Redes Privadas Virtuais VPN – Virtual Private Network

Prof.: Thiago H. Bom Conselho
UNATEC- Rede de Computadores

Problematização

- Uma corporação possui uma matriz e três filiais em uma mesma cidade. O que podemos fazer para interconectá-las?
- Porem, se a matriz tiver em uma cidade e cada filias em cidades distintas? O que fazer agora?
- Ainda está fácil?!? E se a matriz for norte americana, uma filial tupiniquim, outra do sol nascente e a outra nórdica?
- O que FAZER???

Histórico

- Antes da proliferação da internet as redes corporativas eram implementadas, em sua grande maioria, sobre a rede de telefonia comutada ou as linhas privativas, porem demandava inúmeros recursos e complexa estrutura.
- Com o advento da popularização, do aumento da capacidade de transmissão e do barateamento das redes WAN, em particular a internet, encontrou-se ali um forte aliando.

Definição

- *As VPNs são redes sobrepostas às redes públicas, mas com a maioria das propriedades de redes privadas. (TANENBAUM)*
- *As VPNs são túneis de criptografia entre pontos autorizados, criados através de redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos. (CHIN)*

Definição

- Uma rede virtual privada (VPN) é um meio de simular uma rede privada sobre uma rede pública.

- REDE VIRTUAL: rede formada por conexões Virtuais
- CONEXÃO VIRTUAL: conexões temporárias, não físicas, estabelecidas entre os pontos que se deseja estabelecer uma comunicação segura:
  - entre duas máquinas
  - entre uma máquina e a rede
  - entre duas redes

