UNIVERSIDADE PORTUCALENSE

Firewalls

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

O que é um Firewall?

- Interliga redes com diferentes níveis de confiança
- Impõe restrições nos serviços de rede
  - Só o tráfego autorizado é permitido
- Auditoria e controlo de acessos
  - Permite a implementação de alarmes em casos de comportamento anormal
- Defesa do perímetro

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Politicas de firewall

Deny-everything-not-specifically-allowed

Allow-everything-not-specifically-denied

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Firewalls – Filtragem de pacotes

- Funciona na camada de transporte
  - Endereços IP de origem e destino
  - Protocolos (TCP, UDP, ICMP, etc)
  - Portas de origem e destino - TCP ou UDP
  - Flags de TCP (SYN, ACK, FIN, RST, PSH, etc)
  - Tipos de mensagens de ICMP
- Exemplos
  - DNS (porta 53)
    - Negar o tráfego de entrada na porta 53 para servidores que não sejam de confiança

UNIVERSIDADE PORTUCALENSE

Utilização da filtragem de pacotes

- Filtrar informação nas interfaces de entrada ou saída
  - Por exemplo negar o tráfego de entrada de endereços IP spoofed
  - Filtrar o tráfego de saída
- Permitir ou negar alguns serviços
  - É necessário conhecimento da utilização das portas de TCP e UDP

UNIVERSIDADE PORTUCALENSE

Como configurar um filtro de pacotes

- Começar por definir uma política de segurança
- Definir quais os pacotes admissíveis (em termos de expressões lógicas)
- Reescrever as regras na sintaxe do fornecedor do equipamento
- Regras gerais
  - Tudo o que não é expressamente permitido é proibido
  - O que não for necessário deve ser eliminado

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Firewalls – Filtragem de pacotes

- Problemas:
  - É fácil de passar as regras.
  - Bom registo é difícil.
  - Os routers geralmente não podem fazer a autenticação de pontos finais da ligação.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

Segurança e performance

UNIVERSIDADE PORTUCALENSE

- Ataque utilizando a separação em pequenos fragmentos
  - Dividir os cabeçalhos de TCP em vários pacotes pequenos
  - Eliminar ou juntar a informação antes de serem verificados
- A degradação depende do número de regras aplicadas
- A ordem das regras é importante (regras mais utilizadas primeiro)
- A correção é mais importante do que a velocidade

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Exemplo

```
access-list exterior permit tcp any host 193.136.76.72 eq www
access-list exterior permit tcp any host 193.136.76.72 eq ident
access-list exterior permit tcp any host 193.136.76.76 eq www
access-list exterior permit tcp any host 193.136.76.76 eq ident
access-list exterior permit tcp any host 193.136.76.77 eq www
access-list exterior permit tcp any host 193.136.76.77 eq ident
access-list exterior permit tcp any host 193.136.79.66 eq smtp
access-list exterior permit tcp any host 193.136.79.66 eq ident
access-list exterior permit tcp any host 193.136.79.66 eq pop3
access-list exterior permit tcp any host 193.136.79.66 eq www
access-list exterior permit tcp any host 193.136.79.67 eq www
access-list exterior permit tcp any host 193.136.79.68 eq www
```

UNIVERSIDADE PORTUCALENSE

Números de portas

- Ligações TCP
  - As portas do servidor são números menores do que 1024
  - As portas dos clientes são números entre 1024 e 16383
- Atribuição permanente
  - Portas <1024
    - 20,21 para FTP
    - 25 para o SMTP
    - 23 paraTelnet
    - 80 para HTTP
- Utilização variável
  - Portas >1024 devem estar disponíveis para os clientes efetuarem as ligações

UNIVERSIDADE PORTUCALENSE

Firewalls – Stateful Packet Filters

- Os filtros de pacotes tradicionais não examinam a camada do transporte
- Este tipo de filtragem é endereçada por estes filtros
- Examinam cada pacote IP no contexto
  - Registam as ligações cliente-servidor
  - Validam se cada pacote pertence à ligação cliente servidor

