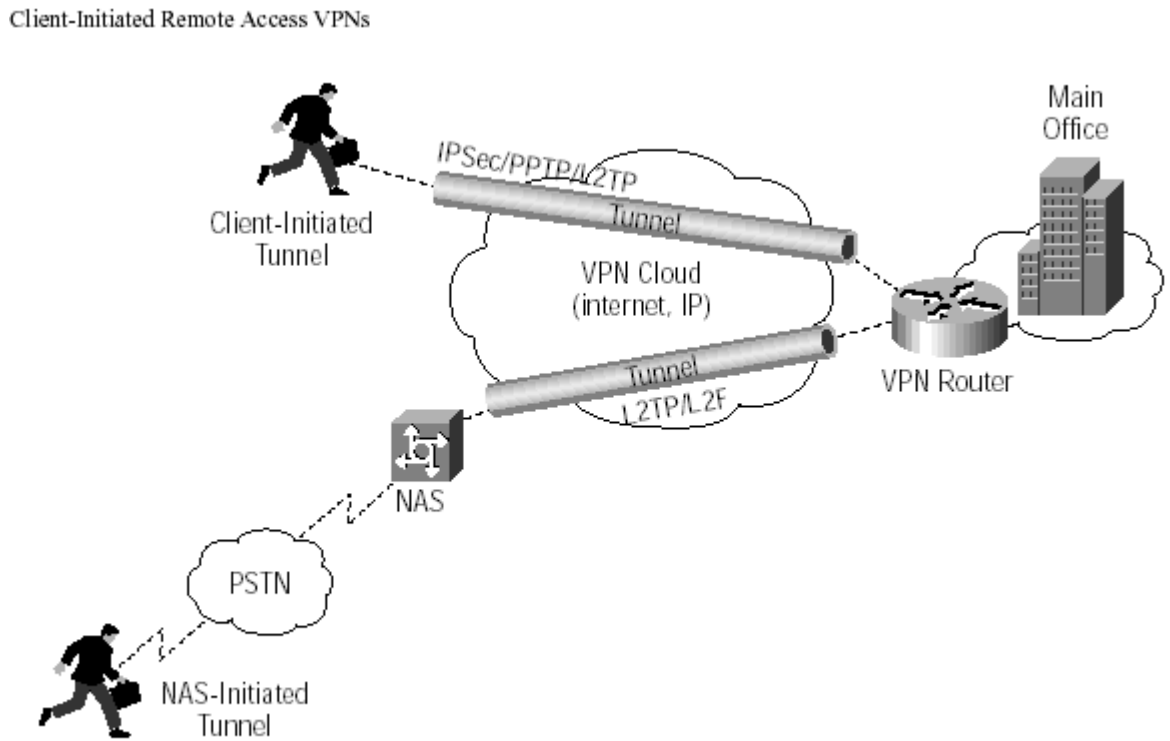
UNIVERSIDADE PORTUCALENSE

VIRTUAL PRIVATE NETWORK (VPN)

