS, SMTP, DNS)
- Transporte (TCP ou UDP)
- Rede (IP)
- Acesso (Ethernet, Anel, FDDI...)
  - Endereço MAC
    - Controle de acesso a rede feito em Switches

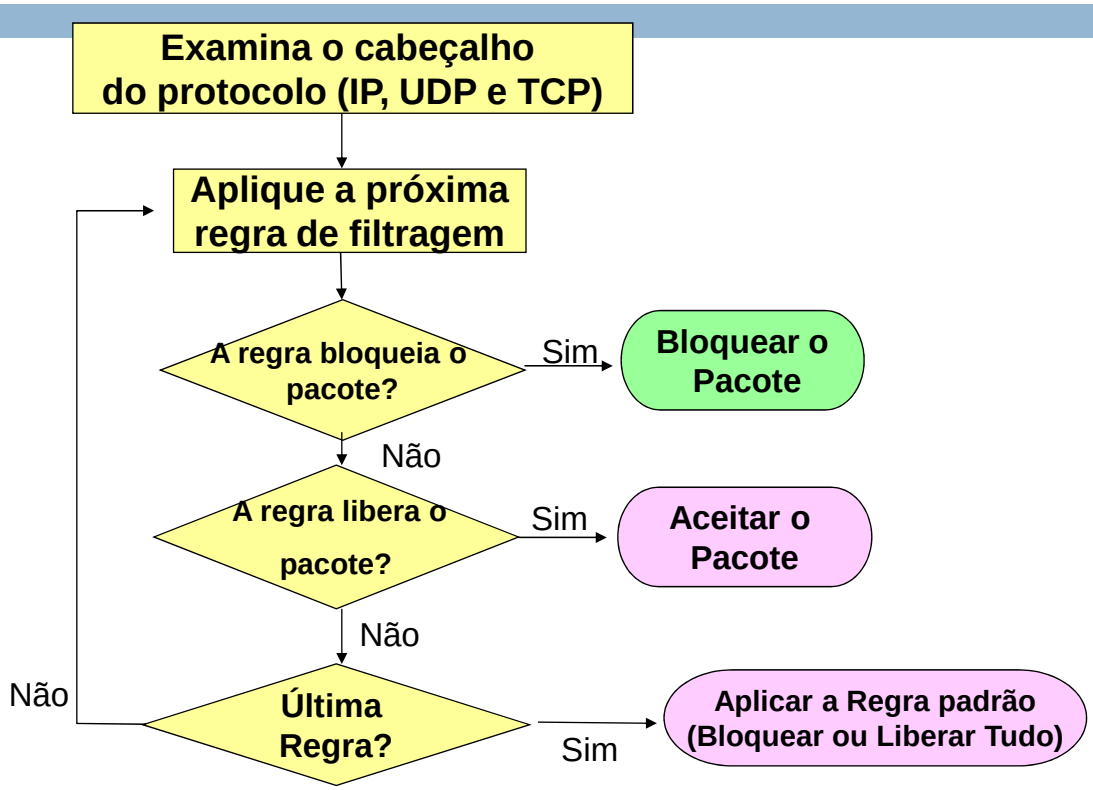
Considerações sobre regras de filtragem

- Estratégias Básicas
  - Default Deny
    - "Tudo o que não for expressamente permitido é proibido"
  - Default Permit
    - "Tudo o que não for expressamente proibido é permitido"

Considerações sobre regras de filtragem

- Default Deny
  - Examine os serviços desejados
  - Considere os riscos de segurança desses serviços e como provê-los de forma segura
  - Permita apenas os serviços que você domina e que tenham necessidade legítima
  - Analise cada nova requisição de serviço
  - Constitui uma proteção contra novas vulnerabilidades em serviços não Habilitados

Regras de Filtragem



Filtragem IP

- Tipos de filtros
  - endereço IP origem
  - endereço IP destino
  - tipo de protocolo
- Considerações sobre
  - endereço de origem
    - pode ser forjado
      - *IP Spoofing*

Filtragem de Pacotes IP

- Proteção usualmente implementada em roteadores e softwares firewall
- Bom desempenho
- Totalmente transparente para o usuário final
- Abordagem "tudo ou nada" em relação a serviços
- Não modifica o serviço nem protege operações individuais do serviço
- Se um serviço desejável possui operações inseguras (bugs), a filtragem de pacotes não pode protegê-lo

