Instituto Superior de Tecnologia em Ciências da Computação de Petrópolis

VPN
Virtual Private Network

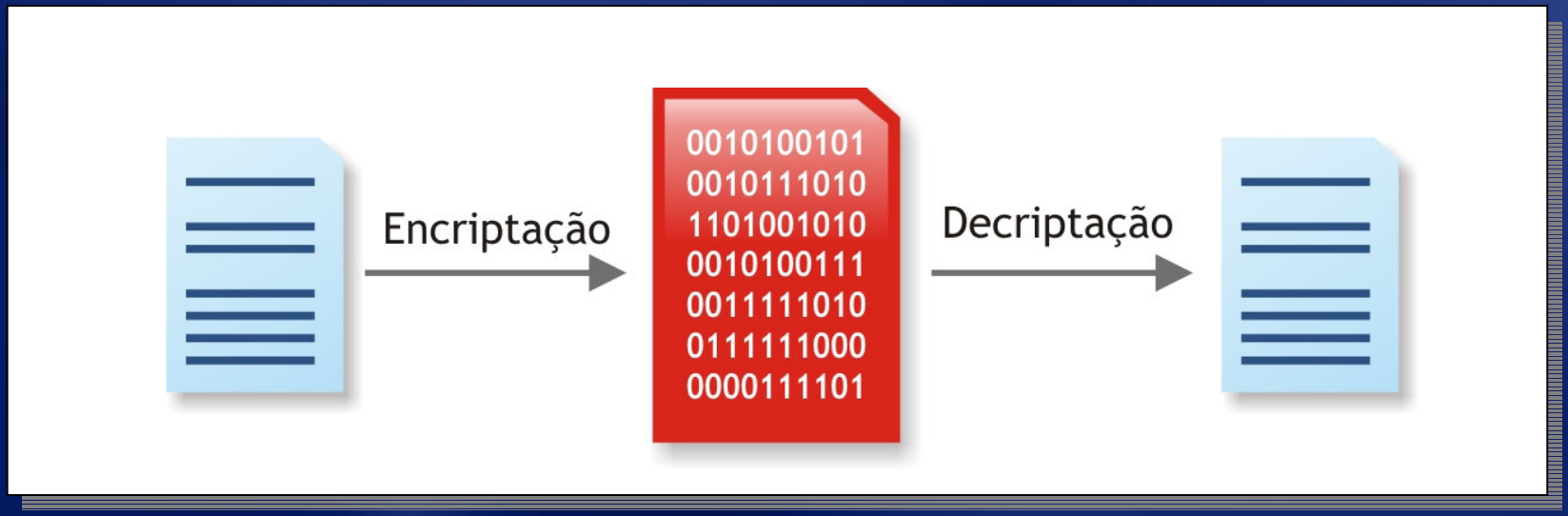
Por: Bruno Fagundes

Segurança

- Confidencialidade;
- Integridade;
- Autenticidade;
- Disponibilidade;

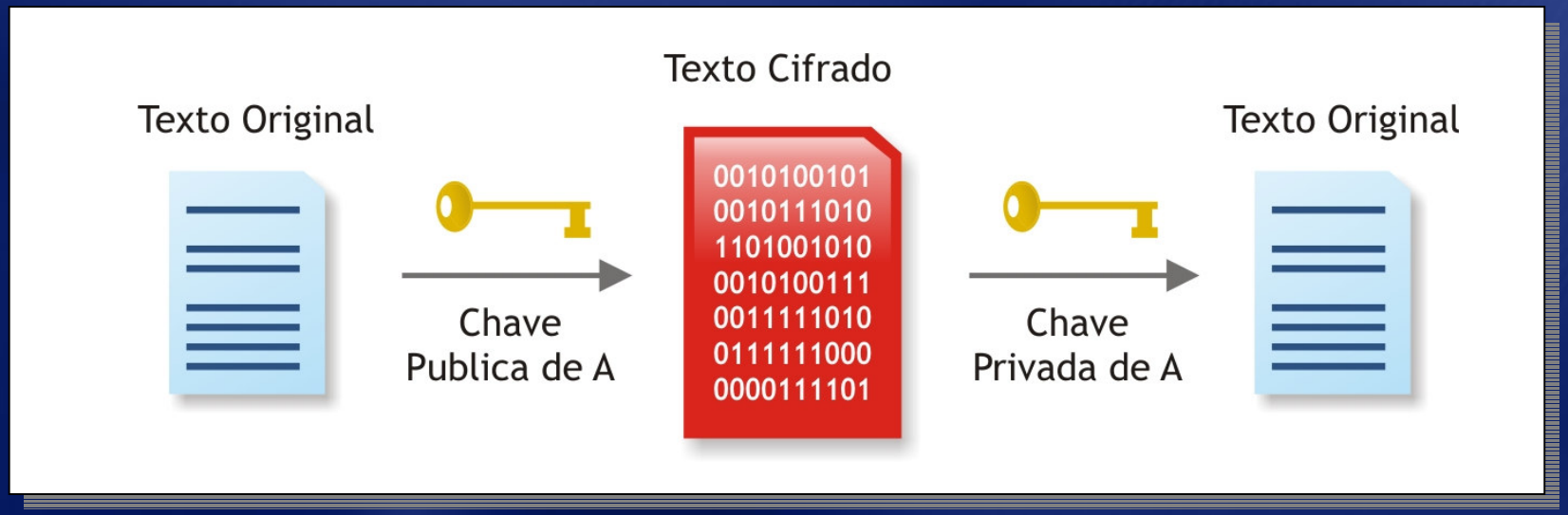
Criptografia

- Criptografia de bloco;
- Criptografia de fluxo;
- Simétrica
  - Algoritmos: AES, RC4, 3DES;



Criptografia

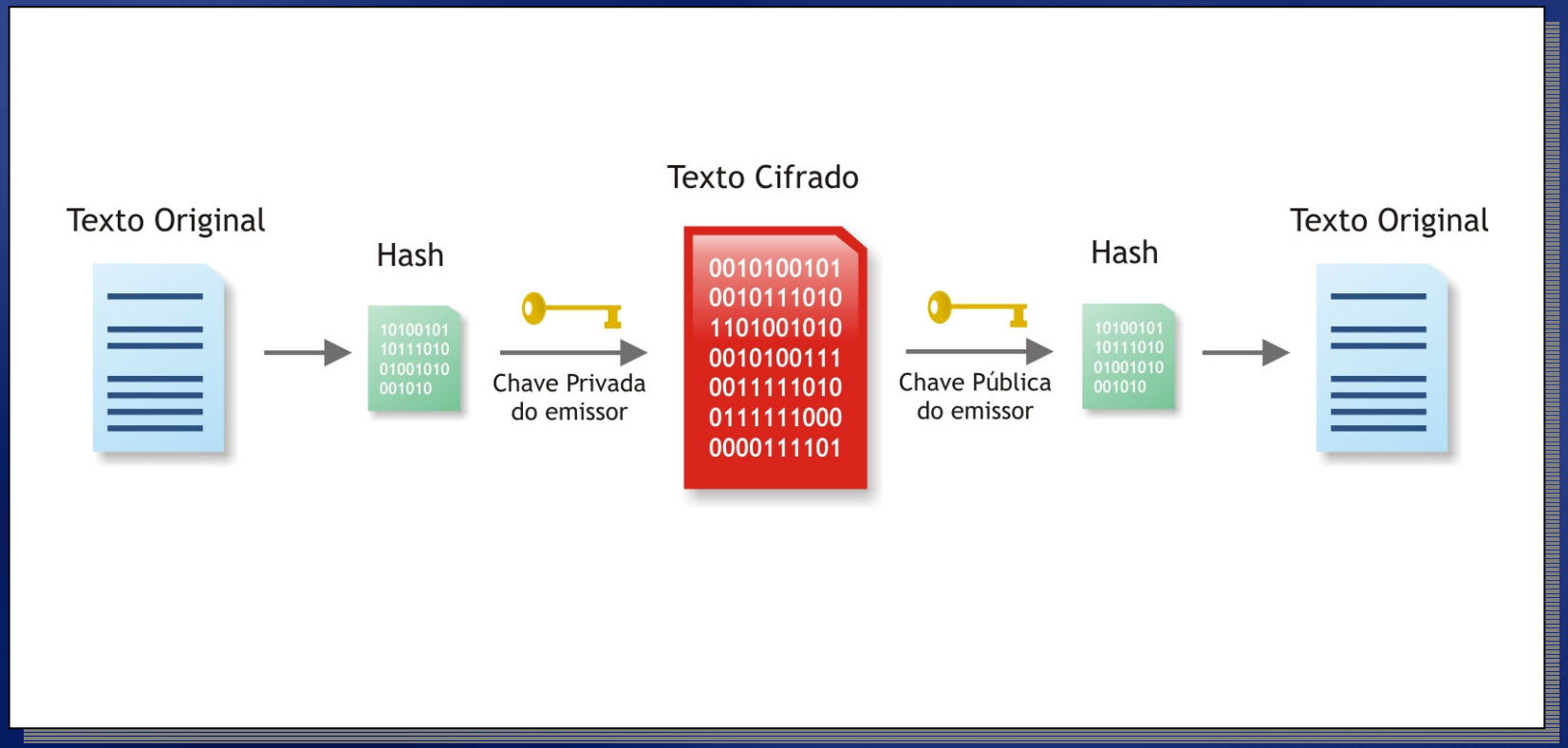
- Assimétrica
  - Chaves públicas e chaves privadas;
  - Algoritmos: ECC, RSA;
- Vantagens / Desvantagens