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network - VPN

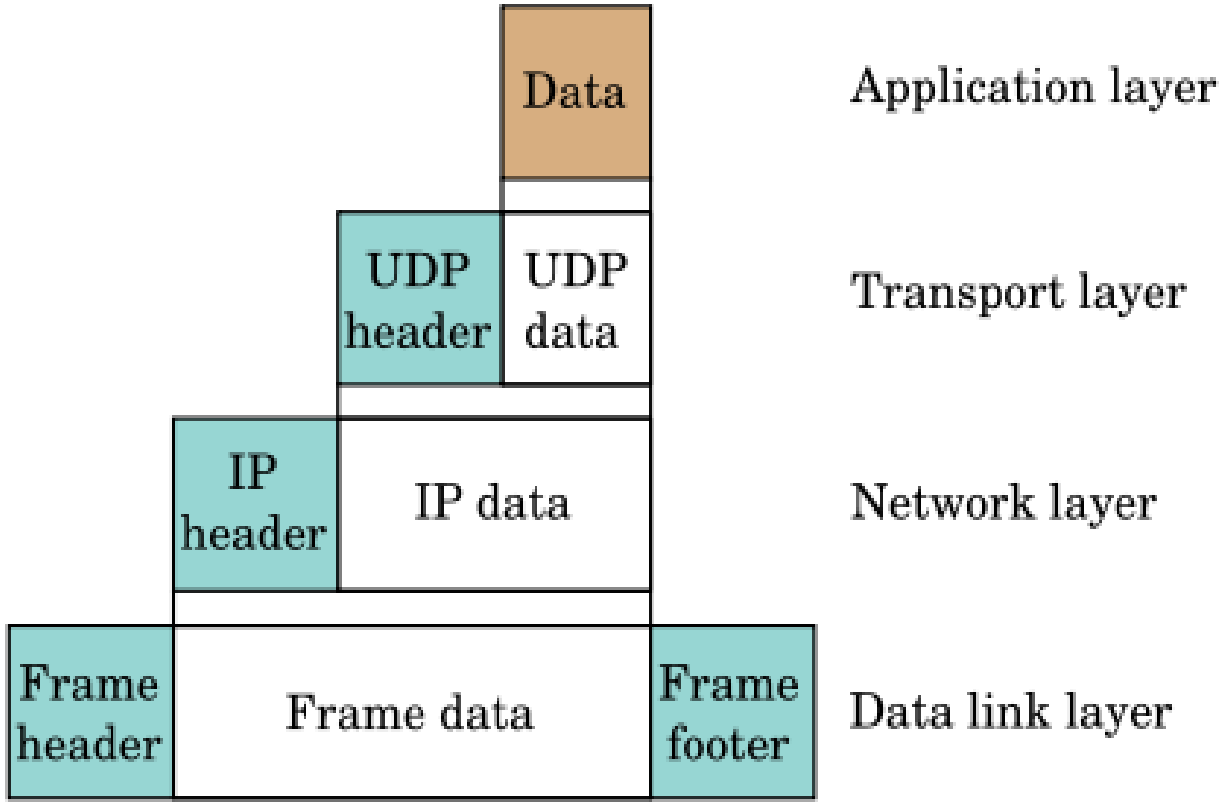


DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

Virtual private network

Encapsulamento

- Encapsulamento



UNIVERSIDADE PORTUCALENSE

Virtual private network

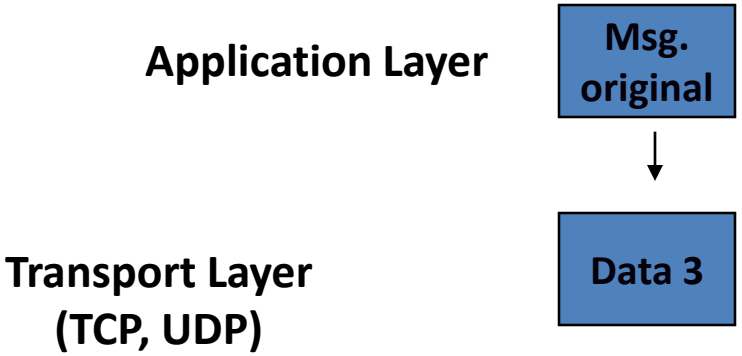
Encapsulamento

Application Layer **Msg. original**

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

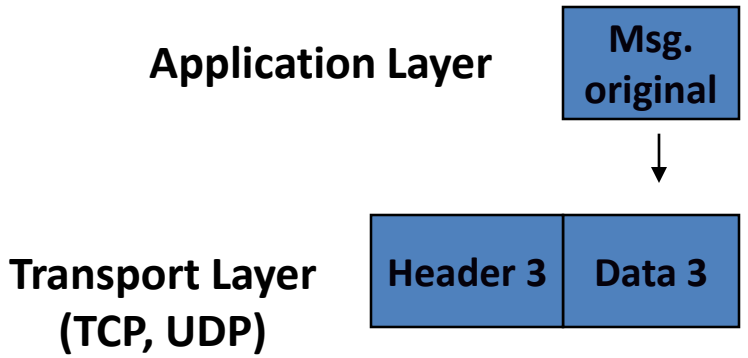
Virtual private network

Encapsulamento



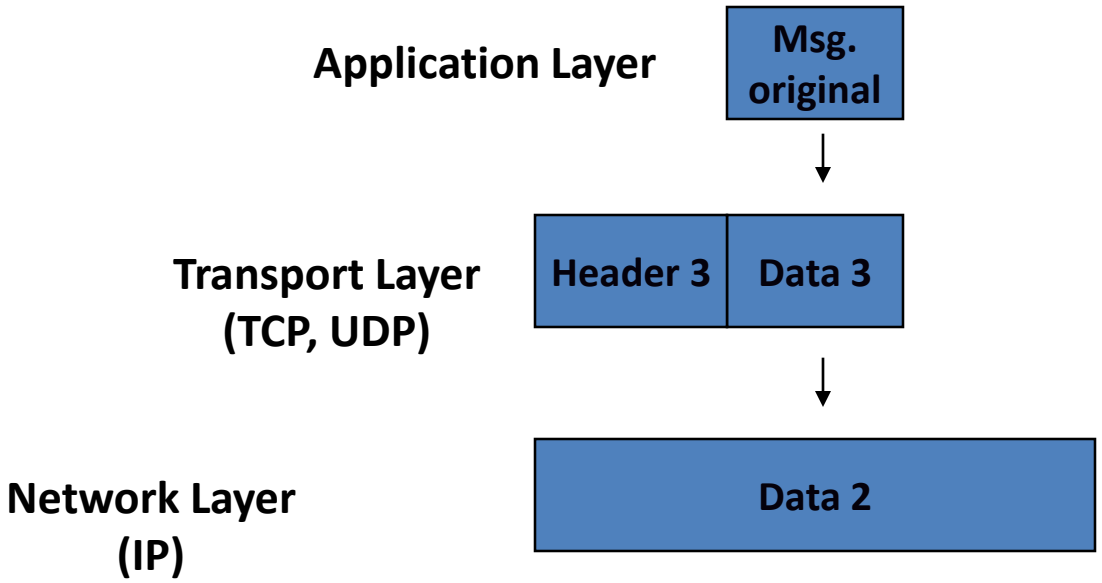
Virtual private network

Encapsulamento



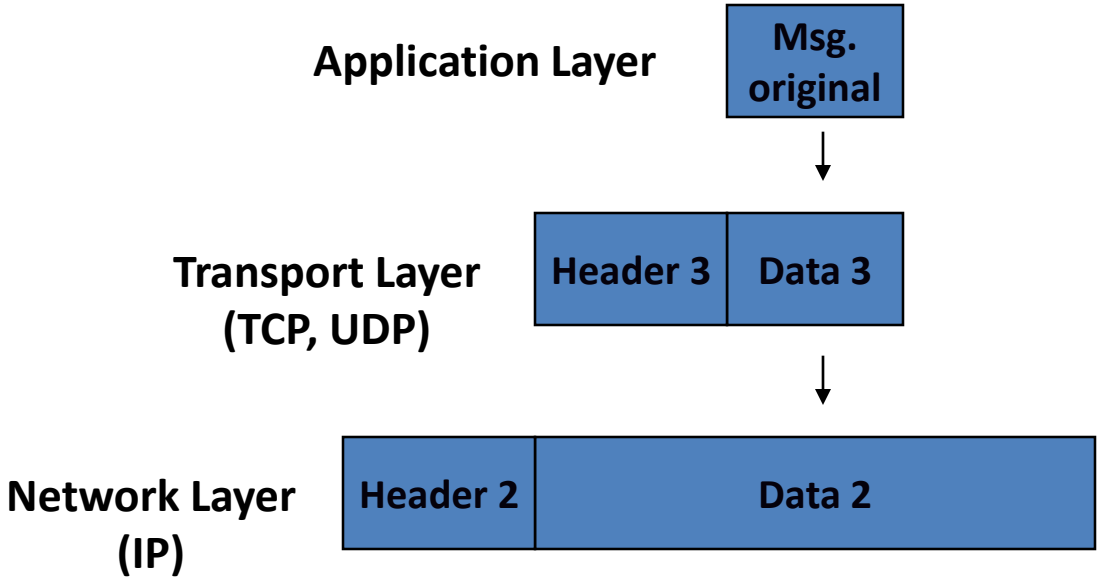
Virtual private network

Encapsulamento



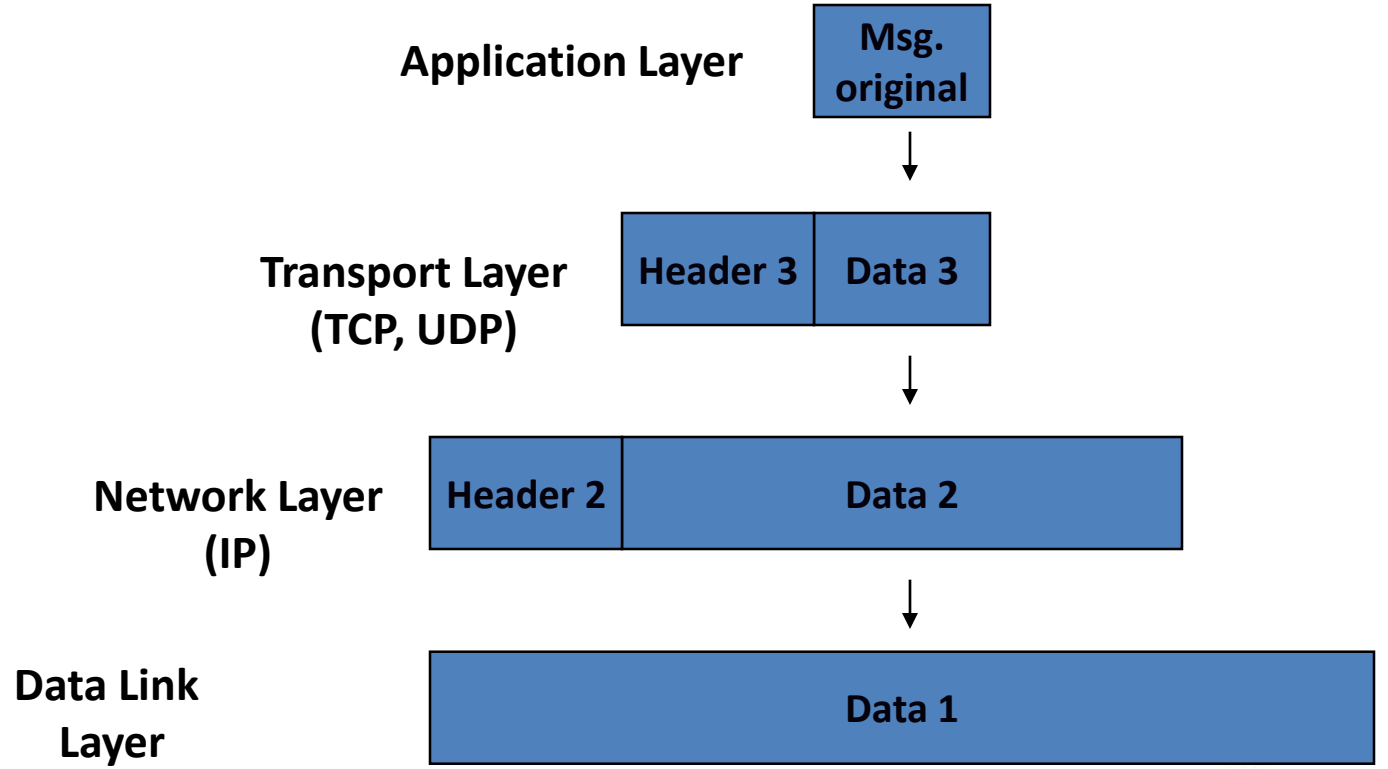
Virtual private network

Encapsulamento



Virtual private network

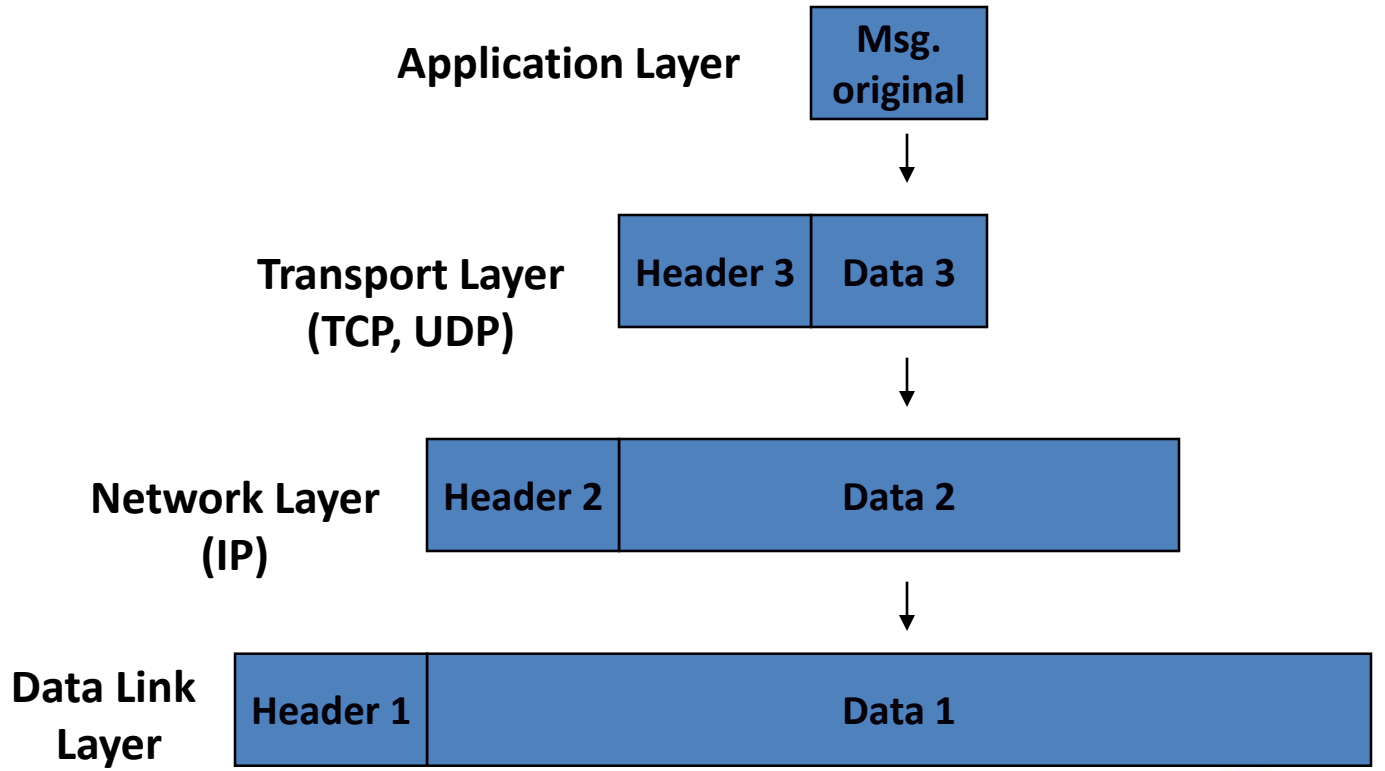
Encapsulamento



UNIVERSIDADE PORTUCALENSE