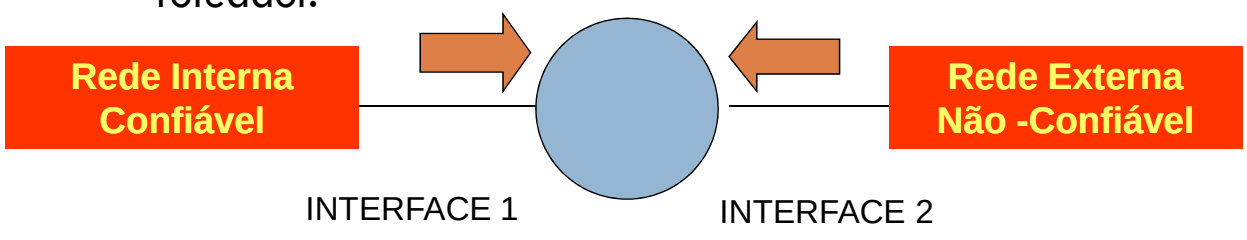
Exemplo de Filtros de Pacotes

- Bloqueie todas as conexões originadas de redes externas, exceto SMTP e HTTP
- Bloqueie sempre serviços perigosos como TFTP, X Windows, NFS, etc.

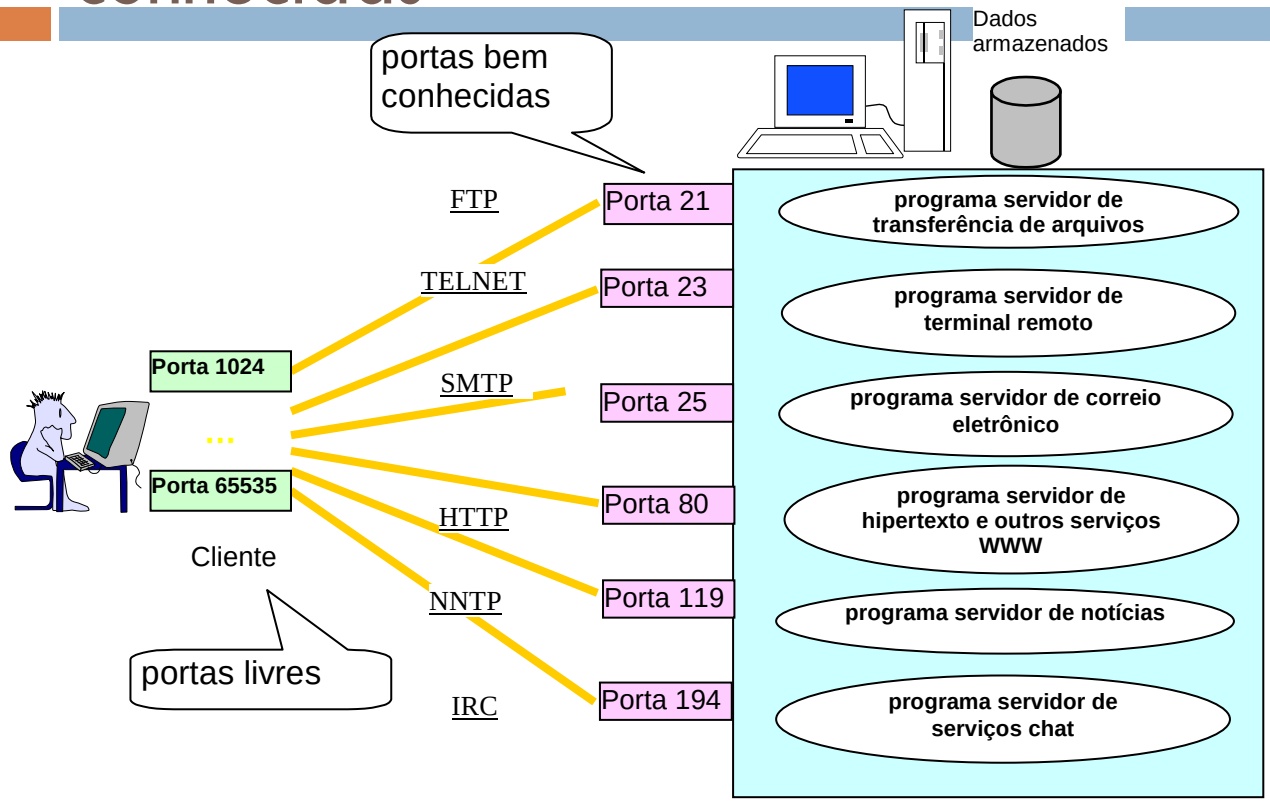
Exemplo

AÇÃO	INTERFACE	IP ORIGEM	IP DESTINO
permitir	1 (sair)	200.17.98.0: 200.17.98.255	*
permitir	2 (entrar)	*	200.17.98.0: 200.17.98.255
bloquear	*	*	*

- Interpretação:
  - Geralmente, as regras são definidas individualmente para cada interface.
  - Cada interface controla apenas os pacotes que entram no roteador.

