Cloud Secure Edge

Acesso remoto, segurança aprimorada

O Cloud Secure Edge™ da SonicWall, antes conhecida como Banyan Security, é uma solução de Security Service Edge (SSE) altamente eficaz e facilmente adotável, que possibilita que seus profissionais acessem com segurança qualquer recurso, de qualquer dispositivo. O sistema permite o acesso simples, seguro e com Zero-trust a recursos privativos e via internet, para todos os seus funcionários e terceirizados, não importa onde se localize a rede em que estão trabalhando. É uma combinação da funcionalidade de múltiplos appliances tradicionais em rede – VPN para acesso remoto, proxy de internet, firewalls, entre outras – em uma solução unificada em nuvem, que melhora a postura de segurança e a experiência de todos os usuários.

Observação: Clientes com firewalls da Gen 7 da SonicWall já implementados podem conectá-los ao Cloud Secure Edge fora da caixa, e gerenciar políticas de acesso por meio de um painel de controle unificado.

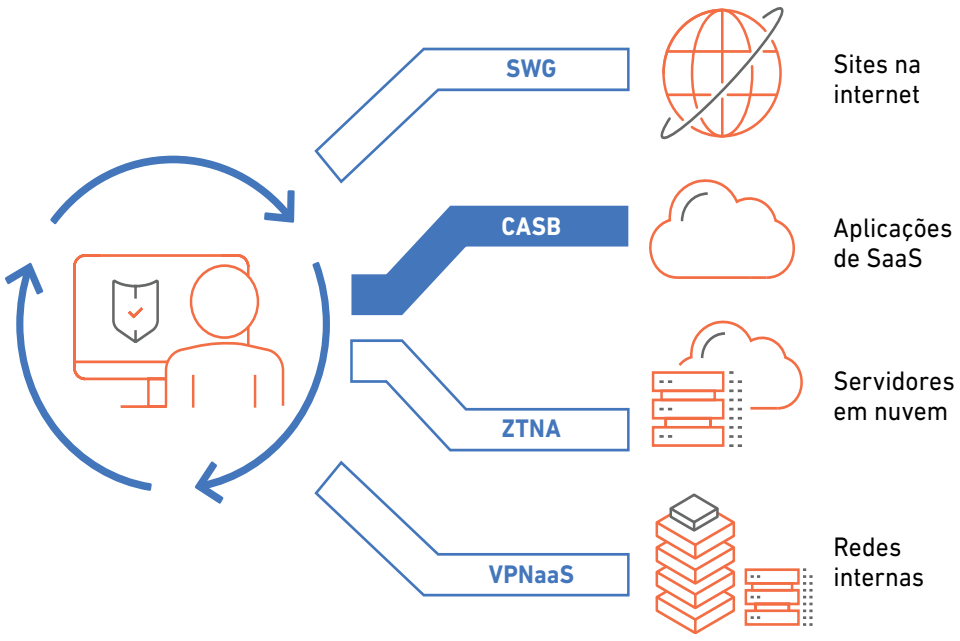

Figura 1: Cloud Secure Edge da SonicWall, proteção do acesso a qualquer recurso, a partir de qualquer dispositivo

DATASHEET

Por que o Cloud Secure Edge da SonicWall?

FÁCIL DE IMPLEMENTAR E GERENCIAR

O Cloud Secure Edge pode ser autônomo ou adicionado aos seus firewalls da Gen 7 da SonicWall já instalados, na modalidade de assinatura mensal. É ideal para MSPs e organizações do tipo DIY com recursos muito sobrecarregados que estejam em busca de um RSI rápido e com baixo custo de manutenção.

PROTEJA-SE CONTRA AS AMEAÇAS MODERNAS

O Cloud Secure inclui controles de segurança Zero-trust, necessários para profissionais que atuam com trabalho híbrido e remoto e que precisam ter acesso a ativos sigilosos e privativos via internet e que precisam trabalhar de qualquer lugar. O sistema emprega uma tecnologia exclusiva baseada em uma pontuação de confiança nos dispositivos, centrada na identidade e criptografia fungível, para oferecer uma segurança líder no setor e uma excelente experiência aos usuários.