Virtual private network

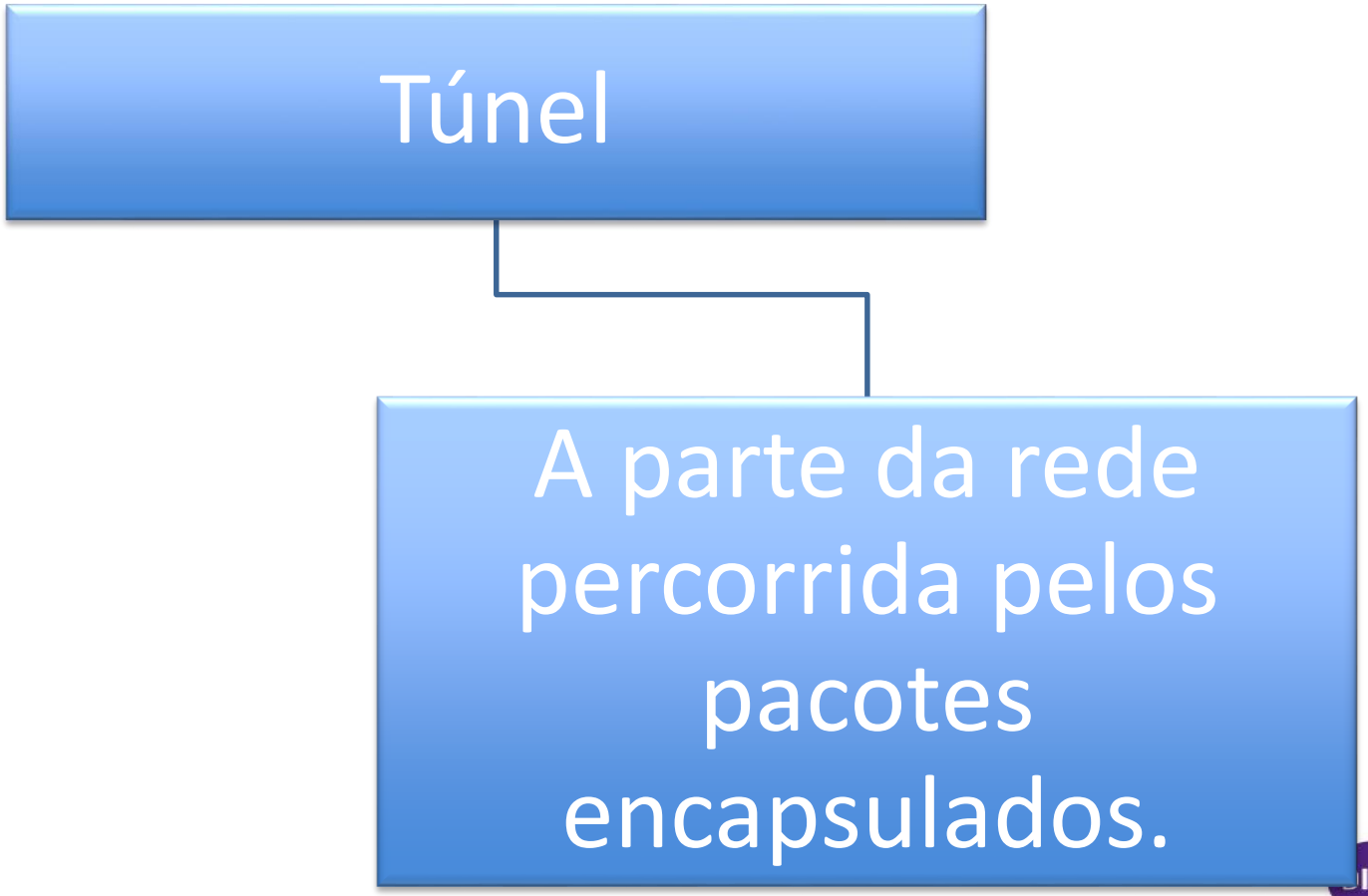
Encapsulamento



UNIVERSIDADE PORTUCALENSE

Virtual private network

Túnel



DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Túnel

- Tunelamento
  - Consiste em encapsular um protocolo dentro de outro.
- Protocolo de tunelamento
  - O protocolo de tunelamento encapsula o protocolo que será transportado, e o cabeçalho do protocolo que encapsulou vai fornecer o destino do pacote do protocolo transportado.

UNIVERSIDADE PORTUCALENSE

Virtual private network

Túnel – tipos de túnel

Voluntário

- Pedido VPN é iniciada pelo cliente
- O cliente continua a ser o ponto final

Obrigatório

- O servidor de VPN cria um túnel de acesso obrigatório para o cliente
- Neste caso, o servidor de acesso dial-up entre o computador do utilizador e o servidor de encapsulamento é o ponto de extremidade do túnel, que actua como um cliente