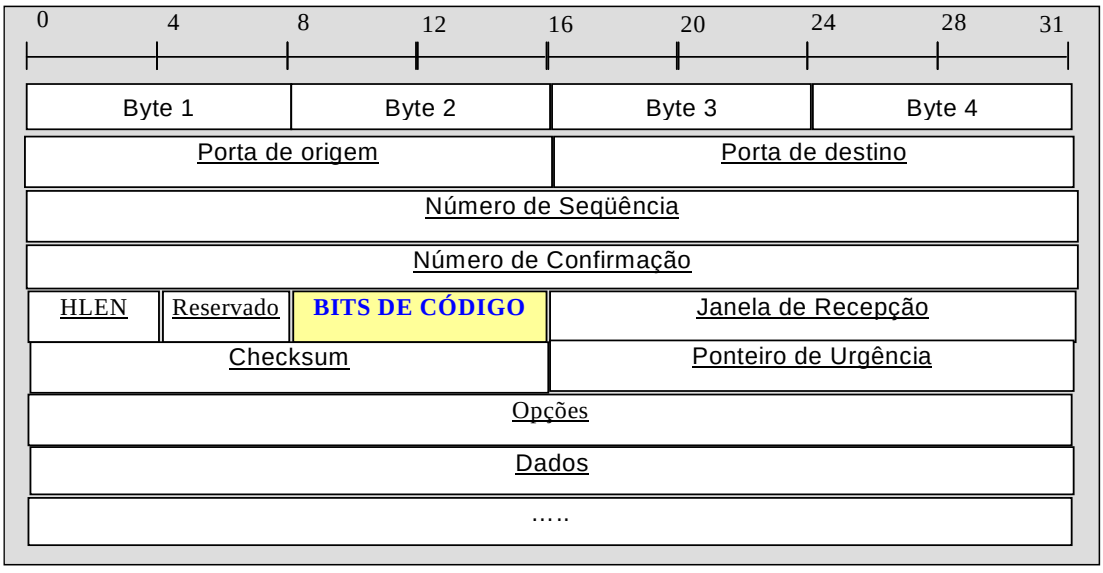


Exemplos de portas bem conhecidas



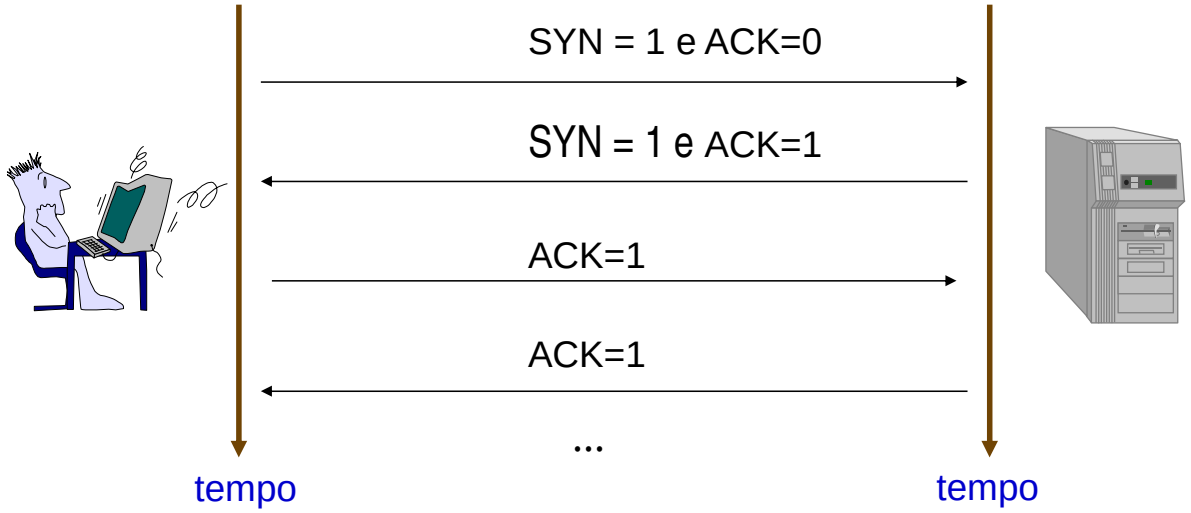
Flags TCP

- RES: Reservado (2 bits)
- URG: Urgent Point
- ACK: Acknowlegment
- PSH: Push Request
- RST: Reset Connection
- SYN: Synchronize Seqüence Number
- FIN: Mais dados do transmissor



Flag ACK

- Uma conexão TCP sempre se inicia com o cliente enviando um pacote com o *flag* SYN = 1 e ACK= 0.



