VPN
Virtual Private Network

Dênio Mariz
denio@ifpb.edu.br

Nov/2008

Definição

- Definição
  - Uma Rede Privada Virtual (VPN) é uma rede privada de dados que usa infraestrutura pública de telecomunicações, mantendo privacidade através do uso de protocolos de tunelamento e procedimentos de segurança
- Objetivo
  - Dar aos usuários as mesmas funcionalidades do uso de canais privativos de dados ao custo do uso de redes públicas compartilhadas
- Por que virtual?
  - Várias redes lógicas (protocolos) convivendo em uma mesma estrutura física, sem a necessidade de hardware especial
- por que privada?
  - A comunicação sobre a VPN é criptografada, de maneira que apenas o destinatário (ou a rede dele) pode entender a informação

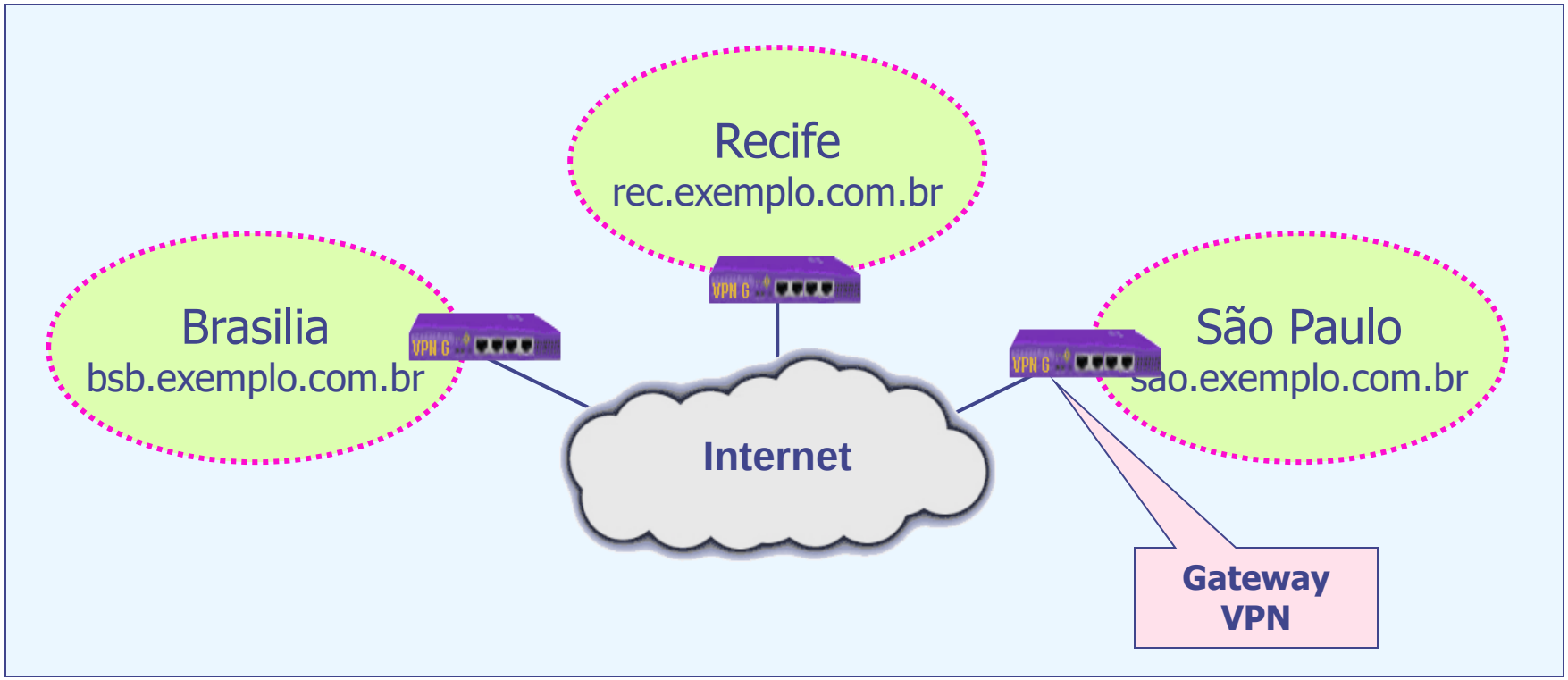
Elementos de uma VPN 1/2

- Túnel criptografado
  - Não podemos garantir que ninguém vai **ler** os pacotes
  - Mas podemos garantir que será ***muito difícil*** para outras pessoas entender a informação contida neles
  - Dados são criptografados no envio e decriptografados no recebimento
- Fim do túnel com Autenticação
  - Além de criptografadas, as mensagens são também autenticadas para garantir que são enviadas/recebidas por usuários válidos.
  - Pacotes são autenticados individualmente
  - Criptografia + autenticação combatem "replay attacks"

