DOCUMENTO EMPRESARIAL

aruba
a Hewlett Packard Enterprise company

AS MELHORES SOLUÇÕES DE SD-WAN E SASE COM ZERO TRUST IMPULSIONAM A EMPRESA DIGITAL

ÍNDICE

SUMÁRIO EXECUTIVO

As empresas continuam adotando a transformação digital com a intenção de aumentar a eficiência, melhorar a satisfação dos clientes, buscar novas oportunidades de mercado, impulsionar a lucratividade e manter uma vantagem competitiva. A migração de aplicativos empresariais para a nuvem é um aspecto fundamental para qualquer iniciativa de transformação digital bem-sucedida. Por quê? Atualmente, existem mais aplicativos sendo executados na nuvem do que em data centers empresariais tradicionais, e a maioria desses aplicativos é consumida na forma de software como serviço (SaaS). Além disso, no mundo que prioriza a nuvem, as empresas precisam garantir acesso direto e seguro aos aplicativos a todo momento, de qualquer lugar e usando qualquer dispositivo. Também desejam garantir que a rede entregue consistentemente a melhor experiência possível tanto para funcionários como para clientes. Por fim, a explosão de dispositivos móveis e IoT no ambiente corporativo aumentou drasticamente a superfície de ataque, expondo as empresas a violações de segurança capazes de comprometer os dados e causar tempo de inatividade da rede.

As redes corporativas atuais nunca foram projetadas para o mundo que prioriza a nuvem, por isso não são suficientes para enfrentar os desafios de cibersegurança da transformação digital. É essencial que as empresas não só protejam os aplicativos na nuvem, mas também protejam os usuários que se conectam a esses aplicativos pela rede de longa distância (WAN). Ao mesmo tempo, a proliferação de dispositivos IoT aumentou significativamente a superfície de ataque, expondo as empresas a uma quantidade cada vez maior de ameaças à cibersegurança.

Portanto, o imperativo estratégico é adotar uma rede de longa distância definida por software (SD-WAN) que seja mais inteligente, mais segura e altamente automatizada e que possa ser integrada de forma otimizada aos serviços de segurança oferecidos na nuvem para criar a melhor arquitetura de borda de serviço de acesso seguro (SASE) da categoria. A SASE deve ser ampliada com segurança zero trust baseada em identidades para implementar segmentação de modo que os usuários e dispositivos IoT só consigam alcançar destinos na rede que estejam de acordo com sua função na empresa.

Como a transformação da WAN e da segurança é uma jornada, uma empresa pode começar modernizando sua WAN ou segurança, mas para alcançar o verdadeiro valor do investimento em nuvem, ambos os aspectos devem ser abordados.

As redes corporativas atuais nunca foram projetadas para o mundo que prioriza a nuvem, por isso não são suficientes para enfrentar os desafios de cibersegurança da transformação digital. É essencial que as empresas não só protejam os aplicativos na nuvem, mas também protejam os usuários que se conectam a esses aplicativos. Ao mesmo tempo, a proliferação de dispositivos IoT aumentou significativamente a superfície de ataque, expondo as empresas a uma quantidade cada vez maior de ameaças à cibersegurança.

Também é igualmente importante evitar dependência de fornecedor ao escolher parceiros de soluções de tecnologia que ofereçam flexibilidade e liberdade de escolha. Com arquiteturas de rede e segurança transformadas, as empresas podem adotar inovações oportunas para acelerar a produtividade, o aumento da receita e a lucratividade, tudo isso sem perder o controle dos custos.

SE OS APLICATIVOS SÃO OFERECIDOS NA NUVEM, A SEGURANÇA TAMBÉM DEVERIA SER

Tradicionalmente, todo o tráfego de aplicativos proveniente de filiais é retornado via serviços MPLS privados para o data center corporativo para inspeção e verificação de segurança (veja a Figura 1). Essa arquitetura fazia sentido quando os aplicativos eram hospedados exclusivamente no data center corporativo. Mas com a migração de aplicativos e serviços para a nuvem, essa arquitetura de rede tradicional deixa a desejar, principalmente porque prejudica o desempenho dos aplicativos e oferece uma experiência inconsistente aos usuários, pois o tráfego destinado à Internet primeiro passa pelo data center e firewall corporativo antes de chegar ao destino.