DESEMPENHO COM PRIVACIDADE

O Cloud Secure Edge foi desenvolvido de baixo para cima, de forma a oferecer um alto desempenho, ao mesmo tempo assegurando a privacidade. Os administradores têm o controle integral de seus dados, ao mesmo tempo certificando-se de que os usuários terão a conexão mais neutra e eficiente possível, e o nível máximo de produtividade, proteção de dados e privacidade.

Estudos de casos comuns

Modernize a VPN/FW com ZTNA

Em vez de depender de ferramentas brutas como firewalls e VPNs obsoletos para proteger os recursos da empresa, o Cloud Secure Edge permite o acesso com privilégios mínimos para aplicações e servidores específicos, com base em fatores combinados de tempo real contextual de usuários e de confiança e sigilosidade dos recursos nos dispositivos.

Funciona em nuvem e pode ser utilizado de forma independente ou em combinação com a infraestrutura de segurança já instalada.

Proteja-se contra as ameaças via internet e o comprometimento de credenciais

A SonicWall implementou PCPs de borda global de alto desempenho para assegurar o roteamento mais eficiente e direto, ao mesmo tempo utilizando controles de fiscalização consistentes, para proteção contra todo tipo de ataque e exposição de risco. Trata-se de uma proteção simples e eficaz contra ataques de phishing e sites mal-intencionados, que também aplica filtros de conteúdo conforme desejados, e a segurança dos dispositivos é verificada logo no início, antes que o acesso seja concedido – como deve ser.

Proteja usuários de alto risco (terceiros/BYOD/M&A)

Ofereça aos usuários terceirizados acesso fácil e seguro somente aos recursos específicos de que precisam, sem qualquer provisionamento adicional desnecessário. O Cloud Secure Edge assegura o acesso com base não apenas na postura de segurança do usuário e no seu dispositivo, mas também na função e no que eles têm autorização para acessar. A gestão é simples, com grupos e funções que podem ser pré-identificados e aplicados conforme o necessário, a partir de um console central. Não é preciso usar patches ou configurar o hardware – nunca.

Licenciamento

O Cloud Secure Edge está disponível para compra com o Secure Private Access (para recursos em redes internas) e com o Secure Internet Access (para recursos na Internet pública).

1. O Secure Private Access conta com dois recursos centrais:
   - ZTNA via túnel (também conhecido como VPN em nuvem ou VPNaaS): Acesso seguro a redes para segmentos de rede específicos.
   - ZTNA baseado em proxy: Acesso seguro a recursos privativos, como aplicações HTTP internas e serviços TCP.
2. O Secure Internet Access conta com três recursos centrais:
   - Segurança por camada de DNS (DNS): Proteção contra ameaças em nível de domínio, que bloqueia domínios mal-intencionados e fiscaliza as políticas de uso aceitáveis.
   - Cloud Access Security Broker (CASB): Fiscalização de políticas de confiança em dispositivos para acesso a aplicações SaaS.
   - Secure Web Gateway (SWG): Filtros de conteúdo para internet para bloquear malware e outras ameaças ocultas no tráfego de internet criptografado.

Os SKUs do Secure Private Access (SPA) e do Secure Internet Access (SIA) estão disponíveis em dois níveis: Básico e Avançado. As licenças são vendidas por usuário.

Recursos em comum

Plano de dados de alto desempenho

Arquitetura de borda dinâmica para conexões rápidas e confiáveis para usuários em todo o mundo

Suporte nativo para todos os sistemas operacionais dos clientes

Desktop (Windows, macOS, Linux) e dispositivos móveis (iOS, Android, ChromeOS)

Interface de gerenciamento de nuvens

Para administradores de TI e segurança, para configurar a conectividade Zero-trust

Pontuação de confiança

Quantificação do nível de confiança e risco associado aos usuários e dispositivos com acesso

Visibilidade acionável

Uma visão completa dos riscos de usuários/dispositivos e aplicações/recursos

Fiscalização contínua de políticas

Com base na sigilosidade dos recursos, onde quer que o usuário esteja localizado

Integrações

Integra-se às ferramentas instaladas (IDP, EDR, MDM, SIEM)

Firewall Connector da SonicWall

Integração fora da caixa com os firewalls da Gen 7 no Modo Global nas versões 7.1.2 ou posteriores

Gestão multiusuários

Políticas de operação em nuvem para gestão multiusuários

Usuários e dispositivos

Acesso único

Use o SSO corporativo com cadastro de usuários just-in-time (JIT)

Gestão de postura

Analise a postura de um dispositivo, como um firewall, criptografia em disco, bloqueio de tela, versão do SO, etc.

