Diretoria de Educação e Tecnologia da Informação

Análise e Desenvolvimento de Sistemas

INSTITUTO FEDERAL RIO GRANDE DO NORTE

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA 1909-2009

Administração de Sistemas Operacionais

Serviço Proxy - SQUID

Prof. Bruno Pereira Pontes
tenpontes@gmail.com

Objetivos

- Entender o funcionamento de um servidor proxy;
- Realizar a instalação e configuração e um servidor proxy baseado em squid;

Sumário

- Ligação da Intranet na Internet;
- Network Address Translation
- Filtro de pacotes X Filtro de conteúdo;
- Definição de Servidor Proxy;
- Características de um Servidor Proxy;
- Porque utilizar o Squid;
- Utilização das ACL;
- Auditoria;
- Instalação e Configuração do Squid;

Intranet na Internet

- Redes internas utilizam endereços inválidos para a Internet;
- Intranet utiliza tecnologia da Internet em ambiente privativo:
  - sistema de endereçamento (IP),
  - protocolos (TCP/UDP),
  - aplicações (SMTP, WWW, FTP, etc.)
- Caso a Intranet deseje conectar-se a Internet, os pacotes não poderão sair com IP de origem privados;

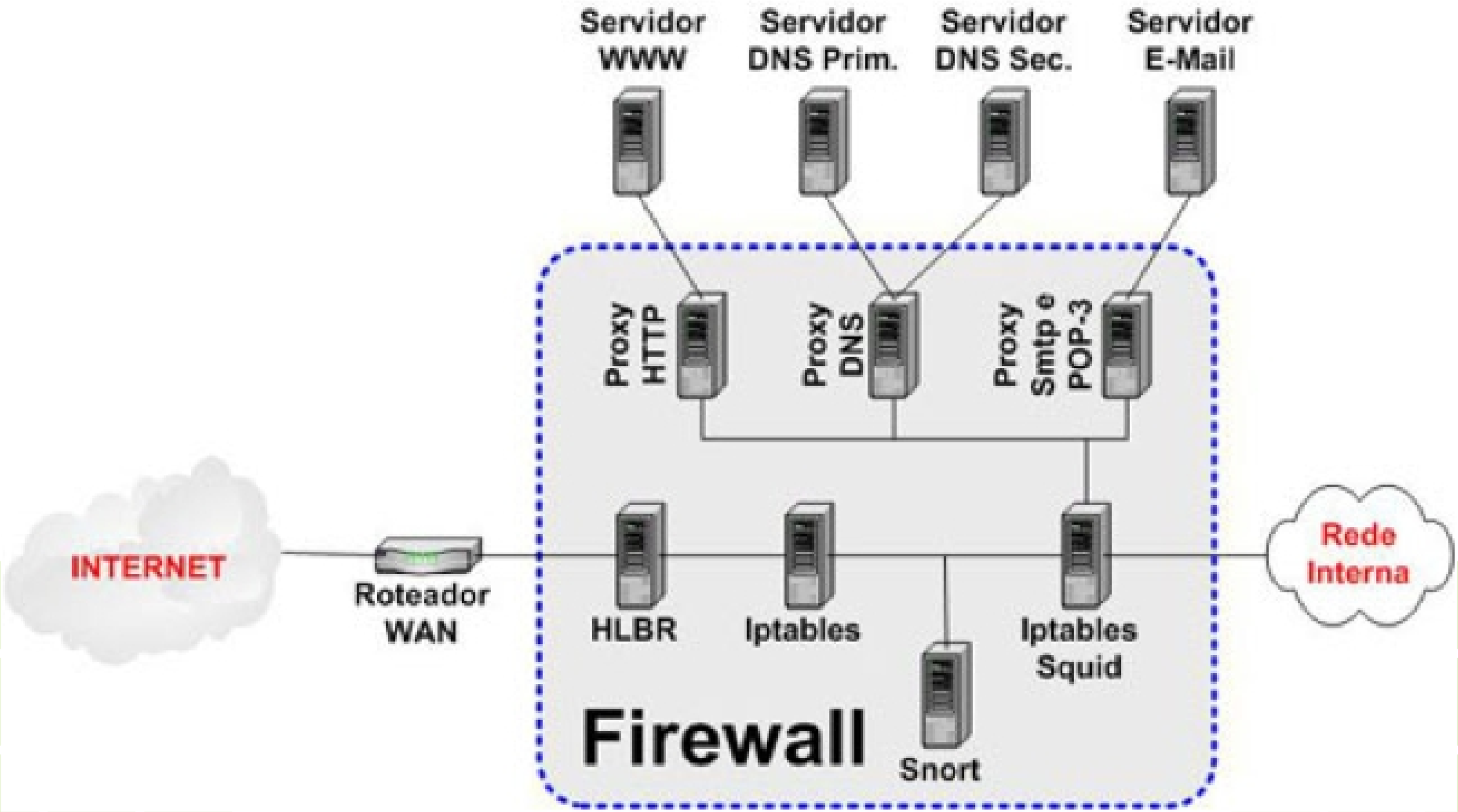
Network Address Translation

- Solução???
  - NAT – Network Address Translation;
  - Funcionalidade presente nos roteadores e Firewall, para traduzir endereços, seja na saída de pacotes para a Internet, seja na chegada de pacotes da Internet para máquinas com IP privado;
  - Sem NAT nada funciona, porque nenhum roteador na Internet tem rota para estes IPs privados;

