



Passar da VPN para o ZTNA

Vantagens do ZTNA e por onde começar



Índice

- 3** O que é o ZTNA?
- 3** O ZTNA melhora a segurança
- 4** O ZTNA aumenta a escala e a flexibilidade
- 5** O ZTNA permite melhorar a produtividade
- 5** O ZTNA é mais rentável
- 6** Não deixe que a VPN o trave



60%

das organizações trocará a sua VPN
por um serviço de ZTNA

O surgimento do teletrabalho trouxe novos desafios de segurança para as organizações.

Com um número cada vez maior de colaboradores a trabalhar a partir de qualquer lugar, as organizações têm de encontrar formas de garantir o acesso remoto e híbrido às suas redes e dados. Uma solução tradicionalmente utilizada é a rede privada virtual (VPN). No entanto, à medida que as ciberameaças continuam a evoluir, as VPN revelaram-se insuficientes para proteger contra ameaças modernas. O acesso à rede de confiança zero (ZTNA) é uma solução muito mais eficaz do que as VPN na proteção de acessos remotos.

O que é o ZTNA?

Criada em abril de 2019 pela Gartner, a expressão acesso à rede de confiança zero (ZTNA) representa um conjunto de novas tecnologias concebidas para o acesso seguro a aplicações privadas. O ZTNA utiliza políticas de acesso granulares para ligar utilizadores autorizados a aplicações específicas, sem conceder acesso ao resto da rede, permitindo assim um acesso segmentado com privilégios mínimos e sem expor nunca as localizações das aplicações na internet, como acontece com as VPN.

A Gartner previu que, até 2023, 60% das organizações teria substituído a sua VPN por um serviço de ZTNA. Isto fez do ZTNA o produto de confiança zero com crescimento mais rápido no setor, com 44% dos responsáveis de TI a estabelecer o ZTNA como ponto de partida para quem procura implementar uma plataforma Security Service Edge (SSE) como parte de uma estratégia Secure Access Service Edge (SASE) mais abrangente.

O ZTNA melhora a segurança

Uma das principais razões pelas quais as empresas estão a adotar o ZTNA é a maior segurança que proporciona. Com uma VPN, os utilizadores entram diretamente na rede corporativa. Uma vez tendo acesso à rede, podem movimentar-se lateralmente e aceder a dados ou recursos confidenciais. Não surpreende que “confiar demasiado nos utilizadores” seja o maior problema das soluções de acesso seguro existentes, segundo o relatório de adoção de SSE de 2024. Embora se possa dizer que isto tenha menor impacto para utilizadores internos, continua a ser preocupante saber que um atacante poderia beneficiar da falta de segmentação.

As soluções de ZTNA são normalmente menos dispendiosas de implementar e manter do que as soluções de VPN. O custo da VPN vai mais além do mero custo do equipamento.



Em contraste, o ZTNA nunca estende o acesso à rede e concede acesso com base no contexto: a identidade do utilizador, o dispositivo utilizado e a aplicação e dados a que pretende aceder. Isto significa que, mesmo que um atacante tente entrar na rede, não só não conseguirá aceder a dados confidenciais sem a autenticação adequada, como o serviço de ZTNA ocultará a própria existência da rede, tornando-a invisível e impossível de rastrear.

O ZTNA aumenta a escala e a flexibilidade

Outra razão para a adoção do ZTNA é a escala e flexibilidade superiores que proporciona. Enquanto as soluções de VPN dependem frequentemente de hardware e dispositivos, as soluções de ZTNA são fornecidas na cloud, o que significa que os utilizadores podem aceder a partir de qualquer lugar e as equipas de TI podem gerir tudo remotamente.

Isto é especialmente útil para empresas com colaboradores híbridos ou remotos, ou que precisem de aceder a recursos a partir de diversos locais. Enquanto as VPN têm limites de capacidade estáticos baseados no tamanho dos dispositivos, a arquitetura cloud do ZTNA permite aumentar ou reduzir facilmente a capacidade conforme as necessidades de cada empresa.

Mais importante ainda, os serviços de ZTNA fornecem políticas de controlo de acesso hipergranulares e flexíveis que podem ser aplicadas ao nível do utilizador e da aplicação. A segmentação através de VPN implica uma complexa segmentação de rede, mas com ZTNA implementar acesso com privilégios mínimos é tão simples como ajustar uma política.

O ZTNA permite melhorar a produtividade

As soluções de ZTNA proporcionam uma experiência de acesso muito melhor do que as VPN. As VPN reduzem a produtividade, obrigando os utilizadores a lidar com velocidades lentas (devido ao tráfego de retorno), desconexões constantes e inícios de sessão repetitivos. Tudo isto interrompe o trabalho e gera frustração.

O ZTNA, por outro lado, oferece uma experiência de utilização mais simples. Permite que os utilizadores acedam facilmente a aplicações privadas, eliminando o tráfego de retorno mantendo-se sempre ativo mesmo com mudanças na rede e simplificando o processo de autenticação com integrações diretas com SSO e outras soluções de gestão de identidade.



O ZTNA é mais rentável

As soluções de ZTNA são geralmente menos dispendiosas de implementar e manter do que as soluções de VPN. O custo de uma VPN vai muito além do preço dos equipamentos. Para além dos concentradores de VPN, são necessários vários dispositivos de segurança instalados localmente, como proteção DDoS, firewalls internos e externos, balanceadores de carga, entre outros. Tudo isto equivale a uma pilha de segurança única para tráfego entrante (as organizações costumam ter entre 3 e 5). Além disso, as equipas de segurança necessitam frequentemente de pessoal dedicado à monitorização e gestão das VPN, retirando recursos de projetos mais importantes. Manter este modelo centrado no perímetro é dispendioso.

Por outro lado, as soluções de ZTNA não exigem instalação ou manutenção locais de hardware ou software custosos. As organizações procuram plataformas SSE para eliminar a necessidade de concentradores de VPN (66%), inspeção SSL (37%), antivírus (36%) e proteção DDoS (44%). De facto, as melhores plataformas SSE oferecem tecnologias ZTNA que eliminam por completo as VPN e a pilha de segurança entrante, resultando numa poupança significativa. O ZTNA também é intuitivo e fácil de gerir, permitindo reduzir drasticamente o número de recursos necessários para gerir o acesso seguro. Por fim, as soluções ZTNA adotam um modelo de preços por subscrição, proporcionando transparência e evitando custos excessivos com licenças.

Não deixe que a VPN o trave

À medida que o número de trabalhadores remotos e híbridos continua a aumentar, é fundamental que as empresas disponham de uma solução moderna de acesso seguro. O acesso à rede de confiança zero (ZTNA) supera as limitações das VPN e oferece mais segurança, flexibilidade, escalabilidade, desempenho e rentabilidade no acesso remoto.

O melhor do ZTNA é que faz parte de uma estratégia de segurança mais ampla. À medida que as organizações procuram adotar uma plataforma Security Service Edge (SSE), verifica-se que a maioria começa precisamente pela adoção do ZTNA. Por onde começar?

Substitua totalmente a VPN com a HPE Networking

Mais informações sobre como utilizar HPE Networking como alternativa à VPN

Consulte a plataforma HPE Networking SSE

arubanetworks.com/products/sse

Tome a decisão de compra certa.
Contacte os nossos especialistas de pré-venda.



Chat com Vendas



Chamada

Visite ArubaNetworks.com



Receber actualizações



© Hewlett Packard Enterprise Development LP. Todos os direitos reservados.

Todos os produtos e os nomes de empresas mencionados são marcas comerciais dos seus respetivos proprietários.
© 2025 Hewlett Packard Enterprise.