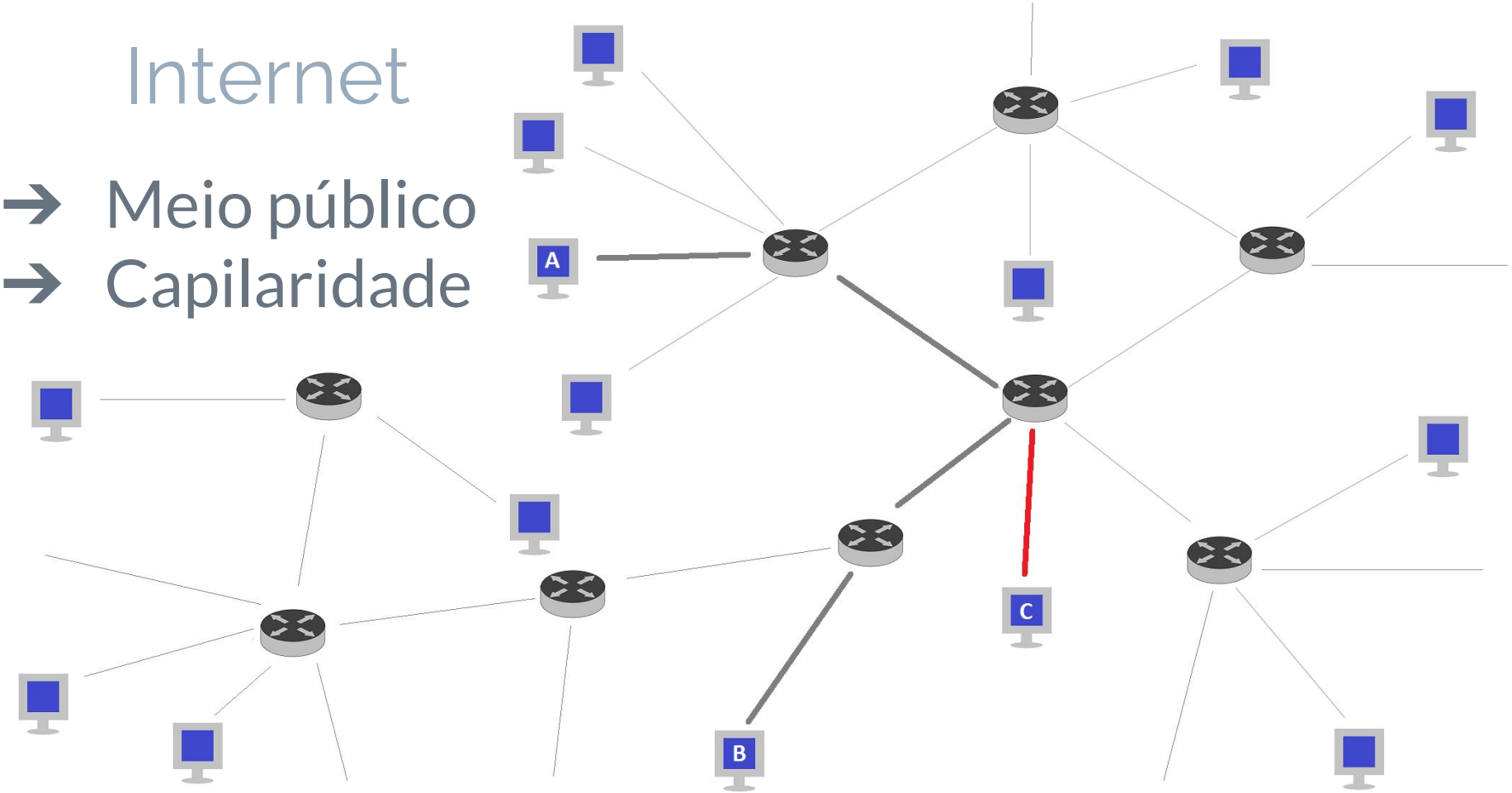
Redes Virtuais Privadas e IPSec

Caio César Riqueza Ramos

Universidade Federal Do Rio de Janeiro
Redes de Computadores I - 2016/1

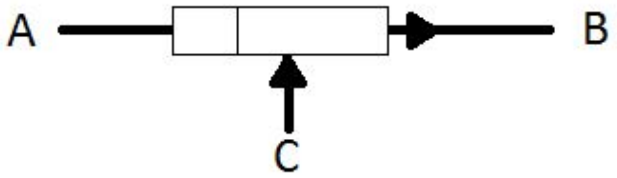
Internet

