6 casos de uso

para substituir completamente a **VPN**

Conheça as alternativas modernas baseadas em nuvem que podem transformar sua rede.

CG//One

Sumário

03	O futuro da conexão segura
04	Capacitando trabalhadores híbridos
05	Acelerando a migração para nuvem
06	Facilitando o acesso a dispositivos não gerenciados (quando fizer sentido)
07	Acelerando a integração de Fusões e Aquisições (M&A)
09	Suporte à central de atendimento remoto
10	Modernizando aplicativos legados
11	Conclusão

O futuro da conexão segura

As VPNs (Redes Privadas Virtuais) foram, por muito tempo, a espinha dorsal da conectividade remota segura para empresas em todo o mundo. No entanto, à medida que os ambientes corporativos evoluem, com o aumento do trabalho híbrido, das aplicações distribuídas e das ameaças cibernéticas mais sofisticadas, as limitações das VPNs tornam-se cada vez mais evidentes.

Soluções modernas baseadas em nuvem estão transformando a forma como as empresas conectam seus usuários, dispositivos e dados de maneira segura, simplificada e escalável.

Para empresas que planejam modernizar a conectividade para a força de trabalho híbrida, o ZTNA é a alternativa moderna à VPN. Mas é importante pontuar que nem todas as soluções ZTNA permitem com sucesso a substituição completa da VPN.

Para atualizar com sucesso sua VPN para o ZTNA, nossa recomendação é identificar e priorizar os principais casos de uso ao planejar uma migração completa. O planejamento útil, combinado com os investimentos em tecnologia certos, permitirá que as equipes finalmente cumpram a promessa de aposentadoria total da VPN.

Neste material, exploraremos alguns casos que mostram como o ZTNA pode superar as limitações das VPNs tradicionais, permitindo que sua empresa atenda às demandas de segurança e conectividade do mundo digital atual.

1. Capacitando trabalhadores híbridos

Com o crescimento expressivo do trabalho híbrido, as soluções de VPN estão cada vez mais ultrapassadas para enfrentar os desafios de segurança e conectividade que uma força de trabalho moderna exige.

As VPNs de acesso remoto oferecem visibilidade limitada sobre as atividades relacionadas a aplicativos, sofrem com problemas de latência e desempenho devido ao backhaul de tráfego e concedem amplo acesso em nível de rede a usuários autenticados, aumentando a superfície de ataque por meio de movimentos laterais irrestritos.

Além disso, concentradores de VPN com vulnerabilidades não corrigidas tornaram-se alvos frequentes de ciberataques.

É preciso repensar como proteger e conectar sua equipe no cenário atual.

Dicas para implementar:

Um inventário de implantações de VPN é um excelente ponto de partida para atualizar sua infraestrutura. Certifique-se de incluir:

- Quantas instâncias de serviços de VPN de acesso remoto você opera hoje?
- Qual tráfego de aplicativo está viajando por essas VPNs de acesso remoto?
- Usuários nomeados com acesso via VPN a esses aplicativos.

Funcionários perdem, em média, **11 horas* por ano apenas redefinindo senhas.**

* 1 Business Reporter, “How much time does your organisation spend on managing passwords?”, Sept. 7, 2022. https://www.independent.co.uk/news/business/business-reporter/time-organisation-managing-passwords-b2161856.html

2. Acelerando a migração para nuvem

A transformação digital alcançou um ponto crítico: mais cargas de trabalho agora estão hospedadas em nuvens públicas, em vez de data centers privados. Como consequência, a conectividade com IaaS, tanto para usuários locais quanto remotos, tornou-se uma das principais prioridades das organizações ao planejar sua estratégia de nuvem e implantação.

Na infraestrutura tradicional de VPN de acesso remoto, o tráfego do usuário é roteado pelo data center privado e, em seguida, conectado às nuvens IaaS por meio de MPLS ou outros túneis dedicados, como AWS Direct Connect ou Azure ExpressRoute. Esse backhaul de tráfego não apenas compromete a experiência do usuário e aumenta os custos de infraestrutura, mas também exige um roteamento de rede complexo.

Como uma alternativa moderna às VPNs de acesso remoto legadas, a Netskope oferece conectividade eficiente com nuvens públicas, eliminando a necessidade de hairpin. A conexão é segura, flexível e altamente escalável.

