SOPHOS
Cybersecurity evolved.

Seis principais vantagens do ZTNA

Comparação com VPN de acesso remoto

Documento técnico Sophos. Outubro, 2021

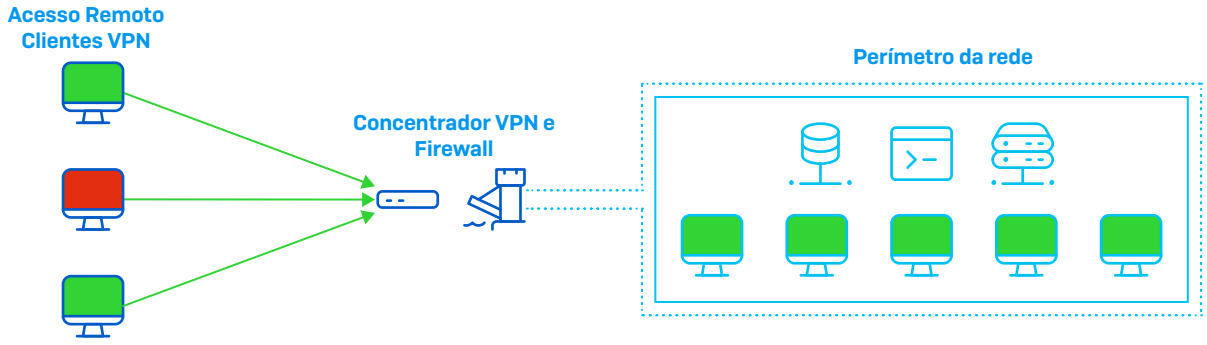
A VPN de acesso remoto tem nos servido muito bem e há muito tempo, mas o aumento no trabalho remoto trouxe à tona as limitações dessa tecnologia. Algumas organizações continuam a obter e explorar o excelente valor da VPN, porém outras muitas estão buscando uma alternativa melhor, algo que resolva os desafios com a VPN de acesso remoto. Várias organizações já começaram a abraçar a nova tecnologia de acesso remoto Next Gen: ZTNA ou Zero Trust Network Access. O ZTNA oferece melhor segurança, controle com maior granularidade, visibilidade aumentada e uma experiência de usuário transparente em comparação com a tradicional VPN de acesso remoto.

Neste guia para compradores de ZTNA examinaremos as limitações e os desafios com a VPN de acesso remoto tradicional e os benefícios que o Zero Trust Network Access pode oferecer e criaremos uma lista dos recursos críticos que você deve procurar na sua nova solução ZTNA.

Desafios com a VPN de acesso remoto

A VPN de acesso remoto tem sido uma constante na maioria das redes por décadas, oferecendo um modo de acessar sistemas e recursos remotamente na rede. Contudo, ela foi desenvolvida durante uma época em que as redes corporativas se assemelhavam a fortalezas medievais: as muralhas do castelo contornadas por um fosso formando o perímetro de segurança ao redor de sua rede de recursos. A VPN oferecia o equivalente a uma portaria de acesso para usuários autorizados entrarem nesse perímetro seguro, mas que, uma vez que adentrassem, teriam acesso total a tudo dentro desse perímetro.

VPN de acesso remoto tradicional



As redes evoluíram substancialmente e estão muito mais distribuídas do que antes. Agora, aplicativos e dados coabitam na nuvem, os usuários trabalham remotamente e as redes estão sitiadas por hackers buscando pontos fracos para explorar.

Administrar uma solução de acesso remoto baseada na VPN tradicional (IPSec/SSL) em qualquer tipo de ambiente moderno pode ser extremamente árduo. Você tem que se engalfinhar com gerenciamento de IP, fluxos e roteamento de tráfego, regras de acesso a firewall, além de implantação e configuração de cliente e certificado. Qualquer coisa além de uns poucos nós e algumas dezenas de usuários já se transforma em uma tarefa de tempo integral desnecessária – e isso é só para manter o processo rodando. Como se não bastasse, a segurança se torna um absoluto pesadelo para monitorar e controlar.

