Oferecido por

Borda de serviço de acesso seguro (SASE)

para leigos

Edição especial da Cisco

Conheça as redes da SASE

Amplie a segurança nativa da nuvem em qualquer lugar

Reduza o custo e a complexidade

Lawrence Miller, CISSP

Sobre a Cisco

A Cisco projeta e vende linhas completas de produtos, presta serviços e oferece soluções integradas para desenvolver e conectar redes em todo o mundo, fortalecendo a Internet.

Como líder de mercado global em nosso setor, ajudamos nossos clientes a se conectarem, digitalizarem e serem bem-sucedidos. Juntos, mudamos a forma como as pessoas trabalham, vivem, se divertem e aprendem.

Há mais de 30 anos, ajudamos nossos clientes a construir redes, automatizar, orquestrar, integrar e digitalizar produtos e serviços baseados em tecnologia da informação (TI).

Em um mundo cada vez mais conectado, a Cisco está ajudando a abrir esse caminho, transformando empresas, governos e cidades em todo o mundo com inovação diferenciada.

Introdução à borda de serviço de acesso seguro (SASE)

umbrella.cisco.com/sase

Com todas as diferentes soluções de segurança (e siglas) disponíveis, como DNS, SIG, SWG, CASB, FWaaS, SASE, pode ser difícil determinar qual é a melhor abordagem, bem como quais são as tecnologias necessárias para reduzir a complexidade e melhorar a velocidade e agilidade, além de proteger a rede. Acesse nosso site para saber mais sobre a SASE e as providências que você pode começar a tomar para manter a empresa protegida.

 www.twitter.com/CiscoUmbrella

 www.facebook.com/CiscoUmbrella

 www.linkedin.com/company/OpenDNS

 www.youtube.com/c/CiscoUmbrella

Borda de serviço de acesso seguro (SASE)

Edição especial da Cisco

por Lawrence Miller, CISSP

for dummies®

Borda de serviço de acesso seguro (SASE) For Dummies®, edição especial da Cisco

Publicado por
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-73551-9 (pbk); ISBN 978-1-119-73685-1 (ebk)

Fabricado nos Estados Unidos da América

10 9 8 7 6 5 4 3 2 1

Créditos do editor

Estas são algumas das pessoas que ajudaram a lançar este livro no mercado:

Editora do projeto: Jennifer Bingham

Editor de aquisições: Ashley Coffey

Gerente editorial: Rev Mengle

Representante de desenvolvimento empresarial: Karen Hattan

Editor de produção: Umar Saleem

Ajuda especial: Rachel Ackerly, Lorraine Bellon, Robert Clarke, Josh DeButts, Tori Devereux, Meg Diaz, Barry Fisher, Kiran Ghodgaonkar, David Gormley, Rachel Haag, Kate MacLean, Jonny Noble, Iloyd Noronha, Natalie Pino, Nicole Smith, Christina Soriano e Cynthia Turner-De Vries

Índice

Introdução

As equipes de TI de hoje enfrentam um desafio comum: como habilitar com segurança o universo crescente de usuários móveis, dispositivos e aplicativos de software como serviço (SaaS), sem aumentar a complexidade ou reduzir o desempenho do usuário final; tudo isso enquanto aproveitam os investimentos em segurança atuais. Da mesma forma, os usuários de escritórios remotos e filiais precisam do mesmo nível de desempenho e segurança da rede que os usuários de locais centrais. A TI deve desenvolver estratégias para proteger os usuários - onde quer que trabalhem e em qualquer dispositivo que usem - contra uma variedade de ameaças, incluindo infecções por malware, retornos de chamada de comando e controle, ataques de phishing, acesso não autorizado e uso inaceitável, entre outras.

Este livro analisa o cenário dinâmico de rede e segurança, as lacunas na pilha de segurança atual e as etapas que você pode seguir para manter a empresa segura e protegida à medida que a rede evolui. Essas mudanças estão preparando o caminho para uma nova categoria de solução, que oferece várias funções de segurança na nuvem que são simples, escaláveis e flexíveis para atender às necessidades específicas da empresa e da arquitetura de rede em constante mudança.

O objetivo deste livro é ajudar você a entender as tendências mais recentes de rede e segurança, os desafios mais difíceis que essas mudanças trazem e como as tecnologias de rede e segurança evoluíram ao longo do tempo. Por fim, o livro apresenta uma nova categoria de produto que surgiu para ajudar a resolver esses problemas e como a abordagem da Cisco pode ajudar a empresa no presente e no futuro.

Sobre este livro

Este livro consiste em cinco capítulos que abordam:

- As principais tendências de rede e segurança e os desafios associados (Capítulo 1)
- Diferentes opções de rede e segurança e as principais considerações (Capítulo 2)
- Como uma arquitetura de SD-WAN lida com os desafios das redes modernas (Capítulo 3)

- Como um serviço de segurança multifuncional nativo da nuvem complementa a SD-WAN e lida com os desafios de segurança modernos (Capítulo 4)
- Os principais pontos de segurança da SD-WAN e da nuvem (Capítulo 5)

Cada capítulo foi escrito para ser independente, portanto, se você vir um tópico que desperte seu interesse, não hesite em avançar para esse capítulo. Você pode ler este livro na ordem em que achar adequada (mas não recomendamos que seja de cabeça para baixo ou de trás para a frente).

Hipóteses insensatas

O ditado diz que a maioria das hipóteses sobreviveram à sua inutilidade, mas vou mostrar algumas de qualquer forma.

Você tem formação técnica e trabalha para uma empresa que, como muitas, está procurando uma maneira melhor de gerenciar os desafios de rede e segurança em um empreendimento multicloud híbrido. Como tal, este livro foi escrito para leitores técnicos com uma compreensão geral dos conceitos de nuvem, rede e segurança.

Talvez você seja um executivo ou gerente de TI, como um diretor executivo da informação (CIO), diretor executivo de tecnologia (CTO) ou diretor executivo de segurança da informação (CISO), vice- presidente de TI, diretor de TI ou gerente de rede ou segurança. Ou talvez você seja um arquiteto ou engenheiro de nuvem, rede ou segurança.

Se você se encaixar em uma dessas descrições, esse livro é para você. Se você não se encaixar em nenhuma delas, leia mesmo assim. É um livro excelente e, quando terminar de ler, você saberá um pouco sobre a SD-WAN e a segurança da nuvem.

Ícones usados neste livro

Ao longo deste livro, você encontra ícones especiais para chamar a atenção para informações importantes. Você deve ver:

LEMBRE-SE

Este ícone indica as informações importantes que você deve ter na memória, massa cinzenta ou cachola, juntamente com datas comemorativas e aniversários.

MATERIAL TÉCNICO

Se você busca atingir o sétimo nível dos nerds, anime-se! Este ícone explica o jargão dentro de cada jargão e é disso que os nerds são feitos.

DICA

Dicas são bem-vindas, nunca esperadas. Espero que você goste dessas informações úteis.

AVISO

Esses alertas destacam os avisos dados por sua mãe (provavelmente não), mas oferecem conselhos práticos para ajudá-lo a evitar erros possivelmente caros ou frustrantes.

Além do livro

Nem todas as informações podem ser fornecidas nessas poucas 48 páginas, então, se no final do livro você pensar: "Nossa, que livro fantástico! Como posso saber mais?", acesse `https://umbrella.cisco.com/sase`.

NESTE CAPÍTULO

- Análise de como a rede e a segurança mudaram
- Resolução dos desafios modernos de rede e segurança

Capítulo 1
Redes e segurança: tendências e desafios

A rede corporativa passou por uma grande transformação na última década. Como resultado, os produtos de segurança também estão evoluindo. O mercado está migrando de produtos pontuais de finalidade única para soluções de segurança multifuncionais fortemente integradas em uma oferta de serviços em nuvem. O objetivo é simples: implantar serviços de segurança como e onde você escolher, com a capacidade de controlar e proteger o acesso direto à Internet, as aplicações em nuvem e a proteção para usuários centralizados, remotos e móveis, sem a necessidade de hardware adicional.

Este capítulo discute tendências e desafios modernos que determinam a necessidade de uma nova abordagem de rede e segurança.

Nossa forma de trabalho mudou

Várias tendências importantes evoluíram ao longo da última década para reformular o cenário de rede e segurança.

Adoção da nuvem

O uso de aplicativos e serviços em nuvem pública explodiu na última década. Todos os anos, as empresas produzem mais dados e cada vez mais esses dados estão sendo armazenados em aplicações de software como serviço (SaaS) na nuvem pública. O relatório de 2019 do Enterprise Strategy Group, *The Rise of Direct Internet Access*, projeta que 60% das empresas usarão aplicações de SaaS para mais da metade das necessidades comerciais nos próximos dois anos, em particular nas empresas altamente distribuídas.

