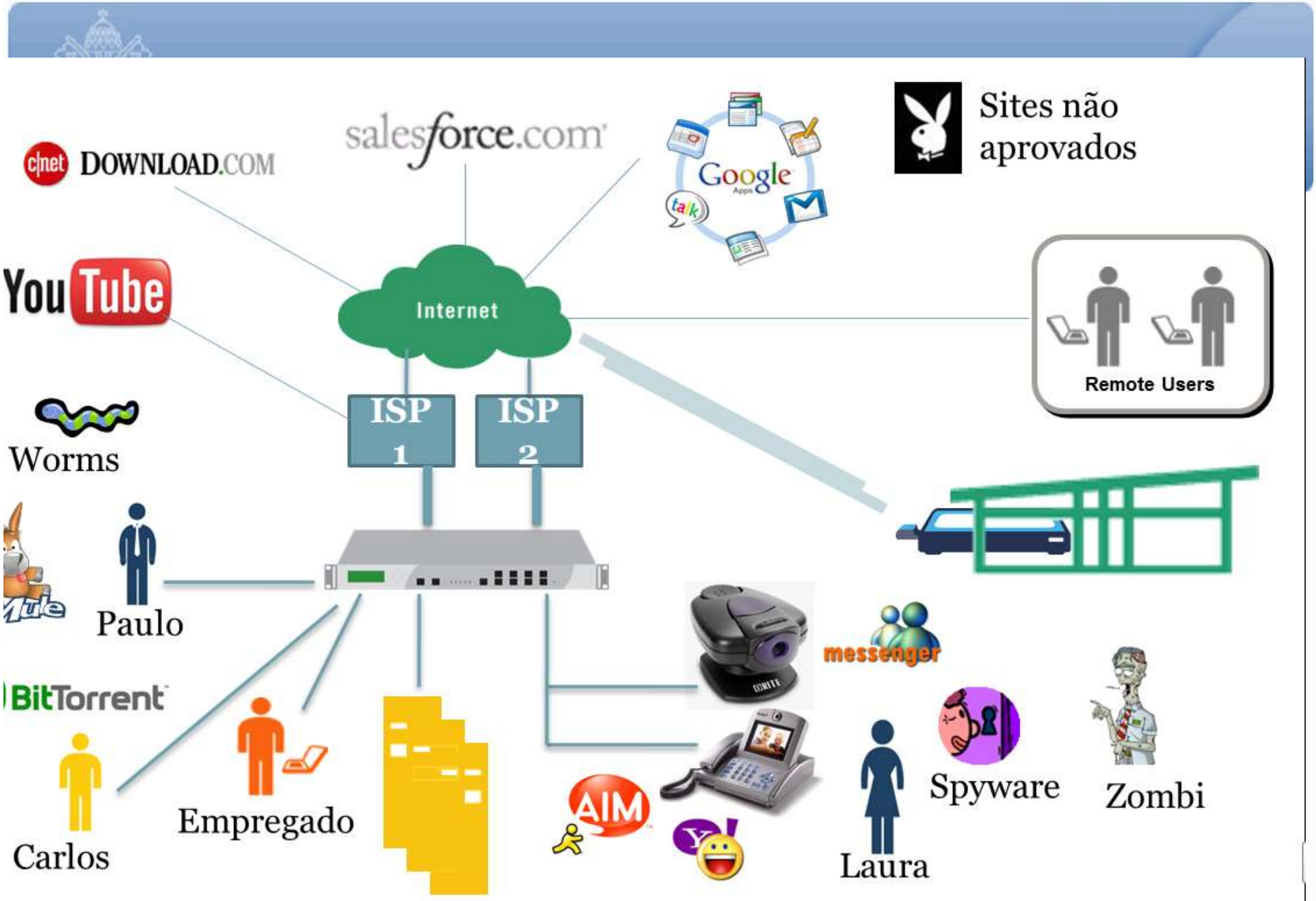
Resumo do que vimos em Segurança da Comunicação

PUC Minas

- Firewall
  - Firewall de pacotes sem estado
  - Firewall de pacotes com estado
  - Gateways de Aplicação