Elementos de uma VPN 2/2

- Rede de Transporte
  - A elegância da VPN é que ela usa a mesma conexão de rede que você já tem
  - Um pacote seguro é construído por um dispositivo VPN e enviado para outro dispositivo VPN usando a rede existente

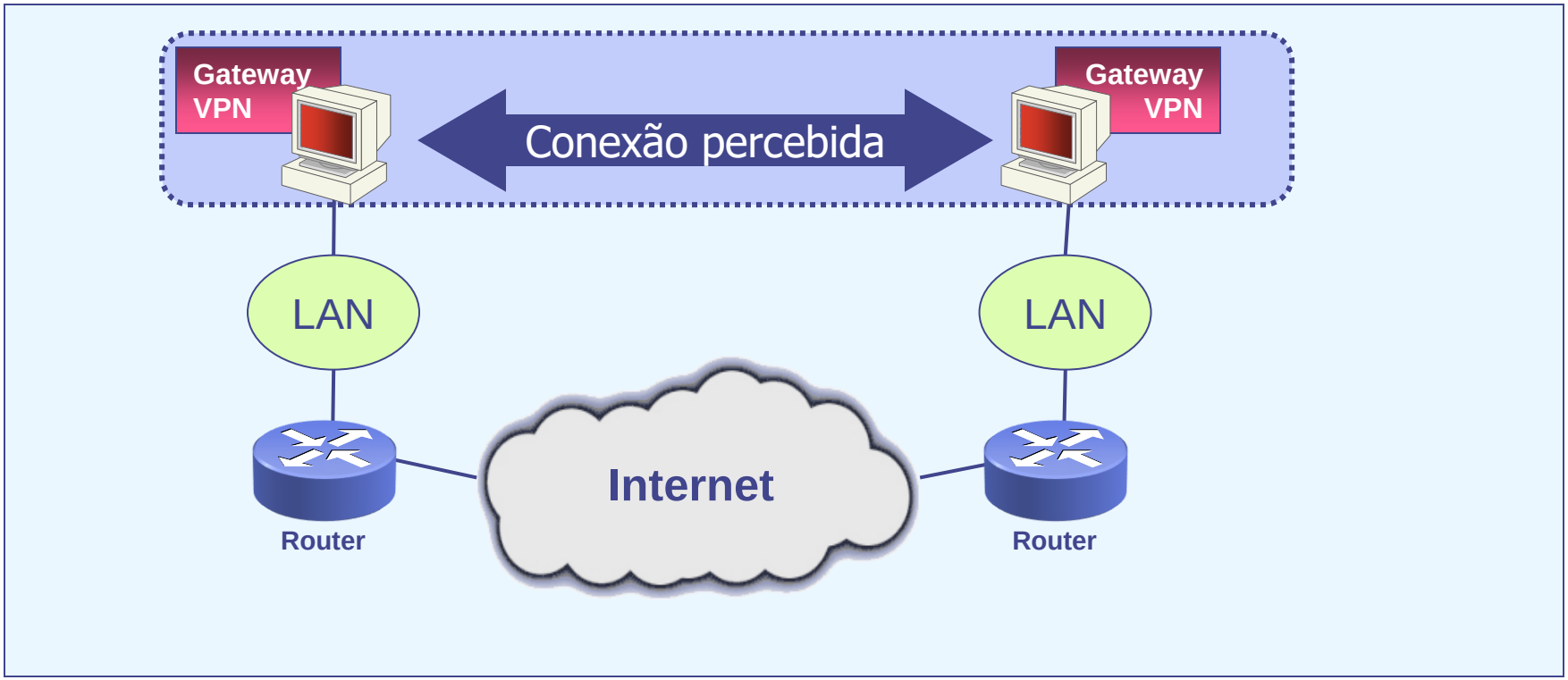
Exemplo de VPN



- **Empresa Exemplo.com.br com escritórios:**
  - **Brasília, Recife, São Paulo**
- **VPN garante tráfego seguro entre escritórios, via Internet**
- **VPN só é de conhecimento do Gateway VPN na borda da rede**
- **Transparente para hosts dentro da rede**

