Atividade Integradora - Extra sala

VPN (Virtual Private Network) é uma tecnologia que cria uma conexão segura e criptografada entre o seu dispositivo e outro ponto na internet. Ela funciona como um "túnel" que protege os dados que você envia e recebe. Ela também impede que terceiros, como hackers, vejam suas atividades online.

Tipos de VPN:

1. Site-to-Site: é uma rede de conexão com que configura diversas redes, usando criptografia. Pode ser corporativa, onde vários escritórios trabalham em conjunto entre si, ou uma rede de filiais, com um escritório central e várias filiais. As redes locais dos dois lados podem se comunicar como se estivessem fisicamente conectadas.

Exemplo: Escritórios em São Paulo e Rio de Janeiro conectados para compartilhar recursos internos.

2. Remote Access: é projetada para usuários individuais que precisam acessar remotamente uma rede corporativa. O funcionário instala um cliente VPN no dispositivo, que estabelece uma conexão segura com a rede da empresa. Assim, mesmo estando fora do escritório, ele pode acessar servidores, arquivos e sistemas internos como se estivesse no local.

Exemplo: Funcionário em home office acessa o servidor da empresa.

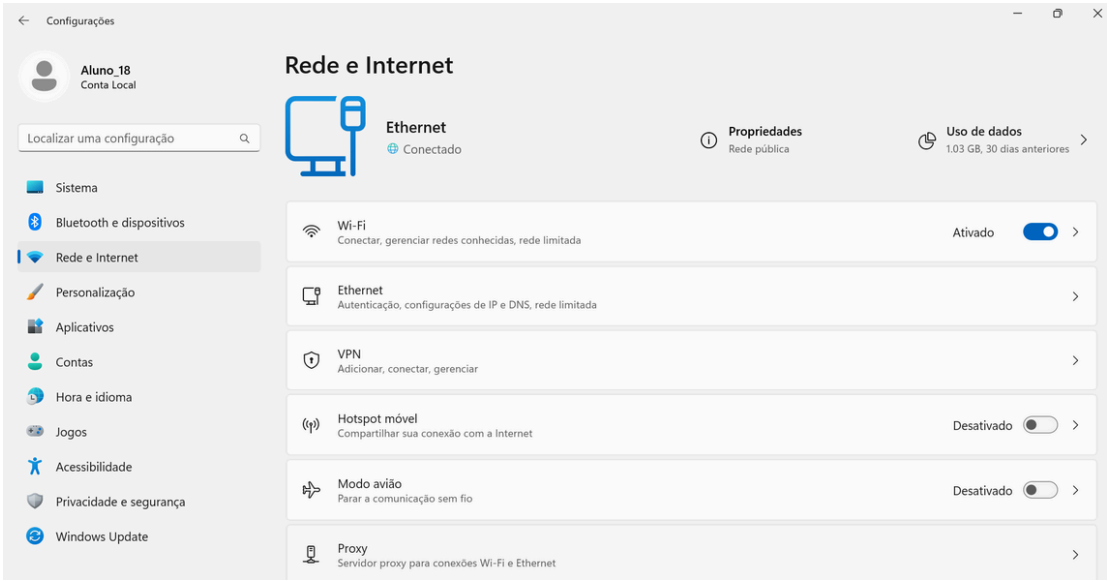
3.Client-to-Cloud: conecta diretamente o dispositivo de um usuário ou cliente a um serviço hospedado na nuvem. É muito usado por empresas que utilizam a nuvem como armazenamento de dados ou plataformas de colaboração, garantindo que a conexão seja segura e criptografada. Isso elimina a necessidade de passar pela rede corporativa para acessar os serviços.

