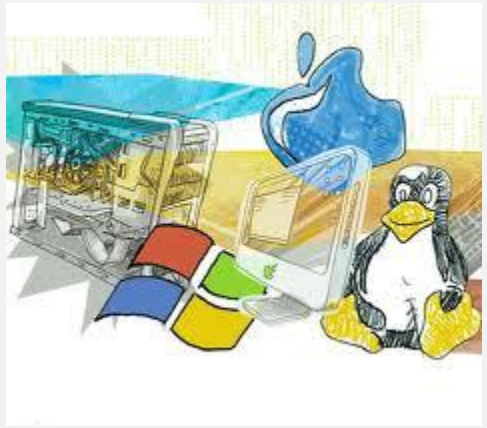
Serviços de Rede 1

2019-2020

Instituto Politécnico de Coimbra

Departamento de Engenharia Informática



Serviços de Rede 1

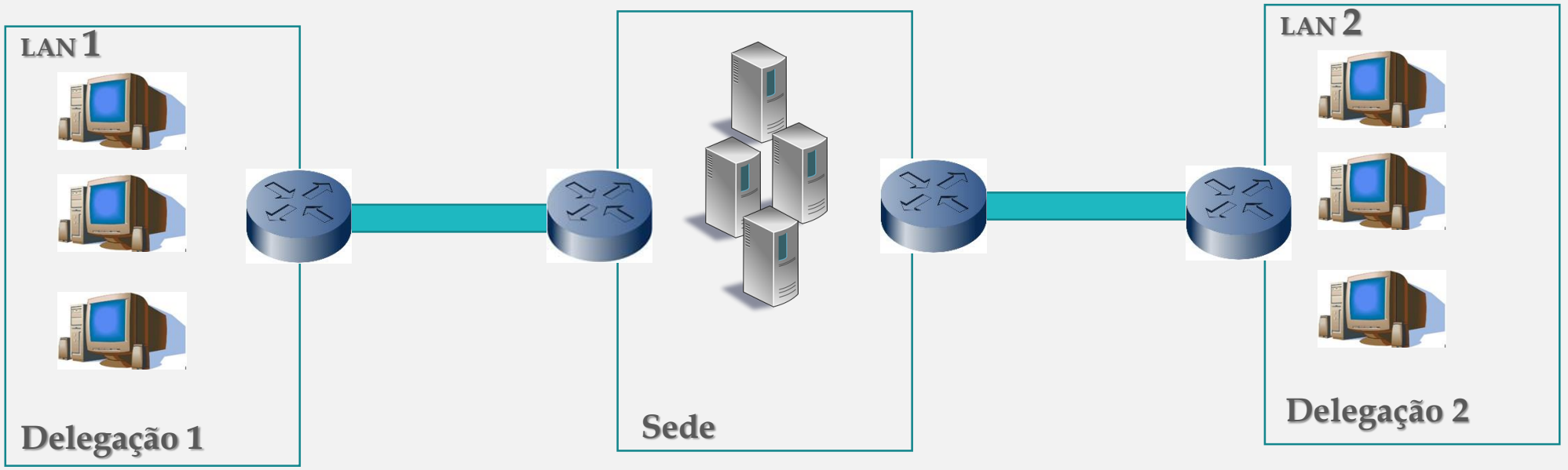
Virtual Private Network - VPN

VPN

- Como nenhum homem é uma ilha e o mundo está a ficar mais pequeno, é previsível que necessite de se ligar a computadores remotos usando para isso a sua rede e mais qualquer coisa…
- A razão de ter acesso remoto:
  - Solução para ligar redes locais de outras empresas do mesmo grupo empresarial.
  - Solução para acesso remoto a utilizadores deslocalizados.
  - Solução para encriptação do trafego numa ligação publica
  - Solução global para acesso à Internet.

Introdução

- No passado a única possibilidade de dar acesso remoto ou interligar redes locais era muito caro porque obrigava a existência de ligações ponto-a-ponto privadas alugadas aos operadores de telecomunicações.



Introdução

- O conceito surgiu a partir da necessidade de utilizar redes de comunicação não confiáveis (logo não seguras) para a transmissão de dados privados de uma forma segura.
- ***V****irtual* ***P****rivate* ***N****etwork - VPN*
  - *Network* – porque pelo menos temos uma ligação entre duas máquinas.
  - *Virtual* – porque a ligação é feita sem a utilização de um meio físico dedicado.
  - *Private* – porque estamos a ceder a recursos privados
- Uma VPN é assim uma extensão virtual de uma rede privada (por exemplo a LAN).
- As VPNs permitem assim dar os mesmos recursos e vantagens comunicacionais das redes tradicionais mas sem a necessidade de instalação, configuração e manutenção de equipamentos de conexão.

Introdução

- Com a Internet foi possível implementar este tipo de ligações a baixo custo porque é oferecido aos seus utilizadores remotas as mesmas possibilidades/funcionalidades que as linhas dedicadas privadas, utilizando "como portadoras" as linhas públicas de telecomunicações que suportam a ligação à Internet.
- A ligação pode ser efetuada, de modo seguro, através de redes partilhadas ou públicas (utilizando por exemplo o acesso Internet da organização).

Introdução

- **Permite:**
  - o envio de dados entre um computador e a rede interna de modo similar a uma ligação privada ponto a ponto.
  - a ligação entre duas redes locais utilizando a rede publica de comunicações.
- A ligação é efetuada através da criação de um túnel encriptado sobre a rede pública de comunicações para garantir mecanismos de segurança e confidencialidade da informação.

Introdução

- Benefícios:
  - **Segurança** com o controlo dos acessos não autorizados a recursos e a dados.
  - **Redução de custos** já que permite eliminar a necessidade de aquisição/aluguer de linhas dedicadas, utilizando a(s) ligação (ões) à Internet.
  - **Escalabilidade** permitindo que a rede possa crescer sem a necessidade de instalação de nova infraestrutura.

Introdução

- Desvantagens
  - Na sua implementação e manutenção necessitam de uma compreensão dos problemas de segurança da rede pública e de precauções próprias com o processo de entrega de dados.
  - A disponibilidade e performance de uma VPN (particularmente sobre a Internet) de uma organização, depende de fatores que estão fora do seu controle.
  - As tecnologias VPN de vendedores diferentes podem não funcionar bem em conjunto devido a normas proprietárias.
  - Precisam de acomodar outros protocolos além do IP o que implica maior processamento e complexidade protocolar.

Introdução

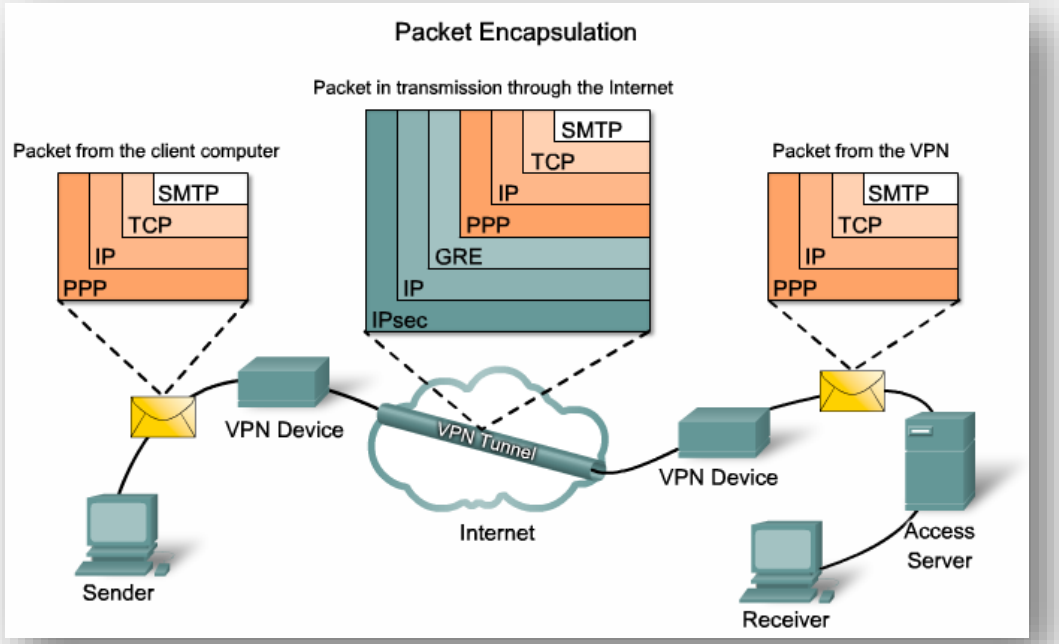
- As VPN devem garantir 4 pontos chave:
  - Autenticação
    - Garantir que a informação recebida foi enviada pelo verdadeiro emissor.
  - Controlo de acesso
    - Garantir que só os utilizadores autorizados acedem aos recursos.
  - Confidencialidade
    - Garantir que apenas o emissor e recetor têm acesso aos dados que são transmitidos.
  - Integridade
    - Garantir que os dados não são alterados/adulterados no processo de transporte.

Introdução

- Na implementação de uma VPN existem três conceitos fundamentais:
  - Encapsulamento
  - Túnel (*Tunneling)*
  - Encriptação
- Para que seja emulada uma ligação *ponto a ponto* os dados são encriptados e encapsulados num pacote com informação suficiente para que possa atingir o seu destino de forma **segura** e **confiável** navegando num túnel próprio.

Encapsulamento

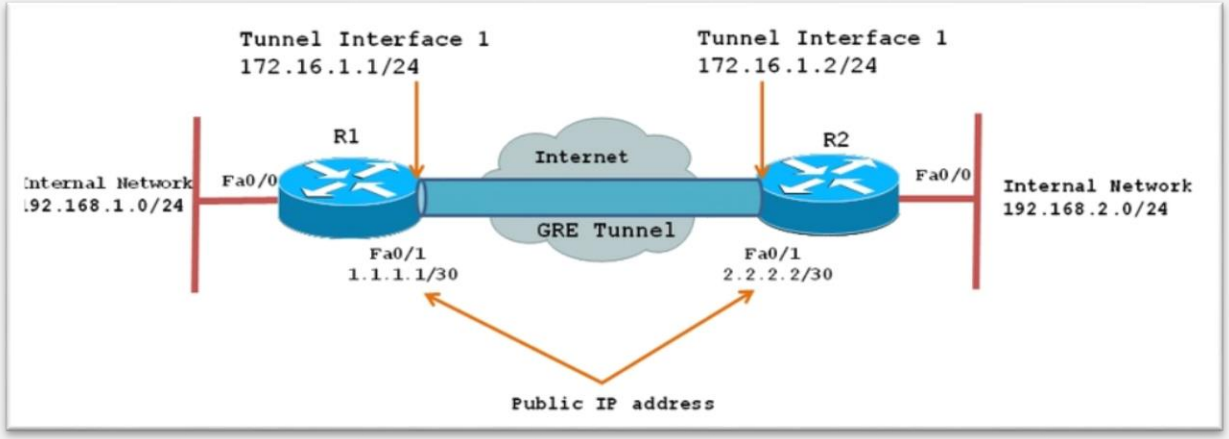
- Em redes de dados, o conceito de encapsulamento é a inclusão de dados de um protocolo de uma camada superior dentro de um protocolo de uma camada inferior.



Fonte: www.cisco.com

Túnel

- A parte da conexão em que os dados transitam encriptados chama-se **túnel**.
- Túnel é a denominação do caminho lógico percorrido pelos pacotes encapsulados.
- A rede VPN poder ser construída sobre uma rede pública (Internet) ou uma rede privada.



Fonte: www.cisco.com

Encriptação

- Para ter uma VPN segura necessita de proceder à encriptação dos dados antes dos enviar pelo túnel.
- Encriptação é o processo de transformar informação (referida como texto original) usando um algoritmo (chamado cifra) de modo a impossibilitar a sua leitura a todos exceto aqueles que possuam uma informação particular, geralmente referida como chave.
- Mesmo que os pacotes sejam intercetados, torna-se praticamente impossível efetuar a sua desencriptação caso não se possuam as 'chaves' adequadas.

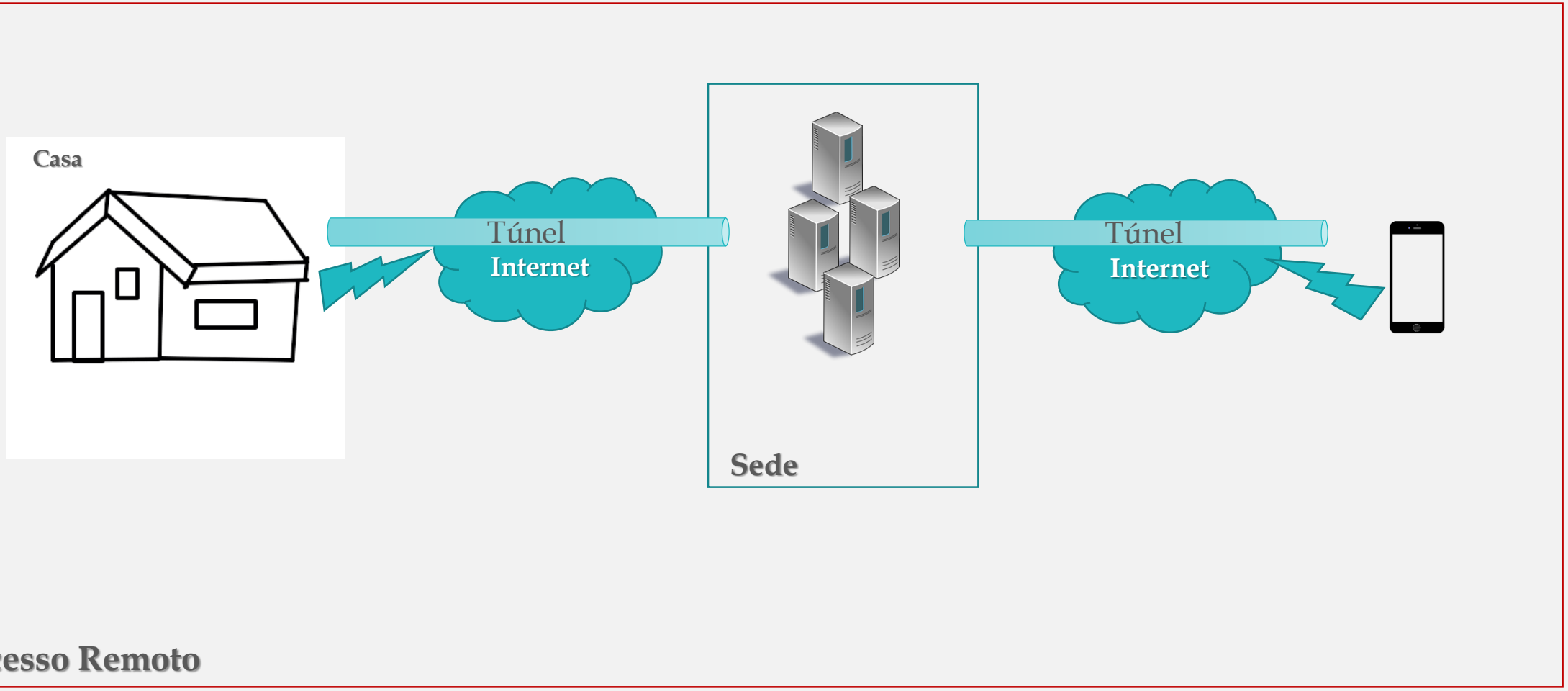
Implementações

- Podemos ter diferentes implementações da VPN, consoante o tipo de ligação, tecnologia, meios ligados e infraestrutura de telecomunicações utilizada.
  - *Demand-dial VPN Networking*
  - *Always-on VPN Networking*

Demand-dial VPN Networking

- A implementação deste acesso é semelhante a uma conexão *dial-up* entre dois equipamentos em localidades diferentes.
- A diferença é que os pacotes são transferidos por um túnel e não através da simples conexão convencional.
- Por exemplo, um utilizador liga-se a um fornecedor de serviços através da rede publica e através dessa ligação estabelece um túnel com a rede remota, podendo transferir dados com segurança.
- Pode utilizar a Internet ou outra ligação para proporcionar o acesso dos postos de trabalho à rede.
- Usado sobretudo para fornecer acesso remoto aos trabalhadores.