UTM

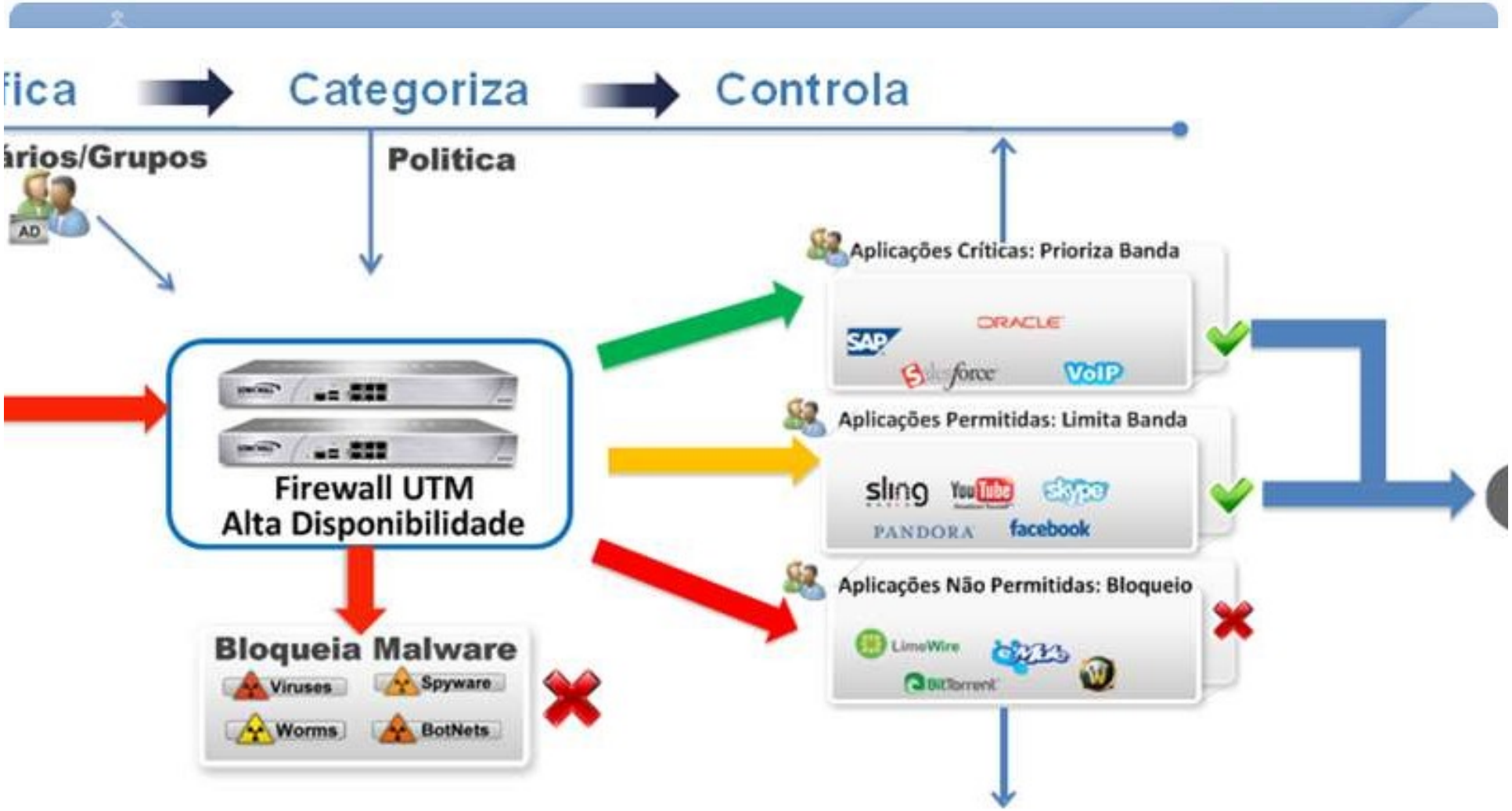
- UTM (Unified Threat Management) – Gerenciador Unificado de Ameaças: Como o próprio nome diz agrega várias funções de segurança da rede em um único equipamento com o objetivo de simplificar a administração do ambiente.



Fonte: Apresentação UTM SonicWall – empresa Altasnet http://www.altasnet.com.br

Serviços

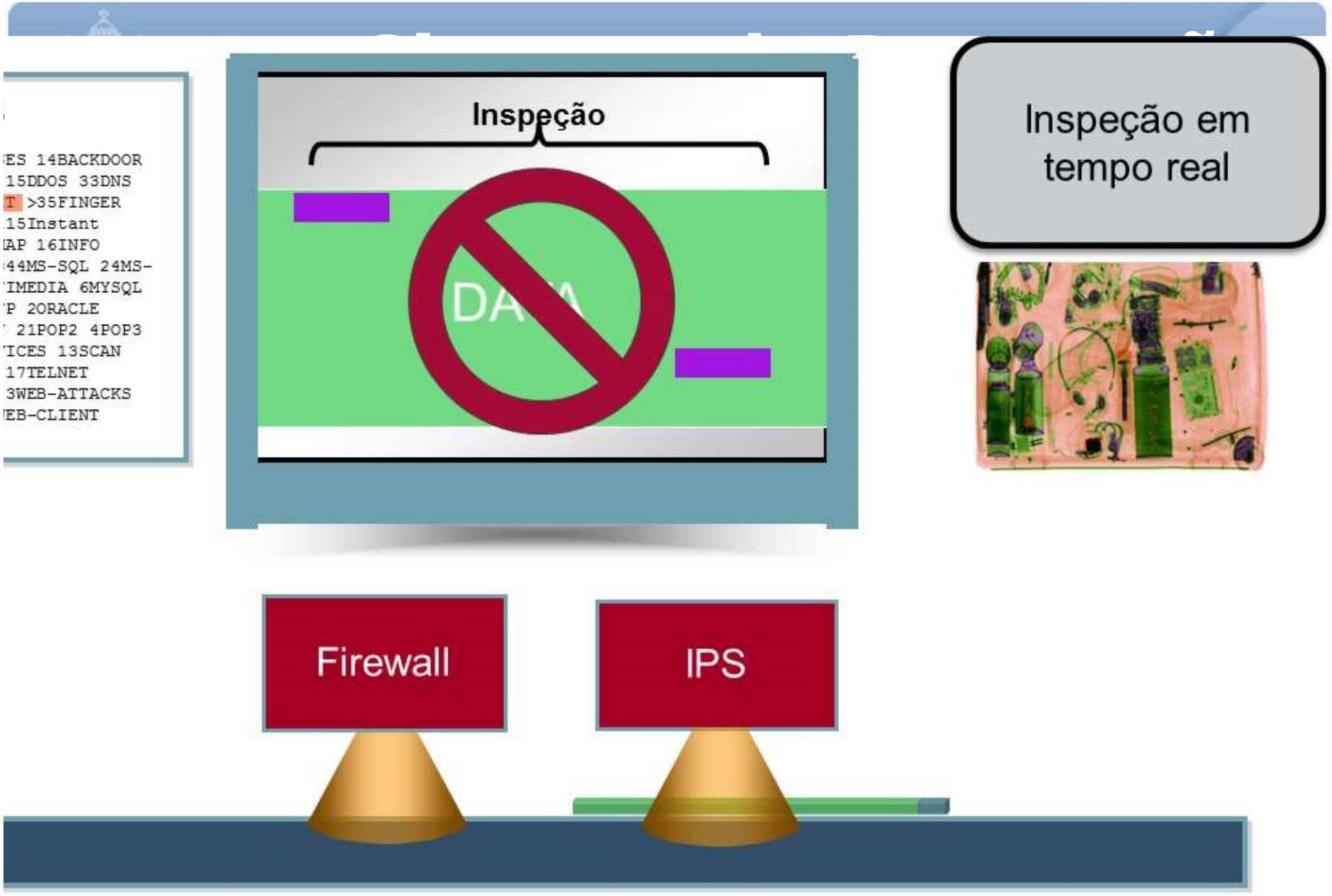
- Firewall
- VPN
- Balanceamento de Carga e redundância de link;
- Priorização de largura de banda;
- IPS – Sistema de Detecção contra intrusos
- Gateway Antivírus;
- Filtro de Conteúdo;