UNIVERSIDADE PORTUCALENSE

Virtual private network

VPN

O conceito de VPN surgiu para suprir a necessida de de utilizar redes de comunicação não confiáveis (por exemplo, a Internet) para transferir informações de forma segura.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

O que é uma VPN

- Virtual Private Network
  - Conexão segura e privada através de uma rede pública
  - Criptografia e protocolos de encapsulamento
  - Necessita de pontos de envio e receção configurados
  - Permite aos utilizadores o acesso a recursos privados de rede
  - Vários tipos de VPN

UNIVERSIDADE PORTUCALENSE

Virtual private network

O que é uma VPN

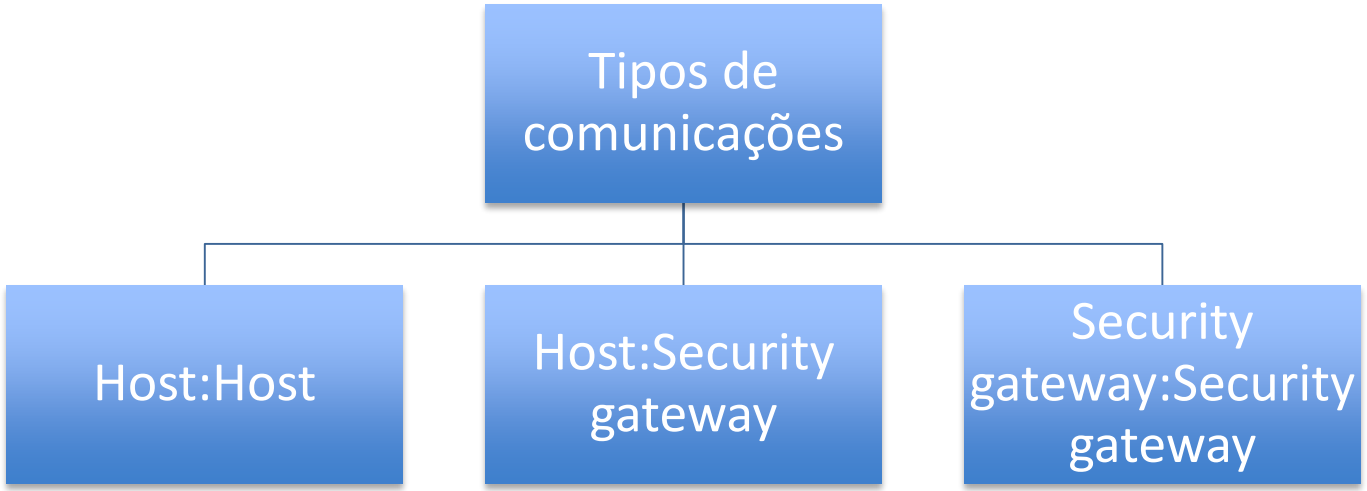
- Acesso remoto via Internet.
- Conexão de LANs via Internet.
- Conexão de computadores numa Intranet.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