Network Address Translation

- Normalmente é colocado na interface externa do Firewall.
- Quando um pacote vai atravessar esta interface, o sistema de NAT faz as trocas necessárias.
- Pode-se dividir o NAT em:
  - NAT de saída para a Internet;
  - NAT de entrada;
- Os sistemas de NAT possuem uma tabela interna para desfazer as trocas, quando o pacote de resposta voltar;

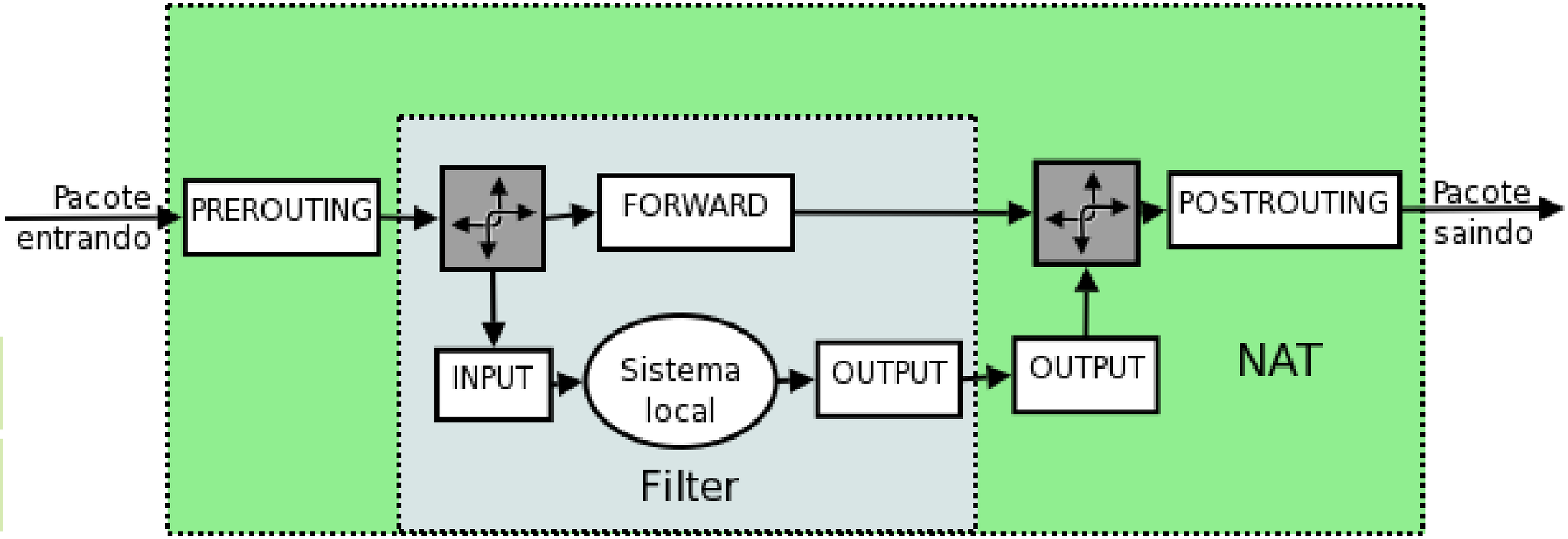
Network Address Translation



Network Address Translation

Como configurar o NAT no Linux???

