WHITE PAPER

Além da SD-WAN:

Segurança Zero Trust e a Internet como WAN corporativa

Por que SD-WAN, acesso seguro e proteção contra ameaças andam juntos

Akamai

O futuro da rede de longa distância empresarial

As redes de longa distância (WANs) já existem desde a década de 1960, no início da comunicação entre computadores. Elas continuaram a ser desenvolvidas e aprimoradas à medida que a tecnologia evoluiu e as demandas de tráfego aumentaram. Para as empresas de hoje, as WANs são a infraestrutura que permite uma rede unificada entre locais.

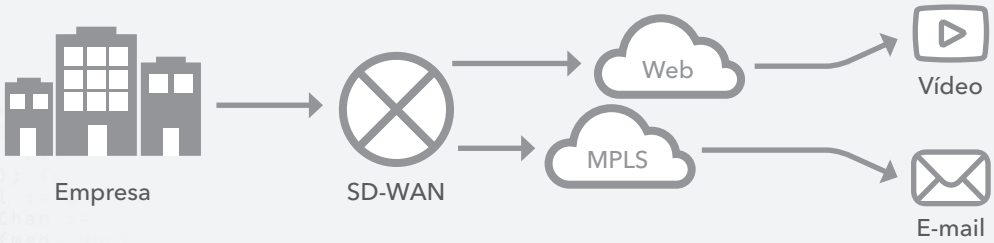
Mas essa subestrutura importante tem algumas restrições. As WANs geralmente entregam largura de banda baixa ou insuficiente, causam problemas com o desempenho de aplicações específicas, não são totalmente confiáveis e podem representar um risco de segurança para seus negócios. Além disso, as WANs são frequentemente construídas em linhas alugadas ou são alugadas por provedores de serviços cuja infraestrutura usa comutação de circuitos ou métodos de comutação de pacotes, como modo de transferência assíncrona (ATM) e comutação multiprotocolo de rótulo (MPLS), além da Internet pública. Embora esta última seja uma opção um pouco menos dispendiosa, ainda é um status quo muito caro e não proporciona escalabilidade.

A rede corporativa está se transformando

Em resposta a esses desafios de desempenho, segurança e financeiros, as empresas estão adotando WANs definidas por software (SD-WANs), reduzindo custos e permitindo agilidade.

Surgindo da inovação das redes definidas por software (SDN) e da virtualização de funções de rede (NFV) que foram originalmente usadas em data centers, os departamentos de TI adotaram rapidamente a tecnologia para as redes que conectavam as organizações.

Em poucas palavras, a SD-WAN separa planos de dados e de controle da rede de longa distância. A SD-WAN monitora o desempenho da combinação de conexões de dados por WAN (MPLS, ATM e Internet) e seleciona a conexão mais adequada para cada tipo de tráfego com base no atual desempenho de link, no custo da conexão e nas necessidades da aplicação ou do serviço.



SD-WAN em ação

Uma SD-WAN pode rotear e-mails por MPLS porque a latência não é um problema importante, e o custo por bit enviado é muito baixo. Por outro lado, a SD-WAN pode rotear o tráfego de videoconferência pela Internet para garantir desempenho ideal e latência mínima, mas com um custo por bit enviado mais alto.

A Internet pode se tornar a nova WAN corporativa?

SD-WANs certamente podem ser flexíveis, eficientes e econômicas se usarem vários serviços de transferência de dados, incluindo a Internet pública. No entanto, como não há garantia de desempenho ou SLA (Acordo de Nível de Serviço) para essas opções de transferência, as SD-WANs usam a Internet exclusivamente para as aplicações cujo desempenho não é crítico.

Para aumentar o uso da Internet para entregar maior tráfego de WAN corporativa de maneira eficiente, econômica e segura, e de uma forma que possa coexistir com as implantações atuais de SD-WAN, você deve adotar uma abordagem que elimine as limitações subjacentes da Internet. Uma maneira de fazer isso é usar uma plataforma de borda para entregar aplicações empresariais seguras, rápidas e confiáveis pela Internet, sem expô-las publicamente na Internet. Isso permite maximizar seu investimento atual em SD-WAN enquanto reduz ainda mais os custos à medida que você transfere mais tráfego para a Internet.

Direcionar uma fatia maior do tráfego corporativo para a Internet simplesmente faz sentido devido à trajetória das redes corporativas modernas. O aumento das cargas de trabalho na nuvem, juntamente com usuários e dispositivos móveis e diversificados, significa que os fluxos de trabalho já dependem muito da Internet. E essa tendência continua crescendo.

E se você pudesse dar um passo adiante, estabelecendo uma WAN corporativa segura, escalável e eficiente na Internet?

Neste documento, discutiremos os processos de transformação de sua rede com SD-WAN e a arquitetura segurança Zero Trust, além de posicionar sua organização para ir além da SD-WAN, adotando uma rede corporativa totalmente baseada na Internet.

Uma plataforma de borda permite que você entregue aplicações empresariais seguras, rápidas e confiáveis pela Internet, sem expô-las publicamente na Internet.

> *Até o final de 2023, mais de 90% das iniciativas de atualização de infraestrutura de borda WAN serão baseadas em plataformas de equipamentos nas instalações do cliente (vCPE) virtualizados ou por aplicações/software de WAN definida por software (SD-WAN) em comparação aos roteadores tradicionais (até 40% hoje).”*
>
> *– Gartner, Quadrante Mágico para Infraestrutura de Borda WAN, outubro de 2018*

O valor da SD-WAN

A SD-WAN fornece, principalmente, balanceamento de links, configuração automática de dispositivos e inserção de serviços de segurança de terceiros. O valor dessas funções, a experiência aprimorada do usuário, a redução dos custos de link e a redução no OpEx, pode ter um impacto significativo. A aceitação é clara, e o aval está bem ilustrado.

Dezenas de fornecedores oferecem diferentes recursos de SD-WAN, que podem ser amplamente generalizados em três categorias:

1. *Controle de link flexível*
2. *Capacidade de gerenciamento*
3. *Inserção de serviço*

Controle de link flexível

O primeiro recurso, controle de link flexível, é o principal estatuto de SD-WAN. Como a nuvem é um dos principais destinos para muitas organizações, reverter o tráfego em uma rede privada para um data center, servindo como um ponto de controle centralizado, não é prático. A SD-WAN resolve esse desafio usando o controle inteligente de tráfego, incluindo a seleção dinâmica de percurso. Além disso, a SD-WAN estabelece interrupções na Internet local ou de filiais, também conhecidas como acesso direto à Internet (DIA), que encaminha o tráfego para a nuvem em vez de transferir para um data center. Dessa forma, todas as aplicações legadas, incluindo de voz e vídeo, são designadas para links MPLS, enquanto as aplicações em nuvem e o tráfego da Internet vão direto para a Internet.

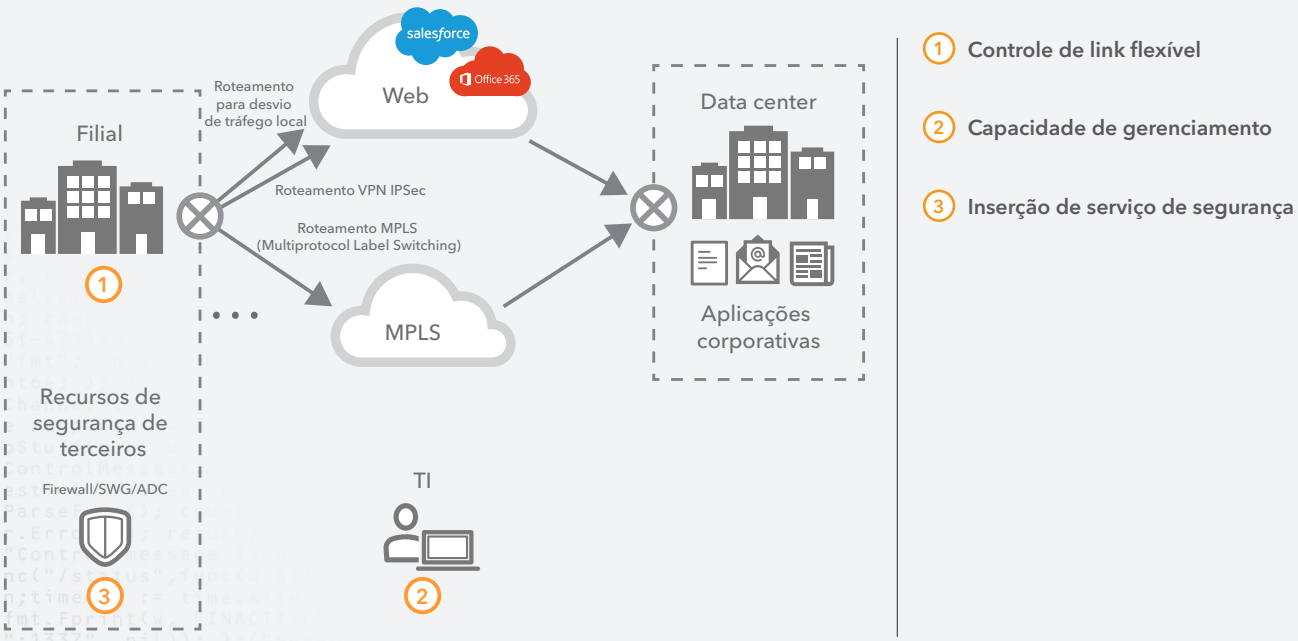
Capacidade de gerenciamento

Os fornecedores de SD-WAN também podem fornecer capacidade de gerenciamento, simplificando a operação e o gerenciamento de dispositivos de rede. Desde a década de 1990, as WANs corporativas são compostas de dispositivos de rede, como switches multicamadas e roteadores. Esses dispositivos foram amplamente gerenciados por aplicação. Em outras palavras, os administradores precisam configurar e manter centenas de milhares de dispositivos individualmente, monitorando a pilha de software de cada dispositivo, em toda a organização. Mesmo que os dispositivos troquem dinamicamente as informações de roteamento ou estabeleçam alta disponibilidade usando protocolos de roteamento, o esforço é enorme. Com a SD-WAN, todo o gerenciamento de dispositivos pode ser feito em um único console centralizado.

Inserção de serviço

Por fim, alguns provedores de SD-WAN são especializados na inserção de serviços. O requisito mínimo para WAN é a capacidade de recuperação de IP, ou seja, conectividade de rede de Camada 3, em toda a organização. No entanto, à medida que a rede evoluiu, as funções de segurança também evoluíram: firewalls, sistemas de proteção contra invasão (IPS) e controladores de entrega de aplicações, para citar alguns. No passado, você precisava de um projeto de roteamento complicado para adicionar esses recursos à rede, pois os dispositivos que fornecem tais serviços geralmente não conseguem interagir com protocolos de roteamento dinâmico (abrir primeiro o caminho mais curto [OSPF], protocolo de gateway de fronteira [BGP]), resultando em uma combinação complexa de roteamento estático e redistribuição. A SD-WAN torna essas tecnologias, muitas vezes entregues por terceiros, fáceis de configurar e simples de gerenciar por meio de um portal unificado.

Valor comercial da SD-WAN

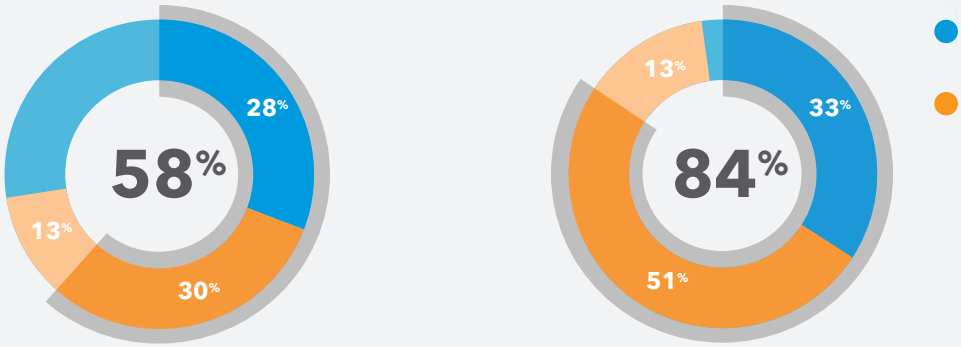


1. Controle de link flexível
2. Capacidade de gerenciamento
3. Inserção de serviço de segurança

Um novo modelo: Segurança Zero Trust

Nova arquitetura exige nova segurança. À medida que as transações migram para a nuvem e para a Internet, as redes se tornaram altamente distribuídas, criando superfícies de ataque adicionais. Aplicações, usuários, dados e dispositivos mudaram para fora da zona de controle tradicional, dissolvendo o que era antes o perímetro empresarial confiável. Dessa forma, criar e aplicar um modelo de segurança que dependa de um perímetro corporativo não é mais viável. Uma estratégia de defesa moderna deve resolver as cargas de trabalho e forças de trabalho distribuídas de hoje.

Até que ponto você concorda/discorda?



"O perímetro de rede é indefensável no ecossistema tecnológico atual de redes de nuvem distribuídas e usuários móveis/remotos."

"A transformação digital necessita de ajustes às estratégias de segurança tradicionais (baseadas em perímetro)."

Forrester Research, Build Your Zero Trust Security Strategy With Microsegmentation (Crie sua estratégia de segurança Zero Trust com microssegmentação), setembro de 2018

O modelo de segurança Zero Trust supõe que não existe um lado "interno" e que todos os dispositivos são igualmente não confiáveis. Cada solicitação de acesso requer autenticação e autorização. As aplicações e os dados são entregues somente após a verificação, e ainda assim, em uma base transitória e com escopo limitado. Essa estrutura de segurança trata todas as aplicações da mesma maneira como lida com a Internet, e considera a rede inteira como comprometida e hostil. Além disso, a visibilidade é essencial; o registro completo e a análise comportamental são indispensáveis.

Os princípios básicos da segurança Zero Trust incluem:

- *Certificar-se de que todos os recursos são acessados com segurança, independentemente do local ou do modelo de hospedagem*
- *Adotar uma estratégia de "privilégio mínimo" e "negação padrão" ao aplicar o acesso a aplicações*
- *Inspecionar e registrar tráfego, para as aplicações que você controla e para aquelas que não controla, a fim de identificar atividades mal-intencionadas*

Há dois componentes principais que suportam a implementação da segurança Zero Trust:

- *Proxy com reconhecimento de identidade para acesso seguro às aplicações*
- *Gateway seguro de Internet para proteção dos usuários*

Proxy com reconhecimento de identidade para acesso seguro às aplicações

Se os usuários, os dados e as aplicações estiverem na nuvem, e o DIA habilitado pela SD-WAN fornecer a conexão, por que não mudar a segurança e a pilha DMZ para a nuvem também? Dessa forma, você pode aproveitar o modelo Zero Trust para garantir o acesso seguro às aplicações que você controla, ao mesmo tempo que reduz o risco associado aos usuários que acessam as aplicações que você não controla.

Se atualmente está optando por uma simples configuração de VPN para fornecer acesso às aplicações corporativas, você provavelmente permite que usuários logados tenham acesso em nível de IP a toda a sua rede. Mas isso é altamente arriscado e vai contra os princípios da segurança Zero Trust. Por que os funcionários de call center devem ter permissão de acesso aos repositórios de código-fonte? Por que uma empresa contratada que usa seu sistema de faturamento deve ter os direitos dos terminais de processamento de cartão de crédito? O acesso deve ser concedido apenas às aplicações necessárias para executar uma função. A VPN tradicional não permite esse acesso granular, em vez disso, exige uma dependência contínua em um modelo de rede hub-and-spoke.

Uma arquitetura de proxy com reconhecimento de identidade (IAP) fornece acesso às aplicações por meio de um proxy baseado em nuvem. A identidade e a autorização ocorrem na borda e são baseadas em princípios de "necessidade de conhecimento", menos privilégios que são semelhantes ao acesso por perímetros definidos por software (SDPs), mas, em vez disso, usam protocolos HTTPS padrão na camada da aplicação (Camada 7).

As duas maneiras de um IAP trabalhar

Você integra uma CDN em transações entre países para melhorar a resposta das aplicações

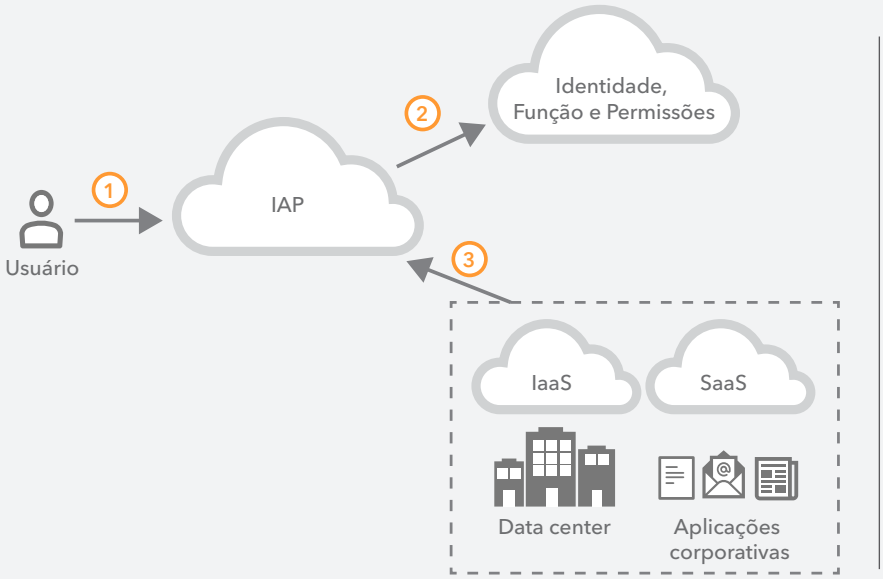
OU

Você usa um Web Application Firewall (WAF) para proteger os servidores da Web corporativos contra vulnerabilidades comuns, como injeção de SQL e scripts entre websites

Um componente essencial de um IAP é uma origem de identidade que verifica a confiança do usuário e do dispositivo (autenticação) e ao que eles têm permissão para acessar (autorização). Essa fonte de identidade pode ser baseada em diretórios corporativos ou provedores de identidade baseados em nuvem. Mesmo antes que a identidade de um usuário seja validada, verificar a postura de um dispositivo pode garantir que o dispositivo que está tentando obter acesso atenda a determinados critérios de segurança, por exemplo, ter um certificado, executar o SO mais recente, ser protegido por senha ou ter a solução apropriada de detecção e resposta de endpoint instalada e operacional.

Um benefício notável do IAP em comparação com outras tecnologias de acesso: Os usuários não são apenas verificados, mas o tráfego dos usuários é inspecionado e as solicitações individuais de aplicações podem ser encerradas, examinadas e autorizadas. Depois que uma transação é encerrada no proxy, serviços adicionais podem ser integrados, permitindo uma melhor experiência do usuário e proteção de aplicações.

Proxy com reconhecimento de identidade (IAP)



1. **Solicitação de acesso**
2. **Confirmar identidade, função e permissões**
3. **Fornecer acesso por meio de proxy**

O IAP também depende dos controles de acesso no nível da aplicação, não das regras de firewall; as políticas configuradas podem refletir a intenção do usuário e da aplicação, não apenas portas e IPs. Assim como os SDPs (Session Description Protocol), essa abordagem pode ocultar as aplicações e outros ativos na nuvem ou atrás do firewall e não é cliente para aplicações da Web.

À medida que a adoção da nuvem cresce, o desafio da migração de aplicações corporativas está em foco. Muitas organizações estão lutando para aproveitar a nuvem para aplicações tradicionais e nativas da nuvem. O IAP não só pode ser usado para autenticar usuários para aplicações SaaS nativas, mas também pode ser usado essencialmente para aplicações legadas "SaaSify" no data center. Além disso, um proxy facilita a migração para a nuvem e a modernização de aplicações sem recorrer a uma estratégia completa de substituição total. Como resultado, as empresas podem adotar uma abordagem metódica e passo a passo para implementar o modelo Zero Trust e, ao mesmo tempo, reduzir a dívida técnica associada a controles legados baseados em perímetro e VPNs tradicionais.

Gateway seguro de Internet para proteção dos usuários

Um aspecto crítico da transição para um modelo de segurança Zero Trust é garantir que os usuários permaneçam seguros ao acessar as aplicações que você não controla. Há um grande número de ameaças virtuais à espreita a cada clique na Internet. Antigamente, quando os usuários eram vinculados à rede corporativa e aos dispositivos gerenciados, a proteção contra malware, ransomware e phishing era tão simples quanto implantar antivírus de endpoints, instalar uma pilha de dispositivos em um data center e reverter o tráfego para inspeção e controle.

Com os usuários em vários locais, a Internet se torna a rede de escolha corporativa. Um SIG baseado em nuvem oferece a você uma base segura, protegendo proativamente os usuários onde quer que eles estejam.

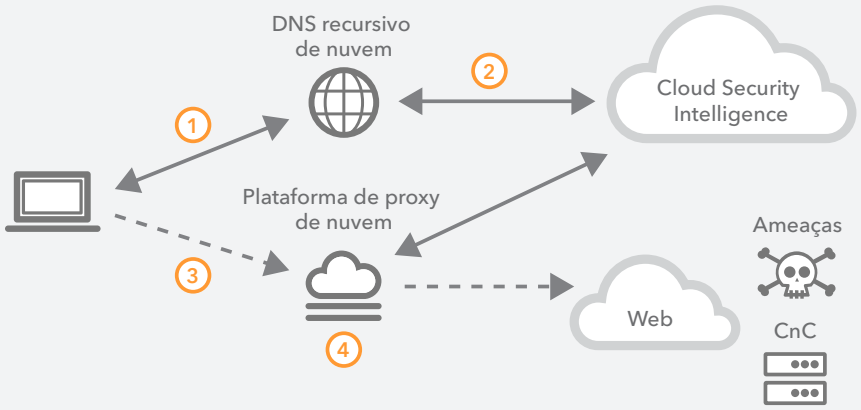
Mas os usuários deixaram o prédio, os dispositivos não são gerenciados e a Internet está se tornando a rede corporativa de escolha. A conectividade da DIA torna obsoletas as soluções centrais de controle e segurança de inspeção. Uma alternativa é replicar a pilha de dispositivos de segurança em cada interrupção da Internet. No entanto, para a maioria das empresas, isso é inviável, tanto logística quanto financeiramente. E, talvez mais importante, a complexidade inerente dessa abordagem introduz falhas de segurança, arquitetadas em oposição direta às práticas recomendadas do modelo Zero Trust.

Um método mais simples, rápido e econômico de proteger o tráfego DIA é usar um gateway de Internet seguro baseado em nuvem (SIG). Um SIG é um acesso seguro para a Internet, protegendo proativamente os usuários, independentemente de sua localização, contra ameaças avançadas, pois propaga tráfego arriscado para controle e inspeção. Isso é obtido ao examinar cada solicitação de DNS, bloquear solicitações a domínios mal-intencionados, permitir que as solicitações a domínios seguros continuem normais e encaminhar solicitações de domínios de risco a um proxy de nuvem para inspeção adicional.

Nessa fase final, quando o proxy recebe uma solicitação HTTPS, ele compara o URL solicitado a uma base de conhecimento de inteligência de ameaças baseada em nuvem e bloqueia os URLs mal-intencionados. Para todos os outros URLs solicitados classificados como de risco, o proxy envia o conteúdo da Web para análise de carga em linha por meio de vários mecanismos de análise de malware. Esses motores usam uma variedade de técnicas de detecção (assinatura, sem assinatura e aprendizado de máquina) para identificar e bloquear ameaças conhecidas e ameaças desconhecidas anteriormente de "dia zero". Com uma variedade de métodos de detecção, você pode direcionar uma carga útil para o motor mais adequado (ou motores), dependendo do tipo de conteúdo, o que garante taxas de detecção ideais e fornece uma baixa taxa de falsos positivos.

É importante observar que essa abordagem é bem diferente da adotada por dispositivos de segurança herdados, como gateways seguros da Web (SWGs). Especificamente, os SWGs promovem todo o tráfego da Internet, inspecionando o bom e o ruim, o que pode ser especialmente prejudicial às páginas da Web complexas e a conteúdos HTTPS mais pesados. Essa abordagem diminui o desempenho, introduz latência e aumenta o volume de websites "inválidos" e aplicações, a consequência da intermediação de todo o tráfego. Os SWGs geralmente resultam em mais incidentes de segurança e falsos positivos, gerando solicitações de suporte técnico e monopolizando recursos de TI.

Arquitetura de Gateway de Internet seguro



1. **Pesquisa de DNS (Sistema de Nomes de Domínio)**
2. **Categorização de domínio como benigno, mal-intencionado ou suspeito**
3. **Domínios suspeitos redirecionados para o proxy de nuvem**
4. **Inteligência de ameaças de URL e análise de carga útil**

Um proxy seletivo inteligente pode aproveitar o DNS como a rampa para a Internet e como uma primeira camada de segurança. Permitir que o tráfego seguro vá direto para a Internet, bloquear o tráfego prejudicial e realizar o proxy somente do tráfego arriscado resulta em:

- *Segurança simplificada*
- *Menor latência e melhor desempenho*
- *Menos páginas da Web e aplicações interrompidas*

Transformação da rede com menos riscos: Implementação do modelo Zero Trust em um ambiente SD-WAN

Muitas organizações que estão migrando para arquiteturas baseadas na Internet consideram a SD-WAN o principal facilitador devido ao seu controle de link e capacidade de potencialmente diminuir o ônus financeiro da propriedade do MPLS. Essas organizações podem usar redes de banda larga ou sem fio para aumentar ou complementar as conexões MPLS, criando uma WAN híbrida. Mas se já adotaram o DIA, então certamente faz sentido empregar um modelo de segurança com a mesma abordagem.

À medida que a SD-WAN é adotada, as empresas precisam evoluir sua segurança de uma estrutura baseada em perímetro para uma estrutura baseada em Zero Trust na borda. Então, onde estamos hoje, e o que vem depois?

As redes com SD-WAN geralmente estão em uma destas três situações, dependendo da abordagem e da estratégia de longo prazo da empresa:

1. *WAN privada tradicional com detalhamento centralizado; ou seja, considerando, mas ainda não implementando a SD-WAN*
2. *Implementação híbrida de WAN privada tradicional para locais existentes e SD-WAN para filiais mais recentes*
3. *Principalmente SD-WAN*

A abordagem da arquitetura de segurança Zero Trust pode se ajustar bem a todos esses cenários. Mas se a empresa já estiver considerando ou implementando a SD-WAN, ela pode já ter adotado a Internet como uma ferramenta de rede empresarial viável e, portanto, está preparada para usar a estratégia de segurança Zero Trust para seu ambiente de rede corporativa.

Vamos examinar as arquiteturas atuais para identificar como cada uma pode implementar o modelo Zero Trust e, em seguida, avançar para o estado futuro desejado.

WAN privada tradicional com detalhamento centralizado

Se as motivações por trás da migração SD-WAN forem custo, agilidade e flexibilidade, benefícios que uma arquitetura de rede baseada na Internet pode oferecer, pode fazer sentido ignorar a SD-WAN completamente e ir direto para uma estrutura Zero Trust. O IAP permite o acesso com base no modelo Zero Trust a aplicações, independentemente da localização, enquanto o SIG fornece aos usuários acesso seguro à Internet, tudo sem que as organizações tenham que criar pilhas de segurança em cada intervalo da Internet.

Um ponto para ter em mente: se a empresa já oferece suporte a serviços em tempo real, como VoIP e videoconferência, por meio de um provedor de serviços de Internet em nuvem, ela está idealmente posicionada para adotar totalmente uma arquitetura de rede e acesso baseada na Internet. Se esses serviços ainda estiverem hospedados, principalmente, no local, poderá haver um caso para reter algum nível de rede "privada" entre locais, seja privada (por exemplo, baseado em MPLS) ou baseada em SD-WAN.

Híbrido com WAN tradicional e SD-WAN

Neste cenário, as organizações já deram o primeiro passo para uma arquitetura baseada na Internet mais eficiente.

Nesses ambientes, é importante entender como o tráfego do usuário é tratado:

- *Os usuários têm acesso direto à Internet em escritórios remotos ou o link da Internet é usado apenas para retornar a comunicação em rede para os principais locais?*
- *Onde estão situadas as aplicações principais do usuário? No local, em um data center ou na nuvem?*
- *Se for usada a nuvem, como os usuários se conectam a essas aplicações? A conexão é facilitada por DIA em uma filial ou revisada para um link de conexão direta?*
- *Qual é a extensão do uso de aplicações SaaS?*
- *Para o DIA na filial, qual é o nível de abrangência da pilha de segurança em cada local?*

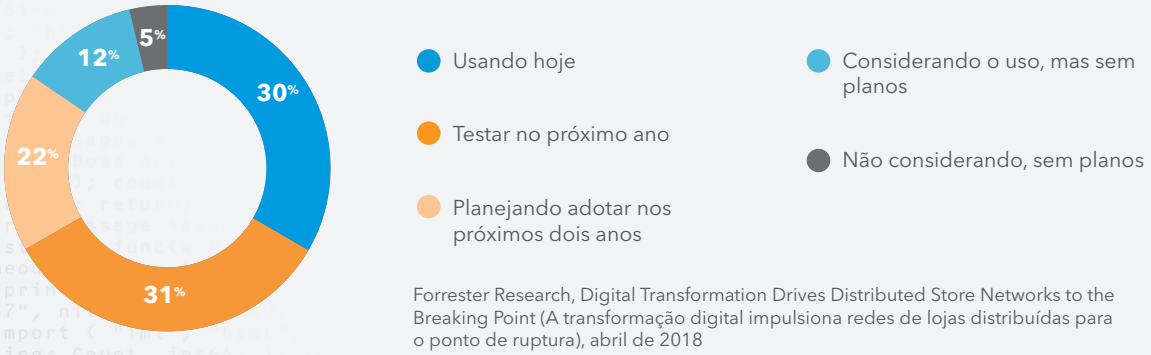
Naturalmente as respostas variam, dependendo do tratamento do tráfego de usuários, e, desse modo, a migração de rede terá graus de complexidade variáveis. Mas existem duas constantes: Haverá um aumento no uso da Internet e uma necessidade de fazer a transição da segurança baseada em perímetro para um modelo Zero Trust.

Por exemplo, uma situação em que há alguma conectividade DIA em um escritório remoto. Um SIG pode oferecer proteção adicional para a pilha de segurança centralizada, bem como substituir algumas das pilhas, reduzindo a complexidade e o custo.

Se os usuários acessarem aplicações baseadas em nuvem, uma abordagem baseada em IAP poderá fortalecer a postura de segurança da organização e melhorar a experiência do usuário. Isso também pode aumentar o desempenho da aplicação, permitindo o acesso direto a aplicações pela Internet com uma CDN (Rede de Entrega de Conteúdo).

Você pode continuar mudando da WAN tradicional para um ambiente SD-WAN, permitindo o DIA para escritórios remotos e adotando os princípios da segurança Zero Trust.

Quais são seus planos de negócios para usar a tecnologia de rede definida por software (SD-WAN) hoje?



Forrester Research, Digital Transformation Drives Distributed Store Networks to the Breaking Point (A transformação digital impulsiona redes de lojas distribuídas para o ponto de ruptura), abril de 2018