O que é uma VPN



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Porquê utilizar VPNS

- Diferentes tipos de ameaças continuam a aumentar – segurança;
- Está disponível e apoiada;
- Permite ligar de qualquer ponto e garantir uma comunicação segura com a instituição;
- Suportada em várias plataformas;
- Estende a rede do campus para utilizadores remotos

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Virtual private network

Se não se utilizarem VPNS

- Vulnerável a vários agentes que ameaçam a segurança
- Quebra de privacidade – packet sniffers, texto em claro
- Falta de integridade – modificação das transações
- Falsificação de identidade – “imitações”
- Difícil de segurar

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN

- Autenticação dos utilizadores
- Gestão de endereços
- Encriptação de dados
- Gestão de chaves
- Suporte para vários protocolos

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN – autenticação dos utilizadores

A VPN deve ser capaz de autenticar os utilizadores e permitir só o acesso à rede aos utilizadores autenticados

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN – gestão de endereços

Atribuir endereços a clientes e garantir que os endereços privados são mantidas em sigilo na VPN

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN – encriptação da informação

Encriptar e desencriptar a informação para garantir que terceiros não têm acesso

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN – gestão de chaves

As chaves devem ser geradas e atualizadas para a criptografia no servidor e no cliente

As chaves são necessárias para criptografia

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Requisitos básicos de uma VPN – suporte para vários protocolos

A tecnologia VPN deve suportar protocolos comuns sobre a Internet, como por exemplo IP, IPX etc. ..

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns

- Protocolos de tunelamento
  - **Point-to-Point Tunneling Protocol** (PPTP)
    - Desenhado para conetividade cliente/servidor
    - Ligação ponto a ponto entre dois computadores
    - Layer 2 (somente em redes IP)
    - Da Microsoft
  - **Layer 2 Tunneling Protocol** (L2TP)
    - Combina a funcionalidade de PPTP/L2F ((Layer 2 Forwarding da Cisco)
    - da IETF (Internet Engineering Task Force)
    - Funciona sobre vários protocolos e não apenas IP
  - **GRE (Generic Routing Encapsulation)**
    - da Cisco.

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns - GRE

- Os túneis criados a partir do protocolo GRE (Generic Routing Protocol) são configurados entre os routers fonte e destino, respetivamente de chegada e saída dos pacotes de dados;

- Os pacotes, a serem enviados através do túnel, são encapsulados num pacote GRE que contém um cabeçalho onde existe o endereço do roteador de destino.

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns - GRE

- Os túneis implementados a partir do protocolo GRE são utilizados na interligação de redes LAN-to-LAN
- Ao chegarem no roteador de destino, os pacotes são descapsulados (retirados os cabeçalhos GRE) e seguem até ao destino determinado pelo endereço de seu cabeçalho original.
- GRE foi desenhado para ser “**stateless**” (trata cada pedido como uma transação independente, isto é sem relação com pedidos anteriores). Um ponto terminal não monitora o estado do outro ponto;

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns - PPP

- **PPTP** da **Microsoft** permite que pacotes de redes locais (como IP, IPX e NetBEUI), sejam encriptados e encapsulados para serem enviados através de **redes IP privadas** ou **públicas como a Internet**.

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns – L2TP

- No momento da ligação (entre o utilizador remoto e o provedor de acesso) e após a devida autenticação e configuração, é estabelecido um túnel até um ponto de terminação (um router, por exemplo), onde a conexão PPP é encerrada.

UNIVERSIDADE PORTUCALENSE

Virtual private network

Protocolos mais comuns

- Internet Protocol Security (IPSec)
- Secure Sockets Layer (SSL)
- Microsoft Point-to-Point Encryption (MPPE)
- Extensible Authentication Protocol (EAP)
- Remote Authentication Dial-in User Service (RADIUS)

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec – o IP não é um protocolo seguro

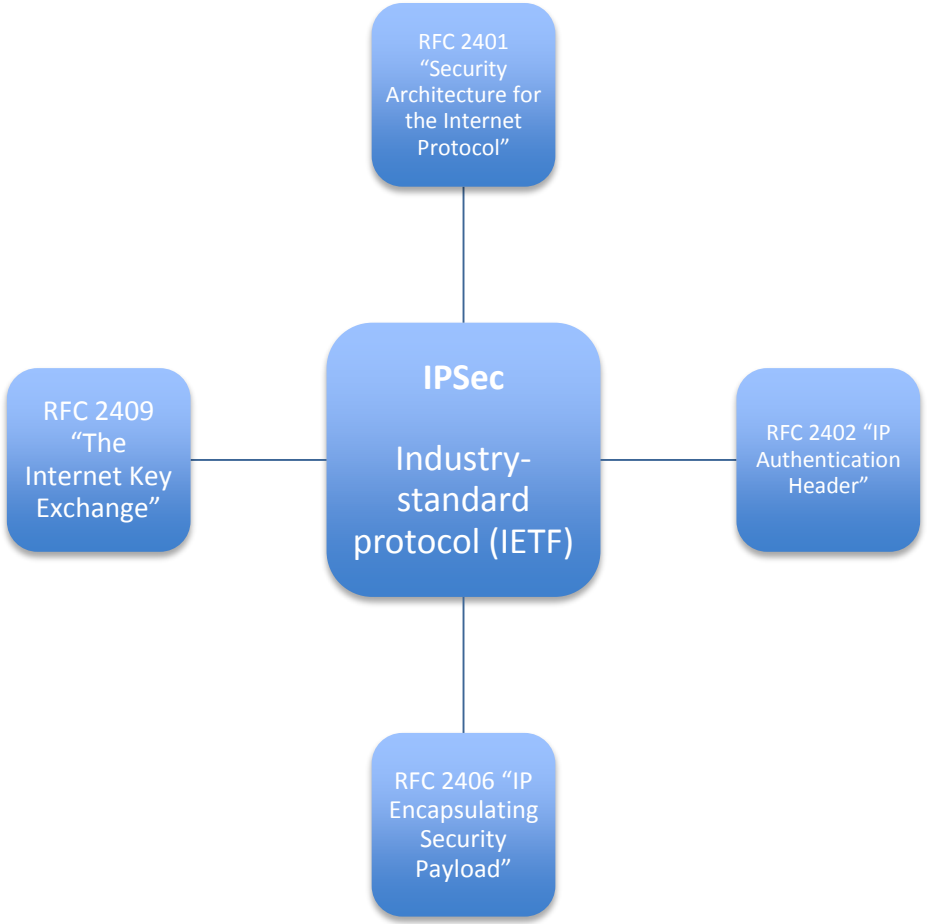
- **Protocolo IP foi concebido nos anos 70 e inicio de 80**
- **Parte do Projeto DARPA Internet**
  - **Rede muito pequena**
  - **Todos os hosts são conhecidos!**
  - **Assim como os utilizadores!**
  - **Portanto, a segurança não foi um problema.**