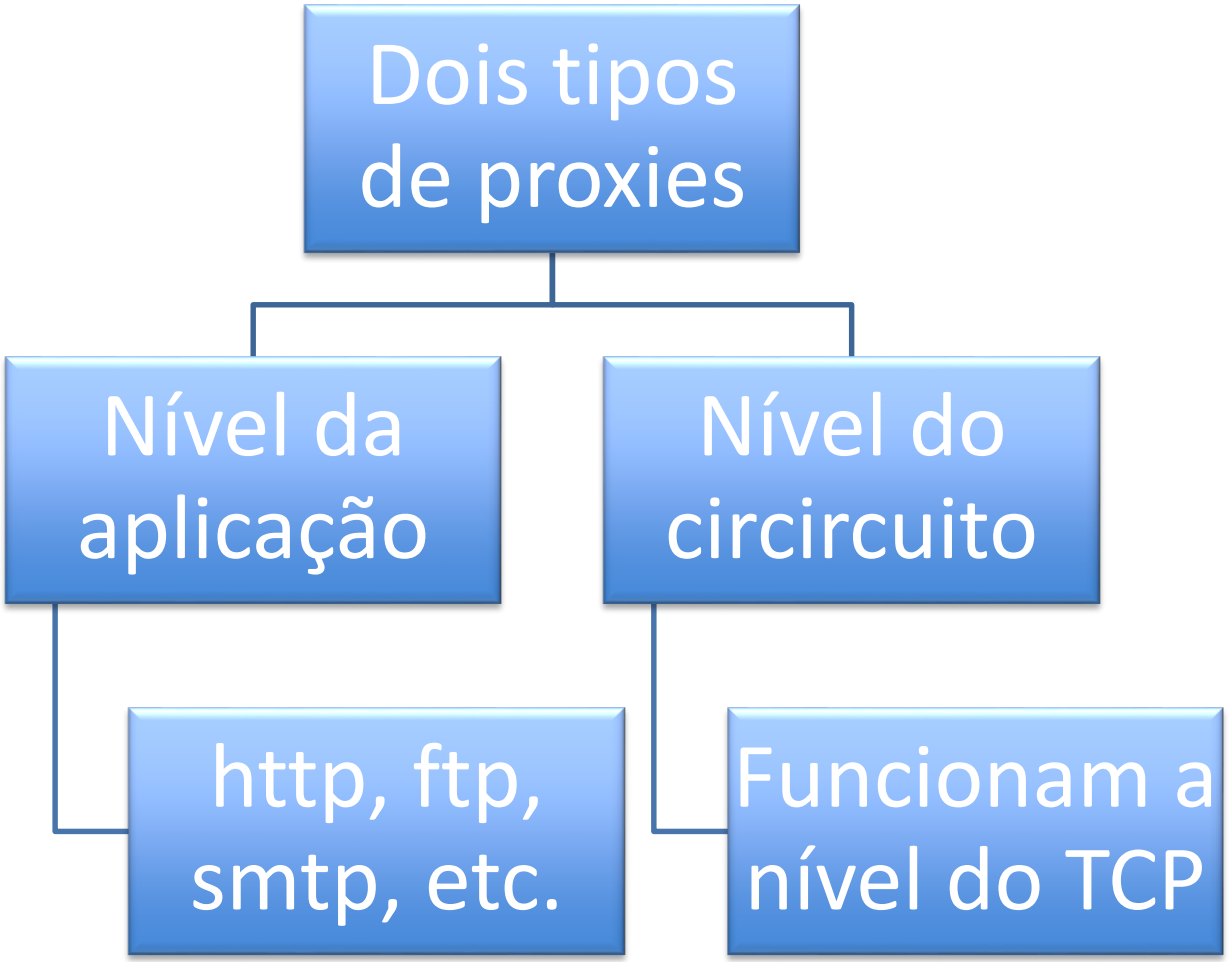
UNIVERSIDADE PORTUCALENSE

Firewall Gateways

- Este tipo de firewall executa um conjunto de proxy de aplicação
  - Os proxies filtram tráfego de entrada a saída
  - Todo o tráfego de entrada é redirecionado para a firewall
  - Todo o tráfego de saída parece ser enviado pelo firewall

