SO

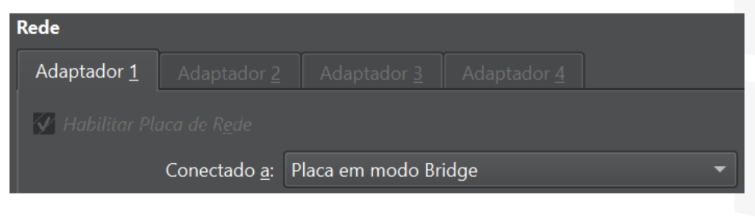
COMPARTILHAMENTO VIA REDE e VPN

O compartilhamento de pastas via rede, permite que outros computadores acessem as pastas configuradas.

Isso é muito utilizado em ambientes corporativos, onde normalmente temos um servidor que compartilha essas pastas ao demais computadores.

**Primeiros Passos**

* Alterar o nome da máquina já existente para: cliente;
* Criar uma nova VM com nome de servidor;
* Verificar se ambas VMs estão com o adaptador de redeconfigurado como “Placa em modo Bridge”



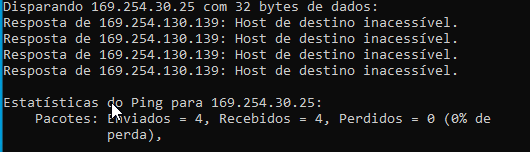
**Realizando Ping (Servidor)**

Agora é necessário verificarmos se ambas máquinas estão de fato

na mesma rede:

* Acesse o CMD;
* Insira o comando: ping ip\_da\_maquina;
* TODOS os pacotes devem ser recebidos.

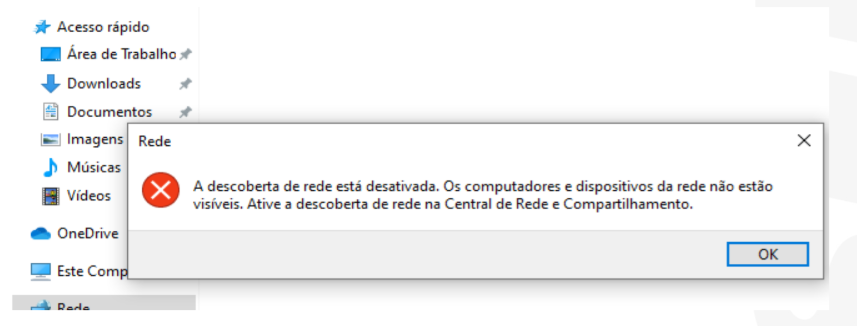
Nesse momento, o ping não deu certo, então, devemos ativar a descoberta de rede.



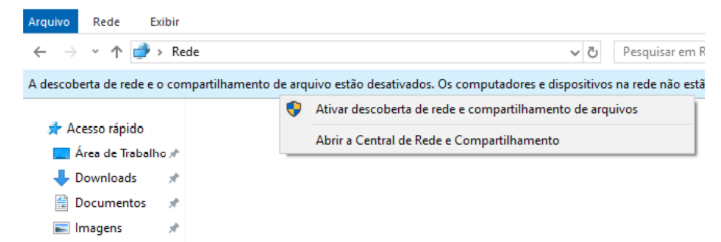
**Ativando a Descoberta de Rede e Compartilhamento de Arquivos (Ambos)**

Para que os computadores que estão conectados na mesma rede possam visualizar a pasta que será compartilhada, é necessário ativar a descoberta de rede privada.

* Acesse o explorador de arquivos e clique em “Rede”

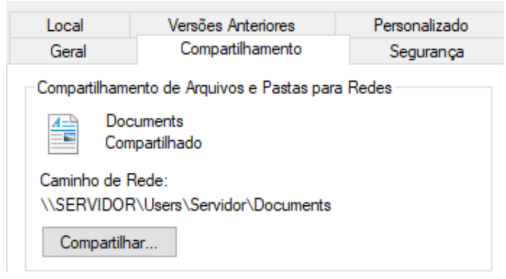


* Clique em OK;
* Clique na mensagem que aparecerá na parte de cima do Explorador de Arquivos;
* Selecione a opção: “Ativar descoberta de rede e compartilhamento de arquivos”.