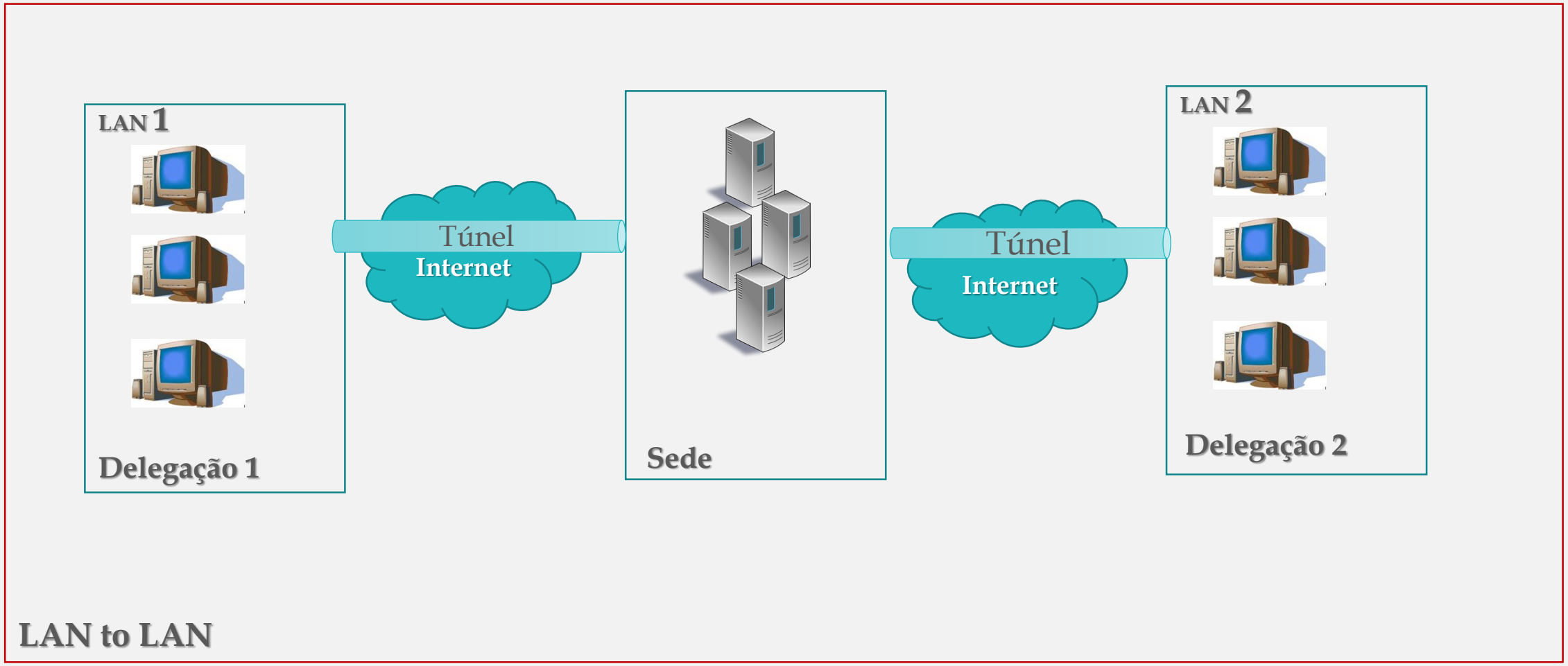
Introdução



Always-on VPN Networking

- O acesso por link dedicado, interligando dois pontos de uma rede, é conhecido como ligação LAN-to-LAN ou *Always-on VPN Networking*.
- O link dedicado as redes são interligadas por túneis que passam pelo *backbone* de rede pública.
- Habitualmente utilizado para ligação de delegações de empresas à sua sede.

Introdução

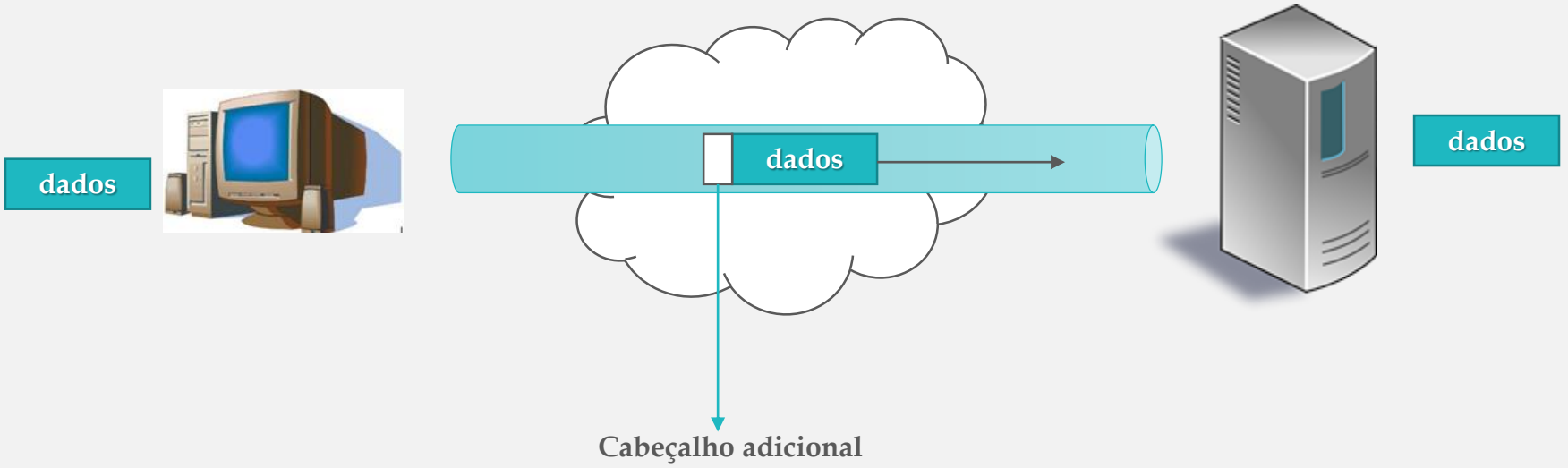

LAN 1
Delegação 1
Túnel
Internet
Sede
Túnel
Internet
LAN 2
Delegação 2
LAN to LAN

Componentes básicos

- **Autenticação de utilizadores**
  - Verificação da identidade dos utilizadores, autorização de acessos e sistema de logs
- **Gestão de endereços**
  - Atribuição de endereços da rede ao cliente remoto (IP, gateway, dns server,...)
- **Encriptação de dados**
  - Os dados que são enviados através da rede de suporte deverão ser encriptados de modo a garantir a sua confidencialidade
- **Gestão de chaves**
  - Para permitir a encriptação baseado em chaves é necessário fornecer um mecanismo de gestão das chaves – só com este mecanismo é possível efectivar a criação de um túnel

Tunneling

Tunneling



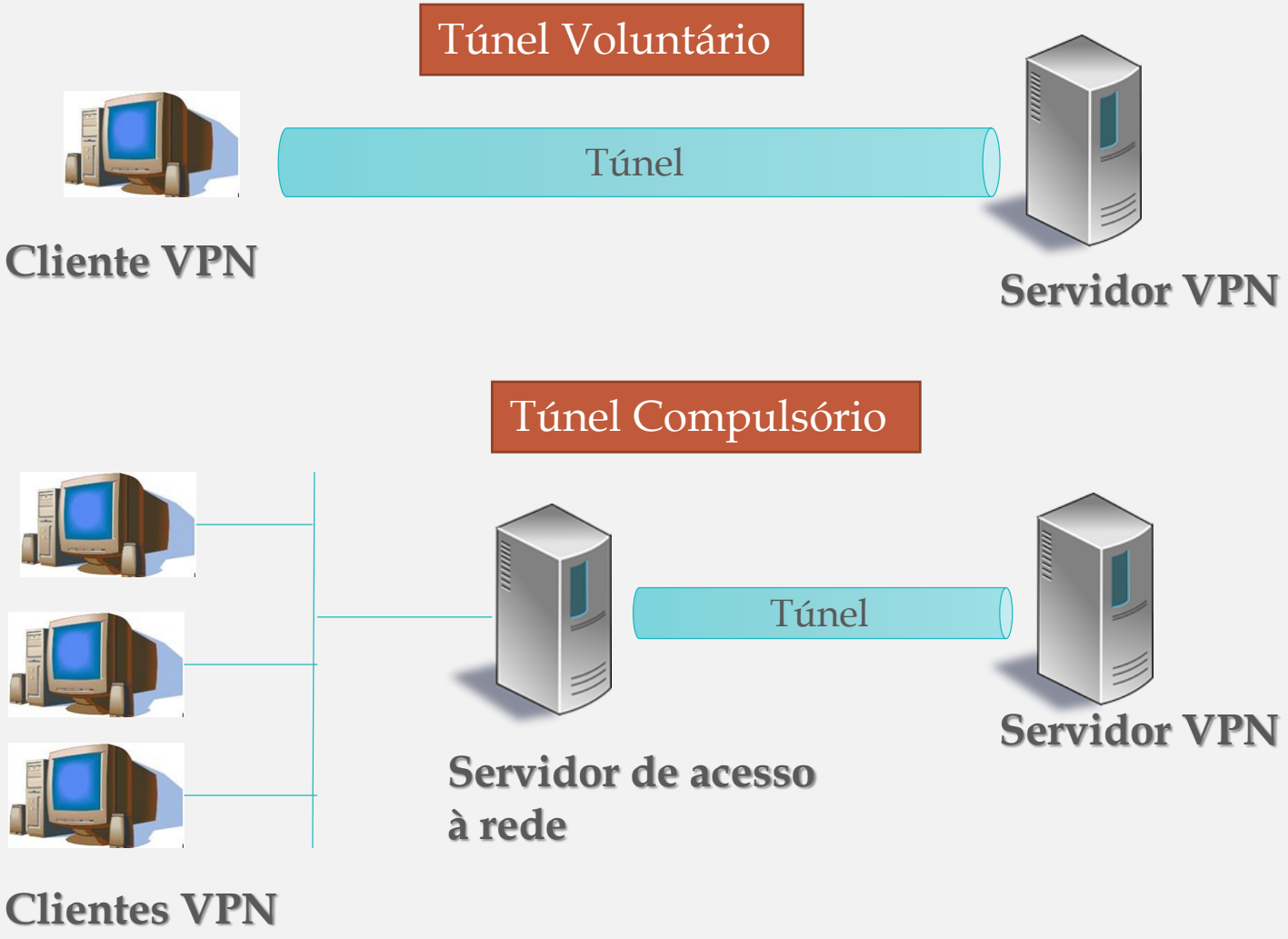
Tunneling

- Método em que se usa a infra-estrutura de rede intermediária, para efectuar a transferência de dados entre duas redes, mas garantindo a privacidade e controlo sobre os dados originais.
- Os dados transmitidos podem corresponder a pacotes ou frames de diferentes protocolos.
- Em vez de serem enviados os pacotes, estes são encriptados e encapsulados num pacote do protocolo de *tunneling* inserindo-lhe ainda um novo cabeçalho (*header*).
- O *header* adicional contém a informação de *routing* necessária para efectuar a entrega.

Tipos de Túneis

- **Túnel Voluntário** - um cliente emite um pedido VPN para configurar e criar um túnel. Neste caso, o computador do utilizador funciona como uma das extremidades do túnel e, também, como cliente do túnel.
- **Túnel Compulsório** - um servidor de acesso *dial* VPN configura e cria um túnel. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do utilizador e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

Tunneling


Túnel Voluntário
Túnel
Cliente VPN
Servidor VPN
Túnel Compulsório
Túnel
Servidor de acesso à rede
Servidor VPN
Clientes VPN

Tunneling

- Para que um túnel seja estabelecido é necessário que o servidor e o cliente utilizem o mesmo protocolo.
- Para o estabelecimento do túnel, são necessárias duas fases:
  - **Estabelecimento do túnel**
    - Negociação de variáveis, endereço, encriptação e compressão.
  - **Transmissão**
    - Encapsulamento e encriptação.
    - Envio.
    - Desencapsulamento e desencriptação.