Hash

- Características
  - Mapeia um valor de entrada em um valor de saída; Não existe correlação direta entre estes valores; A saída possui um tamanho fixo.
- Propriedades
  - A partir do hash é desejável que não seja possível descobrir a mensagem original; É improvável que se encontrem duas mensagens com o mesmo hash.
- Algoritmos: MD5, SHA-1, SHA-2

Assinatura Digital



Ataques

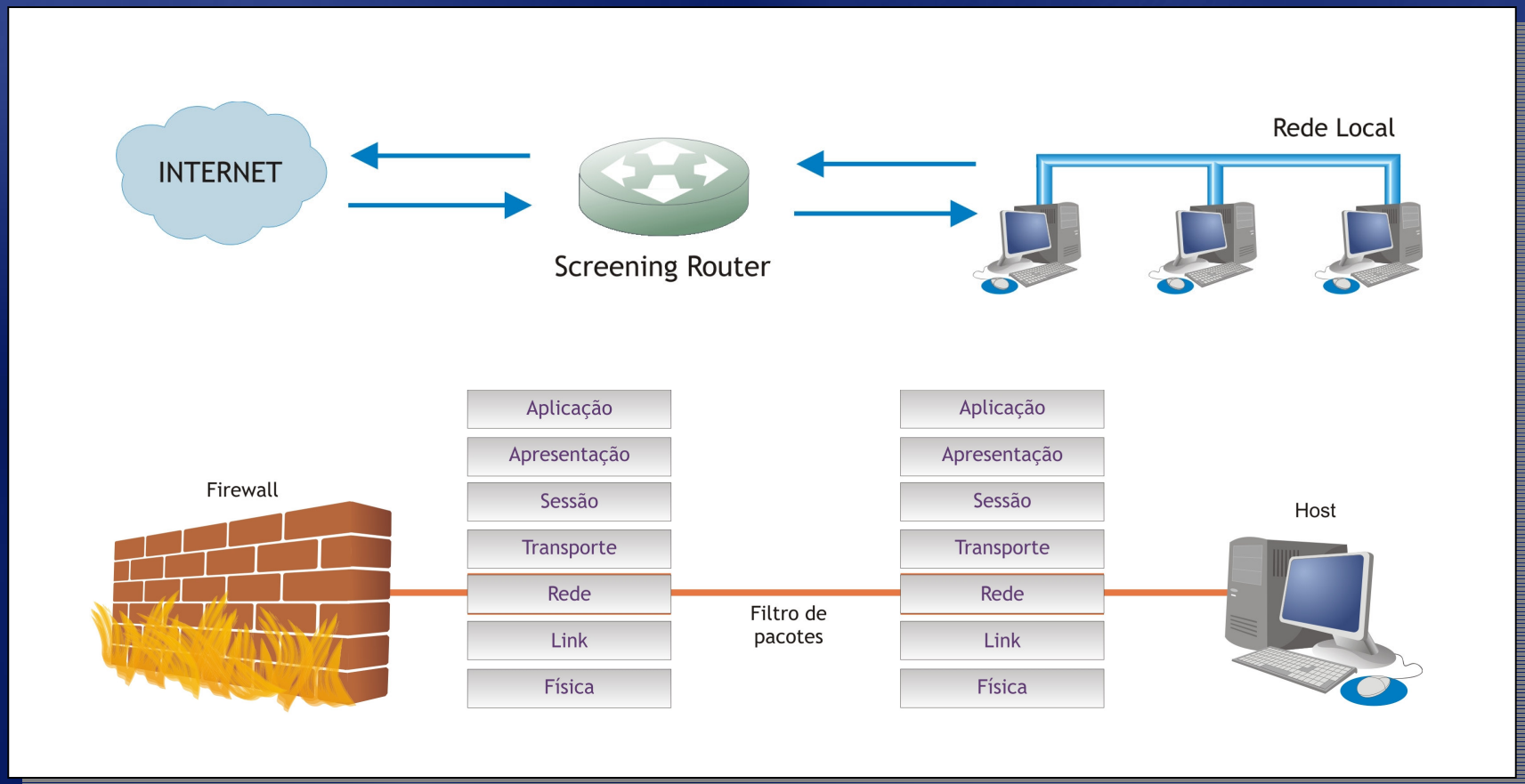
- Engenharia Social;
- Criptoanálise;
- Força bruta;
- Men-in-the-middle;
- Replay;

Firewall

- O que um firewall pode fazer?
- O que um firewall não pode fazer?
- Conceitos
  - Bastion host;
  - DMZ;