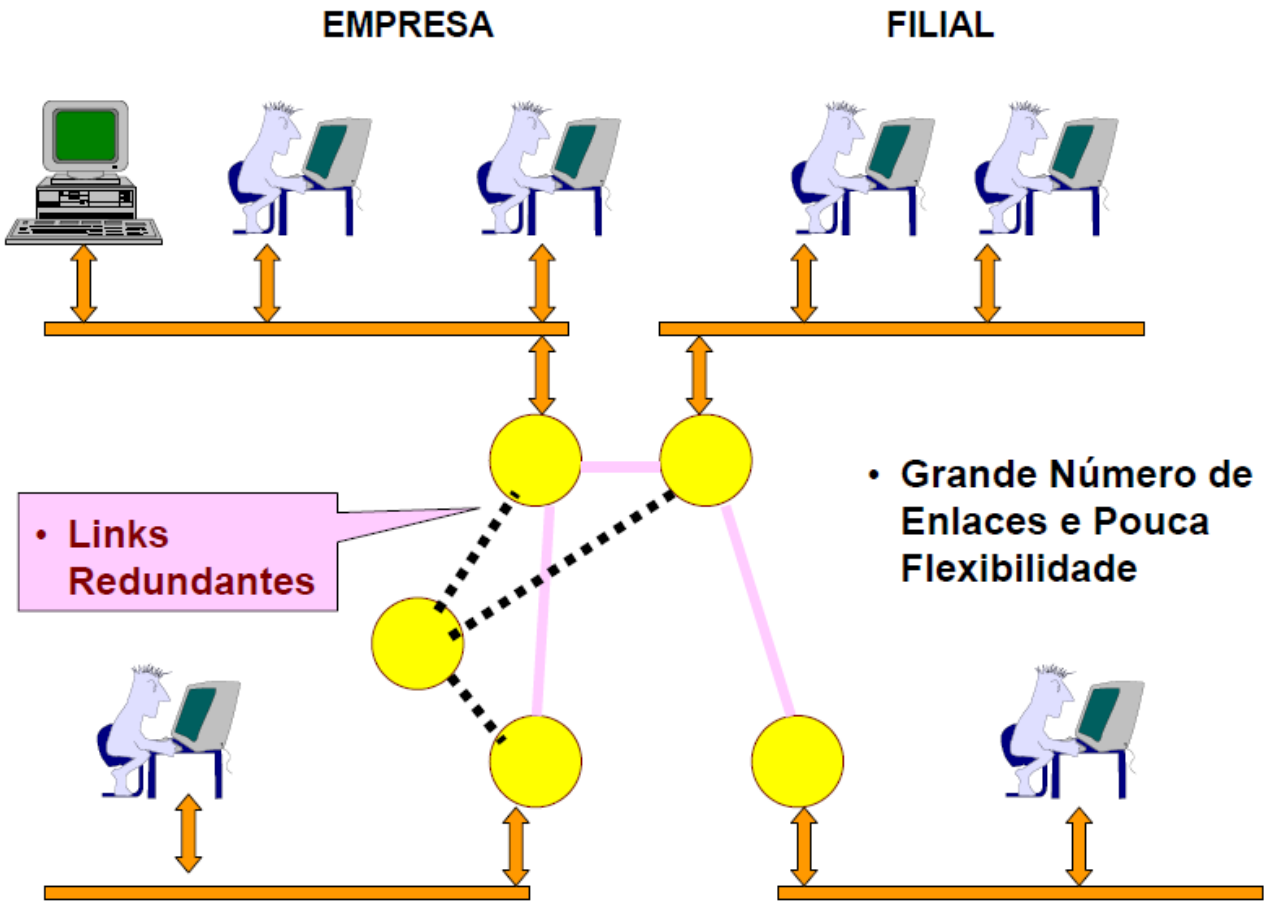
VPN X Linhas Privadas

- A principal motivação para as VPN's é a possibilidade de utilizar a Internet como meio físico de comunicação, sendo uma alternativa muito mais viável que a alocação de linhas privativas.

VPN X Linhas Privadas

- Linhas Privativas:
  - segurança por isolação física dos enlaces de comunicação.
  - custos elevados de implantação e manutenção, principalmente para longas distâncias.
  - o custo aumenta com o número de pontos que compõe a linha privativa.
- Linhas Virtuais Privativas:
  - segurança por criptografia e autenticação.
  - permite criar redes privativas com uma infinidade de enlaces sem aumento de custo significativo.

