VPN
(Virtual Private Network)

VPN - Virtual Private Network

- O conceito de VPN surgiu a partir da necessidade de se utilizar redes de comunicação não confiáveis (por exemplo, a Internet) para trafegar informações de forma segura.

VPN - Virtual Private Network

- Uma VPN proporciona conexões, nas quais o acesso e a troca de informações, somente são permitidas a usuários, que estão em redes distintas que façam parte de uma mesma comunidade de interesse (uma empresa).

VPN - Virtual Private Network

- Uma VPN pode interligar duas ou mais redes via Internet ou através de um link privado, o que possibilita estabelecer um túnel que passa através dessa VPN.

VPN - Virtual Private Network

- Uma rede VPN utiliza um padrão de criptografia mundial, criado pelo IETF (Internet Engineering Task Force), o que torna todo o tráfego de informação nesse túnel, seguro.

Tunelamento

- VPN se baseia na tecnologia de tunelamento.
- Consiste em encapsular um protocolo dentro de outro.
- O protocolo de tunelamento encapsula o protocolo que será transportado, e o cabeçalho do protocolo que encapsulou vai fornecer o destino do pacote do protocolo transportado.

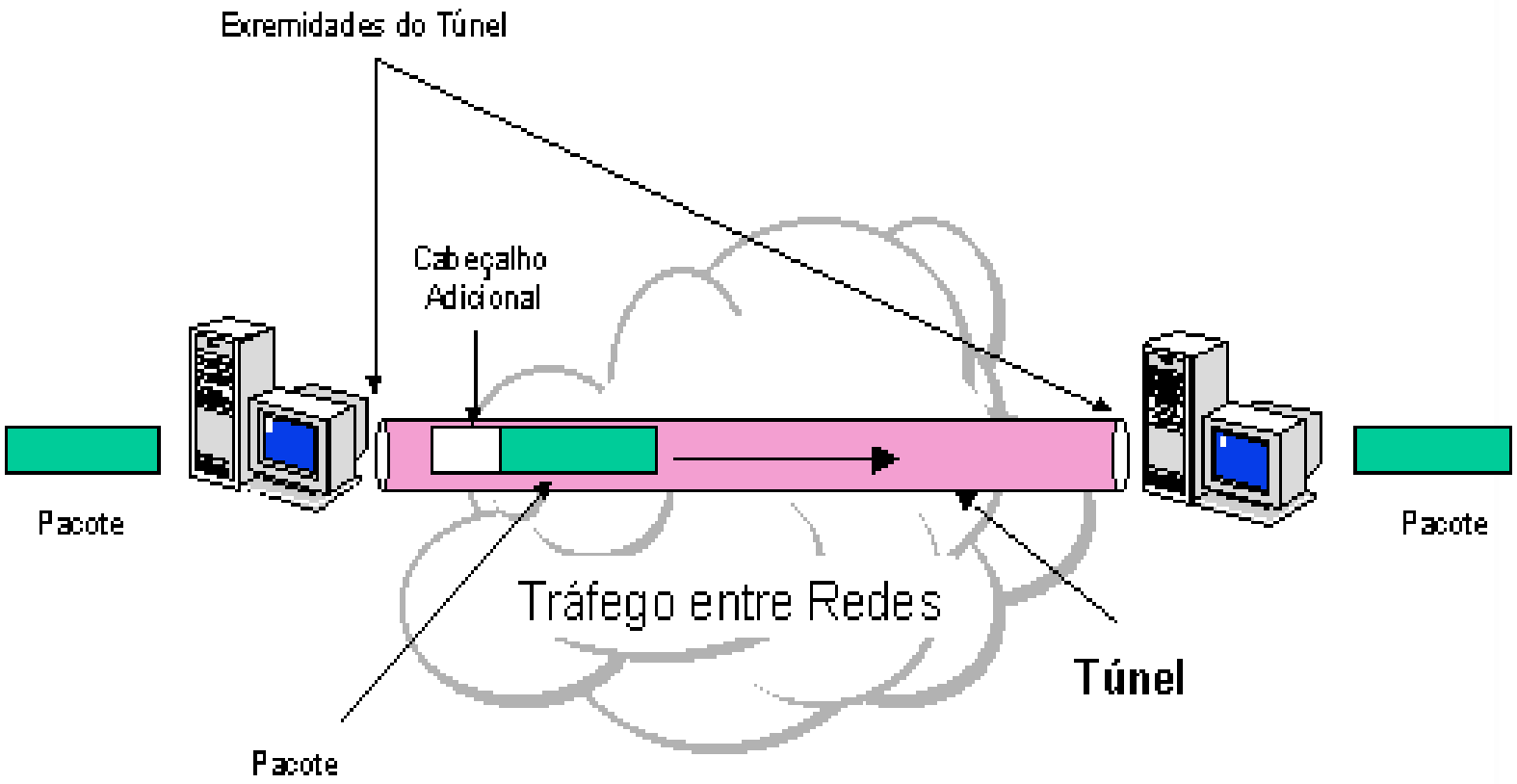
Tunelamento

- Um quadro destinado a outra rede é recebido por um roteador multiprotocolo, na borda da rede.

- O roteador encapsula esse quadro dentro de outro pacote e o envia ao router na outra extremidade da rede

- O roteador que recebeu o pacote remove os cabeçalhos e então entrega o quadro na rede remota.

Tunelamento



VPN - Virtual Private Network

- No caso de VPN, é acrescentado a criptografia, antes do tunelamento.

- Tunelamento VPN =

  [pacote xxx]

  + [Criptografia do pacote xxx]

  + [Encapsulamento do pacote criptografado sobre IP]

VPN - Virtual Private Network

- **Túnel** é a denominação do **caminho lógico percorrido pelos pacotes encapsulados**.

- A rede VPN poder ser construída sobre uma rede pública (Internet) ou privada.