DICA

O crescimento da adoção da nuvem corporativa é ainda mais evidenciado no relatório *RightScale State of the Cloud* de 2019 da Flexera, que constatou que a adoção da nuvem pública, incluindo SaaS e infraestrutura como serviço (IaaS), cresceu para 91% entre as empresas. Hoje, um terço das cargas de trabalho empresariais é executado em nuvens públicas e quase metade é executada em nuvens privadas (consulte a Figura 1-1).

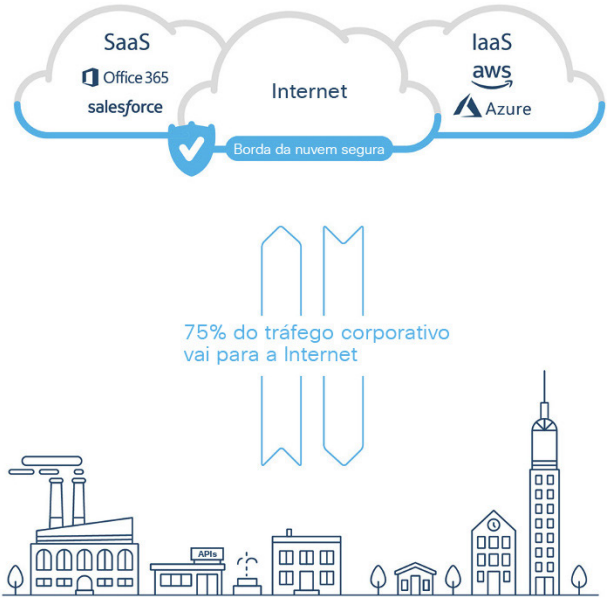


FIGURA 1-1: é essencial ter uma segurança eficaz para proteger o volume cada vez maior de Internet, aplicativos de SaaS e tráfego de IaaS em todos os locais.

Escritórios remotos

Os dias de funcionários que trabalham juntos no mesmo lugar, a sede da empresa, acabaram há muito tempo. À medida que as empresas se expandem para novos mercados, adquirindo empresas menores e ocupando o espaço dos escritórios, o número de escritórios remotos e filiais e também aumenta. Para as empresas de médio porte, os escritórios remotos ou satélites geram a maior parte da receita; a pesquisa do Enterprise Strategy Group sugere que 80% dos usuários estão localizados em escritórios remotos ou filiais. Esses usuários precisam ser protegidos, bem como suas contrapartes nos escritórios principais, mesmo que o tráfego de rede vá diretamente para a Internet, em vez de fazer backhaul para o data center corporativo.

LEMBRE-SE

Um escritório remoto ou filial é um local comercial dedicado (não residencial) com mais de um funcionário. Esse local pode ser conectado a um data center principal por meio de uma WAN ou pode ser conectado diretamente à Internet. Os escritórios remotos e filiais normalmente recebem algum nível de suporte de tecnologia das sedes, e a maioria (embora não todos) normalmente tem um ou mais servidores no local, para fornecer aos usuários serviços de arquivo, impressão e outros serviços de TI.

Alguns locais de escritórios remotos podem ser conectados a uma matriz através de um link de WAN de MPLS (Multiprotocol Label Switching). No entanto, está se tornando cada vez mais comum que os escritórios remotos sejam conectados ao escritório principal por uma rede VPN (Virtual Private Network) por meio de um link de DIA (Direct Internet Access) ou que tenham um link secundário de DIA para atuar como backup do link primário de MPLS.

DICA

À medida que as empresas se tornam mais descentralizadas, a crescente população de funcionários remotos e filiais precisa de uma nova abordagem de rede e segurança.

Usuários móveis

Os notebooks substituíram os desktops e se tornaram o dispositivo principal de muitos usuários corporativos. Da mesma forma, a computação móvel libertou os funcionários, à medida que os dispositivos móveis se tornaram mais eficazes do que muitos desktops e sua utilização se proliferou. Em virtude dessas tendências de tecnologia, agora a maior parte do trabalho pode ser realizada praticamente em qualquer lugar e as empresas modernas reconhecem cada vez mais que o trabalho é uma

atividade, não um lugar. De acordo com o Enterprise Strategy Group, 50% da força de trabalho será móvel até 2021 e um artigo da Forbes de fevereiro de 2019 observou que "O trabalho remoto não é mais um 'privilégio', 'estilo de vida' ou 'política'. Trabalho remoto, teletrabalho e flexibilidade no local de trabalho se tornaram oficialmente um setor global".

LEMBRE-SE

Um *usuário móvel* é qualquer funcionário que trabalhe em casa ou em outro local que não seja a empresa (como no escritório do cliente ou em trânsito) pelo menos um dia por semana. Os usuários móveis podem usar dispositivos corporativos e/ou pessoais e acessar a rede corporativa por meio de uma VPN ou se conectar diretamente à Internet para acessar aplicações em nuvem para desempenhar suas funções.

Mais tráfego de rede

Os novos aplicativos, incluindo armazenamento em nuvem pública e videoconferência, usam muitos dados e exigem grandes volumes de tráfego de rede para sustentar a crescente demanda dos funcionários. Esse aumento da carga de tráfego está sobrecarregando cada vez mais a infraestrutura de rede atual e os processos de segurança centralizada, resultando em baixo desempenho, menor produtividade e uma experiência do usuário geral insatisfatória.

Compreensão dos desafios de rede e segurança

Muitos novos desafios de rede e segurança também foram criados ao longo da última década, o que exige soluções inovadoras para resolvê-los com eficiência.

Aumento dos custos da arquitetura de rede tradicional

A função tradicional de uma WAN era conectar os usuários na filial ou no campus às aplicações hospedadas nos servidores em um data center centralizado. Normalmente, para garantir conectividade segura e confiável eram usados circuitos MPLS. No entanto, o provisionamento e a manutenção desses circuitos dedicados são caros, especialmente em comparação à disponibilidade generalizada de outras opções de DIA mais baratas para as empresas atualmente.

MATERIAL TÉCNICO

O MPLS é uma técnica de roteamento que usa rótulos de caminho virtual, em vez de endereços de endpoint de rede, para direcionar o tráfego através da rede, o que reduz a carga nos roteadores e acelera a distribuição de tráfego. O MPLS oferece uma qualidade de serviço (QoS) mais confiável para aplicações que consomem muita largura de banda ou são sensíveis à latência. As tecnologias de MPLS são aplicáveis a qualquer protocolo de camada de rede (daí o nome "multiprotocolo") e são muito usadas pelas empresas, por exemplo, para fazer o backhaul do tráfego de rede essencial para os negócios das filiais para o data center.

Ineficiências no modelo de rede centralizada

Um modelo de rede centralizada fazia sentido quando o data center corporativo era o principal destino para os usuários acessarem aplicações e dados na rede. O tráfego de Internet era relativamente insignificante e poderia ser facilmente gerido pelos circuitos de MPLS atuais. O tráfego de rede pode ser roteado e priorizado conforme necessário para garantir um desempenho eficiente e confiável, embora recursos limitados e caros da equipe de TI, como equipes de rede e segurança, possam gerenciar a rede de maneira centralizada em todos os locais.

Tradicionalmente, uma empresa fazia backhaul (ou seja, redirecionava) do tráfego de rede das filiais para a sede para aplicar políticas de segurança, geralmente usando links de MPLS. Mas, na era digital moderna, essa abordagem não é eficiente. À medida que as empresas adotam cada vez mais aplicações de SaaS, bem como recursos de plataforma como serviço (PaaS) e IaaS e cargas de trabalho distribuídas em várias nuvens, a experiência do usuário com as aplicações foi prejudicada. O backhaul do tráfego ligado à Internet em redes de MPLS criadas para oferecer acesso rápido e confiável ao data center é caro e pode ser lento. A verdade é que as redes de MPLS não são uma maneira eficiente ou eficaz de lidar com a explosão sem precedentes do tráfego de Internet causada pela adoção da nuvem.

MATERIAL TÉCNICO

O backhaul do tráfego destinado à Internet é feito efetivamente na rede de MPLS para um headend (como sede corporativa ou data center), que o direciona por meio de um conjunto de verificações de segurança e depois fornece acesso à Internet; porém, infelizmente, também atua como gargalo.

MATERIAL TÉCNICO

Os links de WAN atuais que usam MPLS não podem atender às demandas cada vez maiores de largura de banda dos usuários que precisam de acesso rápido e confiável à Internet para aumentar a produtividade. Para atender à necessidade cada vez maior de DIA (Direct Internet Access) para aplicações em nuvem, mais empresas (79% de acordo com o Enterprise Strategy Group) estão investigando ou já estão usando o DIA de banda larga nas filiais, em vez de fazer o backhaul do tráfego por meio do MPLS. Embora esses links de DIA resolvam os problemas de desempenho associados ao backhaul do tráfego para um local de headend de MPLS, eles geralmente são fornecidos por provedores de serviços de Internet (ISPs), como links de banda larga. É importante verificar as garantias de resiliência, priorização da qualidade de serviço (QoS) e contrato de nível de serviço (SLA).