UNIVERSIDADE PORTUCALENSE

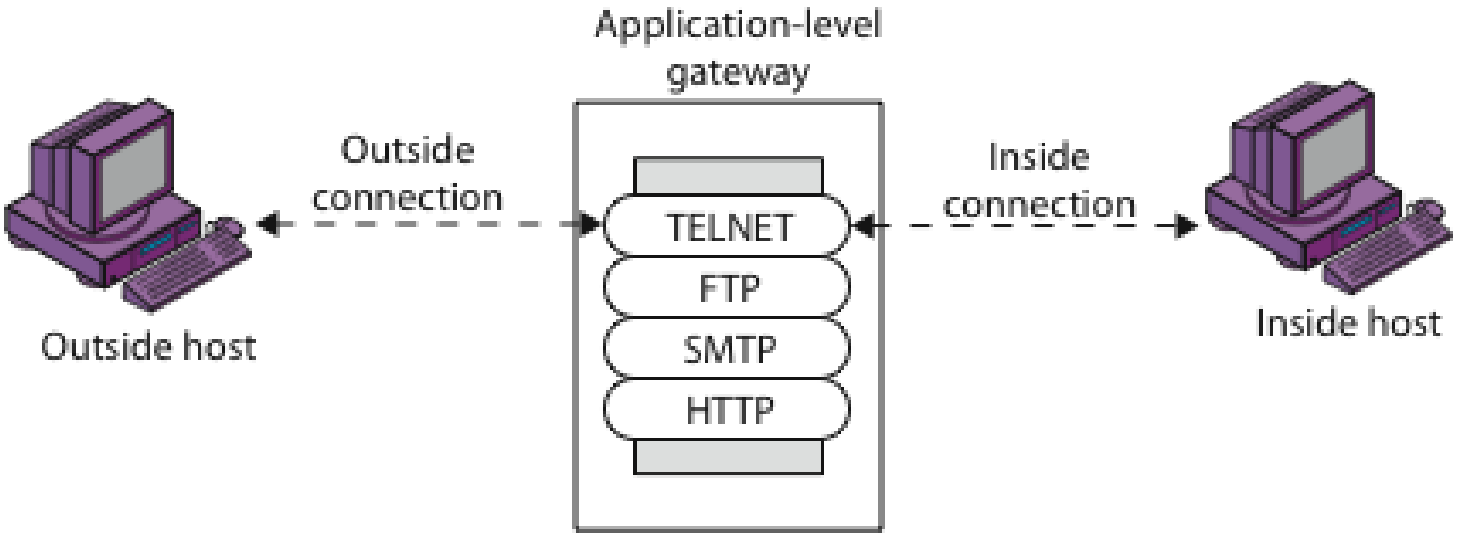
Firewall Gateways



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Firewalls – Aplicacionais (Application Level)