Em resumo, a VPM de acesso remoto tradicional tem um rol de limitações e desafios desnecessários:

1. **Confiança implícita** – A VPN de acesso remoto faz um bom trabalho ao levá-lo através do perímetro e pela rede corporativa como se você estive presente fisicamente, mas, nesse ponto, você já é implicitamente confiável e recebeu acesso amplo aos recursos na rede que podem ser desnecessários e um enorme risco à segurança.
2. **Possível vetor de ameaças** – A VPN de acesso remoto não tem noção do estado do dispositivo usado para se conectar à rede corporativa, criando um possível conduíte de entrada de ameaças à rede a partir de dispositivos que possam estar comprometidos.
3. **Transporte ineficiente** – A VPN de acesso remoto oferece um único ponto de presença na rede, que possivelmente exigirá transporte de tráfego a partir de várias localizações, datacenters ou aplicativos através do túnel de VPN de acesso remoto.
4. **Falta de visibilidade** – A VPN de acesso remoto não tem noção do tráfego e dos padrões de uso que está facilitando a visualização das atividades do usuário e de uso do aplicativo e tornando o problema mais desafiador.
5. **Experiência do usuário** – Os clientes VPN de acesso remoto são notórios por oferecerem uma experiência insatisfatória ao usuário, adicionando latência ou afetando o desempenho negativamente, criando problemas de conectividade e, geralmente, sendo um estorvo para o pessoal do helpdesk.
6. **Administração, implantação e registro** – Os clientes VPN de acesso remoto são difíceis de configurar, implantar, registrar novos usuários e desativar os usuários removidos do sistema. A VPN também é difícil de administrar no lado do firewall ou gateway, especialmente com vários nós, regras de acesso a firewall, gerenciamento de IP, e fluxos e roteamento de tráfego. Não tarda muito para se tornar um trabalho de período integral.

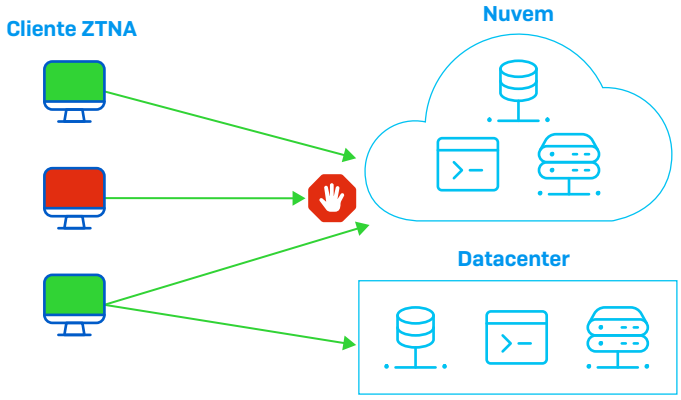
O que é ZTNA e como funciona

O ZTNA, ou Zero Trust Network Access, foi criado desde o princípio para lidar com os desafios e limitações da VPN de acesso remoto, oferecendo uma melhor solução para os usuários para uma conexão segura aos aplicativos e dados de que precisam para fazer o trabalho, porém nada mais. Existem algumas diferenças fundamentais que distinguem a ZTNA da VPN de acesso remoto.

O conceito por trás do nome ZTNA se baseia no princípio do Zero Trust: confie, mas confira. Essencialmente, o Zero Trust elimina o conceito perimetral das antigas muralhas contornadas por fossos e o substitui por um perímetro isolado por cada usuário, dispositivo e aplicativo na rede, interconectando-os somente após validar suas credenciais, verificar a integridade do dispositivo e confirmar a política de acesso. Isso melhora sensivelmente a segurança, segmentação e controle.