IPTABLES



Network Address Translation

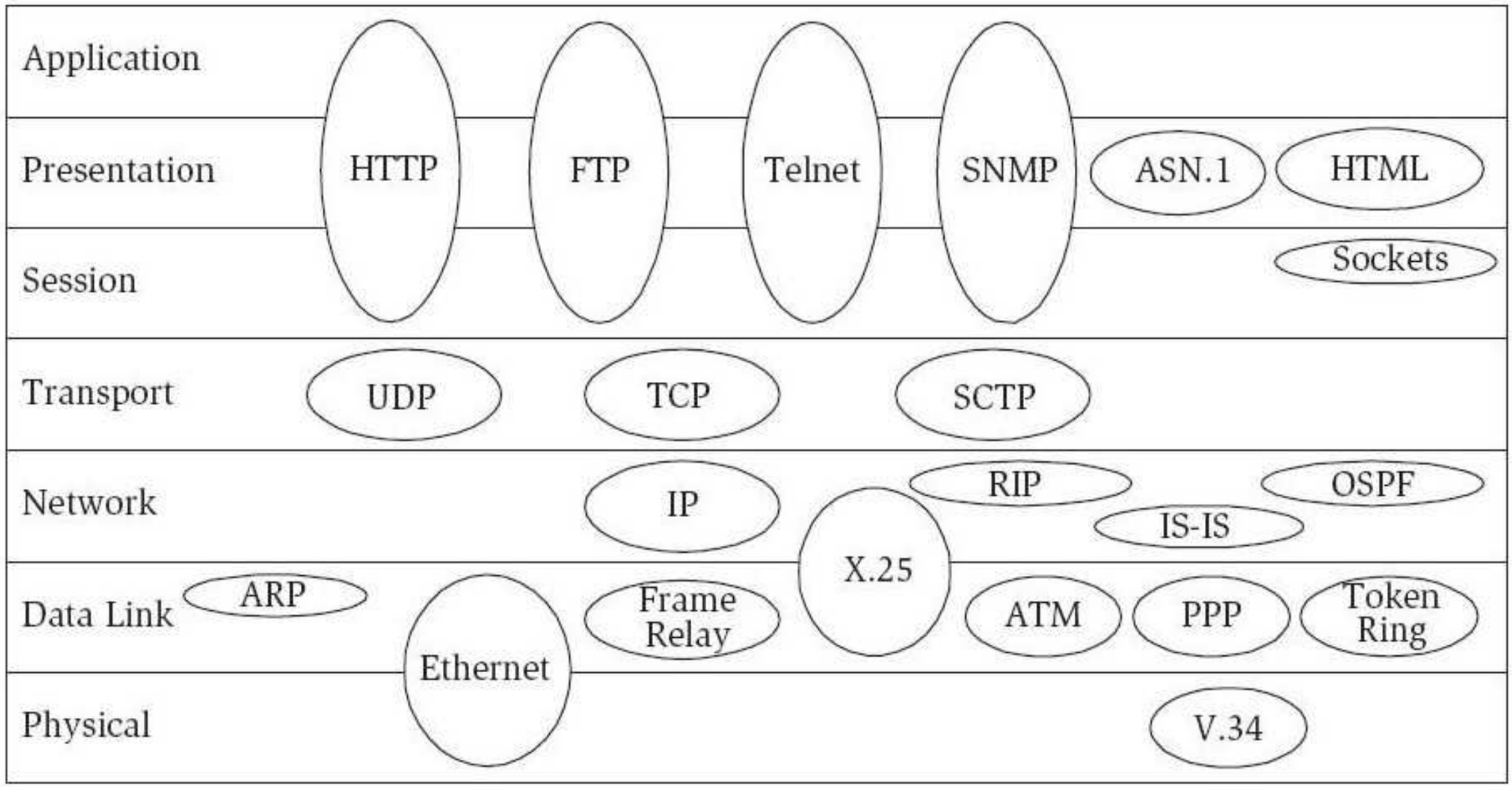
- Exemplo de regras:
  - Quando usar IP fixo:
    - iptables -t nat -A POSTROUTING -o eth2 -j SNAT --to-source 200.20.10.10
  - Quando usar IP não fixo (acessos dinâmicos);
    - iptables -t nat -A POSTROUTING -o eth2 -j MASQUERADE
- Pode-se fazer NAT apenas de protocolos e portas específicas:
  - NAT para pacotes TCP com destino na porta 22 (ssh)
    - iptables -t nat -A POSTROUTING -o eth2 -p tcp --dport 22 -j MASQUERADE

Filtros de pacote e conteúdo

- Presentes geralmente no perímetro da rede, funcionando como intermediário entre a Intranet e Internet;
- Possuem a capacidade de filtrar o tráfego transmitido para dentro e fora da rede, baseado em regras pré-definidas
  - Filtro de pacotes analisa tráfego nas camadas de rede e transporte (endereço de IP, faixa de endereço de IP e faixa e número de porta TCP/UDP);
    - Ex: iptables
  - Filtro de conteúdo analise tráfego na camada de aplicação (HTTP, FTP, outras URL's e pesquisa DNS. Também filtros de URL's baseados em conteúdo);
    - Ex: squid

Filtros de pacote e conteúdo

- Filtro de Pacotes – Camada 3-4
- Filtro de Conteúdo – Camada 7



Definição de Servidor Proxy

- O termo “servidor proxy “ou “serviço de proxy”, vem de uma palavra em inglês que significa procuração.
- Em termos técnicos, servidor proxy é um software que tem um “procuração” de um ou mais hosts para buscar na internet uma informação solicitada.
- Ele é o responsável pela ligação da rede interna com a rede externa e tem como características principais a filtragem de conteúdo e o registro de páginas já visitadas (cache);
- Servidores Proxy não suportam todos os protocolos. Geralmente suportam HTTP e FTP;

Características de um Proxy

- Listas de controles de acesso;
- Cache;
- Autenticação;
- Proxy transparente;

Características de um Proxy

- Listas de controles de acesso:
  - Também conhecidas como acls, permite que o administrador restrinja o acesso a determinados sites baseados em critérios estipulados em listas de controles.

Características de um Proxy

- Cache:
  - Armazena temporariamente páginas da Web e arquivos de FTP para solicitações de clientes proxy. Esta funcionalidade aumenta o desempenho do acesso as páginas.