Reparação de danos personalizada

Configure as instruções para reparação da postura dos dispositivos, como mensagens e links, exibidos para os usuários finais

Perfis de confiança

Personalize os efeitos de fatores e políticas com base nos grupos de usuários e dispositivos

Visibilidade e conformidade

Fluxo de eventos em tempo real

Monitore o fluxo de atividades de usuários e dispositivos em tempo real

Geração de relatórios de postura de dispositivos

Rastreie todos os dispositivos – gerenciados ou não – acesse recursos corporativos, bem como sua postura de segurança

Geração de relatórios das atividades administrativas

Registre todas as atividades administrativas na Central de Controle em Nuvem

Operações e automação

API Restful

Endpoint RESTful para configurar objetos CSE no Plano de Controle

Clientes de API – pybanyan, terraform

Biblioteca Python e terraform para automação e gerenciamento

Registro de dispositivos Zero Touch

Instalação do aplicativo Banyan no seu acervo de dispositivos sem exigir qualquer tipo de interação de usuários finais

	Secure Private Access		Secure Internet Access	
Recurso	**Básico**	**Avançado**	**Básico**	**Avançado**
Principais recursos				
Túnel ZTNA (VPNaaS) para habilitar o acesso a redes específicas	✓	✓		
Proxy ZTNA para se conectar em segurança a aplicações HTTP e serviços TCP internos		✓		
Segurança por camada DNS para proteção contra ameaças via internet			✓	✓
Cloud Access Security Broker (CASB) para fiscalizar as políticas de confiança dos dispositivos em aplicações SaaS				✓
Secure Web Gateway (SWG) para filtrar malware e outras ameaças ocultas no tráfego criptografado via internet				✓
Acesso seguro à rede				
Redes privativas (faixas RFC-1918) e domínios privativos (servidores DNS internos)	✓	✓		
Divisão de tráfego em túneis para sub-redes e domínios específicos (privativos ou públicos)	✓	✓		
Operação em túneis completa para todos os tipos de tráfego	✓	✓		
Políticas de acesso a redes/camada 4 com base em CIDRs e FQDNs	✓	✓		
Acesso seguro a recursos privativos				
Acesso a sites internos utilizando fluxos de conexão OpenId somente em navegadores		✓		
SSH para servidores Linux		✓		
RDP para máquinas com Windows		✓		
Clientes nativos para acessar servidores de bancos de dados como PostgreSQL e MySQL		✓		
Clientes de Kubernetes para acessar núcleos		✓		
Autenticação de certificados SSH, autorização de gestores e registro de auditorias		✓		
Políticas da camada 7 para acesso a APIs, páginas da internet		✓		
Proteção contra ameaças via internet				
Segurança na camada DNS, bloqueando domínios com malware, phishing, botnets e outros riscos			✓	✓
Classificação de conteúdo			✓	✓
Bloqueios personalizados			✓	✓
Segurança em aplicações SaaS				
Visibilidade de aplicações em nuvem/Shadow IT				✓
IP Allowlisting para aplicações em nuvem por meio da borda da SonicWall				✓
Confiança nos dispositivos para Okta				✓
Confiança nos dispositivos para Azure AD				✓
Confiança nos dispositivos para outros IDPs como OneLogin, Jumpcloud				✓
Serviço de filtração de conteúdo da web				
Filtração de URLs				✓
Proteção contra malware				✓
Usuários e dispositivos				
Autenticação sem senha com IDP Federation		✓		✓
Acesso fiscalizado por políticas para dispositivos não registrados, com certificado de dispositivo confiável		✓		✓
Acesso sem clientes		✓		✓
Contas de serviços (tokens de API para acesso programático, como geração de scripts e automação por meio do plano de dados)		✓		✓