Outra diferença fundamental em como o ZTNA opera é que os usuários não ficam simplesmente largados na rede com total liberdade de movimento. Pelo contrário, os túneis individuais são estabelecidos entre o usuário e o gateway específico para o aplicativo ao qual tem autorização de acesso, e nada mais, oferecendo um nível de microssegmentação muito mais seguro. Isso oferece vários benefícios para a segurança, controle, visibilidade, eficiência e desempenho. Por exemplo, a VPN de acesso remoto não oferece nenhum insight sobre quais aplicativos os usuários acessam, enquanto a ZTNA pode oferecer status e atividade em tempo real de todos os aplicativos, mostrando o seu valor inestimável para a identificação de possíveis problemas e a realização de auditorias de licenciamento. A microssegmentação que a ZTNA oferece garante que não haja movimentos laterais no acesso do dispositivo ou usuário entre recursos na rede. Literalmente, cada usuário, dispositivo e aplicativo ou recurso demarca o seu próprio perímetro de segurança, dispensando quaisquer outros conceitos implícitos de confiança.

Zero Trust Network Access



Inerentemente, a ZTNA também é mais dinâmica e transparente por natureza, trabalhando em segundo plano sem exigir interação do usuário além da validação inicial de identidade. Essa experiência pode ser tão tranquila que os usuários nem mesmo notarão que estão conectados a aplicativos por meio de túneis de segurança criptografados.

Vantagens do ZTNA

O Zero Trust Network Access oferece grandes benefícios em diferentes formas, mas, essencialmente, ele é adotado por um ou mais destes motivos:

- **Trabalhar de casa:** as soluções ZTNA facilitam o gerenciamento do acesso remoto dos funcionários que trabalham de casa. Elas deixam a implantação e o registro muito mais fácil e flexível, transformando o trabalho árduo com uma VPN em algo muito menos laborioso, além da transparência e simplicidade extras para o seu pessoal que trabalha remotamente.
- **Microssegmentação de aplicativo:** as soluções ZTNA oferecem segurança de aplicativo muito melhor com a microssegmentação, a integração da integridade do aplicativo nas políticas de acesso, a verificação contínua de autenticação e a mera eliminação da confiança implícita e do movimento lateral que acompanha a VPN.
- **Detenção de ransomwares:** as soluções ZTNA eliminam um vetor comum de ataque por ransomware e outros ataques de infiltração na rede. Como os usuários do ZTNA não estão mais "na rede", as ameaças que poderiam montar suas bases de operações através da VPN não têm para onde ir quando se trata de um ZTNA.
- **Integração rápida de novos aplicativos e usuários:** o ZTNA possibilita melhor segurança e maior agilidade nos ambientes em que os usuários vão e vêm incessantemente. Implemente novos aplicativos com rapidez e segurança, registre ou elimine usuários e dispositivos facilmente, e obtenha insights sobre o status e uso do aplicativo.

Em resumo, as vantagens do ZTNA em comparação às soluções de VPN de acesso remoto tradicional incluem:

1. **Zero Trust** – O ZTNA se baseia no princípio do Zero Trust: "confie, mas confira", proporcionando segurança e microssegmentação sensivelmente melhores ao tratar eficientemente cada usuário e dispositivo como seus próprios perímetros e avaliando e verificando constantemente a identidade e a integridade para obter acesso a aplicativos e dados corporativos. Os usuários têm acesso apenas a aplicativos e dados definidos explicitamente por suas políticas, reduzindo o movimento lateral e os riscos que o acompanham.
2. **Integridade do dispositivo** – O ZTNA complementa a conformidade com a integridade do dispositivo nas políticas de acesso, dando a você a opção de rejeitar o acesso de sistemas fora de conformidade, infectados ou comprometidos a aplicativos e dados corporativos, eliminando um importante vetor de ameaça e reduzindo o risco de roubo ou vazamento de dados.
3. **Funciona em qualquer lugar** – O ZTNA é uma rede independente, capaz de operar igualmente bem e com segurança a partir de qualquer rede, seja em casa, no hotel, em um café ou no escritório. O gerenciamento de conexão é seguro e transparente independentemente de onde o usuário e o dispositivo estão localizados, simplificando a experiência de trabalho do usuário em qualquer lugar.
4. **Mais transparente** – O ZTNA oferece uma ótima experiência ao usuário final, estabelecendo automaticamente conexões de segurança sob demanda nos bastidores, conforme necessárias. A maioria dos usuários nem mesmo notará que a solução ZTNA está por trás da proteção de seus dados.
5. **Melhor visibilidade** – O ZTNA pode oferecer visibilidade aumentada da atividade do aplicativo importante para o monitoramento do status do aplicativo, planejamento da capacidade de processo, e gerenciamento e auditoria de licenças.
6. **Facilidade de administração** – Em geral, as soluções ZTNA são mais enxutas e claras, o que facilita a implantação e o gerenciamento. Elas também são mais ágeis para acompanhar a constante entrada e saída de usuários em ambientes superativos, transformando a administração diária em uma tarefa rápida e menos laboriosa.