Tunneling

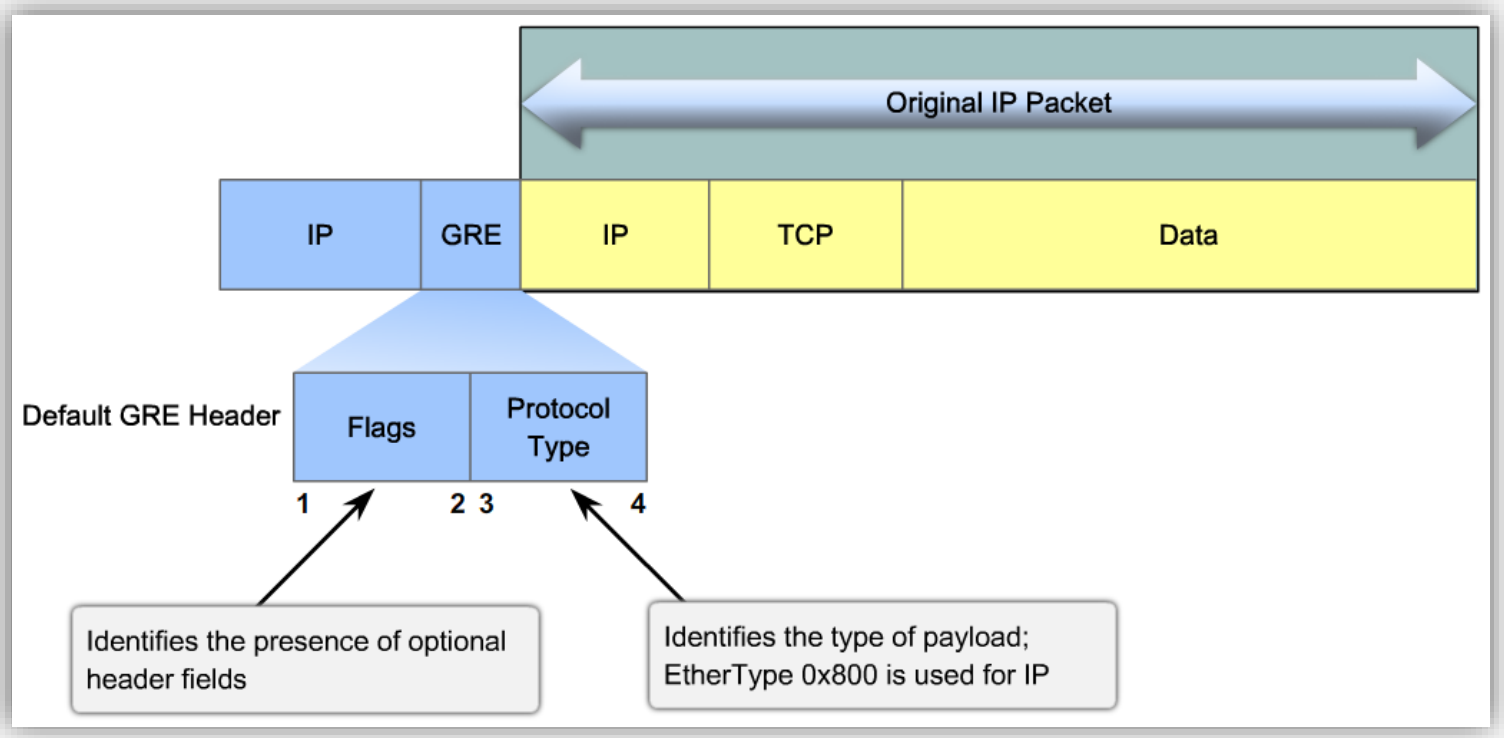
- Podem ser utilizados diferentes protocolos:
  - **GRE** *(**Generic Routing Encapsulation**)* da Cisco.
  - **PPTP** (***Point-to-Point Tunneling Protocol***) da Microsoft.
  - **L2F e L2TP** (***Layer 2 Tunneling Protocol***) da IETF (*Internet Engineering Task Force*).
  - **IPSEC**
  - **Open VPN**
  - **SSL**

GRE - *Generic Routing Encapsulation*

- Protocolo desenvolvido pela Cisco.
- Protocolo descrito pelos RFCs 1702 e 2784.
- O funcionamento deste tipo de túnel é muito simples, e consiste em pegar nos pacotes originas, adicionar o cabeçalho GRE, e enviar ao IP de destino (o endereço do destino é especificado no cabeçalho GRE), quando o pacote encapsulado chega na outra ponta do túnel (IP de destino) é retirado o cabeçalho GRE, sobrando apenas o pacote original, o qual é encaminhado normalmente ao destinatário.
- Suporta múltiplos protocolos.
- Através da introdução de uma cabeçalho adicional é possível a transmissão de múltiplos protocolos no mesmo túnel.
- Suporta *multicast*.

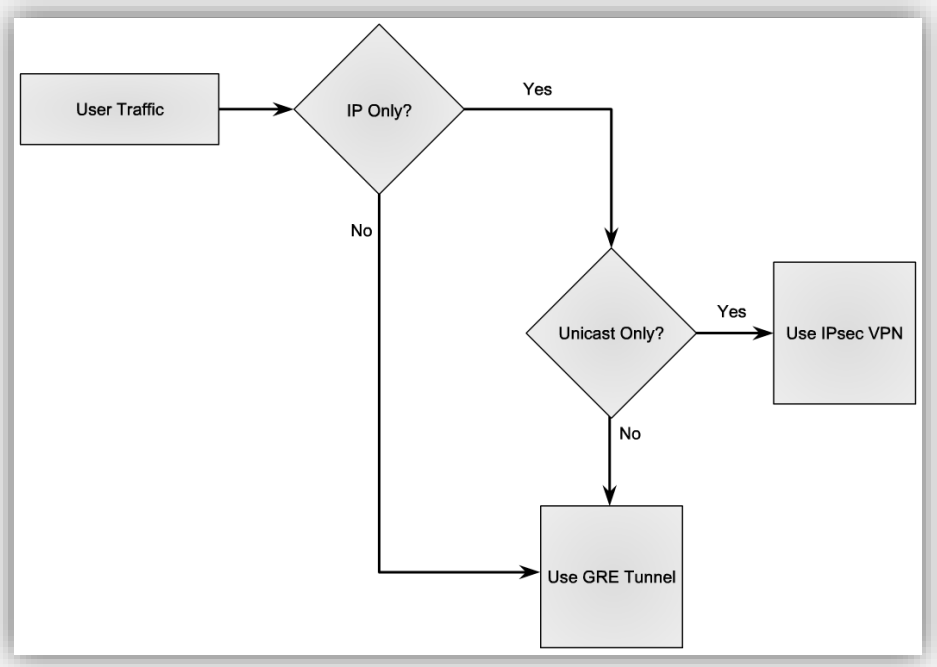
GRE - *Generic Routing Encapsulation*

- Os pacotes IP são encapsulados num pacote GRE
  - *Implica um* payload adicional de, pelo menos, 24 bytes

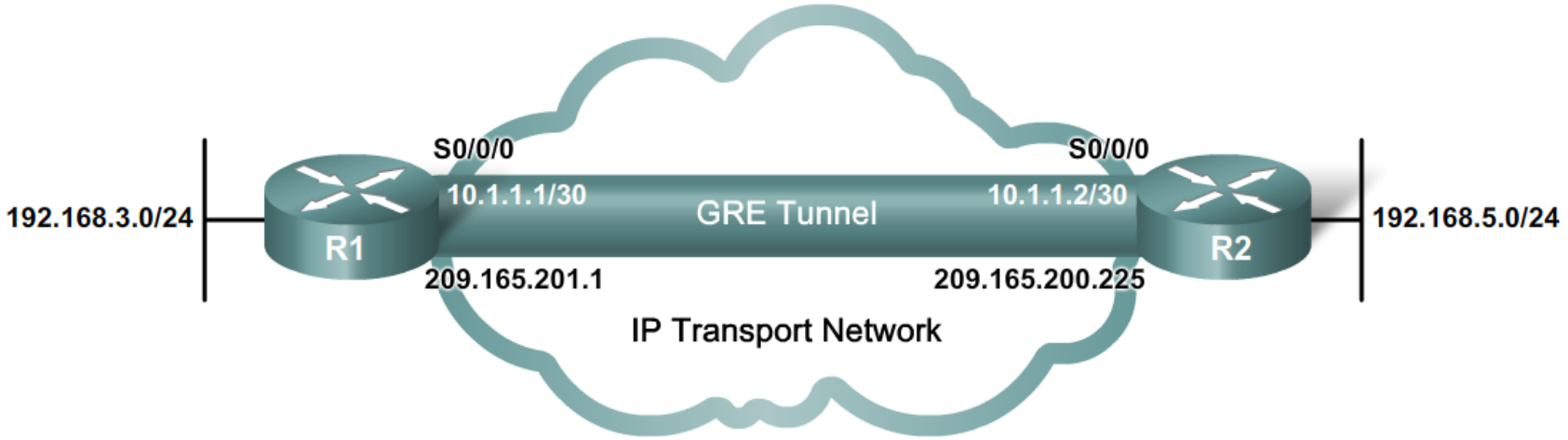


GRE - *Generic Routing Encapsulation*

- Contudo, os túneis GRE não fornecem mecanismos de encriptação de dados.
  - Solução:
    - Recorrer a protocolos específicos que funcionam sobre GRE
    - Recorrer a IPSec



GRE - *Configuração*




```
R1(config)# interface tunnel 0
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# tunnel source serial 0/0/0
R1(config-if)# tunnel destination 209.165.200.225
R1(config-if)# tunnel mode gre ip
R1(config-if)#
```

```
R2(config)# interface tunnel 0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
R2(config-if)# tunnel source serial 0/0/0
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# tunnel mode gre ip
R2(config-if)#
```

GRE tunnel is up and the protocol is up if:

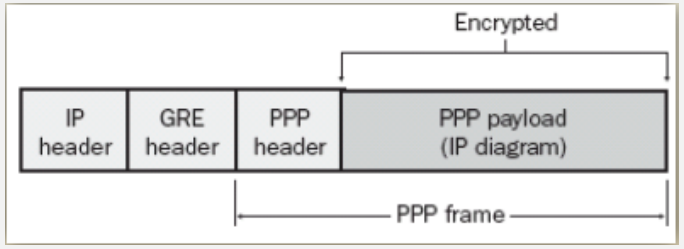
- Tunnel source and destination are configured
- Tunnel destination is in routing table
- GRE keepalives are received (if used)
- GRE is the default tunnel mode

PPTP- Point-to-Point Tunneling Protocol

- Desenvolvido por um consórcio US-Robotics, Microsoft, 3Com, Ascend e ECI.
- Amplamente utilizado em sistemas operativos windows. Contudo, como apresenta alguns problemas de segurança pelo que começou a ser menos utilizado para soluções em que a segurança é um aspeto crítico.
- Utiliza-se quadros PPP (Point-to-Point Protocol), como unidades de troca de informação, encapsulando os pacotes IP.
- Autenticação feita através dos protocolos PAP,CHAP e MS-CHAP.
- Criptografia através do MPPE.

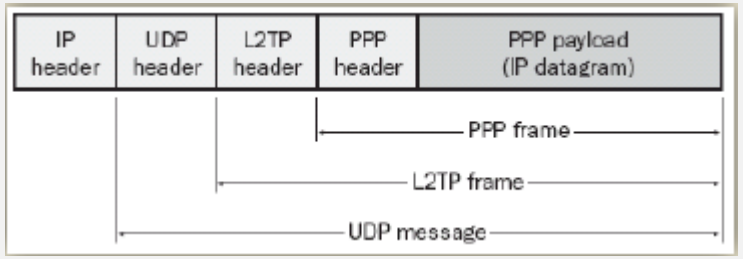
PPTP- Point-to-Point Tunneling Protocol

- Permite que o tráfego sejam criptografados e encapsulados para serem enviados através de redes IP privadas ou públicas como a Internet.
- Principais características:
  - Todo o trafego é enviado pela porta TCP 1723.
  - O túnel é iniciado pelo servidor de acesso.
  - Os túneis são estáticos.
  - Controle está nas mãos do provedor do serviço.
  - A encriptação começa depois da ligação.
  - Requer a autenticação dos utilizadores.
  - Não requer uma infraestrutura de certificados.
  - Suporta NAT.



L2TP- Layer 2 Tunneling Protocol

- L2TP (***Layer 2 Tunneling Protocol***) da **IETF** (*Internet Engineering Task Force*).
- As principais características são as seguintes:
  - Túneis iniciados pelo utilizador.
  - Túneis "on-demand".
  - Controle nas mãos do utilizador.
  - A encriptação começa antes da ligação.
  - Requer autenticação de utilizadores e dos próprios computadores que tentam estabelecer a ligação.
  - Requer uma infraestrutura de certificados.
  - Não é compatível com sistema NAT.

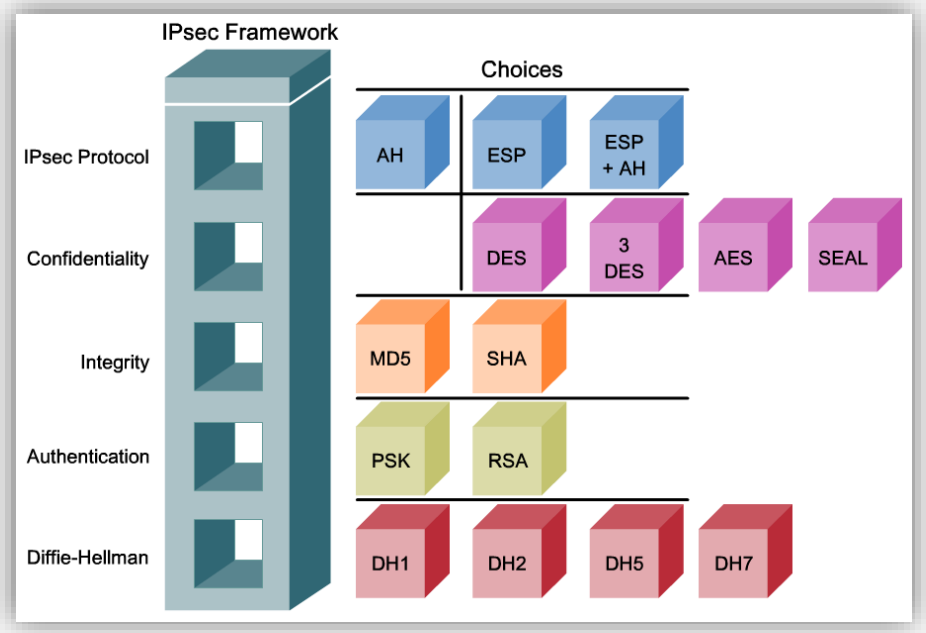


IPSec

- O RFC 1825, publicado em 1995, estabeleceu a arquitetura de segurança por meio da especificação dos protocolos AH e ESP cujos cabeçalhos seriam usados para fornecer serviços de segurança (autenticidade, integridade e confidencialidade) no IPv4 e IPv6.
- Detalhes da sua implementação foram inicialmente especificados nas RFC 1826 e RFC 1827.
- O RFC 1825 definiu a necessidade de existência de um protocolo de gestão de chaves como necessário ao uso de AH ou ESP, bem como especificou o conceito de Security Association (SA) como um conjunto de informações que definem uma ligação que suporta estes protocolos.
- Em novembro 1998 o IPSec teve novas definições que foram descritas nos RFC 2401 a 2412. Este conjunto de RFCs ficou conhecido como "antigo IPsec" ou "IPsec-v2".
- Em 2005 a arquitetura IPsec foi novamente renovada e expandida para uma terceira geração de RFCs (RFC 4301, 4302 e 4306, dentre outras), o que se convencionou chamar "IPsec-v3", ou "novo IPsec".
- Tem por objetivo proteger os dados “assinando” digitalmente e encriptando os mesmos antes de os transmitir.
- Consiste numa *framework* que suporta diferentes mecanismos para:
  - manter a confidencialidade e integridade dos dados.
  - autenticar a fonte de dados.
- Funciona ao nível da camada de rede (OSI Layer 3).