- Meio público
- Capilaridade



Tipos de ataque

- Replay
- Spoofing
- Connection hijacking
- Sniffing



Soluções

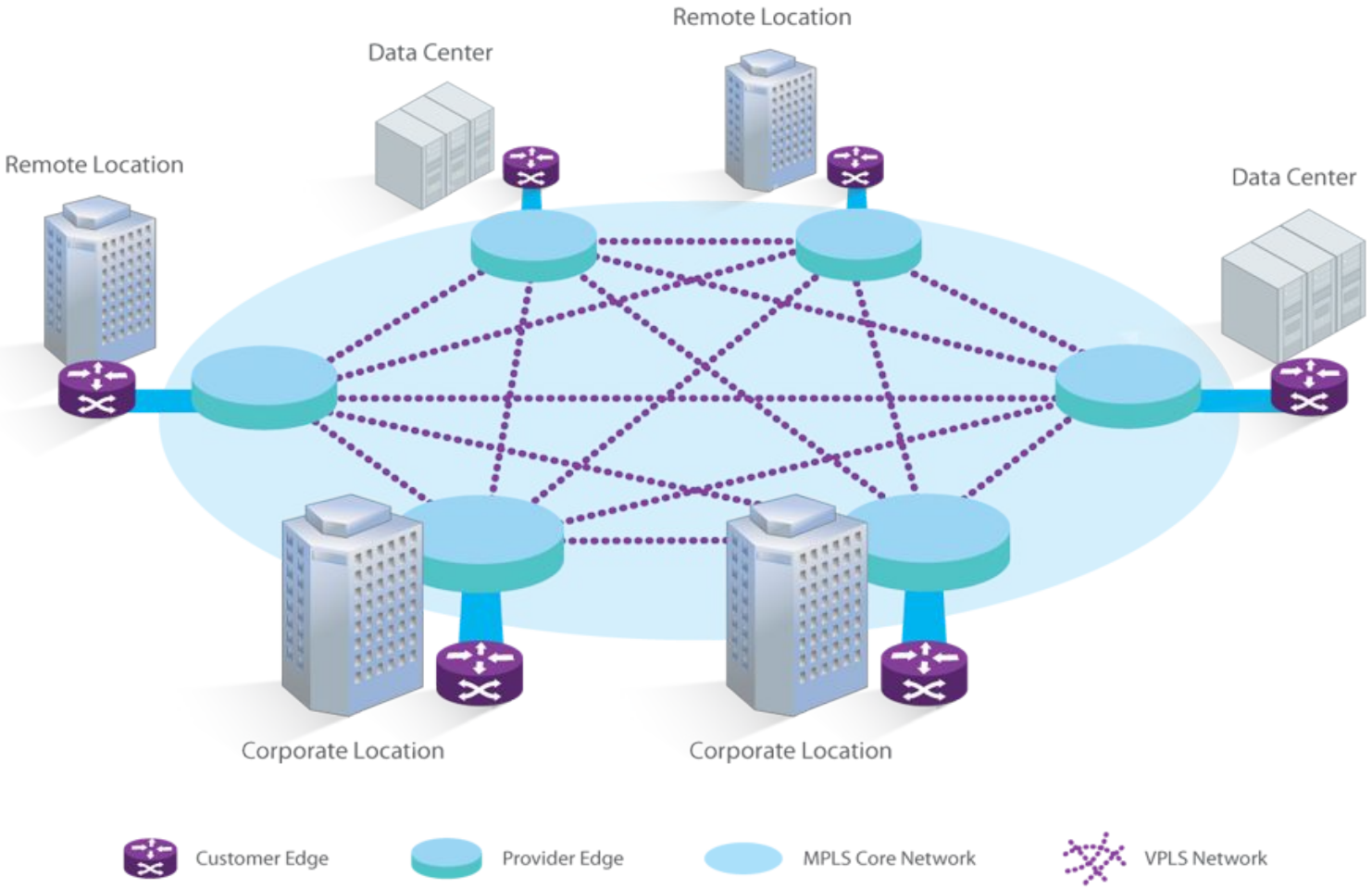
- ➔ Link direto
- ➔ De alguma maneira utilizar o TCP/IP de forma segura… VPN!

