e-book

Os 6 casos de uso mais convincentes para

Substituição completa da VPN legada

netskope

Introdução

A infraestrutura legada de VPN para acesso remoto há muito tempo representa um risco à segurança. Sua ampla conectividade de rede atrai invasores e permite movimentação lateral não autorizada. Forçar usuários remotos a fazer backhaul de tráfego não local por meio da VPN apenas para retornar à Internet resulta em uma experiência ruim para o usuário e acarreta altos custos e complexidade de roteamento.

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

Para uma migração bem-sucedida de VPN legada para ZTNA, recomendamos identificar e priorizar os principais casos de uso ao planejar a transição completa. Um planejamento útil, junto com os investimentos certos em tecnologia, permitirá que as equipes finalmente cumpram a promessa de aposentadoria total da VPN.

1. Capacitar trabalhadores híbridos

Com a maioria dos funcionários agora favorecendo um modelo de trabalho híbrido, as soluções VPN legadas se mostram inadequadas para enfrentar os desafios essenciais de segurança e conectividade necessários para capacitar a força de trabalho. O acesso remoto VPN fornece pouca visibilidade sobre atividades relacionadas a aplicações e sofre com latência e problemas de desempenho por meio de backhaul de tráfego, e fornece amplo acesso em nível de rede para usuários autenticados, expandindo a superfície de ataque devido a movimentos laterais irrestritos. Além disso, concentradores de VPN com vulnerabilidades não corrigidas atuam como grandes vetores de ataque para ataques cibernéticos.

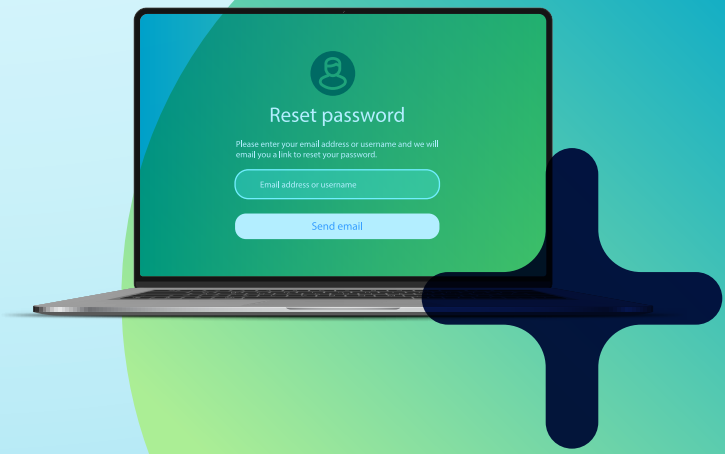
Ao atualizar as soluções VPN remotas legadas para uma solução ZTNA, como o Netskope One Private Access, as organizações poderão lidar com riscos de segurança relacionados à VPN, permitindo acesso com privilégio mínimo e reconhecimento de identidade e contexto a aplicações privadas, minimizando ao mesmo tempo movimentos laterais não autorizados. O Netskope One Private Access oferece visibilidade em tempo real do tráfego detalhado de aplicações e das atividades dos usuários e permite a imposição consistente de políticas para funcionários que se conectam de qualquer local, seja remoto ou on-premises. Além disso, a solução pode estabelecer conectividade segura de pré-login, facilitando a integração segura de novos dispositivos e a redefinição de senhas para trabalhadores remotos, além de garantir que apenas dispositivos autorizados tenham acesso a recursos internos essenciais, como serviços de diretório.

11 horas por ano
perdidas por funcionários redefinindo senhas[1]

DICAS DE IMPLEMENTAÇÃO:

Um inventário de implantações de VPN é uma boa maneira de começar a atualizar sua infraestrutura. Isso deve incluir:

- **Quantas instâncias de serviços VPN de acesso remoto você opera hoje**
- **Que tipo de tráfego de aplicações está passando por essas VPNs de acesso remoto**
- **Usuários nomeados com acesso VPN a essas aplicações**



[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. Acelerar a migração para nuvem

A transformação digital atingiu um ponto crítico: Cada vez mais cargas de trabalho estão sendo hospedadas em nuvens públicas em vez de em data centers privados. Como resultado, a conectividade com IaaS, para usuários on-premises e remotos, tornou-se uma prioridade e uma das principais preocupações das organizações à medida que planejam sua estratégia de nuvem e implantação. Na infraestrutura VPN típica de acesso remoto, o tráfego do usuário é roteado pelo data center privado e então conectado às nuvens IaaS usando MPLS ou outros túneis dedicados, como AWS Direct Connect ou Azure ExpressRoute. O tráfego de backhaul não só leva a uma experiência ruim para o usuário e aumenta as despesas de infraestrutura, mas também requer roteamento de rede complexo.