Seg. da WEB

Questões Sociais

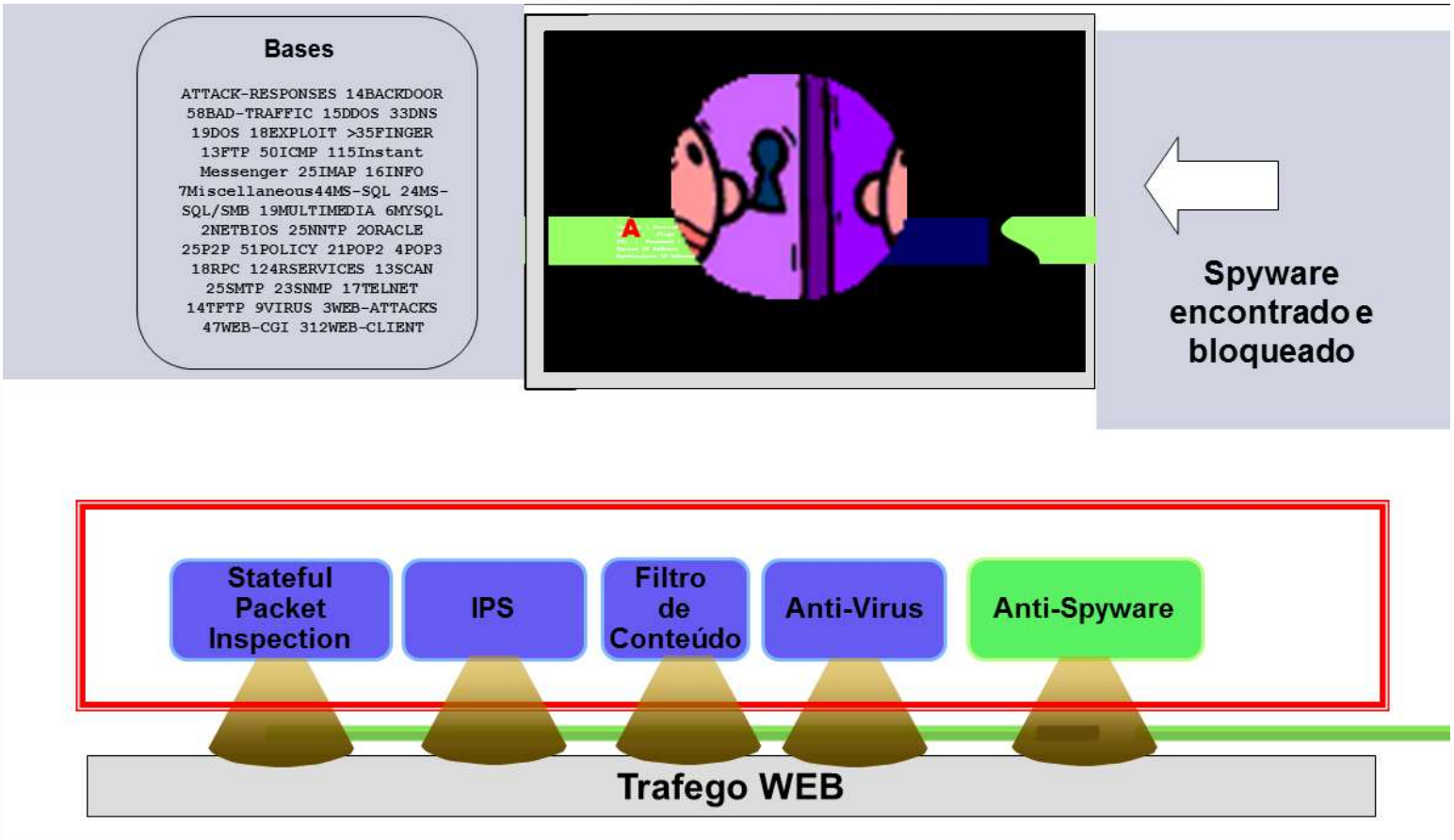
Fonte: Apresentação UTM SonicWall – empresa Altasnet http://www.altasnet.com.br



