BRUNO PEREIRA PONTES

Construção de um firewall completo utilizando o FwBuilder

O Palestrante

Bruno Pontes

- Tecnólogo em Desenvolvimento de Software - IFRN;
- Professor do IFB;

http://docente.ifb.edu.br/brunopontes

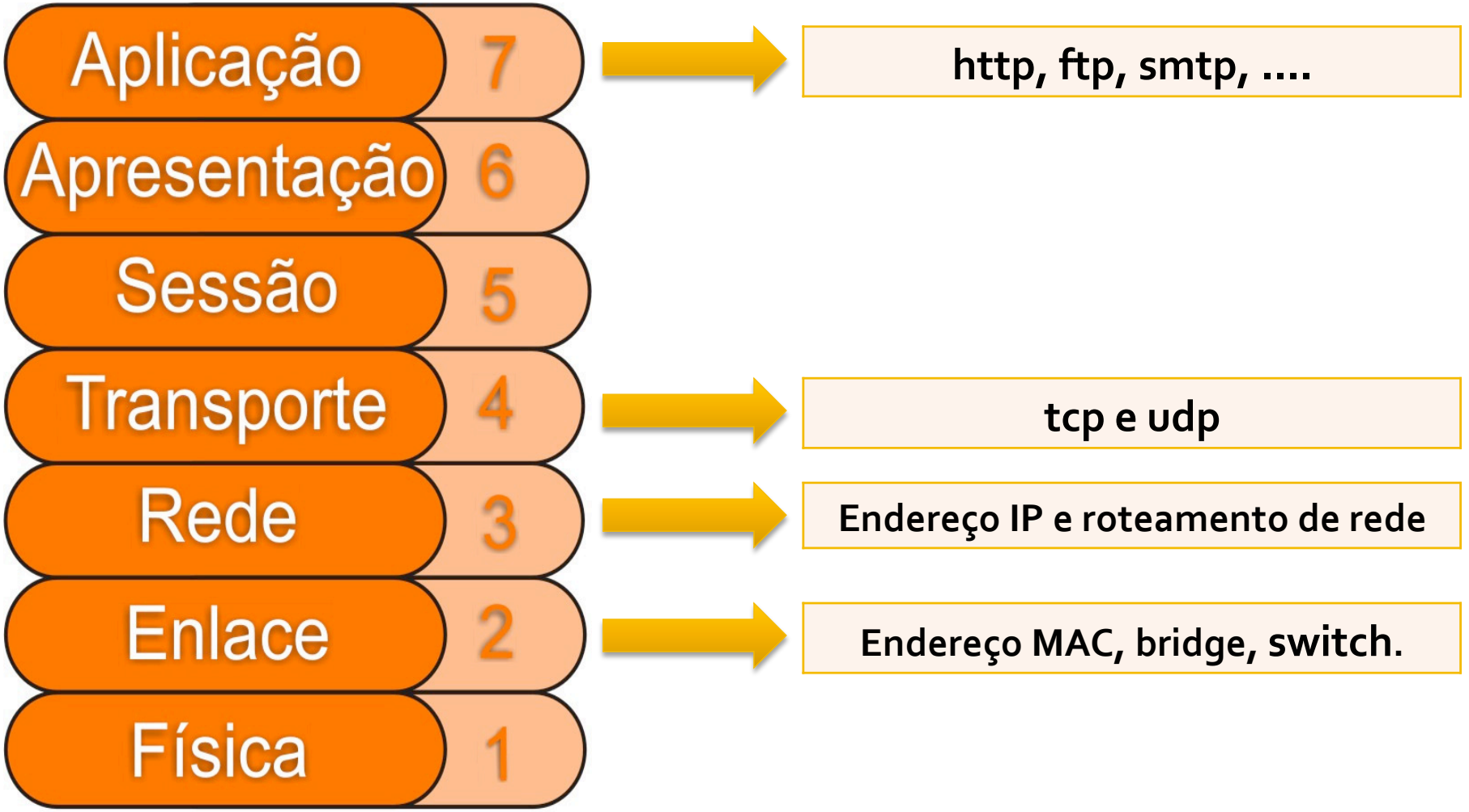
Agenda

- Introdução
- O que é um Firewall?
- Um pouco de história
- Firewall nos dias atuais
- IPTables
- O **FirewallBuilder**
- *Hands-On*
- Conclusão

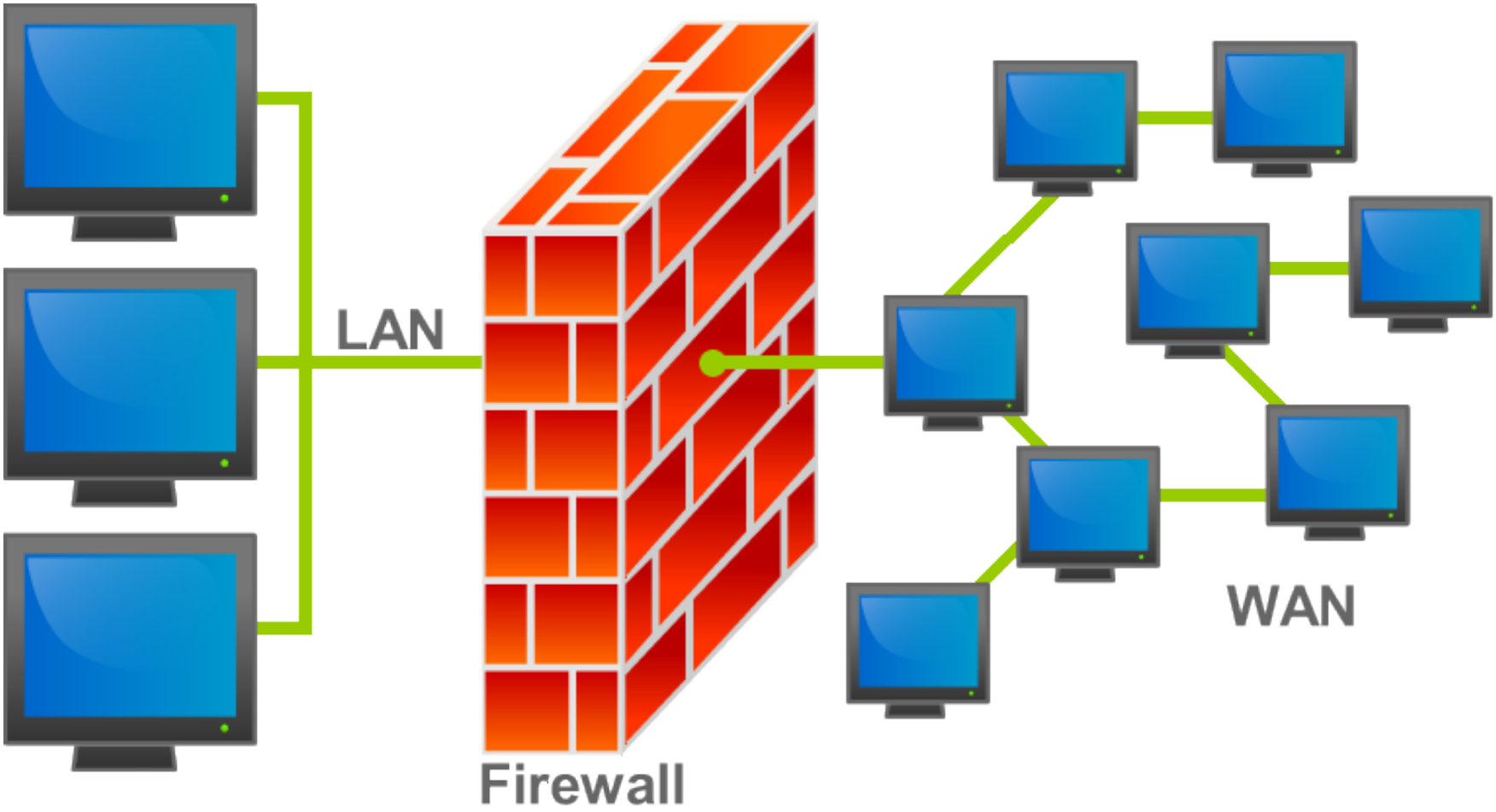
Introdução – Modelo OSI

- Open Systems Interconnection.
- Possui 7 camadas, numeradas de baixo para cima.
- Criado para prover compatibilidade entre produtos de rede de fabricantes diferentes.
- O seu entendimento é fundamental para o estudo dos sistemas de firewall.
- Um tráfego de rede nem sempre atingirá as camadas superiores.