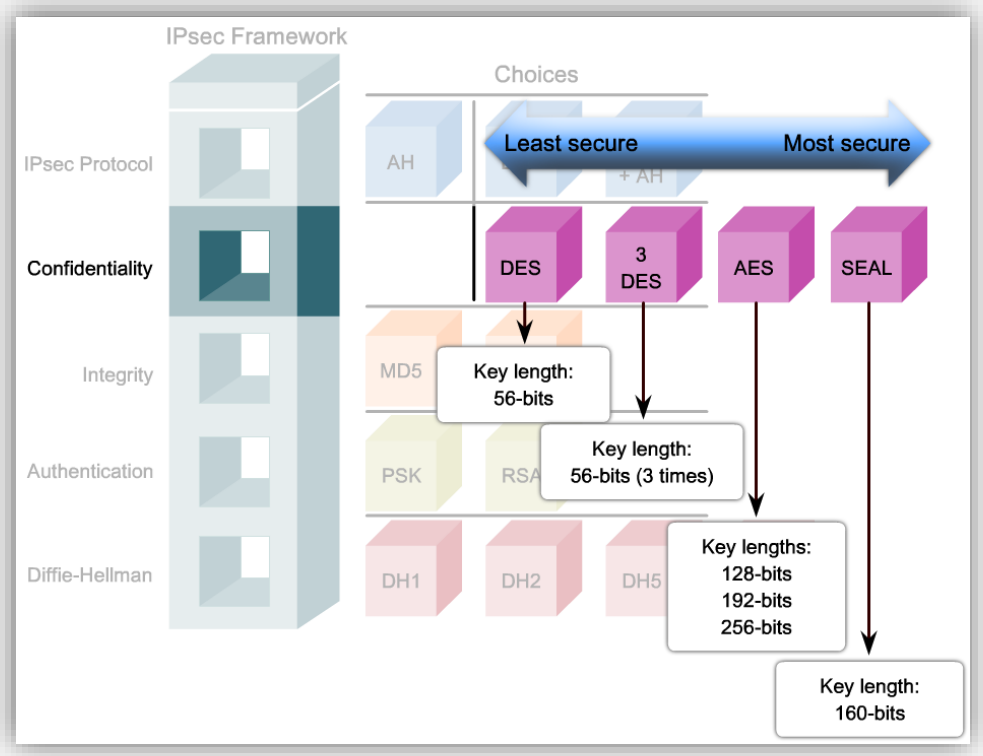
IPSec

- Constituído por 5 “blocos”:
  - Protocolos IPSec
  - Confidencialidade
  - Integridade
  - Autenticação
  - Gestão de troca de chaves de segurança



Confidencialidade

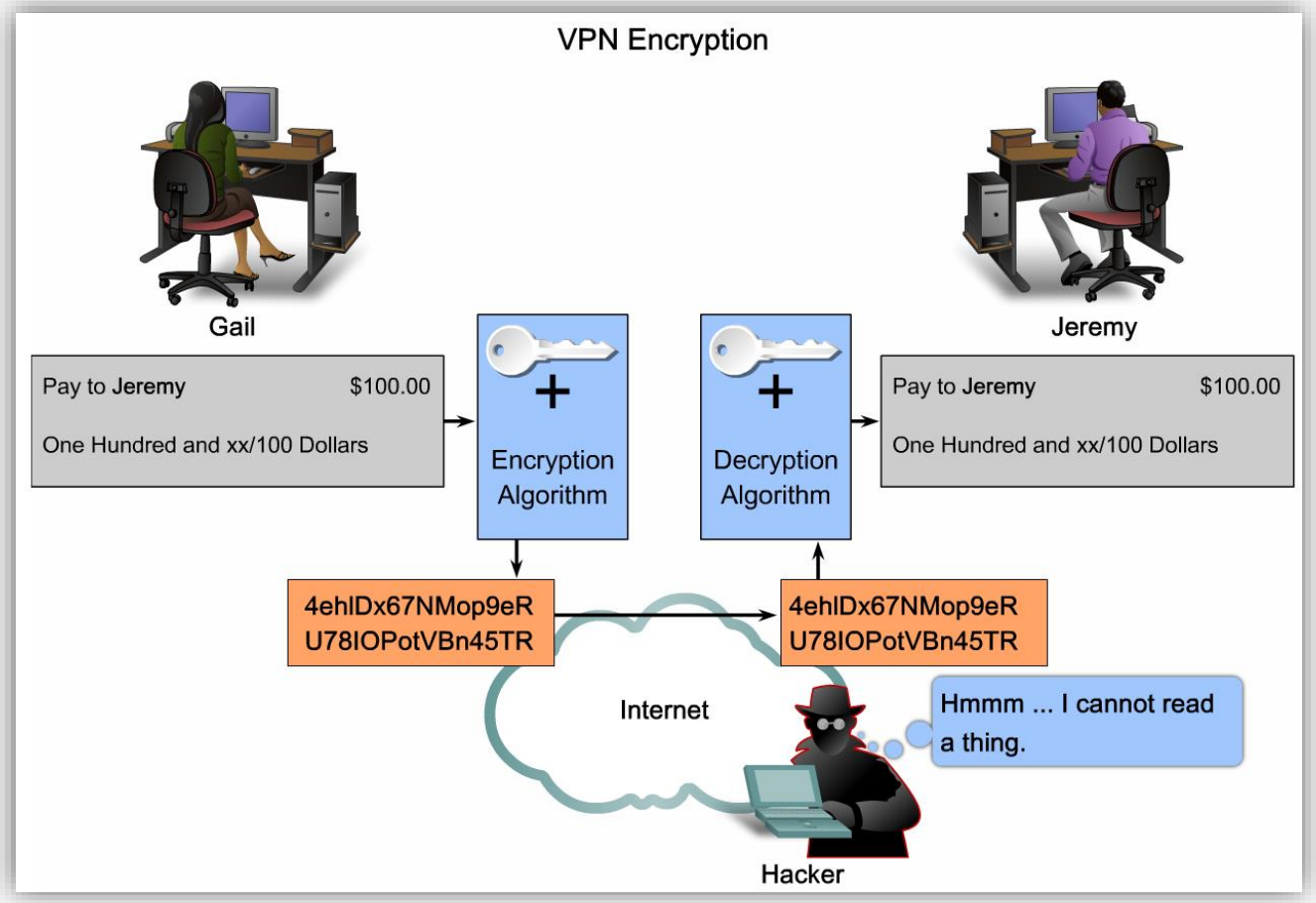
- Protege a privacidade na troca de informação através da encriptação dos dados.
- É a garantia que a informação se mantem protegida contra a sua revelação não autorizada.



Confidencialidade

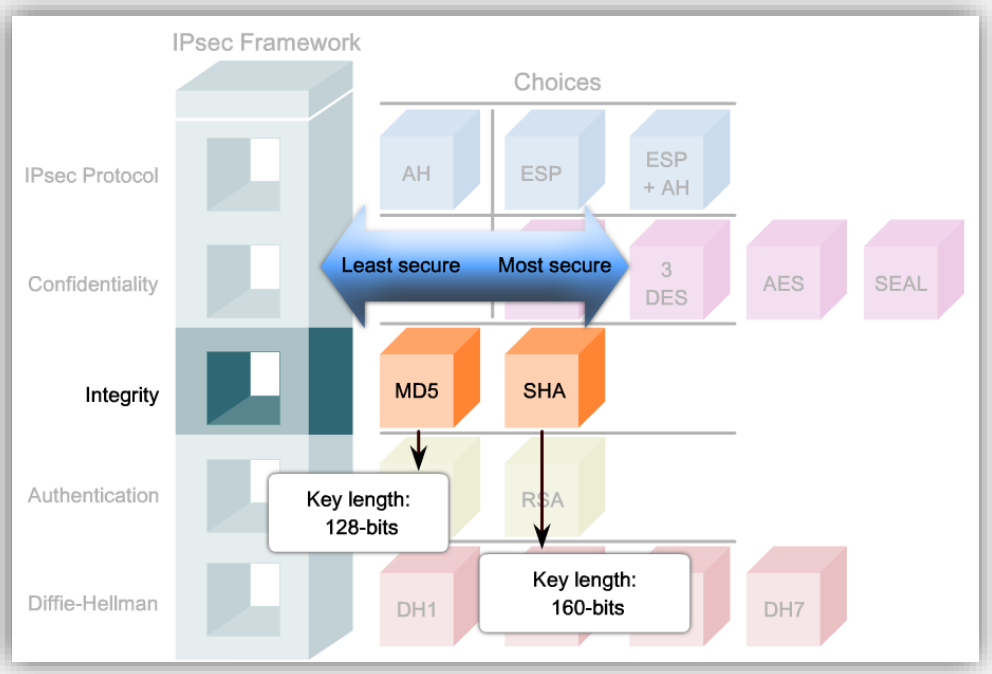
- Chaves secretas não devem ser trocadas pela rede por razões obvias.
- Chaves secretas e públicas são criadas aos pares e mantém uma relação matemática.
- Dados criptografados com a chave pública de alguém, só podem ser recompostos com a chave privada dessa mesma pessoa.
- Chaves públicas podem ser trocadas pela rede livremente.

Confidencialidade



Integridade

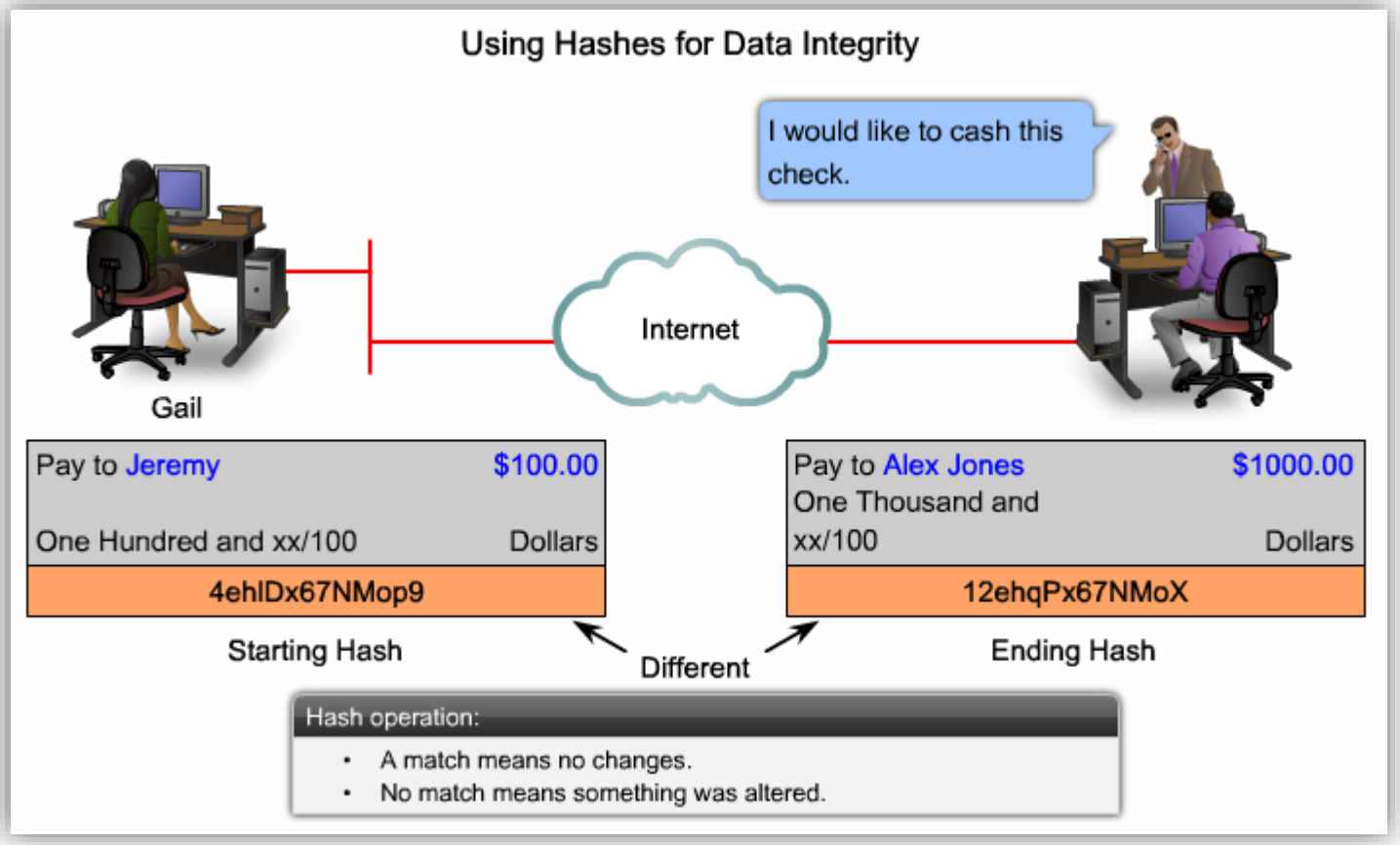
- Garantir que a informação transmitida não foi alterada de forma alguma.
- A integridade dos dados é garantida através de algoritmos *Hashed Message Authentication Codes* (HMAC)



Integridade

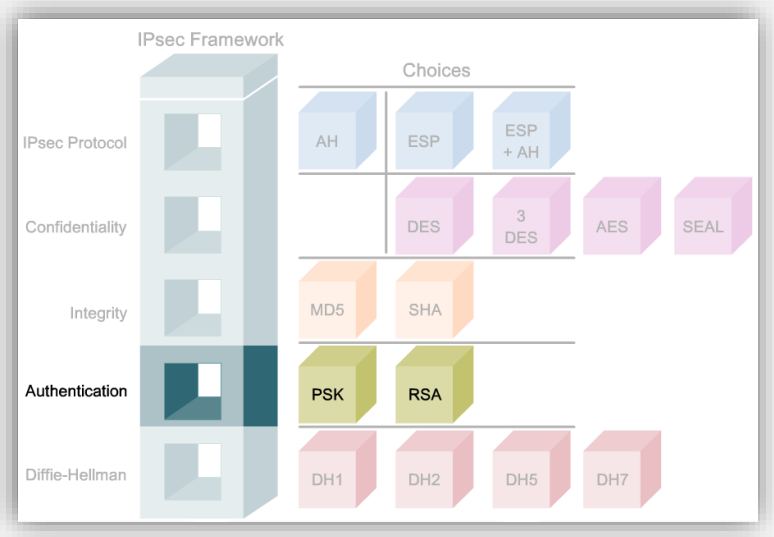
- *One way hash function*
  - espécie de um "checksum" [função $f(x) = y$] para um conjunto de dados segundo um padrão conhecido.
  - Gerado na saída e conferido na chegada.
- *Message-authentication codes* (MACs)
  - adicionar uma chave à função hash. O emissor cria o arquivo a ser enviado; calcula o MAC baseado na chave partilhada com o receptor e adiciona-a ao arquivo; receptor lê o arquivo, calcula o MAC e compara com o que veio anexado ao arquivo.