Além do mais, com a quantidade cada vez maior de funcionários trabalhando fora da rede corporativa e conectando-se diretamente aos aplicativos de nuvem, a tradicional segurança baseada em perímetro torna-se insuficiente. A nuvem e a abordagem SaaS mudaram para sempre a forma como os usuários se conectam e interagem com os aplicativos. Ao transformar suas arquiteturas de WAN e segurança, as empresas conseguem garantir acesso direto e seguro a aplicativos e serviços em ambientes multicloud, independentemente da localização ou dos dispositivos usados para acessá-los.

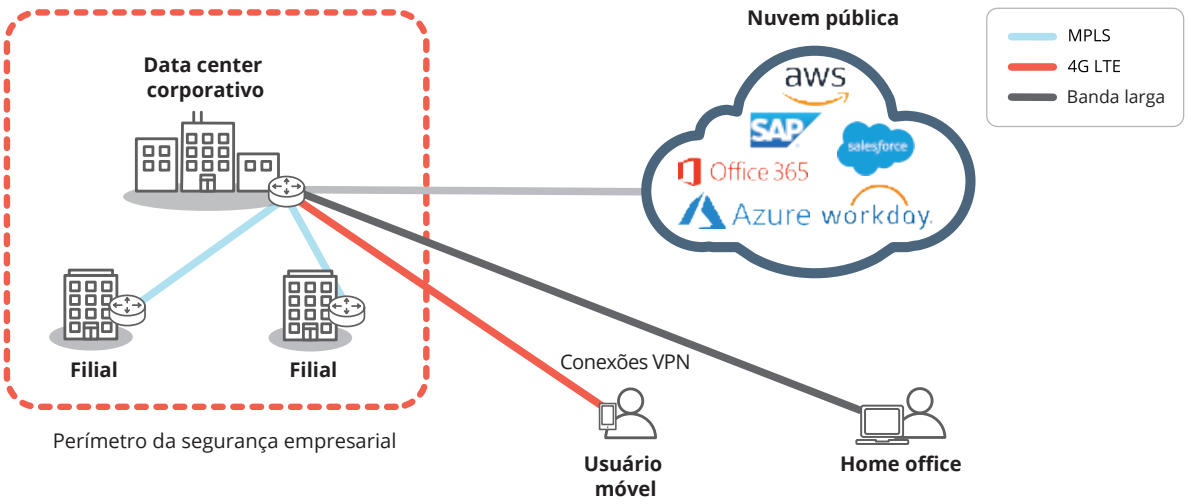

Figura 1: WANs empresariais tradicionais e abordagens de segurança baseadas em perímetro não foram concebidas para a nuvem. O retorno de todo o tráfego de aplicativos de filiais para o data center prejudica o desempenho e proporciona uma experiência de usuário inconsistente.

Em 2019, a Gartner cunhou o termo SASE, ou borda de serviço de acesso seguro, para uma estrutura que combina SD-WAN com funções de Borda de serviço de segurança (SSE) na nuvem, incluindo gateway da web seguro (SWG), firewall como serviço (FWaaS), agente de segurança de acesso à nuvem (CASB) e acesso à rede zero trust (ZTNA). Anteriormente, essas funções eram exclusivas e dedicadas, mas, agora, podem ser oferecidas na nuvem de maneira unificada, conforme mostra a Figura 2.

Os pioneiros na adoção de soluções de SSE deixaram de implementar uma SD-WAN que não aplicasse breakout de Internet adaptável diretamente das filiais. Dessa forma, não conseguiam conduzir o tráfego diretamente de uma filial para a nuvem. Sem o componente da SD-WAN, o tráfego destinado à nuvem continuava sendo retornado para o data center, afetando negativamente o desempenho do aplicativo.

A adoção de soluções de borda de serviço de segurança e SD-WAN elimina o custo e a complexidade associados ao gerenciamento de vários firewalls no local, mas ainda exige funcionalidade de firewall nas filiais para bloquear possíveis ameaças. Conforme mostrado na Figura 3, usando uma solução avançada de SD-WAN, as empresas podem se conectar diretamente à nuvem por meio de um breakout de Internet adaptável usando conexões de banda larga. A inteligência para reconhecer aplicativos permitidos possibilita o breakout local de uma filial para o ponto de presença (PoP) mais próximo, eliminando a latência e proporcionando a melhor experiência possível para aplicativos de nuvem e SaaS confiáveis, como Microsoft Office 365, 8x8 e RingCentral. O reconhecimento dos aplicativos também possibilita o envio de outros tráfegos associados à Internet primeiro para um provedor de segurança na nuvem para inspeção avançada antes do

