INSTITUTO FEDERAL DE SÃO PAULO

ANDREY NAGATANI

DOUGLAS GUSTAVO DA SILVA

FELIPE APARECIDO AMERICO COSTA

GABRIELA MAYUMI MATHIAS KADOKI

GABRIEL LUÍS DE LIMA CAPODEFERRO

GABRIEL RAMOS DE SOUZA

JOSÉ MARCELO RODRIGUES ARAUJO

LEANDRO BARBOSA DE PAULA

SEGURANÇA DIGITAL: Tudo Sobre VPNs

BRAGANÇA PTA - SP

2024

INSTITUTO FEDERAL DE SÃO PAULO

Andrey Nagatani BP3044505

Douglas Gustavo da Silva BP3055043

Felipe Aparecido Americo Costa BP3054179

Gabriela Mayumi Mathias Kadoki BP3053555

Gabriel Luís de Lima Capodeferro BP3053628

Gabriel Ramos de Souza BP3000958

José Marcelo Rodrigues Araujo BP3016331

Leandro Barbosa de Paula BP3053717

Segurança Digital: Tudo sobre VPNs

Trabalho de dissertação, apresentado como requisito parcial para aprovação na disciplina de EXTENSÃO COMO METODOLOGIA DE ENSINO 1 em _____, pelo Instituto Federal de São Paulo.

Bragança Pta - SP

2024

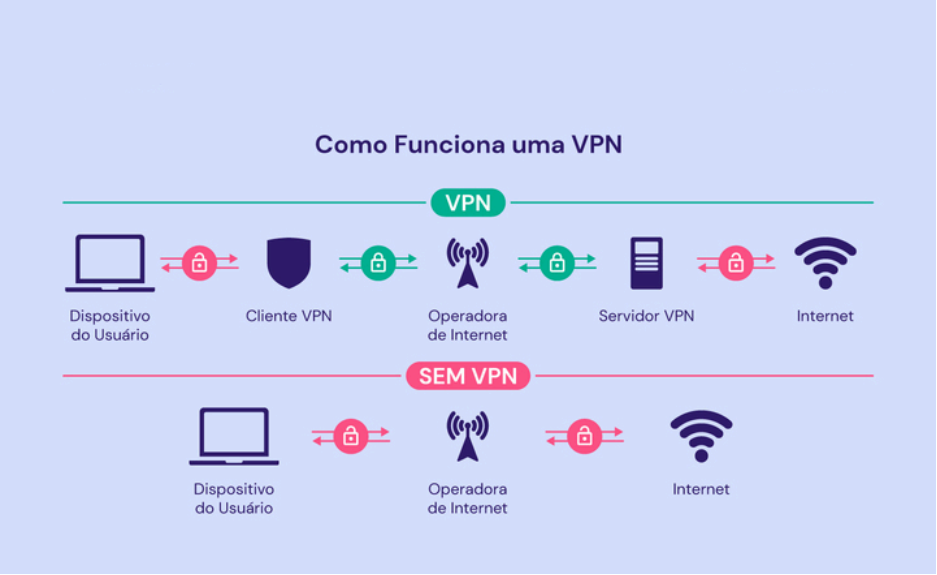
Sumário

O que é uma VPN

Uma VPN, ou Rede Privada Virtual, é uma tecnologia que cria uma conexão segura e criptografada entre o seu dispositivo e a internet. Basicamente, ela permite que você navegue de forma anônima, escondendo seu endereço IP e local real. Como definido pela VPN Mentor, "uma VPN permite que você acesse a internet como se estivesse em outro lugar, protegendo sua privacidade e dados pessoais".

Uma analogia popular usada para explicar VPNs é dizer que a VPN funciona como se fosse um túnel, quando usada a sua conexão com a internet passa por este túnel que encapsula a sua conexão(criptografia) protegendo os seus dados e identidade, qualquer agente que esteja do lado de fora deste túnel não pode ver as suas informações.