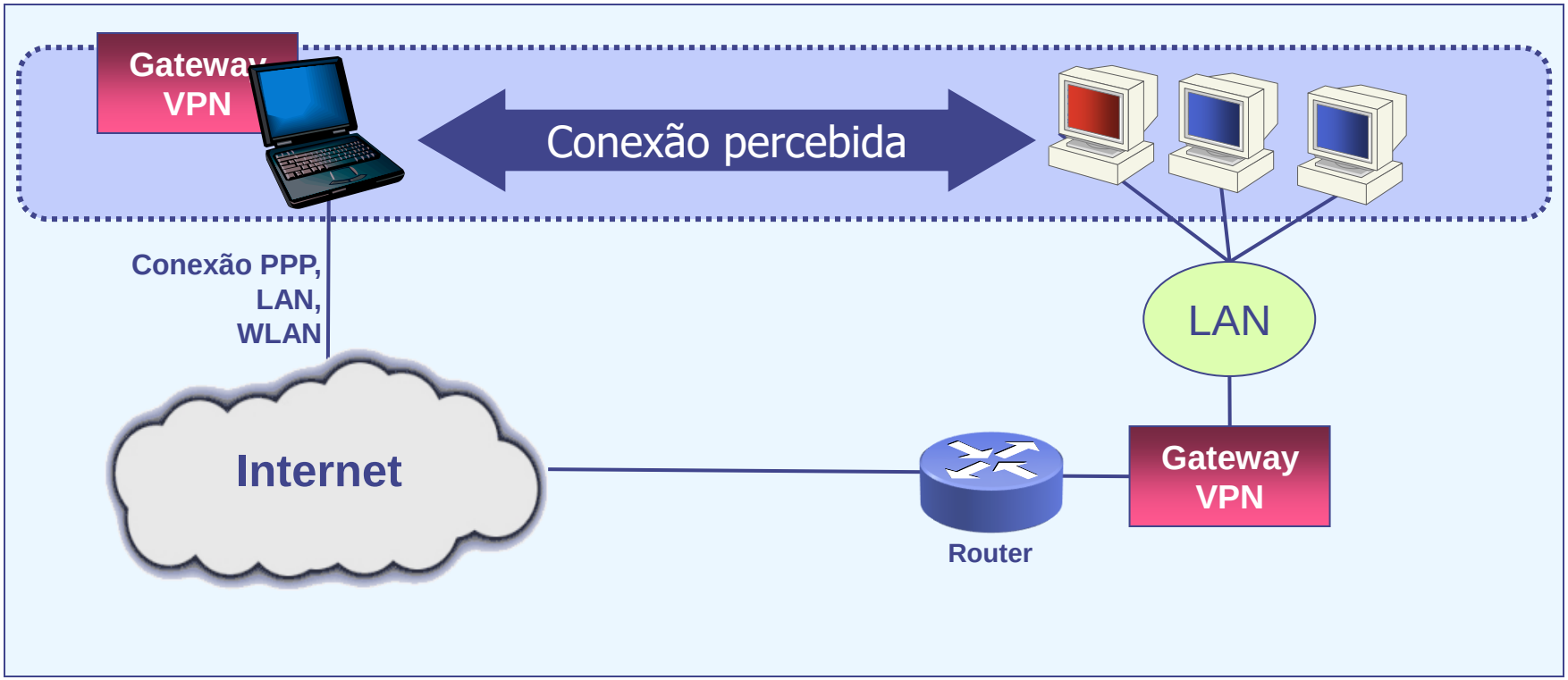
Topologias VPN

- Host-to-Host
  - Software para suporte à VPN rodam em cada lado
  - Ex: servidores sincronizando dados