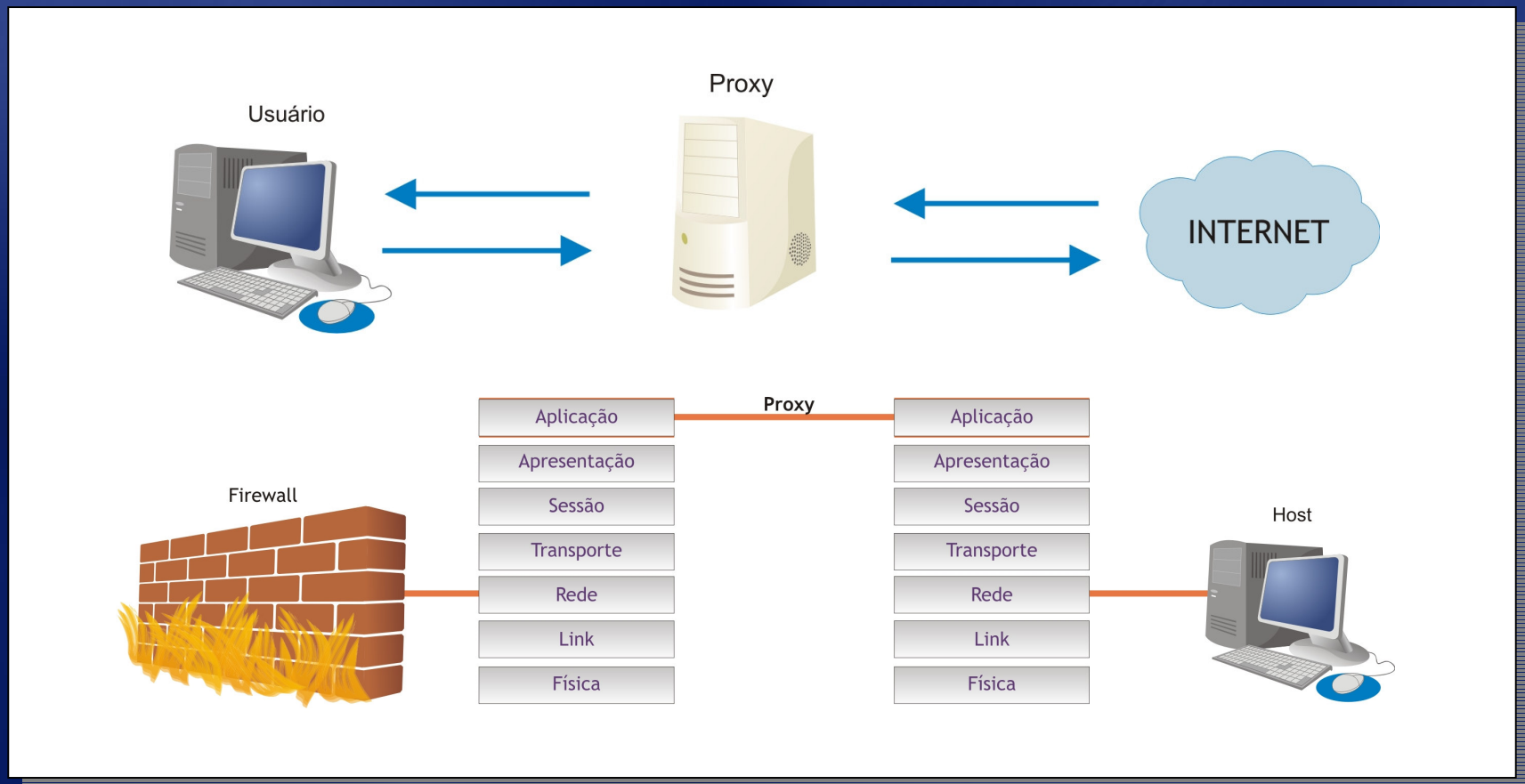
Firewall

- Filtro de pacotes



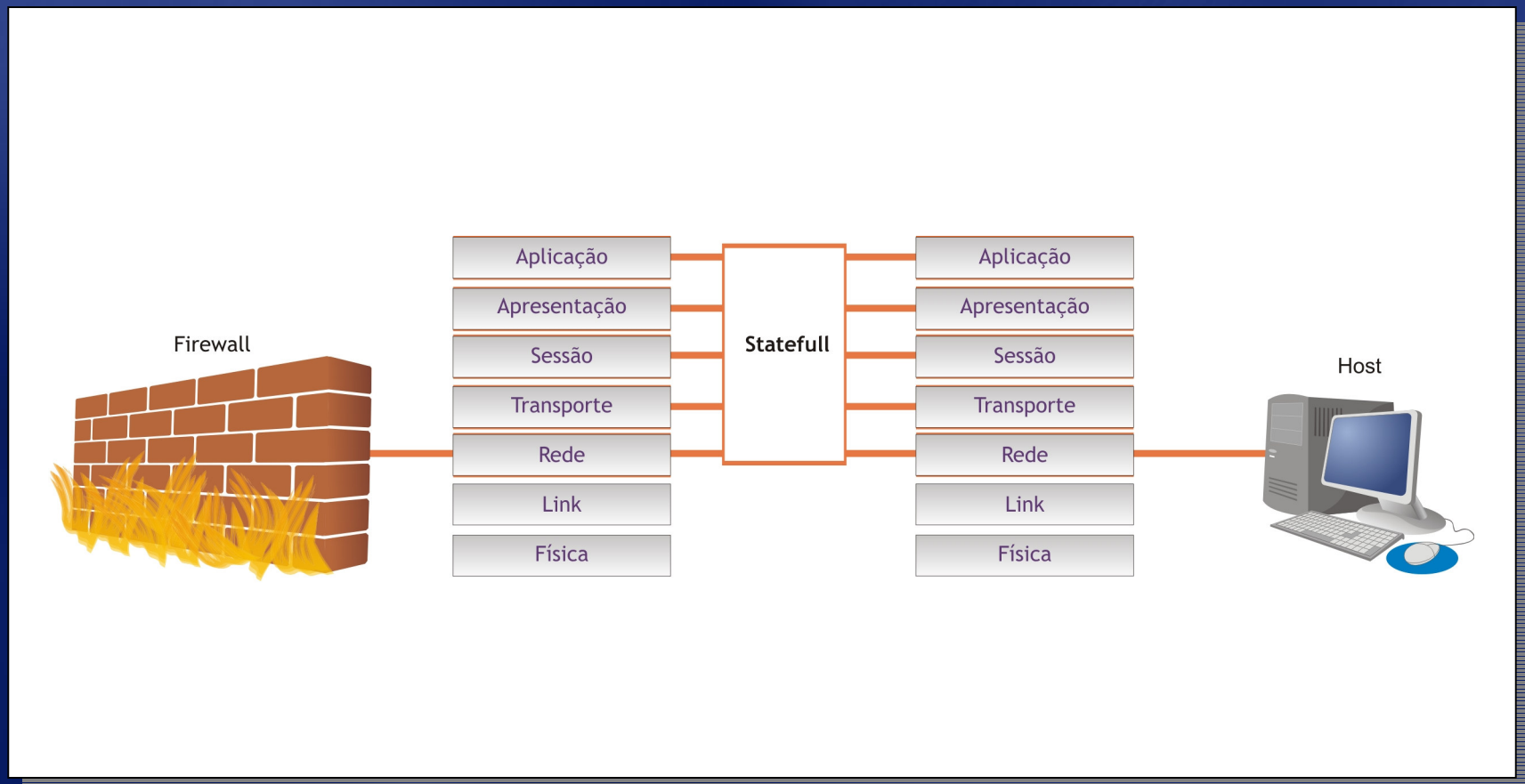
Firewall

- Servidor Proxy e Proxy Cache



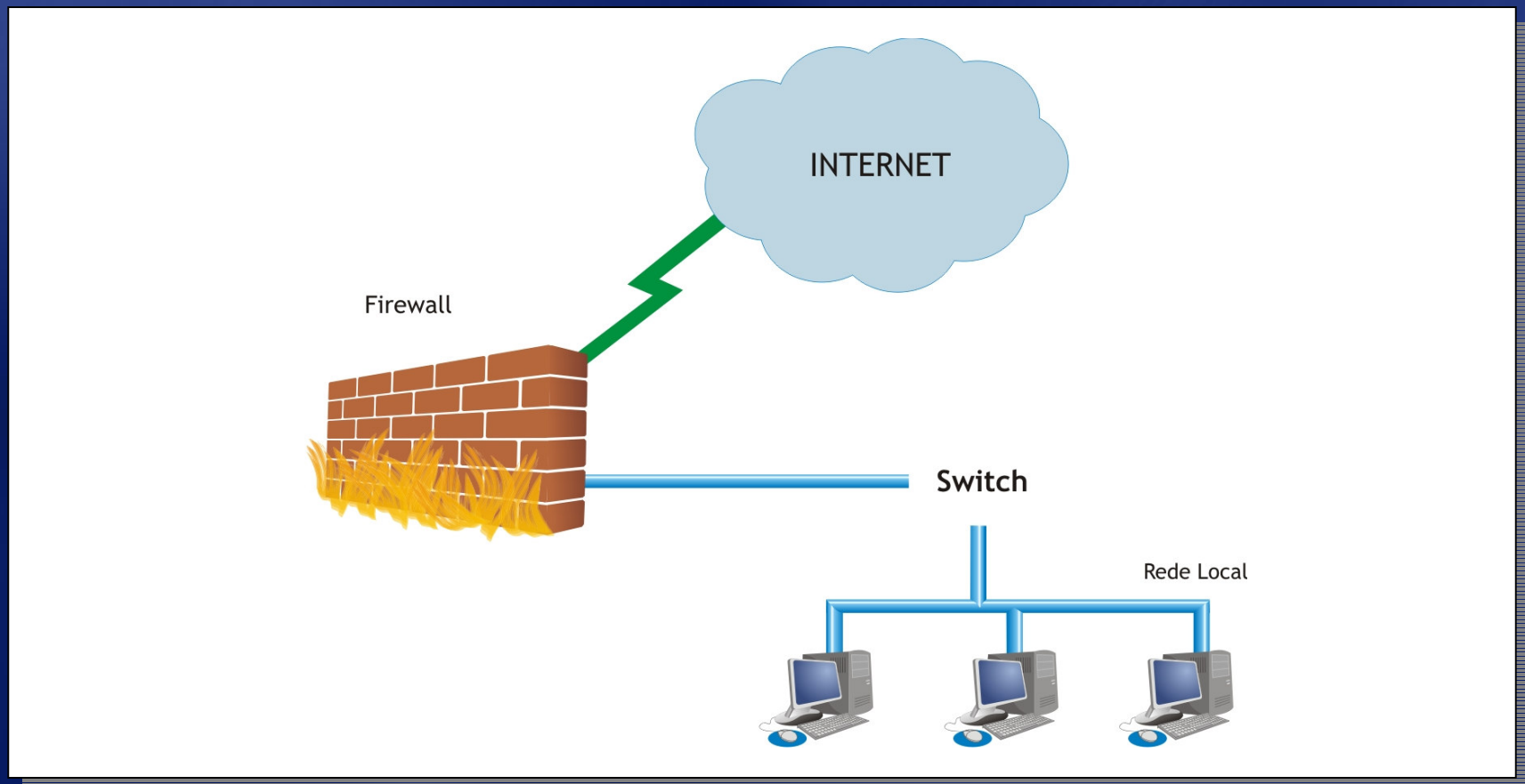
Firewall

- Statefull



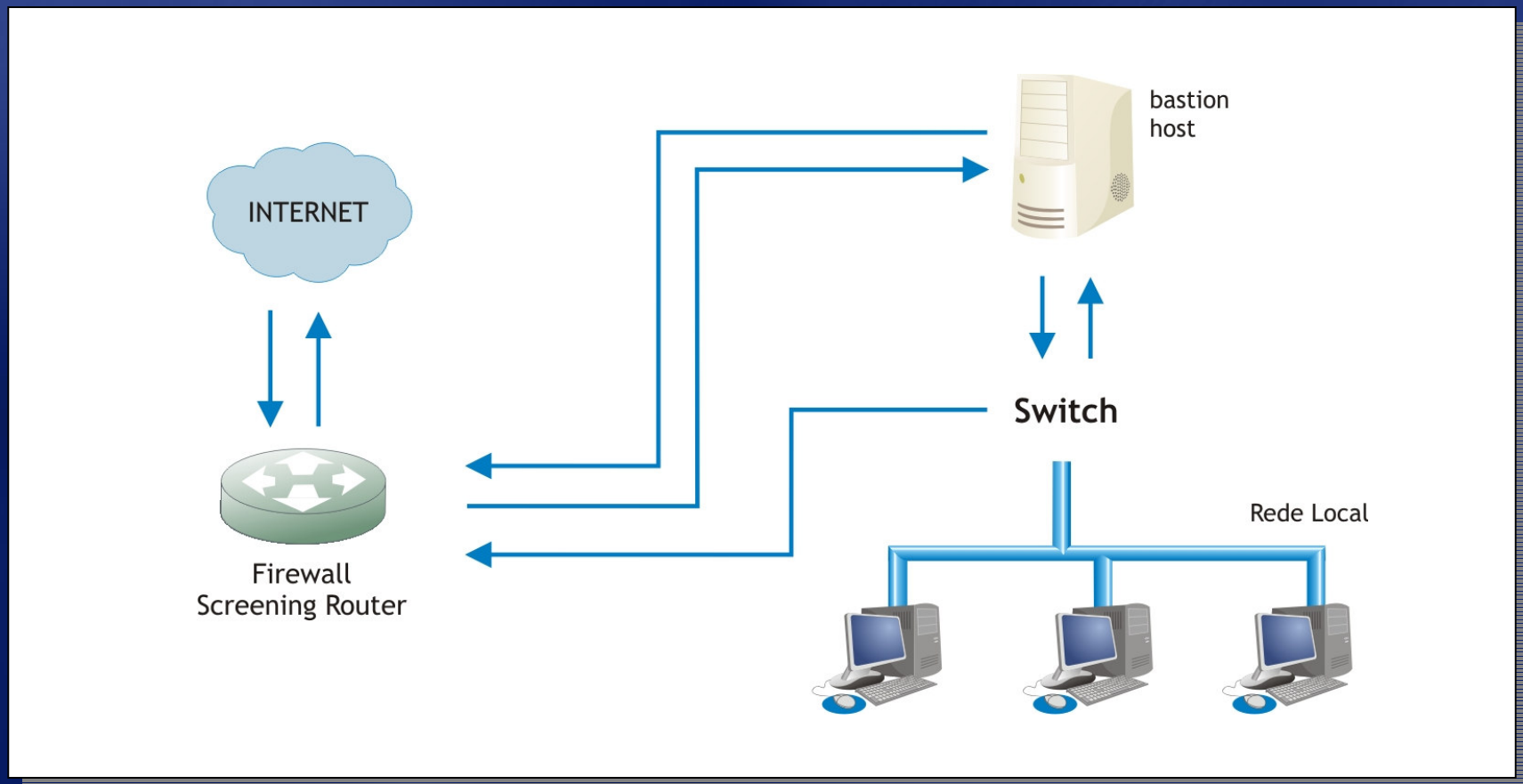
Firewall