Introdução – Modelo OSI



O que é firewall?



História do Firewall

- Nasceu no final dos anos 80;
  - Expansão das redes acadêmicas e militares;
  - Surgimento da Internet;
  - Popularização dos computadores;

História do Firewall

- Primeira geração – Filtro de pacotes:
  - Restringir tráfego baseado no endereço IP de origem ou destino;
  - Restringir tráfego através da porta (TCP ou UDP) do serviço;
- Segunda geração – Filtros de estado de sessão:
  - Armazena o estado das conexões e filtra com base nesse estado;
  - Três estados para uma conexão: -
    - NEW: Novas conexões;
    - ESTABLISHED: Conexões já estabelecidas;
    - RELATED: Conexões relacionadas a outras existentes.

História do Firewall

- Terceira geração – Gateway de Aplicação:
  - Restringir acesso FTP a usuários anônimos;
  - Restringir acesso HTTP para portais de entretenimento;
  - Restringir acesso a protocolos desconhecidos na porta 443 (HTTP/S).

Tipos de Firewall

- Filtro de pacotes
  - Análise individual dos pacotes
  - Funciona nas camadas 3 e 4
  - Desvantagem: IP Spoofing
- Stateful Firewall
  - Análise individual dos pacotes
  - Funciona nas camadas 3 e 4
  - Análise do estado das conexões

Tipos de Firewall

- Firewall de Aplicação
  - Análise individual dos pacotes
  - Funciona nas camadas 3, 4 e 7 (Aplicação)
  - Foco nas vulnerabilidades das aplicações
  - Analisa o conteúdo de cada pacote
  - Ex.: Squid.

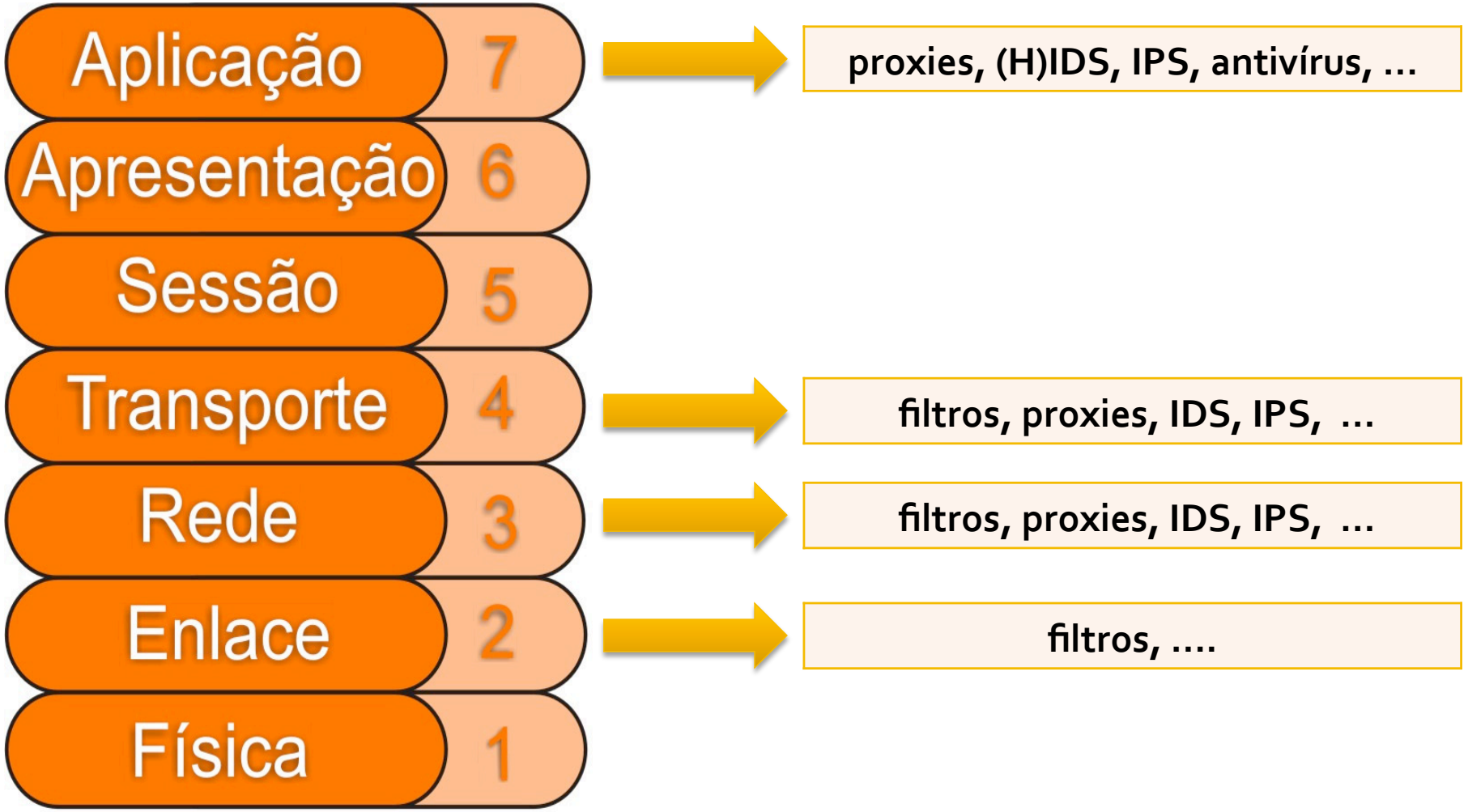
Firewall hoje!!!

- Firewall é um sistema;
- Firewall é todo o esforço voltado para a segurança da rede;
- Os sistemas de firewall podem ser compostos por diversos elementos, como filtros de pacotes, filtros de estados, proxies (forward e reverso), IDS, IPS, HIDS, antivírus de rede etc;
- Não é possível ter um sistema de firewall apenas com uma máquina;
- IMPORTANTE: segurança, conforto e funcionalidade: use dois e abandone um. Exemplo: sites de bancos.
- IMPORTANTÍSSIMO: segurança em profundidade.