Abordagem

- ➔ Visão geral VPN
- ➔ Aplicações
- ➔ Segurança
- ➔ IPSec
- ➔ Arquitetura do IPSec
- ➔ Construção de uma VPN utilizando IPSec

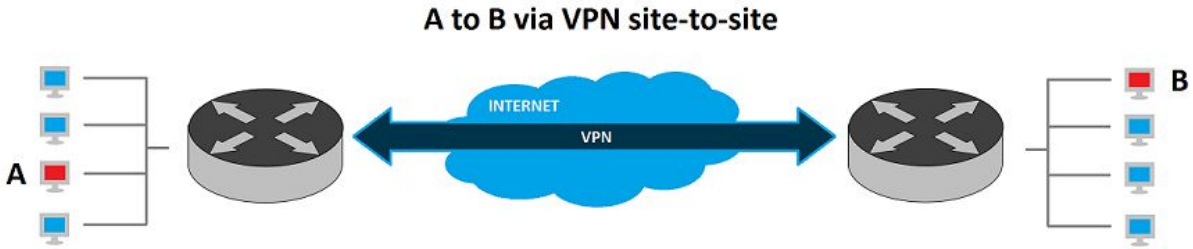
VPN - O que é?

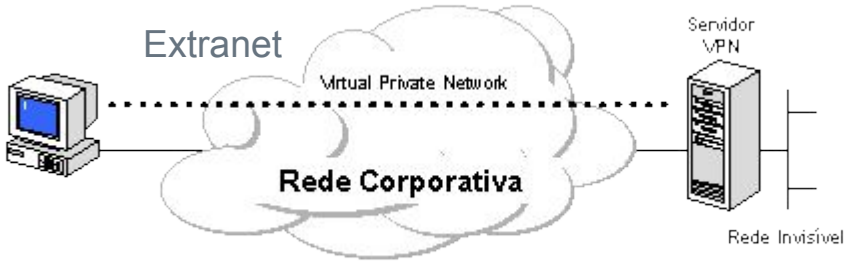
- Túnel virtual em meio público
- Site-to-site ou client-to-site
- Pode emular diversos tipos de rede
  - VLL - Virtual Leased Line
  - VPRN - Virtual Private Routed Network
  - VPDN - Virtual Private Dial Network
  - VPLS - Virtual Private LAN Network