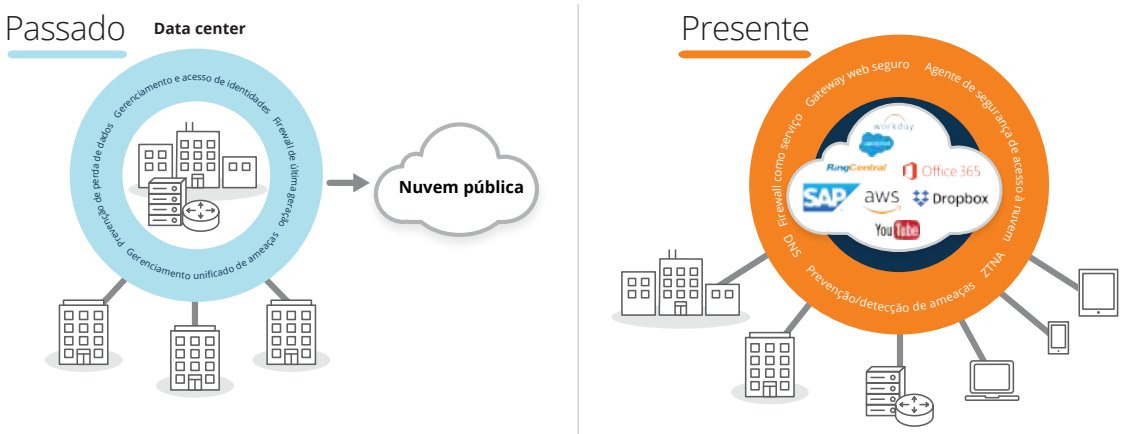

Figura 2: No passado, o objetivo era proteger o data center empresarial em que os aplicativos eram exclusivamente hospedados. Hoje, com a migração e execução dos aplicativos na nuvem, a segurança empresarial baseada em perímetro está se tornando cada vez mais ineficaz. É fundamental pensar diferente e migrar a segurança para a nuvem.

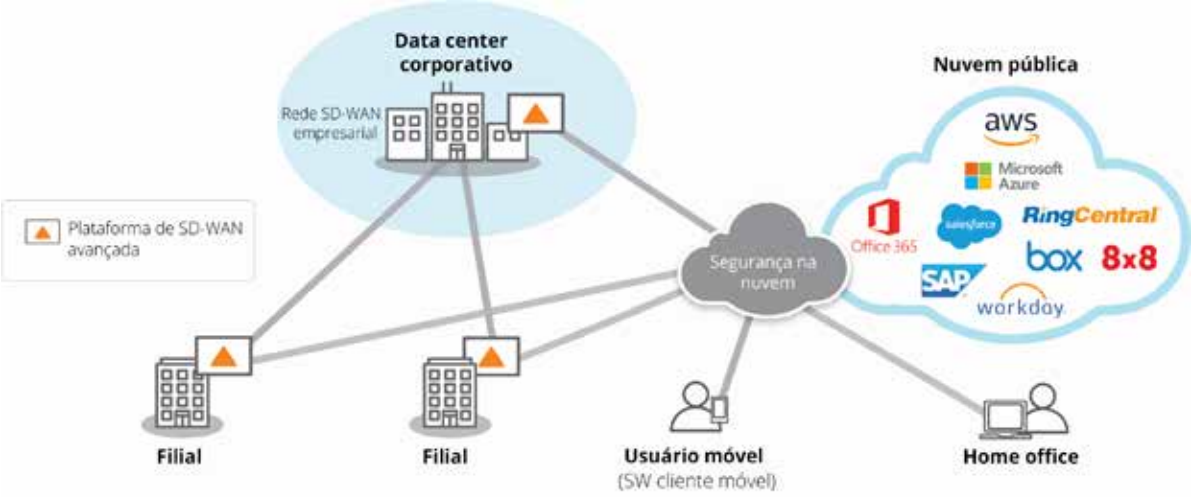

Figura 3: Uma SD-WAN avançada oferece uma rampa segura de acesso à nuvem para as empresas. As filiais podem usar conexões de banda larga e breakout de Internet adaptável para conectar usuários a aplicativos de nuvem diretamente, otimizando o desempenho do aplicativo e a experiência do usuário. A combinação de SD-WAN avançada e segurança na nuvem cria uma borda de serviço de acesso seguro (SASE) que garante que os usuários, dispositivos e aplicativos estejam sempre protegidos.

encaminhamento para um provedor de SaaS. Recursos avançados de SD-WAN integrados com serviços modernos de segurança na nuvem garantem consistência na aplicação de políticas e no controle de acesso para usuários, dispositivos, aplicativos e IoT. Isso permite que as empresas imponham a conformidade, evitem tempo de inatividade e reduzam o risco de comprometimento dos dados associado a violações de segurança.