- Dual homed-host



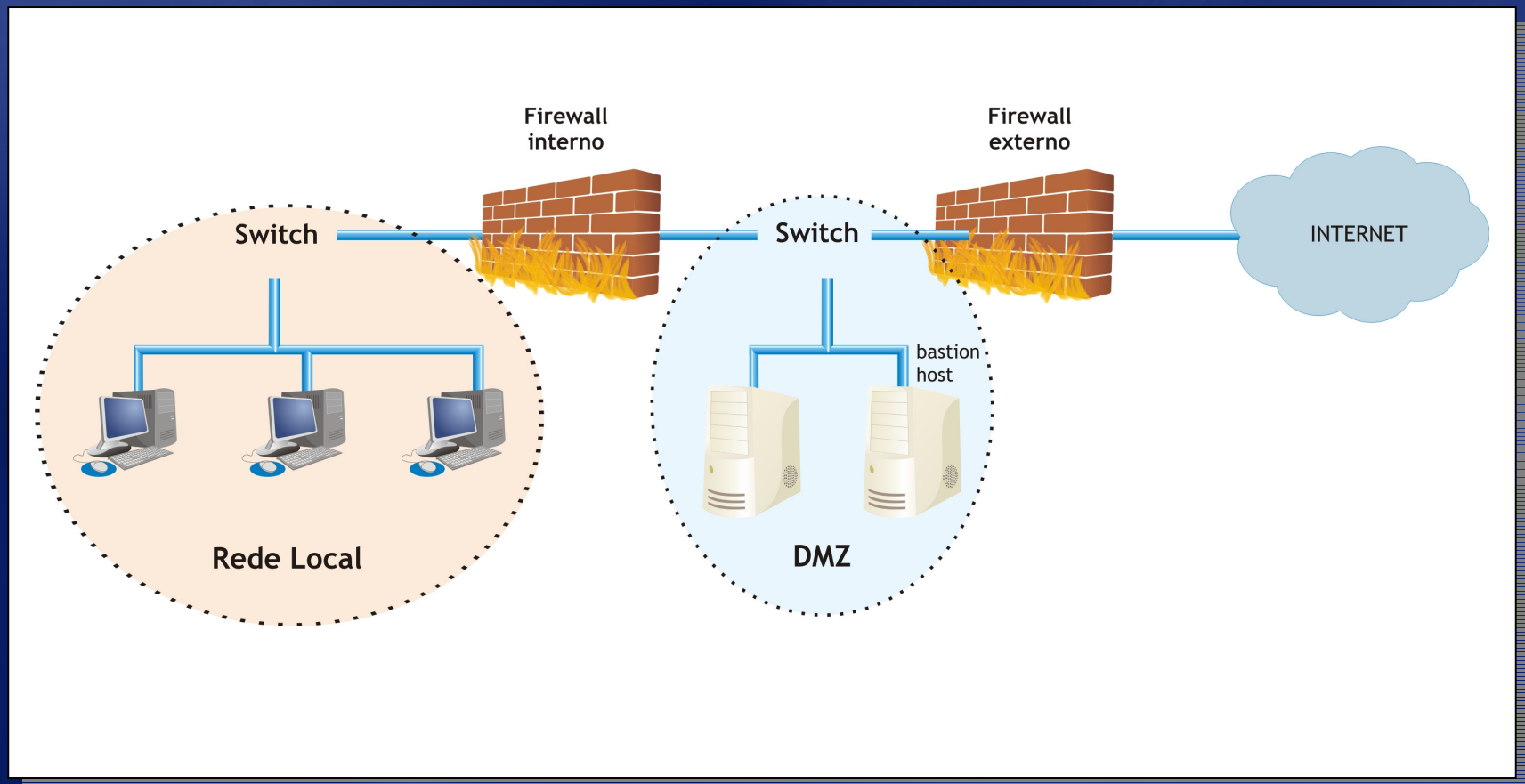
Firewall

- Screened host



Firewall

- Screened Subnet

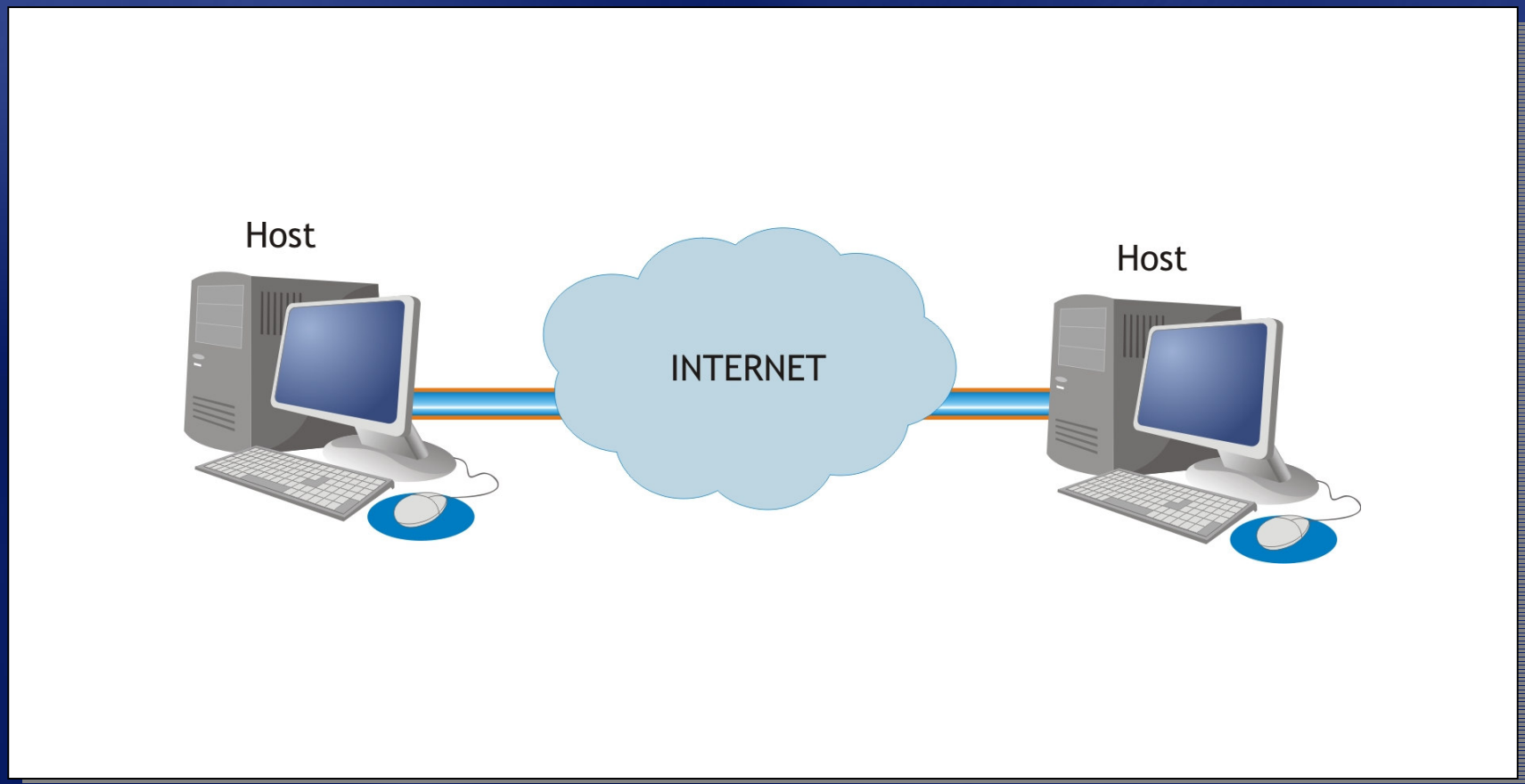


VPN

- Motivação;
- Tunelamento;
  - Forma como os dados trafegam pela conexão. O pacote é criptografado e encapsulado dentro de outro pacote e então enviado.
- Autenticação das extremidades;
  - Garantir que somente usuários autorizados possam utilizar o serviço.
- Transporte subjacente.
  - Adição de novos cabeçalhos aos pacotes permitindo sua instalação em qualquer ponto da rede.