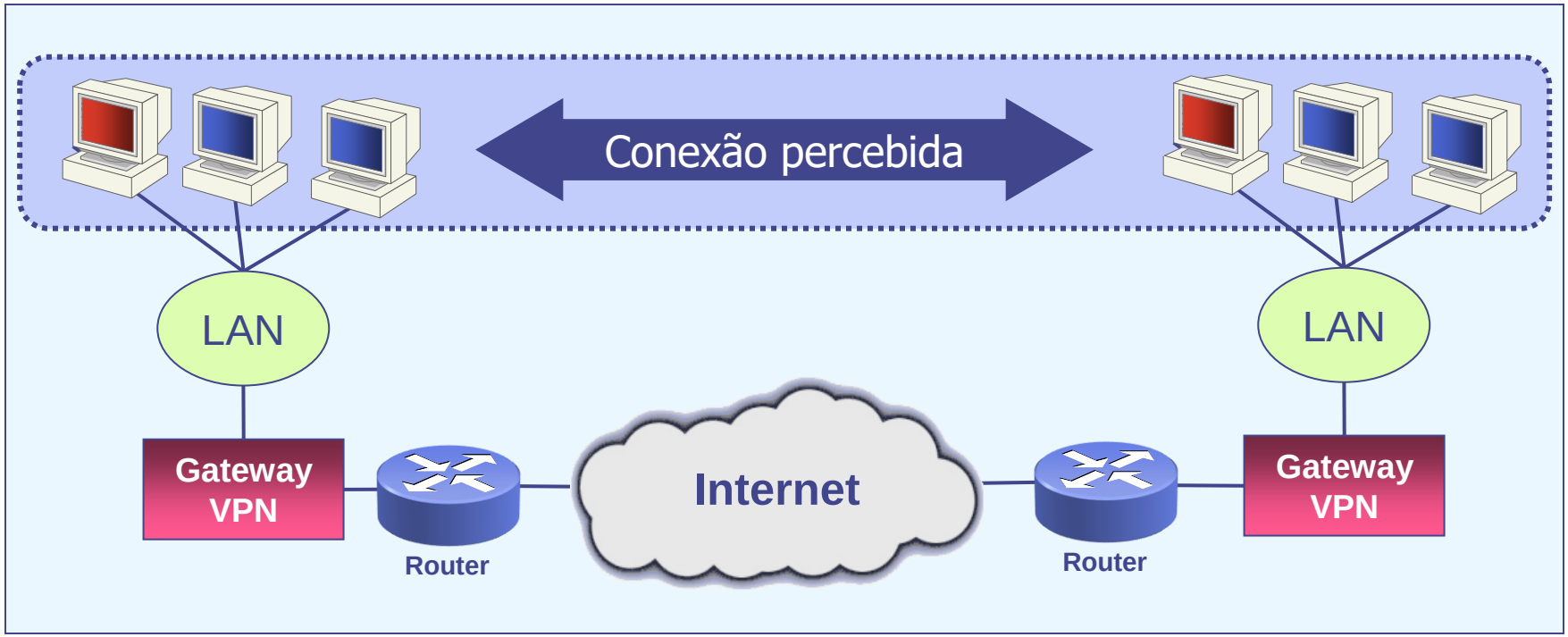
Topologias VPN

- Host-to-Network (ou "road warrior")
  - Host roda gateway VPN
  - Tráfego é ilegível do host até o Gateway VPN
  - Ex: Hosts móveis conectados remotamente (em casa)



Topologias VPN

- Network-to-Network
  - **Conecta 2+ LANs (intranets)**
  - **LAN remota na VPN é transparente para os hosts**
  - **Dados são ilegíveis entre os Gateways VPN**
  - **Dados são planos na rede interna**



VPN - Virtual Private Network

Protocolo IPSec

IPSec – Características de Segurança

- Autenticação
  - Verifica a identidade do remetente de cada pacote
- Proteção de Integridade
  - Garante que se os dados forem alterados em trânsito, a alteração será indentificada
- Replay Protection
  - Previne atacante de salvar pacotes criptografados e resubmetê-los depois sem ser detectado
- Confidencialidade
  - Esconde o tráfego transmitido aplicando criptografia com uma chave compartilhada entre os pares envolvidos

Estabelecendo um "Caminho Seguro"

- Para criar um caminho seguro (túnel) entre dois pontos eles precisam:
  - concordar com um conjunto de protocolos de segurança a usar.
  - decidir qual algoritmo de criptografia será usado.
  - trocar chaves públicas para criptografar mensagens
- Usando o túnel:
  - Basta enviar pacotes para a rede, de acordo com os protocolos e algoritmos combinados
  - Apenas os roteadores finais precisam de protocolos especiais e criptografia
  - Nenhum outro roteador da Internet é alterado
  - Nenhum roteamento especial é necessário

IPSec – Conceitos Básicos

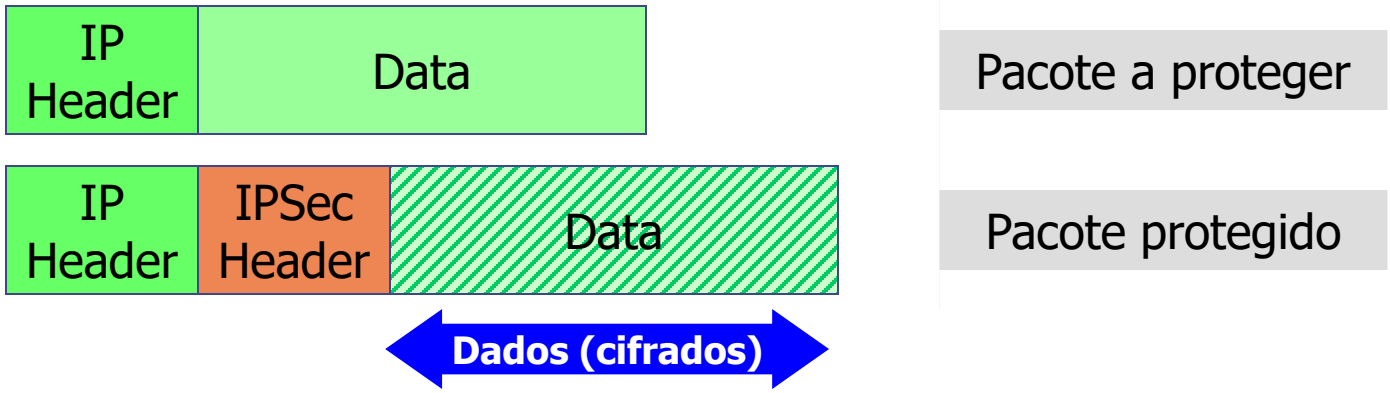
- SA - Secure Associations
  - Identifica uma conexão lógica entre dois pontos IPSec (um para cada sentido do trânsito)
  - Armazena informações necessárias para proteger dados na VPN (algoritmos, chaves, protocolos)
  - Cada pacote IPSec carrega um SPI - Secure Parameter Index, que indica qual SA usar
- SAD – Secure Associations Database
  - Armazena as várias SAs em uso pelo VPN Gateway
- SPD - Secure Policy Database
  - Um conjunto de regras e políticas
  - Usado para tomar decisões quanto ao que fazer com pacotes IP específicos (descartar, encaminhar plano, criptografar)