O NPA (Netskope Private Access), fornecido pela CG One, protege dados e recursos com controles de acesso em nível de aplicativo, baseados na identidade do usuário e na postura de segurança do dispositivo. Diferentemente das soluções tradicionais, o NPA utiliza conectividade lógica, não baseada em IP. Isso simplifica significativamente as operações de nuvem e rede, permitindo automação e eliminando o backhaul de tráfego.

Dicas para implementar:

As organizações que buscam substituir sua VPN também devem procurar instâncias de VPN em nuvem, como AWS Client VPN ou Azure VPN Gateway. Elas devem aproveitar ferramentas de automação, como módulos Terraform, para automatizar a implantação, configuração e dimensionamento de NPA Publishers em execução no EC2 e outros ambientes de nuvem.

3. Facilitando o acesso a dispositivos não gerenciados (quando fizer sentido)

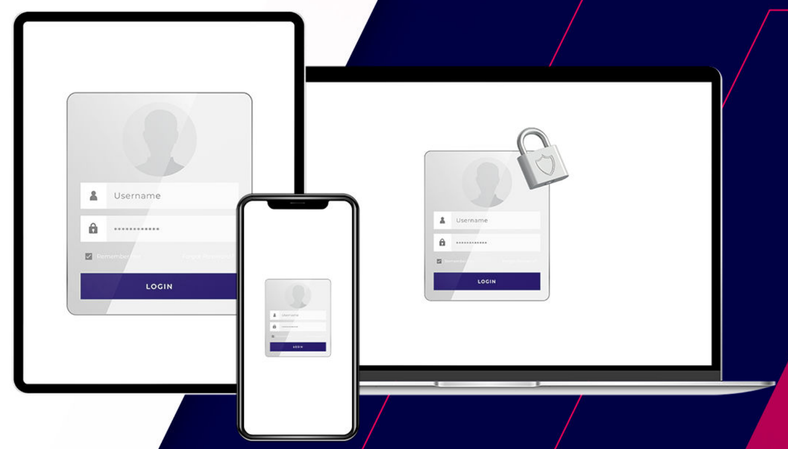
As organizações precisam conceder a contratados externos, provedores de serviços e parceiros acesso seguro aos recursos corporativos. Ao mesmo tempo, os funcionários também exigem acesso contínuo a recursos privados usando seus dispositivos pessoais. Isso leva ao desafio de facilitar o acesso a dispositivos não gerenciados sem o risco de expor os recursos na internet pública ou DMZ.

Exigir um software específico para fins especiais pode não ser viável, pois os usuários podem relutar em instalar software em seus dispositivos pessoais. Conceder acesso VPN a dispositivos não gerenciados pode resultar em muitos acessos.

Você pode provisionar com segurança o acesso a dispositivos não gerenciados para usuários de terceiros e BYOD de funcionários sem os riscos associados a VPN, DMZ ou exposição de recursos à Internet pública.

O Netskope Private Access oferece suporte à implantação sem cliente para dispositivos não gerenciados, fornecendo acesso seguro e de confiança zero a aplicativos privados, hospedados no local ou na nuvem. A implantação do ZTNA para não clientes permite acesso sem atrito e baseado em navegador por meio de uma arquitetura de proxy reverso que é integrada a provedores de identidade (IdP) para autenticar os usuários que tentam acessar aplicativos privados. Aproveitando os mesmos controles DLP na plataforma Netskope SSE, as organizações podem manter visibilidade granular e política de proteção de dados consistente em todos os dispositivos, gerenciados e não gerenciados.

Em média, um funcionário usa **2,5* dispositivos no trabalho**, o que inclui dispositivos não corporativos, como laptops pessoais, smartphones e tablets.



*2 Zippia. “26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace” Zippia.com. Oct. 17, 2022. https://www.zippia.com/advice/byod-statistics/