Como uma alternativa moderna às VPNs de acesso remoto legadas, a Netskope permite conectividade eficiente à nuvem pública sem a necessidade de hairpin. A conexão é segura, flexível e altamente escalável. O Netskope One Private Access ajuda a proteger dados e recursos com controle de acesso em nível de aplicação com base na identidade do usuário e na postura de segurança do dispositivo. Ao utilizar conectividade lógica em vez de baseada em IP, ele simplifica drasticamente as operações de nuvem e rede, permitindo a automação e eliminando o backhaul de tráfego.

DICAS DE IMPLEMENTAÇÃO:

Organizações que buscam substituir a VPN de acesso remoto também devem procurar instâncias VPN em nuvem, como AWS Client VPN ou Azure VPN Gateway. Elas devem utilizar ferramentas de automação, como módulos Terraform, para automatizar a implantação, a configuração e o dimensionamento de publicadores do Netskope One Private Access em execução no EC2 e outros ambientes em nuvem.

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

As organizações precisam conceder a prestadores de serviços e parceiros externos acesso seguro a 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 de dispositivos não gerenciados sem o risco de expor os recursos na Internet pública ou na DMZ. Exigir um software cliente 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 acesso excessivo.

Você pode provisionar com segurança o acesso a dispositivos não gerenciados para usuários terceirizados e quarteirizados e BYOD de funcionários sem os riscos associados a VPN, DMZ ou exposição de recursos à Internet pública. O Netskope One Private Access oferece suporte à implantação sem cliente para dispositivos não gerenciados, fornecendo acesso seguro e zero trust a aplicações privadas, hospedadas on-premises ou na nuvem.

A implantação do ZTNA sem cliente permite acesso sem obstáculos e baseado em navegador por meio de uma arquitetura de proxy reverso que é integrada com IdPs (identity providers) para autenticar os usuários que tentam acessar aplicações privadas. Utilizando os mesmos controles DLP na plataforma Netskope One 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**, que incluem dispositivos não corporativos, como laptops pessoais, smartphones e tablets.[2]

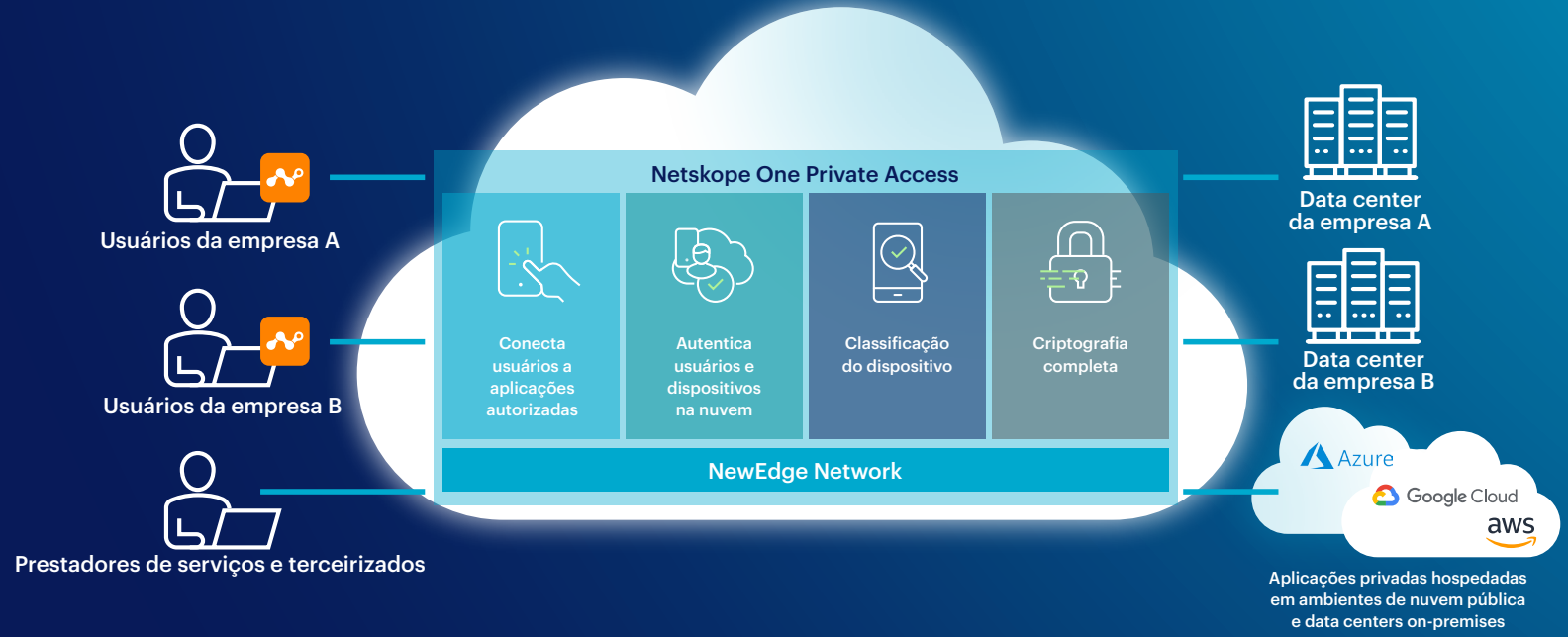
[2]Zippia. "26 Surprising BYOD Statistics [2023]: BYOD Trends In The Workplace" Zippia.com. 17 de outubro de 2022. https://www.zippia.com/advice/byod-statistics/

4. Acelerar a integração de fusões e aquisições

As atividades de fusão e aquisição são eventos acelerados, de alto risco e que exigem muito tempo. Para equipes de TI, rede e segurança, fusões e aquisições apresentam um conjunto único de desafios. O sucesso de fusões e aquisições é impulsionado pela rapidez com que a integração das duas empresas pode ser concluída.

As equipes de operações de TI têm o desafio de fornecer acesso imediato, conectando usuários de ambas as entidades a aplicações internas mais importantes e, ao mesmo tempo, garantindo a segurança de dados confidenciais. Os métodos tradicionais de combinação de redes são caros, demorados e complexos, frequentemente resultando em conflitos de IP e exigindo a renumeração de endereços. As regras de firewall geralmente não conseguem oferecer controle de acesso granular, tornando ambas as redes vulneráveis.

Fornecido como uma solução unificada, o Netskope One Private Access integra recursos de ZTNA/SD-WAN em um único cliente de endpoint leve, permitindo aposentar completamente — não apenas substituir parcialmente — VPNs de acesso remoto para todos os casos de uso de acesso a aplicações relevantes. Um cliente SASE unificado direciona automaticamente o tráfego de usuários para seus destinos, sejam aplicações em nuvem, aplicações privadas, IaaS ou web. O Netskope One Private Access permite que as organizações gerem valor comercial rapidamente durante atividades de fusões e aquisições conectando funcionários, prestadores de serviços e consultores a recursos essenciais de imediato, mesmo para aplicações legadas. Esta solução elimina a necessidade de configuração de VPN e combinação de redes, permitindo que as empresas iniciem a integração imediatamente com segurança. O acesso é concedido com base em critérios de confiança adaptáveis, considerando a identidade do usuário, a segurança do dispositivo e outros fatores contextuais. Ao fornecer acesso seletivo a aplicações e dados, o Netskope One Private Access reduz o risco de movimentação lateral e exposição de informações confidenciais.



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

5. Suporte a contact centers remotos

Existem **1,8 milhão** de funcionários de call center em todo o mundo e 52% dos call centers nos EUA empregam agentes remotos.[3] Esses agentes são representantes de atendimento ao cliente, agentes de reservas de viagens, prestadores de consultoria em saúde e outras funções. Embora muitos call centers estejam se atualizando para UCaaS (unified communication as a service) baseado em nuvem, muitas organizações ainda usam VoIP hospedado on-premises e, frequentemente, roteiam chamadas por meio de VPN de acesso remoto. Para funcionários de call centers remotos, a qualidade do VoIP pode ser tudo ou nada quando se depende de VPNs. Eles tendem a ficar sobrecarregados, contribuindo para maior instabilidade e latência nas chamadas VoIP, o que pode ser frustrante para as pessoas nos dois lados da linha.

Até agora, a maioria das soluções ZTNA entregues em nuvem não oferece suporte a sistemas VoIP hospedados on-premises, forçando as organizações a manter infraestrutura ZTNA e VPN.