SONICWALL

Usuários e dispositivos (continuação)				
Integração com SCIM para gerenciar designações de usuários		✓		✓
Integrações de EDR (p. ex. CrowdStrike, SentinelOne, Microsoft Defender)		✓		✓
Integrações MDM/UEM (p. ex. JAMF, Kandji, Jumpcloud, Intune, Workspace One)		✓		✓
Visibilidade e conformidade				
Integração com SIEM (p. ex. Splunk, Elastic, Sumo Logic)		✓		✓
Descoberta de Redes Privativas (aplicações não aprovadas acessadas por usuários ou dispositivos)		✓		n/a
Descoberta de Recursos de IaaS		✓		n/a
Descoberta de aplicações de SaaS		n/a		✓
Operações e automação				
Implementação de borda privativa: Hospedagem do gateway com confirmação de identidade da SonicWall na sua própria infraestrutura		✗	n/a	n/a
Serviços e suporte				
Suporte 24x7	✓	✓	✓	✓
Suporte Premier		suplemento		suplemento
Serviços de implementação remota		suplemento		suplemento

Resumo

O Cloud Secure Edge da SonicWall é uma solução de Security Service Edge com uma combinação de um TCO líder do setor e segurança Zero-trust de nível empresarial. A borda oferece acesso simples e protegido com Zero-trust a recursos privativos e via internet, para funcionários e terceiros, onde quer que estejam e qualquer que seja seu dispositivo. O Cloud Secure Edge é uma combinação da funcionalidade de diversas appliances de rede tradicionais – VPN para acesso remoto, proxy de internet, firewall, etc. – em uma solução unificada, multiusuários e operando em nuvem, simples de implementar e fácil de gerenciar, para organizações de todos os portes, maximizando o ROI para você e seus clientes.

Quer saber mais sobre o Cloud Secure Edge da SonicWall? Clique aqui para começar.

Fale com o executivo da sua conta se quiser adicionar o Cloud Secure Edge aos seus firewalls da Gen 7 da SonicWall já instalados.

Sobre a SonicWall

A SonicWall é uma precursora da segurança cibernética, com mais de 30 anos de especialização e foco incessante sobre seus parceiros. Com capacidade para desenvolver, escalonar e gerenciar a segurança em ambientes em nuvem, híbridos e tradicionais, em tempo real, a SonicWall pode oferecer de forma rápida e econômica soluções de segurança feitas sob medida para qualquer organização, em qualquer lugar do mundo. Com base nos dados do seu próprio centro de pesquisa de ameaças, a SonicWall oferece proteção sem transtornos contra a maioria dos ataques cibernéticos evasivos, bem como inteligência em ameaças acionável para parceiros, clientes e para a comunidade de cibersegurança.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso site na internet para obter informações adicionais.
www.sonicwall.com

© 2024 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.
SonicWall é uma marca registrada da SonicWall Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as demais marcas e marcas registradas são de propriedade dos respectivos titulares. As informações deste documento foram fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Nenhuma licença, expressa ou implícita, por preclusão ou de qualquer espécie, para qualquer direito de propriedade intelectual será concedida por meio deste documento ou em relação à venda de produtos da SonicWall. Salvo na forma estabelecida nos termos e condições, conforme especificado no contrato de licenciamento deste produto, a SonicWall e/ou suas afiliadas presumem isenção de responsabilidade, qualquer que seja, e de qualquer garantia expressa, implícita ou prevista em lei relacionada a seus produtos, incluindo, entre outras, a garantia implícita de comerciabilidade, adequação a um objetivo específico ou não violação. Em hipótese alguma, a SonicWall e/ou suas afiliadas se responsabilizam por qualquer tipo de dano direto, indireto, consequencial, cominatório, especial ou eventual (incluindo, entre outros, danos por lucros cessantes, interrupção de negócios ou perda de informações) decorrentes da utilização ou da incapacidade de utilizar este documento, mesmo se a SonicWall e/ou suas afiliadas tiverem sido orientadas da possibilidade de ocorrência de tais danos. A SonicWall e/ou suas afiliadas não fazem qualquer declaração nem oferecem garantias em relação à precisão ou integridade do conteúdo deste documento e reservam para si o direito de realizar alterações nas especificações e descrições de produtos a qualquer momento e sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não assumem qualquer compromisso pela atualização das informações contidas neste documento.