A MELHOR SOLUÇÃO DE SASE DA CATEGORIA PROPORCIONA LIBERDADE DE ESCOLHA

Com a constante evolução das abordagens de implementação de segurança de rede e a dificuldade do desenvolvimento de soluções de rede complexas, é importante considerar as melhores soluções de rede e segurança da categoria de fornecedores com experiência e foco comprovados. É impensável encontrar um único fornecedor capaz de oferecer os melhores recursos de SASE da categoria em ambos os domínios, e as empresas não devem ser forçadas a se comprometer com recursos básicos em nenhuma das frentes.

Com a segurança como questão prioritária devido ao cenário de aumento contínuo das ameaças, as empresas precisam manter a agilidade para adotar novas soluções de segurança com rapidez e eficiência de custos, sem ficarem presas a um único fornecedor de soluções. Ter uma solução de rede independente oferece a garantia e a tranquilidade que as empresas precisam para selecionar e implantar as soluções de segurança da nuvem que melhor se alinham aos seus requisitos comerciais e de segurança em constante evolução.

Uma solução avançada de SD-WAN integra-se rigorosamente a vários fornecedores de SSE, oferecendo a liberdade de escolha para selecionar as melhores soluções de fornecedores da categoria que unificam SD-WAN e segurança na nuvem usando orquestração automatizada. Com a melhor solução de SASE da categoria, as empresas podem desenvolver uma arquitetura de segurança consistente que bloqueia o impacto de ataques cibernéticos, aumenta a agilidade dos negócios e reduz a complexidade. Em última análise, isso permite que as empresas alcancem um efeito multiplicador em seus investimentos existentes e contínuos feitos em serviços e aplicativos de nuvem.

COMO PROTEGER A IOT EMPRESARIAL COM UMA ABORDAGEM ZERO TRUST

A proliferação de dispositivos IoT entre as empresas revela novas formas de monitorar, relatar, alertar, automatizar e otimizar processos de negócios, desde linhas de manufatura até a automação de HVAC e iluminação para economizar energia. A IoT aumenta a eficiência dos negócios por meio de automação, mas também aumenta a superfície de ataque ao adicionar uma nova dimensão de complexidade. A forma como a TI enfrenta o desafio crescente da segurança em dispositivos móveis é implantando uma solução de acesso à rede zero trust (ZTNA) com base no modelo zero trust. Uma solução de ZTNA opera por meio da instalação de um agente de ponto de extremidade em um dispositivo do usuário, como um laptop, tablet ou smartphone.

Esse agente de software garante que o tráfego do dispositivo seja direcionado para um serviço de segurança na nuvem antes de ir para um aplicativo SaaS ou provedor de IaaS. No entanto, ao contrário de tablets e smartphones, os agentes de software de ZTNA não podem ser instalados em dispositivos IoT pois são dispositivos sem agente. Eles não têm suporte para instalação de agentes de software de terceiros. Por causa disso, as empresas precisam de uma solução de segurança diferente para dispositivos IoT a fim de proteger as redes corporativas contra possíveis vulnerabilidades capazes de violar a rede e interromper as operações comerciais diárias.

Uma SD-WAN avançada compatível com arquiteturas zero trust segmenta a rede de maneira dinâmica e aplica princípios de acesso menos privilegiado, permitindo que as empresas reduzam o risco associado a violações ao implantar dispositivos IoT. Ela garante que os usuários e dispositivos só se comuniquem com destinos consistentes com sua respectiva função com base em identidade, direitos de acesso e postura de segurança. Também orquestra a segmentação de ponta a ponta, abrangendo a LAN-WAN-LAN e LAN-WAN-data center/nuvem da empresa, o que resulta na aplicação consistente e automatizada de políticas de segurança com mais visibilidade. Com a segmentação de ponta a ponta, as empresas conseguem criar segmentos isolados para tráfego de dispositivos IoT. É possível definir uma política de segurança independente para cada segmento ao determinar quais políticas de segurança devem ser aplicadas ao tráfego de dispositivos. Como o tráfego em um segmento é isolado do tráfego de todos os outros segmentos, qualquer acesso não autorizado é impedido. Mesmo que surja uma ameaça, seu impacto será restrito ao segmento em que surgiu.