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec



UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

- Fornece um mecanismo para transmissão segura de dados em redes IP
- Garante a confidencialidade, integridade, autenticidade e não-repudiação de dados
- Trabalha na camada de rede (network layer)
- Muitos componentes - bastante complexo
- Pode ser usado para escalar desde pequenas a grandes redes

UNIVERSIDADE PORTUCALENSE

Virtual private network

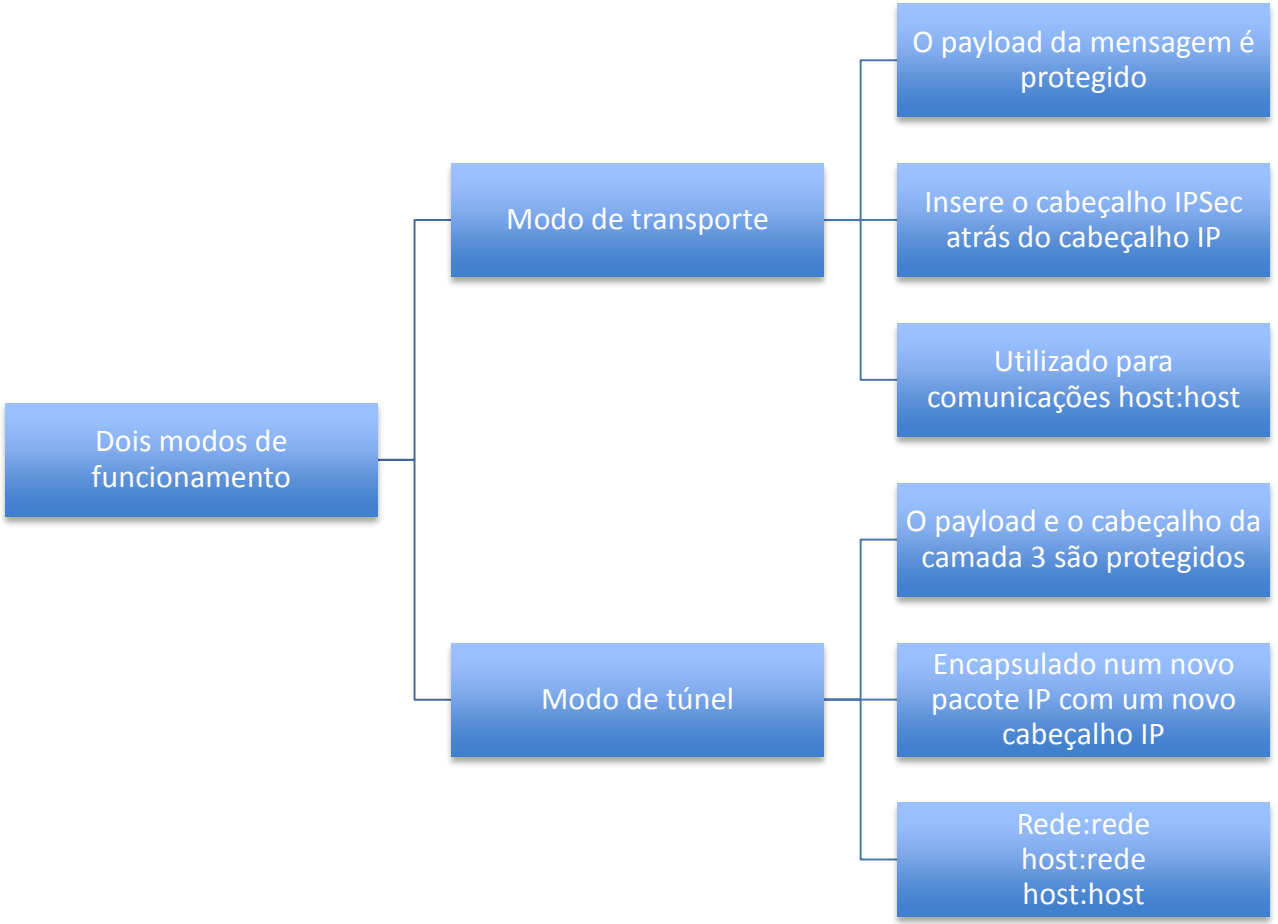
IPSec

- Implementa protocolos básicos de segurança
  - **Authentication Header** (**AH**)
    - Fornece autenticação da sessão
    - Fornece integridade
  - **Encapsulating Security Payload** (**ESP**)
    - Fornece a mesma segurança que o AH
    - Adiciona confidencialidade recorrendo à encriptação
    - Mais frequentemente utilizado em VPN
  - **ISAKMP** - *Internet Security Association and Key Management Protocol*.