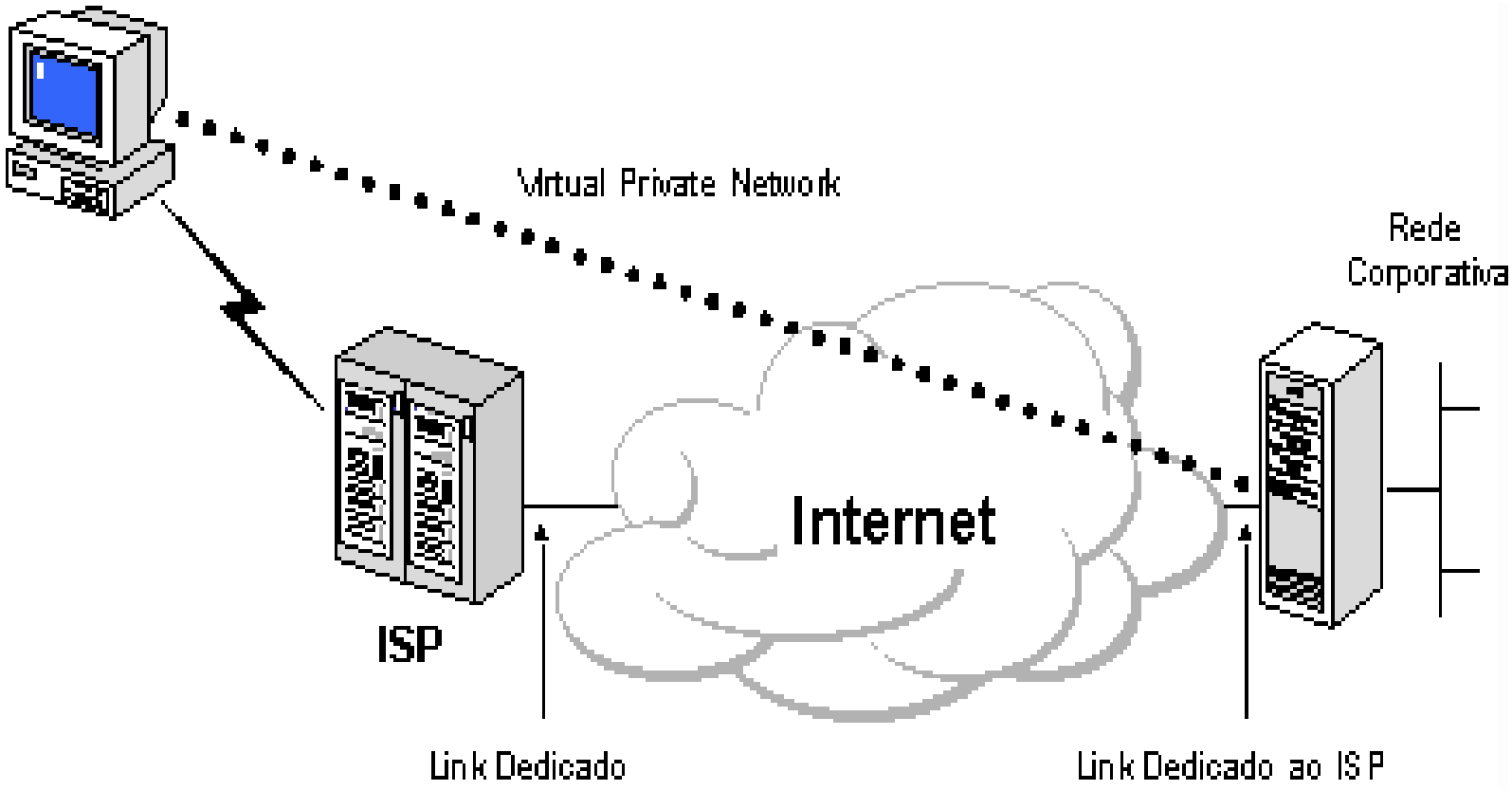
Aplicações para VPN

- Três aplicações ditas mais importantes para as VPNs:
  - Acesso remoto via Internet.
  - Conexão de LANs via Internet.
  - Conexão de computadores numa Intranet.

Acesso remoto via Internet

- O acesso remoto a redes corporativas através da Internet pode ser viabilizado com a VPN através da Internet

