1.Introdução a VPNs

Uma VPN é virtual, pois carrega informações dentro de uma rede privada, mas essas informações são realmente transportadas por uma rede pública. **Uma VPN é privada**, pois o tráfego é criptografado para manter os dados confidenciais enquanto são transportados pela rede pública. Os modernos VPNs agora suportam recursos de criptografia, como segurança do Protocolo da Internet (IPSec) e Secure Sockets Layer (SSL) para proteger o tráfego de rede entre sites.

Benefícios	Descrição
Redução de custos	Com o advento de tecnologias econômicas e de alta largura de banda, as organizações podem usar VPNs para reduzir seus custos de conectividade enquanto aumenta simultaneamente a largura de banda da conexão remota
Segurança	As VPNs fornecem o mais alto nível de segurança disponível, usando protocolos avançados de criptografia e autenticação que protegem os dados de acesso não autorizado
Escalabilidade	As VPNs permitem que as organizações usem a Internet, facilitando a adição novos usuários sem adicionar infraestrutura significativa
Compatibilidade	As VPNs podem ser implementadas em uma ampla variedade de opções de link WAN incluindo todas as tecnologias populares de banda larga. Trabalhadores remotos podem aproveitar essas conexões de alta velocidade para obter acesso seguro às suas redes corporativas

1.1 VPN de site para site

Uma VPN site a site é criada quando os dispositivos de terminação da VPN, também chamados de gateways VPN, são pré-configurados com informações para estabelecer um túnel seguro. O tráfego da VPN é criptografado apenas entre esses dispositivos. Os hosts internos não sabem que uma VPN está sendo usada.

1.2 VPN de acesso remoto

Uma VPN de acesso remoto é criada dinamicamente para estabelecer uma conexão segura entre um cliente e um dispositivo de terminação da VPN.

As VPNs de acesso remoto também permitem que contratados e parceiros tenham acesso limitado a servidores, páginas da Web ou arquivos específicos, conforme necessário. Isso significa que esses usuários podem contribuir para a produtividade dos negócios sem comprometer a segurança da rede.

1.3 Conexão VPN sem cliente

A conexão é protegida usando uma conexão SSL do navegador da web. O SSL é usado principalmente para proteger o tráfego HTTP e HTTPS e os protocolos de e-mail, como IMAP e POP3.

1.4 Conexão VPN baseada no cliente

O software cliente VPN, como o Cisco AnyConnect Secure Mobility Client, deve ser instalado no dispositivo final do usuário remoto. Os usuários devem iniciar a conexão VPN usando o cliente VPN e, em seguida, autenticar no gateway VPN de destino. Quando usuários remotos são autenticados, eles têm acesso a arquivos e aplicativos corporativos. O software cliente VPN criptografa o tráfego usando IPsec ou SSL e o encaminha para o gateway VPN de destino.

O ***SSL*** usa a infraestrutura de chave pública e os certificados digitais para autenticar pares. As tecnologias IPsec e SSL VPN oferecem acesso a praticamente qualquer recurso ou aplicativo de rede. No entanto, quando a segurança é um problema, o IPsec é a escolha superior. Se o suporte e a facilidade de implantação forem os principais problemas, considere o SSL. O tipo de método de VPN implementado é baseado nos requisitos de acesso dos usuários e nos processos de TI da organização.

A tabela compara implantações de acesso remoto IPsec e SSL.

Recurso	IPsec	SSL
Aplicativos suportados	**Extensivo:** Todos os aplicativos baseados em IP são suportado	**Limitado:** Somente aplicativos e arquivos baseados no compartilhamento Web são suportados
Força de autenticação	**Forte:** Usa autenticação bidirecional com chaves compartilhadas ou certificados digitais	**Moderado:** Usando autenticação unidirecional ou bidirecional
Força de criptografia	**Forte:** Usa comprimentos de chave de 56 a 256 bits	**Moderado a forte:** Com comprimentos de chave de 40 bits a 256 bits
Complexidade da conexão	**Médio:** Porque requer um cliente VPN pré-instalado em um host	**Baixo:** Requer apenas um navegador da web em um host
Opção de conexão	**Limitado:** Somente dispositivos específicos com configurações podem se conectar	**Extensivo:** Qualquer dispositivo com um navegador da WEb pode conectar

As VPNs site a site são usadas para conectar redes através de outra rede não confiável, como a Internet. Em uma VPN site a site, os hosts finais enviam e recebem tráfego TCP / IP não criptografado normal por meio de um dispositivo de terminação VPN. O dispositivo de terminação VPN é normalmente chamado de gateway VPN. Um dispositivo de gateway VPN pode ser um roteador ou um firewall.

O gateway VPN encapsula e criptografa o tráfego de saída. Em seguida, ele envia o tráfego através de um túnel VPN pela Internet para um gateway VPN no site de destino. Após o recebimento, o gateway VPN receptor retira os cabeçalhos, descriptografa o conteúdo e retransmite o pacote em direção ao host de destino dentro de sua rede privada. As VPNs site a site geralmente são criadas e protegidas usando a segurança IP (IPsec).