Vejamos um exemplo. Em um local remoto em que dispositivos IoT sem agente, como sistemas de PdV e HVAC, estão instalados (Figura 4 abaixo), uma plataforma avançada de SD-WAN identifica aplicativos usados de maneira exclusiva pelos dispositivos. Uma política do sistema intercepta o tráfego do PdV e o direciona para o data center corporativo que hospeda o aplicativo de processamento de transações com cartão de crédito. Neste exemplo, são aplicados serviços de segurança de firewall existentes implantados no data center. Por outro lado, as políticas do sistema de HVAC segmentam e direcionam o tráfego de HVAC para o serviço de segurança na nuvem para inspeção de segurança adicional antes de chegar ao centro de controle de IoT hospedado na nuvem pública. Como o tráfego da IoT é isolado conforme a política de negócios, uma violação no segmento de HVAC não compromete nem coloca em risco os dados pessoais e de cartão de crédito no segmento de PdV. A segmentação também ajuda empresas a cumprir as obrigações de conformidade do PCI (ou outro) em seus negócios. Como mostrado neste exemplo, uma implantação de segurança abrangente com uma plataforma SD-WAN avançada pode proteger melhor as empresas dinâmicas da atualidade em sua jornada de transformação à medida que incorporam os benefícios da IoT.

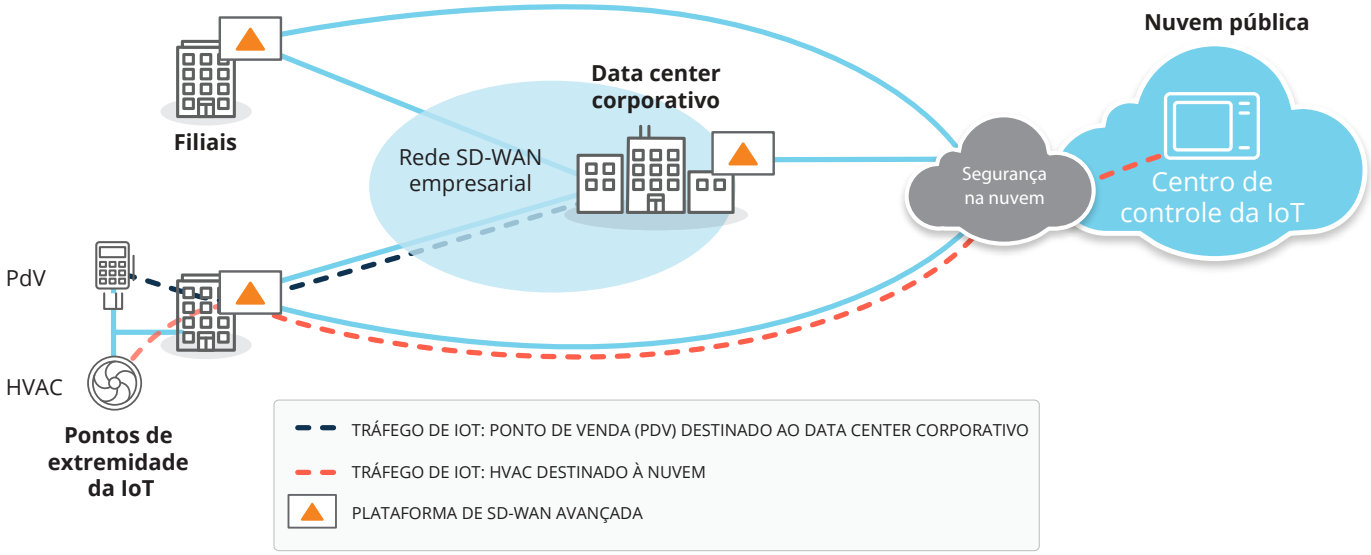

Figura 4: Os pontos de extremidade de IoT estão se multiplicando, e isso representa novos riscos de violações de segurança. Com uma plataforma SD-WAN avançada, as empresas podem proteger os dispositivos IoT ao implementarem uma arquitetura zero trust com segmentação dinâmica da rede. Como mostrado no diagrama, todos os dados de transações de PdV da filial são destinados ao data center empresarial, enquanto o tráfego de HVAC é encaminhado para um centro de controle de IoT na nuvem.

PROTEJA FILIAIS CONTRA AMEAÇAS EXTERNAS COM UMA SD-WAN AVANÇADA

Com a digitalização das empresas, o risco de ataques cibernéticos aumentou significativamente ao longo da última década. Nos ambientes de rede tradicionais baseados em roteador, as filiais acumularam uma grande variedade de equipamentos de rede e segurança, mas esses equipamentos são difíceis de configurar, reparar e manter atualizados com as informações mais recentes sobre ameaças. Os locais remotos também não contam com equipes experientes de TI, o que os expõe a prováveis violações de segurança.

