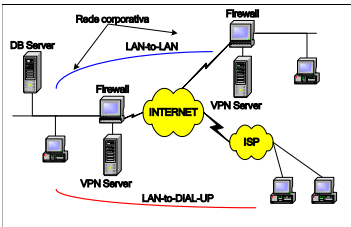


CONCEITOS AVANÇADOS EM IRCs

VIRTUAL PRIVATE NETWORK - VPN

- ❖ VPN: Rede Virtual Privativa que usa a estrutura aberta e distribuída da Internet para a troca de dados segura e confiável entre redes corporativas (ou entre usuários finais e redes corporativas)

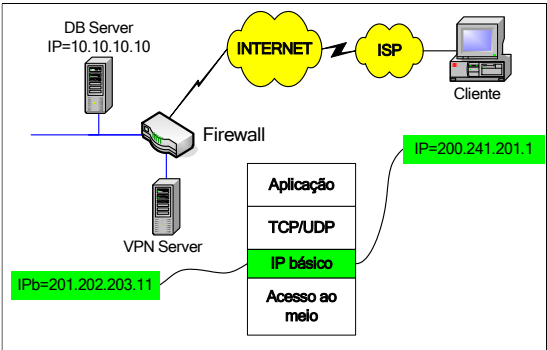
MODELO DE USO



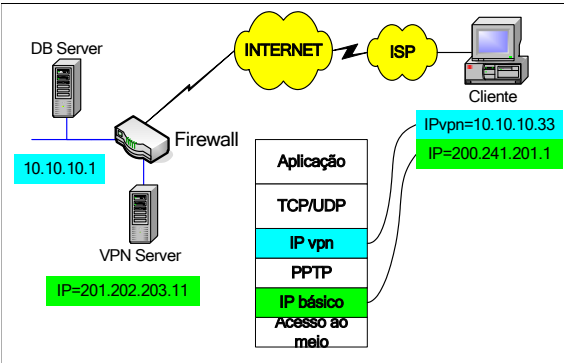
IDÉIA DE FUNCIONAMENTO

- ❖ Permitir a qualquer cliente externo, devidamente identificado e autenticado, ter acesso aos recursos da rede interna como se fizesse parte dela
 - É preciso ser capaz de passar através de Firewalls, sem que seja preciso colocar regras de exceção nos mesmos
 - É preciso, em muitos casos, usar endereçamento privativo (10.x.y.z, p.ex.) nos clientes para poder entrar na rede corporativa que usa endereçamento privativo
 - É preciso estabelecer um túnel de tráfego especial entre os servidores VPN (no caso de LAN-to-LAN) ou entre um servidor VPN e um cliente (no caso de LAN-to-DIAL-UP)
 - O túnel carrega pacotes de um lugar para o outro de forma que os mesmos parecem ser gerados na rede local corporativa (tem o mesmo tipo de endereçamento)

- ❖ VPNs devem prover quatro funções básicas para garantir segurança para os dados:
 - Autenticação: garantindo que os dados são originados de fontes que são quem dizem ser
 - Controle de Acesso: que restringe usuários não autorizados
 - Confidencialidade: evitando que qualquer um leia ou copie dados atravessando a rede
 - Integridade dos dados: evitando que qualquer um adultere dados atravessando a rede
- ❖ O esquema a seguir mostra a implementação da idéia para o protocolo PPTP (Point-to-point Tunneling Protocol), mas que é padrão para os outros protocolos



Situação inicial – comunicação direta entre cliente e VPN Server.



Situação final – comunicação "direta" entre cliente e DB Server.

- ❖ PPTP oferece para o IP vpn uma interface de enlace semelhante à oferecida pelo acesso ao meio ao IP básico
- ❖ Quando o PPTP recebe datagramas IP do IP vpn, com endereçamento VPN (privativo ou não), ele os assina digitalmente e criptografa, gerando novos fragmentos de dados que são entregues ao IP básico que os encapsula em novos datagramas IP com endereçamento real
- ❖ Através do IP básico, o cliente comunica-se com o servidor VPN com endereçamento real, roteado normalmente através da Internet, desde o provedor até a rede corporativa
- ❖ Chegando ao servidor VPN, o conteúdo do datagrama IP básico é decryptografado, tem sua assinatura digital verificada, voltando a ser um datagrama IP vpn que é, por sua vez, encaminhado para a rede corporativa, como se fosse originado dentro dela mesma (com os devidos ajustes no firewall)
- ❖ O firewall deve saber (tabela de rotas) que deve encaminhar para o servidor VPN todos os datagramas destinados ao endereço 10.10.10.33 (e outros endereços reservados para VPN)

PROTÓCOLOS PARA VPN

PPTP: Point-to-point Tunneling Protocol

- ❖ É largamente utilizado para dial-up VPNs
- ❖ Tem suporte (servidor) no Windows Server
- ❖ Tem suporte (cliente) no a partir do Windows XP
- ❖ É baseado no protocolo PPP, usando PAP (*Paswword Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*)
- ❖ Comporta-se como protocolo de camada 2 (enlace), podendo carregar outros protocolos além do IP

IPsec: IP security protocol

- ❖ É derivado dos esforços para implementar segurança no nível IP do IPv6
- ❖ Pode ser usado em dois modos:
 - Transporte: somente o conteúdo transportado por um datagrama IP é autenticado/criptografado
 - Túnel: todo o datagrama IP é autenticado/criptografado e levado através de um túnel (datagrama IP dentro de datagrama IP)
- ❖ Impõe segurança robusta com:
 - Troca de chaves Diffie-Hellman para entrega de chaves secretas entre parceiros através da rede pública
 - Criptografia de chave pública para sinalizar troca de chaves Diffie-Hellman
 - DES / AES para criptografia de dados
 - HMAC, MD5 e SHA para autenticação de pacotes
 - Certificados digitais para validação de chaves públicas
- ❖ Pode usar dois métodos para a troca de chaves (mandatário no IPsec):
 - Manual
 - Automático via Internet Key Exchange (IKE)
- ❖ IPsec é considerado a melhor solução para VPNs em ambiente IP