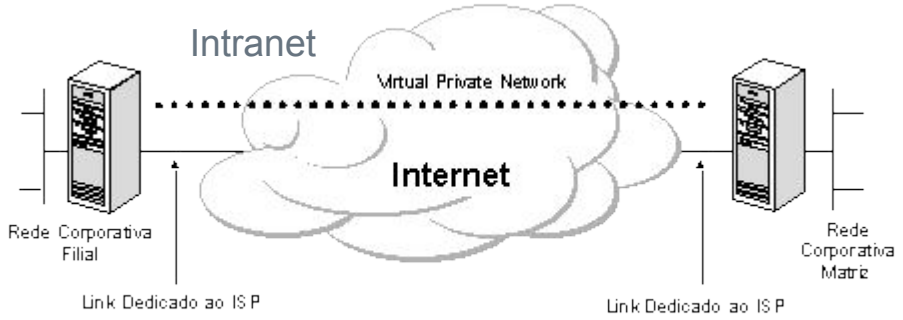


Exemplo de VPLS. Retirado de www.xo.com

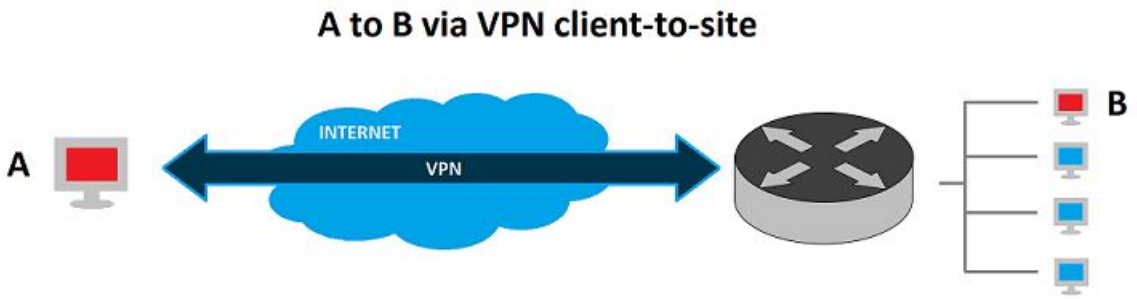
VPN Site-to-site



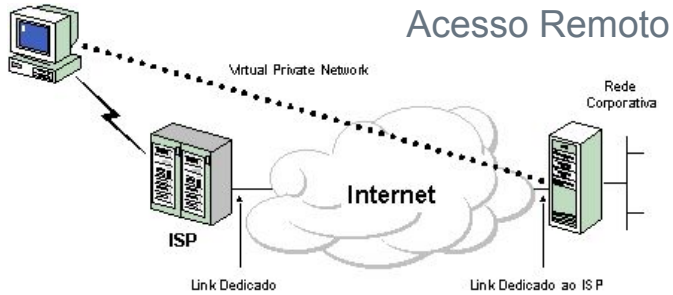




VPN Client-to-site

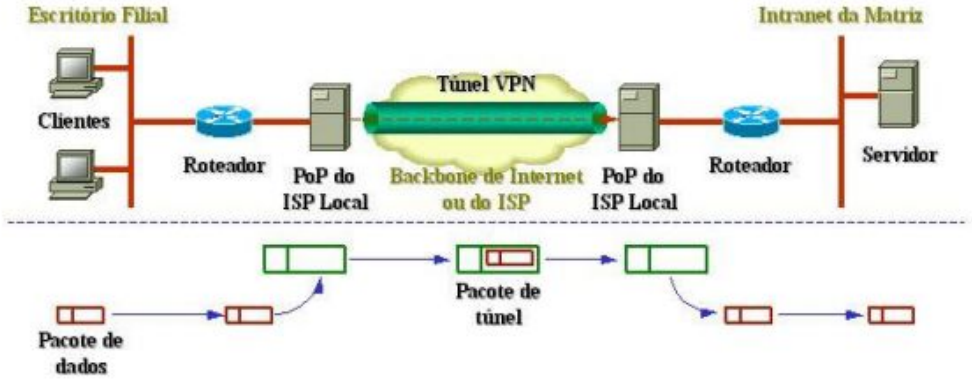


Acesso Remoto



VPN - Elementos

- ➔ Tunelamento
- ➔ Autenticação das extremidades
- ➔ Transporte subjacente



Visão geral de uma VPN - Retirada de Redes Privadas Virtuais - Pedro Celestino

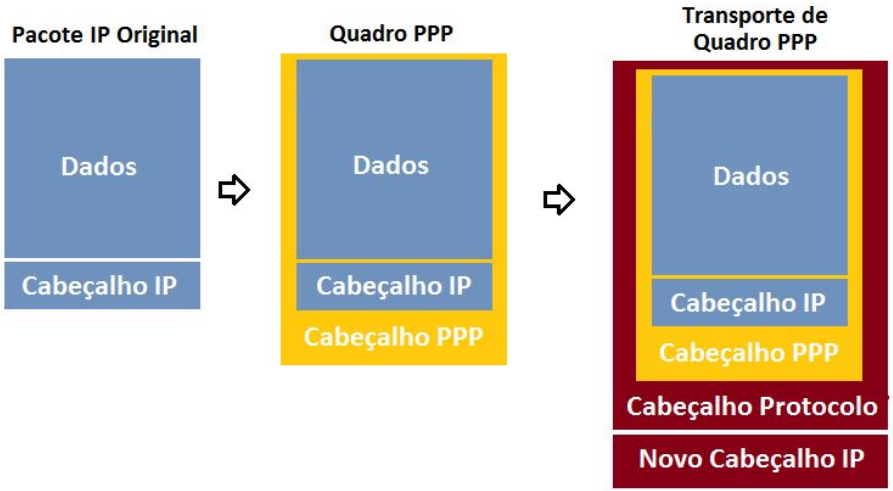
VPN - Segurança

- ➔ Confidencialidade
- ➔ Integridade
- ➔ Autenticidade
- ➔ Anti-Replay
- ➔ AAA(Authentication, Authorization, Accounting)
- ➔ Não-repúdio

VPN - Tunelamento

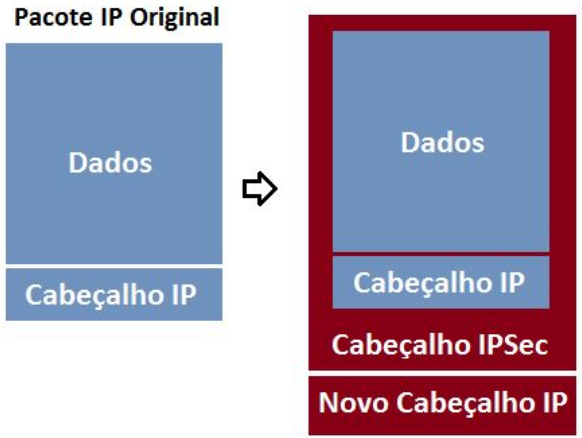
Camada 2 (Enlace):

➔ L2TP, PPTP, L2F e MPLS



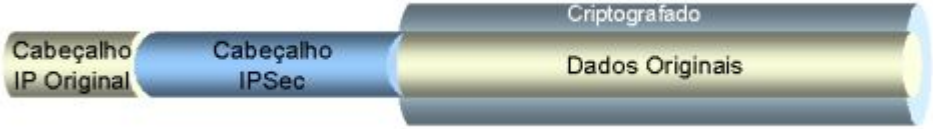