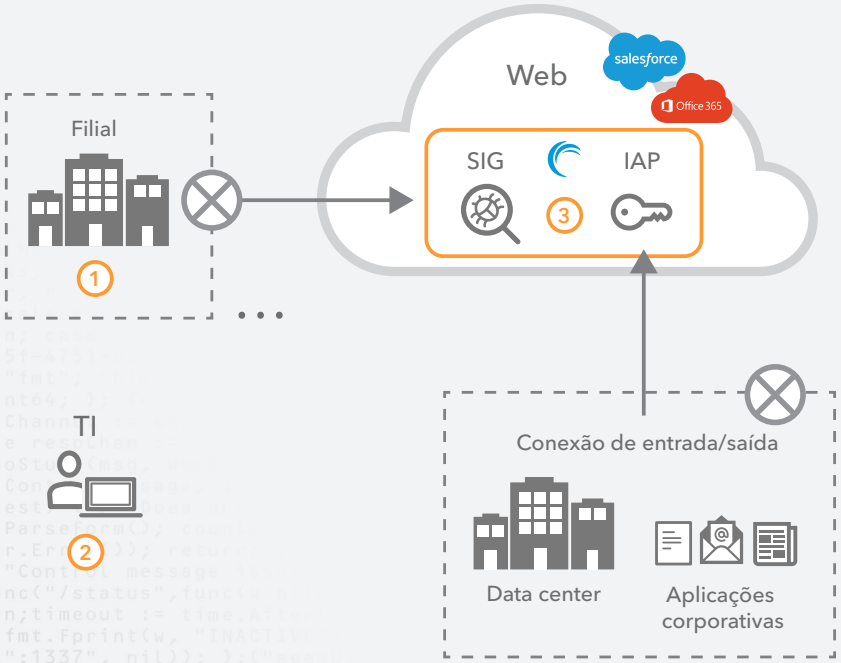
Principalmente SD-WAN

Nesse estado, as organizações provavelmente se afastaram de uma rede WAN privada tradicional, usando roteamento inteligente em links da Internet entre websites para comunicação entre os escritórios, utilizando plenamente as vantagens do DIA. Essas empresas já contam com o acesso à Internet na maioria dos locais; portanto, a evolução da rede para além do SD-WAN é a direção lógica a ser tomada.

A próxima etapa? Comece a reduzir a dependência dos links do MPLS movendo as aplicações para a Internet para entregar agilidade e economia. As aplicações corporativas podem ser acessadas por meio do IAP, mesmo em um ambiente DIA. Se as aplicações já estiverem em um ambiente de nuvem, não faz sentido acessá-las revertendo o tráfego para um data center antes de detalhar em um local central (por exemplo, usando uma topologia de tipo de conexão direta).

Por fim, esse ambiente é adequado para um estado futuro de pura conectividade e acesso baseado na Internet, todas as aplicações corporativos podem ser acessadas por meio do IAP, estejam no local ou baseadas na nuvem. Todo o tráfego do usuário pode ser protegido via SIG. E, se os provedores baseados na Internet entregam comunicação em tempo real, como voz e vídeo, talvez seja possível eliminar completamente a SD-WAN e até mesmo a WAN corporativa. Isso pode reduzir os custos e a complexidade, bem como aumentar a segurança por meio de um modelo de arquitetura Zero Trust.

Valor da arquitetura baseada em Internet com um modelo de segurança Zero Trust



1. **Acesso mais simples à rede**
   - Somente acesso à Internet
   - Sem acesso externo
2. **Capacidade de gerenciamento**
   - Ponto único de gerenciamento
   - Monitoramento do dispositivo
   - Monitoramento do usuário
3. **Mais controle da segurança**
   - Prevenção de ataques de dia zero
   - AAA centralizada (autenticação, autorização e contabilidade)
   - Verificação da postura do cliente
   - Prevenção de phishing, malware e CnC

Transforme sua empresa

A realidade moderna das empresas aumenta a exposição em um ambiente que já está repleto de riscos e complexidade. Um modelo de rede gerenciado por transações hub-and-spoke em uma WAN privada é tão desatualizado quanto a defesa empresarial baseada em perímetro; as arquiteturas de rede e de segurança devem evoluir. Embora a SD-WAN atualmente permita que a rede corporativa lide com o tráfego de forma eficiente e mova as cargas de trabalho para a nuvem, esse modelo de rede deve continuar iterando. A Internet é a WAN corporativa do futuro próximo.

A Akamai acredita que o uso de SD-WAN, combinado com os serviços adequados de segurança e acesso compatíveis com Zero Trust, é o primeiro passo para fazer a transição para a Internet como a rede corporativa. Junte a SD-WAN com a plataforma de borda inteligente da Akamai e aplique a política de acesso e segurança universalmente, garantindo experiências rápidas e confiáveis de aplicações do usuário final pela Internet.

A Akamai pode ajudar a orientar a evolução de sua rede e de sua segurança. Entre em contato com a equipe de sua conta para saber mais sobre uma avaliação do Zero Trust da Akamai. Você receberá recomendações tangíveis de nossos especialistas em segurança sobre onde começar ou como progredir em sua transformação de Zero Trust. Ou acesse *Três maneiras simples de começar a implementar a segurança Zero Trust hoje* para obter recursos para iniciar sua transição.