

Private Access para ZTNA

A transição em grande escala para o trabalho remoto e híbrido gerou uma demanda sem precedentes por soluções de Zero Trust Network Access (ZTNA) baseadas na nuvem. Essas soluções, especialmente como alternativa mais segura e eficiente às VPNs tradicionais, rapidamente se consolidaram no mercado de cibersegurança. Segundo uma previsão do Gartner, “até 2025, pelo menos 70% das novas implantações de acesso remoto serão predominantemente atendidas por soluções de acesso de rede com confiança zero (ZTNA), em vez dos serviços de VPN.”

Acesso seguro e sem atritos para usuários remotos

ZTNA (Zero Trust Network Access) é uma abordagem moderna de segurança cibernética que oferece acesso remoto seguro aos recursos de uma organização com base no princípio de confiança zero. Isso significa que nenhum usuário ou dispositivo é confiável automaticamente, mesmo que esteja dentro da rede corporativa. O acesso é concedido somente após uma verificação rigorosa de identidade e contexto, garantindo que cada solicitação de acesso seja segura.

Nos últimos anos, o mercado adotou o acrônimo ZTNA para descrever soluções voltadas a acesso seguro, destacando o modelo em que o usuário só obtém conexão aos recursos da rede quando realmente precisa e apenas ao conteúdo para o qual está autorizado. Essa abordagem reduz significativamente a superfície de ataque e limita a movimentação lateral dentro da rede, protegendo dados sensíveis e garantindo maior controle sobre as operações.

O Netskope Private Access (NPA), fornecido pela CG One, conecta perfeitamente usuários em qualquer lugar a recursos privados. Um componente integral das soluções Netskope Security Service Edge (SSE), o NPA reduz os riscos comerciais, protege os dados, simplifica a infraestrutura de TI e permite acesso remoto seguro com uma experiência de usuário superior.

Conheça os principais casos de uso:



Transformação de segurança:

Zero Trust Network Access (ZTNA) que conecta usuários autenticados a aplicativos autorizados, não à rede subjacente.

Substituir VPN de acesso remoto:

reduz os riscos e a exposição associados à rede privada virtual (VPN) de acesso remoto.

Suporte à nuvem híbrida:

fornece uma experiência perfeita ao usuário final para acessar aplicativos em data centers privados e ambientes de nuvem pública.

Acesso de terceiros:

com acesso de navegador sem cliente para aplicativos da web privados.

Integração de fusões e aquisições:

fornece acesso no primeiro dia a recursos internos sem a complexidade de combinar redes.

Acesso DevOps:

acesso nativo a recursos hospedados em ambientes de nuvem privada virtual (VPC).



Principais benefícios



Acesso de rede Zero Trust a aplicativos privados

O ZTNA fornece acesso a aplicativos privados, não à rede. Com políticas granulares de controle de acesso em nível de aplicativo, a confiança é concedida com base na identidade do usuário, associação ao grupo e na postura de segurança dos dispositivos.



Experiência de usuário superior com conectividade direta e rápida

Ignore o roteamento de rede complexo e aumente a produtividade do usuário com conectividade rápida e sem atritos para aplicativos. Aproveite o NewEdge, uma nuvem privada de segurança de alto desempenho e alta disponibilidade que é amplamente pareada com provedores de serviços de nuvem.



Redução da superfície de ataque

Melhore a postura de segurança e reduza a superfície geral de ataque eliminando a exposição de protocolos e serviços à internet pública.



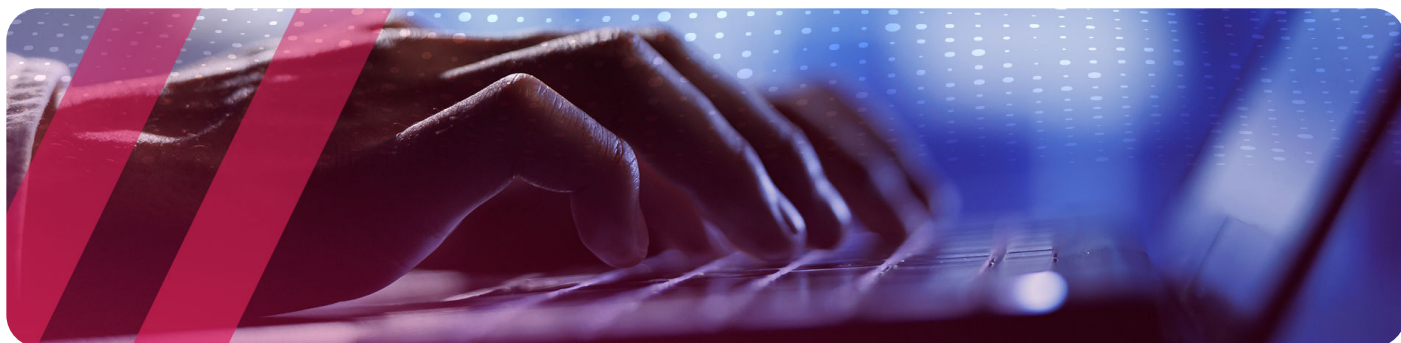
Proteja os dados e reduza o risco interno