Acesso remoto via Internet

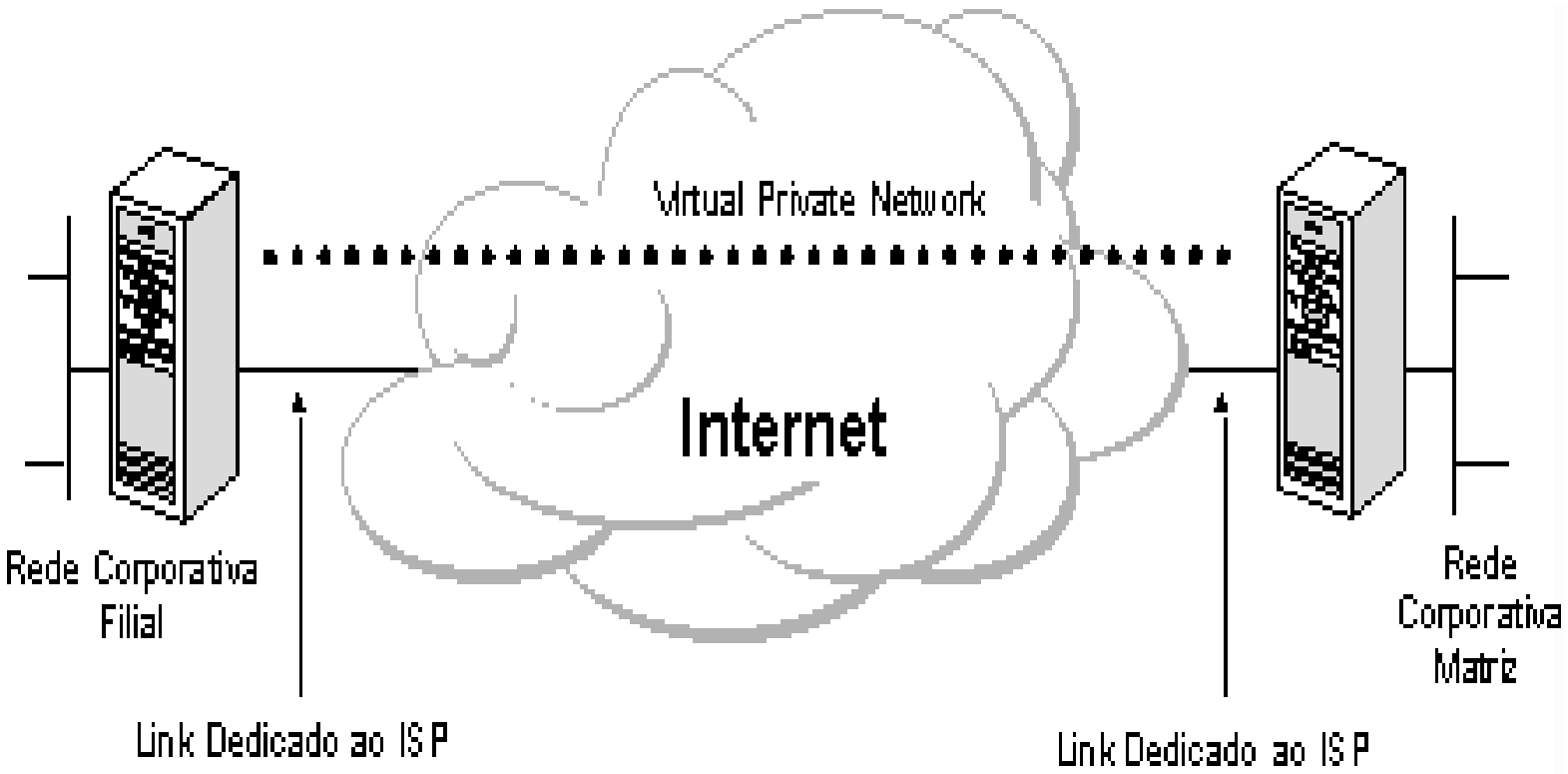


Fonte: RNP

Acesso remoto via Internet

- A máquina do usuário estabelece uma conexão com o servidor de VPN corporativo
- É criada uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