Integridade

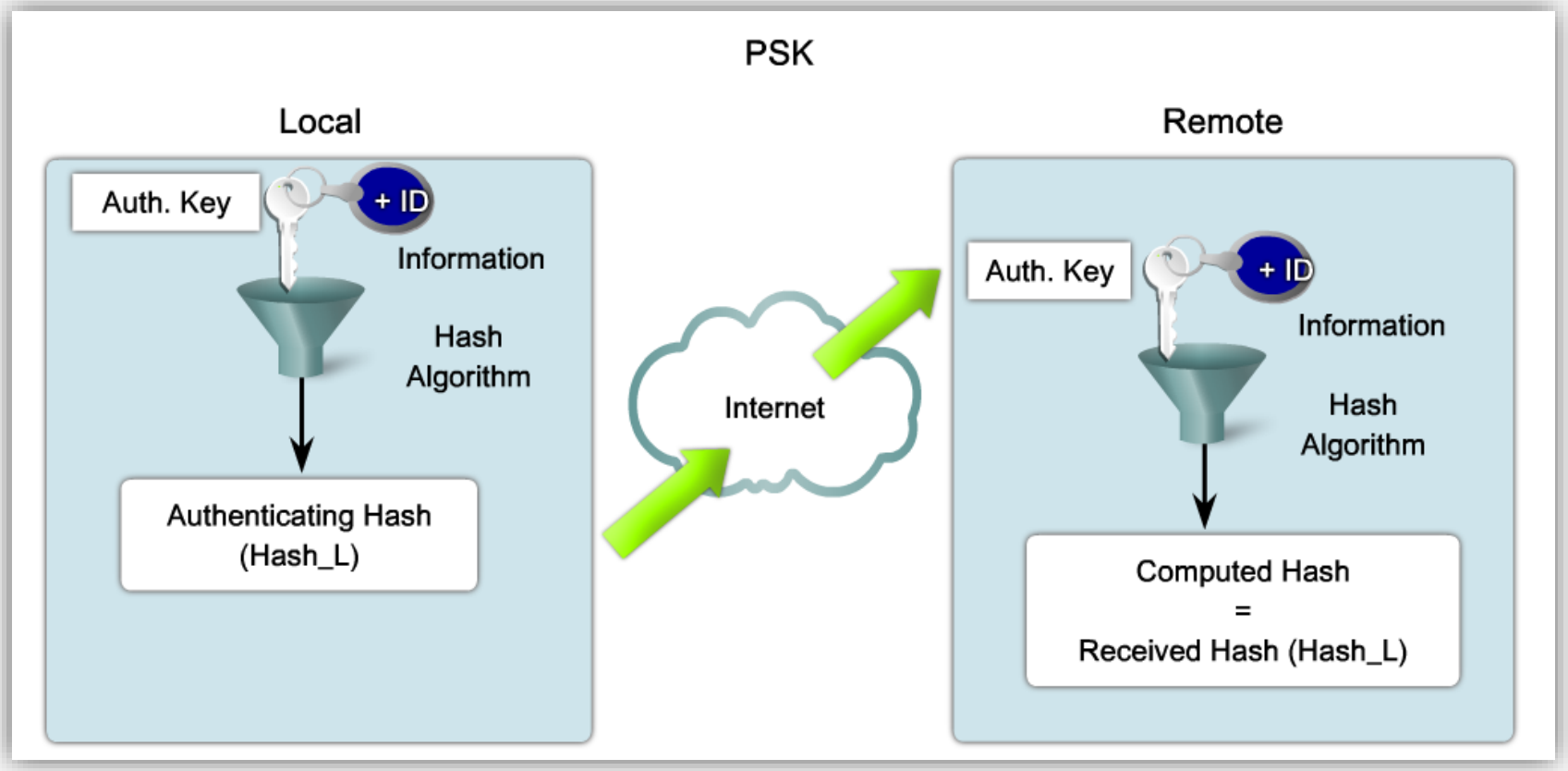


Autenticação

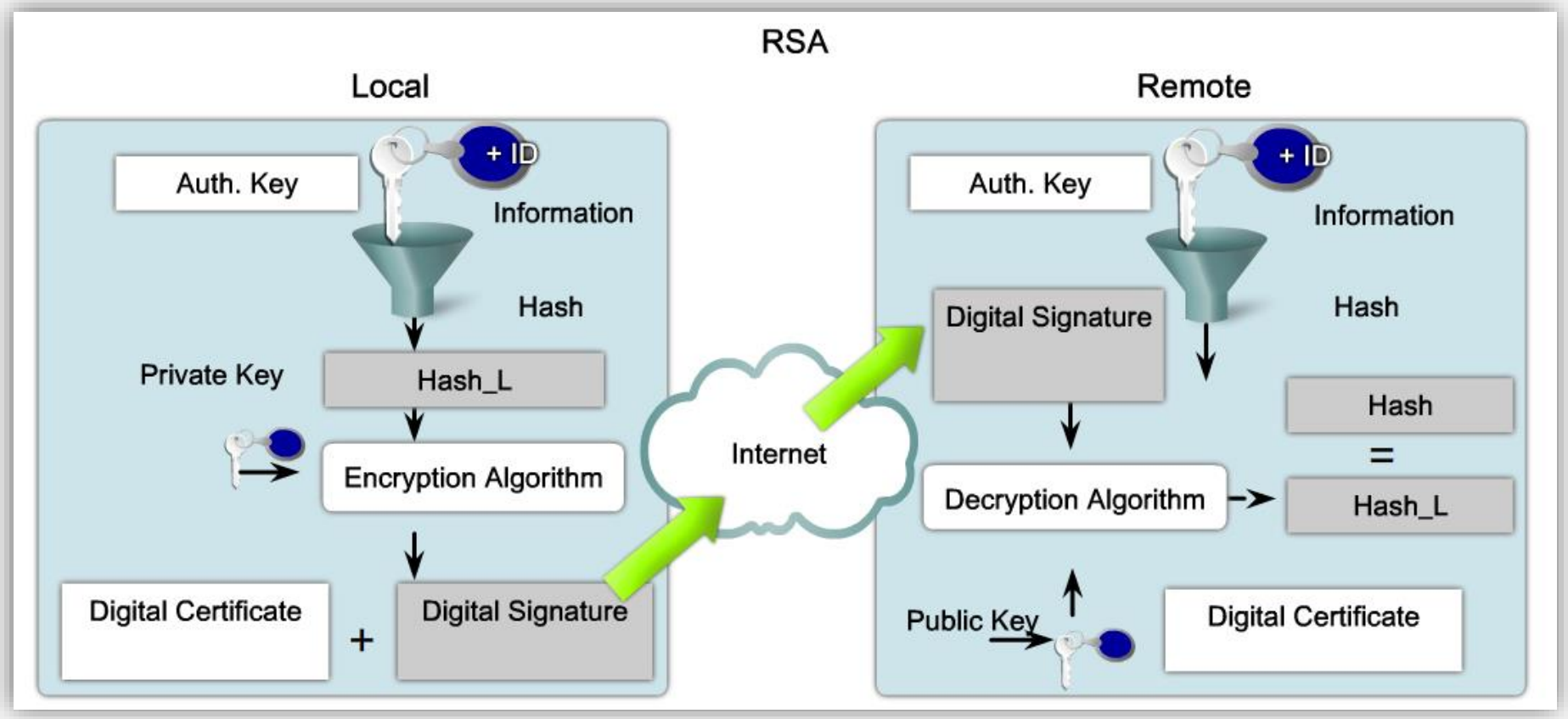
- A verificação da identidade do equipamento do lado oposto deve ser realizada antes de ser iniciada a comunicação de dados ou seja na fase de estabelecimento do túnel.
- Dois métodos base para realizar a autenticação
  - Pre-Shared Keys (PSK)
  - RSA Signatures



Pre-Shared Keys

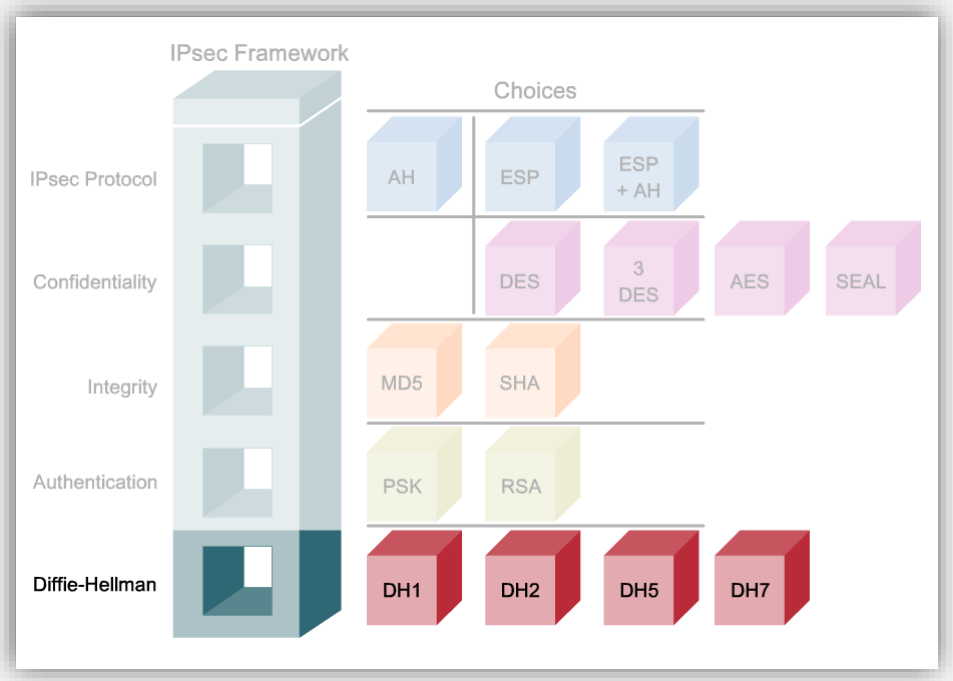


RSA Signatures



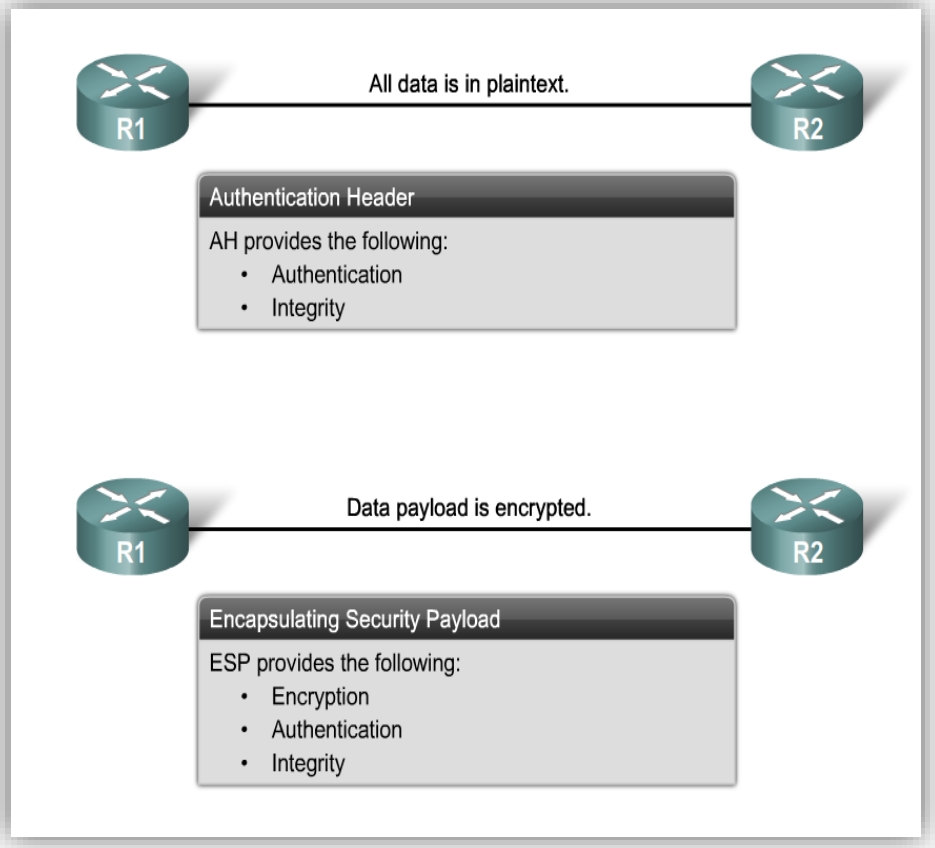
Gestão de chaves

- A gestão das chaves necessárias para o bom funcionamento dos diversos algoritmos é garantida através do método *Diffie-Hellman*. Com este protocolo são geradas em ambos os lados a mesma chave simétrica.



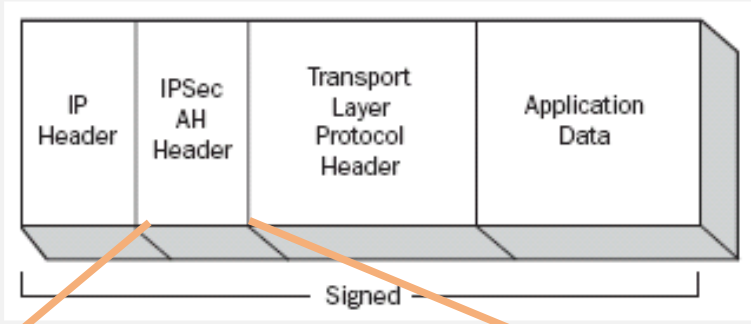
Protocolos IPSec

- Os principais protocolos usados no IPSec são:
  - ***Authentication Header*** (AH)
  - ***Encapsulating Security Payload*** (ESP)
  - ***IKE:*** (*Internet Key Exchange*)



Authentication Header (AH)

- Este protocolo não encripta os dados, mas permite a autenticação, proteção contra ataques de repetição e de manutenção de integridade dos dados.



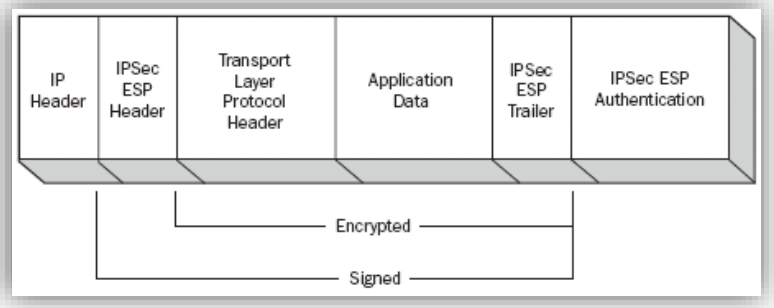
Next Header	Payload Length	Reserved
Security Parameters Index		
Sequence Number		
Authentication Data		

Authentication Header (AH)

- Campos do cabeçalho:
  - *Next header*
    - O código do protocolo que deu origem à existência do cabeçalho AH, normalmente TCP, UDP, ICMP
  - *Payload length*
    - Tamanho do cabeçalho AH
  - *Security Parameters Index*
    - Parâmetros de segurança, resultado da negociação
  - *Sequence Number*
    - Contém um valor que é iniciado em 1 e é incrementado por cada pacote que é enviado
  - *Authentication Data*
    - Contém um '*integrity check value*' (ICV) calculado pelo computador origem e recalculado, para comparação, no computador destino

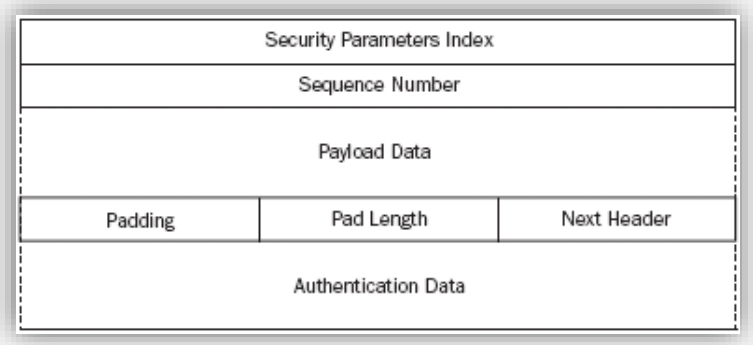
IP Encapsulating Security Payload (ESP)

- É o protocolo que permite a encriptação dos dados nos pacotes
- Também fornece mecanismos de autenticação, anti repetição e verificação de integridade
- Insere um cabeçalho e um campo de terminação específico



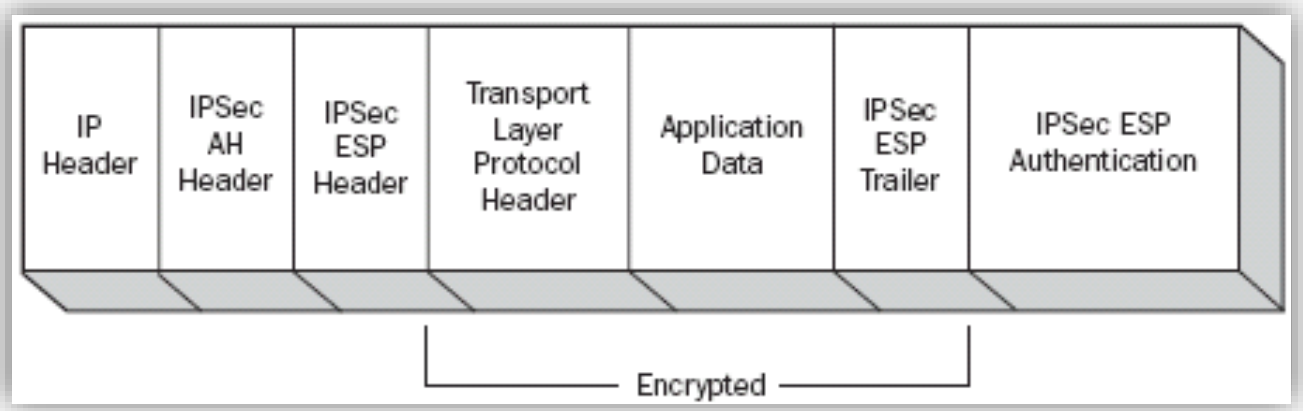
IP Encapsulating Security Payload (ESP)

- Campos da mensagem
  - *Security Parameters Index*
    - identifica os parâmetros de segurança em combinação com o endereço de IP;
  - *Sequence Number*
    - um número crescente, usado para impedir ataques repetitivos;
  - *Payload Data*
    - Contém a informação original existente no pacote IP original e, normalmente, corresponde a informação TCP, UDP ou ICMP
  - *Pad length*
    - Número de bytes acrescentados (campo *padding*) de modo a efectuar um alinhamento de 32 bits
  - *Next Header*
    - O código do protocolo que deu origem a esta mensagem e correspondente à informação existente em *Payload Data*
  - *Authentication Data*
    - contém os dados usados para autenticação do pacote.