Detecte anomalias de uso, atividades e comportamento de dados (UEBA), aplique regras e políticas avançadas de DLP e aplique políticas de acesso adotivas com base nos riscos do usuário.



Simplifique as operações

Construído na plataforma Netskope SSE que unifica ZTNA, CASB, SWG e Cloud Firewall em um único cliente, um mecanismo de política e um único console de gerenciamento, fornecendo aplicação de política consistente, facilidade de gerenciamento e visibilidade.



Suas necessidades	Nossa solução
Ampla aplicação e suporte	Suporte para acesso iniciado pelo cliente a aplicativos empresariais criados nos protocolos TCP e UDP, permitindo assim o acesso a aplicativos da Web e clientes non-web/thick clients. Por exemplo, SSH, RDP, Microsoft Windows Active Directory).
Acesso de terceiros	Suporte para acesso de navegador para aplicativos da web privados (por exemplo, aplicativos HTTP ou HTTPS), com inspeção opcional com regras DLP para a proteção de dados.
Política granular para controle de acesso	Aproveite a identidade do usuário e do dispositivo junto com informações de risco unificadas para permitir o acesso a aplicativos privados.
Application Discovery	Acelere a adoção do ZTNA simplificando o processo de descoberta de aplicativos, definição de políticas e autorização de acesso. Os administradores de rede obtêm insights detalhados sobre o cenário de aplicativos privados, utilização, usuários e padrões de tráfego.
Gerenciamento de infraestrutura privada	O Publisher Dashboard fornece insights sobre o tráfego de aplicativos, a saúde do publisher e a utilização, permitindo decisão sobre alocação de recursos, otimização de conexão e solução de problemas.
Análise e relatórios	O Advanced Analytics fornece visibilidade em tempo real do tráfego detalhado do aplicativo e das atividades do usuário, além de alertar sobre violações de políticas.
Automação de API	Os administradores podem automatizar todo o processo de descoberta e gerenciamento de aplicativos usando APIs. As APIs também estão disponíveis para gerenciamento do Publisher. Elas são cheias de recursos e têm paridade com a Netskope UI.
Proteção de dados	O NPA suporta controles DLP para evitar exfiltração de dados, alavancando o mecanismo DLP da Netskope. Isso significa que os dados são classificados apenas uma vez, e os mesmos perfis DLP e resposta a incidentes podem ser usados para aplicativos SaaS, públicos e privados.
Conectividade segura no pré-login	Integre rapidamente novos funcionários e habilite o provisionamento de autoatendimento em um novo PC. Os administradores podem aproveitar certificados de dispositivos empresariais para garantir que apenas dispositivos sancionados tenham acesso a aplicativos internos.
Conexão direta e rápida	O tráfego do usuário para o aplicativo é roteado de forma otimizada por meio da nuvem privada de segurança Netskope NewEdge, com sua cobertura global, seleção de trânsito premium e amplo peering com provedores de nuvem, para oferecer uma experiência de usuário superior e desempenho rápido do aplicativo.
Atualização automática	Permita que os administradores programem atualizações de software, garantindo assim que os editores do NPA e o sistema operacional host estejam sempre com a versão mais recente do software.
Plataforma unificada	Um único cliente, um mecanismo de política e uma única interface de usuário de administrador para configuração de aplicativos, políticas, análises e relatórios em todos os serviços do Netskope.
Componentes de implementação	
Netskope Client	O NPA é habilitado no Netskope Client. Suporta Microsoft Windows, Apple Mac OS e iOS, Chrome OS (Chromebook) e Android. Com o Browser Access, o NPA funciona com qualquer dispositivo que execute um navegador da web suportado.
Publisher	O Publisher é um gateway de aplicativo que inicia a conexão de saída para o Netskope Security Cloud, eliminando o risco de acesso de rede de entrada. Os Publishers podem ser implantados em servidores executando Ubuntu, em ambientes virtualizados usando VMware e Hyper-V e em ambientes de nuvem pública, como AWS, Azure e GCP.

CG//One

Torne sua
operação mais
segura ainda
hoje com o
**Private Access
para ZTNA.**



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.