Questões Sociais

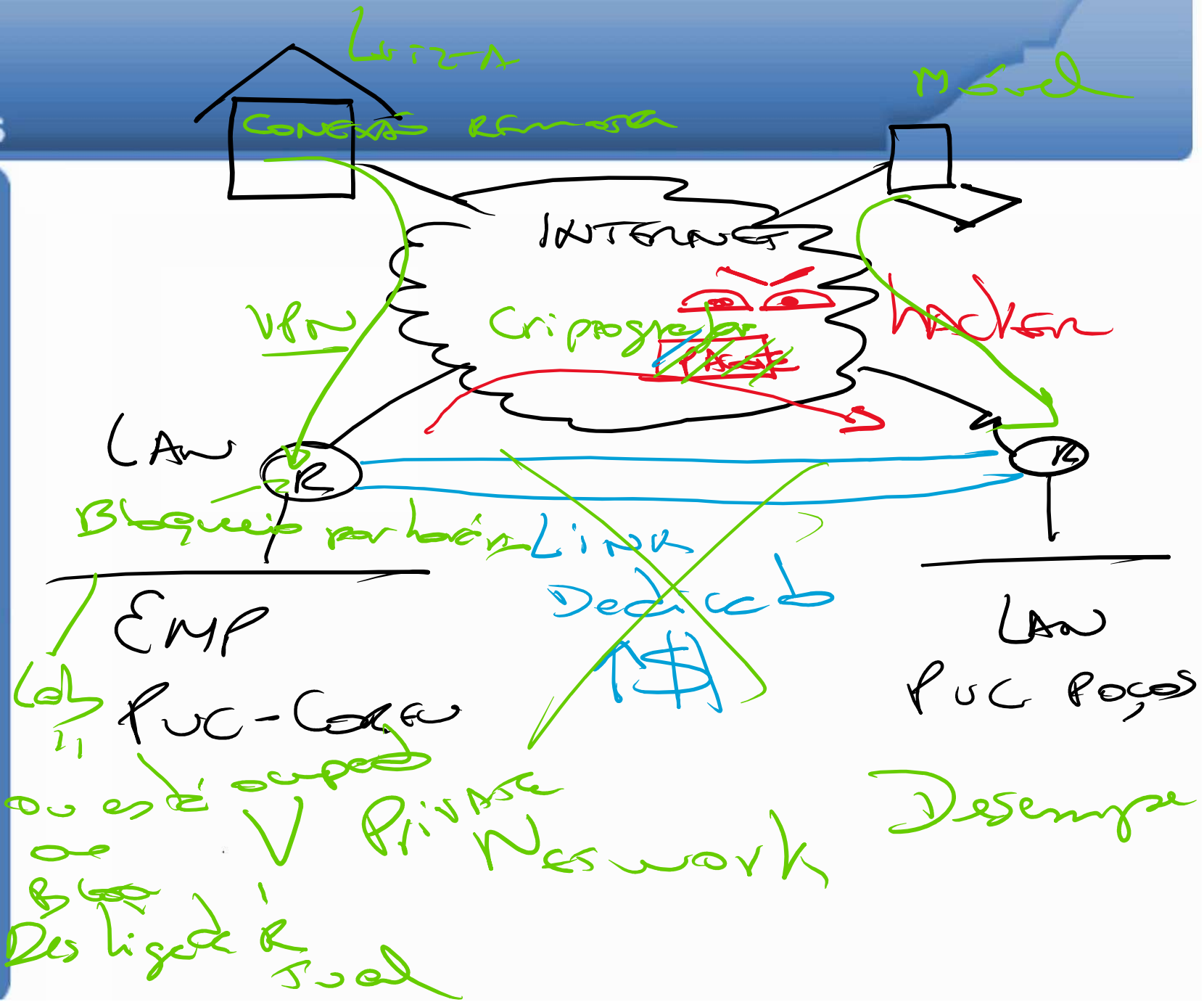
Fonte: Apresentação UTM SonicWall – empresa Altasnet http://www.altasnet.com.br