Guia para compradores: o que procurar em uma solução ZTNA

Verifique a lista de tópicos de compatibilidade que as plataformas devem obviamente oferecer para clientes, gateways e provedores de identidade, e pondere também estas capacidades importantes em comparação com as soluções ZTNA de diferentes fornecedores:

Entregue na nuvem, gerenciada na nuvem

O gerenciamento na nuvem oferece benefícios incríveis: instalação e utilização instantâneas, redução da infraestrutura de gerenciamento, implantação e registro, e permissão de acesso em qualquer lugar. Umas das maiores vantagens do gerenciamento na nuvem é a capacidade de fazer login imediatamente e começar a trabalhar, sem precisar de servidores de gerenciamento adicionais ou infraestrutura extra. O gerenciamento na nuvem também oferece o acesso instantâneo seguro em qualquer lugar e em qualquer dispositivo, para assegurar que você possa trabalhar do seu jeito. Também facilita o registro de novos usuários localizados em qualquer parte do mundo.

Integração com as suas outras soluções de segurança cibernética

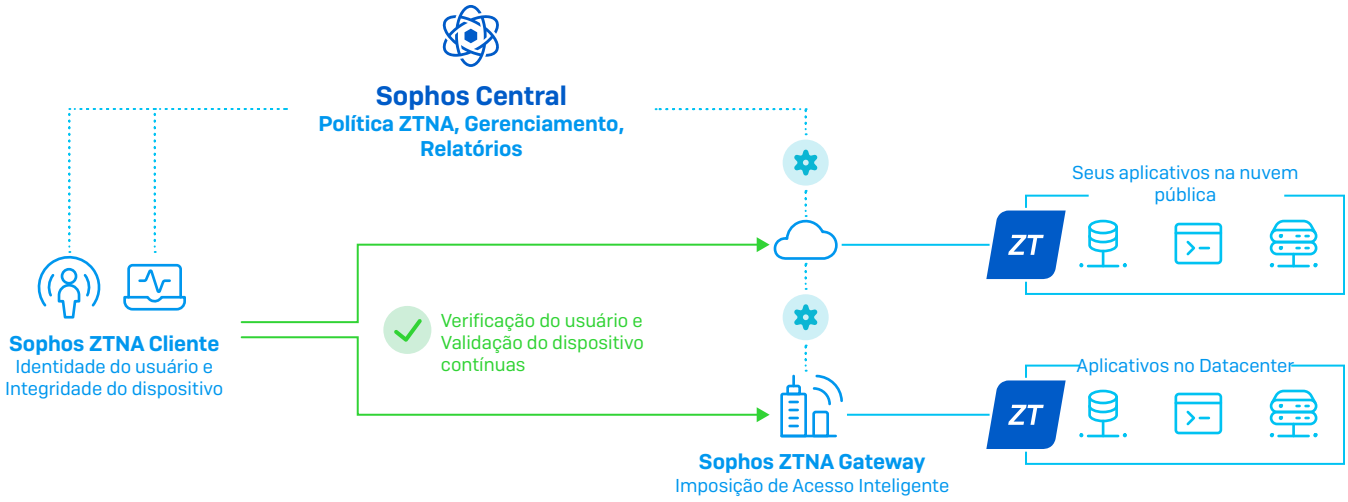
A maioria das soluções ZTNA funciona perfeitamente bem como produtos independentes, mas não podemos ignorar os grandes benefícios de ter uma solução hermeticamente integrada com os seus outros produtos de segurança cibernética, como firewalls e endpoints. Um painel de gerenciamento na nuvem integrado pode ser um multiplicador de força para você ou sua equipe. Usando esse painel unificado para gerenciar toda a sua segurança de TI, que também inclui o ZTNA, você reduz o tempo de treinamento e a carga diária de gerenciamento. Nele você pode ver insights únicos de todos os seus produtos de segurança de TI, especialmente útil quando compartilham telemetria, aumentando a sua segurança significativamente com resposta em tempo real quando uma ameaça ou um dispositivo comprometido entra na rede. Eles podem operar em conjunto e responder instantaneamente a um ataque ou ameaça e parar o invasor, bloqueando seus movimentos e evitando que se infiltre lateralmente na rede ou que roube os seus dados.