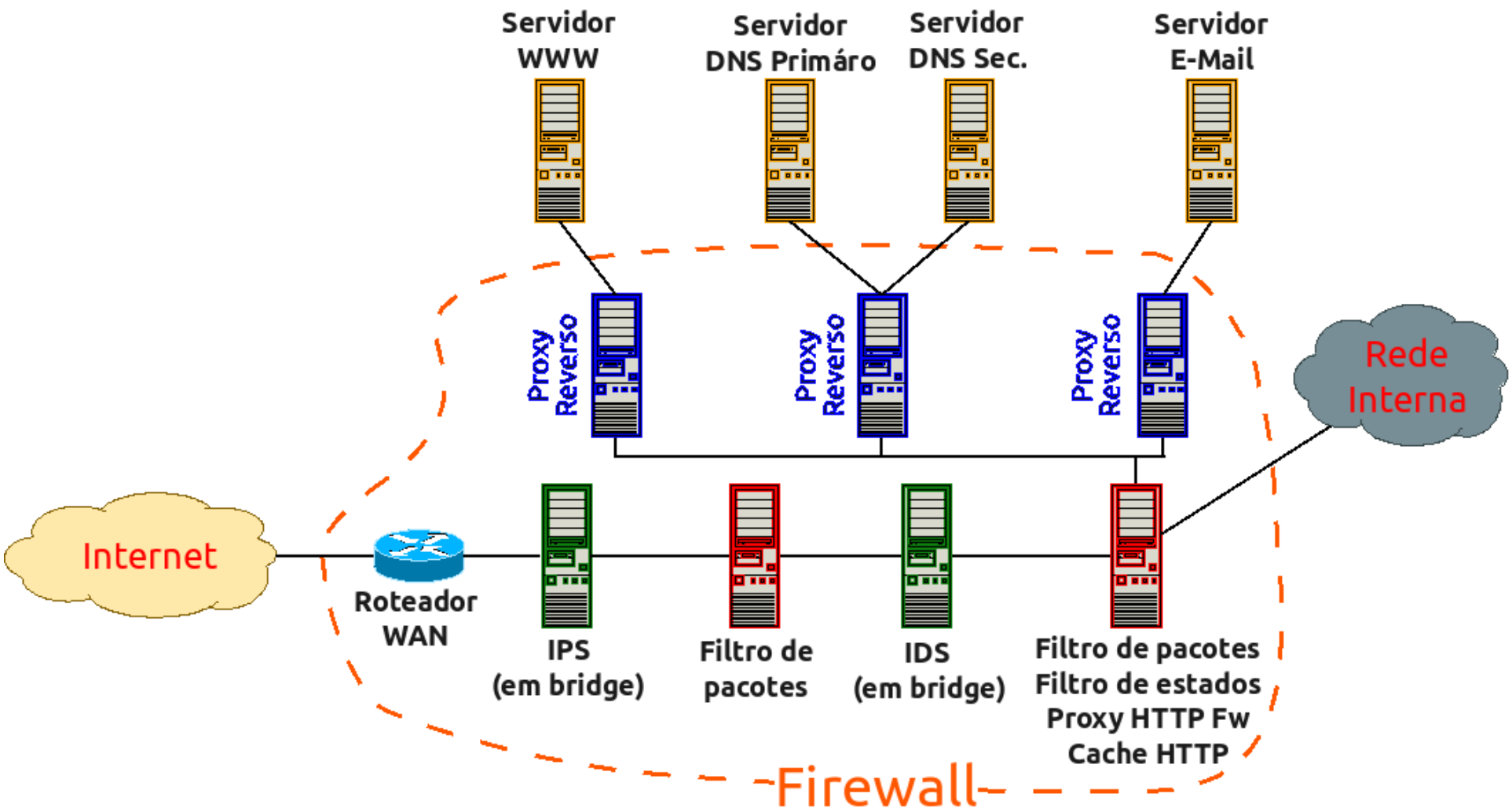
Firewall hoje – Elementos de Firewall

- Filtros de pacotes: Netfilter (Iptables), ebtables e PF.
- Filtros de estados: Netfilter (Iptables) e PF.
- IDS: Snort e Labrea.
- IPS: HLBR e Snort In-Line.
- Proxy: Squid, totd, apt-cache search proxy :-)
- Port scan detector: psad e PortSentry.
- Filtros de aplicações: L7-Filter e IPP2P.
- Antivírus: Clamav.
- Outros: apt-cache search firewall / apt-cache search honey.

Elementos Firewall X Modelo OSI



Firewall hoje – Sistema de Firewall



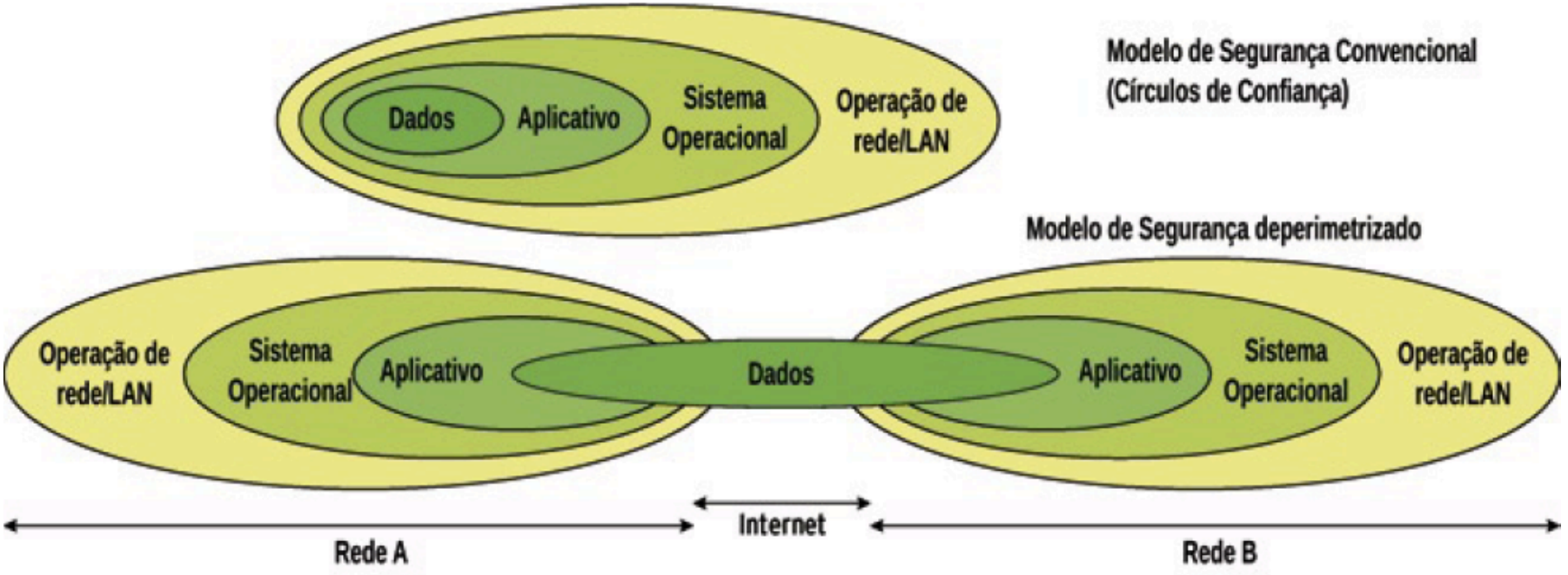
Firewall hoje - Para que serve?

- Proteger uma rede de ataques externos;
- Reforçar a Política de Segurança da empresa;
- Controlar e restringir o acesso aos serviços disponibilizados;
- Registrar a comunicação entre as máquinas internas e externas;
- Esconder máquinas internas;
- Converter endereços IP (NAT);
- Balancear a carga dos servidores
- Oferecer integração com outros mecanismos de segurança (IDS, anti-vírus, autenticação forte ...)
- Coletar informações sobre os eventos relacionados à segurança
- . . . . . .

Firewall hoje - Para que não serve?