Camada 3 (Rede):

➔ IPSec



IPSec

➔ Modo Transporte



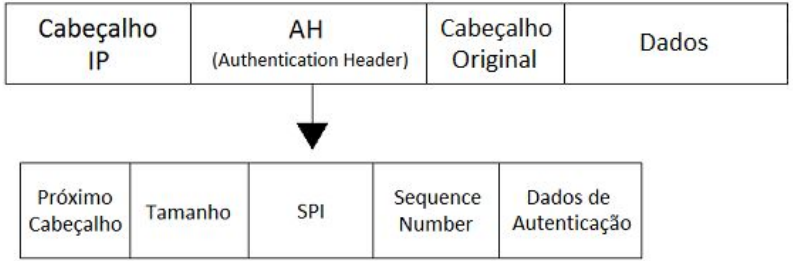
IPSec modo Transporte - Retirada de Redes Privadas Virtuais - Pedro Celestino

➔ Modo Túnel

IPSec modo Túnel - Retirada de Redes Privadas Virtuais - Pedro Celestino

IPSec

➔ Authentication Header(AH)



- Integridade
- Anti-Replay
- Autenticidade

➔ Encapsulating Security Payload(ESP)

- Integridade
- Anti-Replay
- Autenticidade
- Confidencialidade

Cabeçalho IPSec

- ➔ Dados de autenticação(hash)
- ➔ SPI: índice da associação de segurança
- ➔ Número de sequência

IPSec - Associação de Segurança

- Conceito mais importante de IPSec
- Conjunto de regras preestabelecidas
  - Algoritmo de autenticação
  - Algoritmo de criptografia
  - Tempo de vida útil
- Gerenciamento de chaves?