**Criando um pasta compartilhada (Servidor):**

* Em Documentos, crie uma pasta “compartilhada”;
* Acesse as propriedades da pasta e vá para aba “Compartilhamento”;
* Selecione “Compartilhar”;



**Compartilhando a pasta:**

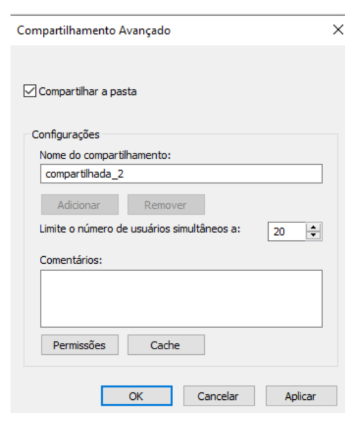
* Na tela “Acesso à Rede” selecione “Todos”;
* Clique em “Adicionar”
* Clique em “Compartilhar”



**Compartilhamento avançado**

Após os passos anteriores, acesse novamente as propriedades da pasta e “Compartilhamento”

* Acesse compartilhamento avançado;
* Marque a caixa “Compartilhar Pasta”;
* Clique em “Aplicar”.



**Acessando a pasta compartilhada (Cliente)**

Para acessar a pasta:

* Acessa “Executar” (Windows + R);
* Digite “\\nome\_da\_maquina\nome\_da\_pasta”.

**Mapeando a pasta compartilhada**

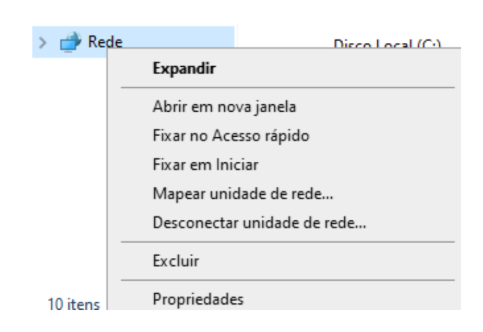
O mapeamento de uma pasta compartilhada vai permitir o Cliente visualizar a pasta da mesma forma que um Disco.

Ele também traz a informação de armazenamento que possui aquela pasta (Mesmo do Servidor).

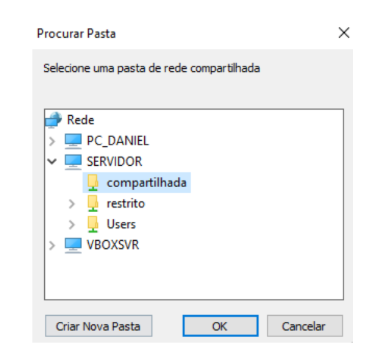
Ele serve como atalho para o cliente, para que não seja necessário ficar acessando a pasta pelo caminho toda vez.

**No computador cliente:**

* Acesse o explorador de Arquivos;
* Clique com o botão direito em “Rede”;
* Selecione a opção: “Mapear unidade de rede…”.



* Escolha uma letra para o mapeamento;
* Clique em “Procurar” para informar a pasta que vai ser mapeada;
* Clique em “Concluir"



* Acesse “Meu Computador”;
* Observe o Mapeamento criado.

**VPN**

**Redes Privadas x Redes Públicas**

**Privada:**

* Isolada ao acesso público
* Acesso Restrito
* Administração centralizada
* Maior controle sobre o tráfego de dados
* Menor exposição a ameaças

Exemplos:

* Redes LAN
* Redes Domésticas

**Pública:**

* Acesso aberto e não controlado
* Segurança limitada ou inexistente
* Administração geralmente mínima
* Tráfego potencialmente monitorado
* Alta exposição a riscos de segurança (Sem criptografia)

Exemplos:

* Redes de cafeterias, parques etc.

Riscos:

* Ataque MitM (Man-in-the-Middle): O hacker cria um ponto de acesso falso e quando você se conecta; todo o tráfego passsa pelo computador dele antes de ir à internet.
* Sniffing de pacotes: Uso de ferramentas para pegar e analisar pacotes de dados (Podem ver seu e-mail, suas senhas, etc.)
* Evil Twin: O hacker cria uma REDE falsa que imita a rede legítima
* Malware e vírus: Propagação entre vários usuários conectados na rede.