- Controlar comunicação entre máquinas da mesma sub-rede
- Impedir ataques de pessoas internas
- Controlar tráfego de informações
  - Por outros meios magnéticos
  - Por modem
  - Por fax ou telefone
  - ...
- Impedir ataques via "acesso legítimo" aos serviços internos

Firewall hoje – Sistema ultrapassado?



http://www.jerichoforum.org

Nosso objetivo hoje

Filtro de Pacotes

Filtro de Estados

IPTables

- Filtro de pacotes inserido no linux desde o kernel 2.4
- Possui tabelas
  - raw: onde são feitas algumas alterações em mais baixo nível nos pacotes
  - filter: nesta tabela cabem as regras responsáveis pela filtragem de pacotes
  - nat: mudanças nos cabeçalhos dos pacotes (incluindo NAT e IP Masquerade)
  - mangle: usada para alterações específicas nos pacotes

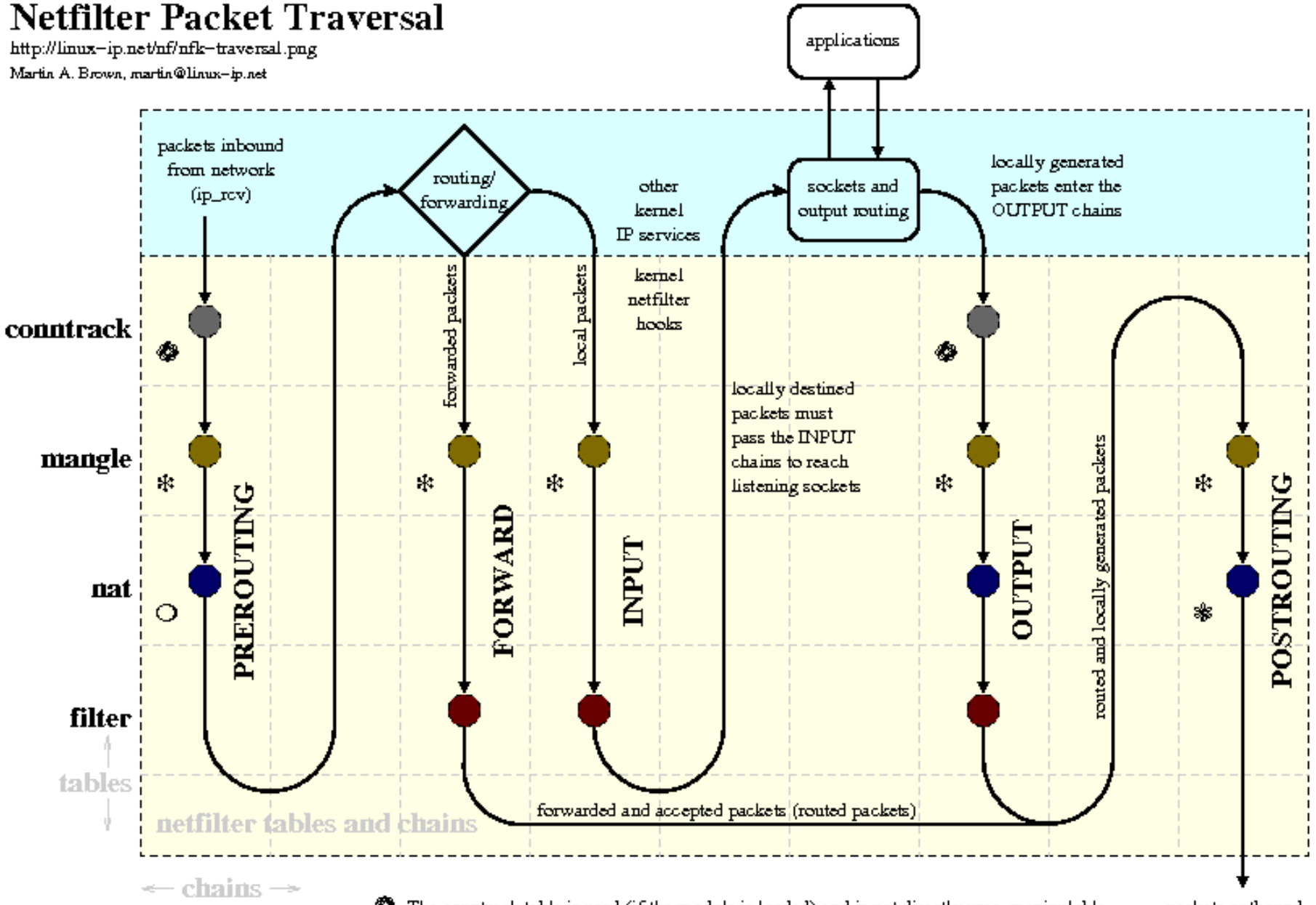
IPTables

- Cadeias
  - PREROUTING: tráfego ingressante na máquina (incluindo tráfego gerado localmente com destino local)
  - INPUT: tráfego que tem como destino a própria máquina
  - FORWARD: tráfego passante pela máquina
  - OUTPUT: tráfego gerado localmente (tanto com destino local como remoto)
  - POSTROUTING: todo tráfego que "sai" da máquina (incluindo tráfego gerado localmente com destino local)

Netfilter Packet Traversal

http://linux-ip.net/nf/nfk-traversal.png

Martin A. Brown, martin@linux-ip.net



❁ The conntrack table is used (if the module is loaded) and is not directly user-manipulable.

❄ The targets MARK, TOS, and TTL are available only in the mangle table.

○ The nat PREROUTING table supports the DNAT target.

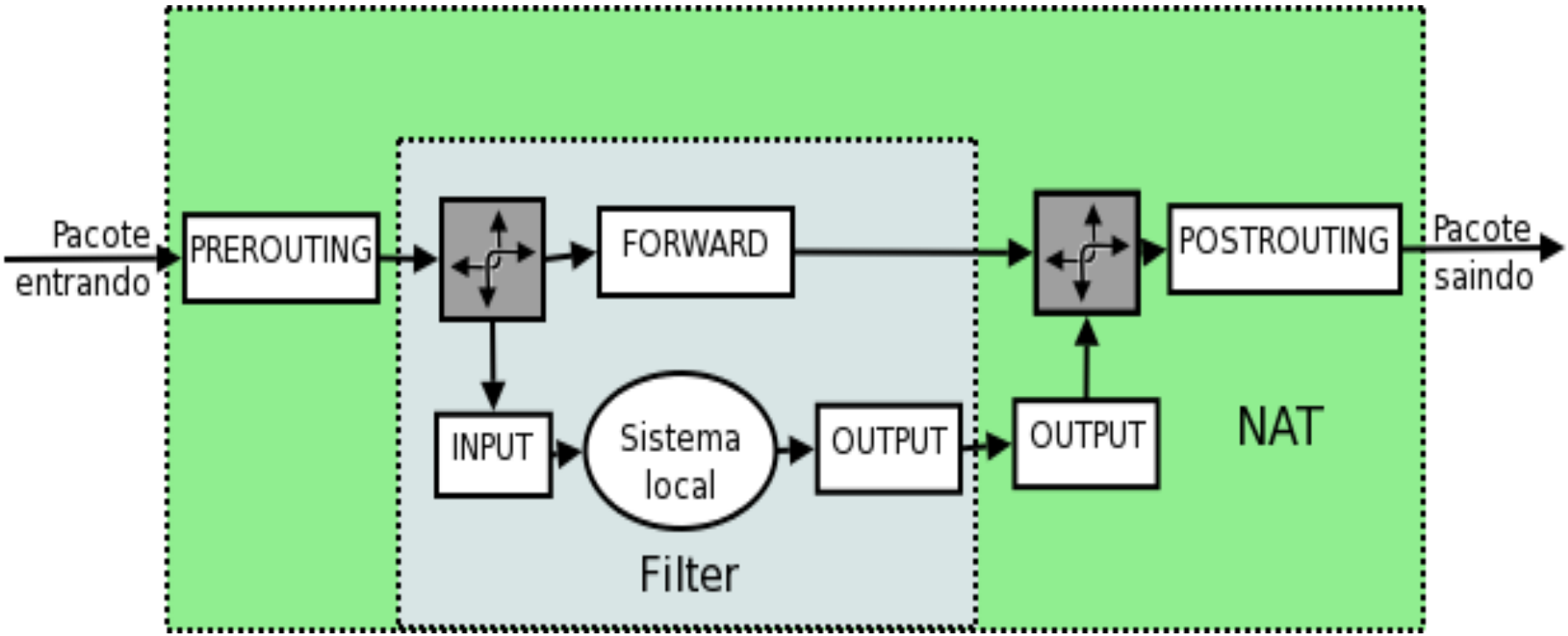
❃ The nat POSTROUTING table supports SNAT and MASQUERADE targets.