Problemas de desempenho com aplicativos de SaaS de «administração de empresas»

Atualmente, muitos aplicativos de SaaS se tornaram os aplicativos corporativos principais de «administração de empresa». Alguns exemplos incluem Salesforce, Office 365 e Workday. O backhaul do tráfego de SaaS por meio de links caros de WAN de MPLS para um headend corporativo cria congestionamento e latência de rede. Isso, por sua vez, causa problemas de desempenho que resultam em perda de produtividade e frustração do usuário. A complexidade da WAN pode causar outros problemas de desempenho em virtude de decisões de roteamento abaixo do ideal, classificação e priorização de tráfego inadequadas e aplicação de política ineficiente.

Quando os usuários enfrentam problemas de desempenho com aplicativos aprovados pela empresa, geralmente eles recorrem a aplicativos não autorizados e possivelmente de risco para realizar o trabalho. Essa cultura de TI paralela na qual o departamento de TI e os controles de segurança são violados é um grande problema. Mais de 1.200 serviços em nuvem são usados hoje em dia nas empresas de grande porte, e o Enterprise Strategy Group informa que 98% desses serviços são aplicativos de SaaS não aprovados e não autorizados.

AVISO

Embora muitas empresas implementem políticas de segurança que exigem que usuários remotos ou móveis façam backhaul do tráfego de rede em túneis de VPN, 85% das empresas acreditam que os usuários violam essas políticas corporativas de VPN, de acordo com o Enterprise Strategy Group.

Muitas ferramentas de segurança não integradas e muitos desafios de integração

As equipes de segurança são constantemente bombardeadas por enormes volumes de dados de produtos de segurança independentes, que não são integrados a outros produtos e exigem diferentes níveis de conhecimento e conjuntos de habilidades para sua operação e manutenção. O Enterprise Strategy Group relata que 31% das empresas usam mais de 50 ferramentas diferentes e a pesquisa da Cisco indica que a maioria delas acha difícil orquestrar os alertas dessas ferramentas diversificadas. Essa falta de integração e interoperabilidade torna difícil, se não impossível, para os analistas de segurança monitorar e correlacionar informações de segurança e ameaças em tempo real.

LEMBRE-SE

Esses desafios aumentaram exponencialmente com a proliferação de filiais e escritórios remotos. Cada local normalmente requer, no mínimo, um roteador e firewall. Em locais remotos e filiais, muitas vezes, eles são adquiridos como componentes básicos que fornecem funcionalidade limitada e recursos de gerenciamento remoto. Ao migrar para o DIA em locais remotos, é necessário oferecer o nível certo de segurança para os usuários, como segurança da Web, firewalls, prevenção contra perda de dados etc. No entanto, é inviável comprar uma pilha separada de dispositivos de segurança para cada local. Mesmo que alguns desses componentes nas filiais incluam ferramentas de segurança, normalmente não há equipe de TI nesses locais para mantê-los. Com o tempo, o hardware não consegue suportar as cargas de tráfego cada vez maiores, então as ferramentas de segurança precisam ser transferidas desses dispositivos para a nuvem, onde podem ser aplicadas e gerenciadas de maneira centralizada.

DICA

Há uma luz no fim do túnel. De acordo com o estudo referencial do Cisco CISO, 93% dos CISOs concordam que a migração da segurança para a nuvem aumentou a eficiência, permitindo que as equipes de segurança se concentrem em outras áreas.

Escassez de talentos em segurança e aumento dos custos com pessoal

A escassez mundial de profissionais de segurança e o alto investimento contínuo necessário para treinar e manter equipes de segurança qualificadas são um problema muito real para empresas de todo o mundo. De acordo com a Cybersecurity Ventures, 3,5 milhões de empregos de

segurança cibernética em todo o mundo não serão preenchidos até 2021. O Enterprise Strategy Group e o ISSA relatam ainda que 74% dos entrevistados dizem que a escassez de funcionários qualificados em segurança cibernética teve um impacto significativo nas empresas.

Novas ameaças cibernéticas que se aproveitam das lacunas de segurança

As ameaças cibernéticas avançadas, incluindo ransomware, RATs (remote access trojans) e ameaças avançadas persistentes (APTs), evoluíram para aproveitar a falta de visibilidade e controle na rede distribuída moderna. Usuários remotos e de filiais são especificamente suscetíveis a muitas dessas ameaças porque as empresas se afastaram de um modelo de segurança centralizado e geralmente não conseguem aplicar políticas de segurança coerentes na rede. Recursos limitados de segurança e equipe de TI em locais remotos tornam esses usuários ainda mais suscetíveis a violações ou ataques bem-sucedidos. Os criminosos cibernéticos entendem que os funcionários remotos são normalmente mais vulneráveis e, portanto, visam locais remotos e usuários móveis.

AVISO

De acordo com o Enterprise Strategy Group, 68% das empresas sofreram ataques nos últimos 12 meses, nos quais uma filial ou usuário móvel foi o motivo do comprometimento.

DICA

As empresas modernas precisam considerar opções de rede e segurança inovadoras para resolver com sucesso os desafios de rede corporativa de hoje. Você pode encontrar mais informações sobre isso no Capítulo 2.

NESTE CAPÍTULO

- Reconhecimento das limitações de MPLS
- Inovação com a SD-WAN
- Resolução de ameaças de segurança com SWGs e SIGs
- Introdução à borda de serviço de acesso seguro (SASE)

Capítulo 2
A evolução das soluções de rede e segurança

O cenário de rede e segurança está evoluindo de várias soluções pontuais diferentes para plataformas de rede e segurança totalmente integradas, multifuncionais e fornecidas na nuvem.

Essa mudança está acontecendo porque as empresas precisam cada vez mais da flexibilidade e da capacidade de implantar serviços de rede e segurança como e onde quiserem. Elas precisam controlar e proteger o acesso à Internet, gerenciar o uso de aplicações em nuvem e fornecer proteção para usuários móveis, enquanto reduzem a pressão sobre os recursos e eliminam a necessidade de hardware.

Neste capítulo, você saberá como a rede e a segurança evoluíram da WAN tradicional para a SD-WAN e dos gateways de Web seguro (SWGs) para os gateways de Internet seguro (SIGs). Há também informações sobre o novo conceito combinado de borda de serviço de acesso seguro (SASE).

Análise das tecnologias tradicionais de WAN

Por quase duas décadas, a tecnologia de WAN imprescindível para infraestrutura de rede de TI, voz e dados tem sido as arquiteturas de rede de MPLS (Multiprotocol Label Switching). As redes de MPLS fornecem um backbone de rede resiliente para conectar sedes corporativas e filiais remotas. O MPLS oferece a capacidade de priorizar o tráfego de voz, vídeo e dados na rede para atender a requisitos comerciais específicos, e os pacotes podem ser enviados por uma rede de MPLS privada.

No entanto, atualmente, as empresas precisam de mais controle, flexibilidade e gerenciamento centralizado dos ambientes de WAN do que o MPLS pode oferecer, o que está gerando a necessidade de mudança. Os custos associados ao provisionamento e à manutenção dos links de WAN de MPLS privado podem ser um catalisador suficiente para a mudança. Normalmente, as redes de MPLS são fornecidas por provedores de serviços de Internet (ISPs) e outros provedores de serviços, tanto as empresas de telecomunicações reconhecidas quanto as empresas menores não muito reconhecidas.

Além disso, as ineficiências de uma rede de MPLS que faz o backhaul do tráfego associado à Internet nos links das filiais de um headend corporativo adicionam custo, complexidade, problemas de desempenho e latência. Muitas empresas instalam inevitavelmente um link secundário de DIA nas filiais para descarregar parte desse tráfego de Internet. Essa solução aumenta os custos recorrentes e introduz ainda mais complexidade. O tráfego de rede pode não ser necessariamente roteado pelo melhor link em determinado momento e a largura de banda em um link ou outro pode ser subutilizada.

Em relação à segurança, o tráfego associado à Internet precisa ser minimamente protegido pela segurança da camada DNS ou por um firewall, mas também pode exigir filtragem de conteúdo na Web, prevenção contra perda de dados, detecção de malware em tempo real e outros serviços de segurança. A falta de visibilidade e um ponto de aplicação de políticas centralizado tornam difícil, se não impossível, para as equipes de segurança garantir um ambiente operacional seguro e compatível (consulte a Figura 2-1).

FIGURA 2-1: os desafios das arquiteturas de WAN atuais incluem complexidade, custo, atrasos e interrupções.

Análise das soluções de SD-WAN

Configurar vários roteadores conectados a circuitos diferentes (por exemplo, um link de MPLS e um link de Internet de banda larga) para rotear o tráfego de rede de forma eficiente e ideal pode ser um desafio. Em muitos casos, você pode estar limitado a uma opção de balanceamento de carga simples, especialmente se você não tiver uma equipe de rede disponível em vários locais remotos.

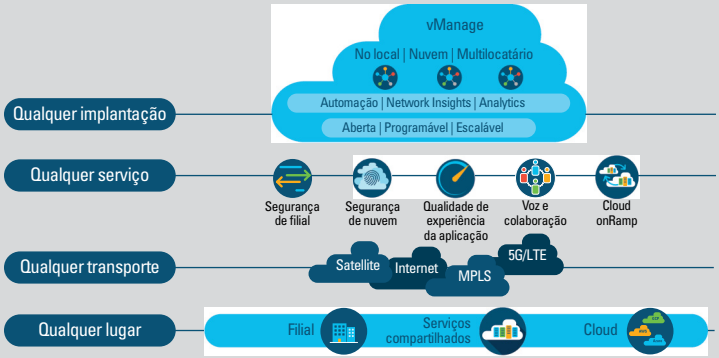
Além do balanceamento de carga simples, a capacidade de largura de banda disponível pode não ser usada durante períodos de congestionamento. Por exemplo, a conexão de Internet de banda larga pode estar funcionando lentamente durante determinado período, enquanto o link de MPLS caro está relativamente descongestionado e pode ser realmente capaz de fornecer conectividade mais rápida com a Internet. A incapacidade de agregar links diferentes significa desperdício de capacidade de largura de banda e menos satisfação do funcionário.

EXEMPLO DA CISCO SD-WAN

A Cisco SD-WAN é uma arquitetura segura com escalabilidade em nuvem, aberta, programável e escalável. Permite estabelecer rapidamente uma malha de sobreposição de SD-WAN para conectar data centers, filiais, campi e instalações de serviços compartilhados. Essa conexão pode melhorar a velocidade, segurança e eficiência da rede. A Cisco SD-WAN é compatível com (veja a figura abaixo):

- **Qualquer implantação:** gerenciamento de WAN flexível para ambientes locais, em nuvem e multilocatário.
- **Qualquer serviço:** um conjunto completo de serviços, incluindo segurança de filial, segurança da nuvem, qualidade de experiência da aplicação, voz e colaboração, e cloud on-ramp.
- **Qualquer transporte:** implante a WAN em qualquer tipo de conexão, inclusive satélite, Internet, MPLS e 5G/LTE.
- **Qualquer local:** plataformas físicas ou virtuais estão disponíveis para filial, serviços compartilhados e nuvem.

Arquitetura de SD-WAN com escalabilidade em nuvem segura



Fonte: Cisco.

DICA

Uma solução de SD-WAN pode resolver esses cenários e fornecer outros recursos avançados de roteamento para otimizar o tráfego de rede, conforme necessário. Os recursos e as considerações adicionais incluem:

- Roteamento de tráfego em links diferentes com base no destino
- Roteamento de tráfego em links diferentes com base no custo

- Agregação de vários links para oferecer maior largura de banda total
- Redirecionamento de tráfego em um link alternativo quando um link está congestionado, instável ou inativo
- Priorização de determinado tráfego de aplicações, como voz e vídeo, para garantir a qualidade de serviço

A SD-WAN combina e otimiza as tecnologias de WAN tradicionais, como MPLS e conexões de Internet de banda larga. Isso permite que as empresas roteiem com eficiência o tráfego de rede para vários locais remotos de filial, enquanto fornecem recursos avançados de monitoramento e gerenciamento. A SD-WAN monitora o tráfego de rede em todos os links disponíveis em tempo real e seleciona dinamicamente a melhor rota para cada pacote de dados que passa pela rede.

DICA

A International Data Corporation prevê que o mercado global de SD-WAN chegará a US$ 8 bilhões até 2021, e pesquisas da Forrester revelam que 64% das empresas norte-americanas estão planejando implementar a SD-WAN no próximo ano.

Combate às ameaças de segurança da Internet

Na maior parte dos últimos 25 anos, a segurança de rede se concentrou na detecção e prevenção de ameaças de malware (como vírus, ransomware, spam e phishing), identificação e bloqueio do uso não autorizado da Internet (como navegação em conteúdo inapropriado e download de conteúdo pirata) e garantia de desempenho da rede (com proxy de cache e produtos anti-DDoS).

LEMBRE-SE

Em 2017, vários fornecedores e analistas do setor definiram um novo conceito, o gateway de Internet seguro (SIG). Embora o SWG seja criado principalmente para tráfego na Web, esse novo tipo de solução nativa da nuvem oferece várias funções em mais tipos de tráfego, como segurança DNS, SWG, firewall como serviço (FWaaS) e agente de segurança de acesso à nuvem (CASB), para melhorar a segurança e o desempenho, reduzindo custos e tarefas de manutenção. Um SIG oferece um amplo conjunto de segurança da nuvem para que as empresas possam proteger os usuários, independentemente de onde estiverem. Pode ser facilmente dimensionado para abranger tráfego e usuários adicionais com mais eficiência do que a abordagem mais antiga do dispositivo de SWG local.

Aventurar-se com a SASE

Em 2019, a Gartner publicou um relatório chamado *The Future of Network Security Is in the Cloud*. Neste relatório, a Gartner apresentou o conceito de borda de serviço de acesso seguro (SASE). O conceito de SASE inclui um conjunto de funcionalidades de segurança ainda mais amplo do que um SIG, além da convergência da funcionalidade de rede. Uma solução de SASE pode proteger a nuvem, o data center e as bordas da rede de filial, bem como oferecer uma malha de SD-WAN segura em conexões diferentes (consulte a Figura 2-2).


DICA

No relatório *The Future of Network Security Is in the Cloud*, a Gartner compartilhou a previsão de que "em 2023, 20% das empresas terão adotado recursos de SWG, CASB, [acesso à rede zero trust] e FWaaS de filial do mesmo fornecedor, que foi menos de 5% em 2019".

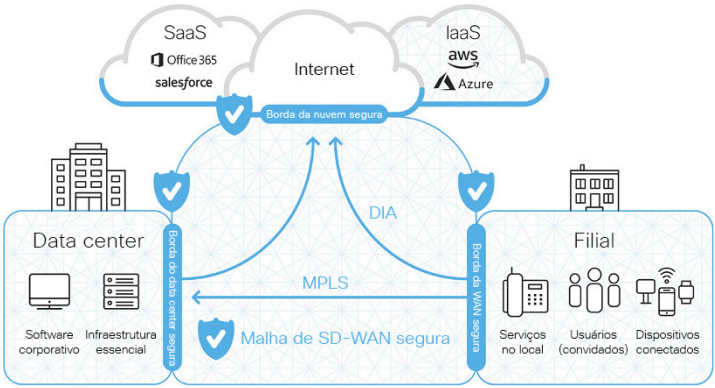


FIGURA 2-2: a SD-WAN é um elemento de rede essencial nas soluções de SASE que pode direcionar o tráfego para a proteção da nuvem, do data center e das redes de borda de filial.

NESTE CAPÍTULO

- Análise dos desafios de segurança na era da nuvem
- Reconhecimento das principais características e benefícios da SASE
- Introdução à SASE

Capítulo 3
SASE: combinação de segurança e funcionalidade de rede

Neste capítulo, você aprende sobre os desafios de segurança criados no novo modelo de arquitetura de rede, as funcionalidades necessárias em uma solução de segurança, os problemas que devem ser considerados ao implantar a solução e como uma solução de borda de serviço de acesso seguro (SASE) pode ajudar.

Reconhecimento dos desafios de segurança

A segurança de rede não está mais restrita ao data center, mas sim à nuvem. À medida que o trabalho sai do escritório e a segurança migra para a nuvem, o modelo de segurança baseado no perímetro já testado não consegue acompanhar o ritmo. Para obter sucesso, as equipes de TI precisam identificar uma nova abordagem para controlar e proteger usuários, aplicativos, dispositivos e dados, em todo e qualquer lugar.

Hoje, o uso em larga escala das aplicações em nuvem se tornou essencial para as operações comerciais em todos os locais. De acordo com a pesquisa do Enterprise Strategy Group, 32% das empresas relatam que agora a maioria dos aplicativos é baseada em software como serviço (SaaS) e esse número deve aumentar para 60% em dois anos. A

abordagem de segurança centralizada tornou-se inviável devido ao alto custo de backhaul do tráfego e aos problemas de desempenho resultantes das filiais.

Para superar esses problemas de custo e desempenho, muitas empresas estão adotando uma abordagem de rede mais descentralizada a fim de otimizar o desempenho em locais remotos. Isso permite um caminho de DIA (Direct Internet Access) mais eficiente para esses escritórios, mas também destaca um conjunto de novos desafios de segurança, incluindo:

- **Lacunas na visibilidade e na cobertura:** as políticas de segurança centralizada não podem ser gerenciadas e aplicadas de forma eficaz em uma rede descentralizada. Isso ocorre porque a maioria do tráfego das filiais para a nuvem e para a Internet não cruza um ponto centralizado de aplicação de políticas. Isso resulta em lacunas na visibilidade e na cobertura, o que aumenta o risco de uma violação bem-sucedida ou infração da conformidade.
- **Volume e complexidade das ferramentas de segurança:** as equipes de segurança já estão com dificuldades para acompanhar as ameaças de segurança cibernética. Muitas delas têm um grande número de soluções pontuais difíceis de integrar e gerenciar. Esses produtos pontuais geram milhares de alertas, tornando muito difícil, se não impossível, para os analistas acompanharem. Como resultado, muitos alertas permanecem intactos.
- **Orçamentos e recursos de segurança limitados:** os orçamentos de TI e de segurança já são restritos. A implantação de várias soluções de segurança pontuais e caras, como firewalls, gateways de Web seguros (SWGs), sistemas de detecção e prevenção contra invasão (IDS e IPS) e prevenção de perda de dados (DlP) para vários locais e o gerenciamento remoto dessas soluções com recursos de segurança limitados são inviáveis e ineficientes.

Principais características e benefícios da SASE

No relatório de agosto de 2019, *The Future of Network Security Is in the Cloud*, a Gartner definiu o conceito de borda de serviço de acesso seguro (SASE) como "uma oferta emergente que combina recursos abrangentes de [WAN] com funções abrangentes de segurança de rede (como SWG, [agente de segurança de acesso à nuvem], [firewall como serviço] e [acesso à rede zero trust]) para atender às necessidades dinâmicas de acesso seguro das empresas digitais".

Estas são quatro características principais das empresas submetidas à transformação digital que estão preparando o terreno para esse novo conceito:

- **Centrada em identidade:** a Gartner sugere que "a transformação digital das empresas inverte os padrões de design de serviços de rede e segurança, mudando o ponto focal para a identidade do usuário e/ou dispositivo, em vez do data center". Além disso, a "identidade do usuário/dispositivo/ serviço é uma das partes do contexto mais significativas que podem ser levadas em conta na política aplicada".
- **Nativa da nuvem:** a Gartner descreve as empresas digitais modernas como tendo "[m]ais dados confidenciais localizados fora do data center corporativo em serviços em nuvem do que dentro" e "[m]ais tráfego de usuários destinado para serviços em nuvem pública do que para o data center corporativo".
- **Computação de borda:** para apoiar o conceito de SASE, a Gartner descreve uma "estrutura/malha mundial de rede e recursos de segurança de rede que pode ser aplicada quando e onde necessário, para conectar entidades aos recursos de rede aos quais precisam acessar".
- **Distribuída mundialmente:** a Gartner descreve a necessidade de um "quadro de distribuição inteligente", em que as "identidades estão conectadas aos recursos de rede por meio da malha mundial de recursos de acesso seguro do fornecedor de SASE".

LEMBRE-SE

O conceito de SASE consolida diversos recursos e funções de rede e segurança, tradicionalmente fornecidos em várias soluções pontuais independentes, em uma única plataforma nativa da nuvem totalmente integrada.

Os possíveis benefícios comerciais do conceito de SASE incluem o seguinte:

- Reduzir o custo e a complexidade
- Ativar o acesso remoto e móvel seguro
- Fornecer roteamento baseado em políticas e otimizado para latência
- Melhorar o acesso contínuo e seguro para usuários
- Melhorar a segurança com políticas confiáveis
- Atualizar a proteção contra ameaças e as políticas, sem atualizações de hardware e software

- Restringir o acesso de acordo com a identidade do usuário, do dispositivo e da aplicação
- Aumentar a eficiência da rede e da equipe de segurança com gerenciamento centralizado de políticas

COMO A AVRIL ESTENDE A PROTEÇÃO PARA AS FILIAIS COM O CISCO UMBRELLA

Atualmente, o DIA permite que as filiais melhorem significativamente o desempenho da rede, eliminando a latência ao suprimir a necessidade de backhaul do tráfego para o data center. Mas, como resultado, o tráfego de Internet desses locais não é visto ou protegido pela pilha de segurança centralizada, o que pode deixar usuários e dados confidenciais expostos.

Para adotar o uso cada vez maior do DIA, as equipes de TI precisam de um serviço simplificado fornecido na nuvem, que unifique a eficácia de várias soluções de segurança pontuais em um único console. Essa solução é o Cisco Umbrella.

A Avril, um grupo agroindustrial francês, precisava fornecer às filiais uma solução de segurança confiável, que pudesse continuar crescendo à medida que a Avril adquirisse novas empresas e divisões. Para proteger esses locais e ainda oferecer um DIA rápido, eles precisavam de um serviço de segurança fornecido na nuvem, que pudesse funcionar nas bordas externas da rede, oferecendo uma linha de frente de proteção.

Ao usar a rede integrada e a arquitetura de segurança do Cisco Umbrella, a Avril pode proteger usuários de filiais, dispositivos conectados e uso de aplicativos em dezenas de milhares de breakouts de DIA. Aproveitando a segurança do Umbrella para estender a proteção a todos os lugares, a Avril conseguiu reduzir consideravelmente o risco de extração de dados e malware em todas as portas e protocolos. Simples de implantar e fácil de gerenciar na nuvem, o Umbrella também permite que a Avril continue expandindo a proteção para acompanhar as novas necessidades e o novo crescimento.

Com o Cisco Umbrella, a Avril Group conseguiu reduzir o ransomware em 100%, proteger usuários móveis que trabalham fora da rede e reduzir o tempo de gerenciamento de segurança em relação às soluções anteriores.

Marc Tournier, gerente de segurança da informação e conformidade (CISO) da Avril, ficou impressionado com o rápido retorno do investimento. "O Umbrella protegeu toda a rede da empresa em 10 minutos."

Esses benefícios são fundamentais para empresas que precisam resolver os desafios modernos de rede e segurança de uma força de trabalho cada vez mais voltada para a nuvem, móvel e global.

Início da jornada de SASE

SASE é um conceito geral. Para simplificar, você deve procurar uma maneira flexível de começar e fazer um progresso demonstrável em relação aos objetivos da empresa. Dito isso, os dois principais conceitos de SASE são a consolidação e a simplificação, por isso faz sentido traçar um curso que inclua elementos de rede e segurança de um único fornecedor. Há muitas vantagens técnicas, de custo e de desempenho do usuário final nesse tipo de abordagem combinada (consulte a Figura 3-1).

Fonte: Cisco

FIGURA 3-1: os benefícios de uma abordagem integrada de rede e segurança.

Pensando nesses benefícios combinados, faz sentido olhar para a primeira etapa lógica de rede e segurança.

Primeira etapa de rede

Comece analisando os muitos benefícios da SD-WAN e inicie uma avaliação para mostrar o impacto que ela pode ter nos custos dos serviços de rede, desempenho e tarefas de gerenciamento. Ao elaborar um plano de SD-WAN, você também deve decidir a melhor maneira de proteger os novos fluxos de tráfego, especialmente no número crescente de filiais remotas e usuários móveis. Procure um fornecedor com um portfólio sólido de tecnologia de rede, que ofereça uma ampla variedade de recursos de rede como serviço no futuro.

Primeira etapa de segurança

Procure uma solução nativa da nuvem que possa substituir com flexibilidade e até melhorar os recursos atuais da pilha de segurança. Procure uma solução que possa lidar com um amplo conjunto de tarefas de segurança e apresente dados em um único console, para ajudar a simplificar a implantação, as investigações e as tarefas de manutenção contínua.

AVISO

Não recrie os desafios resultantes das pilhas de segurança no local com um grande número de soluções pontuais separadas.

NESTE CAPÍTULO

- Saber o que procurar em uma solução de SASE
- Como a Cisco SD-WAN e o Cisco Umbrella atendem aos principais requisitos de SASE

Capítulo 4
Os componentes da SASE e a abordagem da Cisco

Neste capítulo, você aprende sobre os principais componentes a serem procurados em uma solução de borda de serviço de acesso seguro (SASE) e lê sobre um exemplo da abordagem que a Cisco está adotando para a convergência de segurança da nuvem e da rede.

Principais componentes da solução SASE

Veja os principais componentes que compõem uma solução de SASE. (Saiba mais sobre a SASE no Capítulo 3.)

SD-WAN

Uma SD-WAN é uma WAN virtual que permite às empresas usar qualquer combinação de serviços de transporte, incluindo MPLS, LTE celular e 5G, e banda larga, para conectar os usuários aos locais de rede com segurança. Ela pode selecionar o método de comunicação mais eficiente, reduzindo os custos e simplificando o gerenciamento.

Segurança da camada do sistema de nomes de domínio

A resolução DNS é a primeira etapa quando um usuário tenta acessar um site ou outro serviço na Internet. Portanto, aplicar a segurança nas camadas DNS e IP é a primeira linha de defesa contra ameaças e é uma ótima maneira de interromper ataques, antes que os usuários sejam conectados a destinos inadequados.

Gateway de Web seguro

Um proxy da Web na nuvem ou um gateway de Web seguro (SWG) oferece funções de segurança como detecção de malware, sandbox de arquivos e inteligência de ameaças dinâmica, descriptografia SSL, filtragem de conteúdo e aplicativo e prevenção de perda de dados (DLP).

Firewall como serviço

O firewall como serviço (FWaaS) é a funcionalidade de firewall entregue na nuvem para proteger o tráfego de Internet fora da Web. Normalmente, inclui visibilidade e controle das camadas 3 e 4 (IP, porta e protocolo), com as regras da camada 7 (controle de aplicações) e anonimização de IP.

Agente de segurança de acesso à nuvem

Os agentes de segurança de acesso à nuvem (CASBs) ajudam a controlar e proteger o uso de software como serviço (SaaS) na nuvem. As soluções de CASB permitem que as empresas apliquem as políticas de segurança interna e os regulamentos de conformidade. O valor dos CASBs é derivado da capacidade de fornecer informações sobre o uso de aplicações na nuvem em todas as plataformas de nuvem e de identificar o uso não autorizado. Os CASBs usam a descoberta automática para detectar as aplicações na nuvem em uso e identificar aplicações e usuários de alto risco, além de outros fatores de risco importantes. Eles normalmente incluem a funcionalidade de DLP e a capacidade de detectar e fornecer alertas quando ocorre uma atividade anormal do usuário, para ajudar a interromper ameaças internas e externas.

Acesso à rede Zero Trust

A estrutura de segurança Zero Trust da Forrester adota a abordagem de segurança de "confiar nunca, verificar sempre". O acesso à rede Zero Trust (ZTNA) verifica a identidade do usuário e estabelece a confiança do dispositivo, antes de conceder acesso às aplicações autorizadas, ajudando as empresas a evitar o acesso não autorizado, conter violações e limitar o movimento lateral de um invasor na rede. O ZTNA requer uma abordagem de autenticação multifatorial baseada em nuvem forte.

Abordagem da Cisco para a SASE

A Cisco oferece os principais recursos de SASE, bem como funcionalidades adicionais por meio de vários componentes principais de rede e segurança.

Cisco SD-WAN: rede flexível gerenciada em nuvem

A abordagem da Cisco para a SASE aproveita uma arquitetura de SD-WAN em nuvem (consulte a Figura 4-1) criada para atender às necessidades complexas das WANs modernas em três áreas principais:

- Otimização avançada de aplicações, que oferece uma experiência da aplicação previsível, à medida que a estratégia de aplicações comerciais evolui
- Segurança multicamada, que oferece a flexibilidade de implantar a segurança certa no lugar certo, seja no local ou na nuvem
- Simplicidade em escala empresarial, que permite políticas de ponta a ponta, do usuário à aplicação, em milhares de sites

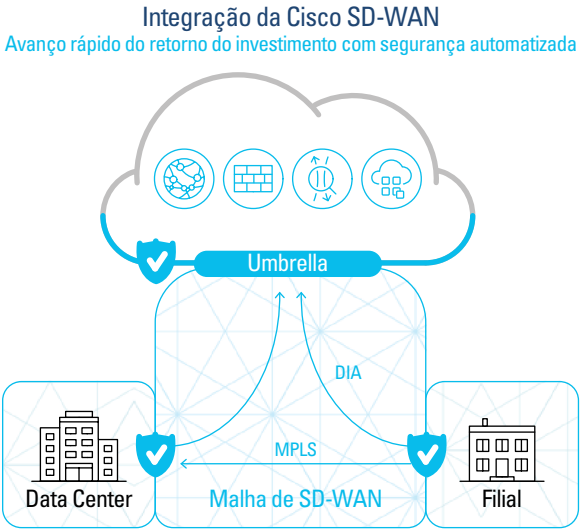


FIGURA 4-1: a arquitetura em nuvem da Cisco SD-WAN.

A solução Cisco SD-WAN contém os seguintes quatro componentes principais, que trabalham juntos para formar a malha da Cisco SD-WAN (consulte a Figura 4-2):

- **Cisco vManage** (plano de gerenciamento)
- **Cisco vBond** (plano de orquestração)
- **Cisco vSmart** (plano de controle)
- **Roteadores Cisco WAN Edge** (malha de rede)

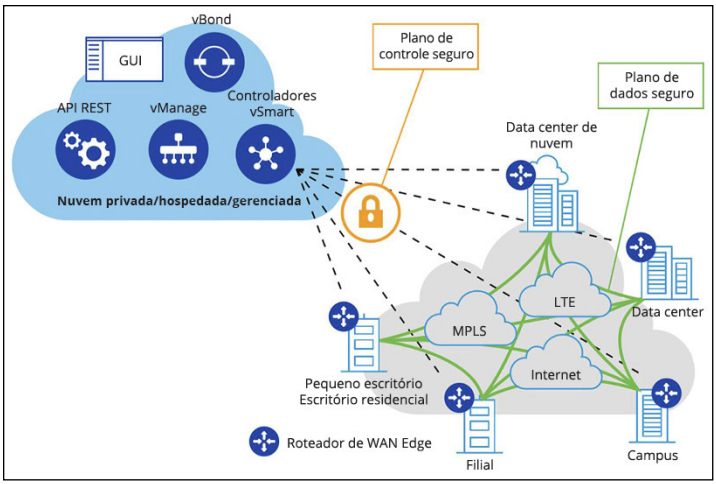


FIGURA 4-2: integração da Cisco SD-WAN.

Cisco Umbrella: segurança multifuncional nativa da nuvem

O Cisco Umbrella é um serviço de segurança em nuvem que oferece uma experiência de Internet segura, confiável e rápida. Ao unificar várias funções de segurança em um único serviço, o Umbrella ajuda empresas de todos os portes a adotar o DIA, proteger as aplicações em nuvem e estender a proteção a usuários móveis e filiais.

LEMBRE-SE

Ao ativar essas funções combinadas, em vez de soluções pontuais, o Umbrella reduz consideravelmente o tempo, o custo e os recursos normalmente necessários para implantação, configuração, integração e gerenciamento de uma pilha de produtos de segurança independentes.

O Cisco Umbrella oferece um conjunto principal de funções de segurança em um console na nuvem (consulte a Figura 4-3):

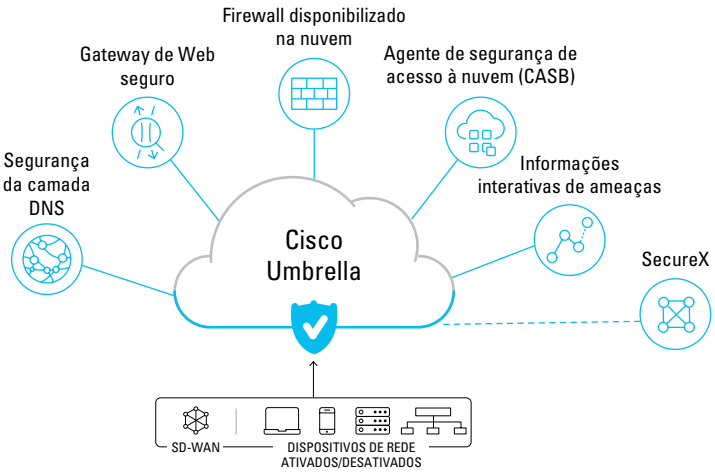


FIGURE 4-3: Cisco Umbrella delivers SASE security capabilities and more.

FIGURA 4-3: o Cisco Umbrella oferece recursos de segurança de SASE e muito mais.

Segurança da camada DNS

O Umbrella bloqueia as solicitações de destinos mal-intencionados e indesejados antes que uma conexão seja estabelecida, interrompendo ameaças por qualquer porta ou protocolo antes que atinjam a rede ou os endpoints. Como um serviço oferecido na nuvem, o Umbrella:

- Fornece a visibilidade necessária para proteger o acesso à Internet em todos os dispositivos de rede, escritórios e usuários remotos
- Registra e categoriza a atividade do DNS por tipo de ameaça à segurança ou conteúdo da Web e as ações tomadas, independentemente de ter sido bloqueada ou permitida
- Pode ser implementado rapidamente para abranger milhares de locais e usuários em minutos, proporcionando um imediato retorno sobre o investimento

Gateway de Web seguro (SWG)

O Cisco Umbrella inclui um proxy na nuvem que pode registrar e inspecionar todo o tráfego da Web para obter maior transparência, controle e proteção. como:

- Inspeção em tempo real dos arquivos de entrada em busca de malware e outras ameaças, usando o mecanismo Cisco Advanced Malware Protection (AMP) e recursos de terceiros
- Sandbox avançado de arquivos fornecido pelo Cisco Threat Grid
- Descriptografia de SSL completa ou seletiva para proteger ainda mais contra ataques ocultos
- Bloqueio de atividades específicas do usuário em aplicativos específicos (por exemplo, uploads de arquivos, anexos e publicações/compartilhamentos)
- Filtragem de conteúdo por categoria ou URls (uniform resource locators) específicos para bloquear destinos que violam políticas ou regras de conformidade

MATERIAL TÉCNICO

Túneis IPsec, agentes do AnyConnect, arquivos de PAC e encadeamento de proxy podem ser usados para encaminhar o tráfego da Web para o Cisco Umbrella.