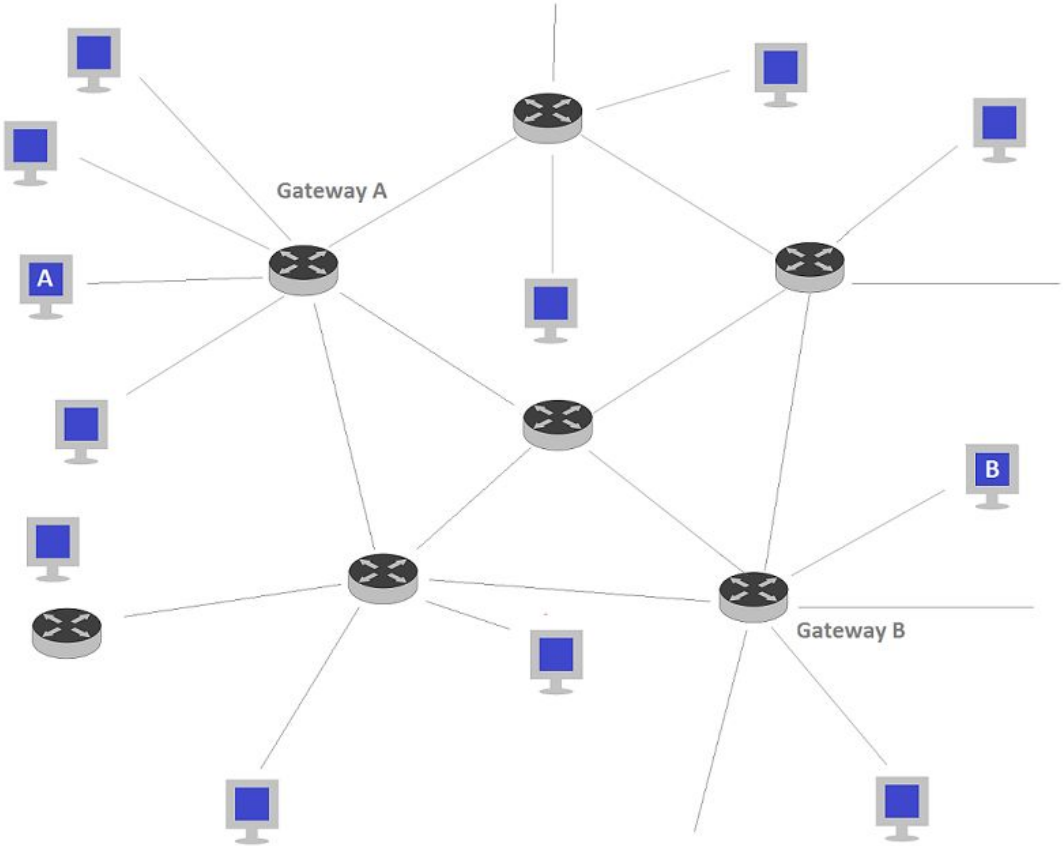
IPSec - Internet Key Exchange (IKE)

- Gerenciamento de chaves
- Define a associação de segurança
- Dividido em 2 fases:
  - Fase 1 - Diffie-Hellman para estabelecer a IKE SA
  - Fase 2 - Na IKE SA, estabelece o IPSec SA