Como funciona uma VPN?



Quando você se conecta à internet sem usar uma rede virtual privada (VPN), sua operadora atua como a principal intermediária entre seu dispositivo e a web. O provedor de internet fornece um endereço de IP único para seu dispositivo (como computador, celular ou tablet) e monitora todos os sites que você acessa.

Ao usar uma VPN, a conexão da rede virtual é ativada no seu dispositivo. Assim, todas as suas solicitações na internet são enviadas por um túnel criptografado. Os dados que saem do seu dispositivo são direcionados por um servidor VPN antes de alcançar o servidor de destino.

Depois que a solicitação é processada no servidor do site, as informações são enviadas de volta para você através da mesma conexão VPN criptografada, seguindo o mesmo processo de roteamento.

Portanto, mesmo ao utilizar uma VPN, a conexão do seu dispositivo ainda passa pela operadora. No entanto, como a conexão está criptografada e roteada através do servidor VPN, seu provedor não consegue ver os sites que você visita. Ele apenas saberá que você está conectado a uma VPN e que está trocando tráfego criptografado entre seu dispositivo e um servidor.

Para entender melhor como uma VPN funciona, aqui estão alguns dos processos principais que ela realiza e seus benefícios:

- **Proxying**: A VPN atua como um proxy, escondendo seu endereço de IP e sua localização, aumentando assim seu anonimato online. Os sites que você acessa verão apenas o IP e a localização do servidor VPN em vez de suas informações pessoais.
- **Autenticação**: Esse processo assegura que seu cliente VPN se conecte apenas ao servidor VPN desejado, prevenindo a interceptação de dados por terceiros.
- **Tunneling**: A VPN cria um “túnel criptografado” para processar o tráfego na internet, encapsulando cada pacote de dados dentro de outro, dificultando a ação de terceiros mal-intencionados.
- **Criptografia**: Embora muitos sites usem SSL/TLS ou HTTPS para criptografar dados trocados, uma VPN criptografa todo o tráfego na rede. Muitos provedores de VPN aplicam técnicas de criptografia avançadas, tornando quase impossível a leitura dos seus dados de navegação.

Esses processos trabalham em conjunto para proteger suas informações contra seu provedor de internet e outras entidades que possam tentar interceptar seus dados.

Aqui estão algumas informações pessoais que a tecnologia VPN pode ocultar quando ativada:

- **Endereço de IP**: Este é o identificador único do seu dispositivo. A partir dele, é possível deduzir informações sensíveis, como seu provedor de internet, país, cidade e até mesmo seu endereço residencial. A VPN substitui seu IP pelo IP do servidor VPN.
- **Localização**: Como a VPN oculta seu verdadeiro endereço de IP, é possível fazer parecer que você está navegando de um lugar diferente. Por exemplo, se você estiver no Brasil, mas conectado a um servidor no Reino Unido, os outros usuários acreditarão que você está no Reino Unido.
- **Histórico de navegação e busca**: Com sua conexão em uma VPN criptografada, seu provedor de internet e usuários externos não poderão ver suas buscas online nem onde você está navegando, ajudando a evitar anúncios direcionados e a proteger sua privacidade de forma geral.

Para que serve uma VPN?

Privacidade online, A VPN oculta suas atividades na internet de provedores de serviços e possíveis bisbilhoteiros. Segundo a Electronic Frontier Foundation, "usar uma VPN é uma maneira eficaz de proteger sua privacidade ao navegar na internet".

Acesso a conteúdos restritos por *geoblocking*, muitas vezes, serviços de streaming e sites têm restrições geográficas. Com uma VPN, você pode se conectar a um servidor em outro país e acessar conteúdos que normalmente não estariam disponíveis na sua região.

Segurança em redes públicas, ao usar Wi-Fi público, seus dados estão vulneráveis a ataques. Uma VPN protege suas informações, como senhas e dados bancários, garantindo uma camada extra de segurança.