cf. http://www.docum.org/qos/kptd/

cf. http://open-source.arkoon.net/kernel/kernel_net.png

cf. http://iptables-tutorial.frozentux.net/

IPTables


Pacote
entrando
PREROUTING
FORWARD
POSTROUTING
Pacote
saindo
INPUT
Sistema
local
OUTPUT
OUTPUT
NAT
Filter

IPTables

- Regras
  - -p PROTOCOLO: especifica um protocolo (por exemplo tcp ou udp)
  - -s ENDEREÇO: especifica um endereço de origem
  - -d ENDEREÇO: especifica um endereço de destino
  - -i INTERFACE: especifica a interface de rede na qual o pacote ingressou
  - -o INTERFACE: especifica a interface de rede na qual o pacote irá sair da máquina

IPTables

- Alvo/Ação
  - ACCEPT: aceita o pacote, e diz ao netfilter para continuar o processamento do pacote na próxima cadeia/tabela
  - DROP: diz ao netfilter para ignorar completamente o pacote
  - REJECT: diz ao netfilter para rejeitar o pacote
  - LOG: Cria um log referente à regra, em /var/log/messages. Usar antes de outras ações.

IPTables

- Criando Regras
  - iptables -t TABLE -A CADEIA REGRAS -j ALVO

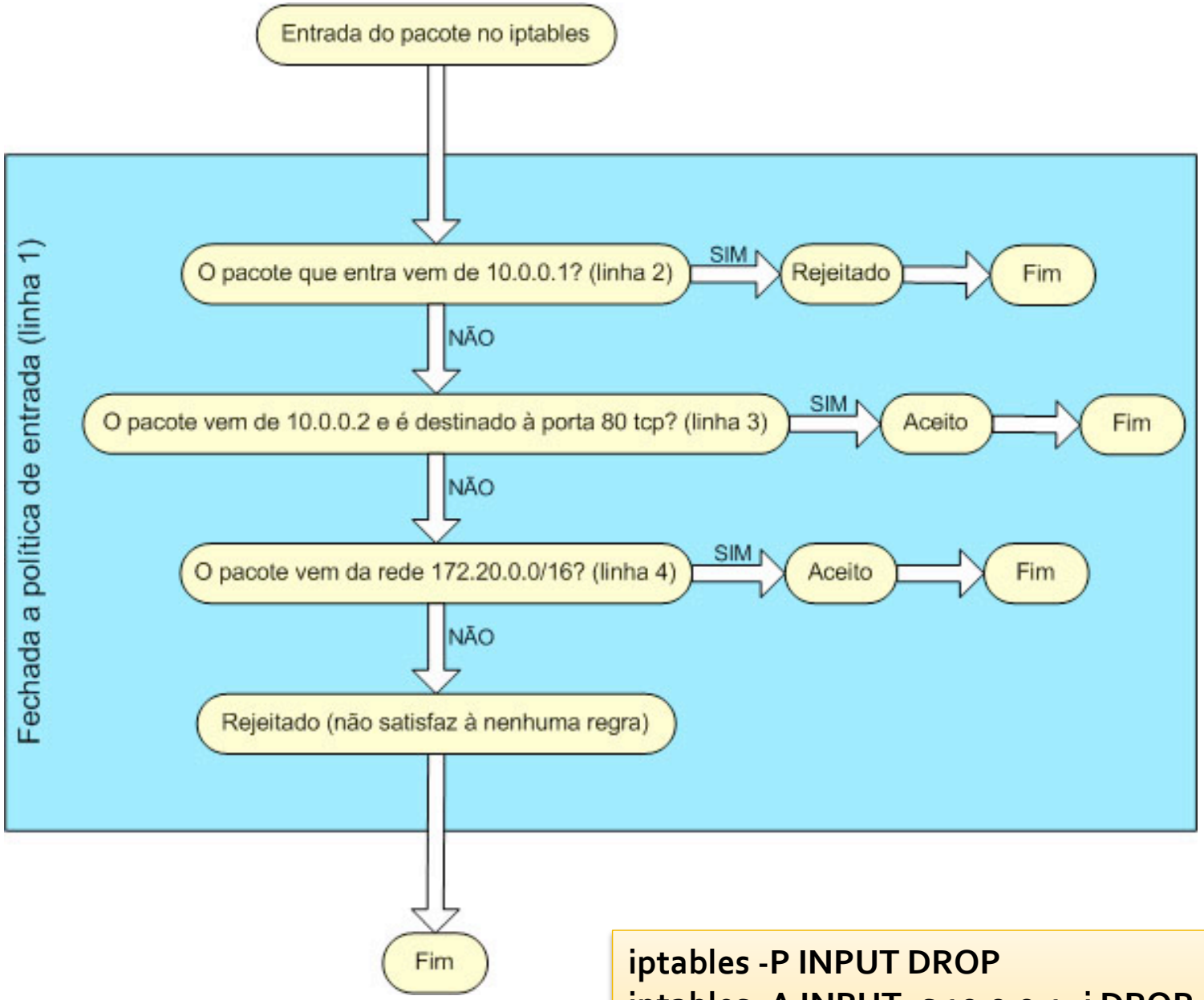
- Principais opções:
  - **-P** --> Policy (política). Altera a política da chain;
  - **-A** --> Append (anexar). Acresce uma nova regra à chain. Tem prioridade sobre o –P;
  - **-L** --> List (listar). Lista as regras existentes.
  - **-F** --> Flush (esvaziar). Remove todas as regras existentes. No entanto, não altera a política (-P)