IPSec - Protocolos

- Baseado em vários protocolos (RFC 2401-2412)
- Protocolos de Gerenciamento de Chaves
  - IKE – Internet Key Exchange
  - ISAKMP – Internet Security Association and Key Management Protocol
- Cabeçalhos especiais
  - AH – Autentication Header
  - ESP – Encapsulating Security Payload
  - IPCOMP – IP Compression

IPSec – Modos de Operação

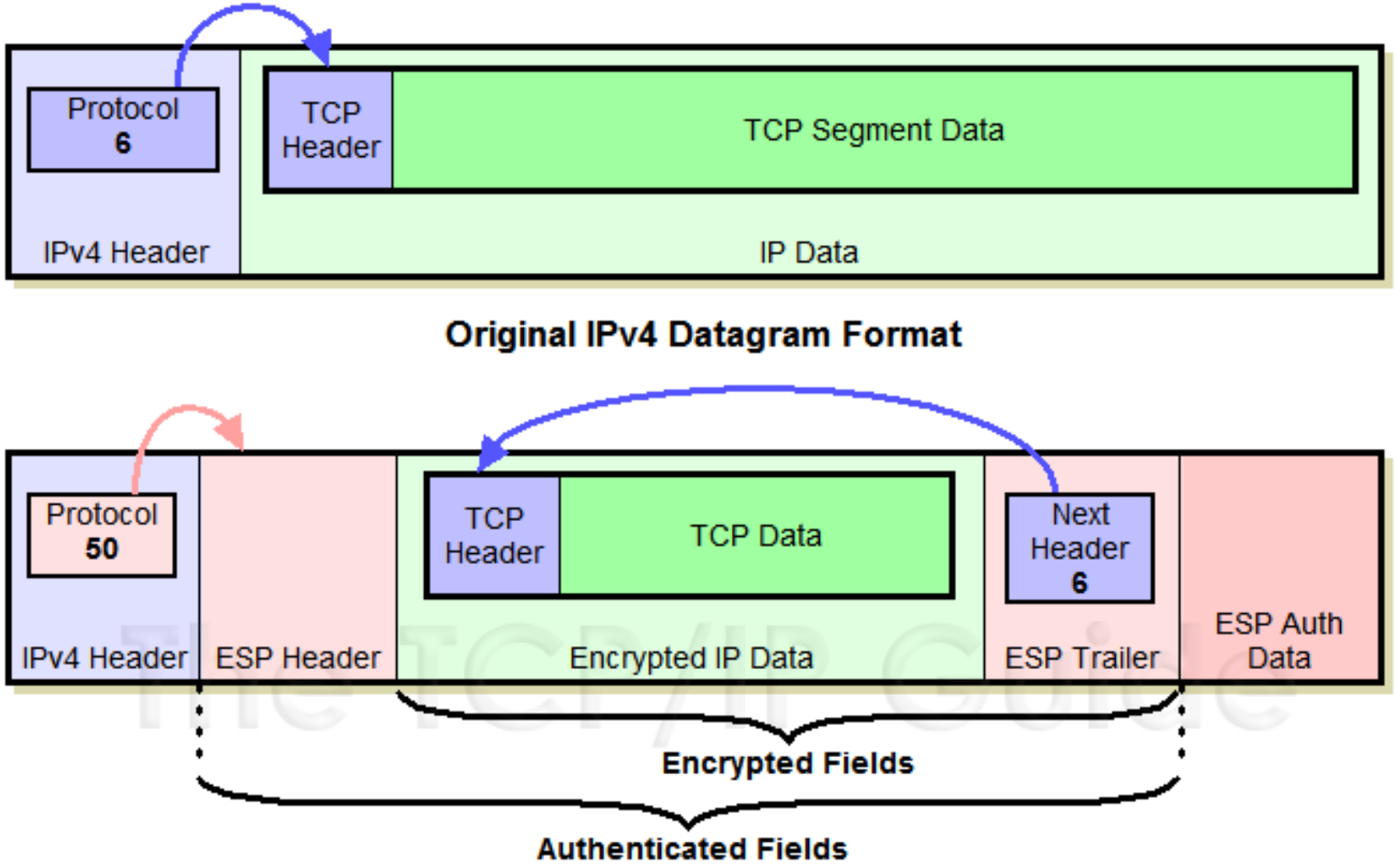
➔ Modo Transporte



➔ Modo Transporte

- Mantém o cabeçalho IP do pacote original
- Acrescenta um cabeçalho IPSec
- Cabeçalho IPSec pode conter assinatura dos dados
- Permite: verificação da integridade, autenticação da origem, não-repúdio, confidencialidade
- Não esconde informações do cabeçalho original