AH e ESP

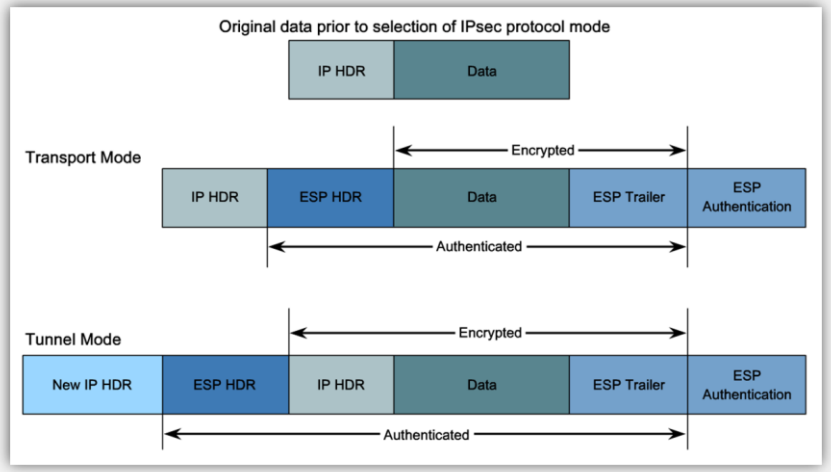
- O IPSec pode usar uma combinação do AH e do ESP



- O ESP não inclui no cálculo do ICV o cabeçalho IP (só inclui o que está entre o cabeçalho e a cauda ESP).
- O AH por seu turno inclui a maior parte da informação presente no cabeçalho IP para o cálculo do seu ICV.

IPSec – Modos de operação

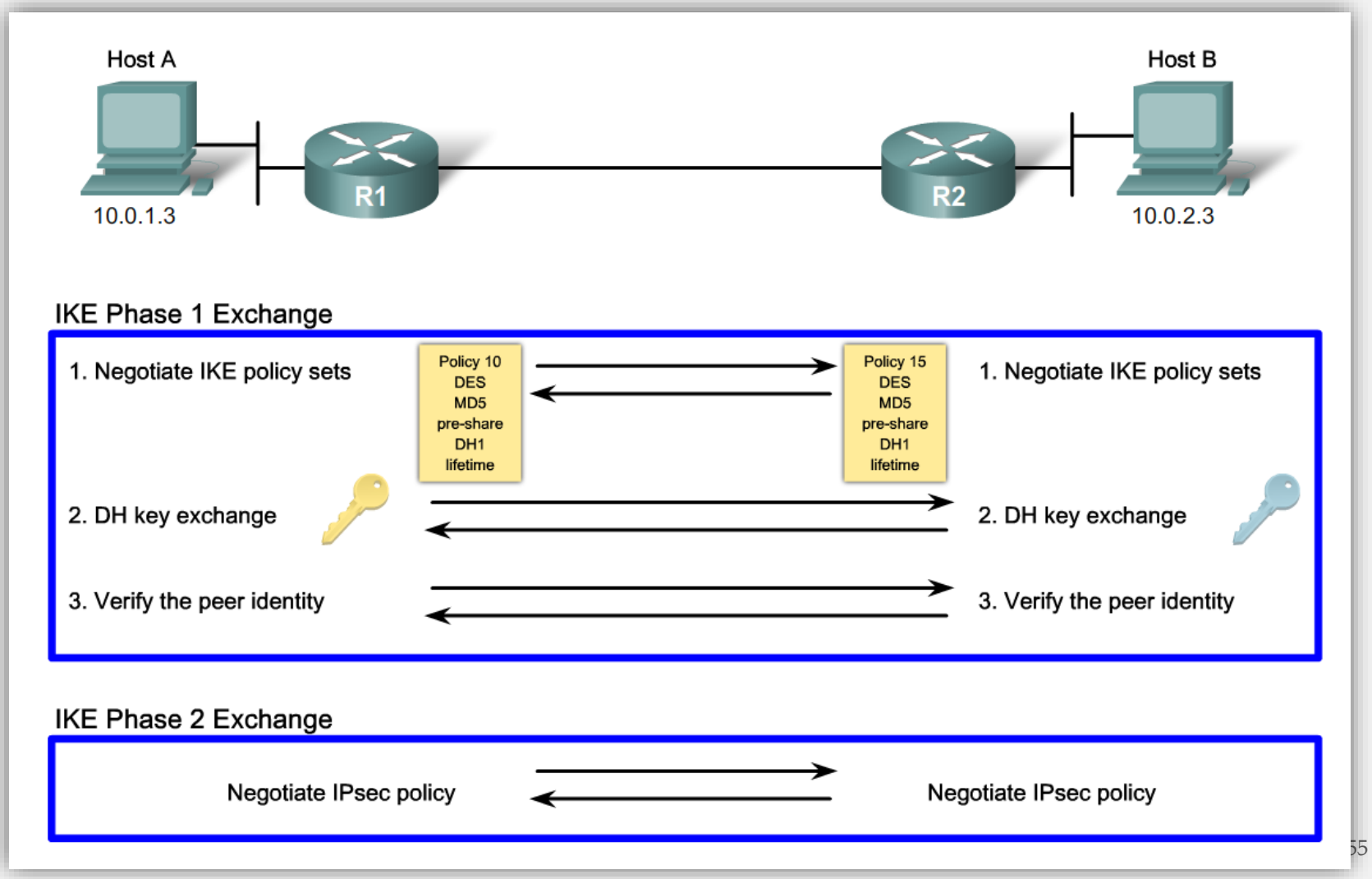
- O IPSec pode operar em dois modos
  - **Transport mode – Modo de transporte**
    - Usado para proteger a comunicação entre dois computadores de uma rede.
    - Os dois computadores têm que suportar IPSec, mas os equipamentos intermediários não necessitam de suportar.
    - Cabeçalho do datagrama IP é mantido.
    - Usados endereços originais (globais).
    - Alguns campos do cabeçalho não são protegidos.
  - **Tunnel mode – Modo de túnel**
    - Usado para proteger a comunicação de WANs e, particularmente, VPNs.
    - Os dois computadores não precisam de suportar IPSec.
    - Os routers dos dois lados da WAN necessitam de suportar IPSec.
    - Datagrama original encapsulado dentro do novo pacote.
    - Protege completamente o datagrama original.
    - Datagrama original pode ter endereços privados.



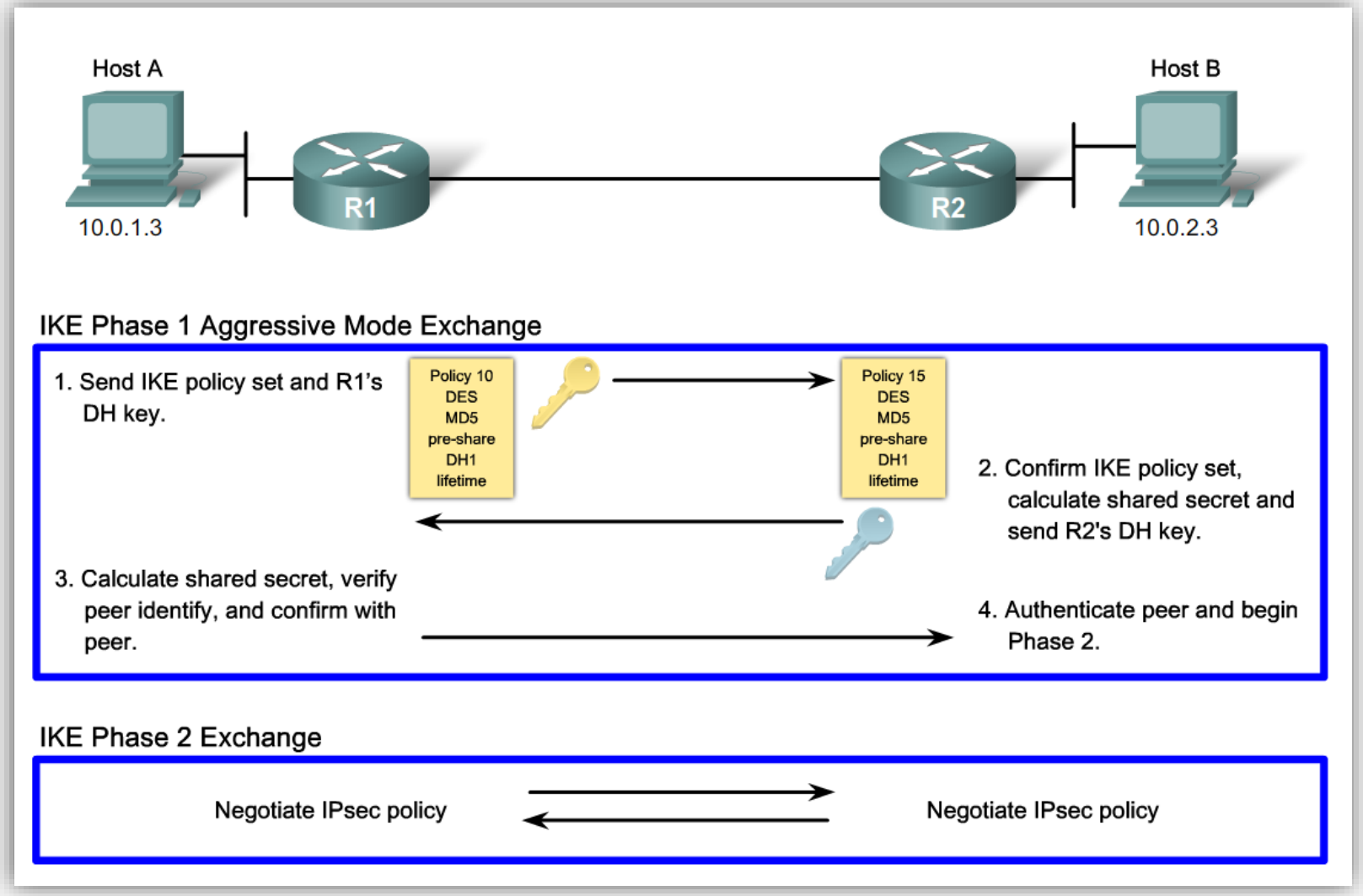
Internet Key Exchange (IKE)

- Usado para negociação dos parâmetros e chaves do IPSec.
- É um protocolo híbrido baseado em framework, definido pelo Internet Security Association and Key Manengement Protocol – ISAKMP.
- O conjunto de parâmetros negociados entre dois dispositivos é designado por Security Association (SA).
- Utiliza o porto UDP 500.

