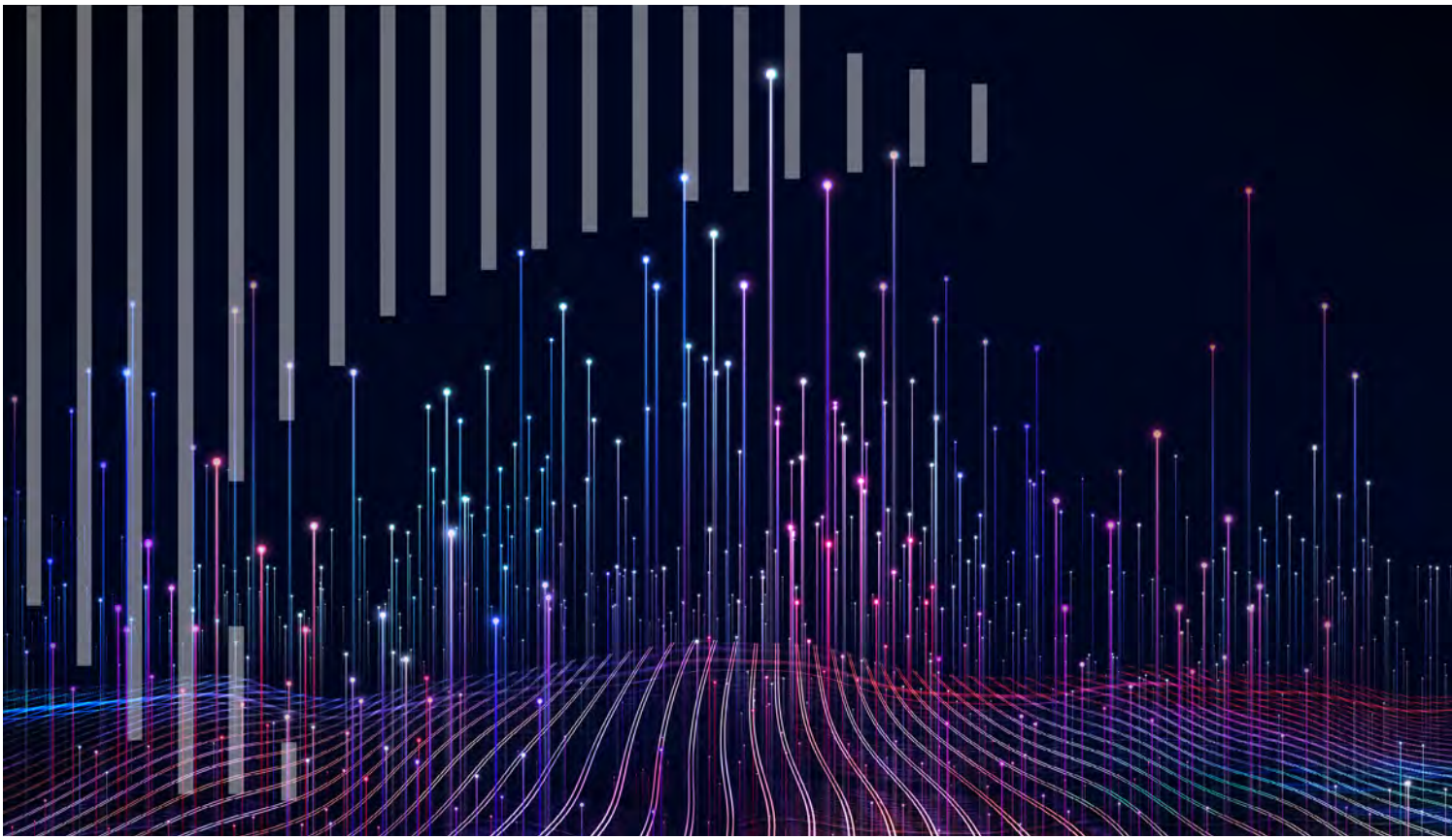
Linhas de produtos SonicWall

Junho 2022



Visão geral

Proteja a nuvem pública/privada, os aplicativos, os usuários e os dados da sua organização com um nível profundo de proteção que não compromete o desempenho da sua rede. A plataforma Capture Cloud da SonicWall integra com solidez segurança, gestão, análises e inteligência de ameaças em tempo real em toda a linha de produtos SonicWall para segurança de rede, wireless, e-mail, dispositivos móveis, web e nuvem. Essa abordagem permite que pequenas e médias empresas, ambientes corporativos de grande porte, pontos de venda de varejo, empresas do setor da educação, saúde, governo e provedores de serviços experimentem nosso ecossistema de segurança completo que aproveita o poder, a agilidade e a escalabilidade da nuvem.