Linhas Privadas

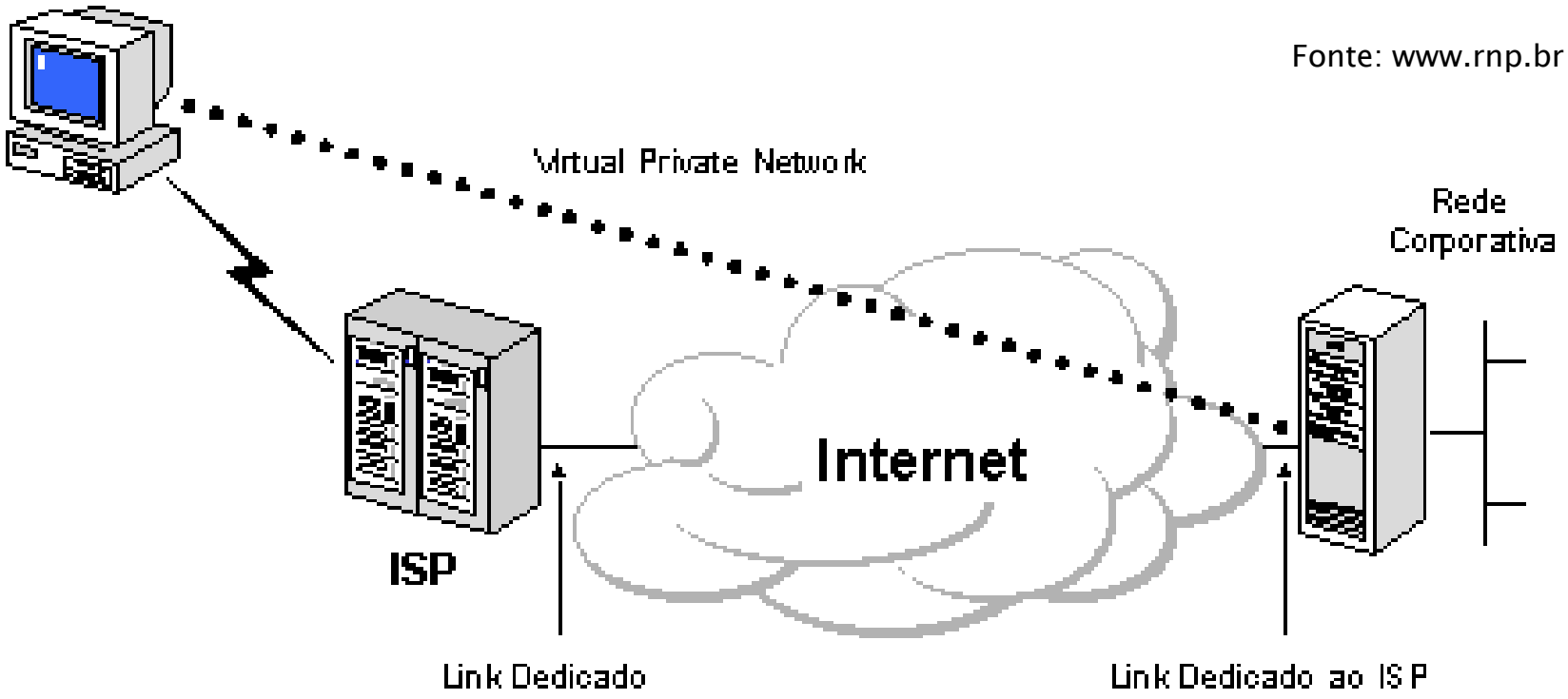


Aplicações para Redes Privadas Virtuais

- Acesso remoto sobre Internet ou VPN de Acesso:
  - Acesso remoto de usuários móveis e pequenos escritórios à uma rede corporativa
    - mesmas políticas de segurança de uma rede privada.
  - Método de Acesso
    - MODEM, RDSI, ADSL, CABO, etc.
  - As VPNs de acesso classificam em tipos, dependendo do ponto onde começa a rede segura:
    - A) Iniciada pelo Cliente
    - B) Iniciada pelo Servidor de Acesso a Rede (NAS)

Aplicações para Redes Privadas Virtuais

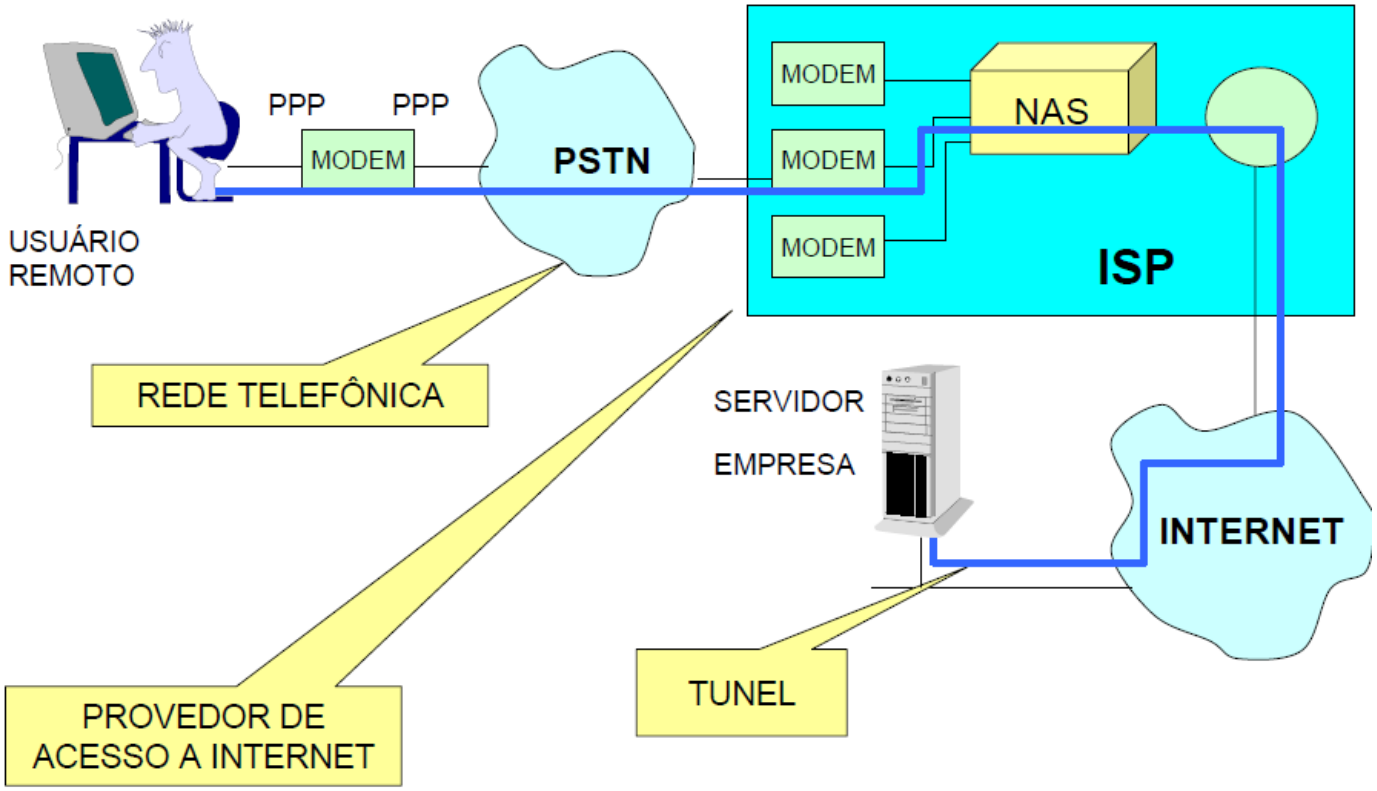
- Acesso remoto sobre Internet:



Fonte: www.rnp.br

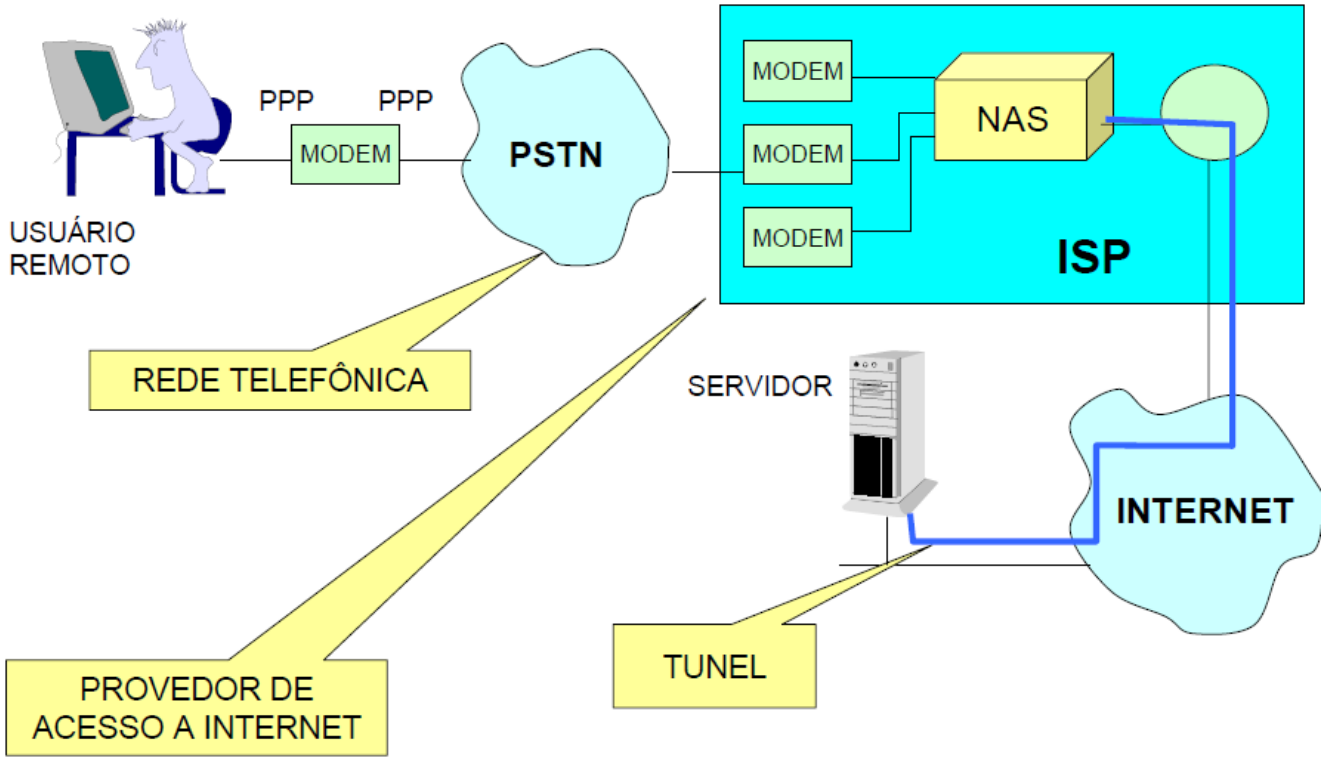
Tipos VPN de Acesso

Iniciada pelo Cliente



Tipos VPN de Acesso

Iniciada pelo Servidor de Acesso a Rede (NAS)



