Trey Research Corporation

Redes virtuais privadas: uma visão geral técnica para a Fabrikam, Inc.

15 de dezembro de 2023

Redes virtuais privadas (VPNs) são uma solução popular de segurança de rede que ajuda a criptografar o tráfego de rede. As VPNs atuam como um túnel seguro e criptografam o tráfego da Internet, tornando mais difícil para terceiros rastrearem atividades e roubarem dados[1].

Prós da implementação de VPNs:

- As VPNs fornecem uma camada de privacidade e segurança ao criptografarem o tráfego da Internet, dificultando que terceiros rastreiem atividades e roubem dados.
- As VPNs são especialmente úteis para proteger contra ataques ao usar Wi-Fi público em locais como aeroportos ou bibliotecas, pois atuam como um túnel seguro e criptografam o tráfego da Internet.
- As VPNs podem ocultar os sites que você visita do seu provedor de serviços de Internet, já que todo o tráfego de entrada e saída do seu computador passa pelos servidores da VPN, ou pelos servidores que a VPN paga para usar [1].
- As VPNs podem contornar restrições geográficas de conteúdo [2] mascarando seu endereço IP e criptografando sua conexão com a Internet. Ao se conectar a um servidor VPN, seu tráfego de Internet é redirecionado através desse servidor, que atribui a você um novo endereço IP. É como se você estivesse navegando na Internet a partir de uma localização diferente, podendo acessar conteúdo com restrições geográficas.

Contras da implementação de VPNs:

- As velocidades de conexão podem ser mais lentas do que as fornecidas pelo seu provedor de serviços de Internet (ISP). Isso ocorre porque as VPNs adicionam uma camada extra de criptografia e roteamento ao seu tráfego de Internet [2].
- O uso de VPNs é proibido em alguns países autoritários. Em certos países, as VPNs são proibidas ou altamente regulamentadas [2].
- O uso de VPNs gratuitas pode expor você a anúncios, malware e vazamentos. As VPNs gratuitas podem vender dados do usuário para anunciantes de terceiros ou inserir anúncios em páginas da Web [2].

Especificações de instalação:

- Uma VPN estabelece um túnel criptografado entre o sistema que executa o cliente VPN e um servidor VPN, pelo qual encaminha o tráfego para o restante da rede corporativa [4]. As etapas incluem:

    1. Um cliente VPN é instalado no dispositivo do usuário, que criptografa todo o tráfego entre o dispositivo e o servidor VPN.
    2. O servidor VPN descriptografa o tráfego e o encaminha para o destino pretendido.
    3. O servidor de destino responde à solicitação enviando o tráfego de volta para o servidor VPN.
    4. O servidor VPN criptografa o tráfego e o envia de volta para o cliente VPN.
    5. O cliente VPN descriptografa o tráfego e o envia para o dispositivo do usuário [1].

- Para instalar e configurar um servidor VPN, siga estas etapas:
    1. Crie um perfil VPN no seu computador.
    2. Clique em "Iniciar" e, em seguida, clique em "Configurações" para abrir o menu de configurações.
    3. No menu de configurações, clique em "Rede e Internet" e, em seguida, em "VPN".
    4. Selecione "Adicionar uma conexão VPN".
    5. Na janela "Adicionar uma conexão VPN", há algumas tarefas a serem realizadas.
    6. Salve as alterações feitas [5].

Riscos e mitigações:

- Os invasores reconhecem o trabalho remoto como um vetor de ameaça há algum tempo. O ambiente de trabalho remoto é especialmente atraente para os invasores por vários motivos. Em primeiro lugar, o ambiente das redes domésticas não é gerenciado profissionalmente. O aspecto mais crítico é que muitos dos sistemas de redes domésticas não são atualizados regularmente, e alguns deles estão desatualizados em relação à mitigação de vulnerabilidades. Para permanecer na rede corporativa após explorar um sistema, um invasor precisa evitar a detecção e resistir à correção. Além disso, as redes domésticas são favoráveis a isso, pois geralmente têm pouca ou nenhuma detecção de ameaças e a correção é feita apenas quando um computador é formatado ou desativado por problemas de desempenho. Para proteger adequadamente o ambiente de trabalho remoto, é necessário expandir a abordagem de confiança zero. Não é apenas a rede que deve ser considerada hostil, mas tudo o que não estiver sob o controle da empresa [4].
- Mantenha as VPNs, os dispositivos da infraestrutura de rede e os dispositivos utilizados para acesso remoto a ambientes de trabalho atualizados com as últimas correções de software e configurações de segurança [6].

Melhores práticas de implementação:

Estas são algumas das melhores práticas para implementar VPNs em uma rede corporativa:

- Selecione VPNs baseadas em padrões que utilizem os padrões aceitos, como os protocolos IKE/IPSec, que geralmente são menos arriscadas e mais seguras do que as VPNs que utilizam os protocolos SSL/TLS com código personalizado para enviar tráfego sobre TLS [12].
- Use uma VPN com criptografia forte. Confirme que os algoritmos de criptografia, os algoritmos de autenticação e os protocolos usados por uma VPN são fortes e validados pela FIP. Configure todas as VPNs para usar autenticação multifator (MFA) e substitua a autenticação baseada em senha por autenticação de cliente através de certificados digitais (armazenados em cartões inteligentes) sempre que possível [12].
- Gerencie vulnerabilidades de software. A exploração de vulnerabilidades em VPNs é um vetor de ataque comum para criminosos cibernéticos. Selecione um fornecedor de VPN com um histórico sólido de aplicação de patches de vulnerabilidades e solicite uma lista de materiais de software (SBOM) para validar que o código de terceiros está atualizado e seguro. Além disso, procure um produto que possa realizar a validação de seu código durante a execução

para detectar possíveis invasões. Após implantar uma VPN, verifique regularmente e aplique prontamente as atualizações de software [1][2].

- Prepare-se para picos de uso. O pessoal de segurança da informação deve testar as limitações da VPN em preparação para o uso em massa [2].
- Evite VPNs gratuitas. O uso de VPNs gratuitas pode expor você a anúncios, malware e vazamentos [3].