Características de um Proxy

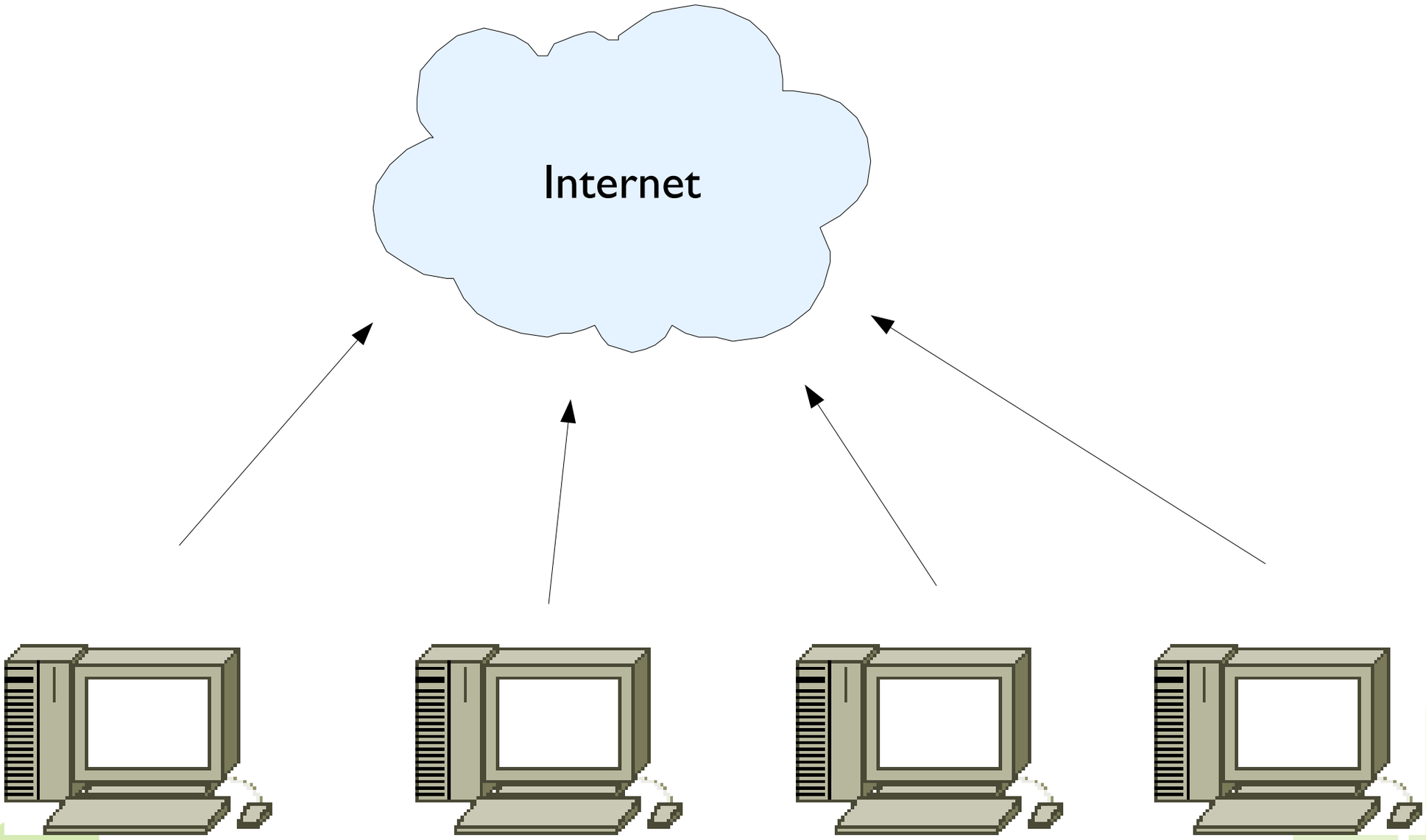
- Autenticação:
  - Permite autenticar clientes através de login, baseados em usuário e senha.

Características de um Proxy

- Proxy Transparente:
  - Com o proxy transparente não é necessário a configuração no navegador do cliente;
  - Realiza-se uma configuração no roteador padrão da rede local de forma que toda solicitação de tráfego externo é direcionada para o proxy;
  - Esse recurso de Proxy Transparente não funciona com autenticação de usuários;
  - Deverá ser feito redirecionamento da porta 80:
    - iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128