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

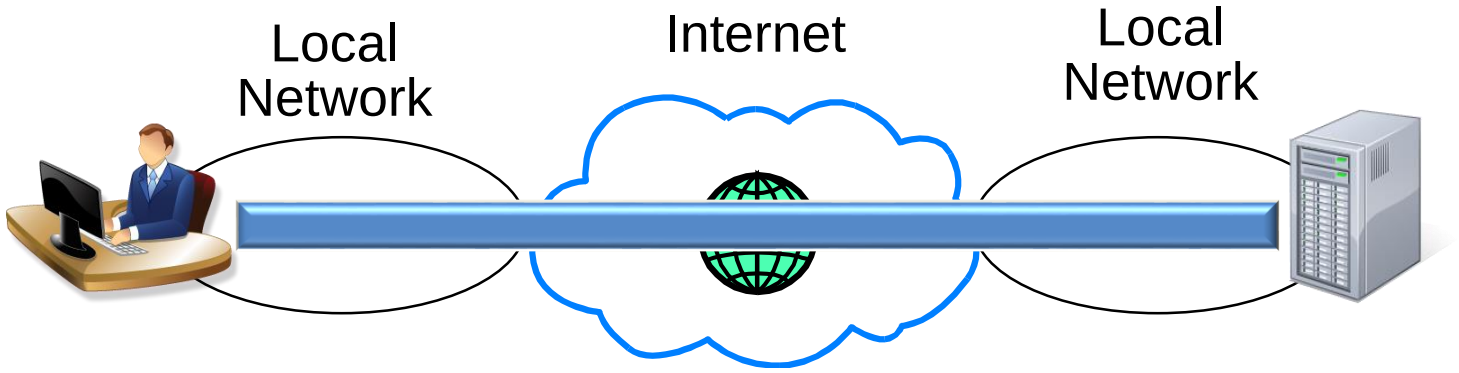


UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

Transport mode



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

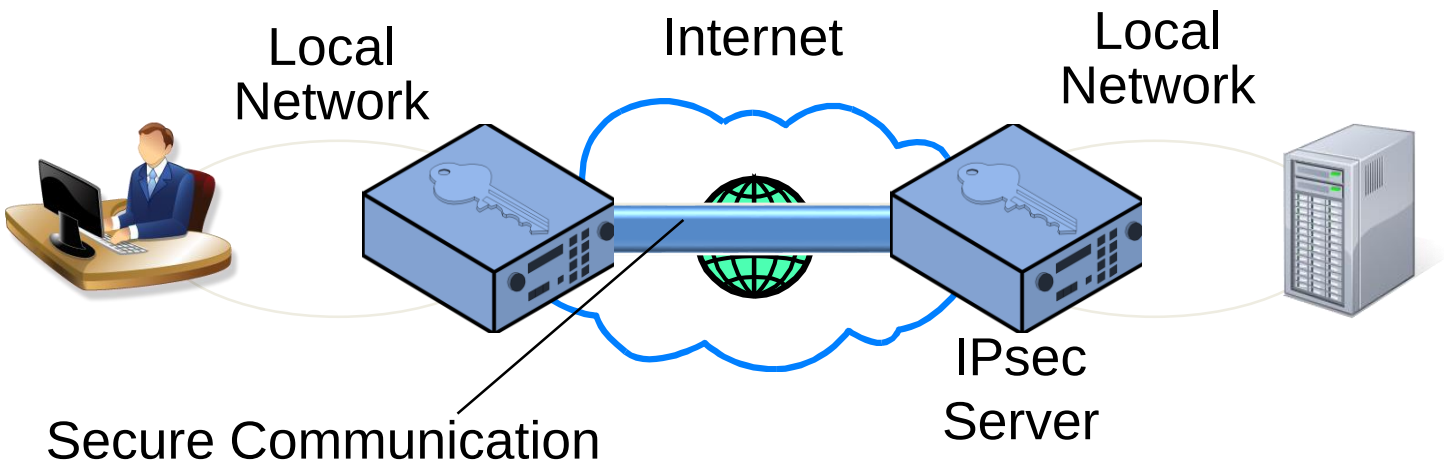
Secure Communication

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

Tunnel mode



UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

- Modo de transporte (Transport Mode)
  - Adiciona, depois do cabeçalho IP, um cabeçalho de segurança ao pacote IP;
  - Endereços de origem e destino dos podem ser aprendidos por terceiros;
  - Apenas o campo de dados original é protegido

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

- Modo túnel (Tunnel Mode)
  - Adiciona um cabeçalho de segurança antes do cabeçalho IP original;
  - São conhecidos os endereços dos servidores de origem e destino e não os dos hosts em comunicação;
  - Protege o campo de dados e o campo de IP original.

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec

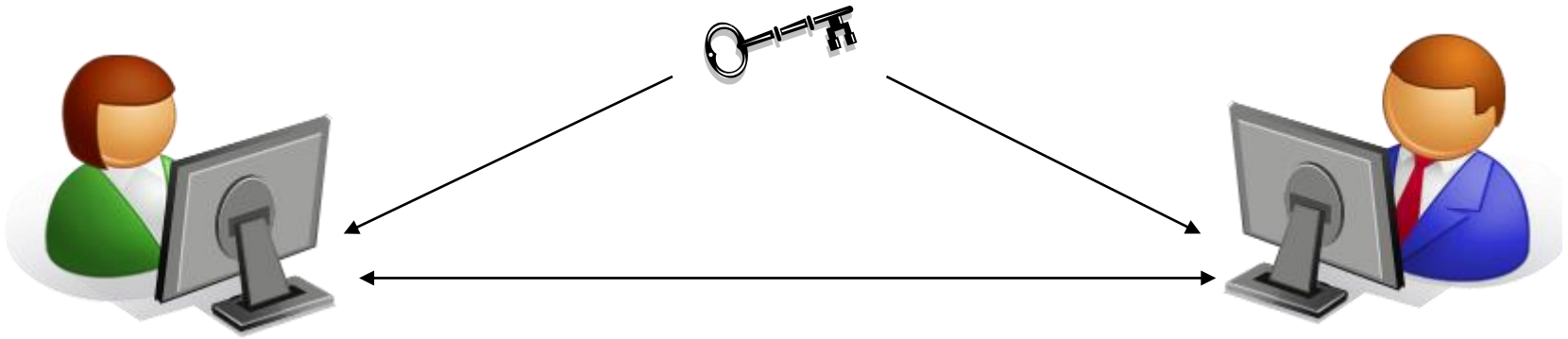
- Internet Key Exchange (IKE)
  - Troca e negociação de políticas de segurança;
  - Estabelecer sessões de segurança;
    - Identificadas como Associações de Segurança;
  - Troca de chaves;
  - Gestão de chaves;
  - Pode ser usado fora IPsec.