Além de proteger as operações na nuvem com a melhor solução de SASE da categoria, uma solução avançada de SD-WAN pode proteger as filiais contra ameaças mal-intencionadas. É desenvolvida com um firewall de última geração que inclui recursos de defesa contra ameaças, como detecção e prevenção de intrusão (IDS/IPS) e DDoS para proteção das filiais contra ameaças mal-intencionadas.

Um sistema IDS baseado em assinaturas geralmente monitora o tráfego de rede em busca de padrões que correspondem à assinatura de um ataque específico. Quando uma intrusão é detectada, o sensor oferece ações como recusar, inspecionar e permitir tráfego. Os sistemas de prevenção de intrusões podem operar em modo restrito ou eficaz. No modo restrito, o tráfego passa pelo sensor de modo que seja imediatamente bloqueado se ocorrer uma intrusão. No modo eficaz, uma cópia do tráfego é enviada para análise, proporcionando mais eficiência sem afetar o desempenho da rede. Uma intrusão é bloqueada depois que é detectada. As empresas podem escolher entre os modos restrito e eficaz de acordo com seus requisitos de segurança.

Uma SD-WAN avançada também consegue detectar de forma dinâmica ataques DDoS, como ataques de protocolo, inundações ICMP, inundações SYN e ataques de falsificação de IP. Quando um comportamento anormal é detectado na rede, a solução limita o número de solicitações usando ações como obsolescência acelerada, recusa de excedente e bloqueio de origem. Além disso, ela consegue encaminhar o tráfego por meio de links da rede não afetados em caso de um ataque DDoS, garantindo a continuidade dos negócios.

Ao integrar recursos avançados de segurança e rede em uma única solução SD-WAN, como roteamento, otimização de WAN e firewall de última geração, as empresas podem simplificar consideravelmente suas operações de rede em filiais. Além disso, políticas de segurança podem ser enviadas automaticamente de um local central para as filiais com Zero Touch Provisioning, que facilita a configuração das políticas de segurança e rede. Novas filiais são preparadas com rapidez e facilidade, e alterações nas políticas de segurança podem ser distribuídas automaticamente para centenas ou milhares de filiais em questão de minutos com minimização dos erros.

A TRANSFORMAÇÃO DA WAN É ESSENCIAL PARA UMA TRANSFORMAÇÃO DIGITAL BEM-SUCEDIDA

Além de todos os benefícios da migração para uma arquitetura moderna de segurança na nuvem, há um valor enorme na transformação da WAN para as empresas atuais que priorizam a nuvem. As WANs tradicionais centradas em roteador nunca foram projetadas para a nuvem. As empresas precisam modernizar sua arquitetura de WAN e repensar a melhor forma de arquitetar suas redes de filiais a fim de melhorar o desempenho e a segurança dos aplicativos de nuvem. As empresas estão aumentando o uso de nuvem e SaaS, com foco em oferecer a melhor experiência possível aos usuários.

A transformação da WAN envolve oferecer um caminho mais eficiente e uma experiência melhor entre os usuários e a nuvem. Conforme descrito anteriormente, a adoção de breakout de Internet adaptável para aplicativos SaaS e hospedados na nuvem diretamente das filiais não só otimiza a largura de banda disponível, mas também reduz qualquer latência que possa afetar negativamente a produtividade do usuário.

Muitas empresas estão transformando suas bordas de rede e adotando SD-WAN para conectar locais de filiais usando conexões de Internet de banda larga. A SD-WAN oferece seleção de caminhos inteligente e orientada por aplicativos entre vários links WAN (MPLS, Internet de banda larga, LTE etc.) com base em políticas definidas centralmente. Os benefícios da SD-WAN incluem:

- Disponibilização de aplicativos de negócios com eficiência de custos
- Melhoria do desempenho do aplicativo, da disponibilidade e da qualidade da experiência do usuário final
- Cumprimento dos requisitos de filiais/locais remotos modernos
- Acomodação de serviços e aplicativos baseados na nuvem e SaaS
- Melhoria da eficiência de TI na filial por meio de provisionamento de serviços automatizados

COMO CUMPRIR AS EXIGÊNCIAS DE SLAS DE APLICATIVOS

O resultado direto disso é o aumento da produtividade empresarial e da agilidade dos negócios. As empresas precisam de uma rede de alto desempenho, desenvolvida sobre uma base de alta disponibilidade capaz de oferecer suporte a aplicativos críticos para os negócios com confiabilidade. A segurança nunca deve ser uma consideração tardia. A capacidade de oferecer suporte a recursos de microssegmentação e aplicação de políticas granulares permite que as empresas protejam a WAN, cumpram os requisitos de conformidade e se defendam de violações.