Quando usar uma VPN?

- Navegando em redes públicas: Sempre que você se conectar a uma rede Wi-Fi pública, é recomendável usar uma VPN para proteger seus dados.
- Ao acessar conteúdo restrito: Se você deseja assistir a um filme ou programa que não está disponível na sua região, uma VPN pode ser a solução.
- Para maior privacidade: Se você se preocupa com rastreamento online e deseja navegar de forma mais anônima, usar uma VPN é uma boa prática.

Em resumo, uma VPN é uma ferramenta essencial para quem busca mais privacidade e segurança na internet.

É seguro usar uma VPN?

Sim, usar uma VPN pode ser seguro, mas a sua segurança está diretamente relacionada ao provedor de VPN que for escolhido. No mercado atual existem diversos provedores variando entre provedores gratuitos e pagos, provedores que mantém ou não logs de utilização, quais tipos de criptografia são utilizados e por último em qual região o provedor opera.

Qual VPN usar

Não existe uma recomendação absoluta, um provedor que outrora seria considerado seguro pode ser comprometido, da mesma forma em que provedores considerados inseguros podem realizar correções e melhorias.

Quem precisa usar uma VPN precisa estar atento ao mundo da cibersegurança acompanhando o status de provedores de interesse. Porém podemos dizer que você deve fugir de provedores que oferecem serviços de VPN gratuitos, como diz o ditado popular moderno:

‘Se o serviço é de graça, você é o produto;’

Provedores que oferecem VPNs de forma gratuita dependem de formas alternativas para adquirir uma fonte de renda, seja por mostrar anúncios em seus

produtos ou até mesmo coletando os seus dados de usos para vendê-los a terceiros.

Se você deseja escolher um provedor pago busque por aqueles que oferecem transparências em seus serviços com auditorias públicas e a garantia de que logs de uso não serão mantidos. Por último, para aqueles que desejam controle total e a garantia de que suas necessidades serão atendidas não existe melhor opção do que a de hospedar a sua própria VPN.

Hospedar a sua própria VPN

Nos dias de hoje, a privacidade online é mais importante do que nunca. Uma VPN (Rede Privada Virtual) é uma ferramenta poderosa que ajuda a proteger suas informações, mascarando seu endereço IP e criptografando sua conexão. Embora existam muitos serviços de VPN disponíveis, hospedar sua própria VPN oferece controle total sobre seus dados e configurações. Aqui estão algumas vantagens e um guia básico para você começar.

Vantagens de Hospedar Sua Própria VPN

1. **Controle Total**: Ao hospedar sua própria VPN, você tem controle absoluto sobre suas configurações de segurança e privacidade. Isso significa que você pode ajustar as políticas de segurança de acordo com suas necessidades.
2. **Privacidade Aumentada**: Usar um serviço de terceiros pode implicar em riscos, já que seus dados podem ser armazenados ou monitorados. Com uma VPN própria, você reduz esses riscos, mantendo suas informações longe de olhares curiosos.
3. **Custo-efetivo**: Embora haja um investimento inicial em hardware ou serviços de nuvem, a longo prazo, uma VPN própria pode ser mais econômica do que pagar mensalmente por um serviço.
4. **Acesso Remoto**: Você pode acessar sua rede local de qualquer lugar do mundo, como se estivesse em casa, permitindo o acesso seguro a arquivos e dispositivos.