Conexão de LANs via Internet

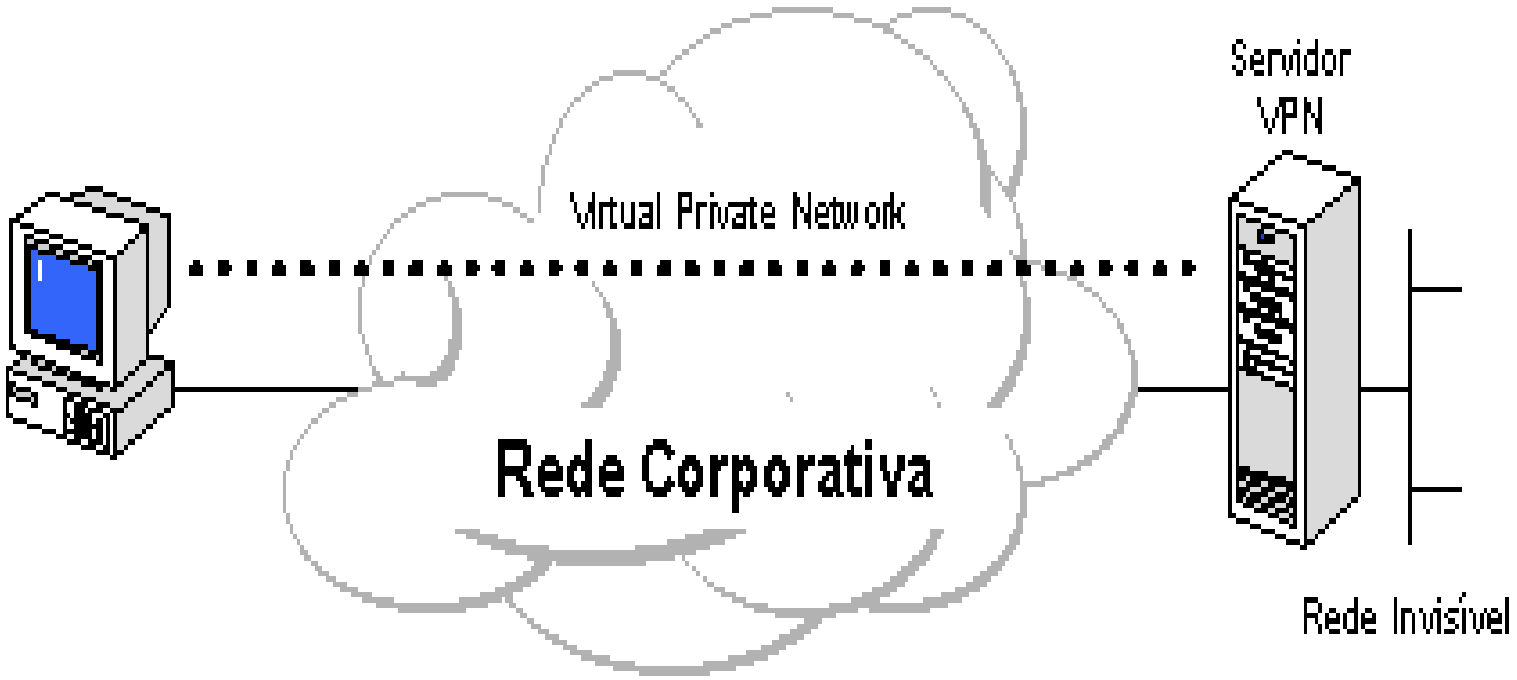


Conexão de LANs via Internet

- Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet.

- O software de VPN assegura esta interconexão formando a WAN corporativa.

VPN em uma Intranet



Fonte: RNP

VPN em uma 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.

- **Em redes locais, o mais comum é o uso de VLANs para isolar o tráfego da rede entre segmentos virtuais**

Requisitos básicos

- Autenticação de usuários.
- Gerenciamento de endereço.
- Criptografia de dados.
- Gerenciamento de chaves.
- Suporte a múltiplos protocolos.

Autenticação de Usuários

- Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas.

- Deve dispor de mecanismos de auditoria, provendo informações referentes aos acessos efetuados - quem acessou, o quê e quando foi acessado.

Gerenciamento de Endereço

- O **endereço do cliente** na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

Criptografia de Dados

- Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação.

- O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

Gerenciamento de Chaves

- O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas.

- O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

Suporte a Múltiplos Protocolos

- Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos usadas nas redes públicas

Exemplos de protocolos

- PPTP (***Point-to-Point Tunneling Protocol***)
- L2TP (***Layer 2 Tunneling Protocol***) da **IETF** (*Internet Engineering Task Force*).
- L2F (*Layer 2 Forwarding*) da Cisco é utilizada para VPNs discadas.
- IPsec (IP Security Protocol)

Tunelamento em Nível 3 (IP sobre IP)

- **Encapsulam pacotes IP com um cabeçalho adicional deste mesmo protocolo** antes de enviá-los através da rede.

- O *IP Security Tunnel Mode* (**IPSec**) da **IETF permite que pacotes IP sejam criptografados e encapsulados com cabeçalho adicional deste mesmo protocolo** para serem transportados numa rede IP pública ou privada.

Tunelamento em Nível 3 (IP sobre IP)

- **O IPSec é um protocolo desenvolvido para IPv6**, devendo, no futuro, se constituir como padrão para todas as formas de VPN caso o IPv6 venha de fato substituir o IPv4.

- O **IPSec** sofreu adaptações possibilitando, também, a sua utilização com o **IPv4**.

Segurança da Comunicação

- Se o IPSec for utilizado no “tunelamento”, será possível agregar todo o tráfego entre dois pares de escritórios quaisquer em uma única SA autenticada e criptografada, fornecendo:
  - controle de integridade,
  - sigilo e
  - até mesmo uma considerável imunidade à análise de tráfego.