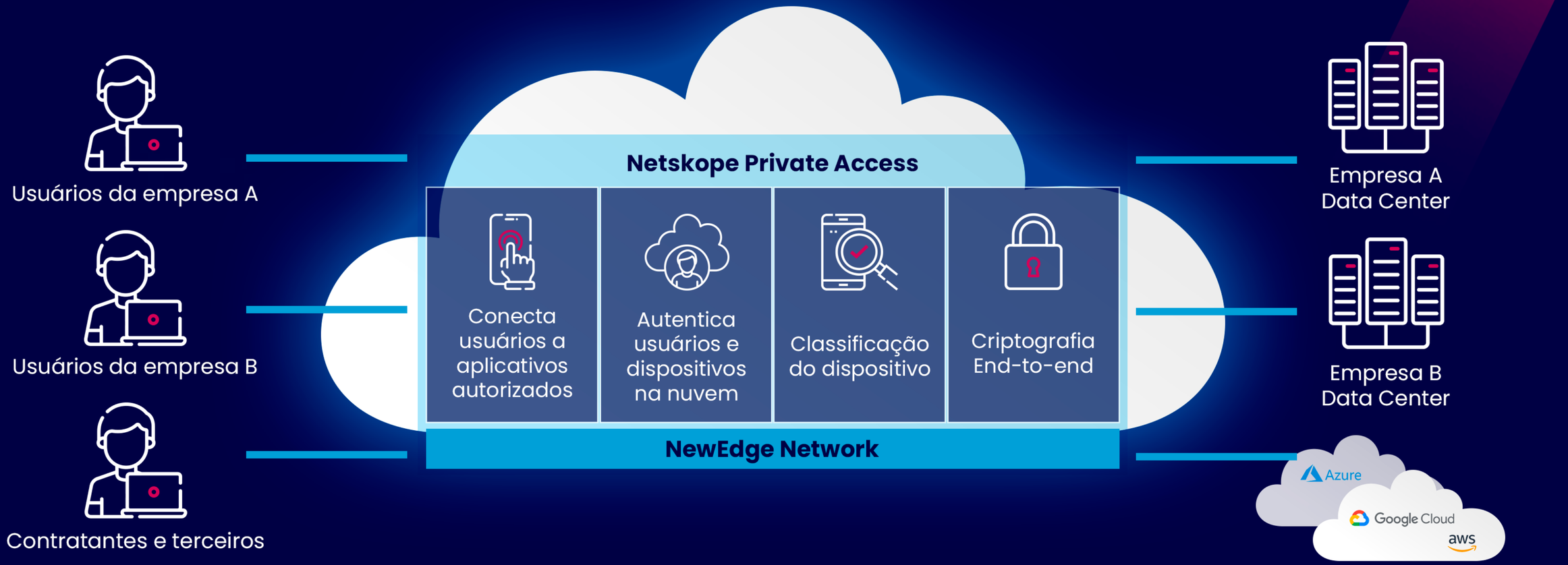
4. Acelerando a integração de Fusões e Aquisições (M&A)

Fusões e Aquisições são eventos rápidos, de alto risco e sensíveis ao tempo. Para as equipes de TI, redes e segurança, esses processos apresentam um conjunto único de desafios. O sucesso de uma Fusão e Aquisição depende da agilidade com que a integração das duas empresas é concluída.

As equipes de operações de TI são desafiadas a fornecer acesso no primeiro dia, conectando usuários de ambas as entidades a aplicativos internos de missão crítica e, ao mesmo tempo, garantindo a segurança de dados confidenciais. Os métodos tradicionais de mesclar duas redes são um processo caro, demorado e complexo que geralmente resulta em conflito de IP e requer renumeração de endereços. As regras de firewall geralmente não podem oferecer controle de acesso granular, tornando ambas as redes vulneráveis.

A Netskope introduziu recentemente o ZTNA Next, integrando o ZTNA entregue na nuvem com o endpoint SD-WAN. Um cliente SASE unificado direciona automaticamente o tráfego do usuário para seus destinos, sejam aplicativos na nuvem, aplicativos privados, IaaS ou web. O ZTNA Next, fornecido pela CG One, permite que as organizações percebam o valor comercial em atividades de Fusões e Aquisições, permitindo que as organizações conectem funcionários, contratados e consultores apenas aos recursos críticos de que precisam no primeiro dia, mesmo para aplicativos legados e sem esperar que a infraestrutura VPN seja configurada e eliminando a necessidade de mesclar redes.

Isso permite que as empresas comecem imediatamente a combinar seus negócios de forma segura. Os critérios de confiança adaptáveis para concessão de acesso consideram a identidade do usuário, a higiene do dispositivo e outros dados contextuais. Ao conceder aos usuários acesso seletivo a aplicativos e dados, o ZTNA Next minimiza o risco de movimentação lateral e exposição de dados confidenciais.



Forneça acesso imediato aos recursos internos sem a complexidade de combinar redes, configurar VPN site a site e regras de firewall.

5. Suporte à central de atendimento remoto

Esses profissionais atuam como representantes de atendimento ao cliente, agentes de reservas de viagens, consultores de saúde e em outras funções. Embora muitos call centers estejam migrando para soluções de comunicação unificada como serviço (UCaaS) baseadas em nuvem, muitas organizações ainda utilizam sistemas de VoIP legados hospedados localmente, frequentemente roteando chamadas por meio de VPNs de acesso remoto.