Flags TCP

- Para bloquear uma conexão TCP, basta filtrar o primeiro pacote enviado
- O primeiro pacote contém toda a informação necessária para a conexão, sendo caracterizado pelo flag ACK=0
- Todos os demais pacotes da conexão TCP possuem flag ACK=1
- Controlando o flag ACK, é possível permitir que hosts internos iniciem conexões com hosts externos e proibir inícios de conexão na direção oposta
  - Conexão estabelecida ("established")
    - permit tcp any any established

Exemplo de Regras de Filtragem

regra	ação	interface/ sentido	protocolo	IP origem	IP destino	Porta origem	Porta destino	Flag ACK
1	aceitar	rede interna/ para fora	TCP	interno	externo	>= 1024	80	*
2	aceitar	rede externa/ para dentro	TCP	externo	interno	80	> 1023	1
3	rejeitar	*	*	*	*	*	*	*

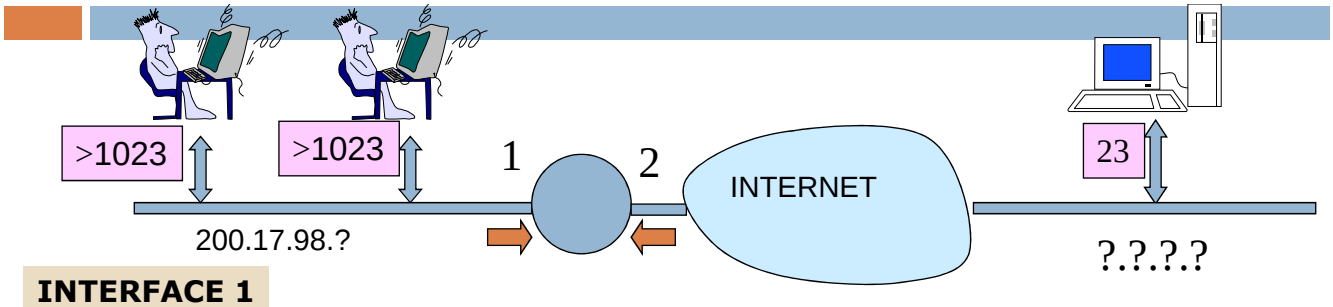
- O símbolo "*" indica que qualquer valor é aceitável para regra.

Exemplo

Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Int/Ext	tcp	interno	*	> 1023	23	*
permitir	Ext/Int	tcp	*	interno	23	> 1023	1
negar	*	*	*	*	*	*	*

- **Tudo que não é permitido é PROIBIDO!**
- Interpretação:
  - Hosts Internos podem acessar servidores de telnet internos ou externos.
  - Hosts externos podem apenas responder a requisições, não podem iniciar um diálogo (estabelecer uma conexão).

Exemplo



INTERFACE 1

Ação	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	tcp	200.17.98.0:24	*	> 1023	23	*
negar	*	*	*	*	*	*

INTERFACE 2

Ação	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
Permitir	tcp	*	200.17.98.0:24	23	> 1023	1
negar	*	*	*	*	*	*

