Linha de Produtos da SonicWall: Visão Geral

Firewalls de Próxima Geração

High End: Série NS*sp*

Firewalls instancias são desenvolvidos para empresas distribuídas de grande porte, data centers e MSSPs, que oferecem proteção de alta velocidade, alta densidade de portas e taxa de transferência acima de 100 Gbps.

Mid-Range: Série NS*a*

Eficácia e desempenho de segurança validados pelo setor para redes de médio porte, filiais e empresas distribuídas.

Básicos: Série TZ

Plataforma integrada de prevenção de ameaças e SD-WAN para implantações em residências, organizações de pequeno/médio porte e SD-Branch.

Virtuais: Série NS*v*

Firewalls virtuais com modelos de licença flexíveis para blindar todos os componentes importantes de sua infraestrutura de nuvem pública e privada.

Série SonicWave

Segurança e desempenho desenvolvidos para a próxima onda de dispositivos sem fio, gerenciados por meio da nuvem com SonicWall Wireless Network Manager.

Série SMA

Acesso simples e seguro com aplicação de política aos recursos da rede e da nuvem.

SonicWall Switch

Oferece switching inteligente para conectividade segura de próxima geração de implantações de SMB e SD-Branch.

Segurança de E-mail ESA Series

Uma solução de várias camadas que protege contra ameaças avançadas de e-mail, entregue em fatores de forma de appliances, VM e nuvem SaaS.

Capture Security appliance (CS*a*)

Teste de arquivos on-premise e prevenção de malware.

Gerenciamento e Análises

Global Management System (GMS)
Network Security Manager
Wireless Network Manager

Governar de modo centralizado, gerenciar riscos e cumprir.

Capture Client

Uma plataforma de cliente unificada com um painel global que oferece vários recursos de proteção de endpoint, inclusive proteção avançada contra malware, sandboxing, Inteligência de Vulnerabilidade de Aplicações e restauração em caso de infecção.

Cloud Edge Secure Access

Uma aplicação SaaS potente que oferece rede como serviço simples para conectividade de site para site e de nuvem híbrida para AWS, Azure e Google Cloud. No processo, ela combina as abordagens de segurança Zero-Trust e Least-Privilege em uma oferta integrada.

Cloud App Security

Uma solução nativa para nuvem que oferece segurança de próxima geração para aplicações SaaS, como Office 365 e G Suite, para proteger e-mail, dados e credenciais de usuários contra ameaças avançadas, ao mesmo tempo que alcança a conformidade na nuvem.

Serviços de Assinatura de Firewall de Próxima Geração

O Threat Protection Service Suite inclui serviços básicos de segurança necessários para garantir que a rede esteja protegida contra ameaças em um pacote econômico. Disponível apenas na série TZ270/370/470, este pacote inclui Antivírus de Gateway, Prevenção de Invasões e Controle de Aplicações, Serviço de Filtragem de Conteúdo, Visibilidade de Rede e Suporte 24x7.

O Essential Protection Services Suite oferece todos os serviços de segurança essenciais para proteger contra ameaças conhecidas e desconhecidas. Isso inclui Capture Advanced Threat Protection com Tecnologia RTDMI, Antivírus de Gateway, Prevenção de Invasões e Controle de Aplicações, Serviço de Filtragem de Conteúdo, Serviço Abrangente Antispam, Visibilidade de Rede e Suporte 24x7.

O Advanced Protection Services Suite oferece segurança avançada para a rede. Esse pacote inclui pacotes de serviços essenciais juntamente com gerenciamento de nuvem e relatórios baseados em nuvem por sete dias.

Saiba mais em sonicwall.com

Perguntas Qualificatórias

Firewalls de Próxima Geração

- Você consegue dar conta do aumento da largura de banda que gera necessidades de desempenho em gigabits ou multi-gigabit?
- Seu firewall atual é capaz de realizar a inspeção de ameaças na velocidade do recebimento de ameaças?
- Quais são seus critérios de requisitos de desempenho?
- Número total de usuários/redes protegidos pelo firewall?
- Número total de sessões/conexões no desempenho máximo?
- Quantos locais e usuários remotos se conectarão ao firewall?
- Como você avalia a eficácia de seus controles de segurança?
- Qual é seu tipo de conexão de Internet? Qual é a velocidade?
- O que você está fazendo para se proteger contra novas ameaças, como ataques de zero-day?
- Seu sandbox tem capacidade para detectar e bloquear ameaças ocultas na memória profunda?
- Quantos motores seu sandbox incorpora?
- Seu sandbox pode manter os arquivos no gateway antes de serem liberados?
- Você sabe se o firewall de sua organização está inspecionando o tráfego HTTPS?
- Você teve interrupções no serviço de rede ou tempo de inatividade em decorrência da inspeção do tráfego HTTPS?
- Seu firewall virtual é tão eficiente quanto seu firewall físico?
- Como você está protegendo seus ambientes de nuvem pública ou privada?
- Você pode implementar zoneamento de segurança e microssegmentação adequados em sua rede virtual?
- Você tem visibilidade e controle completos de seu tráfego virtual?
- Você teria interesse em reduzir custos, substituindo MPLS por SD-WAN para ter uma rede privada segura?