Passos para Hospedar Sua Própria VPN

1. **Escolha a Plataforma**: Você pode optar por um servidor físico em casa ou usar um serviço de nuvem como Amazon Web Services, DigitalOcean ou Linode. Para iniciantes, a nuvem pode ser mais simples.
2. **Selecione um Software de VPN**: Existem várias opções disponíveis, como OpenVPN, WireGuard e SoftEther. O OpenVPN é popular pela sua robustez, enquanto o WireGuard é conhecido por ser leve e fácil de configurar.
3. **Instalação do Servidor**:
    - **Em um servidor local**: Instale o sistema operacional (como Ubuntu) e configure o software de VPN escolhido.
    - **Em um servidor na nuvem**: Crie uma instância e siga as instruções de instalação do software.
4. **Configuração da Rede**: Configure as regras de firewall para permitir o tráfego da VPN. Isso é crucial para garantir que a conexão seja segura.
5. **Configuração dos Clientes**: Após configurar o servidor, instale e configure o cliente de VPN em seus dispositivos (computadores, smartphones, etc.). Isso geralmente envolve a criação de perfis com as credenciais de acesso.
6. **Testes e Manutenção**: Após a configuração, realize testes para garantir que a conexão esteja funcionando corretamente. Mantenha o software sempre atualizado para garantir a segurança.

Wireguard

O WireGuard é uma VPN extremamente simples, porém rápida e moderna, que utiliza criptografia de última geração. Seu objetivo é ser mais rápido, mais simples, mais enxuto e mais útil que o IPsec, evitando a enorme dor de cabeça. Pretende ser consideravelmente mais eficiente do que o OpenVPN.

O WireGuard foi projetado como uma VPN de uso geral para ser executado tanto em interfaces incorporadas quanto em supercomputadores, adequado para muitas circunstâncias diferentes. Inicialmente lançado para o kernel do Linux, agora é multiplataforma (Windows, macOS, BSD, iOS, Android) e amplamente

implementável. No momento, ele está em pleno desenvolvimento, mas já pode ser considerado a solução de VPN mais segura, mais fácil de usar e mais simples do setor.

OpenVPN

O OpenVPN é um software livre e open-source para criar redes privadas virtuais do tipo ponto-a-ponto ou server-to-multiclient através de túneis criptografados entre computadores.

Ele é capaz de estabelecer conexões diretas entre computadores mesmo que estes estejam atrás de Nat Firewalls sem necessidade de reconfiguração da sua rede. Ele foi escrito por James Yonan e publicado sob licença GNU General Public Licence (GPL).

Conclusão

Apesar de uma tema extremamente técnico, é importante entender o conceito de uma VPN, que são apenas uma das várias camadas que compõem uma navegação segura, e nem sempre VPN é a resposta ideal, diferentes cenários exigem diferentes respostas.

VPNs são uma ferramenta poderosa em um cenário que pede por ela, sendo corretamente configurada e utilizada caso contrário pode se tornar uma vulnerabilidade.

Com este trabalho esperamos ter esclarecido o que é e como funciona uma VPN, agora você saberá se a VPN é a estratégia ideal ou não para a sua situação.

Referências:

1. "virtual private network". NIST Computer Security Resource Center Glossary. Archived from the original on 2 January 2023. Retrieved 2 January 2023.
2. "What Is a VPN? - Virtual Private Network". Cisco. Archived from the original on 31 December 2021. Retrieved 5 September 2021.
3. Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p. 7. ISBN 9781587050336.
4. RFC 3809 - Generic Requirements for Provider Provisioned Virtual Private Networks. sec. 1.1. doi:10.17487/RFC3809. RFC 3809.
5. "Connect to a VPN in Windows - Microsoft Support". support.microsoft.com. Retrieved 11 July 2024.
6. "Connect to a virtual private network (VPN) on Android". Retrieved 11 July 2024.
7. "VPN settings overview for Apple devices". Apple Support. Retrieved 11 July 2024.
8. "IPsec/IKEv2 Library". Android Open Source Project. Retrieved 11 July 2024.
9. RFC 6434, "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2011)
10. https://www.cisa.gov/topics/cybersecurity-best-practices
11. https://www.hostinger.com.br/tutoriais/o-que-e-vpn#Como_uma_VPN_Funciona
12. https://www.wireguard.com/papers/wireguard.pdf
13. https://openvpn.net/