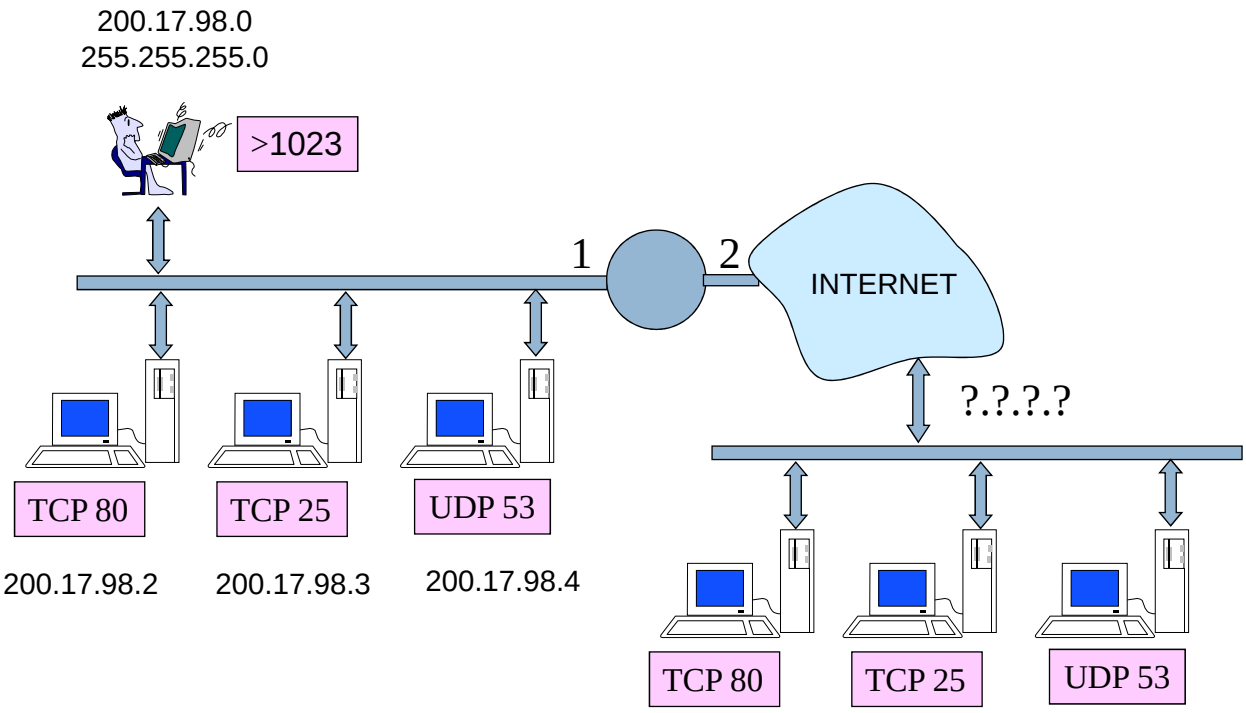
Seqüência de Criação de Regras

- A seqüência na qual as regras são aplicadas pode alterar completamente o resultado da política de segurança. Por exemplo, as regras de aceite ou negação incondicional devem ser sempre as últimas regras da lista.

O deslocamento de uma regra genérica para cima anula as demais.

Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Int/Ext	tcp	interno	*	> 1023	23	*
permitir	Ext/Int	tcp	*	interno	23	> 1023	1
permitir	Ext/Int	tcp	*	interno	>1023	80	*
permitir	Int/Ext	tcp	interno	*	80	> 1023	1
negar	*	*	*	*	*	*	*

Exercício



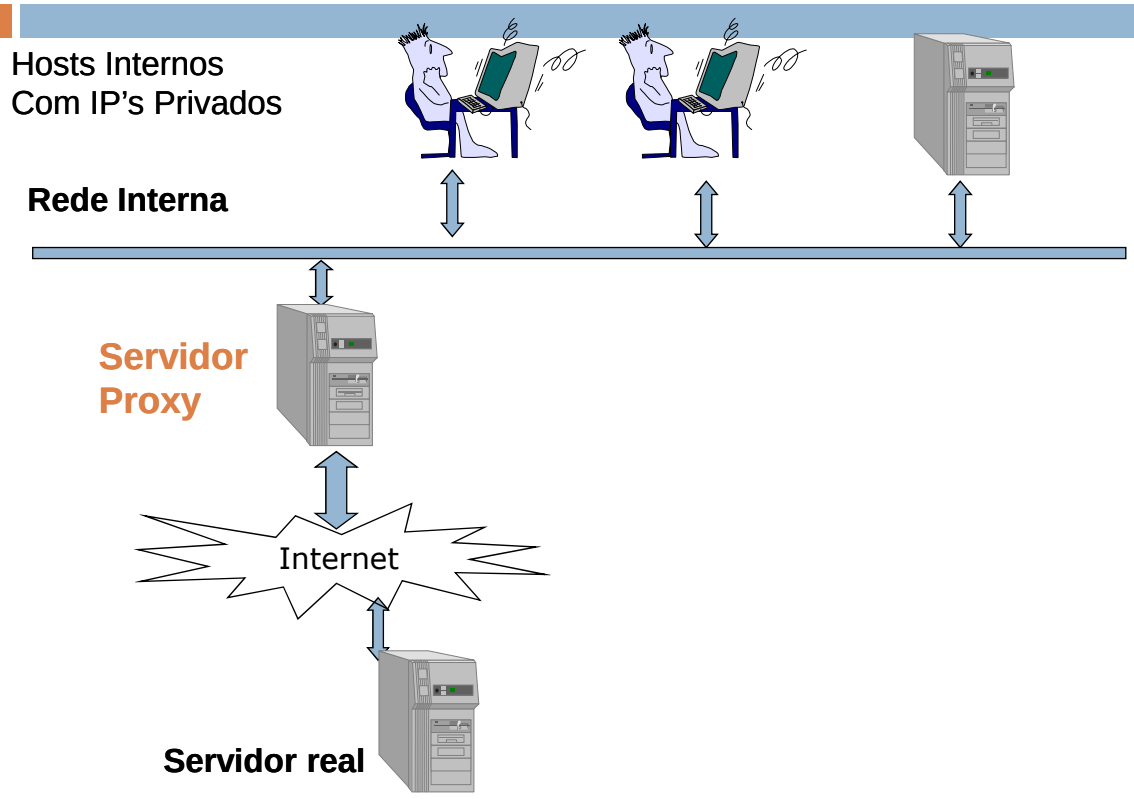
Exercício

- Defina as regras de filtragem para implementar a seguinte política de segurança:
  a) Os computadores da rede Interna podem acessar qualquer servidor Web na Internet.
  b) Computadores da rede Externa podem acessar apenas o servidor Web da rede Interna.
  c) O servidor DNS interno deve poder se comunicar com outros servidores DNS na Internet.
  d) O servidor de email interno deve poder se comunicar com outros servidores de email da Internet.
  e) Todos os demais acessos são proibidos.