As empresas precisam da agilidade para acelerar novas filiais e ajustar dinamicamente políticas e regras de segurança. A capacidade de propagar contexto de políticas é um requisito essencial para a automação de filiais. Isso deixa o conceito de uma solução SD-WAN avançada muito atraente e pode ajudar as empresas a eliminar a necessidade de ter vários dispositivos realizando funções dedicadas de segurança e, em troca, simplificar e consolidar – ou "diluir" – a arquitetura de borda da WAN na filial. Uma plataforma de borda SD-WAN avançada permite que as empresas transformem sua WAN por meio de unificação da SD-WAN, roteamento, otimização da WAN, segmentação e segurança de filial em uma única plataforma com gerenciamento centralizado.

A orquestração centralizada da SD-WAN e uma abordagem específica para aplicativos garantem que as prioridades dos negócios sejam sempre refletidas no comportamento da rede. A unificação da orquestração da rede e das políticas de segurança garante que a QoS e a segurança sejam aplicadas e impostas de forma consistente aos aplicativos, ou classes de aplicativos, independentemente de como ou onde eles estão sendo acessados. O desempenho e a segurança dos aplicativos podem ser ditados por políticas de negócios de cima para baixo, não por restrições de tecnologia de baixo para cima. Uma SD-WAN avançada monitora continuamente o estado da rede e dos aplicativos, detecta mudanças nas condições e aciona respostas imediatas e automatizadas em tempo real para eliminar o impacto de eventos de quedas de energia, apagões e ameaças de segurança. Além disso, a automação da conectividade da plataforma de nuvem com integrações via interfaces programáveis de aplicativos (APIs) simplifica as operações de TI, oferecendo às empresas acesso oportuno a serviços de segurança na nuvem, IaaS e SaaS.

A rede atual exige visibilidade, capacidade de programação e automação de ponta a ponta para garantir de forma dinâmica o desempenho, a segurança e a mais alta qualidade da experiência exigidos em ambientes multicloud. Uma WAN inteligente projetada com a melhor solução de SD-WAN da categoria e soluções de segurança na nuvem promove iniciativas de transformação digital e permite que as empresas evoluam e adotem inovações oportunas sem limitar a produtividade e o crescimento, tudo isso enquanto minimizam a exposição aos riscos de segurança.

CONCLUSÃO

À medida que as empresas modernas que priorizam a nuvem continuam migrando aplicativos do data center para a nuvem, elas precisam adotar a transformação da WAN e da segurança para alcançar o retorno máximo de seus investimentos em nuvem. A SASE, ou borda de serviço de acesso seguro, guia o setor nesta nova direção. Conforme mostra a Figura 5, é importante que as empresas levem em consideração a transformação da WAN e da segurança durante o projeto de uma borda de serviço de acesso seguro para viabilizar uma experiência otimizada.

Uma plataforma de SD-WAN avançada oferece conexão otimizada com diversos dos melhores serviços de segurança da nuvem da categoria, proporcionando o que há de melhor em arquitetura SASE. Em última análise, nenhum fornecedor de SASE terá a capacidade de oferecer as melhores tecnologias de segurança e rede da categoria em uma única plataforma. No cenário de ameaças em constante evolução, as empresas devem permanecer ágeis para adotar novas soluções de segurança de forma rápida e econômica. As empresas estão respaldadas para avaliar plataformas que oferecem a liberdade de escolha fundamental para integrar a melhor solução de SASE da categoria. Com isso, as empresas podem evitar ficar presas a soluções proprietárias de um único fornecedor ou ter que se contentar com capacidades e recursos básicos.