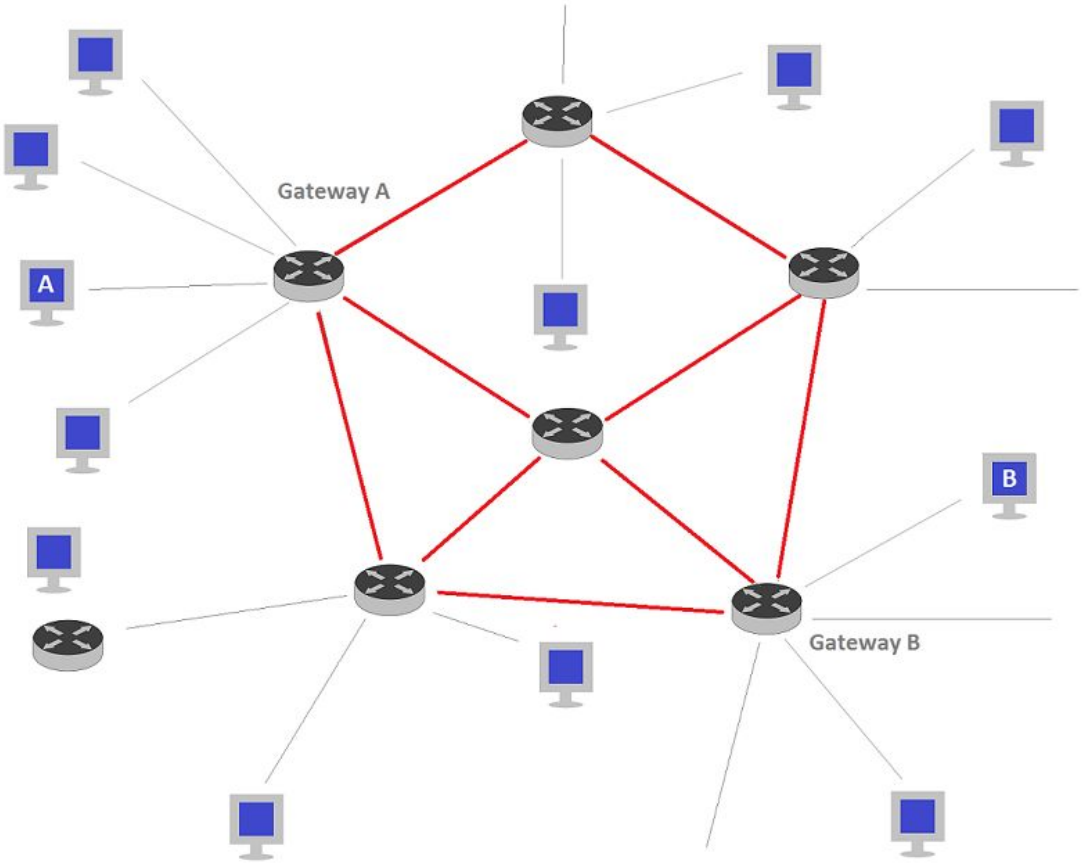
IPSec - Recapitulando

- Modo túnel/transporte
- AH, ESP ou os dois
- Associação de segurança (Túnel)
  - Conjunto de regras(configurações acima)
  - Algoritmos de criptografia/autenticação
- IKE (Construtor)
  - Gerenciamento de chaves
  - Fase 1 e Fase 2;

Construção de VPN com IPSec



Construção de VPN com IPSec



Construção de VPN com IPSec

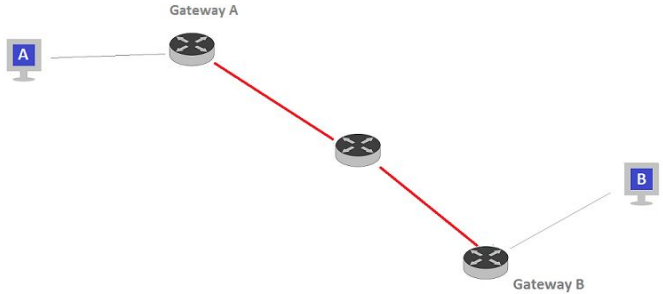
➔ Definir o caminho

access-list 101 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255

Access lists determine traffic to encrypt.