Checagem de tráfego WEB

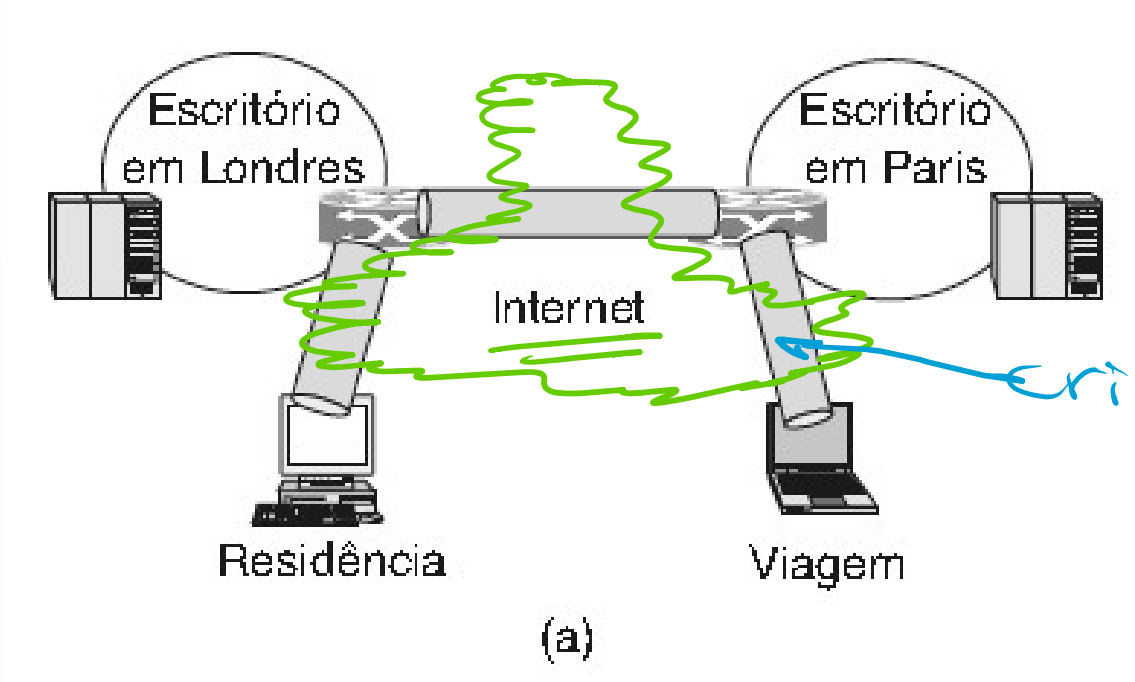


Fonte: Apresentação UTM SonicWall – empresa Altasnet http://www.altasnet.com.br

PUC Minas

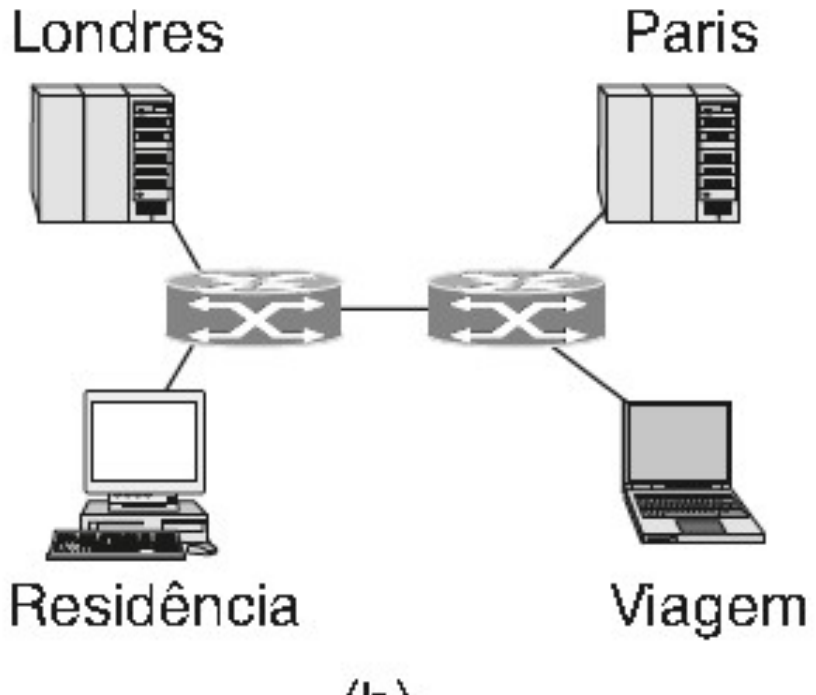


VPNs – Virtual Private Networks (1)



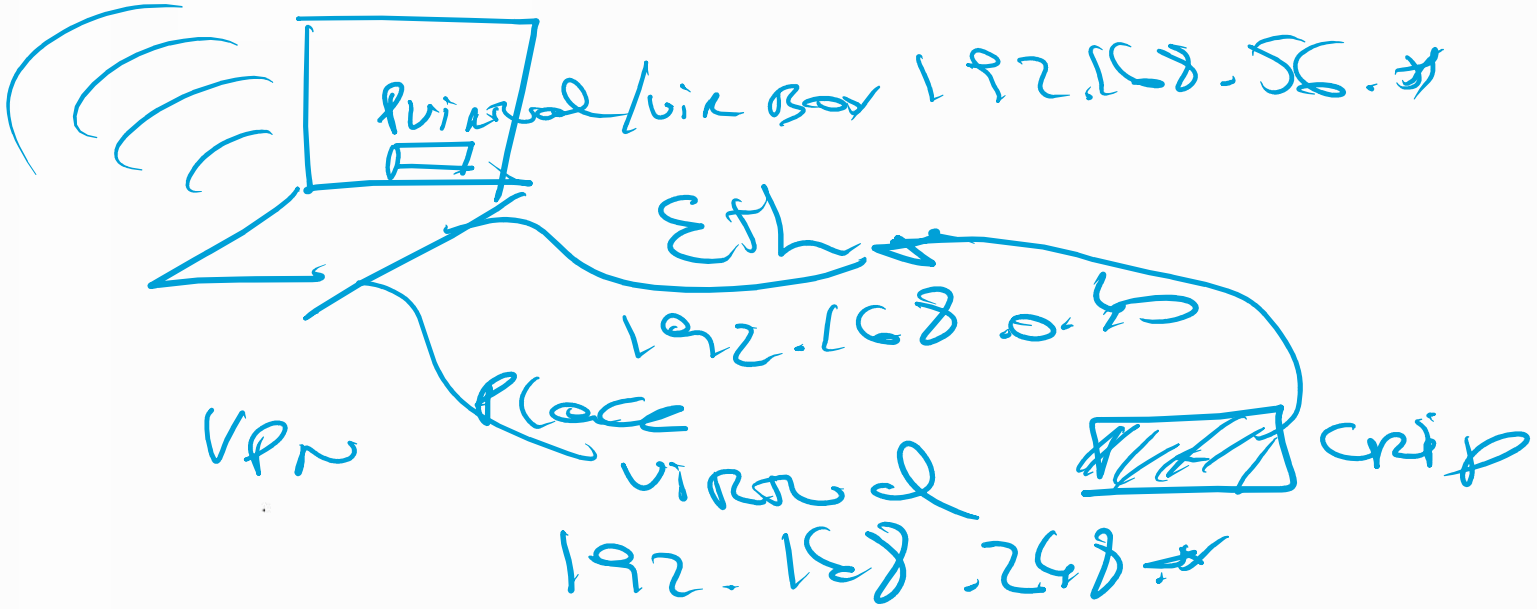
Uma rede privada virtual (VPN).

VPNs – Virtual Private Networks (2)