Exercício

AÇÃO	INTERFACE	PROTOCOLO	IP ORIGEM	IP DESTINO	PORTA ORIGEM	PORTA DESTINO	FLAG ACK

Servidores Proxy

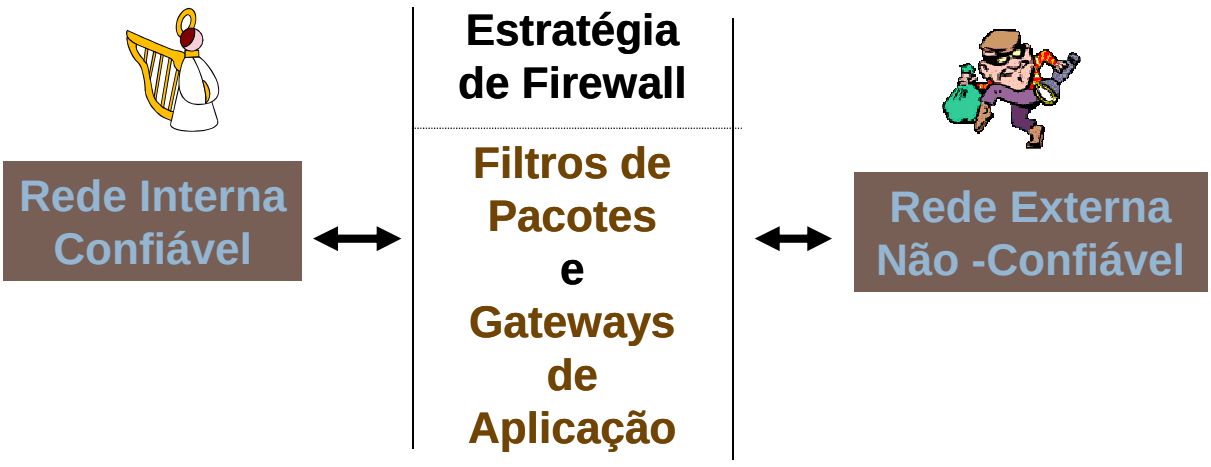


Servidores Proxy

- Servidores proxy (procuradores) são programas que lidam com servidores externos em nome de clientes internos
- Os clientes proxy comunicam-se com servidores proxy, que, por sua vez, enviam as solicitações aprovadas para os servidores reais, bem como encaminham as respostas destas solicitações de volta para os clientes
- Atuam até ao nível de camada de aplicação

Arquiteturas de Filtros de Pacotes

- Filtros de Pacotes são os principais componentes dos Firewalls.



Arquiteturas Básicas de Firewall

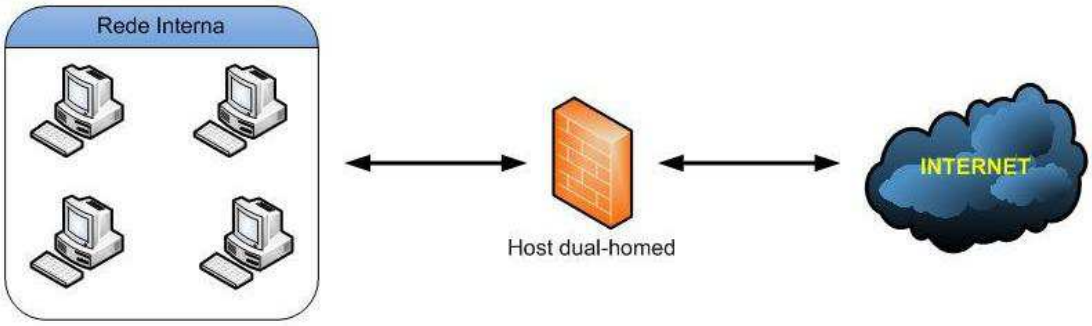
- A arquitetura de um firewall é definida de acordo com as necessidades da organização, tendo tantos níveis de acesso quanto forem necessários.
  - Pode-se montar uma arquitetura eficiente utilizando técnicas de rede desmilitarizada (DMZ), sistemas de detecção de intrusão (IDS), analisadores de pacotes em camada 7, etc.

Arquiteturas Básicas de Firewall

- Vamos descrever aqui três arquiteturas de firewall:
  1. Dual-Homed Host com Proxy
  2. Filtragem Simples de Pacotes (*Screened host architecture*)
  3. DMZ (Rede de Perímetro) (*Screened subnet*)
     - Uma rede adicionada entre a rede protegida e uma rede externa, com o objetivo de proporcionar uma camada a mais de segurança. Também chamada de DMZ (De-Militarized Zone).