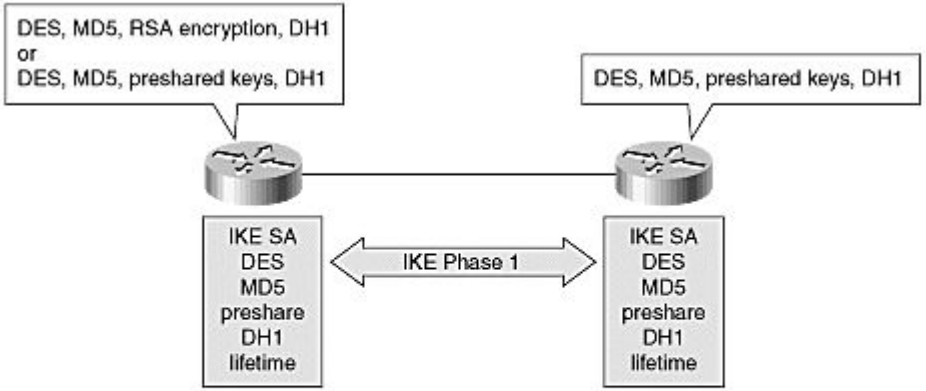
- Permit—Traffic must be encrypted.
- Deny—Traffic sent unencrypted.

Retirada de CiscoPress by Andrew Manson



Construção de VPN com IPSec

➔ IKE Fase 1



- Authenticates IPSec peers
- Negotiates matching policy to protect IKE exchange
- Exchanges keys via Diffie-Hellman
- Establishes IKE security association

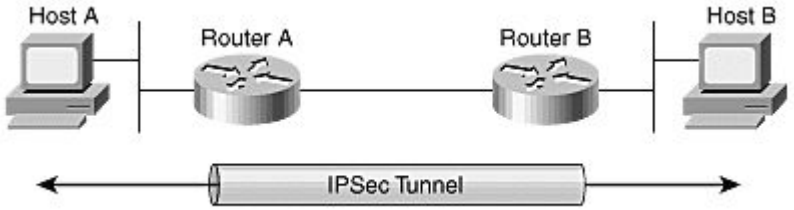
Retirada de CiscoPress by Andrew Manson

Construção de VPN com IPSec

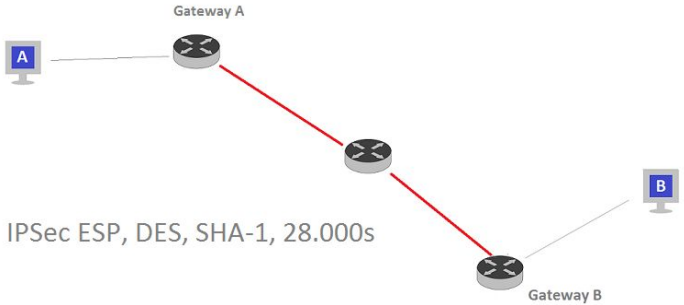
- IKE Fase 2
  - ESP;
  - AH;
  - Algoritmo de Criptografia(DES, 3DES, AES);
  - Algoritmo de Autenticação(MD5, SHA-1);
  - Tempo de vida do IPSec SA;

Construção de VPN com IPSec

- Troca de dados



Retirada de CiscoPress by Andrew Manson



- SA é unidirecional!

Perguntas

- Quais os conceitos de segurança geralmente presentes em uma VPN?

Perguntas

- Em quais camadas do modelo OSI pode ser feito o tunelamento de uma VPN? E quais são os protocolos que existem para cada camada?

Perguntas

➔ Por que o protocolo IPSec é considerado melhor que os outros?

Perguntas

- Quais são as fases de construção de uma VPN utilizando o protocolo IPSec?

Perguntas

➔ Como funciona o IPSec no modo túnel? (Qual estrutura)