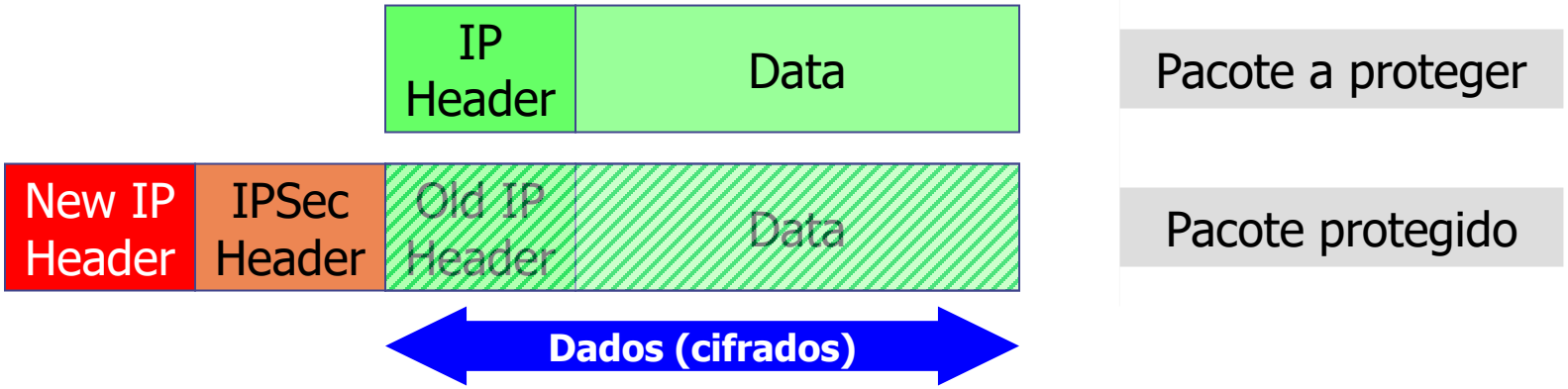
IPSec – Modo Transporte (detalhe)