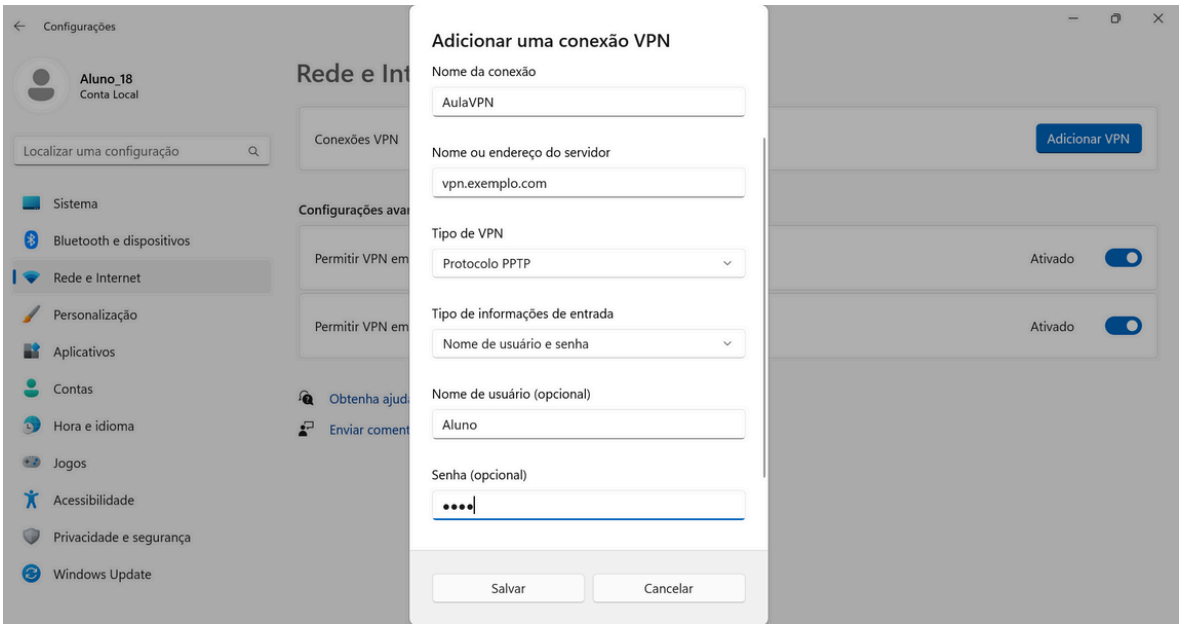
Exemplo: Usuário acessa dados no Google Drive em um Wi-Fi público.

Aspecto	Site-to-Site	Remote Access	Client-to-Cloud
Vantagens	Conecta redes inteiras de forma segura e eficiente.	Permite acesso remoto a sistemas corporativos.	Facilita acesso direto a serviços na nuvem.
	Reduz custos com links dedicados entre filiais.	Ideal para home office e trabalho remoto.	Evita a dependência da rede corporativa para uso na nuvem.
	Garante comunicação estável entre escritórios.	Criptografa os dados do usuário.	Simples de configurar para uso em dispositivos móveis.
Desvantagens	Requer infraestrutura mais complexa e custo inicial alto.	Pode ser mais lenta em conexões de internet instáveis.	Depende da segurança do serviço de nuvem usado.
	Menos flexível para usuários individuais.	Vulnerável a configurações inadequadas.	Não conecta à rede local corporativa, apenas à nuvem.
	Exige maior experiência técnica para configuração.	Exige instalação de software cliente.	Pode ter custos adicionais por serviços na nuvem.

Tarefa 2 - Configuração de VPN

Passo a passo para configurar uma VPN no seu computador:





A configuração de uma VPN, como feita anteriormente, é importante para proteger dados em redes públicas, como o Wi-Fi do SENAI. Ela cria o “túnel” (dito na pesquisa) criptografado entre o dispositivo do usuário e o servidor, garantindo que os dados transmitidos sejam protegidos. A criptografia dificulta que invasores leiam informações. Além disso, a autenticação com nome de usuário e senha impede o acesso não autorizado.

No entanto, o uso de uma VPN pode impactar o desempenho da rede. A criptografia pode aumentar a latência, resultando em um tempo maior para o envio e recebimento dos dados. A velocidade da conexão também pode ser reduzida, pois os dados precisam passar pelo servidor VPN. Em redes públicas congestionadas, como no SENAI, esses efeitos podem ser mais visíveis.