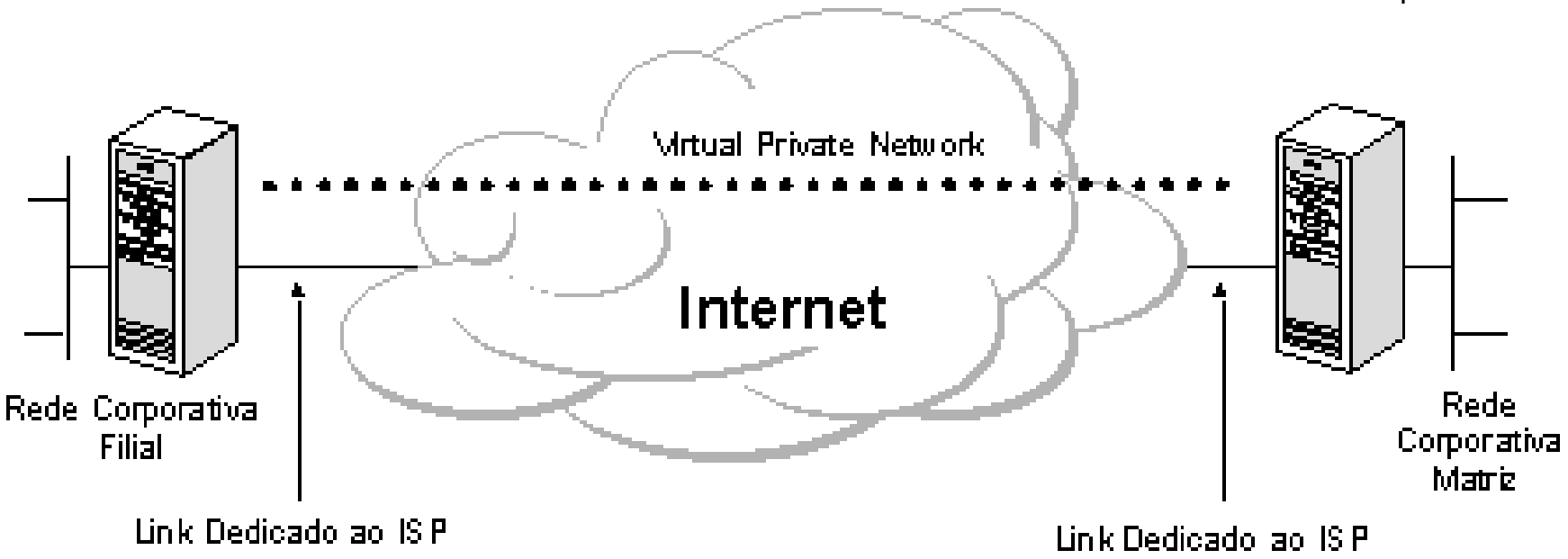
Aplicações para Redes Privadas Virtuais

- Conexão de LANs sobre Internet ou Intranet VPN
  - Permite construir uma intranet utilizando recursos de uma infra-estrutura de comunicação pública (por exemplo, Internet).
  - Uma Intranet VPN é uma VPN que liga os escritórios regionais e remotos à rede interna da matriz através de uma infra-estrutura compartilhada com a utilização de conexões dedicadas.