Firewall disponibilizado na nuvem

Com o firewall do Cisco Umbrella, todas as atividades são registradas e o tráfego indesejado é bloqueado usando as regras de IP, porta e protocolo. Para encaminhar o tráfego, basta configurar um túnel IPsec em qualquer dispositivo de rede. O gerenciamento é feito pelo painel do Umbrella e, à medida que novos túneis são criados, as políticas de segurança podem ser aplicadas automaticamente para facilitar a configuração e garantir a aplicação uniforme em todo o ambiente.

O firewall disponibilizado na nuvem do Cisco Umbrella oferece:

- Visibilidade e controle do tráfego da Internet em todas as portas e protocolos
- Políticas personalizáveis de IP, porta e protocolo no painel do Umbrella
- Visibilidade e controle de aplicações da camada 7

Funcionalidade do agente de segurança de acesso à nuvem (CASB)

O Cisco Umbrella expõe a TI invisível ao fornecer o recurso para detectar e gerar relatórios sobre as aplicações em nuvem usadas em todo o ambiente. O Umbrella App Discovery oferece:

- Maior visibilidade dos aplicativos de nuvem em uso e volume de tráfego
- Detalhes do aplicativo e informações de risco
- Capacidade de bloquear/permitir aplicativos específicos

DICA

As informações do CASB permitem um melhor gerenciamento da adoção da nuvem, a redução de riscos e a capacidade de bloquear o uso de aplicações em nuvem ofensivas ou inadequadas no ambiente de trabalho.

Inteligência de ameaças interativa

O Cisco Umbrella analisa mais de 200 bilhões de solicitações de DNS diariamente, retiradas da rede global da Cisco em um grande banco de dados de gráficos. Também funciona continuamente com modelos estatísticos e de aprendizado de máquina. Essas informações são constantemente analisadas por pesquisadores de segurança do Umbrella e complementadas com a inteligência do Cisco Talos para descobrir e bloquear com eficiência uma vasta gama de ameaças. O Umbrella é alimentado por essa inteligência de ameaças e a Cisco oferece acesso a esses dados para acelerar a detecção e a resposta a ameaças.

Os analistas podem aproveitar o Umbrella Investigate para obter inteligência avançada sobre domínios, IPs e malware na Internet. O Investigate oferece:

- Ampla visibilidade das ameaças atuais e futuras
- Melhor priorização das investigações de incidentes
- Investigações e resposta a incidentes mais rápidas

DICA

A visão da Internet exclusiva da Cisco permite que o Umbrella descubra domínios, IPs e URLs mal-intencionados antes que sejam usados em ataques e ajuda os analistas a acelerar as investigações.

Integração de Umbrella e SD-WAN

Com a integração do Cisco Umbrella e da Cisco SD-WAN, você pode implantar o Umbrella em toda a rede e obter segurança avançada na nuvem para proteger contra ameaças na Internet. O Umbrella oferece a flexibilidade de criar políticas de segurança com base no nível de visibilidade e proteção que você precisa, tudo em um único painel.


DICA

Para obter segurança da camada DNS, o Umbrella pode ser implantado em centenas de dispositivos com uma única configuração no painel da Cisco SD-WAN vManage. Para obter segurança adicional e controles mais granulares, os recursos de firewall e SWG do Umbrella podem ser implantados por meio de um único túnel IPsec. A Cisco abriu novos caminhos na automação, conexão e implantação dos túneis que conectam o tráfego de SD-WAN a serviços de segurança na nuvem. Essa abordagem integrada protege com eficiência os usuários das filiais, os dispositivos conectados e o uso de aplicações contra todas as invasões do DIA.

Cisco SecureX

A plataforma Cisco SecureX conecta a amplitude do portfólio de segurança integrado da Cisco e as ferramentas adicionais de terceiros para proporcionar uma experiência confiável e simplificada, a fim de unificar a visibilidade, viabilizar a automação e reforçar a segurança. Ela agrega os dados do AMP for Endpoints, Umbrella, SWE, SWC, ESA/WSA por meio de SMA, NGFW Eventing por meio de SSE, Orbital, Threat Grid, Duo, CDO e Tetration para melhorar a inteligência e agilizar o tempo de resposta.

Você pode visualizar imediatamente a ameaça e seu impacto organizacional, além de obter um veredicto resumido para as observações que você está investigando por meio de um gráfico de relações visualmente intuitivo. Ela permite fazer a triagem, priorizar, rastrear e responder a alertas de alta fidelidade por meio do Gerenciador de incidentes integrado. Em seguida, você pode executar ações de resposta rápida em vários produtos de segurança: isolar hosts, bloquear arquivos e domínios e bloquear IPs; tudo isso em uma interface prática (consulte a Figura 4-4).

O SecureX capacita as equipes do centro de operações de segurança (SOC) com um único console para correção direta, o acesso à inteligência de ameaças e as ferramentas, como o livro de casos e o gerenciador de incidentes. Isso supera muitos desafios, tornando as investigações de ameaças mais rápidas, mais simples e mais eficientes.

FIGURA 4-4: o Cisco SecureX simplifica a segurança com melhor visibilidade e automação.

Zero Trust com Cisco Duo

Para empresas de todos os portes que precisam proteger dados confidenciais em escala, a solução de acesso confiável do Cisco Duo é uma plataforma de segurança Zero Trust centrada no usuário para todos os usuários, dispositivos e aplicações. A autenticação multifatorial (MFA) do Duo permite verificar a identidade de todos os usuários, antes de conceder acesso a aplicações corporativas. Você também pode garantir que os dispositivos atendam aos padrões de segurança, desenvolver e gerenciar políticas de acesso e simplificar o acesso remoto e o logon único (SSO) para aplicações corporativas.

Benefícios combinados exclusivos para a Cisco

Aproveitando insights do Cisco Talos, uma das maiores equipes comerciais de inteligência de ameaças do mundo, com mais de 300 pesquisadores, o Umbrella descobre e bloqueia um amplo espectro de domínios, IPs, URLs e arquivos mal-intencionados que estão sendo usados em ataques. Além disso, o Cisco Umbrella alimenta grandes volumes de atividades globais na Internet (mais de 200 bilhões de solicitações por dia) em uma combinação de modelos estatísticos e de aprendizado de máquina para identificar novos ataques que estão sendo preparados na Internet.

O Umbrella tem uma infraestrutura de nuvem altamente resiliente que possui quase 100% de tempo de atividade desde 2006. Usando o roteamento Anycast, qualquer um dos mais de 30 data centers da Cisco em todo o mundo está disponível com o mesmo endereço IP único. Como resultado, as solicitações são enviadas de forma transparente para o data center mais próximo e mais rápido, e o failover é automático. O Umbrella oferece pares com mais de 900 dos principais ISPs, CDNs e plataformas de SaaS para oferecer o caminho mais rápido para qualquer solicitação, o que resulta em velocidade superior, segurança eficaz e excelente experiência do usuário.

DICA

Para obter mais informações sobre a solução de SASE do Cisco Umbrella, acesse `https://umbrella.cisco.com/sase`.

NESTE CAPÍTULO

- Reconhecimento da natureza dinâmica do trabalho e da rede
- Tratamento de aplicativos e serviços em nuvem
- Como resolver as ameaças modernas e atrair e reter os principais talentos de segurança
- Introdução à SASE

Capítulo 5
Dez pontos principais

Estes são os dez pontos principais que devem ser levados em conta sobre a SD-WAN e a segurança da nuvem.

Mais escritórios remotos e usuários móveis

O número de usuários de escritórios remotos, dispositivos móveis e roaming está aumentando e, muitas vezes, esses usuários são alguns dos alvos mais suscetíveis a invasores. As oportunidades de erros, como clicar em um link de e-mail mal-intencionado ou visitar um site mal-intencionado, também estão aumentando. Como esses usuários remotos e móveis podem não ter acesso a um recurso de TI local, podem ser menos propensos a entrar em contato com o suporte técnico ou com a equipe de segurança quando surgir um problema.