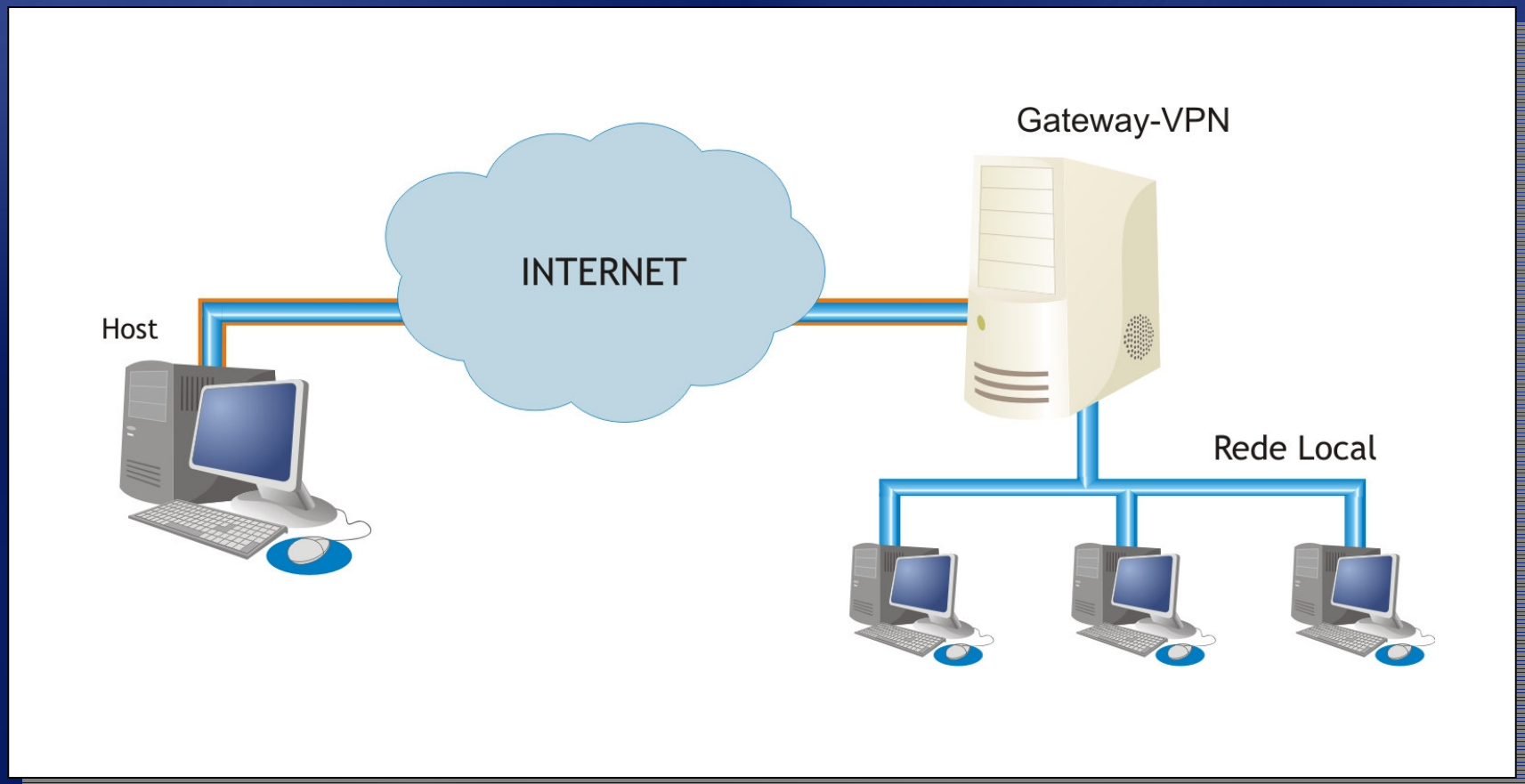
VPN

- Topologia host-host



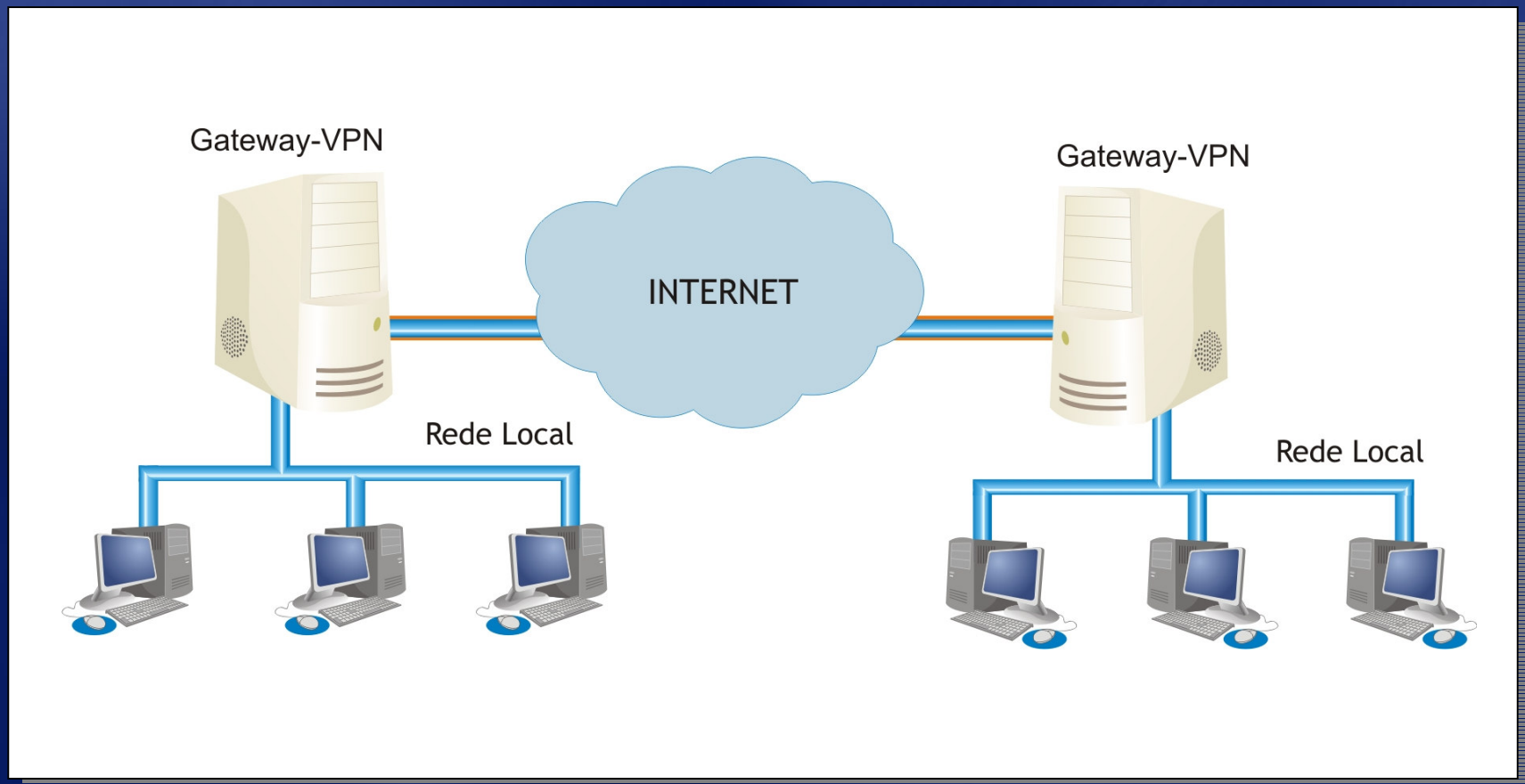
VPN

- Topologia host-gateway



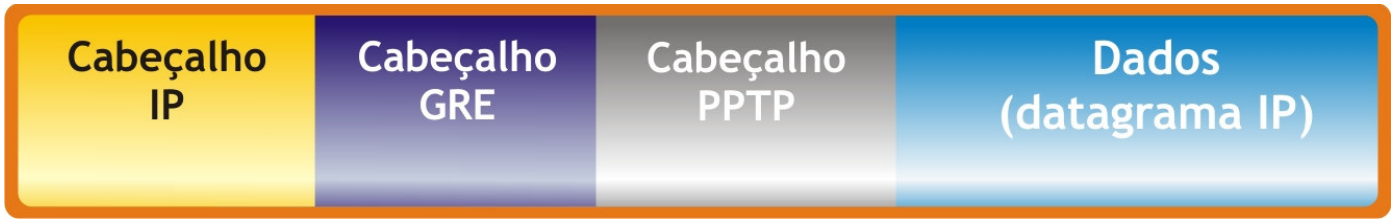
VPN

- Topologia gateway-gateway



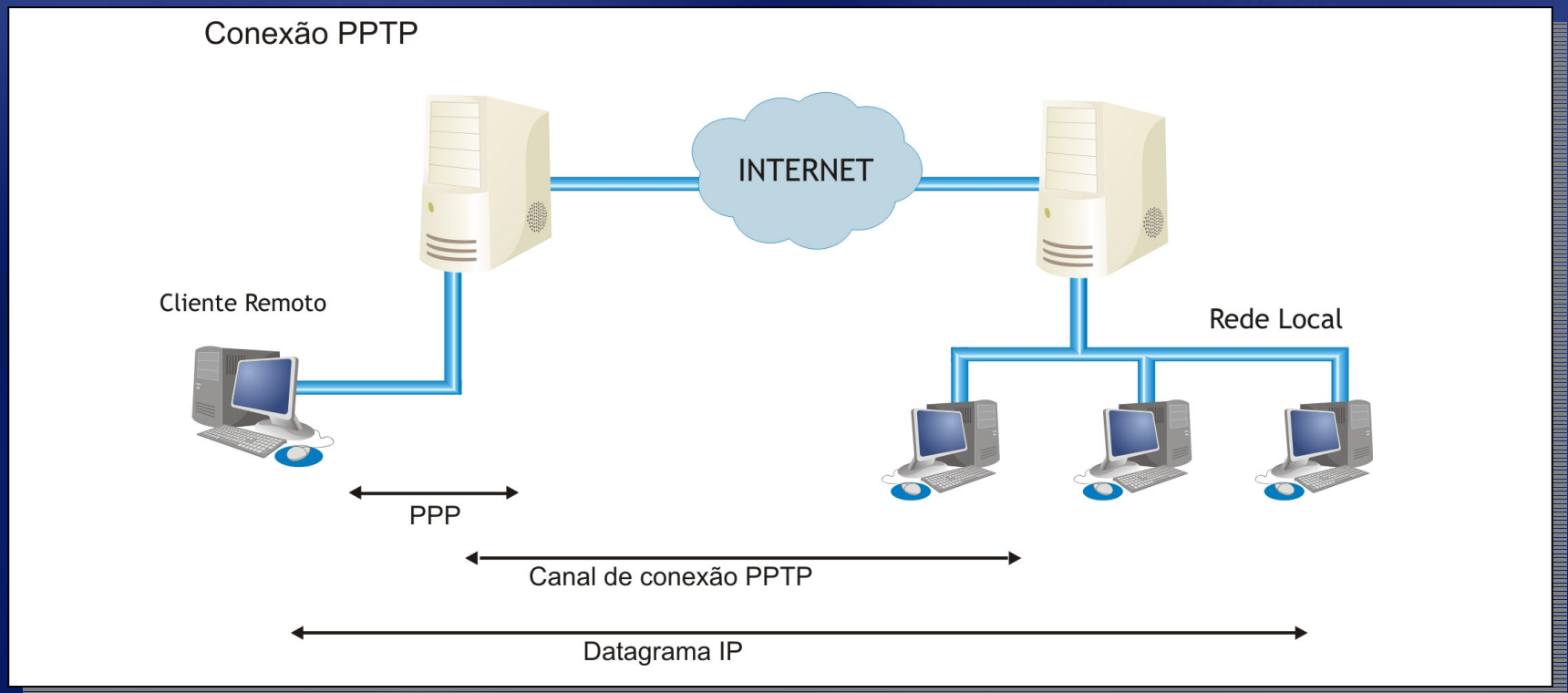
VPN

- Protocolo PPTP
  - Criado pelo PPTP Fórum.
  - Utiliza uma versão modificada do protocolo GRE para tunelamento.