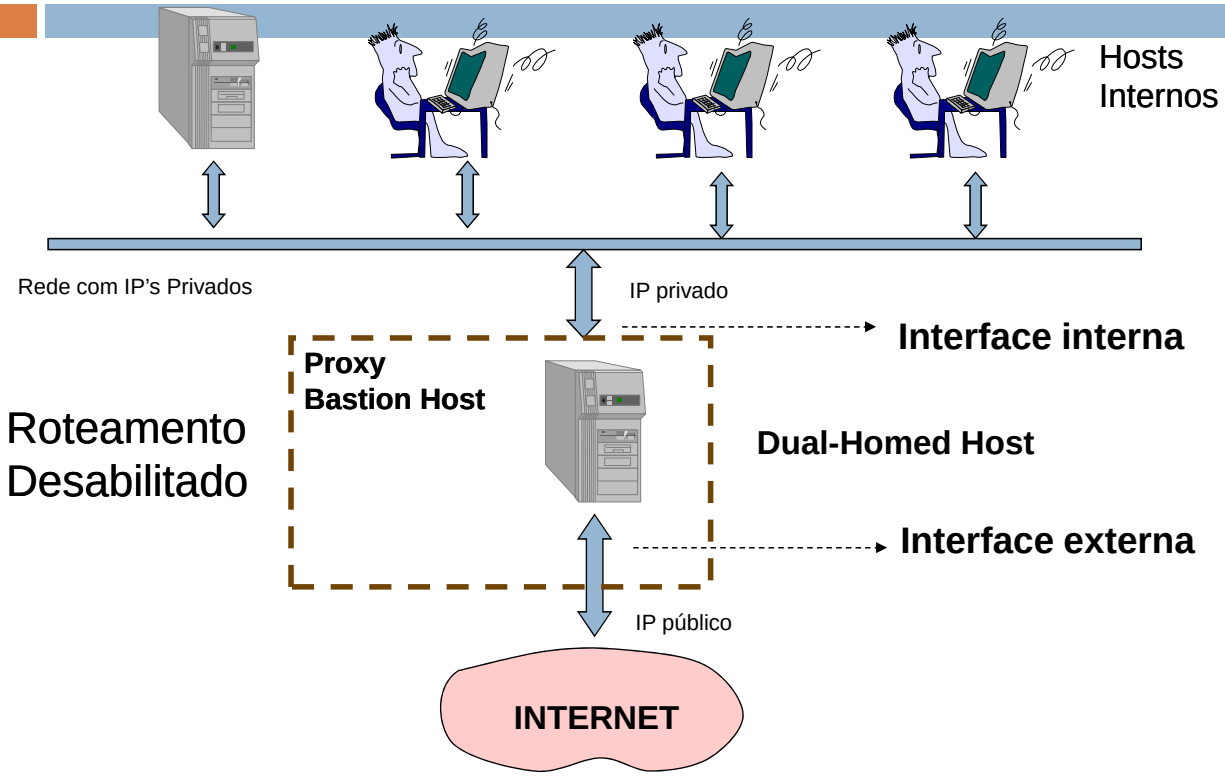
1) Dual-Homed

- Esta arquitetura e formada por um host com pelo menos duas placas de rede.
- Neste caso, o firewall tem a função de roteamento desativada, ou seja, os pacotes da rede interna não são encaminhados diretamente a uma rede externa.



- Para que exista comunicação externa e necessário a intermediação de um proxy.

1) Dual-Homed com Proxy

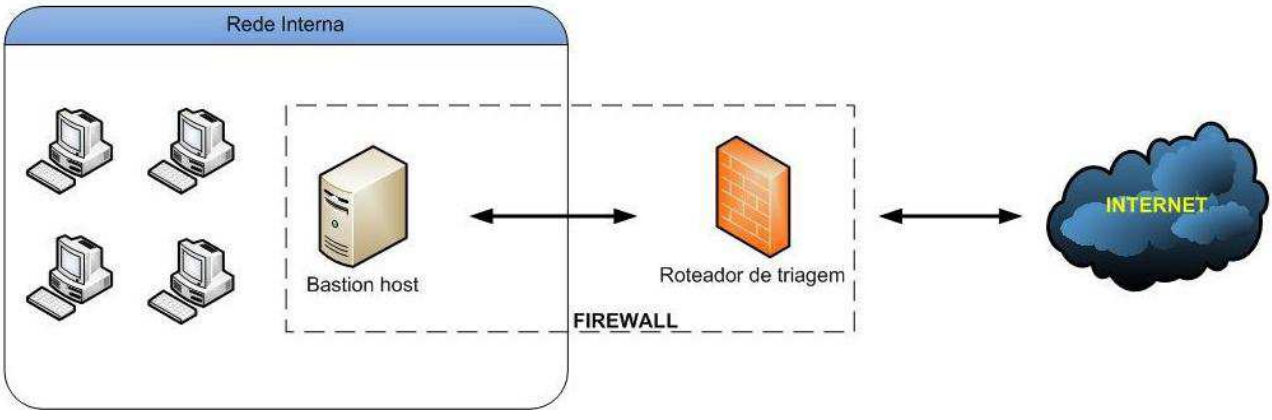


1) Dual-Homed

- O uso de host dual-homed fornece um alto nível de controle, e a desvantagem desta arquitetura é que ele passa a ser o único ponto de falha, logo a segurança deste host deve ser impecável.
- O uso apropriado dessa arquitetura é indicado para algumas das situações abaixo:
  - O tráfego para a Internet é pequeno;
  - Nenhum serviço está sendo oferecido a usuários baseados na Internet;
  - A rede que está sendo protegida não contém dados extremamente valiosos.