Exemplos de Regras

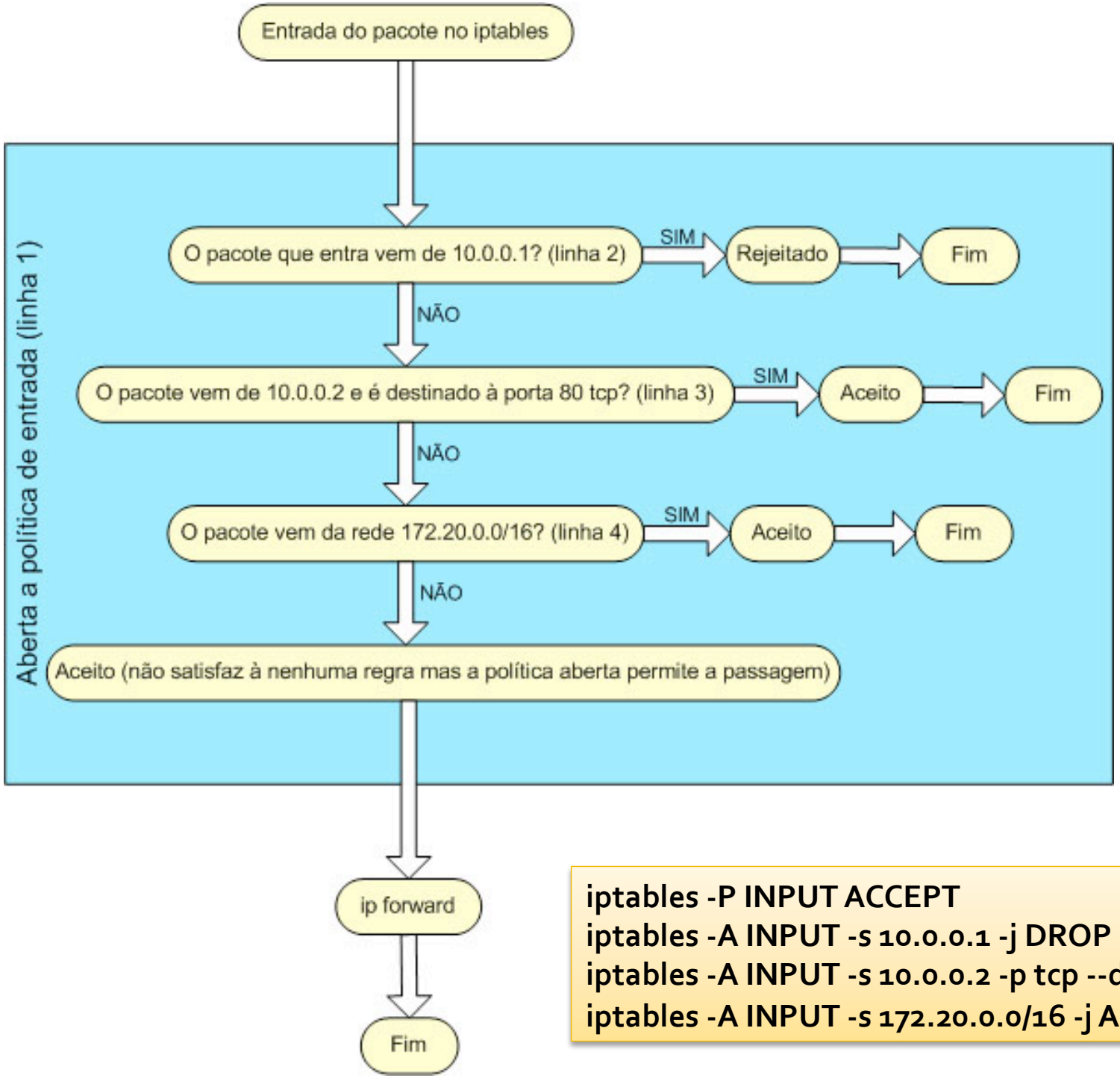
- Bloqueando a entrada para a porta 80
  - iptables -A INPUT --dport 80 -j DROP
- Liberando o acesso a internet
  - iptables -t nat -A POSTROUTING –o etho -j MASQUERADE
- Redirecionando a porta 666 para a porta 80
  - iptables -t nat -A PREROUTING -s 10.0.0.0/8 -p tcp --dport 666 -j REDIRECT --to-port 80

Impasses e ordem das regras

- As regras serão interpretadas na ordem em que aparecerem;
- Sempre que um pacote se adequar a uma regra, tal regra processará o pacote e irá finalizar;
  - Isso não se aplicará às regras terminadas com -j LOG.
- Conclusão: se houver impasse entre regras, sempre valerá a primeira.

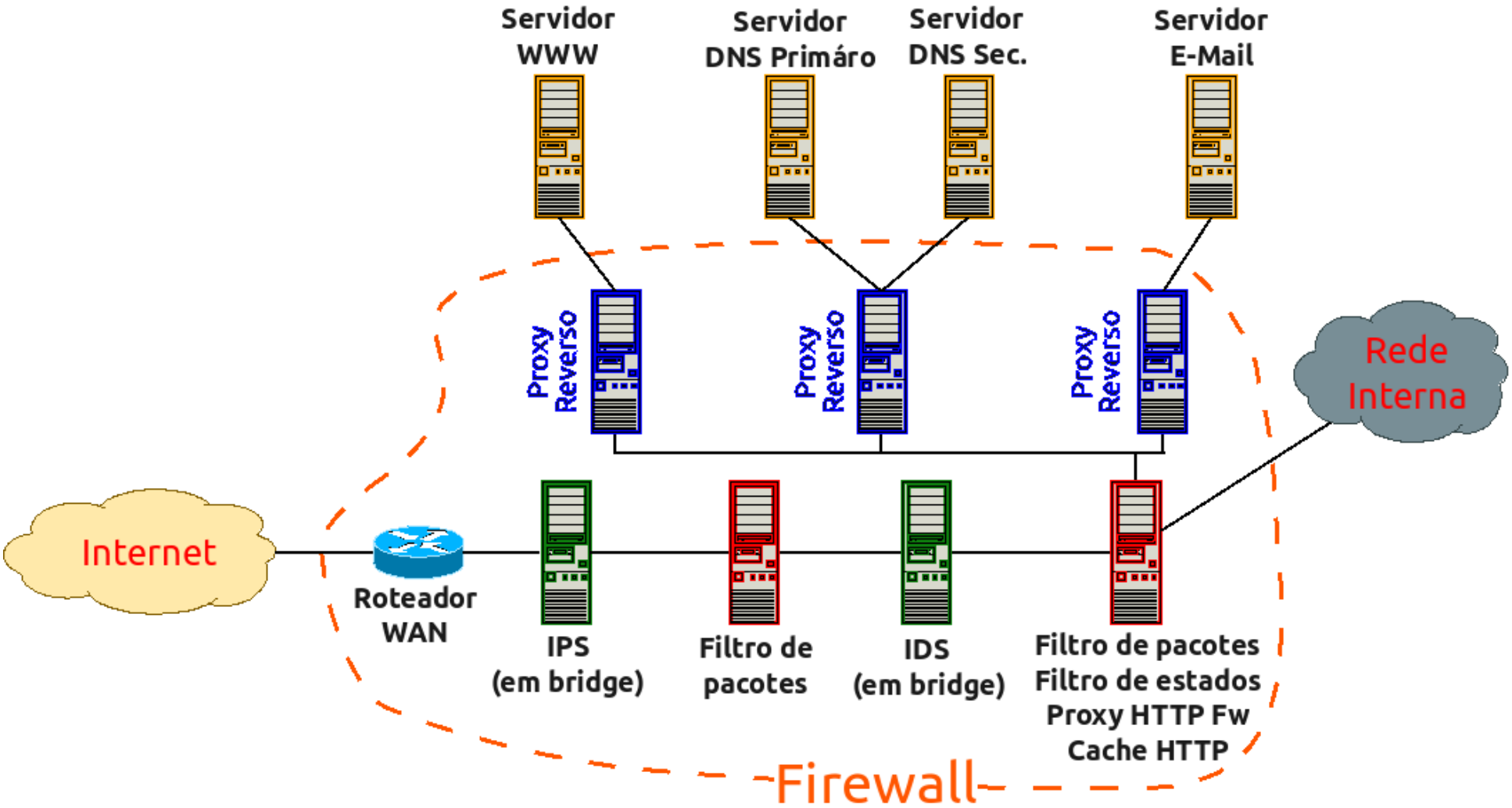



```
iptables -P INPUT DROP
iptables -A INPUT -s 10.0.0.1 -j DROP
iptables -A INPUT -s 10.0.0.2 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 172.20.0.0/16 -j ACCEPT
```




```
iptables -P INPUT ACCEPT
iptables -A INPUT -s 10.0.0.1 -j DROP
iptables -A INPUT -s 10.0.0.2 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -s 172.20.0.0/16 -j ACCEPT
```

Construção do Filtro



Construção do Filtro

- Para redes pequenas, construir na "unha" é uma tarefa não tão complicada;
- Mas, para redes mais complexas, com vários filtros/roteadores, torna-se uma tarefa quase que impraticável;
- A utilização de um software de apoio torna-se indispensável. Qual???