Para funcionários de call center remoto, a qualidade do VoIP pode ser imprevisível quando depende de VPNs. Eles tendem a ficar sobrecarregados, contribuindo para maior instabilidade e latência com chamadas VoIP, o que pode ser frustrante para todos os envolvidos.

Até agora, a maioria das soluções ZTNA fornecidas na nuvem não oferece suporte a sistemas VoIP hospedados no local, forçando as organizações a manter infraestrutura ZTNA e VPN.

O Netskope ZTNA Next oferece recursos convergentes de ZTNA e SD-WAN entregues como uma única solução. Com direcionamento dinâmico de tráfego e QoS com reconhecimento de contexto, aumentando a produtividade dos funcionários do call center remoto com experiência garantida de aplicativo de voz e vídeo, ao mesmo tempo em que aprimora a postura de segurança com acesso de confiança zero a todos os recursos internos.

Há 1,8 milhão* de funcionários de call centers em todo o mundo, e **52% dos call centers** nos EUA empregam profissionais remotos.

* 3Source: “Call Center Statistics – 2023” Truelist.com. Jan. 1, 2023. https://truelist.co/blog/call=-center-statistics/#:~:text-The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.

6. Modernizando aplicativos legados

Testar a compatibilidade é uma etapa crítica na atualização da tecnologia. As organizações que estão implantando o ZTNA também precisam testar a compatibilidade dos aplicativos. Durante esse processo, as organizações provavelmente descobrirão alguns aplicativos legados que são incompatíveis com a maioria das soluções ZTNA atuais.

Por exemplo, aplicativos legados que exigem tráfego iniciado pelo servidor não funcionam bem com a "conectividade de dentro para fora" de uma solução ZTNA moderna, que exige que o tráfego seja iniciado pelo endpoint. Esses sistemas legados geralmente são proprietários e exigem tempo, recursos e planejamento cuidadoso para redesenhar e modernizar (e geralmente isso significa migrar para ambientes IaaS hospedados na nuvem).

O Netskope ZTNA Next resolve todos esses exemplos de aplicativos legados, no entanto, fornecendo acesso seguro e otimizado a todos os aplicativos privados de um único cliente integrado. As organizações podem, portanto, estender a longevidade dos aplicativos legados, reduzir o custo de gerenciamento de várias soluções de acesso remoto e fornecer acesso rápido e confiável aos aplicativos, independentemente de onde estejam hospedados.

Conclusão

Se antes eram consideradas tecnologia de ponta, as VPNs de acesso remoto legadas agora representam um desafio significativo. Para as equipes de segurança, elas são uma fonte constante de vulnerabilidades; para as equipes de infraestrutura e operações, comprometem o desempenho da rede, degradando, assim, a experiência geral dos usuários.

Por outro lado, muitas das soluções ZTNA disponíveis atualmente ainda não são uma solução definitiva. Quando essas soluções não abrangem todos os casos de uso relevantes, as organizações acabam realizando apenas uma substituição parcial das VPNs. Isso resulta em uma infraestrutura híbrida — combinando VPNs legadas com "algum" ZTNA — que pode ser ainda mais complexa e difícil de gerenciar do que o cenário anterior.

O ZTNA Next, fornecido pela CG One, foi desenvolvido para ajudar as organizações a acelerar a adoção do modelo zero trust, oferecendo uma solução totalmente integrada que facilita a substituição completa da infraestrutura de VPN. Ele proporciona um caminho claro para eliminar totalmente as VPNs de acesso remoto, atendendo a todos os casos de uso de acesso a aplicativos.

Com essa solução, sua empresa consegue reduzir a superfície de ataque digital, fortalecer a postura de segurança com base nos princípios de zero trust e melhorar a produtividade dos trabalhadores remotos, garantindo uma experiência de acesso a aplicativos otimizada e contínua.

Solicite uma demo gratuita

Somos parceiros oficiais da Netskope no Brasil

Somos a CG One, a evolução da marca Compugraf. Há mais de 40 anos no mercado de tecnologia, oferecemos soluções de cibersegurança escaláveis para detectar e bloquear ataques antes mesmo que aconteçam. Desenvolvemos e gerenciamos soluções de última geração para Segurança da Informação, Proteção de Redes e Gerenciamento Integrado de Riscos.

Entre em contato