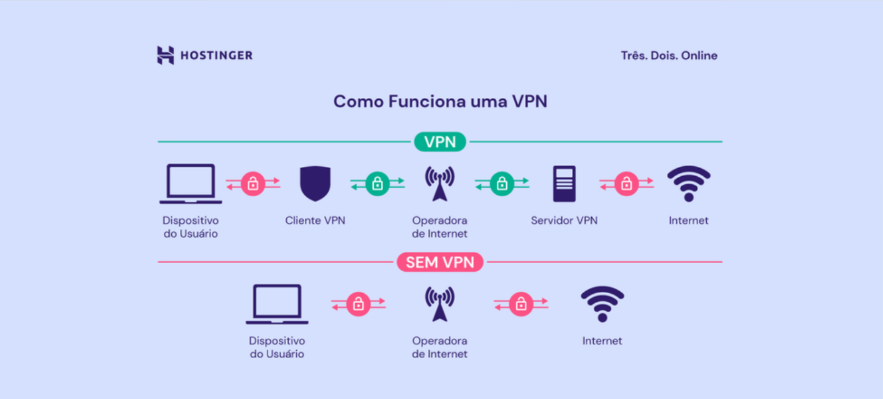
Como VPN resolve esses problemas?

O que é VPN?

Uma Rede Virtual Privada (VPN- Virtual Private Network), é uma tecnologia que cria uma conexão segura sobre uma rede pública, permitindo a criptografia dos pacotes de dados.

O VPN permite que dados sejam transmitidos com segurança entre redes remotas, come se estivessem conectados em uma rede privada. Em resumo, o VPN “transforma” a rede pública em uma rede privada. Ele encapsula seus dados que estavam desprotegidos, como se colocasse dentro de um túnel, não deixando ninguém ver.

Funcionamento na prática:



**Como funciona tecnicamente?**

Estabelecendo Conexão

* O dispositivo do usuário inicia contato com o servidor VPN;
* O servidor autentica o usuário através de credenciais;

Processo de Tunelamento

* Cada pacote de dados é encapsulado dentro de outro pacote;
* O pacote interno contém os dados originais (destinados ao alvo final);
* O pacote externo contém informações de roteamento para o servidor VPN.

Fluxo de Dados

Cliente → [Pacote Criptografados] → Internet Pública → Servidor VPN → [Pacote Descriptografado] → Destino Final

**Características VPN**

* Tunelamento: estabelece um “Túnel” virtual através da internet;
* Criptografia: protege os dados transmitidos contra interceptação;
* Autenticação: Verifica a identidade os usuários e dispositivos que tentam se conectar;
* Encapsulamento: Envolve os pacotes de dados originais em novos pacotes com informações adicionais de roteamento e segurança.

**Tipos de VPN**

* VPN de Acesso Remoto: **conecta** **usuários individuais** a uma rede privada;
* VPN Site-a-Site: **conecta redes inteiras** entre si;
* VPN Intranet: **conecta diversos departamentos** de uma organização;
* VPN Extranet: **conecta a organização com parceiros externos**, clientes e fornecedores.

**Aplicações**

As VPNs possuem diversas aplicações fundamentais em ambientes corporativos, governamentais, individuais e até universitários.

Aplicações Empresariais:

* Permite que funcionários acessem recursos da rede corporativa de qualquer lugar;
* Mantém a segurança dos dados sensíveis durante o acesso externo;
* Permite a interconexão entre filiais;
* Pode estabelecer conexão com parceiros e fornecedores.

Aplicações para Usuários:

* Oculta o endereço IP real e criptografa o tráfego.
* Protege durante o uso de redes Wi-Fi públicas não seguras;
* Dificulta o rastreamento por anunciantes e outros terceiros;
* Permite acesso a conteúdo bloqueado geograficamente;
* Possibilita o uso de serviços não disponíveis em determinadas regiões
* Possibilita o uso de serviços não disponíveis em determinadas regiões.

**Desafios e Limitações**

Bloqueio de VPN

* Alguns países e organizações bloqueiam ativamente conexões VPN.

Confiança no Provedor

* O provedor de VPN pode teoricamente monitorar o tráfego, portanto é importante escolher serviços que tenham políticas claras de não retenção de logs.

Falsos Sensos de Segurança

* VPNs não protegem contra todos os vetores de ataque, é necessário ter bom senso e tomar outras medidas desegurança, não ache que está totalmente seguro.B