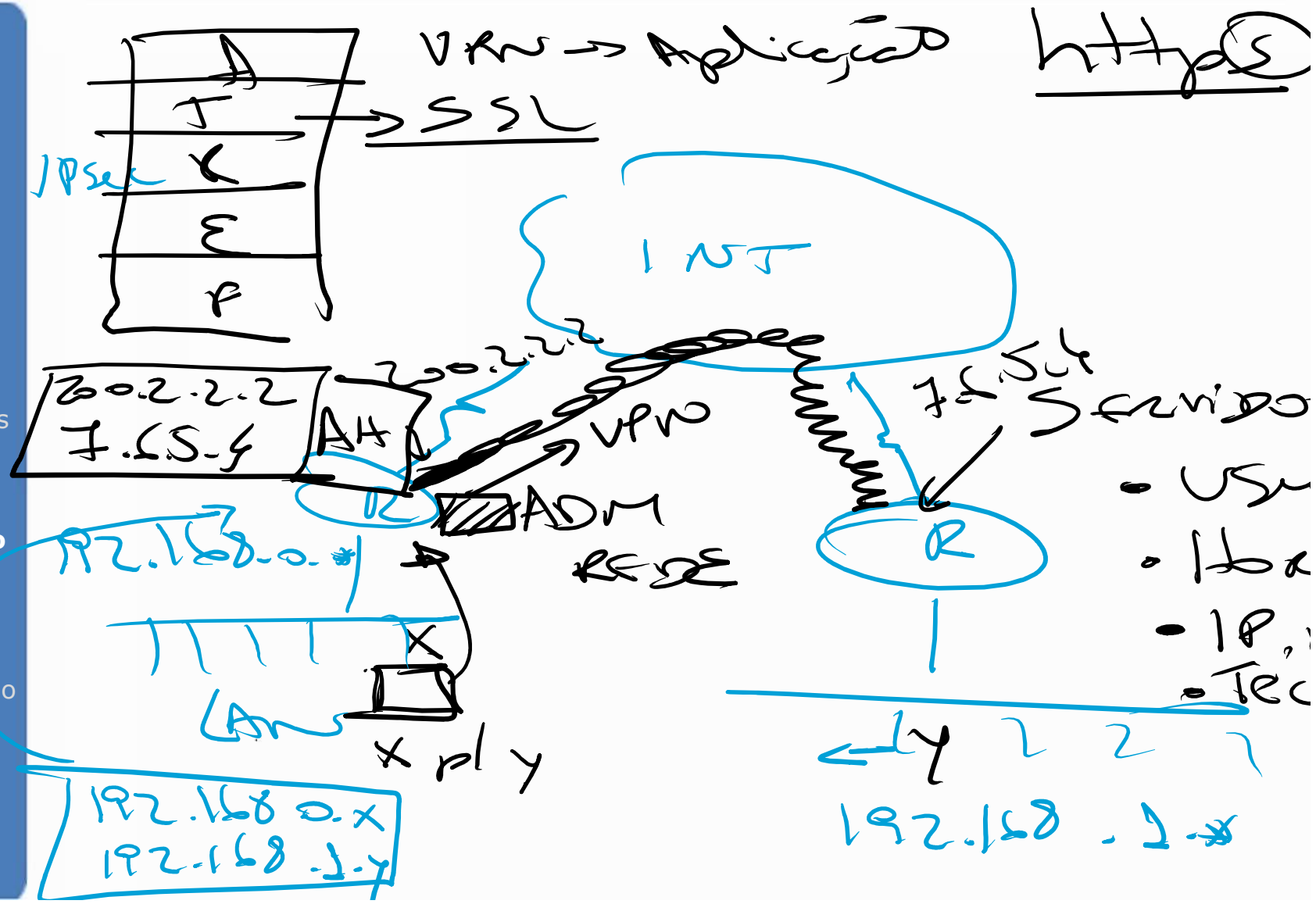
Topologia interna.

PUC Minas



VPNs – Virtual Private Networks (3)

- O tunelamento pode ser **voluntário** (estabelecido pelo próprio usuário) ou **compulsório** (o usuário não sabe que está passando por um túnel)
- O tunelamento e a criptografia garantem a segurança dos dados mas não podem garantir tempos de resposta e taxas de transmissão.



VPNs – Virtual Private Networks (4)

PUC Minas

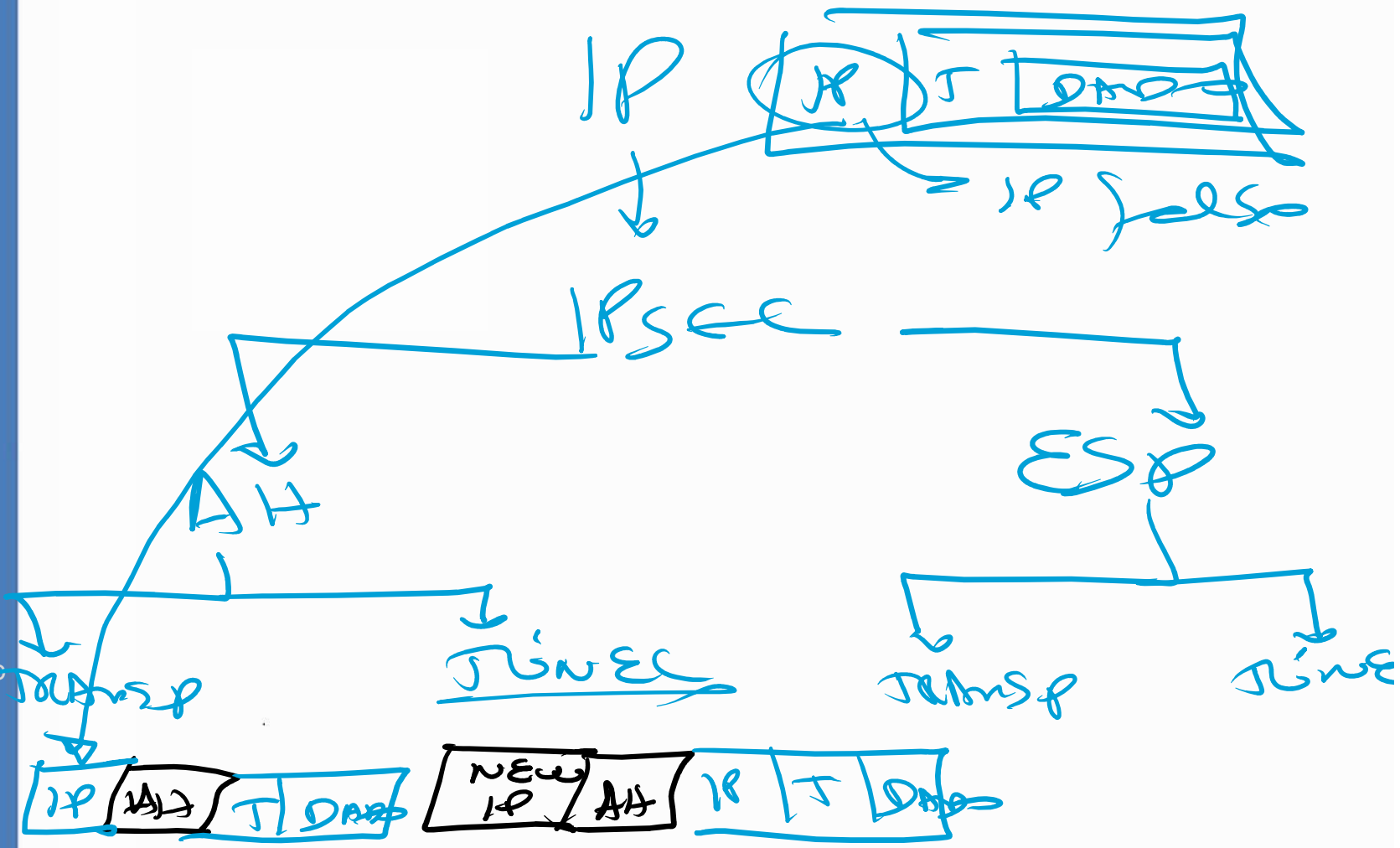
- Requisitos Básicos
  - Autenticação de Usuários
    - Autenticar o usuário e permitir o acesso apenas de usuários autorizados.
    - Auditar qualquer tentativa de acesso, autorizado ou não.
  - Gerenciamento de Endereços
    - Não divulgar os endereços internos da rede, utilizando endereços externos fictícios.
  - Criptografia de Dados
    - Manter a privacidade dos dados na rede pública.