Segurança da Comunicação

- Quando um sistema é criado, cada par de firewall tem de negociar os parâmetros de sua SA, incluindo os serviços, os modos, os algoritmos e as chaves.
- Firewalls, VPNs e IPSec com ESP (*encrypted security payload*) em modo túnel formam uma combinação natural e amplamente usada na prática.
- Vantagem dessa forma de organização de uma VPN – completa transparência para todo o software do usuário (o administrador de sistema tem que configurar e administrar os *firewalls*).

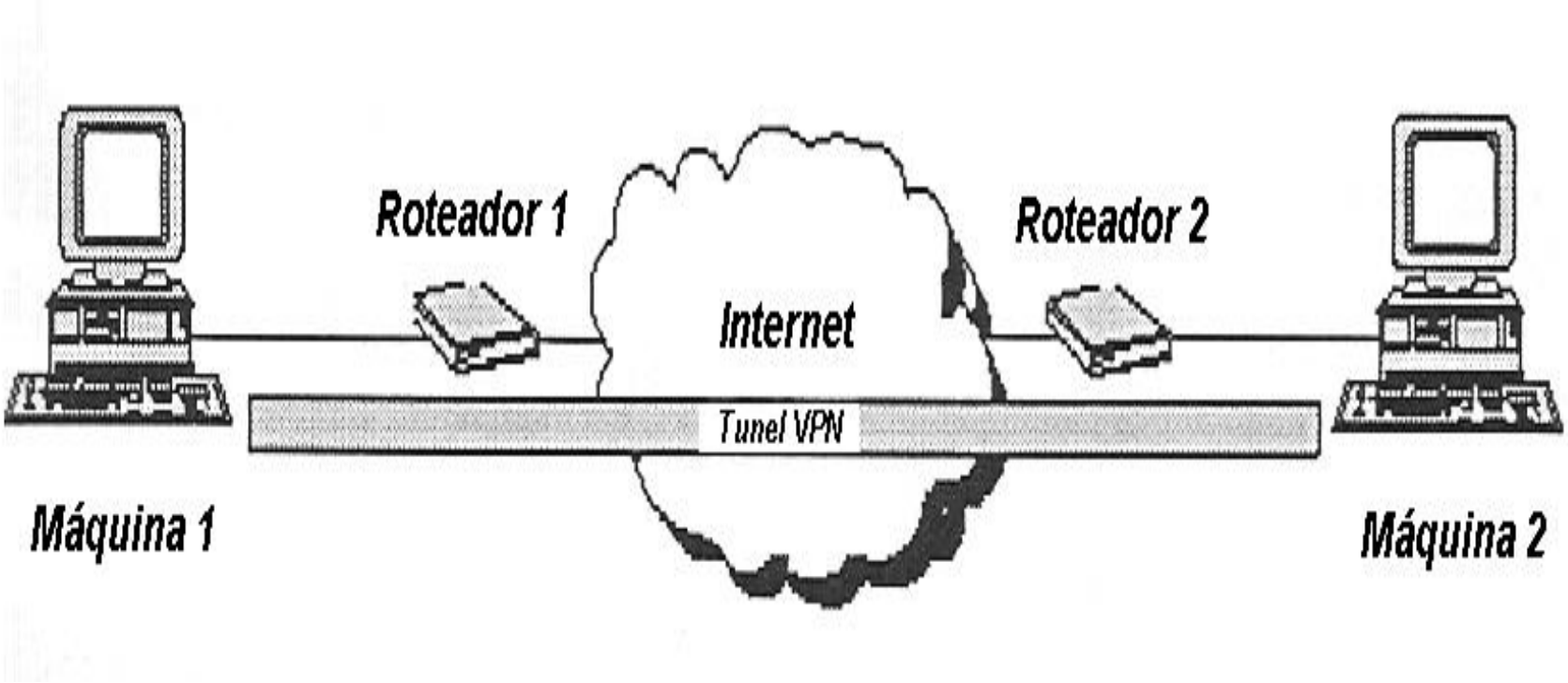
Tipos de túneis

- Os túneis podem ser criados de duas diferentes formas - voluntárias e compulsórias:
  - Túnel Voluntário
  - Túnel Compulsório

Túnel Voluntário

- **O computador do usuário funciona como uma das extremidades do túnel** e, também, como **cliente do túnel** e emite uma solicitação VPN para configurar e criar um túnel voluntário entre duas máquinas, uma máquina em cada rede privada, e que são conectadas via Internet.