FirewallBuilder

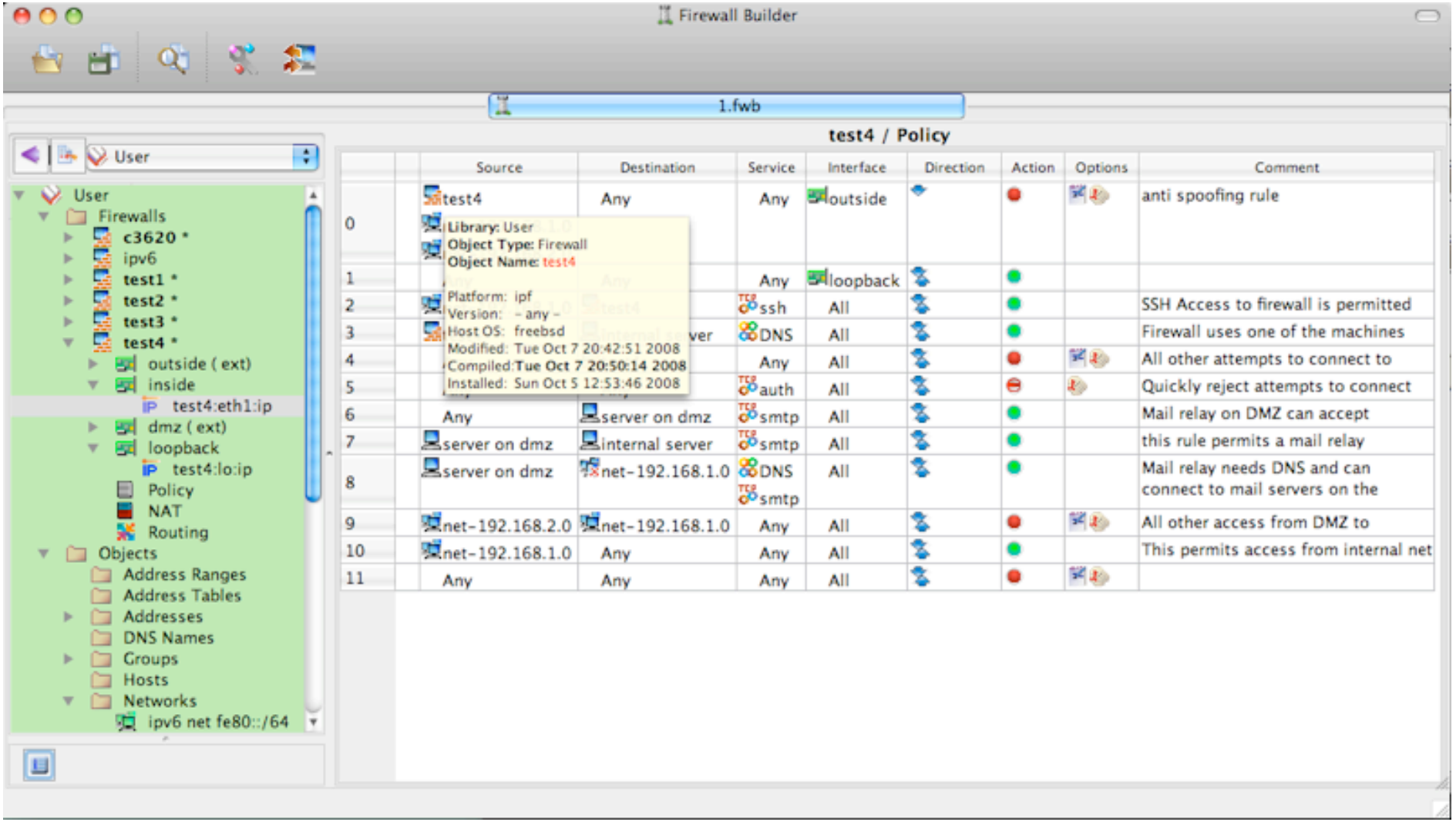
FirewallBuilder

- Ferramenta GUI de configuração e gestão (local e remota) de firewall (filtros);
- Suporta:
  - **iptables (netfilter), ipfilter, pf, ipfw, Cisco PIX (FWSM, ASA) and Cisco routers extended access lists**
- Roda em:
  - Linux, FreeBSD, OpenBSD, Windows and Mac OS X;
- Site oficial:
  - www.fwbuilder.org

