Folha de dados

Zscaler Zero Trust SD-WAN

Conecte filiais, fábricas e data centers com segurança e estenda a segurança zero trust a servidores e dispositivos IoT/TO em qualquer local.

O trabalho híbrido e a transformação da nuvem derrubaram os modelos de rede e segurança baseados em perímetro, com aplicativos privados migrando para a nuvem e usuários acessando aplicativos pela internet pública, em qualquer dispositivo e de qualquer local.

No cenário atual, muitas organizações também aproveitam dispositivos IoT/TO em vários locais — incluindo filiais, fábricas e data centers — para agilizar suas operações. Além disso, um número considerável de clientes depende da comunicação de cargas de trabalho entre servidores e clientes. As abordagens tradicionais, que dependem de WANs legadas, VPNs em malha e firewalls para gerenciar o acesso a aplicativos, tornaram-se ineficazes em um mundo que prioriza tecnologias móveis e na nuvem.

Sobretudo, as soluções WAN legadas sofrem para acompanhar o ritmo à medida que os requisitos organizacionais evoluem. A SD-WAN apresenta vários desafios, como segurança limitada por meio de acesso baseado em rede, uma superfície de ataque expansiva, amplos privilégios de movimento lateral e complexidades de roteamento. A aplicação de princípios zero trust a esta rede geralmente requer a adição de dispositivos de firewall adicionais, aumentando os custos e a complexidade.

Zscaler Zero Trust SD-WAN:

- **Permite a tecnologia zero trust em todos os lugares** para todos os usuários, dispositivos, servidores e IoT/TO, independentemente da localização
- **Melhora o desempenho dos aplicativos** enviando o tráfego das filiais diretamente para a Zero Trust Exchange e o tráfego de aplicativos confiáveis diretamente pela internet com desvio direto da internet
- **Impede o movimento lateral de ameaças:** a tecnologia zero trust cria uma base para conectividade segura que permite a segmentação leste-oeste
- **Elimina a superfície de ataque** conectando filiais e data centers por meio da Zero Trust Exchange, independente do transporte subjacente
- **Permite a descoberta e a classificação de dispositivos IoT invisíveis** com classificação automática de dispositivos baseada em perfis de tráfego
- **Simplifica o acesso seguro aos recursos de TO** com acesso sem cliente baseado em navegador para portas SSH/RDP/VNC em ativos de TO
- **Aplica políticas de encaminhamento refinadas** para tráfego dentro e fora da internet usando ZIA ou ZPA
- **Introduz a implantação pronta para uso:** o provisionamento zero touch (ZTP) simplifica a implantação e reduz o tempo de integração

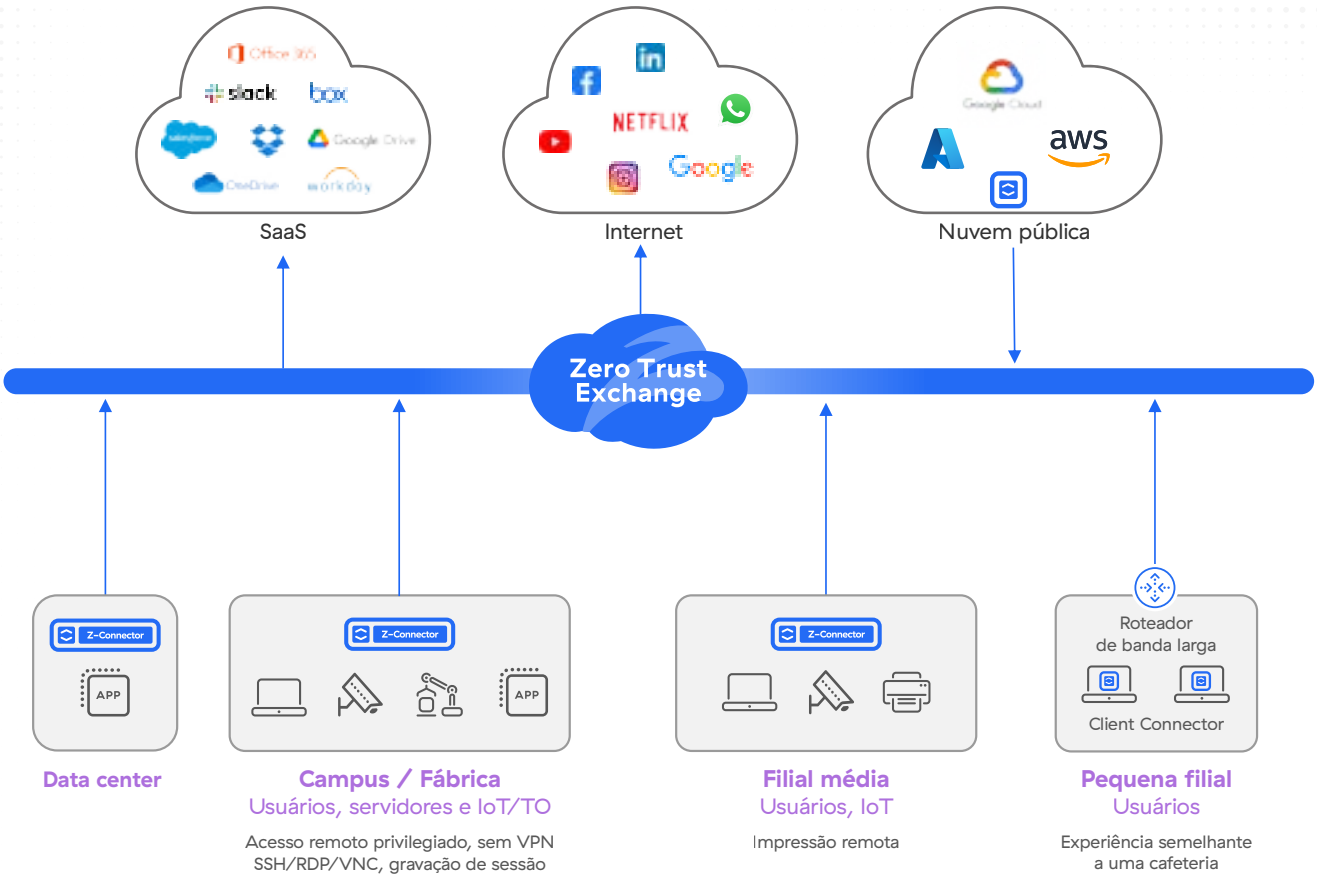

Figura 1: SD-WAN Zero Trust

A SD-WAN Zero Trust conecta com segurança filiais, fábricas e data centers sem a complexidade das VPNs, garantindo acesso zero trust entre usuários, dispositivos e aplicativos IoT/TO com base em políticas organizacionais.

A SD-WAN tradicional não zero trust

As organizações enfrentam vários desafios ao usar arquiteturas de rede e segurança legadas para conectar uma filial à internet ou a outros aplicativos em uma nuvem pública ou ambiente de data center, incluindo:

- **Maior risco de ameaças laterais e ataques na internet** devido ao uso de soluções de conectividade legadas e centradas na rede, como VPNs site a site, firewalls ou SD-WANs tradicionais. Essas soluções estendem demasiadamente a rede confiável de um cliente na internet para outras nuvens e ambientes locais, aumentando a superfície de ataque. Uma colcha de retalhos de dispositivos de segurança, ferramentas e políticas não padronizadas leva a um aumento do risco de segurança devido a lacunas conhecidas e desconhecidas na cobertura de segurança.

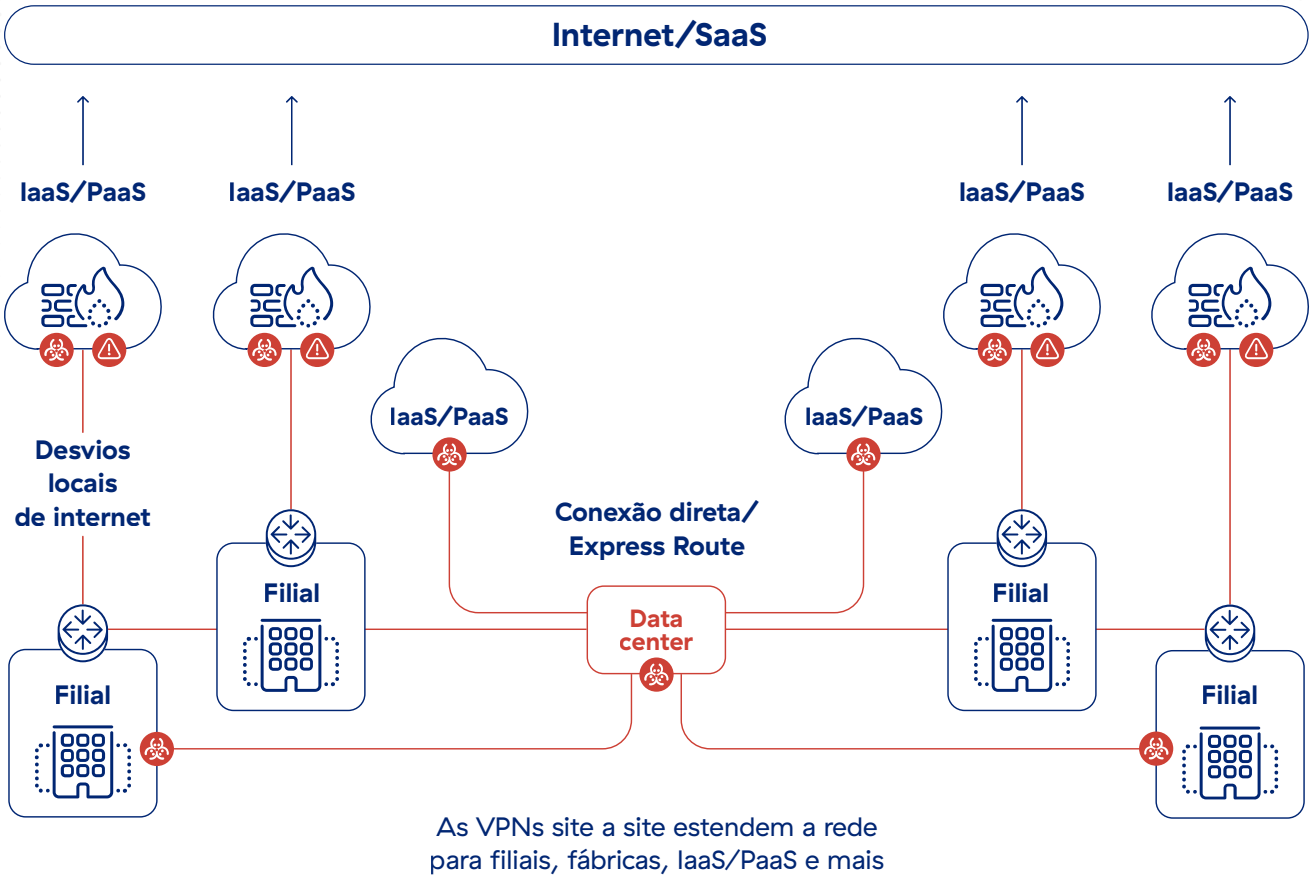

Figura 2: Maior risco de ameaças laterais e ataques na internet com SD-WANs tradicionais

- **Maior complexidade** devido ao roteamento complicado, vários dispositivos e saltos de rede, além do gerenciamento fragmentado de políticas devido à introdução de modelos legados na nuvem. Gerenciar essa complexidade é uma tarefa difícil para as equipes de rede e segurança, pois elas lutam para padronizar a conectividade e impor políticas de segurança em filiais, data centers e na nuvem.
- **Falta de visibilidade** em caminhos de conectividade entre filiais, data centers e a nuvem, o que cria pontos cegos de rede e segurança.
- **Baixo desempenho e escalabilidade** devido ao número crescente de serviços de rede e segurança em ambientes de filiais e data centers, interrupções de tráfego e pontos de estrangulamento para inspeção e controle de segurança centralizados.
- **Custos elevados** devido a dispositivos legados de rede e segurança (por exemplo, firewalls, IPS, roteadores e outros produtos pontuais), provisionamento excessivo de serviços de rede para compensar a falta de escalabilidade e aumento do uso de serviços nativos da nuvem.

Como funciona a SD-WAN Zero Trust

A SD-WAN Zero Trust permite que as organizações criem filiais enxutas, eliminando vários produtos, como roteadores, firewalls e VPNs, com um dispositivo simples e pronto para uso que pode ser implantado rapidamente usando apenas uma conexão de internet. Isso permite reduzir a complexidade associada ao gerenciamento de vários dispositivos e otimizar a funcionalidade geral da filial. A SD-WAN Zero Trust simplifica drasticamente as comunicações das filiais com sobreposição de rede zero trust que permite flexibilidade no encaminhamento e simplicidade no gerenciamento de políticas usando a estrutura comprovada de políticas do ZIA e ZPA.

O tráfego das filiais é encaminhado com segurança diretamente para a Zero Trust Exchange, onde as políticas do ZIA ou ZPA podem ser aplicadas para inspeção de segurança completa e controle de acesso baseado na identidade das comunicações de filiais e data centers. O tráfego de aplicativos confiáveis pode ser enviado diretamente pela internet com desvios diretos de internet. Essa abordagem única oferece três vantagens principais:

- Você passa da conectividade VPN site a site baseada em rede para a comunicação baseada em identidade e aplicativo, para obter a verdadeira segurança zero trust
- A arquitetura legada de castelo e fosso é eliminada sem comprometer a segurança; não há necessidade de produtos legados, como proxies Squid, gateways NAT, IPSs e assim por diante
- Você fornece conectividade distribuída e dimensionável onde quer que seja necessário, com gerenciamento de políticas centralizado e automatizado para simplificar as comunicações de filiais e data centers

Casos de uso de SD-WAN Zero Trust

Substituição de VPN site a site

Conecte filiais diretamente a aplicativos privados sem estender sua WAN ou depender de VPNs, pois ambas aumentam a superfície de ataque da rede. Os aplicativos ficam ocultos por trás das filiais e o acesso é restrito por meio da Zero Trust Exchange a um conjunto de entidades nomeadas. A identidade, o contexto e a adesão à política dos participantes especificados são totalmente verificados antes que o acesso seja permitido, proibindo o movimento lateral em qualquer outro lugar da rede.

Fusões e aquisições

A fusão de duas redes separadas é algo desafiador e demorado. Os problemas variam desde sobreposições de IP e problemas de roteamento até aumento do risco de segurança devido a uma superfície de ataque de rede ampliada. Com a SD-WAN Zero Trust, as redes podem permanecer separadas e as filiais em um ambiente podem se conectar rapidamente a aplicativos privados em outro ambiente, sem interrupções.

Habilitação de acesso direto à internet para filiais

Os modelos de rede e segurança locais tornam-se menos eficazes à medida que as organizações migram seus aplicativos para a nuvem e criam aplicativos nativos da nuvem. A SD-WAN Zero Trust da Zscaler é uma solução desenvolvida especificamente para a transformação de filiais, inaugurando um novo modelo que permite que as filiais se comuniquem com qualquer destino de forma segura e independente da rede subjacente.

Zero trust para conectividade IoT/TO e de servidor

Ativos IoT/TO precisam ser acessados regularmente por funcionários e fornecedores terceirizados para maximizar o tempo de atividade da produção e evitar interrupções causadas por falhas de equipamentos e processos. A SD-WAN Zero Trust para IoT/TO fornece acesso remoto à área de trabalho totalmente isolado e sem cliente para sistemas de destino RDP e SSH, sem a necessidade de instalar um cliente em seu dispositivo usando hosts de salto e VPNs legadas.

Descoberta e visibilidade de IoT/TO invisível

As equipes de TI enfrentam pontos cegos à medida que dispositivos não autorizados e não detectáveis se conectam a redes de filiais, resultando em um aumento da vulnerabilidade dos dispositivos e da superfície de ataque. A Zscaler identifica e classifica os dispositivos para dar às equipes de TI uma visibilidade mais ampla do comportamento para melhores políticas de controle de acesso.

Dispositivos Z-Connector prontos para uso

CARACTERÍSTICAS	ZT 400	ZT 600	ZT 800	ZT VM
				Z-Connector
Tipo	Filiais pequenas/médias	Filial pequena/média	Filial média/grande	Filial e data center
Transferência/ hipervisor	200 Mbps	500 Mbps	1 Gbps	KVM, ESXi
Portas físicas	4 x GbE	6 x GbE	8 x GbE	N/A
Provisionamento zero touch	✓	✓	✓	✓
Política de encaminhamento granular para tráfego de internet, aplicativos privados e WAN direto	✓	✓	✓	✓
Aproveite a filtragem de URL, o controle do tipo de arquivo e as políticas de firewall na nuvem para o tráfego vinculado à internet	✓	✓	✓	✓
Políticas ZPA Zero Trust para dispositivos e servidores IoT	✓	✓	✓	✓
Visibilidade e registro centralizados	✓	✓	✓	✓

RECURSOS DA SD-WAN ZERO TRUST DA ZSCALER	
CARACTERÍSTICAS	**DETALHES**
Recursos	
Provisionamento zero touch e implantação automatizada	• Provisionamento zero touch com modelos predefinidos • Implantação totalmente automatizada • Descoberta dinâmica da localização geográfica de filiais
Política de encaminhamento granular para tráfego de internet e aplicativos privados	• Opções para enviar o tráfego pelo ZIA, ZPA ou direto pela internet • Critérios flexíveis de seleção de tráfego: localização, sublocalização, grupo de localizações, tupla de 5 ou FQDN
Políticas zero trust unificadas	• Política unificada de usuário para aplicativo, dispositivo IoT para aplicativo e servidor para servidor por meio da política aprimorada do ZPA para incluir novos tipos de clientes • Localização e políticas baseadas em localização geográfica • Ativação de política de segurança que inclui IPS, proxy SSL, filtragem de URL e proteção de dados • Pilha de segurança completa com postura configurada para IoT/TO e servidores
Alta disponibilidade	• Duas instâncias de SD-WAN Zero Trust operando em modo HA fornecem suporte adicional para picos de tráfego e redundância em caso de falha de hardware • Tolerância a falhas ativas-passivas usando um endereço IP virtual (VIP) baseado em protocolo de redundância de endereço comum (CARP) • Circuitos ativos-ativos (aparelho único) • Circuitos ativos-ativos (aparelho duplo ao balancear FHRP)
Visibilidade centralizada e registro granular	• Painel centralizado para monitoramento de tráfego e integridade do dispositivo • Filtragem disponível para implantações na nuvem, em data centers e filiais • Registro detalhado de cada sessão e transação para todas as portas e protocolos, incluindo todas as transações DNS públicas e privadas • Integração total com a infraestrutura do Nanolog Streaming Service, com opção de transmitir registros para o sistema SIEM de propriedade do cliente
Encerramento da interface WAN	• Conectividade dupla do ISP (Ethernet) • Multihoming com um único dispositivo
Gerenciamento da interface LAN	• Múltiplas redes LAN L3 • Suporte para marcação 802.1q/VLAN • Servidor DHCP • Gateway DNS
Políticas de firewall no dispositivo	• Controle de acesso granular para tráfego local de LAN para LAN (leste-oeste) • Listas de controle de acesso L3 (ACLs)
Seleção de caminho com reconhecimento de aplicativo	• Seleção de caminho dinâmico para SaaS ou aplicativos privados essenciais para a missão • Conectividade inteligente de POPs da Zscaler • Monitoramento e failover integrados de SLA
Roteamento	• Roteamento estático
Data centers/ POPs da Zscaler	• A Zscaler desenvolveu sua plataforma de segurança na nuvem em mais de 150 data centers em todo o mundo, estrategicamente posicionados onde os clientes estão localizados • Disponibilidade integrada com failover contínuo para o próximo PoP de serviço disponível

zscaler™ | Experience your world, secured.™

Sobre a Zscaler
A Zscaler (NASDAQ: ZS) acelera a transformação digital para que seus clientes possam ter mais agilidade, eficiência, resiliência e segurança. A solução Zscaler Zero Trust Exchange protege milhares de clientes contra ataques cibernéticos e perda de dados, conectando com segurança usuários, dispositivos e aplicativos em qualquer local. Distribuída em mais de 150 data centers globalmente, a Zero Trust Exchange baseada em SSE é a maior plataforma integrada de segurança na nuvem do mundo. Saiba mais em **zscaler.com.br** ou siga-nos no Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (Sede) • 120 Holger Way • San Jose, CA 95134 zscaler.com.br