52%
dos call centers nos EUA empregam agentes remotos

O Netskope One Private Access oferece recursos convergentes de ZTNA e SD-WAN entregues como uma solução única. Com direcionamento dinâmico de tráfego e QoS baseado em contexto, aumente a produtividade de funcionários de controle remoto com experiência garantida em a plicações de voz e vídeo ao mesmo tempo em que melhore a postura de segurança com acesso zero trust a todos os recursos internos.

[3]Fonte: "Call Center Statistics – 2023" Truelist.com. 1º de janeiro de 2023. https://truelist.co/blog/call-center-statistics/#:~:text=The%20number%20of%20people%20working,million%20currently%20to%201.8%20million.

6. Acomodar aplicações legadas

Testar a compatibilidade é uma etapa essencial na atualização tecnológica. As organizações que estão implantando o ZTNA também precisam testar a compatibilidade das aplicações. Durante esse processo, as organizações provavelmente descobrirão algumas aplicações legadas que são incompatíveis com a maioria das soluções ZTNA atuais. Por exemplo, aplicações legadas 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 particulares e exigem tempo, recursos e planejamento cuidadoso para serem redesenhados e modernizados (e muitas vezes isso significa migrar para ambientes IaaS hospedados em nuvem).

O Netskope One Private Access resolve todos esses exemplos de aplicações legadas, fornecendo acesso seguro e otimizado a todas as aplicações privadas a partir de um único cliente integrado. As organizações podem, portanto, estender a longevidade de aplicações legadas, reduzir o custo de gerenciamento de múltiplas soluções de acesso remoto e fornecer acesso rápido e confiável às aplicações, independentemente de onde elas estejam hospedadas.

Conclusão

Embora antes fossem tecnologia de ponta, as VPNs de acesso remoto legadas agora desafiam as equipes de segurança — para quem elas são uma fonte de muita vulnerabilidade a ameaças — e equipes de infraestrutura e operações, para quem elas afetam o desempenho da rede e, como resultado, degradam a experiência geral do usuário.

No entanto, a maioria das soluções ZTNA atuais não é uma solução universal; se não atenderem a todos os casos de uso relevantes, as organizações acabam substituindo apenas parte da VPN, resultando em uma infraestrutura híbrida — VPN legada mais "algum" ZTNA — que pode ser ainda mais complexa do que antes.

O Netskope One Private Access foi projetado para ajudar as organizações a acelerarem a adoção do ZTNA zero trust, usando uma solução totalmente integrada que catalisa a substituição bem-sucedida de toda a infraestrutura VPN. Ele oferece um caminho claro para a substituição completa das VPNs de acesso remoto em todos os casos de uso, reduzindo a superfície de ataque digital, fortalecendo a segurança com os princípios zero trust e aumentando a produtividade dos trabalhadores remotos com um acesso otimizado e contínuo às aplicações.

Sobre o Netskope One Private Access

O Netskope One Private Access traz recursos SD-WAN para o ZTNA para permitir conectividade segura e otimizada a todas as aplicações privadas, incluindo VoIP hospedado on-premises, vídeo e assistência remota, permitindo às organizações:

- Modernizar a conectividade e aumentar a segurança.
- Melhorar a experiência do usuário.
- Garantir um acesso altamente confiável e otimizado para aplicações de voz e vídeo.
- Reduzir a complexidade e o custo operacional.
- Acelerar os planos de descontinuação da infraestrutura VPN legada de acesso remoto, eliminando a necessidade de manter ferramentas separadas.
- Alcançar visibilidade e controle sem precedentes sobre o tráfego de aplicações.

O Netskope One Private Access permite aposentar completamente — não apenas a substituir parcialmente — VPNs de acesso remoto para todos os casos de uso de acesso a aplicações relevantes, ao mesmo tempo em que aprimora a postura de segurança e fornece acesso a aplicações otimizado e contínuo.

Sobre a Netskope

A Netskope, líder global em SASE, ajuda organizações a aplicar princípios zero trust e inovações de IA/ML para proteger dados e se defender contra ameaças cibernéticas. Rápida e fácil de usar, a plataforma Netskope One e o Zero Trust Engine patenteado fornecem acesso otimizado e segurança em tempo real para pessoas, dispositivos e dados, onde quer que estejam. Milhares de clientes confiam na Netskope e sua poderosa rede NewEdge para reduzir riscos e obter visibilidade incomparável sobre qualquer atividade em nuvem, web e aplicativos privados — fornecendo segurança e acelerando o desempenho sem comprometimentos. Obtenha mais informações em **netskope.com**.

Interessado em saber mais?

Peça uma demonstração

netskope