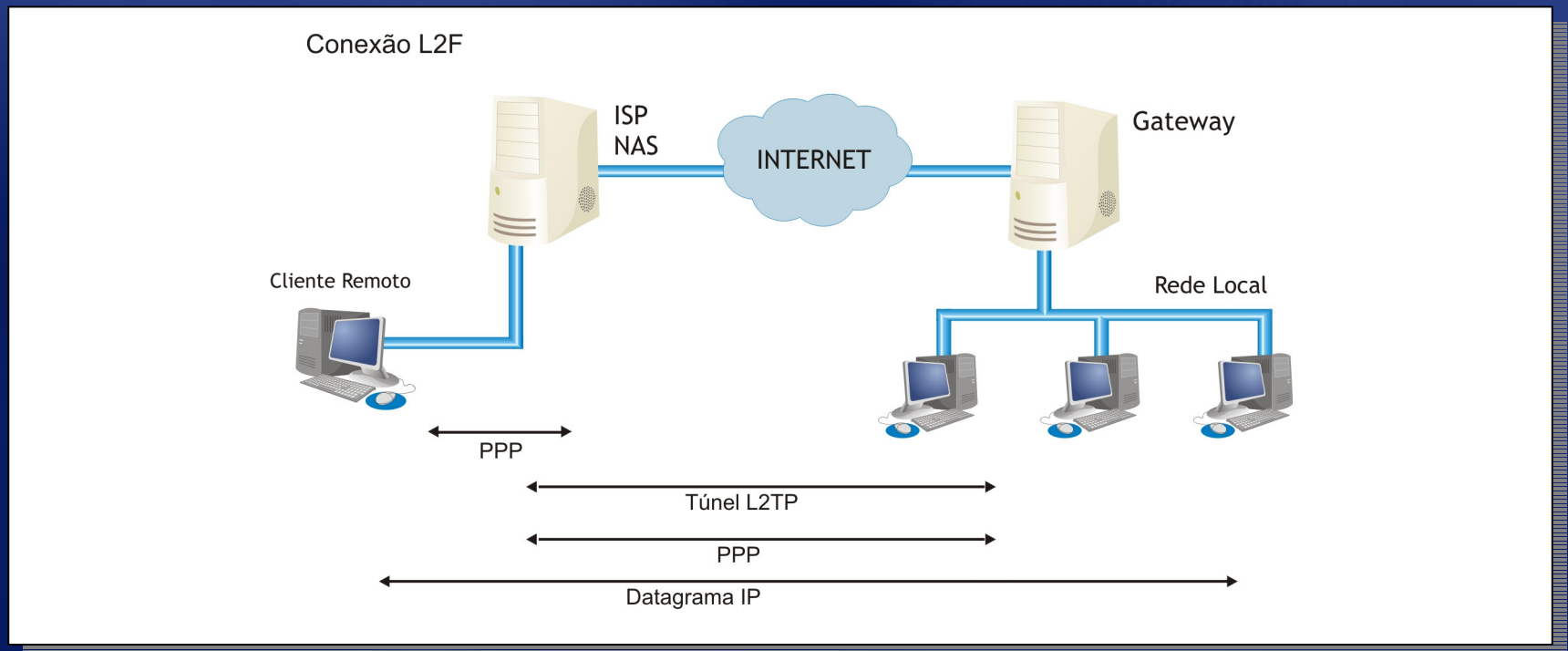
VPN

- Protocolo PPTP
  - Funcionamento



VPN

- Protocolo L2F
  - Independente do IP
  - Funcionamento

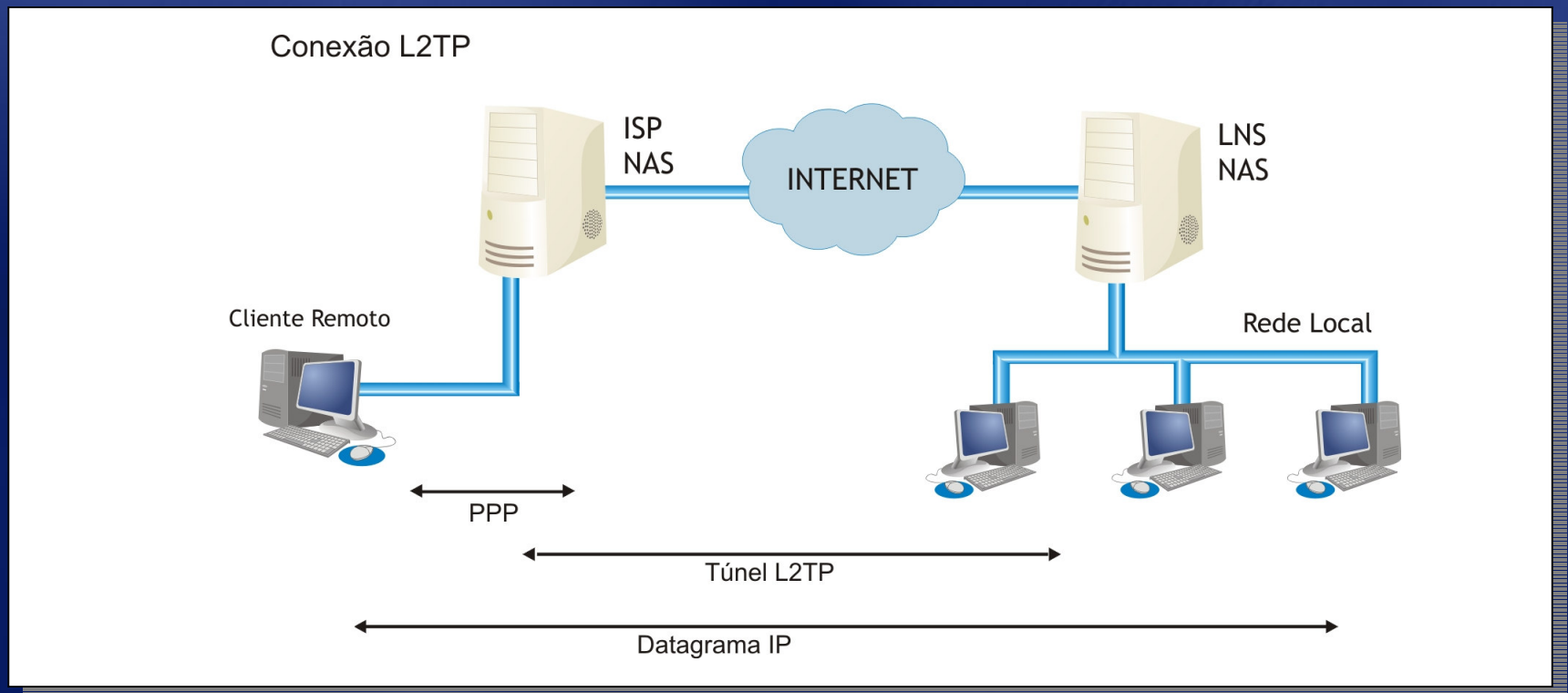


VPN

- Protocolo L2TP
  - Reúne as melhores características do PPTP e L2F;
  - Possui dois modos de tunelamento:
    - Voluntário
    - Compulsório