Experiência do usuário e gerenciamento

Assegure que a solução que pretende usar ofereça uma excelente experiência ao usuário final, bem como facilite a administração e o gerenciamento. Hoje em dia, com mais usuários trabalhando remotamente de infinitas localidades em todo o mundo, o registro e a configuração eficientes do dispositivo são fatores críticos para que os novos usuários possam estar aptos a trabalhar o mais rápido possível. Fique atento em como o agente ZTNA é implantado e na facilidade de adicionar novos usuários às políticas. Esteja certo também de que a solução na qual está investindo permita uma experiência tranquila para os usuários finais e ofereça a visibilidade que você espera, como o insight em tempo real à atividade do aplicativo, que ajudará você a ser mais proativo na identificação de picos de carga, capacidade, utilização de licenças, e mesmo problemas com aplicativos.

ZTNA Sophos

O ZTNA Sophos foi desenvolvido baseado nos princípios do Zero Trust Network Access de facilidade, integração e segurança. O ZTNA Sophos é entregue na nuvem, gerenciado na nuvem e integrado no Sophos Central, a plataforma de relatórios e gerenciamento de segurança cibernética na nuvem mais confiável do mundo. No Sophos Central, você não gerencia apenas o ZTNA, mas também os firewalls da Sophos, endpoints, proteção de servidores, dispositivos móveis, segurança na nuvem e muito mais.



O ZTNA Sophos também é único pela integração hermética que oferece com os endpoints Sophos Intercept X e Sophos Firewall. Isso permite aproveitar as vantagens do Synchronized Security e Security Heartbeat para compartilhar a integridade do dispositivo entre o firewall, o dispositivo, o ZTNA e o Sophos Central para responder automaticamente a ameaças e dispositivos que não apresentam conformidade. Limite o acesso e detenha os sistemas comprometidos automaticamente até que estejam limpos.

Os clientes da Sophos concordam que o tempo que economizam com os benefícios de uma solução de segurança cibernética Sophos totalmente integrada é imenso. Eles dizem que usar um pacote de produtos da Sophos em conjunto com o gerenciamento do Sophos Central e incorporar a tecnologia Synchronized Security para a identificação e resposta automática a ameaças é como duplicar suas equipes de TI. Logicamente que o ZTNA Sophos também funcionará com produtos de segurança de outros fornecedores, mas ele certamente apresenta um funcionamento único quando em conjunto com todo o restante do ecossistema Sophos para concretizar seus benefícios tangíveis de visibilidade, proteção e resposta.

Saiba mais em

sophos.com/ztna

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: Brasil@sophos.com

21-10-07 PTBR (DD)

SOPHOS