Capture Client

- Seus endpoints precisam de proteção avançada constante contra ransomware e ameaças criptografadas?
- Você pode aplicar com facilidade a conformidade com as políticas e o gerenciamento de licenças em todos os endpoints?
- Você tem dificuldades com a visibilidade dos endpoints e com o gerenciamento de sua postura de segurança?
- Seu produto de segurança de endpoint se conecta a um ambiente de sandbox?
- Você pode catalogar as aplicações instaladas nos endpoints e saber quantas vulnerabilidades eles contêm?
- Sua solução atual monitora continuamente a integridade de seu sistema?
- Você pode reverter o dano causado por ransomware e restaurar um estado limpo conhecido anterior?
- Você pode adicionar ou alterar políticas para usuários rapidamente?

Cloud App Security

- Você usa o O365 ou o G Suite?
- Você está usando o Proofpoint ou o Mimecast para proteger o O365/G Suite?
- Você está examinando os e-mails internos do O365?
- Quantas aplicações SaaS autorizadas sua organização está utilizando?
- Você tem dificuldade para garantir a conformidade dos dados armazenados em aplicações SaaS?
- Como você sabe se as credenciais de seus usuários estão comprometidas?
- Você tem visibilidade de quem acessa os dados, onde e quando? (BYOD)

Inspecione a Memória Profunda

Uma tecnologia patenteada, o SonicWall Real-Time Deep Memory Inspection (RTDMI™) detecta e bloqueia proativamente o malware desconhecido do mercado de massa por meio da inspeção profunda da memória em tempo real. Disponível agora com o serviço de sandbox em nuvem SonicWall Capture Advanced Threat Protection (ATP), o motor identifica e mitiga até mesmo as ameaças modernas mais traiçoeiras, incluindo futuras explorações de Meltdown.

Série SonicWave

- Seus funcionários/parceiros/clientes reclamam do baixo desempenho do Wi-Fi?
- Qual seria o número máximo de usuários wireless em qualquer período?
- Você se preocupa com o custo da adição de uma solução wireless segura a sua rede?
- Você está familiarizado com o padrão wireless 802.11ax?
- Você precisa de flexibilidade para gerenciar access points em múltiplas localizações?
- Você planejou sua rede Wi-Fi de maneira eficaz?
- Você precisa de que os APs sejam desconectados dos firewalls?
- Você se preocupa em disponibilizar funcionalidades de segurança avançadas em sua rede Wi-Fi?
- Os serviços de convidado são importantes para você?
- Você exigiria um portal de login de convidado personalizado para integração de convidado?

SonicWall Switch

- Você precisa de switches de acesso com capacidade de gigabit para alimentar dispositivos habilitados para PoE?
- Uma postura de segurança unificada com visibilidade e gerenciamento unificados é importante para você?
- Você está enfrentando desafios com a solução de switches de terceiros que funcionam com o ecossistema da SonicWall?

Acesso Móvel Seguro

- Qual é sua estratégia atual de acesso para força de trabalho remota?
- Qual é sua opinião sobre a implementação de uma abordagem zero-trust de acesso à rede?
- Como você está oferecendo aos usuários acesso seguro aos recursos e aplicações da empresa hospedados no local e na nuvem?
- Você tem visibilidade de todos os usuários e dispositivos que acessam sua rede?
- Como você está protegendo atualmente suas propriedades da Web e seus servidores da Web essenciais para os negócios?

Segurança de E-mail

- Você se preocupa com ameaças de e-mail avançadas, como ransomware, spear-phishing e Comprometimento de E-mail Comercial?
- Sua solução de segurança de e-mail atual oferece recursos de Proteção Avançada contra Ameaças?
- Você se preocupa com o vazamento de e-mails que contenham informações confidenciais?
- Como você cumpre regulações como GDPR, Sarbanes-Oxley, GLBA ou HIPAA?
- Você tem interesse em oferecer serviços de segurança de e-mail gerenciados a seus clientes? (MSSPs)

Gerenciamento e Análises

- Que problemas você poderia resolver com a unificação de suas soluções de segurança em uma plataforma de gerenciamento comum com experiência de painel único de controle?
- Que vantagens operacionais você obterá se puder gerenciar centralmente todos os seus firewalls, APs e switches de qualquer local com um único console na nuvem?
- Você está confiante no que diz respeito a sua capacidade de demonstrar conformidade com as normas de cibersegurança, como PCI, HIPPA e GDPR?
- O que mudaria em sua postura de segurança se você pudesse detectar e responder melhor a ameaças e riscos com rapidez e precisão?
- Que valor você e sua equipe de liderança obteriam com a visibilidade total de ameaças cibernéticas e riscos em sua empresa?

Cloud Edge Secure Access

- Você tem muitos dados confidenciais? Você se preocupa com usuários com excesso de privilégios?
- Você se preocupa com o aumento das regulações de proteção de dados e segurança da informação?
- Você precisa controlar as interações entre funcionários, parceiros de negócios externos e recursos confidenciais?
- Quantas filiais você tem? Você pode integrar uma nova filial com eficiência?
- Quanto tempo você leva para integrar com segurança um usuário remoto?

Datasheet-ProductLineAtAGlance-A4-JK-7095

SONICWALL®