(b) Application-level gateway

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

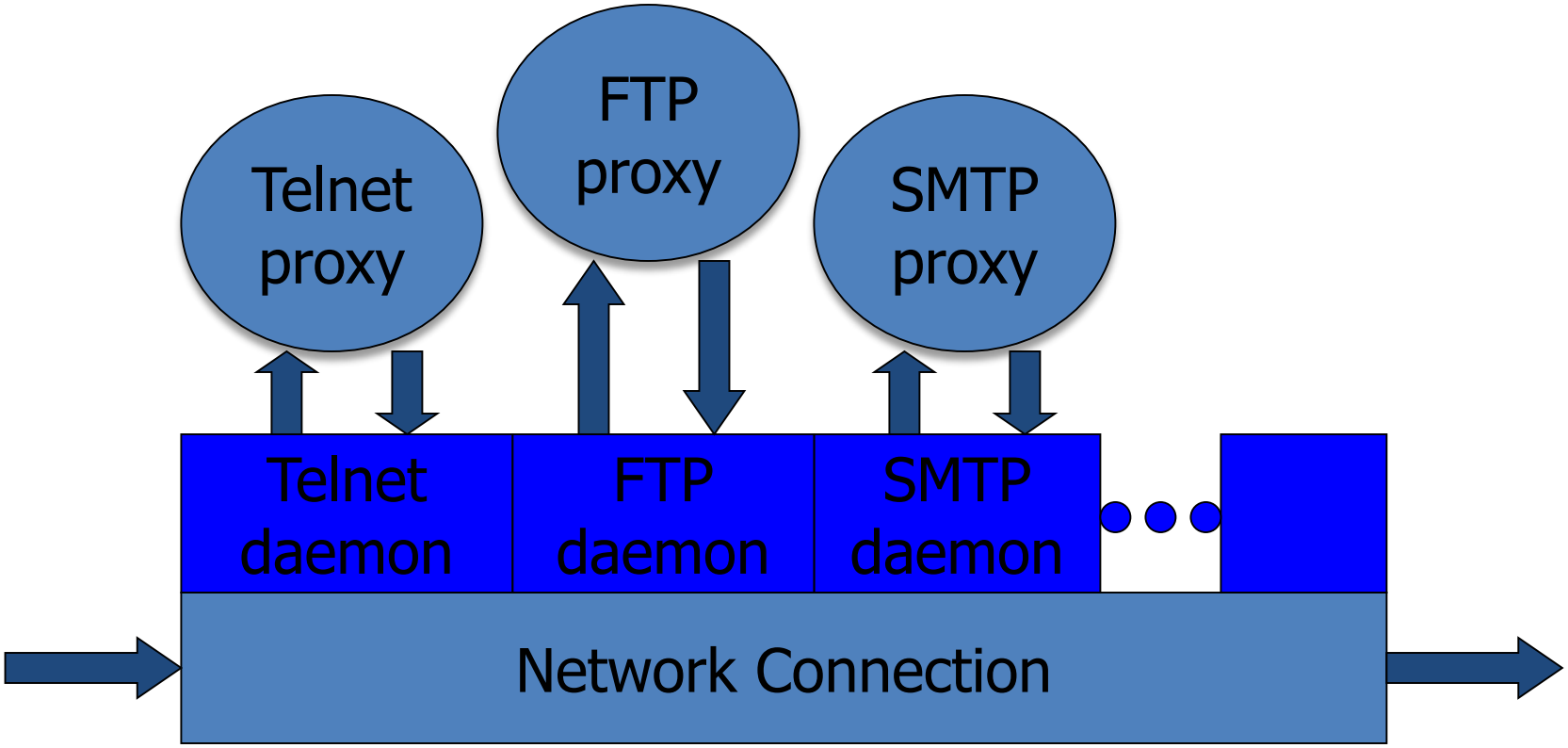
UNIVERSIDADE PORTUCALENSE

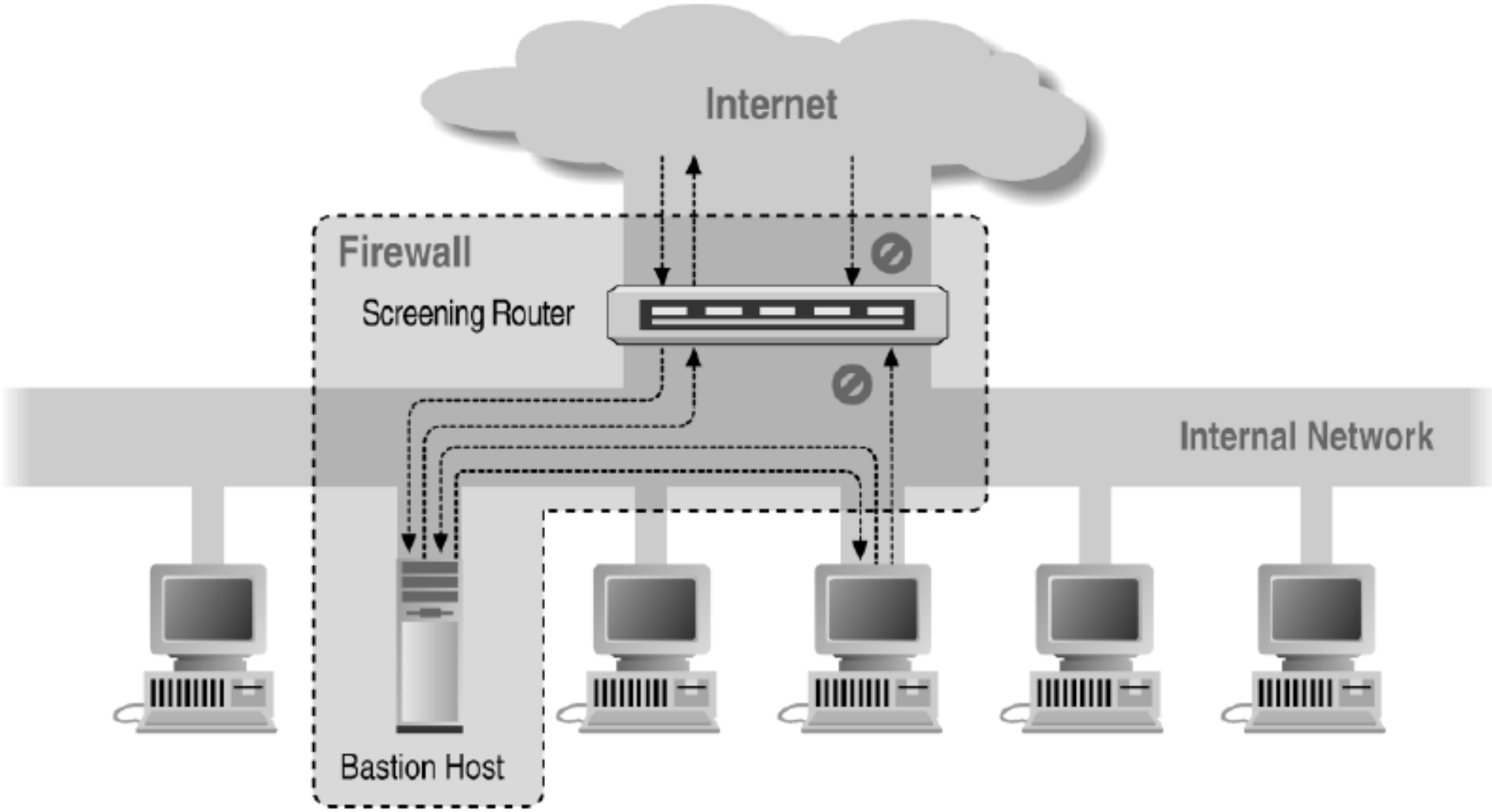
Filtros a nível da aplicação

- Acesso total ao protocolo de comunicações
  - O utilizador requisite os serviços ao proxy
  - O proxy valida a Informação
  - Devolve a Informação ao utilizador
- Necessidade de haver proxies separados para cada serviço
  - SMTP (E-Mail)
  - DNS (Domain Name System)
  - NTP (Network Time Protocol)

UNIVERSIDADE PORTUCALENSE

Firewall aplicacional




Internet
Firewall
Screening Router
Internal Network
Bastion Host

UNIVERSIDADE PORTUCALENSE

Solução perfeita?

- Inúteis contra ataques internos
- Não conseguem proteger contra todos os vírus
- Ponto único de falha (quem conseguir passar o firewall tem acesso à rede interna da instituição)

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

A zona desmilitarizada (DMZ)

A DMZ é um segmento de uma rede ou de uma rede entre a rede protegida e a "rede externa".

É também vulgarmente referida como uma rede de serviço.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

A zona desmilitarizada (DMZ)

O objetivo de uma DMZ é fornecer algum isolamento e segurança extra para os servidores que prestam os serviços da organização ao público em geral.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Intrusion Detection System (IDS)

IDS pode identificar muitos ataques e padrões de tráfego que atravessam um firewall.

Um IDS pode identificar port scans, diferentes ataques na Web, ataques de buffer overflow, etc

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Networtk Address Translation (NAT)

Mapeiam endereços

Utilização de endereços privados

Melhoram a segurança

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Port Address Translation (PAT)

Mapeiam endereços para portas de TCP

Utilização de endereços privados

Melhoram a segurança

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

VPN

VPN (Virtual Private Network)

Funciona como uma rede privada utilizando a Internet.

Utiliza IP Tunneling.

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Serviços adicionais

Antivírus

Filtro de conteúdos

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA