5

— PASSOS PARA UMA —

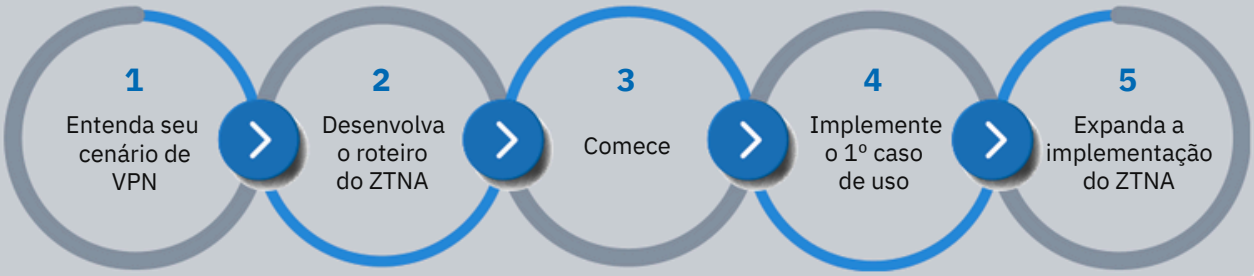
MIGRAÇÃO DE VPN PARA ZTNA

BEM-SUCEDIDA

VIA CONNECT

appgate

As organizações percebem que está na hora de melhorar ou substituir suas redes privadas virtuais (VPNs). Esta tecnologia com décadas de existência não foi projetada para lidar com os desafios de segurança da força de trabalho globalmente distribuída e com o cenário de ameaças crescentes dos dias atuais. O Zero Trust Network Access (ZTNA) é o padrão moderno do setor para um acesso seguro a qualquer coisa, de qualquer lugar, por qualquer pessoa. Embora muitas empresas entendam o valor, a realidade de migrar para fora da tecnologia VPN pode parecer assustadora. Este eBook fornece orientações sobre os cinco passos que as organizações podem tomar para fazer uma transição bem-sucedida de VPN para ZTNA, incluindo as melhores práticas que minimizam a interrupção das operações da empresa.



ÍNDICE

Introdução

As equipes de TI e segurança percebem que está na hora de aprimorar as estratégias de acesso remoto melhorando ou substituindo suas VPNs. Essa mudança de pensamento surge da necessidade de abordar um aumento significativo no número de funcionários remotos, iniciativas de transformação digital acelerada e um cenário de ameaças avançado. As VPNs são cada vez mais deficientes e difíceis de controlar para os ecossistemas de TI atuais, resultando em maior risco e complexidade. O ZTNA é uma solução ideal para combater essas falhas inerentes de VPNs. No entanto, abandonar a VPN pode parecer assustador, pois grandes investimentos ao longo dos anos a enraizou profundamente na camada de segurança.

Este eBook explica como você pode migrar sem problemas da VPN para o ZTNA com uma abordagem incremental de cinco passos que não interrompem as operações da empresa, reduz os riscos e preparam você para o sucesso a longo prazo:

1. Entenda seu cenário de VPN
2. Desenvolva o roteiro do ZTNA
3. Comece
4. Implemente o 1º caso de uso
5. Expanda a implementação do ZTNA

Uma abordagem para ZTNA em fases fortalece e simplifica os controles de acesso sem interromper as operações da empresa.

Limitações da VPN: Inadequada para os desafios de segurança modernos

Introduzida em meados da década de 1990 como uma solução de acesso remoto, a arquitetura VPN já passou do seu auge. Várias agências governamentais dos EUA, incluindo a Agência Nacional de Segurança (NSA), emitiram avisos sobre vulnerabilidades das VPNs. Elas nunca foram projetadas para serem usados com infraestrutura de TI híbrida e uma força de trabalho globalmente dispersa.

INERENTEMENTE INSEGURA

Um dos problemas de segurança mais sérios das VPNs gira em torno de portas abertas. Sem exceção, cada concentrador VPN é implementado de forma que tenha uma presença na Internet com uma porta aberta e de escuta contínua. Os agentes mal-intencionados procuram e entram nas redes por meio dessas portas abertas, inevitavelmente movendo-se lateralmente para alcançar e explorar os alvos.

método de autenticação TCP/IP usado por VPNs é outro ponto fraco. A maioria das VPNs baseiam o acesso "confiável" no endereço IP do usuário. É fácil de se obter/adquirir um conjunto válido de credenciais de login por meio de engenharia social, phishing, smishing, sites falsos... a lista é longa. Até mesmo os códigos de verificação de autenticação de dois fatores são facilmente interceptados. Existem milhões de credenciais de login roubadas na dark web para serem vendidas pelo maior lance. Vez por outra, essa abordagem legada de autenticação é facilmente manipulada por agentes de ameaça e é um erro absoluto, dada a quantidade bruta de dados contextuais disponíveis para validar a identidade do usuário.

QUESTÕES DE COMPLEXIDADE

Administradores de VPN são forçados a fazer uma escolha importante: criar políticas abertas para acesso amplo à rede ou criar políticas restritivas para acesso limitado à rede. Isso é inerentemente problemático porque a escolha mais fácil para a maioria é o acesso amplo à rede em detrimento de políticas restritivas que são complexas, sujeitas a erros e difíceis de gerenciar devido à velocidade de mudança que os negócios exigem (por exemplo, agilidade e transformação digital).

Todos esses problemas são agravados ainda mais pelo aumento da força de trabalho distribuída e pela criação dinâmica de IP inerente às cargas de trabalho em nuvem. É muito difícil gerenciar com eficiência e manter uma postura de segurança robusta.

Além disso, VPNs são soluções isoladas e vinculadas ao hardware que servem apenas para o acesso remoto. Isso torna o escalonamento complicado e caro, ao mesmo tempo que inibe a capacidade de automatizar processos e integração com outras soluções. No final das contas, as VPNs são uma solução somente para acesso remoto. Elas foram projetadas para fazer uma única coisa e não conseguem fazer isso com segurança. Essas limitações técnicas e falhas de projetos são apenas uma pequena amostra do motivo pelo qual você deve considerar fortemente a migração da VPN para o ZTNA.

As VPNs são vinculadas ao hardware e estáticas, enquantoas soluções ZTNA definidas por software fornecem a flexibilidade e escalabilidade exigidas pelas empresas de hoje.

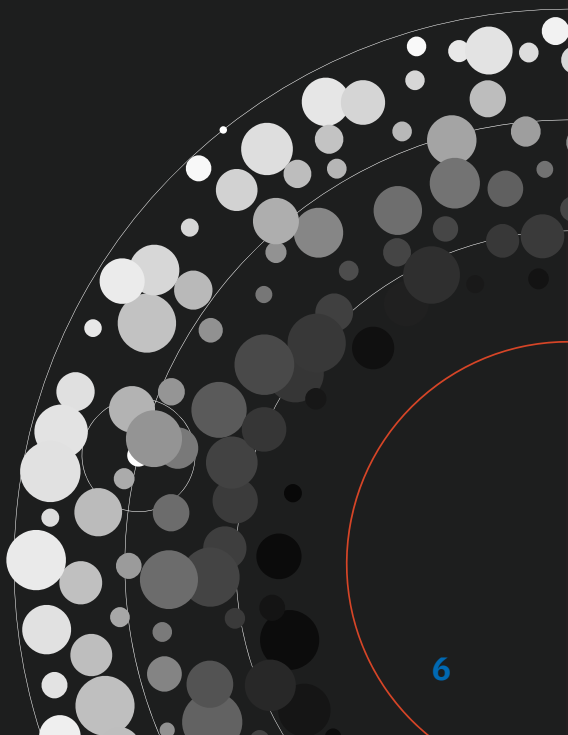
10 RAZÕES PELAS QUAIS ESTÁ NA HORA DE DESCARTAR SUA VPN

1. O modelo de autenticação centrado em IP de VPNs é fraco e não tem consciência contextual ou de identidade.
2. A abordagem “confiar e depois verificar” das VPNs resulta em um ponto de entrada na rede facilmente encontrado.
3. VPNs encorajam o movimento lateral dentro de uma rede plana, aumentando o “raio de explosão” de um ataque.
4. VPNs não têm a capacidade de conduzir a verificação da postura do dispositivo como critério para verificar a confiança.
5. Os concentradores VPN criam gargalos, resultando em baixo desempenho e funcionários frustrados.
6. VPNs criam complexidade de gerenciamento de políticas e firewall.
7. VPNs carecem de interoperabilidade com sistemas de TI, segurança e negócios.
8. VPNs são caras e demoradas para expandir.
9. Os usuários devem alternar entre VPNs para acessar cargas de trabalho distribuídas e heterogêneas.
10. VPNs oferecem apenas configurações ativo-ativo ou ativo-passivo para redundância, o que limita significativamente o rendimento e a escalabilidade.

“As VPNs são antiquadas e, embora possam ter algum valor para uma ‘solução’ imediata, elas precisam ser descartadas.

Elas são agregadoras de vulnerabilidade e um alvo principal para exploração.”

Dr. Chase Cunningham, Dr. Zero Trust



ZTNA x VPN

O ZTNA impõe o "princípio de privilégio mínimo" de acesso à rede, que é um requisito líder do setor. O ZTNA foi arquitetado para as realidades de TI de hoje em comparação com as dos anos 90. Ele oferece benefícios significativos em relação às VPNs. É como comparar o motor a vapor com um motor a combustão. Um cumpriu seu mandato, enquanto o outro reinou supremo porque era mais habilmente projetado para a época.

Estas são as principais diferenças que o ZTNA tem a oferecer em relação à VPN:

- **Redução da superfície de ataque:**

  Enquanto as portas abertas da VPN são facilmente encontradas e exploradas, a arquitetura do ZTNA usa a tecnologia de autorização de pacote único (SPA) para tornar os recursos 100% invisíveis, a menos que autenticada ou considerada uma identidade confiável.

- **Autenticação centrada em identidade:**

  O ZTNA usa endereços IP como critérios de autenticação, mas vai muito além na verificação de identidade. Ele faz isso combinando informações de qualquer armazenamento de identidade e colocando em camadas variáveis contextuais, como hora, data, localização e postura de segurança do dispositivo.

- **Acesso com privilégio mínimo:**

  Usuários e máquinas só têm acesso confiável, mas limitado, aos recursos necessários para realizar seus trabalhos. E com tecnologia SPA e microssegmentação refinada, agentes de ameaças ou dispositivos infectados são incapazes de se mover lateralmente pela rede.

- **APIs programáveis:**

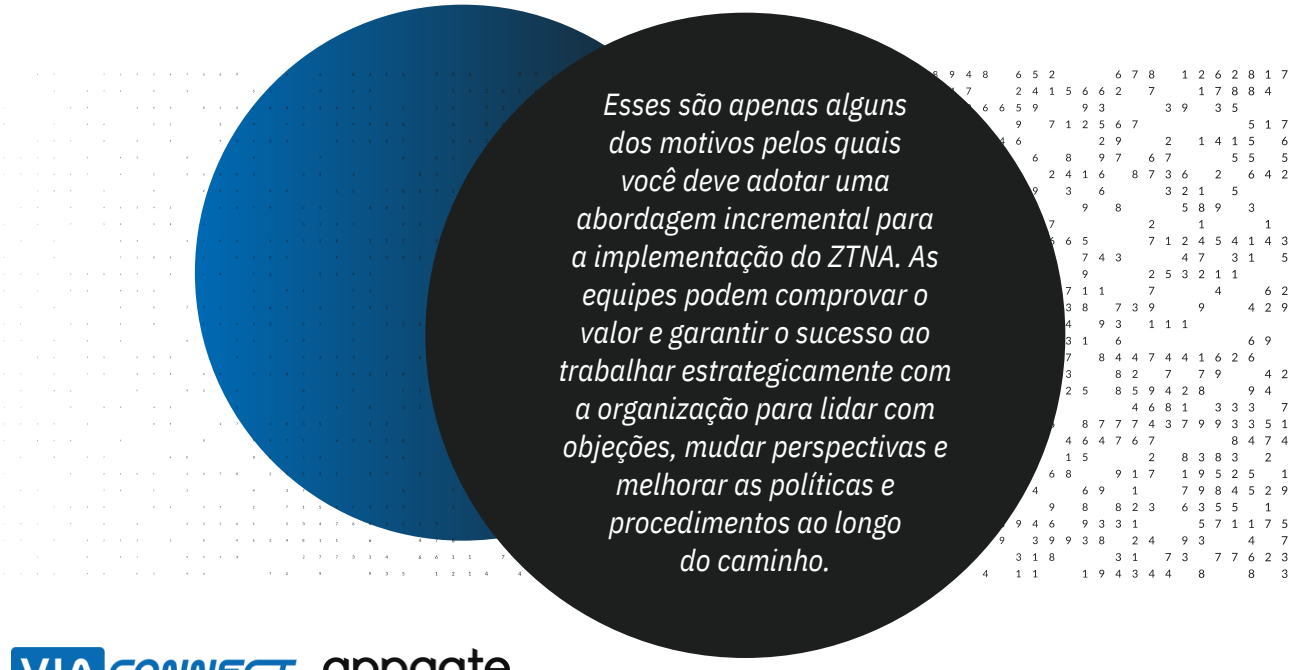
  Ao contrário da natureza isolada da VPN, as soluções ZTNA se integram aos sistemas de negócios, TI e segurança para aumentar a visibilidade da rede e os recursos de automação. A natureza definida por software de soluções ZTNA garante escalonamento contínuo e simultâneo com infraestruturas dinâmicas.

ZTNA e SDP

O modelo ZTNA era originalmente conhecido como perímetro definido por software (SDP). Os nomes são usados alternadamente e se referem a uma postura de segurança de acesso à rede atualizada e mais

LIMITAÇÕES DE VPN X VANTAGENS DE ZTNA

VPN	ZTNA
Centrada na rede: modelo “confiar e depois verificar” com base em uma relação simples de IP e porta.	**Centrado na identidade:** modelo “verificar e depois confiar” com base na identidade, no contexto e nos perfis multidimensionais.
Portas abertas: acesso do usuário normalmente totalmente aberto à rede autenticada, permitindo o movimento lateral não controlado.	**Infraestrutura camuflada:** usuários autorizados acessam apenas recursos aprovados, tornando todo o resto invisível para evitar movimentos laterais.
Vinculada ao hardware: difícil de implementar; estática e não escalonável conforme a infraestrutura muda.	**Definido por software:** elástico e escalonável em todos os ambientes híbridos por meio de integrações com APIs.
Troca de VPN: o acesso do usuário a vários recursos geralmente requer a troca de uma VPN para outra baseada em políticas complexas e sujeitas a erros.	**Conexões simultâneas:** permite que os usuários acessem vários segmentos de rede e recursos digitais por meio de um único ponto de conexão.
Isolada e estática: aplicável apenas para acesso de usuário remoto; incapaz de proteger usuários ou redes loc ais.	**Flexível e dinâmico:** versátil e extensível, indo além dos usuários remotos para fornecer acesso unificado e seguro a todos.



Superando as objeções contra a migração para ZTNA

O desejo de proteger os investimentos e decisões existentes costuma ser a força motriz por trás do motivo pelo qual as organizações não avançam com um plano de migração para ZTNA. A realidade é que você não precisa implementar tudo de uma só vez. Você pode melhorar sua tecnologia de segurança obsoleta e fazer um plano de migração em fases que ofereça melhorias ao longo do tempo.

CUSTOS IRRECUPERÁVEIS

As VPNs estão incorporadas em camadas de tecnologia em todo o mundo, portanto, é comum haver resistência à mudança. Para muitos, a maior objeção é simplesmente que o investimento já foi feito na tecnologia atual. Normalmente, as VPNs representam muitos custos irrecuperáveis, e seus departamentos de TI/segurança provavelmente ficam nervosos com discussões em grande escala sobre “eliminar e substituir”. Na verdade, em uma pesquisa recente que conduzimos com mais de 500 profissionais da infosec, o principal fator para a tomada de decisão foi o desejo de se sentirem seguros em relação aos investimentos em tecnologias anteriores. Ao mesmo tempo, eles classificaram uma tecnologia que crie conexões rápidas e seguras entre usuários e aplicativos como o mais importante entre os critérios de aquisição. Infelizmente, as VPNs são insuficientes nessa área.

Recomendamos uma estratégia de migração incremental de VPN para ZTNA que resolva esses dois fatores. Para começar, desvie o orçamento destinado a novas iniciativas de acesso seguro das VPNs - ou de outra tecnologia obsoleta - para uma solução ZTNA. Outra opção é substituir VPNs com atualizações caras de hardware.

O CONHECIDO X O DESCONHECIDO

VPNs são uma tecnologia conhecida e os usuários finais estão acostumados a trabalhar com elas e em torno delas. Um novo treinamento para as equipes e os chamados de suporte técnico podem ser objeções iniciais à adoção do ZTNA, mas duram pouco quando comparadas a benefícios que incluem complexidade reduzida, melhor experiência do usuário e ganhos de desempenho. Nascidas de uma filosofia de segurança Zero Trust, há um argumento claro para os benefícios operacionais obtidos por meio das soluções ZTNA.

SOBRECARGA DA SOLUÇÃO

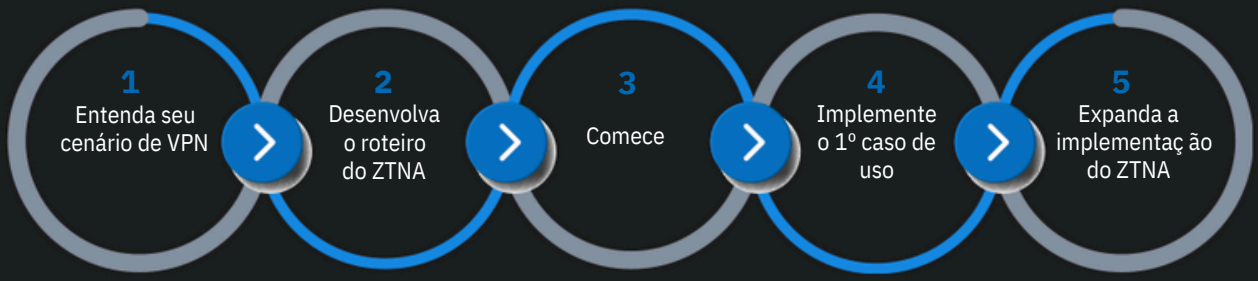
Existe uma objeção natural de que as adições de camadas de tecnologia podem gerar excesso de ferramentas em comparação com a consolidação. Porém, o ZTNA na verdade reduz a dependência por soluções de VPN, NAC e firewall sem “eliminar e substituir”. Isso se deve à extensibilidade de uma única plataforma de acesso privado e sobreposição de mecanismos de política centralizados que resolve as limitações de acesso seguro dessas ferramentas legadas. Portanto, você pode reduzir o número de regras de firewall para gerenciar; acabar com novos investimentos em soluções VPN e abrandar os gargalos do concentrador VPN; e eliminar futuras parcelas em NAC complexas e caras. Esses benefícios operacionais significam que sua equipe sobrecarregada de segurança e TI pode se concentrar em iniciativas de negócios mais focadas em vez de tarefas rotineiras de gerenciamento de políticas inerentes às ferramentas de segurança de rede legadas.

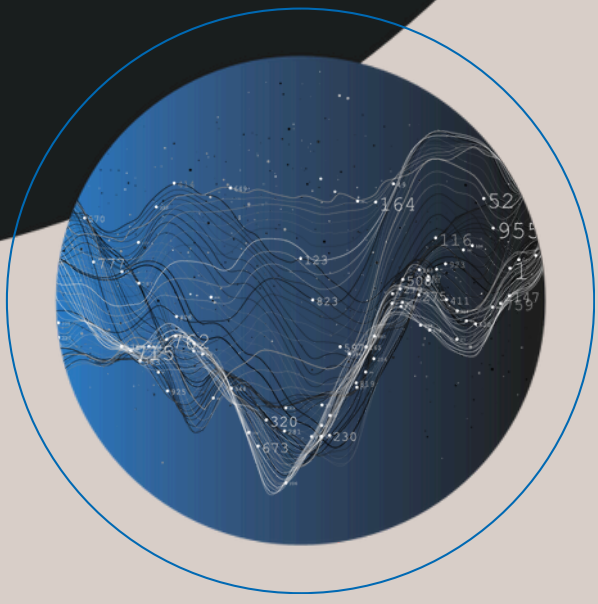
STATUS QUO X MUDANÇA

Outras possíveis objeções incluem a falta de consciência sobre os riscos cibernéticos associados às VPNs e o medo de interromper os negócios com a implementação de uma nova tecnologia. Você pode contra-argumentar isso pesquisando “VPN CVE” no Google para encontrar as manchetes mais recentes relacionadas a vulnerabilidades críticas de VPNs e fazendo uma enquete com sua equipe de TI ou funcionários em geral sobre problemas com chamados de suporte técnico e gerenciamento de políticas relacionados ao gerenciamento de VPNs. A interrupção já existe e deve ser erradicada para alcançar maior eficiência e uma postura de segurança mais robusta e altamente flexível.

Passos para migração de VPN para ZTNA

Grave. Conforme o roteiro emerge, as equipes podem identificar e priorizar os casos de uso. A partir daí, um plano em fases pode ser feito tão rápido e/ou metodicamente quanto sua organização desejar.





1

ENTENDA SEU CENÁRIO DE VPN

Sua avaliação básica de VPN fornece um panorama completo de como as VPNs funcionam dentro da sua organização, considerando também todas as influências técnicas, organizacionais e financeiras.

Cada organização tem sua própria configuração e implementação de VPN exclusivas. Antes de pensar sobre a migração para o ZTNA, você deve ter uma noção clara do seu cenário de VPN existente. Se não existir um mapa da sua estrutura VPN, agora é um excelente momento para criar um para mostrar onde as VPNs são usadas... por aplicativo, segmento de rede e grupo de usuários.

Uma avaliação básica de VPN deve detalhar como suas VPNs são integradas em sua camada de tecnologia. Ela define quais e como os ativos digitais precisam ser protegidos e considera os requisitos tecnológicos, organizacionais e financeiros.

Paralelamente, é aconselhável determinar quais grupos de usuários têm acesso aos dados mais confidenciais ou representam o maior risco para sua empresa se comprometidos. Isso ajuda a identificar pontos problemáticos e como lidar com eles antes que se tornem problemas maiores. Por exemplo, em vez de lançar uma implementação de ZTNA completa para todos os funcionários remotos ao mesmo tempo, pode ser mais inteligente testar o ZTNA com um grupo de usuários menor que represente um alto risco de segurança. Após conquistar uma vitória e reduzir sua postura de risco dentro desse grupo, você pode escalonar para a base de usuários mais ampla.

2

DESENVOLVA O ROTEIRO DO ZTNA

O próximo passo é determinar seu destino final e desenvolver o roteiro do ZTNA para chegar lá. É fundamental considerar o estado final de segurança Zero Trust desejado por sua organização, incluindo sua estratégia de longo prazo. Lembre-se de que o ZTNA é muito mais extensível do que VPNs - e é apenas um ponto de partida natural. Seu roteiro pode ir além da simples solução de acesso remoto e abranger o cenário mais amplo de acesso à rede. Por fim, você pode fornecer acesso seguro para todos os usuários, todos os dispositivos e todas as cargas de trabalho, independentemente de onde estejam.

O ZTNA oferece suporte a muitos outros casos de uso além do acesso remoto, portanto, a priorização depende inteiramente dos objetivos, riscos e postura de segurança desejados pela sua empresa.

OUTROS CASOS DE USO COMUNS DE ZTNA:

- **Migração para nuvem:**
  Mover aplicativos e dados para a nuvem - ou várias nuvens - efetivamente transforma todos os usuários em usuários remotos, mas com algumas diferenças marcantes. O ZTNA é escalonado automaticamente com a resolução dinâmica de IPs associados a cargas de trabalho em nuvem, resultando em privilégios dinâmicos em ambientes multinuvem sem intervenção manual.

- **Acesso seguro para DevOps:**
  As equipes de DevOps exigem acesso remoto a ativos digitais confidenciais hospedados em ambientes multinuvem e no local, o que pode causar atrito e riscos dentro dos recursos limitados de VPNs. O ZTNA pode liberar o DevOps dessas limitações, fornecendo acesso simultâneo a vários ambientes de nuvem, acompanhado da largura de banda e do desempenho que os desenvolvedores precisam para fazer seu trabalho. Isso também oferece uma excelente oportunidade para explorar os recursos de automação usando metadados e recursos de integração (por exemplo, com gerenciamento de serviços de TI).

- **Acesso por terceiros:**
  Terceiros, comofornecedores, contratados e parceiros de negócios, podem facilmente expor sua empresa a riscos associados ao acesso com abuso de privilégios. Os terceiros são invariavelmente remotos por natureza, portanto, muitas organizações dependem de VPNs para gerenciar seu acesso. O ZTNA pode conceder acesso confiável a usuários terceirizados sem arriscar a exposição a recursos não autorizados.

- **Máquina-a-máquina (M2M):**
  Soluções ZTNA mais robustas podem aplicar os mesmos princípios de Zero Trust impostos aos usuários para conexões M2M. Esta é apenas outra maneira de o ZTNA reduzir a superfície de ataque, pois impede o movimento lateral se uma máquina for comprometida.

- **Redes no estilo cibercafé:**
  Este é o objetivo final do ZTNA: uma integração de todos os casos de uso que resulte em um modelo unificado de políticas para usuários, redes, fluxos de trabalho e dispositivos. Basicamente, elimina a necessidade de múltiplos modelos de acesso — seja em trabalho remoto, em um escritório físico ou ao se conectar a ambientes de nuvem ou fluxos de trabalho on-premise.

Usando APIs ricas, o ZTNA pode se integrar e automatizar com sistemas existentes de TI, segurança e negócios, tornando-se uma solução ideal para todos os seus casos de uso de acesso à rede. Esses recursos devem ser levados em consideração no roteiro, pois a automação e as eficiências operacionais provavelmente se tornarão demandas estratégicas para os negócios.

3

COMECE

Agora resta apenas selecionar um fornecedor de ZTNA para que você possa lidar com seu primeiro caso de uso de ZTNA. Você deve considerar várias arquiteturas e recursos que atenderão aos requisitos atuais e futuros para evitar uma troca de fornecedor no meio do caminho ou o acréscimo de uma segunda solução ZTNA a uma camada de tecnologia congestionada.

Os principais fatores de seleção do fornecedor de ZTNA incluem:

- Capacidade de lidar com todos os protocolos, não apenas aplicativos da web.
- Baixa latência, conformidade e segurança para ambientes de nuvem multilocais.
- Compatibilidade com ambientes heterogêneos (diferentes sistemas e infraestruturas).
- Flexibilidade na implementação, como ZTNA como serviço (SaaS) ou auto-hospedado (on-premises).
- Proteção abrangente do tráfego de rede (norte-sul e leste-oeste).
- Integração com automações futuras (APIs, orquestração, etc.).
- Suporte a múltiplos provedores de identidade (Active Directory, LDAP, SAML, etc.).
- Política de segurança unificada, incluindo IoT e filiais seguras (Secure Branch).

Após selecionar sua solução ZTNAi deal, agora chegou a hora de implementar:

• Seleção de infraestrutura - escolha entre:

• Soluções ZTNA auto-hospedadas que requerem implementação leve para gateways econtrolador (mecanismo de política unificado); ou

• Soluções ZTNA “como serviço” que podem ser rapidamente implementadas e reduzem a necessidade de suporte total de TI, contando com a hospedagem na nuvem do fornecedor

• Criação de politicas:

• Seu armazenamento de identidades deve ser unificado para grupos de usuários devido à abordagem centrada em identidade do ZTNA para a criação de políticas.Portanto, seu fornecedor de ZTNA deve oferecer suporte a vários provedores de identidade distintos. Assim você pode definir algumas políticas simples que podem incluir contexto baseado em risco, como hora, data, local, MFA,etc.

• Integração dos usuários:

• Seu primeiro caso de uso e grupo de usuários determinarão se você precisa de um cliente instalado para verificação de postura dos dispositivos e suporte a protocolos ou acesso baseado em navegador para aplicativos da web. Uma solução ZTNA que pode lidar com ambos é ideal para que você tenha uma opção para casos de uso futuros.

• Automação:

• Decida quando a automação reduzirá a complexidade, aumentará a agilidade e facilitará as tarefas administrativas, que podem incluir a integração automatizada com um ITSM, MFA ou sistema de suporte de negócios.

Também é importante planejar para medir o sucesso. Considere monitorar a satisfação dos usuários e as taxas de adoção, chamados reduzidos de suporte técnico ou outros pontos para validar como o ZTNA apoia as metas da empresa. Métricas adicionais podem incluir ganhos de produtividade dos usuários e dos administradores de TI, redução de portas abertas e regras de firewall ou comparação do tempo de instalação entre ZTNA e VPN. Medir e relatar os resultados do primeiro caso de uso para as principais partes interessadas abrirá o caminho para o último passo.

4

IMPLEMENTE O 1º CASO DE USO

Comece selecionado uma porção do seu primeiro caso de uso mais natural, que, conforme discutido, é a migração de VPN para ZTNA. Embora não haja um ponto de lançamento “certo” ou predefinido, seguem pontos a serem considerados para a atualização para acesso remoto seguro com ZTNA:

- **Mitigação de riscos:**
  Uma pergunta natural é “Onde reside o maior risco associado ao acesso por VPN?” Pode ser um subconjunto de usuários privilegiados que acessam recursos confidenciais regularmente. O caso de negócios nesta situação envolve medidas preventivas e como evitar a natureza onerosa de uma violação, que custa em média US $ 1,52 milhão por incidente, de acordo com o Relatório de Custo de Violação de Dados de 2020 da Ponemon.

- **Ganhos de produtividade:**
  Outro ponto lógico para começar é entender onde você pode obter eficiência operacional. Esse pode ser um grande subconjunto de usuários frustrados que enfrentam desvantagens com VPN, como gargalos e problemas de desempenho,resultandoemaumentodechamadosdesuportetécnicoeencargosadministrativos.Eentãohá seus desenvolvedoreseDevOps,queexigemoacessocertoarecursoshíbridosnomomentocertoparaentregar aplicativos em ritmo acelerado.

- **Ciclo orçamentário:**
  Este é um excelentemomentoparacomeçaramigraçãodeVPNparaZTNA.Umagrandeatualizaçãode hardware paraVPNplanejadaparaumcicloorçamentárioapresentaumaaberturaaodiálogosobreacesso seguro em termosde“substituiçãoxatualização”.Asrenovaçõesdesoftwaresde VPNeexpiraçõesde manutenção fornecemoportunidadesatraentessemelhantespararevisão.

- **Novas iniciativas:**
  Novas iniciativasdetransformaçãodigitalouprojetosdemigraçãoparanuvemtambémsãoumaexcelente oportunidade paraadotaroZTNA.Aparceriacomunidadesdenegóciosparaaceleraressasiniciativas-sem sacrificar, mas simfortalecerasegurança-posicionaoZTNAcomoumcatalisadorparaa transformação digital.

5

EXPANDA A IMPLEMENTAÇÃO DO ZTNA

Depois que o caso de uso inicial for comprovado, você pode expandir as implementações do ZTNA em um nível maior. Como a solução é definida por software, é fácil seguir seu roteiro para todos os usuários e todas as cargas de trabalho. Basta adicionar mais gateways, definir novas políticas e incluir mais usuários.

Idealmente, o processo de expansão se moverá horizontal e verticalmente. A expansão horizontal adiciona mais usuários. A expansão vertical cobre novos casos de uso e adiciona integração e automação. A forma como ela é feita e a rapidez com que é concluída dependerá do seu roteiro. As soluções ZTNA podem ser movidas tão rápido ou tão lentamente quanto você precisar.

A expansão pode abranger casos de uso como DevOps, migração para nuvem, servidor para servidor (ou seja, tráfego lateral), dispositivos IoT ou uma rede completa no estilo cibercafé. A expansão bem-sucedida depende de manter o mecanismo de política unificado e centralizado. As soluções ZTNA que oferecem implementação flexível e opções de acesso permitem que você mantenha uma abordagem unificada, fazendo pequenos ajustes na arquitetura para abranger todos os casos de uso. Por exemplo, fornecedores terceirizados podem não permitir a instalação de um cliente em seu terminal. No entanto, uma solução ZTNA completa permitirá o acesso com privilégios mínimos a partir de navegadores de terceiros sem a necessidade de uma nova solução ou GUI de gerenciamento de políticas.

Por fim, conforme sua implementação amadurece, você pode utilizar mais recursos de sua solução. Esses podem incluir:

- **Automatizar políticas:**
  Aproveite os dados de sistemas de identidade e diretório e metadados ambientais para criar ou estender dinamicamente políticas e privilégios

- **Automatizar a infraestrutura:**
  Controle, construa e gerencie a infraestrutura como código com o operador GitHub SDP da Terraform

- **Orquestrar fluxos de trabalho:**
  Integre à operação empresarial existente ou sistemas de suporte de negócios, como gerenciamento de serviços de TI ou plataformas de chamados

- **Aprimorar a verificação de postura:**
  Integre com soluções de terminal para garantir um “dispositivo confiável” ou análise do comportamento do usuário para garantir “usuário confiável” como critério de risco para acesso

- **Colocar dados para trabalhar:**
  Envie atividades de registro de acesso detalhadas para outras ferramentas e extraia informações como critérios de acesso de outras ferramentas, como TIPs, SIEMs e UEBAs

Simplifique a migração com a solução ZTNA da Appgate

A Appgate já ajudou centenas de clientes a mudar de VPN para ZTNA. Somos conhecidos por nossa experiência líder do setor na transição sem complicações de empresas para o SDP da Appgate, uma solução excepcional que passou no teste de migração de VPN para ZTNA muitas vezes.

O SDP da Appgate oferece uma gama completa de recursos de segurança por ZTNA para todos os usuários, dispositivos e cargas de trabalho híbridas:

- **Superfície de ataquereduzida** , tornando portas, cargas de trabalho e aplicativos invisíveis, a menos que o usuário esteja autorizado a acessá- los.
- **Permissões de acesso condicionais** para verificar a identidade do usuário com base em indicadores específicos de contexto, como data, função, localização, postura do dispositivo, etc.
- **Microssegmentação avançada** que limita a autorização para redes protegidas ou cargas de trabalho e é definida por direitos dinâmicos que se ajustam conforme o usuário e o contexto do dispositivo mudam.
- **Gerenciamento de políticas aprimorado** , reduzindo a complexidade com uma única estrutura para todos os usuários, dispositivos, redes e infraestrutura para uma experiência de acesso unificado com configuração consistente em TI heterogênea.
- **Conexiones simultáneas** que melhoram a experiência do usuário e oferecem suporte ao acesso direto simultâneo a todos os recursos aprovados em nuvem, SaaS e locais.

"A arquitetura Zero Trust da Appgate permitiu que todos os nossos funcionários trabalhassem remotamente da segurança de suas casas, mantendo o mais alto nível de segurança exigido por nossos clientes."