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec – O algoritmo de Diffie-Hellman (DH)

- O algoritmo Diffie-Hellman (DH)
  - Troca de chaves através de uma rede insegura



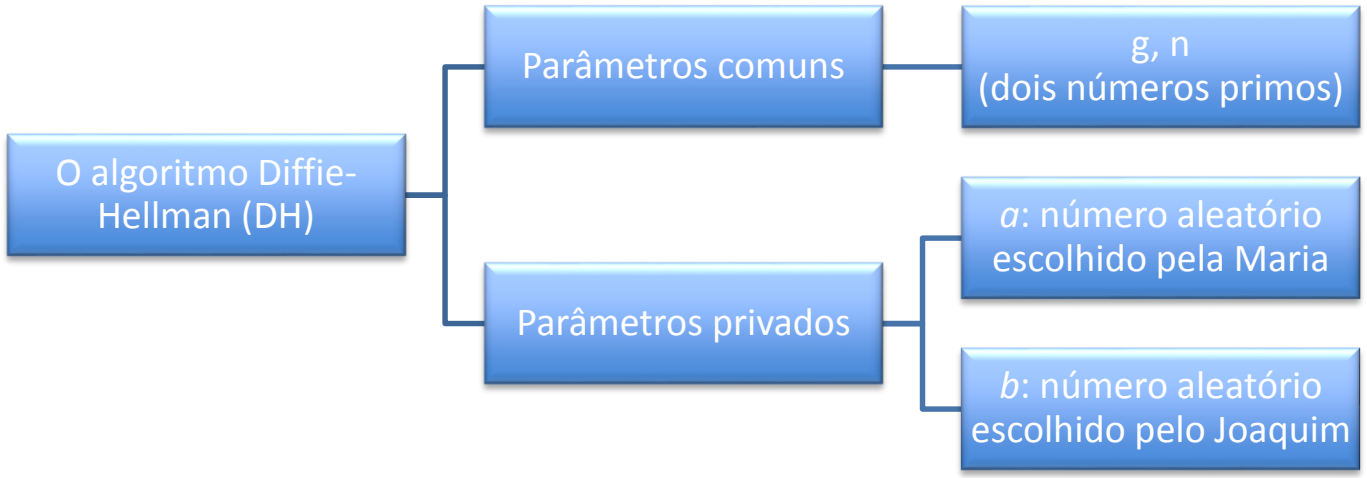
Maria

Joaquim

UNIVERSIDADE PORTUCALENSE

Virtual private network

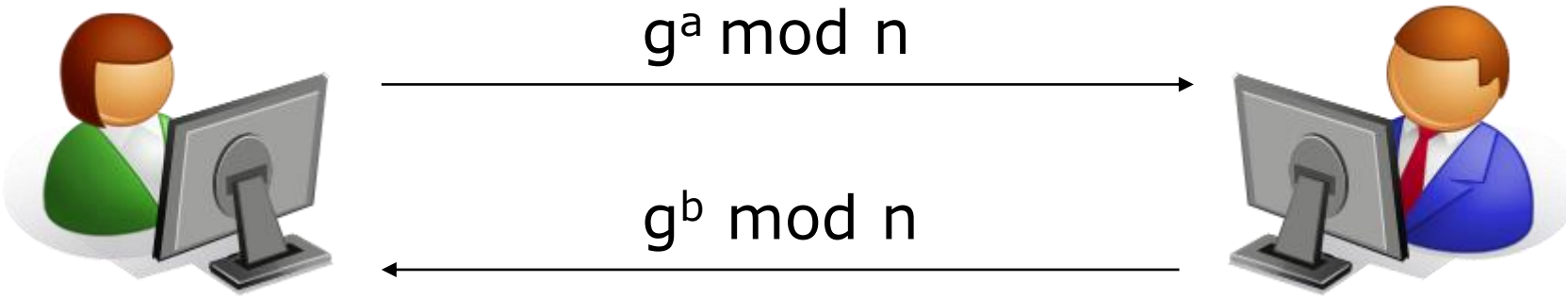
IPSec – O algoritmo de Diffie-Hellman (DH)



UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec – O algoritmo de Diffie-Hellman (DH)



Maria calcula
$((g^b \bmod n)^a \bmod n)$

Resultado $(g^{ab} \bmod n)$

Joaquim calcula
$((g^a \bmod n)^b \bmod n)$

Resultado $(g^{ab} \bmod n)$

Chave da sessão = $g^{ab} \bmod n$

DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec – Security associations

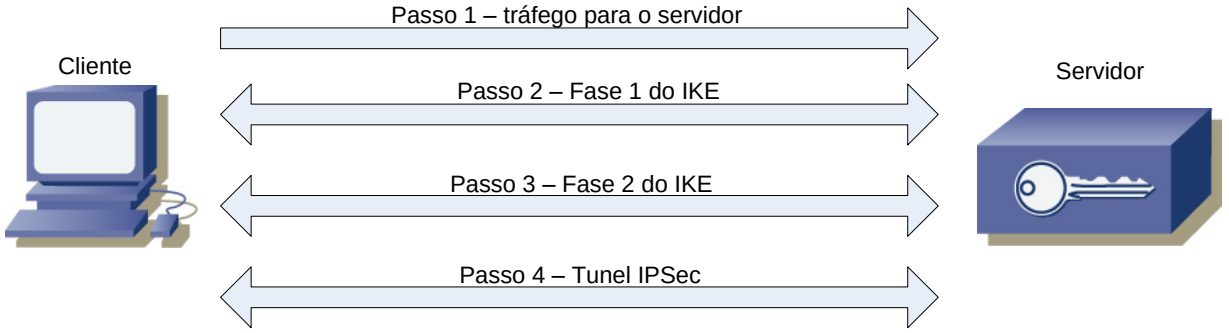
Security Associations (SA)

- Uma relação unidirecional entre emissor e recetor que proporciona segurança para o fluxo de tráfego
- Identificada por três parâmetros:
  - Security Parameters Index (SPI)
  - IP Destination Address
  - Security Protocol Identifier, AH ou ESP
- Tem outros parâmetros
  - Nº da seq. AH info, lifetime etc
- Existe uma base de dados que define os parâmetros associados com cada SA

UNIVERSIDADE PORTUCALENSE

Virtual private network

IPSec



- **Passo 1** (O processo IPSec é iniciado) – O tráfego para ser encriptado de acordo com o especificado pela política de segurança IPSec inicia o processo IKE
- **Passo 2** (Fase 1 do IKE) – O IKE autentica as pontas IPSec e negoceia IKE SAs (associações de segurança)
- **Passo 3** (Fase 2 do IKE) – O IKE negoceia os parâmetros SA do IPSec e estabelece correspondência IPSec SAs nas pontas
- **Passo 4** (Transferência de dados) – O túnel é estabelecido e a informação é transferida em segurança
- **Passo 5** (terminação do túnel) – As SAs são terminadas através da eliminação ou time-out.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Virtual private network

Conclusão

- VPN é uma alternativa segura para uma rede pública insegura;
- Utiliza protocolos standard;
- Tecnologia com muito suporte;
- Estende a rede do Campus para utilizadores remotos;
- Fácil de garantir a segurança dos recursos;