2) *Screened* Host (Filtragem simples)

- Na arquitetura *screened host*, as conexões podem ser abertas da rede interna para Internet ou da rede externa para a rede interna exclusivamente para os *bastion hosts* (como exemplo podemos permitir conexões para o servidor web).

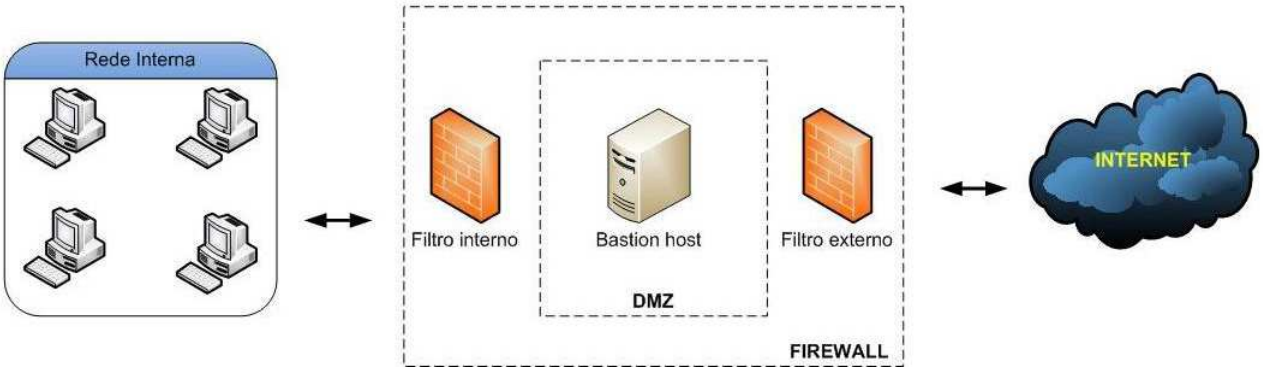


2) *Screened* Host (Filtragem simples)

- O *bastion host* deve manter um alto nível de segurança, nele está justamente o ponto de falha desta arquitetura, caso ele seja invadido, o atacante já estará dentro da rede.
- O uso apropriado desta arquitetura e quando:
  - Poucas conexões estão vindo da Internet.;
  - Não e uma arquitetura apropriada se o host de for um servidor de aplicações publico;
  - A rede que está sendo protegida tem um nível relativamente alto de segurança de host.

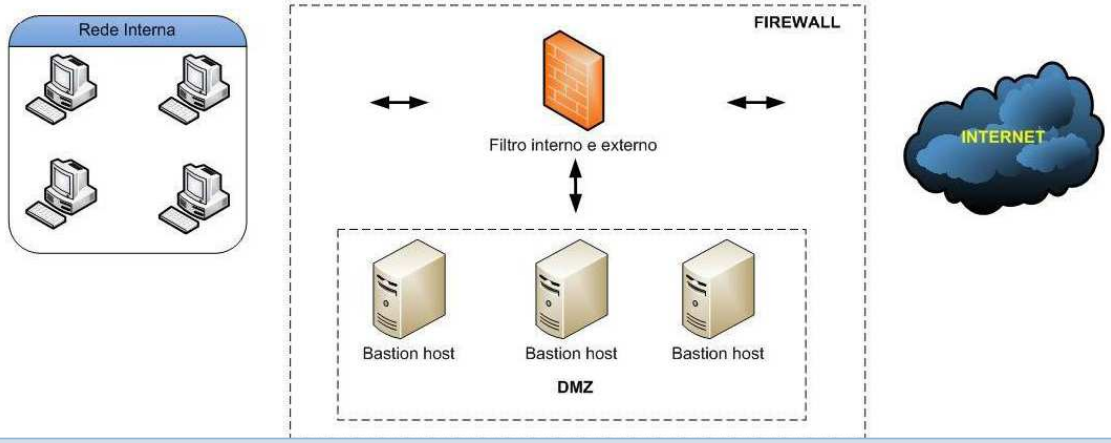
3) Rede de Perímetro (DMZ)

- *Screened Host* com Sub-rede entre firewalls
  - Neste caso o bastion host é colocado entre 2 firewalls, um da rede publica e outro da rede privada.



3) Rede de Perímetro (DMZ)

- Screened Host com Sub-rede própria
  - Neste caso, a DMZ é separada logicamente pelas regras de firewall que gerenciam tanto a rede interna quanto a externa no mesmo local.



O maior problema e que uma configuração malfeita pode dar a falsa sensação de segurança.

Rede de Perímetro com um único Firewall