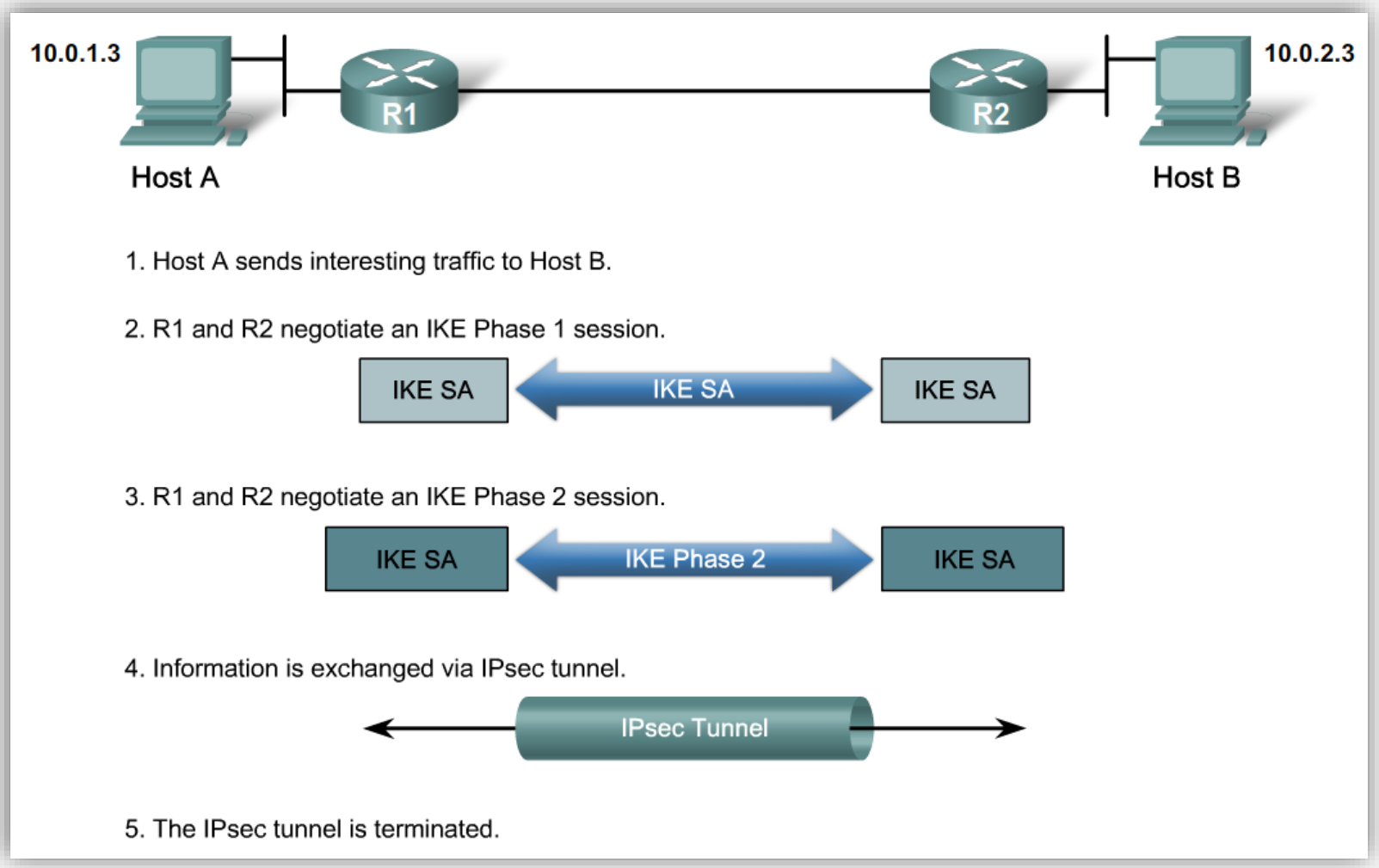
Funcionamento IKE



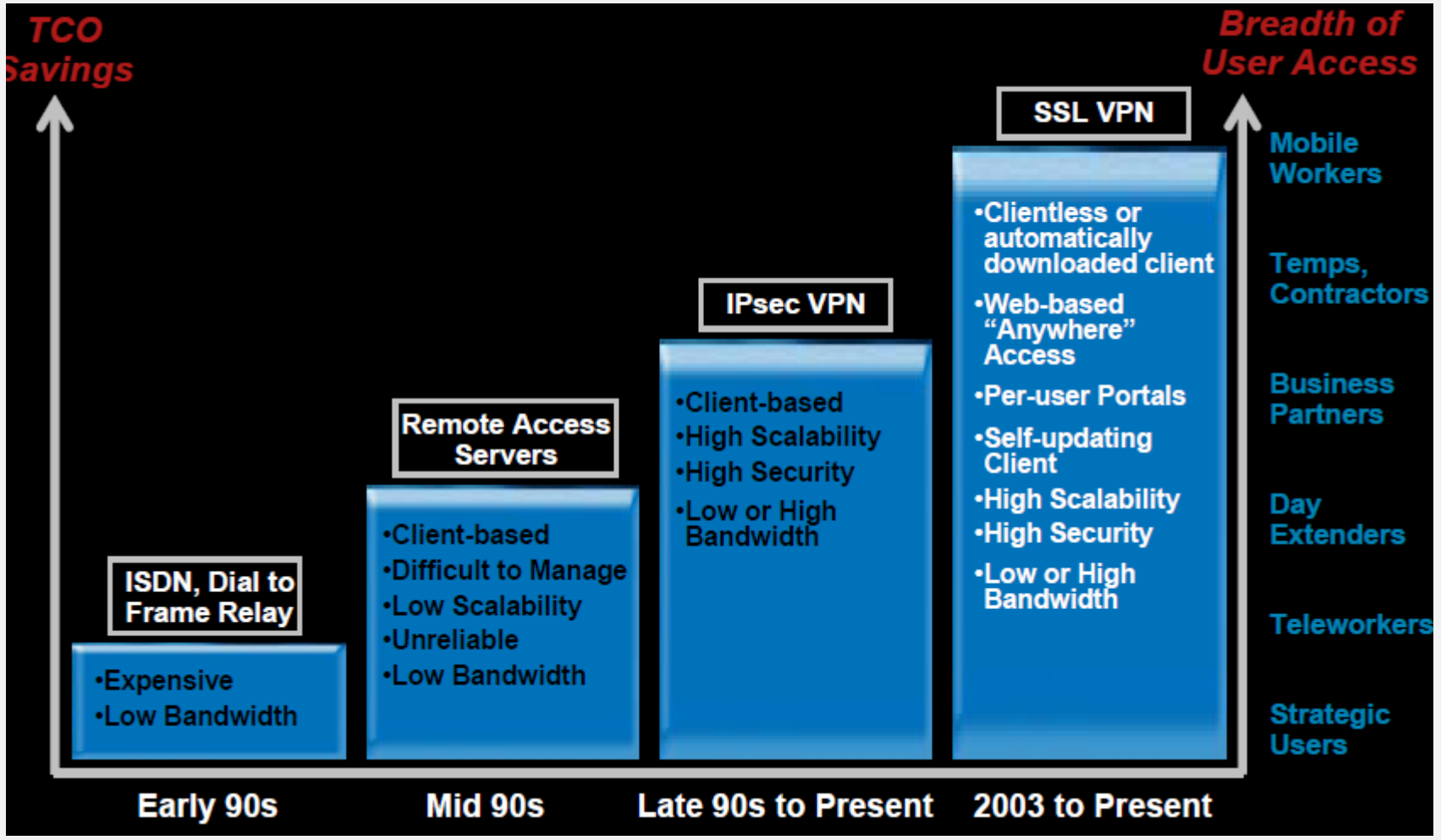
Funcionamento IKE (Aggressive mode)



Ciclo de vida de um túnel IPSec



Acesso remoto - evolução



VPN SSL

- O protocolo Secure Sockets Layer (SSL) foi criado pela *Netscape Communications Corporation*, estando atualmente implementado em todos os browsers.
- Começou por ser um modo de assegurar a segurança das transações de comércio eletrónico, tornou-se uma alternativa de baixo custo ao protocolo IPSec utilizado nas redes privadas virtuais.
- O protocolo SSL baseia-se em certificados – cartões digitais de identificação que são passados entre o servidor e o cliente.
- A simplicidade do protocolo SSL traduz-se na facilidade de instalação e redução de custos no longo prazo devido a um suporte mais simples, por oposição ao protocolo IPSec VPN que requer um cliente dedicado em cada equipamento remoto.

VPN-SSL

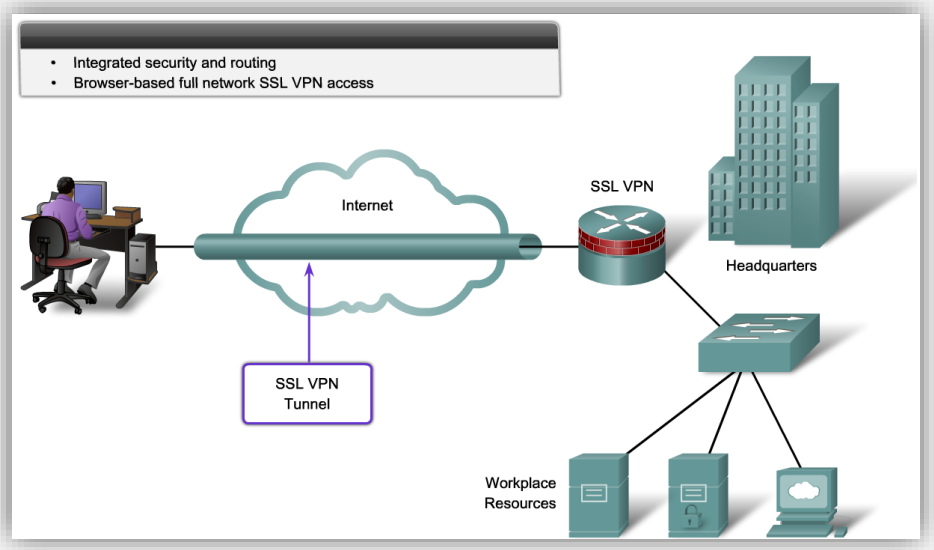
- *"As empresas estão interessadas na tecnologia SSL VPN porque os browsers podem detetá-la. Isto torna esta tecnologia mais flexível do que o protocolo IPSec, que requer um cliente de software separado nos equipamentos remotos"* sublinha o estudo do Gartner.

VPN - SSL

- A restrição da tecnologia SSL de apenas poder suportar aplicações Web foi um obstáculo inicial. Tal afastou alguns dos potenciais clientes cujos utilizadores necessitavam de aceder a aplicações cliente-servidor tradicionais (por exemplo acesso a aplicação VB).
- O crescimento das redes Wi-Fi no interior das organizações empresariais veio auxiliar a penetração da tecnologia SSL VPN. Com os problemas de segurança das redes Wi-Fi que possibilitaram a entrada ilegal nas redes corporativas, os especialistas em segurança pensaram um meio de reduzir o acesso através dos pontos de acesso wireless.
- Como as VPN preenchiam os requisitos porque podiam ser adicionadas às implementações *wireless* existentes para autenticar utilizadores na rede de comunicações e encriptar o tráfego à medida que viajava pelo ar as VPN-SSL eram atrativas e conheceram um grande desenvolvimento.

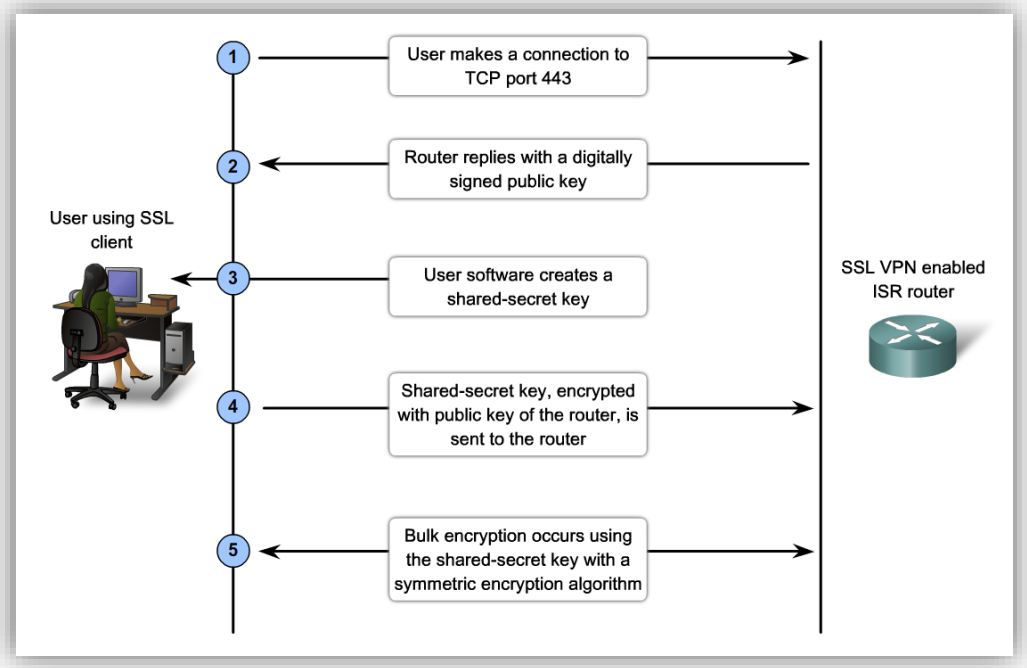
VPN SSL

- Uma das principais vantagens é a utilização de protocolos de suporte que, normalmente, não estão bloqueados nas *firewalls:*
  - Utiliza TCP, porto 443 (HTTPS)
- Suporta métodos "fortes" de autenticação como é o caso do EAP-TLS
- Encriptação - 40-bit ou 128-bit RC4



VPN - SSL

1. O cliente liga-se ao site protegido por SSL e pede-lhe que se autentique. O cliente envia igualmente a lista dos sistemas criptográficos que suporta.
2. Quando o servidor recebe o pedido, envia um certificado, contendo a chave pública do servidor, assinado por uma autoridade de certificação (CA), bem como o nome do sistema criptográfico usado.
3. O cliente por sua vez verifica a validade e autenticidade do certificado, e cria uma chave secreta aleatória, em seguida encripta essa chave secreta com a chave pública do servidor, e envia o resultado para o servidor.
4. O servidor decifra a chave de sessão com a sua chave privada. Assim, as duas entidades estão na posse de uma chave comum da qual são os únicos conhecedores e a partir dessa chave são realizadas o resto das transações.

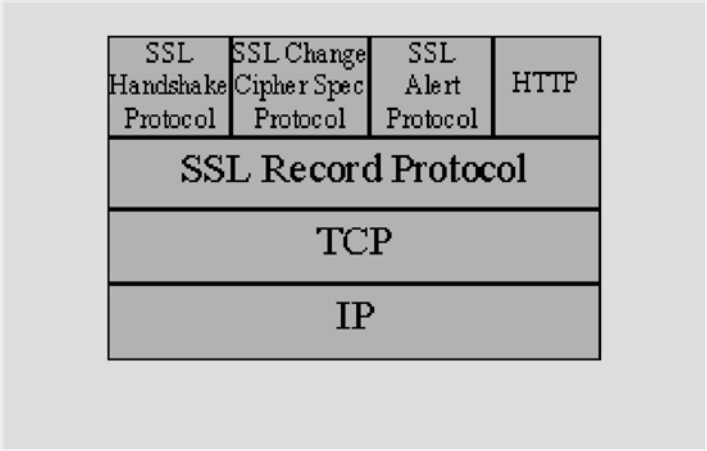


Tipos

- ***Clientless*** — fornece um acesso seguro a recursos privados e acesso a conteúdos. Este modo é utilizado quando o recurso desejado é acessível utilizando um browser tais como acesso à Internet, base de dados e aplicações on-line web.
- ***Thin Client (port-forwarding Java applet)*** — estende as capacidades de criptografia e permite o acesso remoto web a aplicações TCP como Post Office Protocol version 3 (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access protocol (IMAP), Telnet, e Secure Shell (SSH).
- ***Tunnel Mode*** — é baseado na instalação de um cliente que permite o estabelecimento de um túnel entre o cliente e o servidor e assim o acesso a todas as aplicações.

VPN-SSL - Protocolos

- O protocolo SSL é dividido em duas Camadas, sendo uma de mais baixo nível que trabalha com o protocolo de transporte que é denominado protocolo *Record*.
- Este protocolo é responsável por encapsular os dados das camadas superiores em pacotes compactados e cifrados e encaminhá-los à camada de transporte.
- Na camada superior, encontra-se o protocolo de *Handshake,* o CCSP *(Change Cipher Spec Protocol)* e o *Alert Protocol*.



VPN-SSL - Protocolos

- O protocolo *Record* SSL fornece serviços de confiabilidade e integridade de mensagens nas ligações SSL.
- Define um conjunto de formatos e procedimentos pelos quais as mensagens da camada de aplicação são fragmentadas ou misturadas em blocos de um tamanho adequado para as próximas etapas.
- Fornece procedimentos de compactação, proteção, criptografia para as mensagens que são passadas para a camada inferior

VPN-SSL - Protocolos

- O **Protocolo *Handshake*** é responsável por manter a consistência dos estados de uma sessão tanto no cliente quanto no servidor.
- Os dados que formam uma sessão SSL são os seguintes:
  - ***session* ID** é um valor arbitrário escolhido pelo servidor para identificar a sessão;
  - ***peer certificate*** é usado para certificar uma organização. Está no formato X.509 e entre outras coisas contem a chave pública da entidade que está utilizando aquela aplicação;
  - ***compression method*** é o algoritmo usado na compressão dos dados;
  - ***cipherspec*** - especifica que conjunto de algoritmos de encripção e de *hash* utilizados;
  - ***mastersecret*** - é um segredo de 48 bytes compartilhado pelo servidor e pelo
  - cliente;
  - ***isresumable*** - é uma *flag* utilizada para indicar se a sessão pode ou não ser retomada ao iniciar uma nova conexão.

VPN-SSL - Protocolos

- O **protocolo *ChangeCipherSpec*** é responsável por sinalizar alguma modificação nas estratégias ou parâmetros de segurança utilizados
- Formado por uma única mensagem, a *change_cipher_spec*.
- Quando uma das partes do protocolo recebe uma mensagem *change_cipher_spec* durante o processo de *Handshake*, automaticamente troca as informações do estado atual de leitura pelos dados do estado pendente de leitura.