Aplicações para Redes Privadas Virtuais

- Conexão de LANs sobre Internet:

Fonte: www.rnp.br

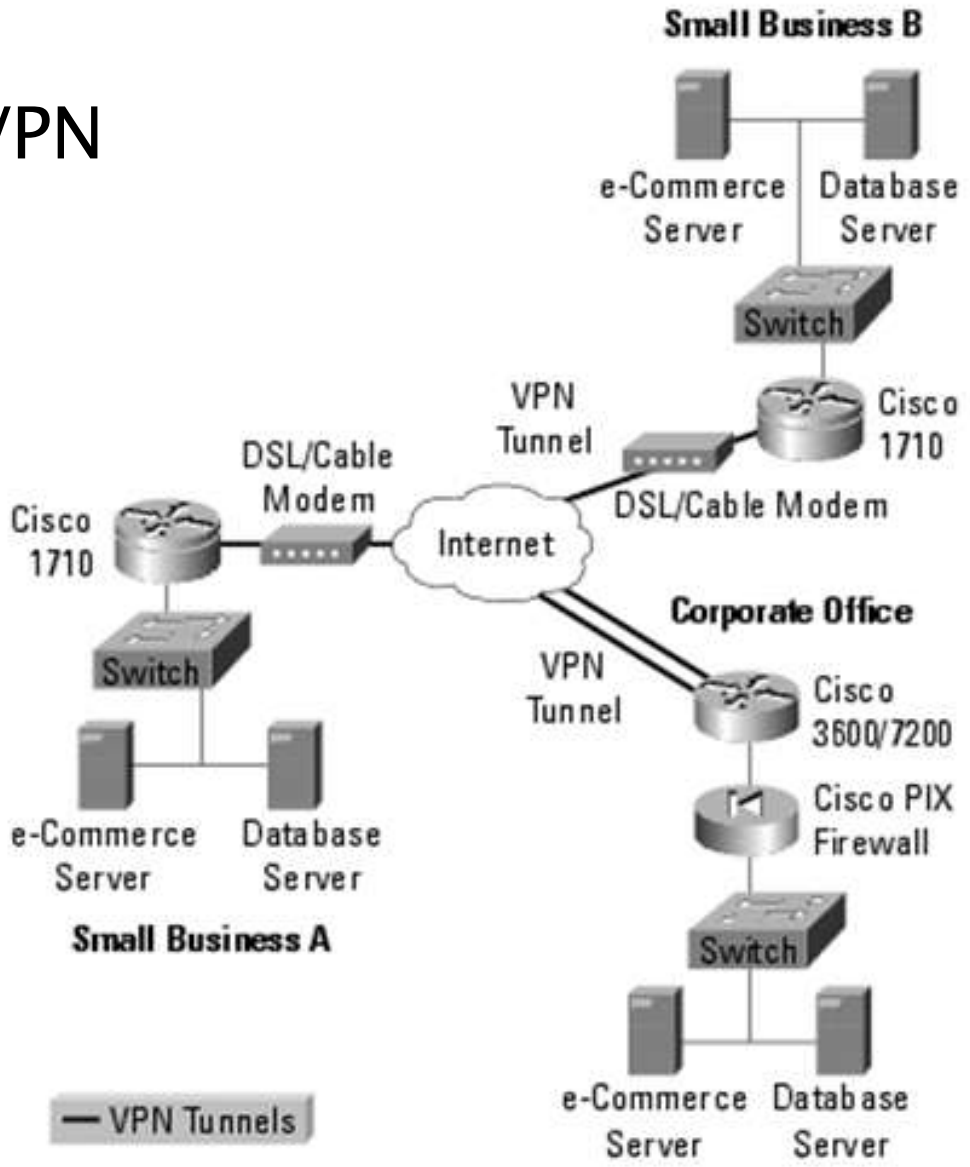


Aplicações para Redes Privadas Virtuais

- Extranet VPN
  - Uma Extranet VPN é uma VPN que liga os associados empresariais à rede da matriz através de uma infra-estrutura compartilhada com a utilização de conexões dedicadas