VPNs – Virtual Private Networks (5)

- Tunelamento na Camada de Enlace:
  - PPTP (*Point-to-Point Tunneling)* da Microsoft permite que o tráfego IP, IPX e NetBEUI sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas.
  - L2TP (*Layer 2 Tunneling Protocol*) da IETF permite que o tráfego IP, IPX e NetBEUI sejam criptografados e enviados através de canais de comunicação de datagrama ponto a ponto tais como IP, X25, Frame Relay ou ATM.
  - L2F (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.
  - CIPE – Empilha tudo dentro de um pacote UDP.

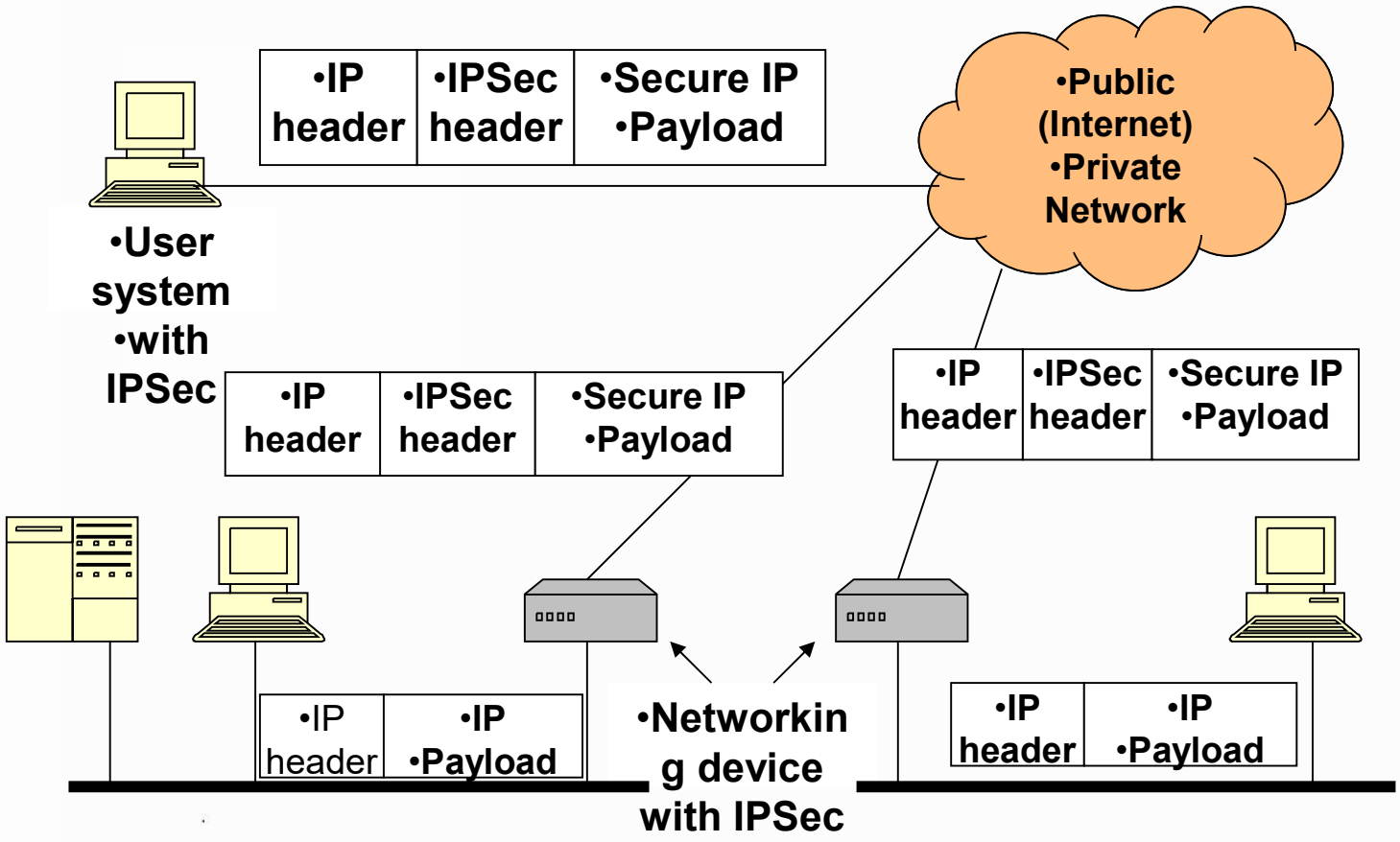
VPNs – Virtual Private Networks (6)

- Tunelamento na Camada de Rede
  - IPsec
- Tunelamento na Camada Transporte
  - SOCKS é usado para tráfego TCP através de um proxy.
  - SOCKS com serviço de NAT
  - SSL (Secure Socket Layer)
  - SSH – abertura de uma sessão remota a um computador que irá trafegar como sendo seu proxy