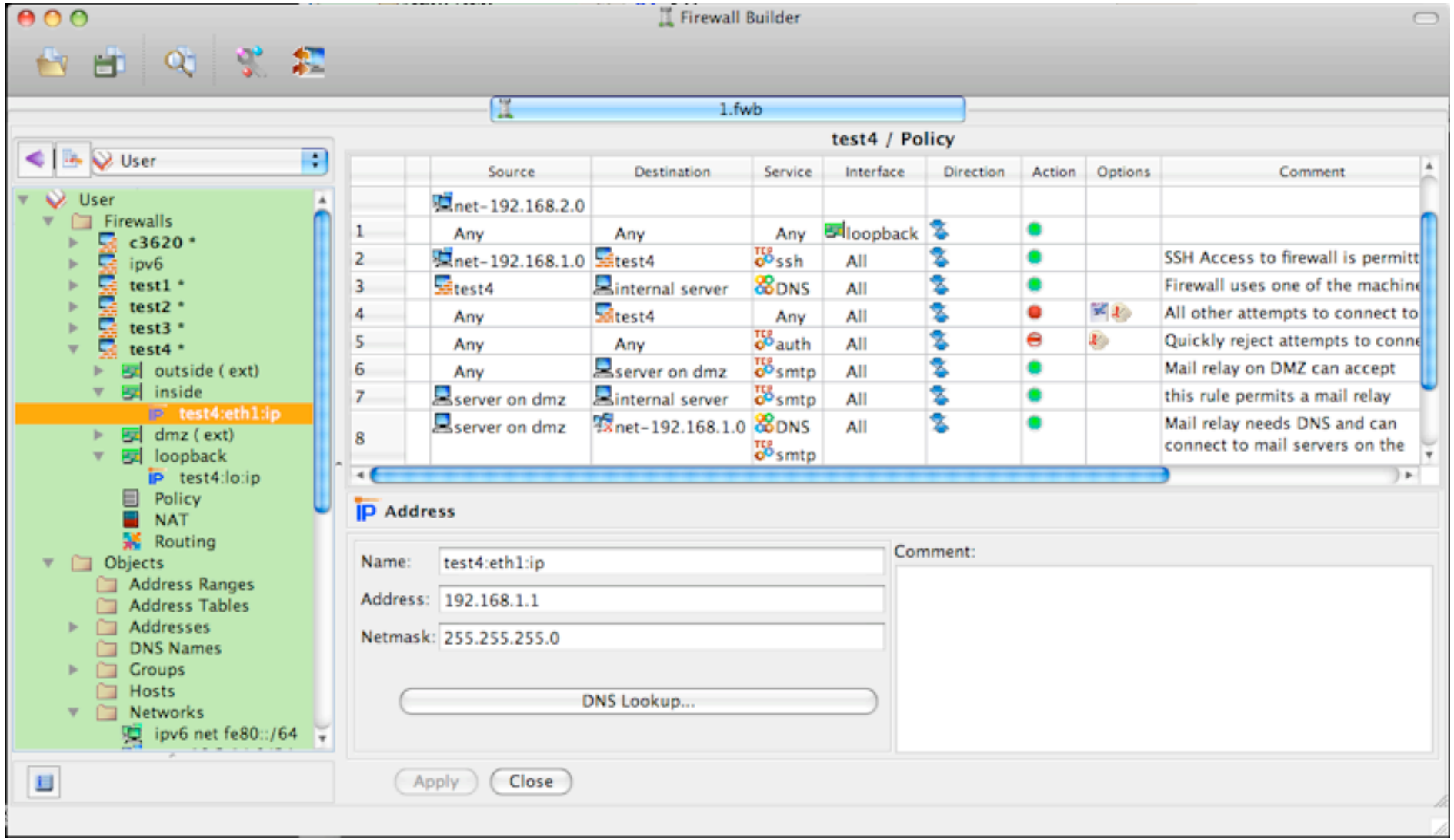
FirewallBuilder

- O site possui vasta documentação;
- Licenciado de duas formas:
  - Packages for Linux (any distribution available under the terms of GPL), FreeBSD or any other operating system or distribution available under the terms of GPL are also available under GPL;
  - Packages of Firewall Builder for commercial OS are distributed under the terms of NetCitadel End User License Agreement.

FirewallBuilder - Telas



FirewallBuilder - Telas



FirewallBuilder

- Colocando a mão na massa!!!!

Dicas importantes I

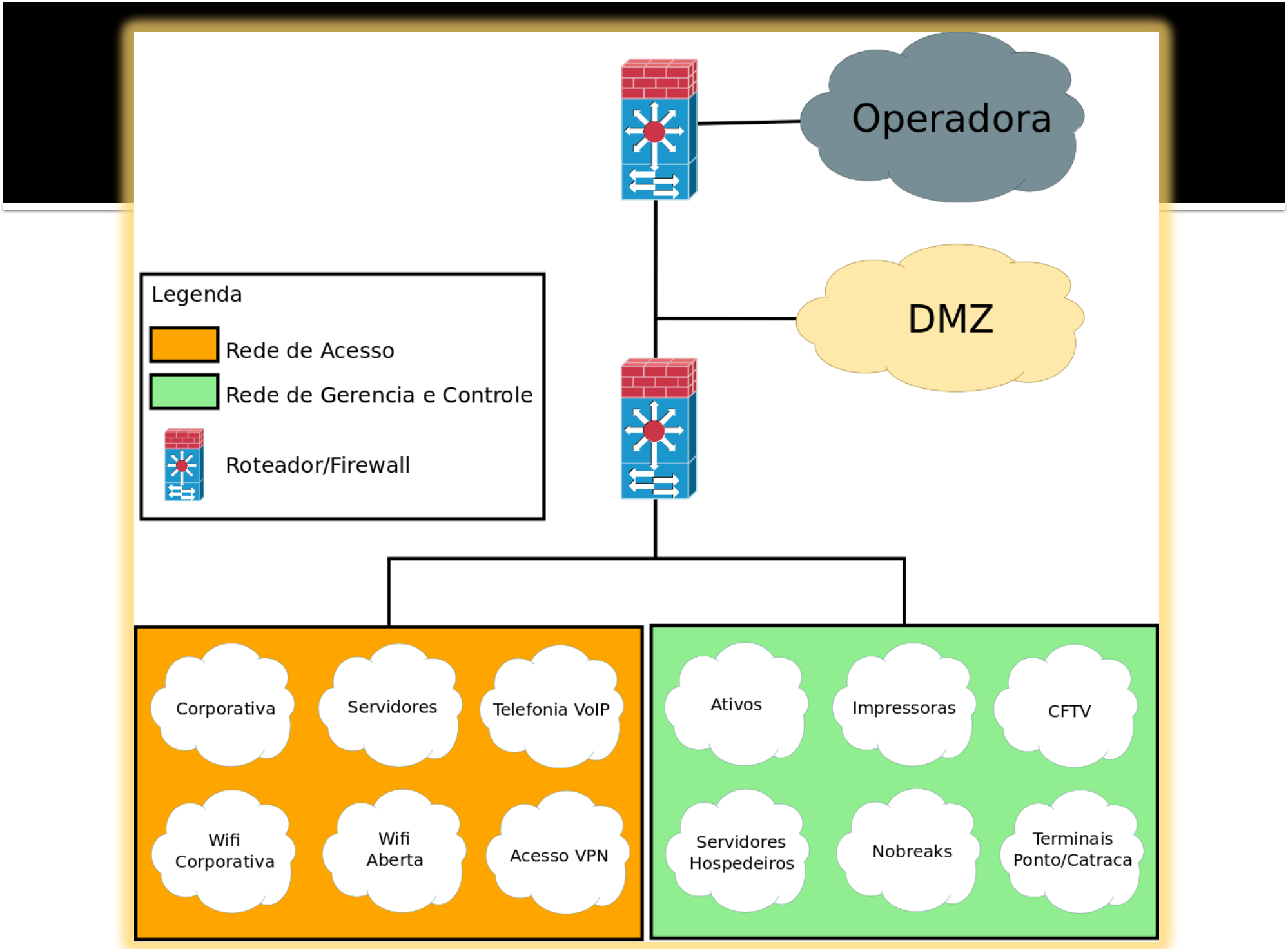
- Prefira topologia de filtro isolado combinado com filtro incorporado;
- Atualize sempre o Iptables e o kernel;
- NUNCA rode qualquer serviço, principalmente os remotos, como telnet e ftp, nas máquinas firewall. Mas...
- ...Se tiver que administrar remotamente uma máquina firewall, utilize ssh. Nesse caso, o ssh não deverá permitir o login como root;
- Nunca cadastre qualquer usuário na máquina Iptables, caso se trate de filtro isolado, a não ser os que irão administrar por ssh;

Dicas importantes II

- Utilize TCP Wrappers totalmente fechado (ALL:ALL em /etc/hosts.deny) em filtros isolados. Abra o ssh (em /etc/hosts.allow) apenas para os clientes que forem fazer administração remota;
- Anule as respostas a ICMP 8 (echo reply) no filtro isolado, para evitar ataques de Ping of Death;
- Não insira referências ao sistema de firewall no DNS;
- Não deixe as máquinas firewall isolado com cara de firewall. Utilize nomes descaracterizados;
- Faça log de ações suspeitas que estiverem ocorrendo na rede;
- Teste, teste, teste novamente.

Dicas importantes III

- Seguimente sua rede. Isso irá facilitará a implementação e gerenciamento das políticas;


Operadora
DMZ
Legenda
Rede de Acesso
Rede de Gerencia e Controle
Roteador/Firewall
Corporativa
Servidores
Telefonia VoIP
Wifi Corporativa
Wifi Aberta
Acesso VPN
Ativos
Impressoras
CFTV
Servidores Hospedeiros
Nobreaks
Terminais Ponto/Catraca

Referências

- http://www.eriberto.pro.br/iptables/ - **João Eriberto Mota Filho;**

- **http://www.fwbuilder.org - Site Oficial do FirewallBuilder;**

Conclusão

Contato

Bruno Pontes

tenpontes@gmail.com