http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-2.htm

IPSec – Modos de Operação

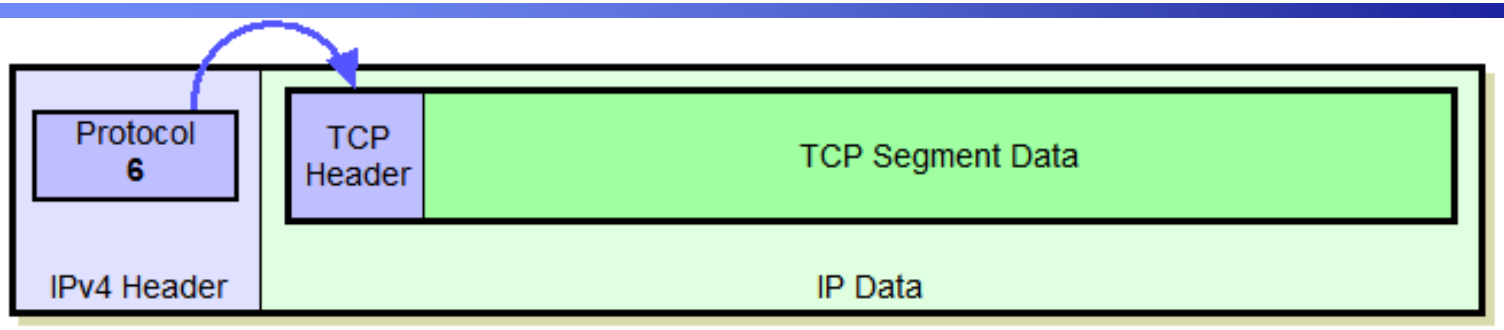
➔ Modo Túnel



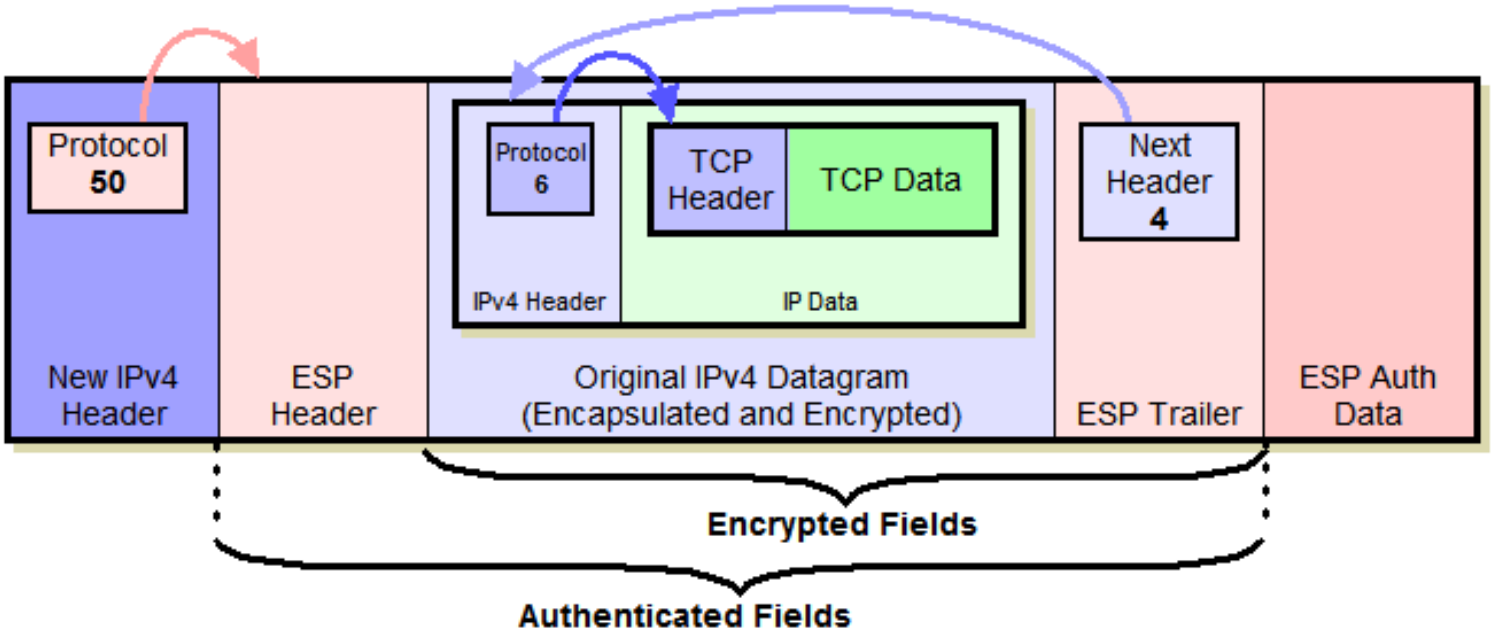
➔ Modo Túnel

- Pacote original é tratado como “dados a enviar”
- Acrescenta um novo cabeçalho IP + cabeçalho IPSec
- Permite: verificação da integridade, autenticação da origem, não-repúdio, confidencialidade
- Esconde completamente as informações do cabeçalho original
- Permite estender logicamente uma rede local (ex: duas redes IP com endereços privados podem se comunicar via Internet)

IPSec – Modo Túnel (detalhe)