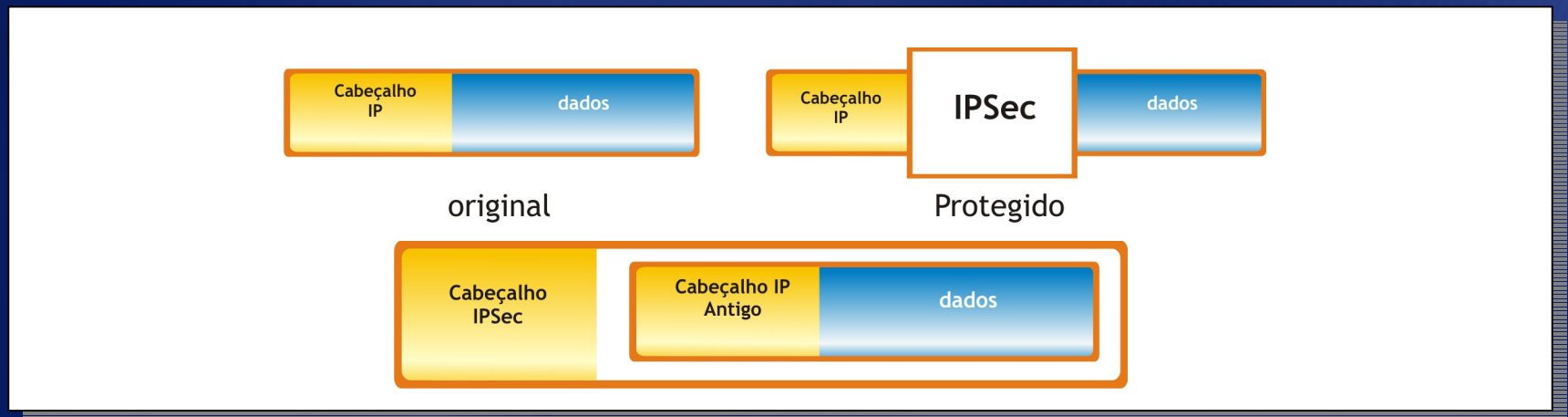
VPN

- Protocolo L2TP
  - Funcionamento



VPN

- IPSec
  - É a alternativa segura para a nova geração IP
  - Trabalha com dois modos:
    - Modo transporte;
    - Modo tunel;



VPN

- IPSec
  - SA (Security Association);
  - Bancos de dados de segurança
    - SPD (Security Policy Database);
    - SAD (Security Association Database);

VPN

- IPSec – Características principais:
  - AH – Authentication Header;
    - Integridade e autenticidade
  - ESP – Encapsulation Header Payload;
    - Confidencialidade;

VPN

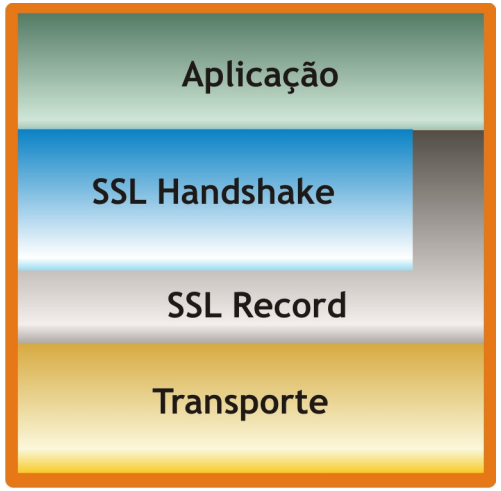
- IPSec – Caracscterísticas principais
  - IKE – Internet Key Exchange
    - Gerência automática de chaves, combina o ISAKMP (distribuição da chaves) com o OAKEY (geração das chaves)

VPN

- SSL
  - SSL/TSL (Netscape/IETF)
  - Objetivos (por prioridade)
    - Sigilo e segurança dos dados;
    - Garantir interoperabilidade;
    - Estrutura para incorporar novos métodos de criptografia;
    - Armazenamento temporário de dados na sessão o que melhorar o desempenho do protocolo.

VPN

- SSL/TSL
  - Atua entre a camada de Aplicação e a camada de Transporte do protocolo TCP.

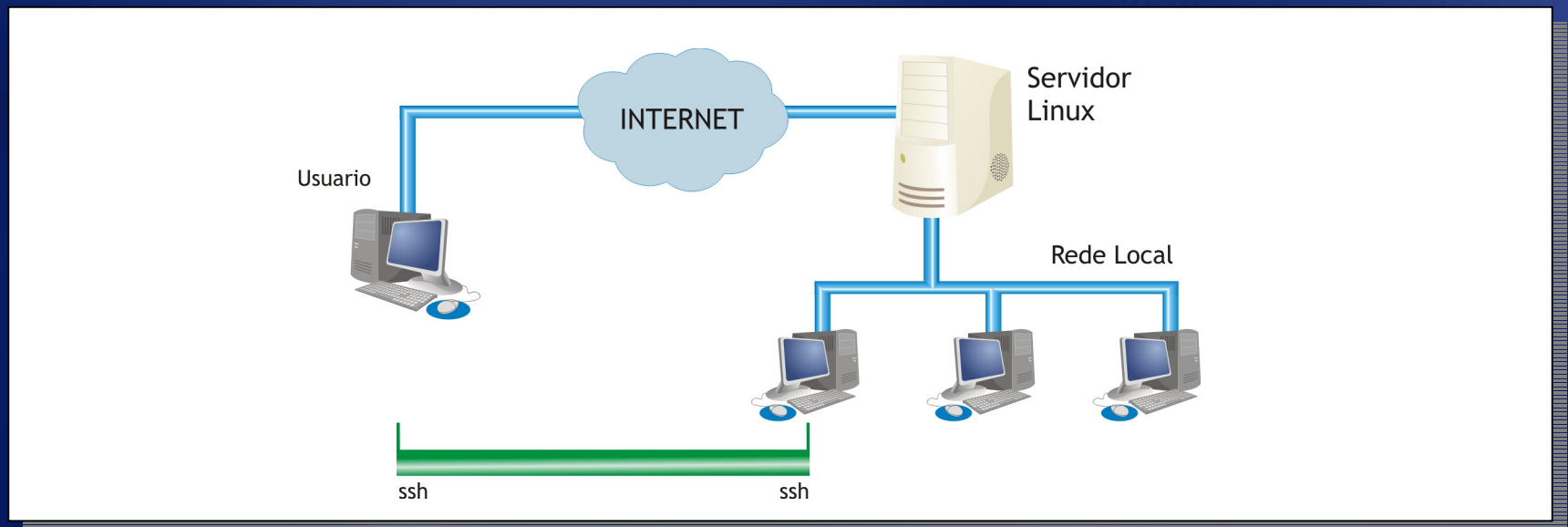


VPN

- SSL
  - SSL Handshake
    - Autenticação do cliente e do servidor;
    - Fornece os parâmetros para o funcionamento do SSL Record;
    - É constituído de duas fases;
      - 1º escolha da chave, autenticação do servidor e a troca da chave mestra;
      - 2º é feita autenticação do cliente

VPN

- SSL
  - SSL Record
    - Encapsula protocolos de nível superior;
    - Provê serviços de autenticação, encriptação, fragmentação e compressão de dados;



VPN

- Implementação
  - Para demonstrar a utilização de uma VPN foi adotado o software OpenVPN, por utilizar o SSL/TSL para criação dos túneis e por ser uma ferramenta open-source. Foram apresentadas topologias host-gateway e gateway-gateway com o intuito de abordar as formas mais comuns de sua implantação.
  - Esta implementação está rodando no LNCC.

VPN

- Conclusão
  - Ao final deste trabalho pode se perceber que as soluções VPN mais seguras são baseadas em IPSec ou SSL;
  - É certamente a maneira mais econômica e segura de se conectar redes através de um meio público;
  - Não basta apenas uma VPN para ter tráfego seguro entre duas redes, também são necessárias outras formas de proteção;
  - Aplicações com tempo de transmissão crítico podem apresentar problemas quando utilizadas em uma conexão VPN.

Dúvidas e Perguntas

Obrigado!