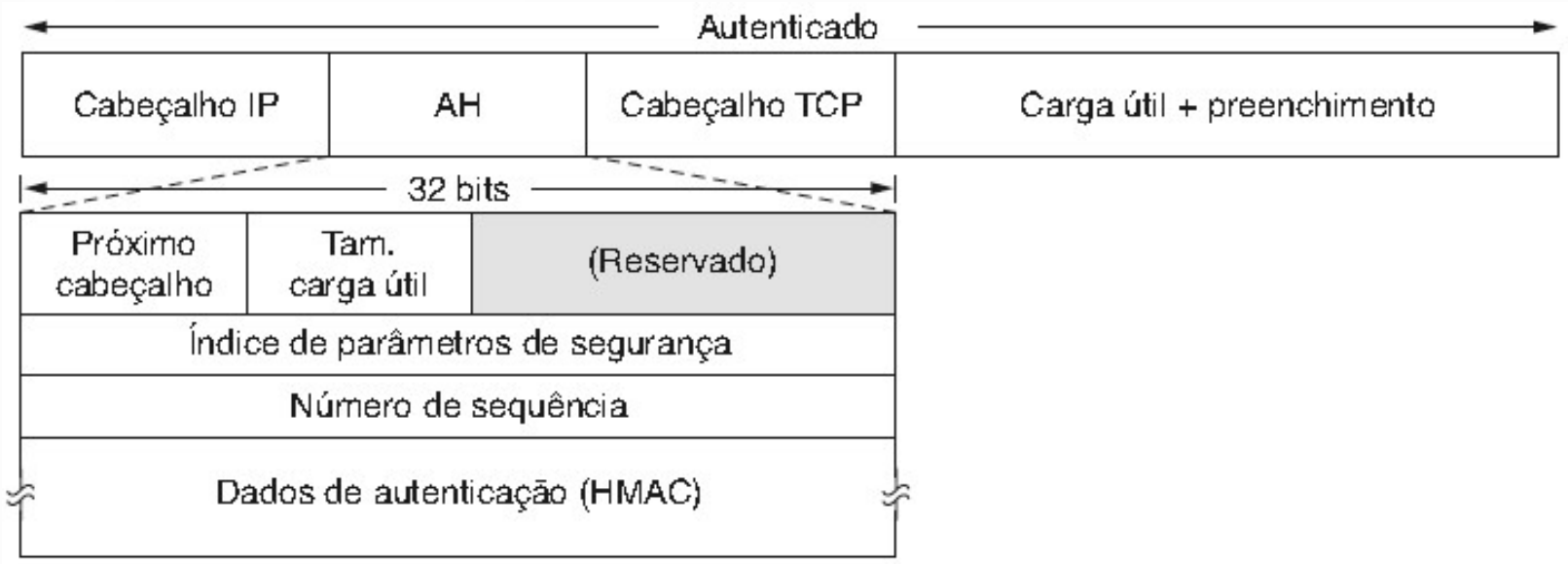
PUC Minas

IPsec (1)



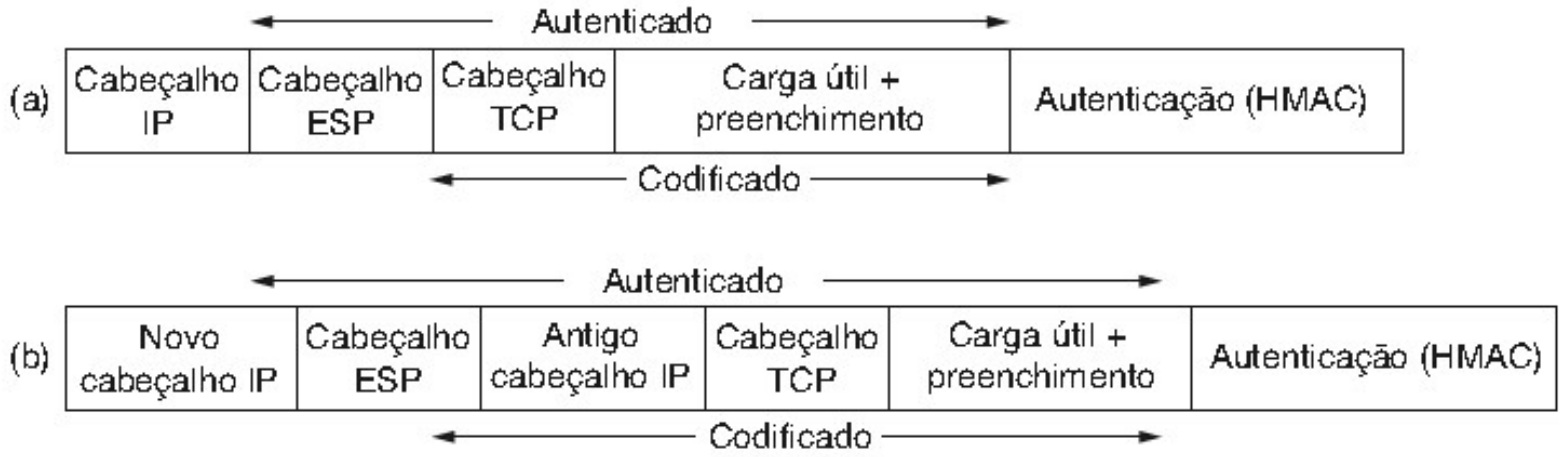
Cenário IPSec.

IPsec (2)



Cabeçalho de autenticação IPsec em modo de transporte para o IPv4.

IPsec (3)



(a) ESP em modo de transporte. (b) ESP em modo túnel.

IPsec (4)

- Modos de Operação
  - Modo Transporte
    - Criptografa apenas a carga útil do pacote IP (protocolo fim-a-fim).
    - O cabeçalho é transmitido em texto plano (inseguro).
  - Modo Túnel
    - Criptografa também o cabeçalho IP (protocolo nó-a-nó).
    - Mais seguro e menos flexível que o modo transporte

VPNs – Virtual Private Networks (7)

- **Conclusão**
  - VPNs são essenciais para a utilização da Internet como meio de transmissão de dados sensíveis
  - A segurança de uma VPN vem dos algoritmos escolhidos e da segurança das senhas
  - VPNs podem ser implementadas em hardware (roteadores) ou software (Windows Server , Linux, etc)