Original IPv4 Datagram Format



http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP-2.htm

IPSec

Camada 2,5

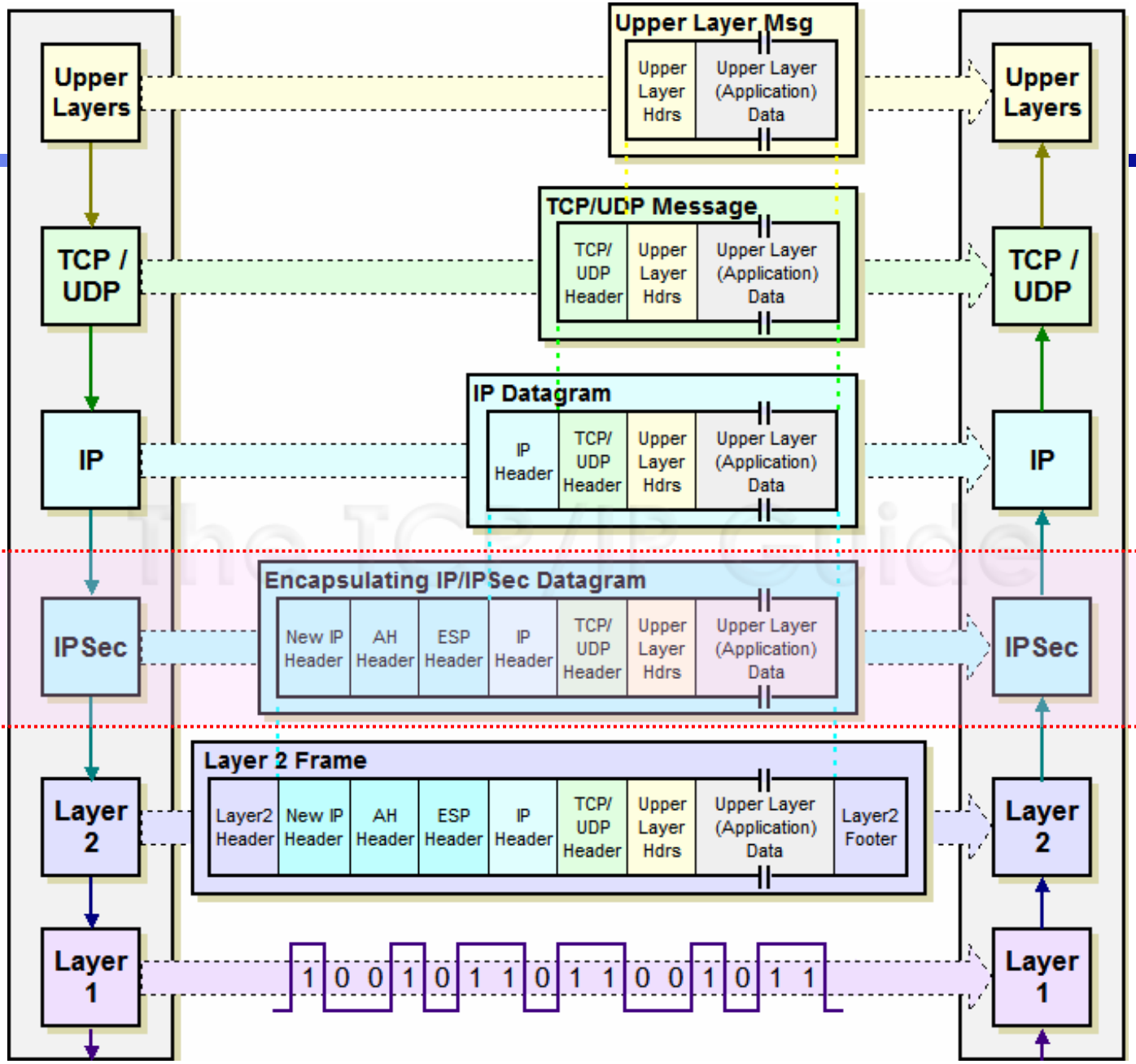


Figura: www.tcpipguide.com/free/t_IPSecModesTransportandTunnel-3.htm

VPN -- Resumo

- Mecanismo para implementar segurança sobre redes públicas
- Aumenta a complexidade do suporte
  - Gerenciamento de chaves
  - Configuração do IPSec + softwares (ex: Windows, Linux)
  - Configuração de gateways
- Aumento de cabeçalhos consomem banda adicional
- Precisa de ajustes no firewall
  - Protocolo 50 (Encapsulating Security Protocol (ESP)),
  - protocolo 51 (Authentication Header (AH)),
  - Porta UDP 500 (IKE), entre outros.
- Criptografia aumenta o atraso dos pacotes
  - Algumas placas de rede já têm CPU para criptografia
- Reduz custo
  - Usa a Internet que voce já tem
  - Existem boas soluções gratuitas ou de baixo custo
- Solução para redes de broadcast inseguras (ex: 802.11, Satélite)
- É o melhor método se voce precisa mesmo proteger seus dados na Internet (ex: entre filiais ou entre funcionário e empresa)

Leitura Adicional :-)

- RFC 1321 - The MD5 Message-Digest Algorithm
- RFC 1828 - IP Authentication using Keyed MD5
- RFC 1829 - The ESP DES-CBC Transform
- RFC 2040 - The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms
- RFC 2085 - HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2104 - HMAC: Keyed-Hashing for Message Authentication
- RFC 2207 - RSVP Extensions for IPsec Data Flows
- RFC 2268 - A Description of the RC2 Encryption Algorithm
- RFC 2367 - PF_KEY Key Management API, Version 2
- RFC 2401 - Security Architecture for the Internet Protocol (**IPsec**)
- RFC 2402 - IP Authentication Header (**AH**)
- RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404 - The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2405 - The ESP DES-CBC Cipher Algorithm With Explicit IV
- RFC 2406 - IP Encapsulating Security Payload (**ESP**)
- RFC 2407 - The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 - Internet Security Association and Key Management Protocol (**ISAKMP**)
- RFC 2409 - The Internet Key Exchange (**IKE**)
- RFC 2411 - IP Security Document Roadmap
- RFC 2412 - The OAKLEY Key Determination Protocol
- RFC 2451 - The ESP CBC-Mode Cipher Algorithms
- RFC 2631 - Diffie-Hellman Key Agreement Method
- RFC 2709 - Security Model with Tunnel-mode IPsec for NAT Domains