VPN-SSL - Protocolos

- O **Protocolo *Alert*** tem como responsabilidade o enio de alerta para o outro lado da ligação por cada erro gerado.
- Dependendo do nível do erro, a ligação pode ser abortada e as mensagens de alerta serão tratadas como mensagens normais sendo compactadas e encriptadas.
- Os níveis das mensagens de alerta são *warnings* e *fatals*.
  - Os *warnings* são simples avisos que informam que alguma coisa não normal aconteceu ou foi detectada.
  - Quando são do tipo *fatals* são apagados todos os dados daquela ligação.

IPSec versus SSL

- Nos quadros seguintes são apresentados as comparações/diferenças entre o IPSec e o SSL

	SSL VPN	IPSec VPN
Aplicação	Aplicações que suportem *web browser*, e-mail e compartilhamento de arquivos.	Serviços baseados em serviços IP.
Encriptação	Forte, porém variável – depende de como o *web browser* foi configurado.	Forte e consistente – a encriptação é amarrada a aplicação.
Autenticação	É variável – pode se usar uma ou duas formas de autenticação. Pode ser feita usando *tokens* e certificação digital.	É forte – pode se usar duas formas de autenticação, utilizando *tokens* e certificação digital.
Segurança	Moderada –pois com qualquer computador é possível estabelecer o túnel VPN.	Forte – devido ao fato da aplicação ser amarrada a um computador/usuário e uma aplicação específicos.
Facilidade de Utilização	Muito alta – o usuário precisa se familiarizar com o *web browser*.	Baixa – é preciso que usuários tenha conhecimento de instalação do software IPSec
Complexidade	Moderada	Alta
Custo	Baixo – pois não requer software em específico.	Alto – pois requer vários níveis de configuração.
Escalabilidade	Alta – facilidade em sua implementação.	Muito alta – funciona independente da aplicação.

IPSec versus SSL

	VPN - baseado em SSL/TLS	VPN - baseado em IPSec
Aplicações Cliente/Servidpr	Sim	Sim
Aplicações Legadas	Sim	Sim
Aplicações HTTP	Sim	Sim
File sharing	Sim	Sim
Aplicações em Mainframe	Sim	Sim
Terminal servers	Sim	Sim
Dependência aplicação de *Server socket*	Sim	Sim
Aplicações *Web*	Sim	Sim
Conteúdo de *Intranet*	Sim	Sim
Voz sobre IP	Não	Sim
File Servers	Sim	Sim
Controle de acesso para Intranets e *Extranets*	Sim	Não
Email	Sim	Sim

Fonte: (ARRAY NETWORKS)

IPSec versus SSL

	VPN - baseado em IPSEC	VPN - baseado em SSL
Tipo de conexão	Fixa	Transitória
Tipo de dispositivo	Dispositivo Gerenciado	Vários dispositivos
Tipo de Acesso	site-to-site	Remoto
Controle de Acesso	Firewall	Através de políticas

Fonte:(WITNETWORKS)

IPSec versus SSL

	VPN - baseado em IPSEC	VPN - baseado em SSL
Proxy protection	Não	Sim
Strong user authentication	Proprietário	Sim
Strong central authorization	Limitado	Sim
Suporte à Single Sign-On (SSO)	Não	Sim
Dual/Stacked Authentication	Não	Sim
Proibe a visibilidade de nomes e IP	Não	Sim
Forms-based Authentication	Não	Sim
Controle ao nível de URL	Não	Sim

Fonte: (ISSA – *INFORMATION SYSTEMS SECURITY ASSOCIATION*)

“ A tecnologia SSL VPN substituiu o protocolo IPSec como a escolha mais fácil para acesso casual e ad hoc dos empregados a VPN e para parceiros de negócio, fornecedores e manutenção exterior” , refere o estudo do Gartner

Teletrabalho

"Modalidade de prestação laboral que se processa em local diverso da sede do dador (empregador), recorrendo às tecnologias de informação e das comunicações."

Teletrabalho

- Com a massificação de tecnologias de banda larga e redes *wireless* torna-se possível trabalhar fora das instalações das empresas.
- Os trabalhadores podem trabalhar em casa ou noutros locais como se estivessem no escritório ou na sala ao lado.
- Permite a criação de SOHOs (*Small Offices and Home Offices*)
- Possibilidade de integrar trabalhadores que de outra forma não poderiam contribuir para o valor acrescentado da empresa
- Facilitar a implementação de soluções para satisfazer necessidades de trabalho contínuo

Teletrabalho

- Existem os seguintes tipos:
  - No Domicílio ("*Electronic Home Work*"): é a forma mais descentralizada de trabalho à distância, em que o trabalhador trabalha na sua própria casa utilizando tecnologias da informação de um modo direto ("online") ou i indirecto (" offline");
  - Em Centros (""*Small Offices* "): traduz-se na actividade exercida em unidades organizacionais geograficamente separadas do estabelecimento principal, mas ligadas a este por meios telemáticos;
  - Móvel ("*Mobile Work*"): actividade exercida à distância por trabalhadores "itinerantes ou nómadas", permanentemente conectados com a empresa por via telemática;
  - Em Telecentros ("*Neighbourdhood Work Center*")en"): espaços organizacionais implantados próximo do domicílio dos trabalhadores, equipados com material telemático partilhado por colaboradores de diversas empresas ou agentes autónomos.

Benefícios do teletrabalho

- Para o trabalhador
  - Maior disponibilidade para sua vida familiar.
  - Diminuição do stress e aumento do bem estar.
  - Elimina os problemas relacionados com deslocação com diminuição dos custos.
  - Redução dos custos de alimentação.
  - Controlar o seu próprio ritmo de trabalho/flexibilidade de horário.
  - Maior autonomia.

Benefícios do teletrabalho

- Para o Empregador
  - Maior flexibilidade na organização do trabalho.
  - Redução dos custos diretos (imobiliário, energia).
  - Combate ao absentismo.
  - Maior flexibilidade de horários.
  - Aumenta as possibilidades de recrutamento de mão de obra especializada.

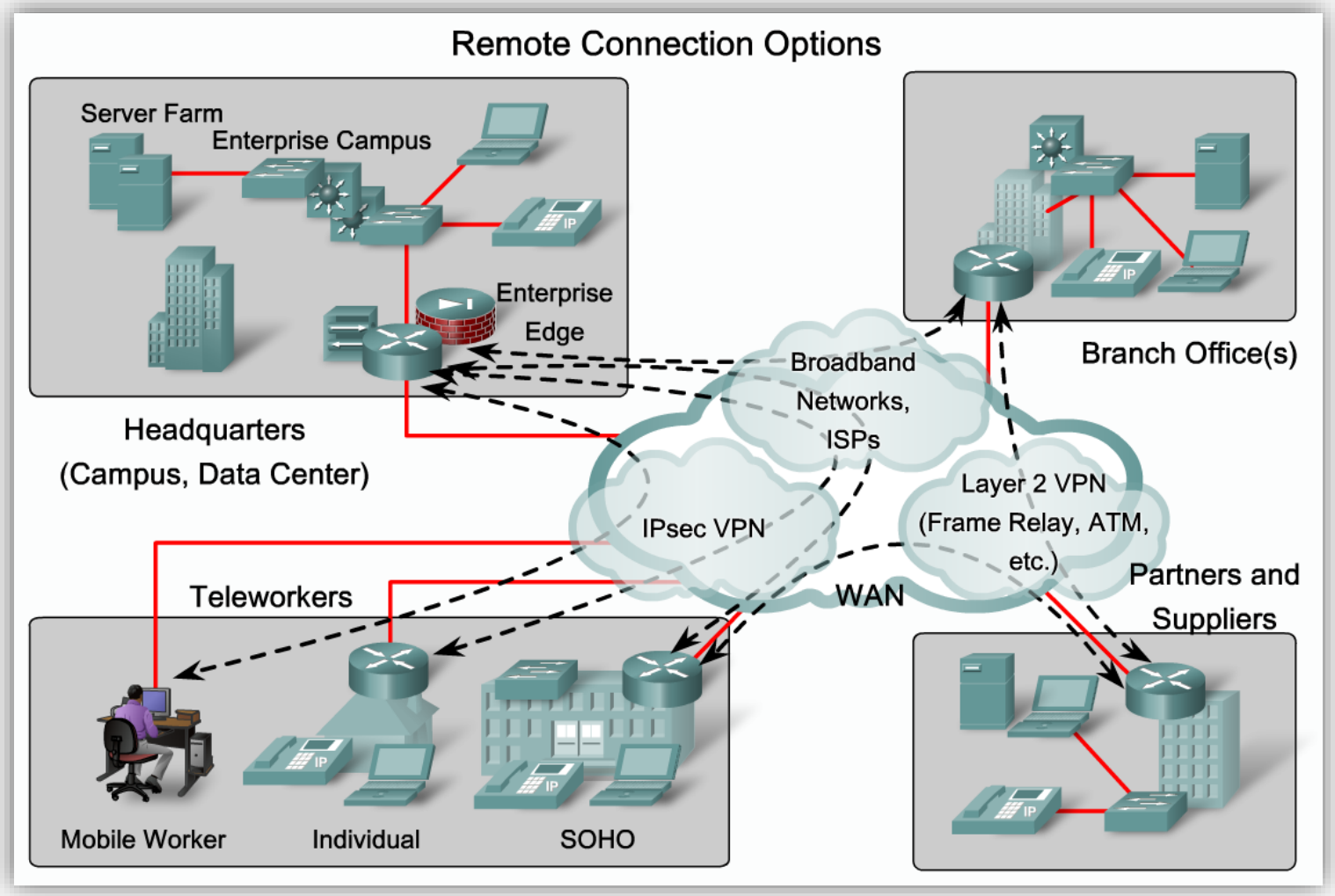
Desvantagens do teletrabalho

- Para o trabalhador
  - Falta de integração com o relacionamento entre colegas.
  - Isolamento social e profissional.
  - Dificuldade em separar a vida profissional e pessoal.
  - Problemas de metodologia/autodisciplina.
  - O espaço comum ao trabalho e à família pode gerar conflitos.

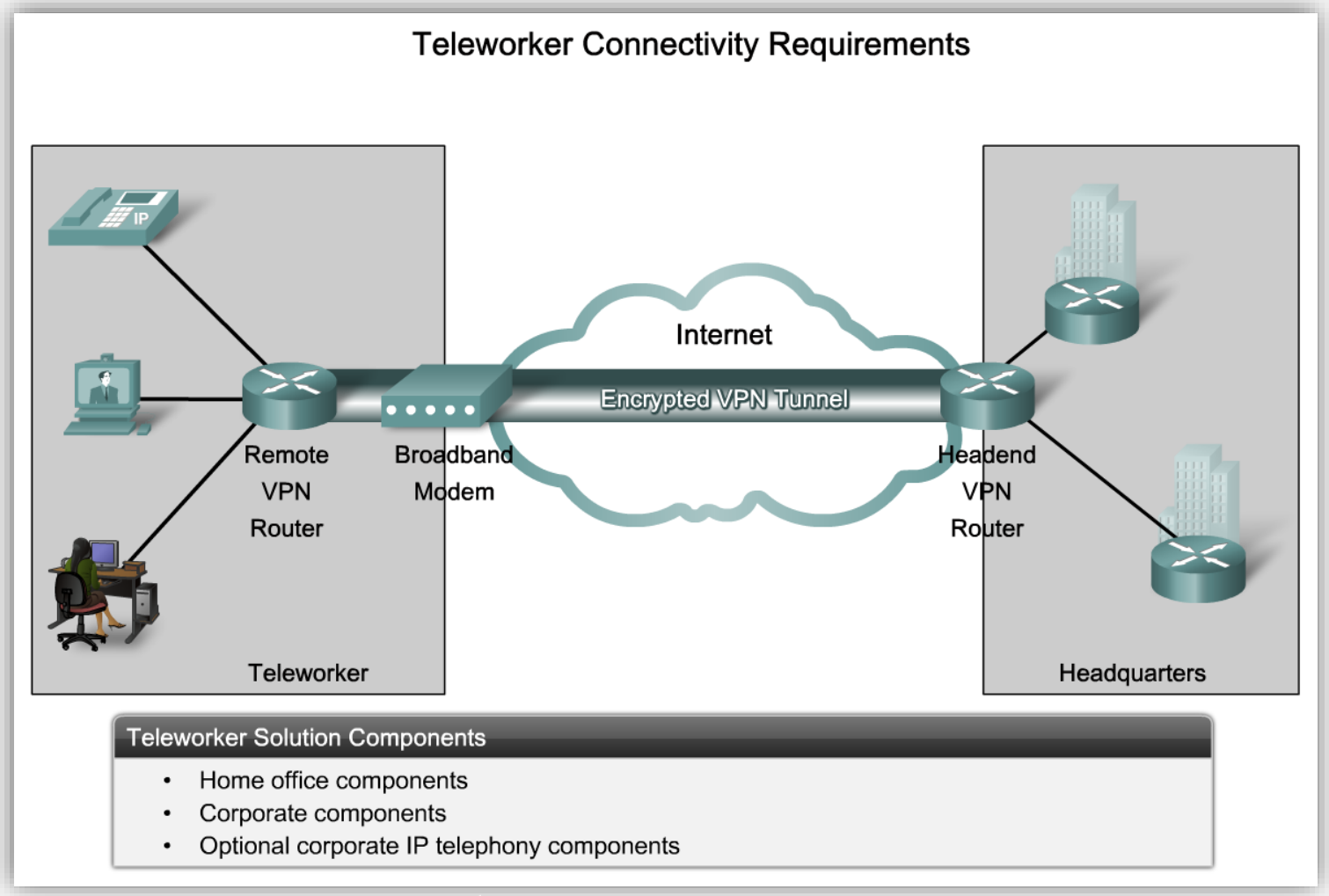
Desvantagens do teletrabalho

- Para o empregador
  - Resistência à mudança no momento da implementação.
  - Dificuldade em supervisionar o trabalho.
  - Problema de motivação dos trabalhadores.
  - Problemas na proteção de dados da empresa.
  - Diminuição da coesão n seio da empresa.
  - Problemas ao implementar o sistema de avaliação de desempenho.

Tecnologias de ligação



Componentes necessários



Dúvidas

Referencias

- *VPN*. In **Infopédia** [Em linha]. Porto: Porto Editora, 2003-2012. [Consult. 2012-05-10].
- www.cisco.com
- VPN Virtual Private Network, Bruno Fagundes, Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis
- http://pt.wikipedia.org/
- Segurança em Redes IP, Faculdade de Engenharia da Universidade do Porto
- http://www.computerworld.com.pt/2010/03/25/ssl-vpn-2/- acedido em maio de 2020.
- http://www.vivaolinux.com.br/artigo/VPN-IPSec-vs-SSL?pagina=5 - acedido em maio de 2020.
- http://www.f5.com/ - acedido em maio de 2020
- http://www.cisco.com – acedido em maio de 2020.
- https://tools.ietf.org/html/rfc6071 - – acedido em maio de 2020.
- “Comparando o uso do IPSEC e do SSL/TLS em VPN”, Marcelo Fontes, 2010