– Chris Edwards, fundador e CEO, The Third Floor

"O SDP da Appgate simplifica muitas coisas para nós... Conseguimos cortar nossas políticas de firewall de cerca de 50 para agora duas ou três."

– Deryk Motietall, Gerente Sênior de Infraestrutura, WW

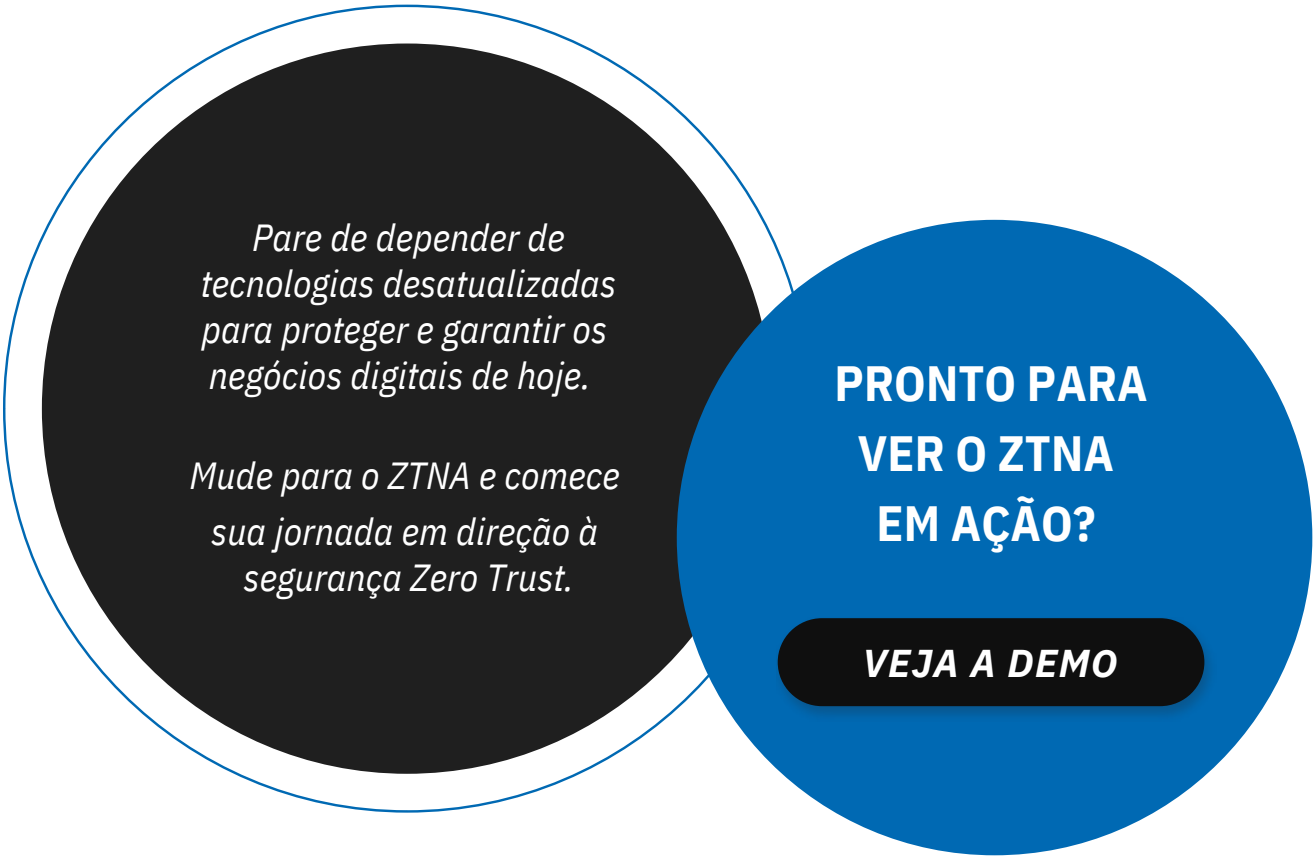
"Como uma prestadora de serviços gerenciados, nossos clientes confiam em nós para proteger seus dados. Estamos sempre procurando melhorar nossa postura de segurança. O SDP da Appgate nos ajudou a atingir esse objetivo."

– Matthew Staver, CTO, Verdant Services

Faça a mudança para o ZTNA

Agora é a hora de substituir ou melhorar sua VPN legada com a supremacia de segurança moderna do ZTNA. O cenário de ameaças cibernéticas cada vez mais sofisticado - combinado com modelos de negócios de trabalho remoto - torna isso uma obrigação.

Comece aos poucos, mas pense grande em termos de metas de segurança a longo prazo. Começando com um caso de uso de ZTNA gerenciável, sua equipe de TI e segurança pode aproveitar seu conhecimento e experiência para implementação incremental em toda a empresa. Isso garante suporte às partes interessadas, melhor adoção dos usuários e interrupção mínima dos negócios.



Sobre a Appgate

Appgate é a empresa de acesso seguro que fornece soluções de segurança cibernética para pessoas, dispositivos e sistemas com base nos princípios de segurança Zero Trust. O Appgate protege mais de 700 organizações governamentais e empresariais. Saiba mais em appgate.com