Da mesma forma, os usuários móveis geralmente não pensam duas vezes antes de se conectarem a um hotspot de Wi-Fi público. Os criminosos cibernéticos aproveitam todas as oportunidades de explorar as vulnerabilidades de Wi-Fi e a confiança inerente que um cliente da lanchonete ou um hóspede de hotel coloca em uma conexão Wi-Fi «segura».

DIA é o novo normal

Com o advento da era da nuvem, as arquiteturas de rede criadas para fornecer conectividade robusta a um data center corporativo agora estão obsoletas e devem evoluir. Atualmente, a maior parte do tráfego de rede ocorre dentro do próprio data center (tráfego de leste a oeste) ou de vários locais de uma empresa para a nuvem pela Internet (tráfego de norte a sul). Como resultado, o backhaul do tráfego de rede de locais remotos ou de filial nos links de WAN de MPLS ou do tráfego de usuários móveis em conexões de VPN não é mais uma opção eficiente ou viável. As empresas estão cada vez mais oferecendo links de banda larga de DIA para os usuários remotos, de filial e móveis para acessar as aplicações de software como serviço (SaaS) sem o baixo desempenho e latência associados ao backhaul do tráfego em um escritório corporativo com uma única pilha de segurança.

Os aplicativos de SaaS estão assumindo o controle

Antes limitados aos aplicativos pessoais que os funcionários baixavam nos smartphones, agora os aplicativos de SaaS se tornaram aplicativos corporativos principais compatíveis com funções comerciais essenciais no ambiente de trabalho digital moderno. O Salesforce permite o gerenciamento do relacionamento com o cliente (CRM), o Workday oferece serviços de folha de pagamento e o Concur fornece o gerenciamento de despesas. Outros aplicativos, como o Office 365, fornecem e-mail e colaboração, e outros aplicativos, como Box, Dropbox, Google Drive e OneDrive, oferecem gerenciamento e armazenamento de arquivos.

Obviamente, parte do atrativo dos aplicativos de SaaS é a facilidade de uso. Para oferecer essa prática experiência do usuário, muitos aplicativos de SaaS fornecem apenas mecanismos fracos de controle de acesso e segurança, ou nem fornecem. Outros têm segurança e controle de acesso robustos, mas às custas da praticidade.

Uma solução de segurança multifuncional nativa da nuvem pode fornecer serviços de agente de segurança de acesso à nuvem (CASB) para garantir que políticas de controle de acesso e segurança robustas e confiáveis sejam aplicadas a todos os aplicativos, por exemplo, ao ativar o login único (SSO) e a inteligência de ameaças integrada.

A antiga forma da rede é lenta e cara

Os onerosos links de WAN de MPLS que conectam filiais remotas e fazem o backhaul de todo o tráfego para um headend corporativo são ineficientes e apresentam problemas de complexidade, desempenho e satisfação do usuário.

A arquitetura de rede atende às novas demandas

A SD-WAN como solução de rede independente é excelente para resolver os desafios da rede corporativa, especialmente em locais remotos e filiais. A SD-WAN permite que as empresas configurem novos locais com rapidez, sem precisar esperar semanas ou meses para provisionar novos links de WAN de MPLS. Em vez disso, um provedor de serviços de Internet (ISP) local pode fornecer um link de DIA, geralmente em apenas alguns dias.

Mas a agilidade e a simplicidade apresentam novos desafios para as equipes de segurança corporativa. Na pressa de se conectar, a segurança pode ser uma consideração tardia para a empresa. Quando a conexão com a Internet estiver ativa, a empresa estará pronta para funcionar, com ou sem segurança. E se a solução de SD-WAN não tiver recursos de segurança integrados, a equipe de segurança pode precisar enviar um firewall separado e/ou outros dispositivos de segurança para o escritório remoto. Conectar um dispositivo não tem problema, mas dois ou três já é pedir demais.

Procurar uma solução que reduza os custos e a complexidade

Em um passado não muito distante, as equipes de segurança corporativa implantaram rotineiramente as melhores soluções de segurança pontual de diferentes fornecedores para atender às necessidades de uma única finalidade: firewalls, gateways de Web seguros (SWGs), IDS e IPS, filtragem de conteúdo da Web, segurança DNS, prevenção de perda de dados (DLP), prevenção contra DDoS e proteção contra malware, para citar apenas alguns. Esses produtos autônomos têm sistemas operacionais e consoles de gerenciamento diferentes e

normalmente oferecem integração limitada (se houver) a outros produtos de segurança.

Infelizmente, na busca de uma estratégia de "defesa detalhada", muitas empresas acabam tendo uma "defesa ad nauseam", pois essas várias ferramentas de segurança não integradas aumentam a complexidade e criam problemas de desempenho na rede.

Não comprometer o desempenho da rede

Em última análise, a experiência do usuário é o que impulsiona a adoção bem-sucedida de iniciativas de transformação digital em uma empresa. O desempenho insatisfatório da rede garante uma experiência do usuário insatisfatória e leva os funcionários frustrados a recorrer a aplicativos e soluções de TI invisível possivelmente de risco.

Garanta que a plataforma de rede e segurança ofereça o desempenho (e segurança) de que seus usuários precisam para manter a produtividade, estejam eles na sede, em escritórios remotos ou filiais ou em trânsito em um dispositivo móvel.

Manter sempre a segurança em primeiro plano

As ameaças cibernéticas estão se tornando mais avançadas e os invasores estão usando novas técnicas para explorar vulnerabilidades e invadir redes específicas. Os e-mails de phishing, que antes eram facilmente identificáveis por erros ortográficos e gramaticais, tornaram-se muito mais difíceis de detectar. O ransomware também ficou muito mais comum, onde o ransomware como serviço (RaaS) torna fácil para praticamente qualquer pessoa iniciar um ataque. E essas estão entre as ameaças menos sofisticadas atualmente. O crime organizado e os estados-nação lançam ataques muito mais avançados, com vastos recursos que podem levar anos para serem detectados e erradicados.

Facilitar a vida da equipe de operações

A escassez mundial de profissionais de segurança qualificados é uma tendência que continuará no futuro próximo. A boa notícia para os profissionais de segurança é que haverá empregos bem pagos nos próximos anos. A má notícia é que o trabalho já árduo de proteger uma rede corporativa está ficando cada vez mais difícil, à medida que as ameaças estão cada vez mais avançadas, e a proliferação de ferramentas de segurança não integradas exige conhecimento e experiência especializados, que precisam ser atualizados e reciclados continuamente.

Atraia e retenha os melhores talentos com a implementação de soluções inovadoras de rede e segurança, que integram funcionalidade em uma única plataforma na nuvem e facilitam a vida de toda a equipe de operações.

Cada jornada começa com um único passo

Com o Cisco Umbrella, você pode começar devagar com a segurança da camada DNS e desenvolver recursos adicionais a partir daí, já que a empresa está pronta.

Uma solução de segurança nativa da nuvem e SD-WAN totalmente integrada pode ajudar as empresas a enfrentar os desafios de rede e segurança da era da computação em nuvem e móvel. Esses produtos de borda de serviço de acesso seguro (SASE) oferecem funcionalidade avançada de rede e segurança em um único painel, permitindo que as equipes de rede e segurança da empresa desenvolvam as redes com a confiança e a agilidade que as empresas modernas exigem.

DICA

Saiba mais sobre a abordagem da Cisco para a SASE em `https://umbrella.cisco.com/sase`.

Observações

Observações

Observações

Observações

Descubra a segurança multifuncional nativa da nuvem

As redes corporativas estão passando por uma transformação significativa. O tráfego da Internet nas filiais foi tradicionalmente encaminhado para um local central em que as funções de segurança são realizadas. Atualmente, as aplicações em nuvem essenciais para os negócios tornam impraticável fazer o backhaul do tráfego nas filiais devido a problemas de custo e desempenho. As empresas precisam de uma solução de rede e segurança totalmente integrada criada para a nuvem. Neste livro, você aprende como a SASE resolve os desafios modernos de rede e segurança.

Dentro...

- Utilizar recursos de SD-WAN
- Otimizar o desempenho da rede de borda
- Proteger o acesso remoto e móvel
- Simplificar o gerenciamento de rede e segurança
- Consumir funções de segurança como serviço
- Acessar a inteligência de ameaças interativa
- Implementar acesso de rede Zero Trust

Lawrence Miller atuou como Primeiro-sargento da Marinha dos EUA e trabalha em tecnologia da informação em vários setores há mais de 25 anos. Ele é coautor de CISSP For Dummies e escreveu mais de 150 livros For Dummies sobre inúmeros temas de tecnologia e segurança.

Acesse Dummies.com®
para ver vídeos, fotos passo a passo, artigos how-to ou para fazer compras!

ISBN: 978-1-119-73551-9
Não destinado à revenda

para leigos®

Também disponível como e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.