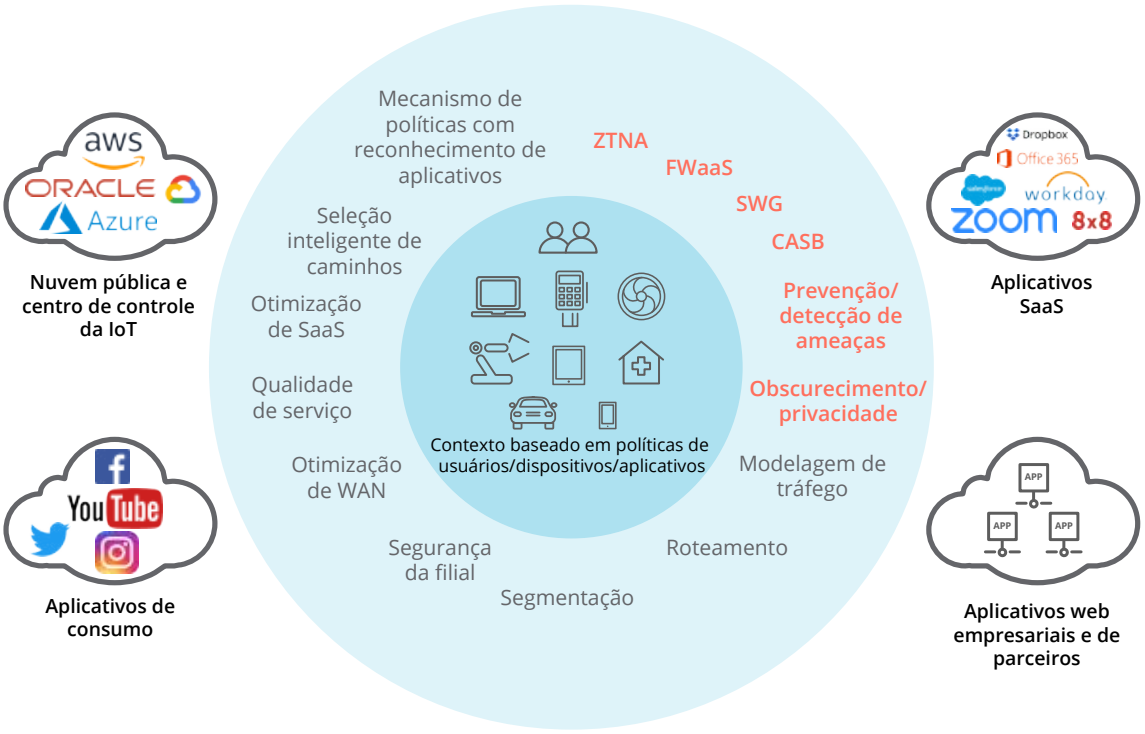

Figura 5: Uma borda de serviço de acesso seguro é necessária para oferecer suporte às iniciativas de transformação digital da empresa, isto é, necessidades de estratégia que prioriza a nuvem e mobilidade da força de trabalho. Em uma arquitetura de SASE robusta, os recursos abrangentes da WAN precisam funcionar em conjunto com as funções abrangentes de segurança de rede para oferecer suporte às necessidades dinâmicas de acesso seguro das empresas digitais para usuários, dispositivos e aplicativos.

Além disso, com a proliferação dos dispositivos IoT, a SASE precisa ser complementada com uma estrutura de segurança zero trust que segmenta dinamicamente o tráfego com base em identidades, para que os usuários e dispositivos IoT só consigam acessar os destinos da rede que sejam consistentes com sua respectiva função na empresa.

Uma SD-WAN avançada pode oferecer suporte às funções fundamentais de segurança necessárias na filial ao integrar um firewall de última geração com recursos de IDS/IPS, além de complementar a segurança na nuvem para proporcionar aplicação otimizada de políticas de segurança de ponta a ponta em toda a empresa. Isso permite que as empresas simplifiquem sua infraestrutura de rede com a oportunidade de fazer a transição para uma arquitetura de WAN moderna e segura que prioriza a nuvem em seu próprio ritmo, sem concessões.

Por fim, para empresas que não estejam prontas para aposentar os firewalls de filiais e migrar completamente para um modelo de segurança na nuvem, é importante encontrar uma plataforma de SD-WAN avançada que proporcione a liberdade de escolha para oferecer suporte à execução das principais soluções de software de gerenciamento unificado de ameaças (UTM) de terceiros como uma solução integrada em filiais. Isso elimina o custo adicional e a complexidade de gerenciamento que normalmente estariam envolvidos com o uso de firewalls dedicados separados, mas também oferece às empresas a flexibilidade para implantar as melhores soluções da categoria, oferecendo uma migração suave para um modelo de segurança na nuvem.

À medida que as empresas continuam realizando investimentos substanciais na nuvem, considerar os requisitos para transformação da WAN e da segurança vai colocá-las no caminho para oferecer a experiência da mais alta qualidade aos usuários enquanto enfrentam os desafios atuais de cibersegurança. Embarcar em uma jornada de transformação da WAN e da segurança fundamentada e sem concessões vai permitir que as empresas protejam seus ativos digitais e alcancem um efeito multiplicador de seus investimentos existentes e contínuos na nuvem.

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932ptl

Fale conosco em www.arubanetworks.com/contact