Aplicações para Redes Privadas Virtuais

- Extranet VPN



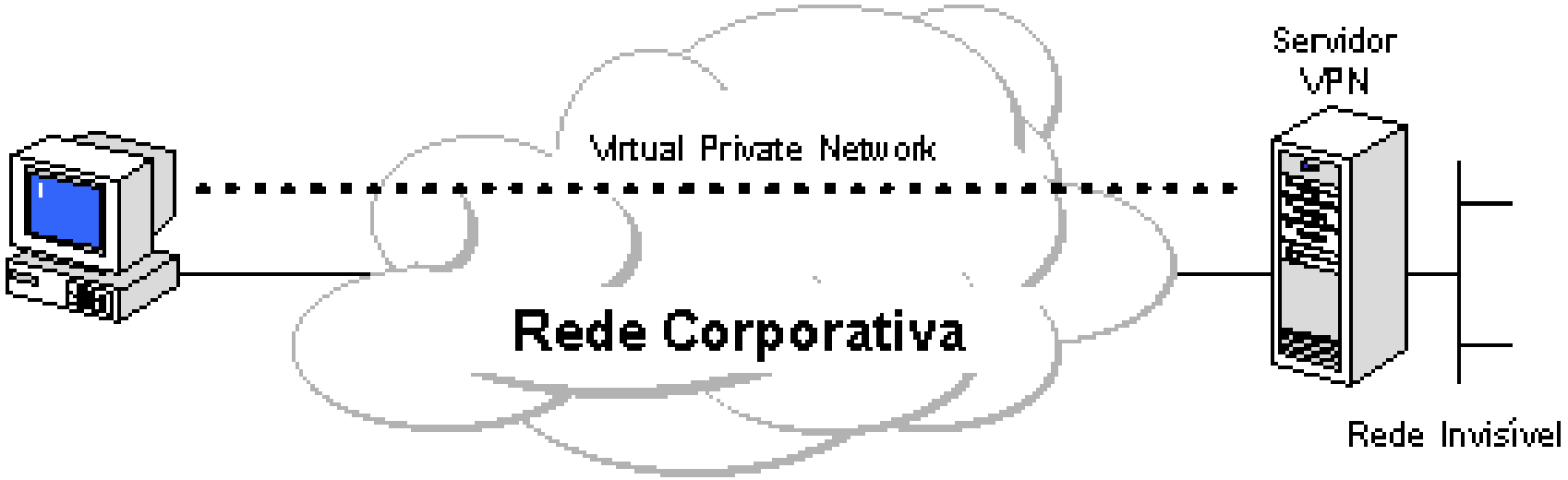
Aplicações para Redes Privadas Virtuais

- Conexão de Computadores a intranet:
  - Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução, apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.
  - As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador possibilitaria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva. Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidencialidade" das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.

Aplicações para Redes Privadas Virtuais

- Conexão de Computadores a intranet:

Fonte: www.rnp.br



Segurança

- Por tratar-se de uma rede compartilhada e com protocolos abertos, a internet, não propicia uma ambiente seguro de dados.
- CHIN enumera os requisitos mínimos desejados em uma VPN, sendo:
  - **Autenticação de Usuários**
  - Gerenciamento de Endereço
  - **Criptografia de Dados**
  - Gerenciamento de Chaves
  - **Tunelamento ou Suporte a Múltiplos Protocolos**