VPN entre duas máquinas



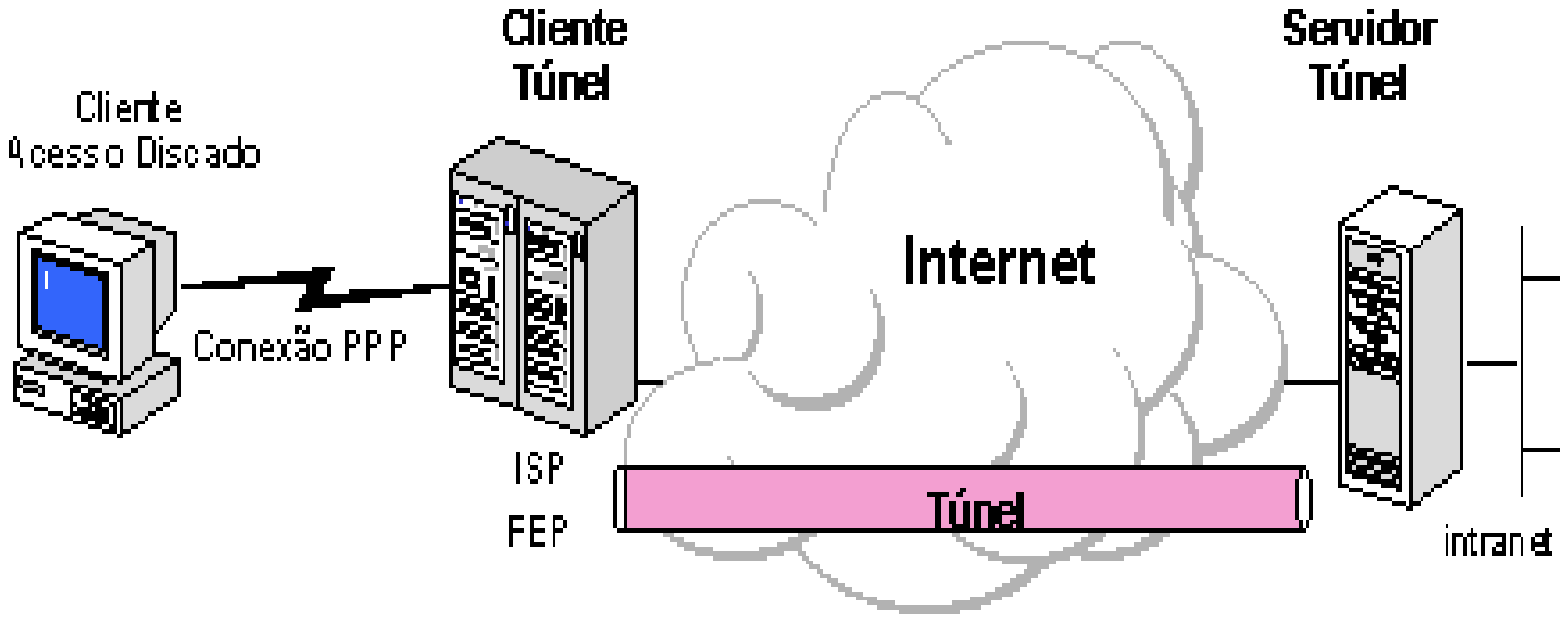
Túnel Compulsório

- **O computador do usuário não funciona como extremidade do túnel**.

- Um **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**.

- Um servidor de acesso discado VPN configura e cria um túnel compulsório.

Tunelamento compulsório



Tunelamento compulsório

- O **computador** ou **dispositivo de rede que provê o túnel** para o **computador-cliente** é conhecido de diversas formas:
  - FEP (*Front End Processor*) no PPTP,
  - LAC (*L2TP Access Concentrator*) no L2TP
  - *IP Security Gateway* no caso do IPSec.

VPN
(Virtual Private Network)