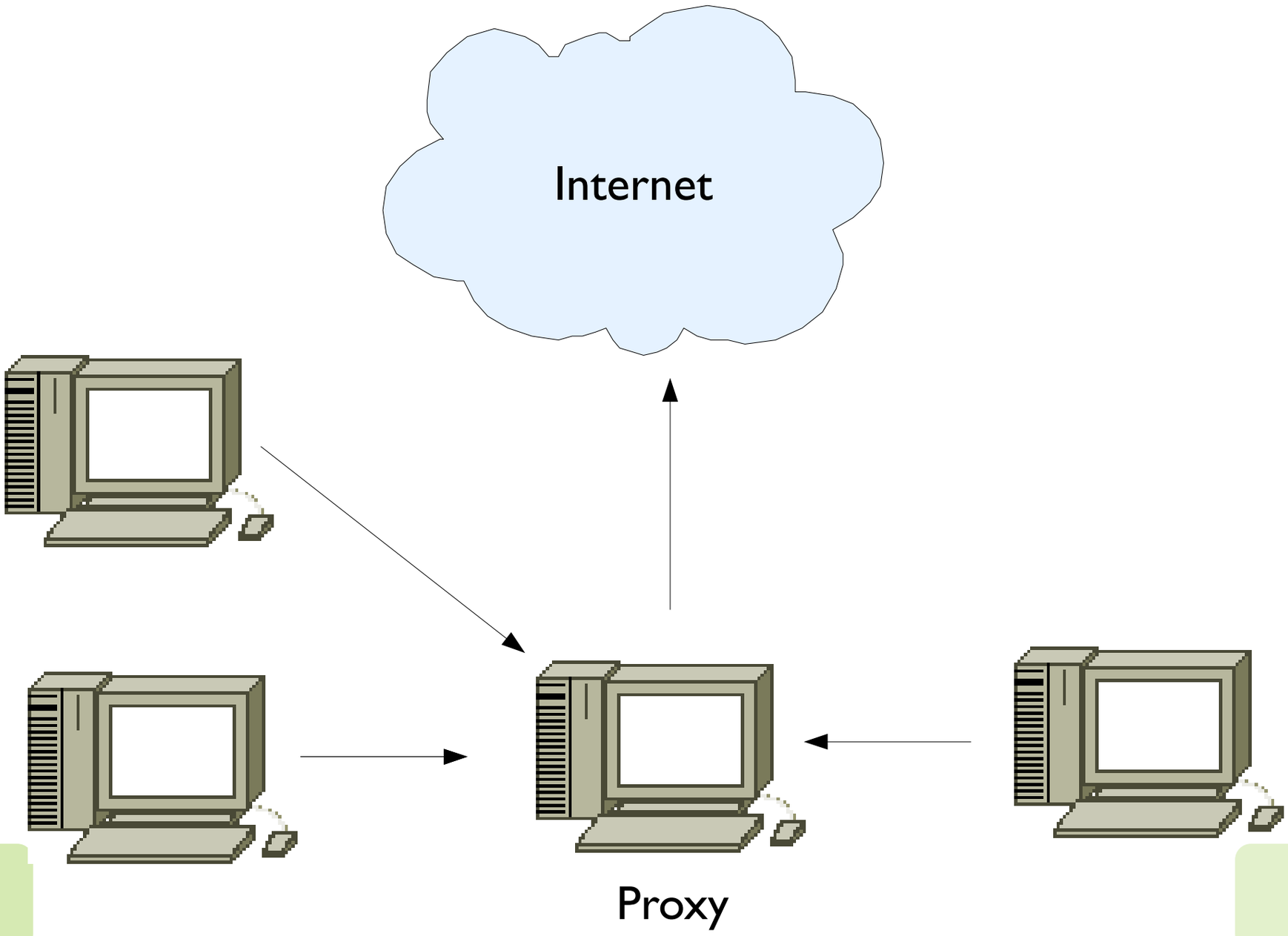
Características de um Proxy

- Infraestrutura do serviço de Proxy:



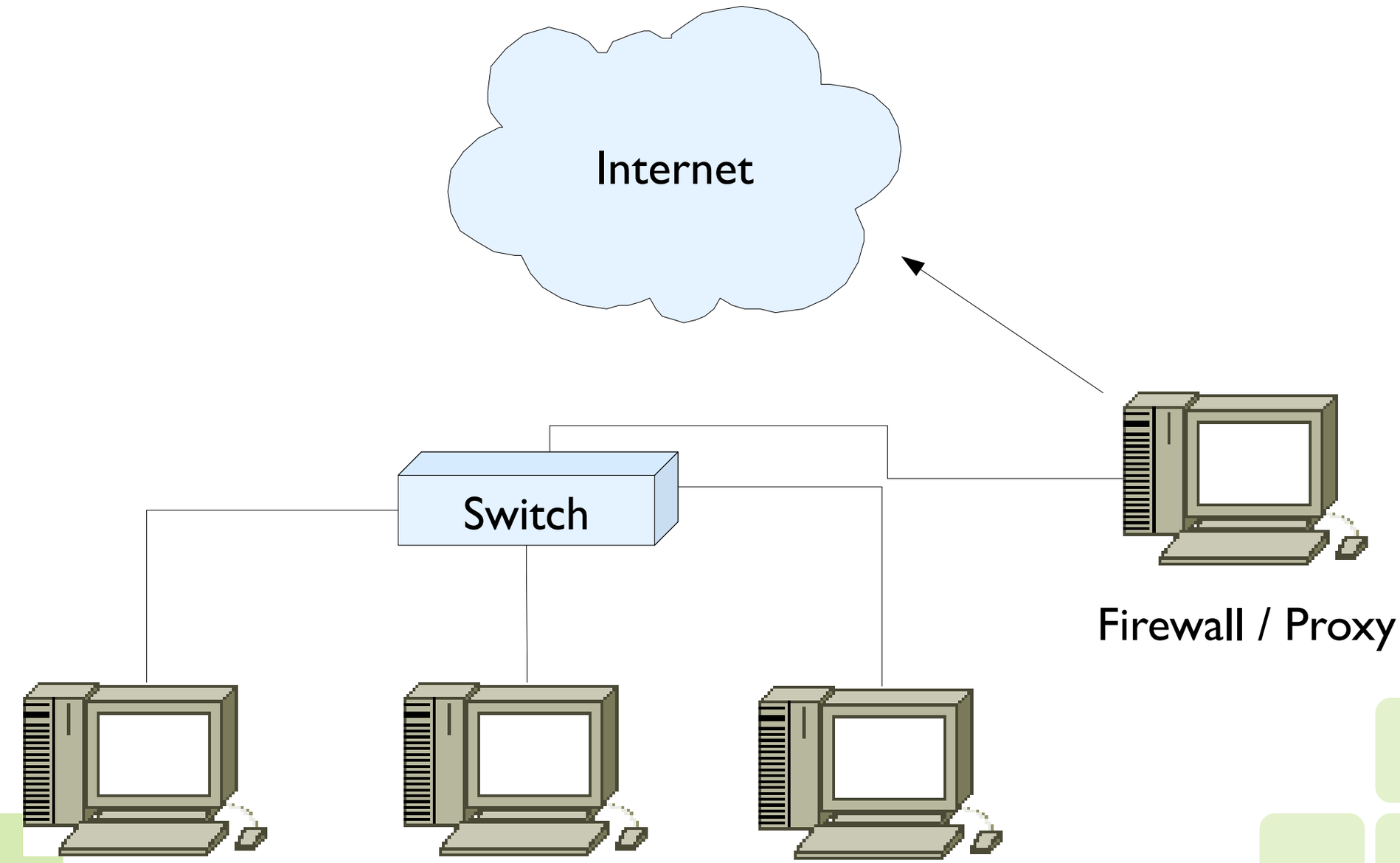
Características de um Proxy

- Infraestrutura do serviço de Proxy:



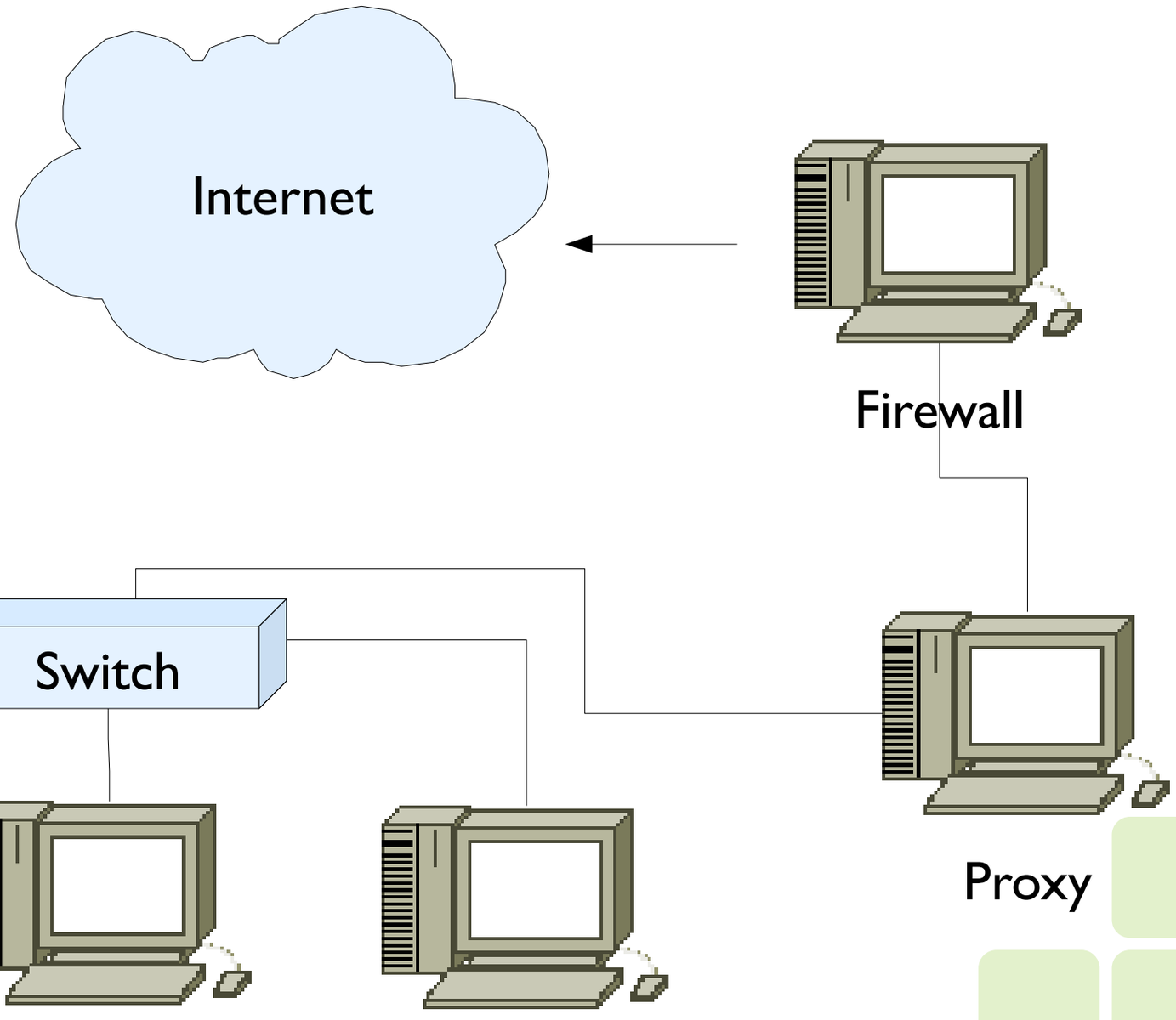
Características de um Proxy

- Infraestrutura do serviço de Proxy:



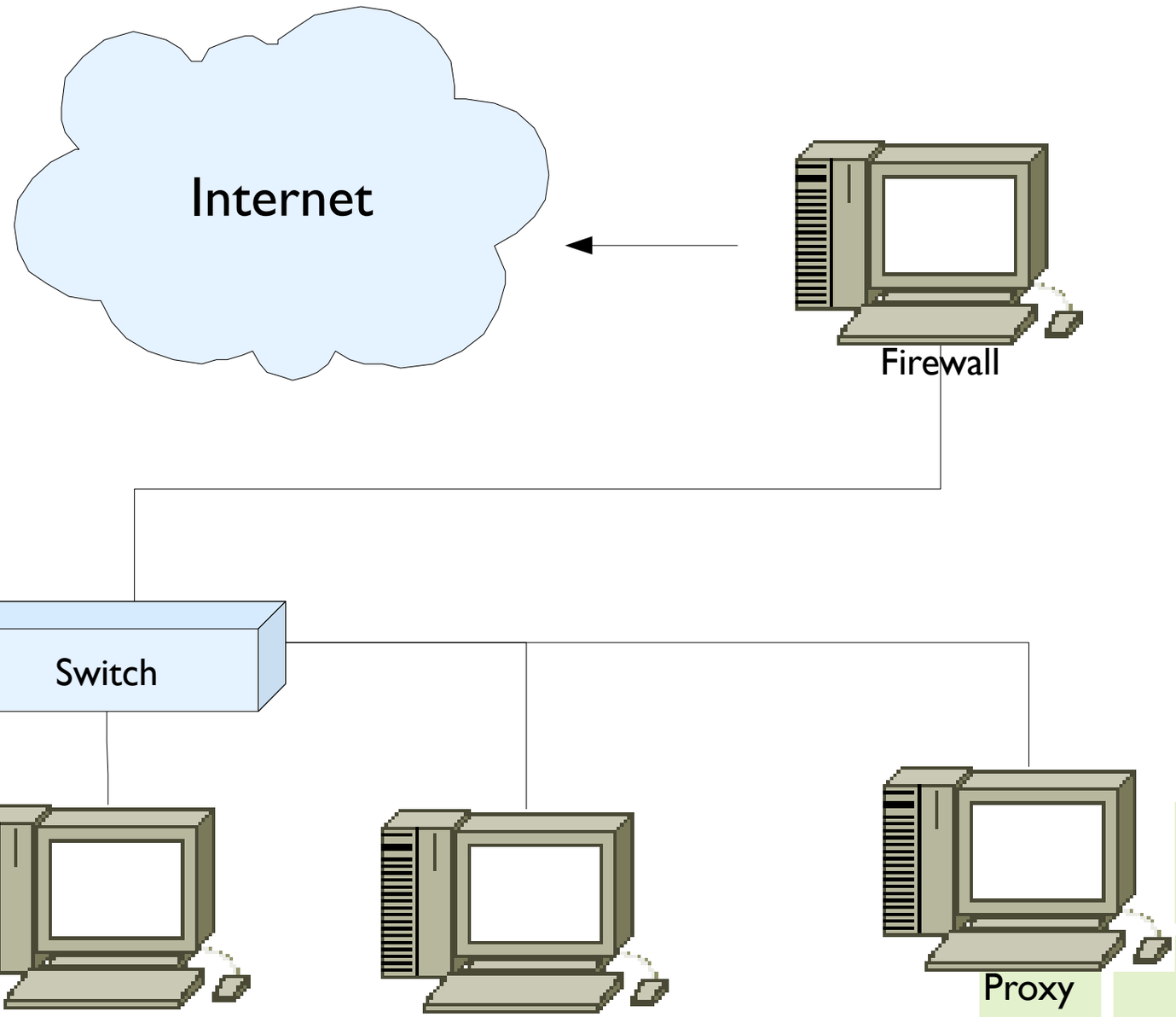
Características de um Proxy

- Infraestrutura do serviço de Proxy:



Características de um Proxy

- Infraestrutura do serviço de Proxy:



Porque utilizar Squid

- Squid é um animal cefalópode (como uma lula, polvo, etc) de dez braços, encontrado nas costas marítimas americanas.
- Existem vários proxy com características diferentes no mercado, porém o proxy SQUID é o mais popular e possui as principais funcionalidades;
  - Cache de Páginas;
  - Autenticação;
  - Proxy Transparente;
  - Registro de Acesso;
  - Segurança (ACL).
- Site oficial: http://www.squid-cache.org/

Porque utilizar Squid

- É um software especializado em fazer a operação de proxy de web e ftp, completamente free e com excelente suporte para operação em servidores Linux;
- O Squid só da acesso a serviços ftp e http/https, caso o administrador queira usar outros serviços deve usar a opção de IP Masquerading;
- Pode ser realizado um controle de acesso:
  - por usuário;
  - por horário de acesso;
  - tipo de arquivo baixado;
  - tamanho do arquivo;

Porque utilizar Squid

- Alguns proxy:
  - AnalogX (Windows);
  - Winconnect (Windows);
  - Delegate (Linux);
  - OOPS (Linux);
  - SQUID (Linux);

Utilização das ACL

- As flexíveis regras de acesso do Squid possibilitam o controle total das requisições feitas pelos usuários;
- De acordo com sua classe de regra, permitem bloquear, retardar, registrar e autorizar os acessos de acordo com diversos parâmetros, como:
  - Origem da requisição;
  - Destino da requisição;
  - Horário da requisição;
  - Endereço MAC;
  - Disponibilidade de banda;
  - Filtros personalizados baseados em strings ou expressões regulares;

Utilização das ACL

- Sintaxe das regas de acesso:

```
acl minharede  src 192.168.0.0/255.255.255.0 _________ Máscara da ACL
 |       |          |      |_ Domínio da ACL
 |       |          |_________ Tipo de ACL
 |       |_____________________Nome da ACL
 |_____________________________ Comando de criação de ACL
```

- Isto cria uma ACL de nome minharede do tipo src (IP de origem) sendo seu domínio 192.168.0.0/255.255.255.0 uma rede classe C.