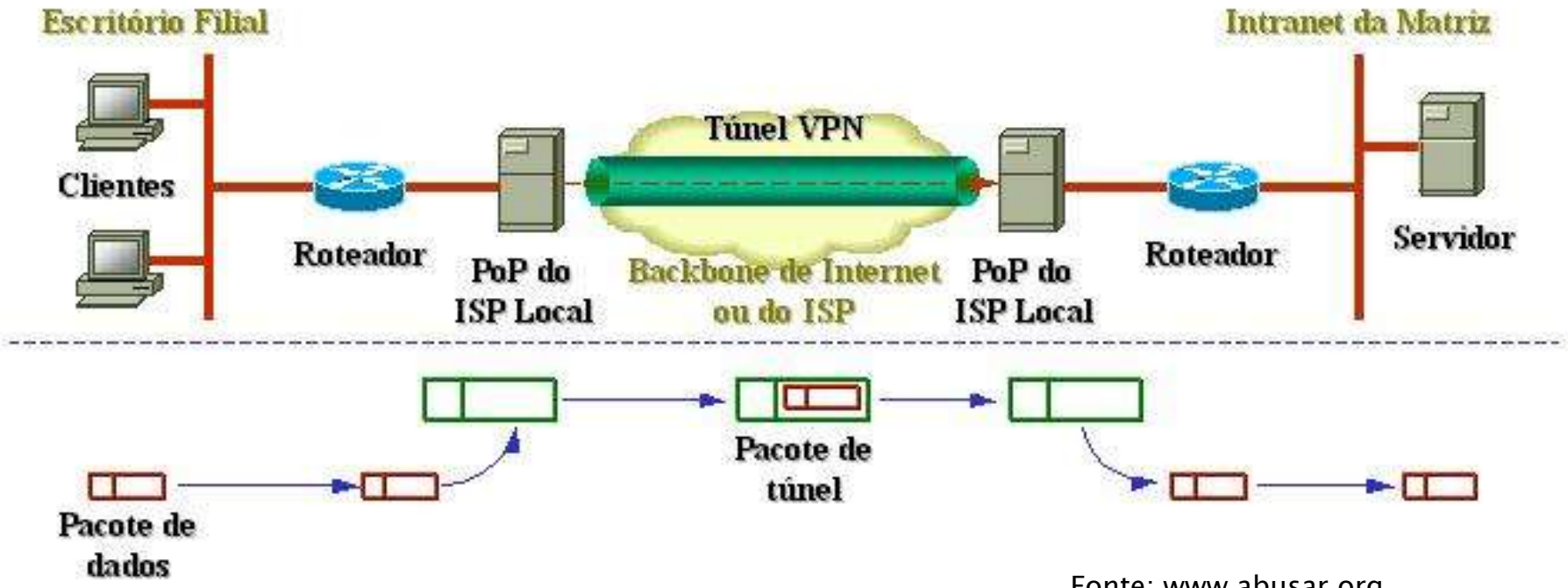
Compatibilidade (Overview)

- As VPN atuais baseiam-se na técnica do tunelamento. Há de se ressaltar também a criação de VPNs pelas técnicas de Endereçamento IP Valido e de Gateways IP.
- O tunelamento pode ser definido como processo de encapsular um protocolo dentro de outro.
- Uma importante característica do tunelamento é a possibilidade de encapsular uma um determinado protocolo em outro diferente.

Tunelamento (Overview)

- O nó de origem adiciona um cabeçalho IP padrão e preserva o pacote original a ser tratado como área de dados, encapsulando assim seu protocolo em pacotes IP.
- Na recepção, o nó de destino desencapsula o pacote original do pacote IP recebido, removendo o cabeçalho IP.

Tunelamento (Overview)



Fonte: www.abusar.org

Protocolos de Tunelamento

- Protocolos de camada 2 – Enlace – (PPP sobre IP): transportam protocolos de camada 3, utilizando quadros como unidade de troca. Os pacotes são encapsulados em quadros PPP;
  - PPTP – Point to Point Tunneling Protocol;
  - L2F – Layer Two Forwading;
  - L2TP – Layer Two Tunneling Protocol;
- Protocolos de camada 3 – Rede – (IP sobre IP): encapsulam pacotes IP com cabeçalhos deste mesmo protocolo antes de enviá-los .
  - IPsec – IP Security Protocol.

Tipos de Túneis

- Túnel Voluntário – um cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel. (CHIN)
- Túnel Compulsório – um servidor de acesso discado VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel. (CHIN)

IPSEC

- IPSec é um protocolo padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.
- O IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.
- Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser utilizado de forma conjunta ou separada, de acordo com a necessidade de cada usuário:
  - Autenticação e Integridade;
  - Confidencialidade.
- Para implementar estas características, o IPSec é composto de 3 mecanismos adicionais:
  - AH - Autentication Header;
  - ESP - Encapsulation Security Payload;
  - ISAKMP - Internet Security Association and Key Management Protocol.

Tecnologias para Implementação de VPN

- Implementação por Hardware
  - Implementada através de roteadores especializados
- Implementação por Software
  - Os computadores cliente e servidor são responsáveis pela construção da VPN e não os dispositivos de rede.
    - Exemplo: PPTP

Conclusão

- Vamos pensar um pouco?!?

Bibliografia e Complementos

- Rede Privada Virtual, CHIN L.K. www.rnp.br
- Redes de Computadores, Tanenbaum A.
- VPN – Virtual Private Network, Zanaroli A.; Lima M.; Rangel R. www.cefet-rj.br
- VPN – Conceitos, Rezende J. www.gta.ufrj.br
- Segurança de Redes de Computadores I – Pinheiro, J. M. S.