Utilização das ACL

- O comando acl define apenas a classe do controle de acesso, ou seja, define apenas a regra e seu domínio;
- Para entrar em vigor, ela deve ser utilizada por um operador.
- Existem vários operadores, no entanto o mais comum é o http_access.
  - http_access allow minha_acl
  - http_acess deny minha_acl
- Squid lê as acls (operadores) de cima para baixo e quando encontra alguma que se aplique ele para.

Utilização das ACL

```
acl acesso_total src "/etc/squid/acesso_total"
acl acesso_restrito src "/etc/squid/acesso_restrito"
acl bloqueado url_regex -i "/etc/squid/bloqueado"

http_access allow acesso_total
http_access deny bloqueado
http_access allow acesso_restrito
http_access deny all
```

Utilização das ACL

- Sempre defina com última diretiva um regra de acesso que bloqueie todas as solicitações de acesso;
- Não crie regras de acesso desnecessárias, evite redundância e diretivas que exijam resolução de nomes dns;
- Caso seja necessário um grande número de diretivas, utilize a integração do squid com programas de terceiros (DansGuardian);

Auditoria

- O SARG (Squid Analysis Report Generator)
  - É uma ferramenta que analisa o arquivo de log "access.log".
  - Permite visualizar através de relatórios:
    - sites acessador pelos usuários;
    - hora de acesso;
    - quantidade de bytes baixados,
    - quantidade de conexões feitas,
    - sites mais acessados,
    - usuários que mais acessam,
    - sites mais negados,
    - as falha de autenticação,
    - . . . .

Auditoria

SARG Squid Analysis Report Generator

Relatorio de acessos dos Usuarios do Squid

ARQUIVO/PERÍODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
2008Dec17-2008Dec17	Wed Dec 17 18:00:37 BRT 2008	31	1.10G	35.53M
2008Dec16-2008Dec16	Wed Dec 17 06:29:00 BRT 2008	29	2.38G	82.35M
2008Dec15-2008Dec15	Tue Dec 16 06:28:49 BRT 2008	28	2.39G	85.65M
2008Dec14-2008Dec14	Mon Dec 15 06:28:44 BRT 2008	7	152.70M	21.81M
2008Dec13-2008Dec13	Sun Dec 14 06:28:33 BRT 2008	11	128.02M	11.63M
2008Dec12-2008Dec12	Sat Dec 13 06:28:38 BRT 2008	31	1.17G	37.95M
2008Dec11-2008Dec11	Fri Dec 12 06:28:33 BRT 2008	30	1.87G	62.54M
2008Dec10-2008Dec10	Thu Dec 11 06:28:29 BRT 2008	32	1.66G	51.95M
2008Dec09-2008Dec09	Wed Dec 10 06:28:23 BRT 2008	32	1.30G	40.82M
2008Dec08-2008Dec08	Tue Dec 9 06:28:17 BRT 2008	32	1.19G	37.28M
2008Dec07-2008Dec07	Mon Dec 8 06:28:11 BRT 2008	12	147.83M	12.31M
2008Dec06-2008Dec06	Sun Dec 7 06:28:14 BRT 2008	16	113.57M	7.09M
2008Dec05-2008Dec05	Sat Dec 6 06:28:10 BRT 2008	24	741.47M	30.89M

Auditoria

Squid Analysis Report Generator

Relatorio de acessos dos Usuarios do Squid

Periodo: 2008Dec17-2008Dec17

Ordem: BYTES, reverse

Topuser

Topsites

Sites & Users

Downloads

NUM		USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
1		192.168.0.183	9.03K	231.18M	20.99%	1.60%	98.40%	03:45:08	13.50M	6.44%
2		192.168.0.199	26.94K	160.84M	14.60%	17.09%	82.91%	07:01:20	25.28M	12.06%
3		192.168.0.165	16.03K	110.07M	9.99%	22.05%	77.95%	05:16:06	18.96M	9.05%
4		192.168.0.106	7.71K	93.54M	8.49%	0.80%	99.20%	02:32:45	9.16M	4.37%
5		192.168.0.117	1.10K	91.91M	8.34%	1.85%	98.15%	00:38:41	2.32M	1.11%
6		192.168.0.120	1.43K	72.38M	6.57%	1.58%	98.42%	00:17:01	1.02M	0.49%
7		192.168.0.103	1.92K	54.58M	4.96%	2.81%	97.19%	00:56:08	3.36M	1.61%
8		192.168.0.144	6.65K	53.55M	4.86%	46.33%	53.67%	01:12:30	4.35M	2.07%
9		192.168.0.159	12.72K	43.75M	3.97%	13.14%	86.86%	16:12:18	58.33M	27.82%
10		192.168.0.192	7.36K	35.02M	3.18%	21.61%	78.39%	01:14:26	4.46M	2.13%
11		192.168.0.83	6.29K	34.06M	3.09%	12.21%	87.79%	01:26:22	5.18M	2.47%

Referências

- Lunardi, Marco Agisander; Squid: Prático e didático;
- MiniCurso de Filtro de Conteúdo utilizando SQUID – III Semana Nacional de Ciência e Tecnologia; Professor Mauro Borges França