A estratégia e a visão da plataforma Capture Cloud para o futuro são a contínua inovação e desenvolvimento de aplicações de segurança compartimentalizadas, na forma de serviços, que são facilmente programáveis e fornecidas on-demand. O sistema compreende os seguintes componentes e recursos centrais principais:

- Segurança de redes
- Segurança de redes com fio
- Segurança de redes sem fio
- Segurança de endpoints
- Aceleração de WAN
- Serviços de segurança avançados
- Cloud App Security
- Cloud Edge Secure Access
- Acesso seguro a dispositivos móveis
- Segurança de e-mails
- Gestão, geração de relatórios e análises
- Serviços e suporte profissionais

A combinação desses elementos garante a defesa cibernética, inteligência em ameaças, análises e colaboração críticas para a missão e em camadas, juntamente com a gestão centralizada, a geração de relatórios e análises que funcionam de forma síncrona.

Segurança de redes

A SonicWall é uma das fornecedoras líderes do mercado de firewalls de próxima geração (*Next-Generation Firewalls* – NGFWs). Tanto o firmware SonicOS quanto o SonicOSX estão no núcleo de todos os NGFW da SonicWall. O SonicOS potencializa nossa arquitetura de hardware escalável, além dos nossos mecanismos patenteados de inspeção profunda de memória em tempo real (*Real-Time Deep Memory Inspection* – RTDMI™), e de inspeção profunda de pacotes (*Reassembly-Free Deep Packet Inspection*® – RFDPI), de baixa latência, que promove a varredura de todo o tráfego, qualquer que seja a porta ou o protocolo.

Nossos NGFWs asseguram que cada byte de cada pacote seja inspecionado, ao mesmo tempo mantendo o alto desempenho e a baixa latência exigidas pelas redes mais utilizadas. Ao contrário dos produtos concorrentes, o mecanismo RFDPI de passagem única permite a varredura simultânea das aplicações, detectando múltiplas ameaças, bem como a análise de arquivos de qualquer tamanho, sem a remontagem de pacotes. Isso permite aos NGFWs da SonicWall ampliar sua atuação drasticamente, estendendo sua segurança com tecnologia de ponta a redes e centros de dados empresariais distribuídos e em pleno crescimento.

Os NGFWs da SonicWall oferecem uma série de recursos robustos, incluindo:

- Sandboxing Capture ATP multimotor baseado em nuvem
- SD-WAN
- APIs REST
- Descriptografia e inspeção de tráfego criptografado
- Serviço de prevenção de intrusões (*Intrusion prevention service* – IPS)
- Proteção contra malware
- Inteligência, controle e visualização em tempo real de aplicações
- Filtro de sites/URLs (filtragem de conteúdo)
- VPN (*Virtual Private Network*) baseado em SSL ou IPSec
- Segurança de redes sem fio
- Segurança híbrida e multinuvem
- Failover/failback dinâmico

Além disso, os firewalls da SonicWall proporcionam uma resposta rápida e proteção contínua contra ameaças de dia zero, vindas da Equipe de pesquisa de ameaças do Capture Labs. Essa equipe coleta, analisa e verifica informações de ameaças entre vetores de uma variedade de fontes de inteligência de ameaças, incluindo mais de um milhão de sensores colocados globalmente em sua rede Capture Threat Network.

Plataforma de serviços de segurança de redes da SonicWall (série NS*sp*)

A plataforma de NGFW da série SonicWall NS*sp* foi projetada para oferecer escalabilidade, confiabilidade e segurança profunda em velocidades de multigigabits, para redes de grande porte.

O ICSA Labs testou os firewalls da SonicWall e constatou sua excelência em eficácia de segurança, com índice de detecção de 100%, sem qualquer falso positivo, nos últimos cinco trimestres consecutivos. Os firewalls da SonicWall definiram o padrão para controle e prevenção de ameaças em aplicativos de alto desempenho, em diversos tipos de instalações, desde pequenas empresas a centros de dados, operadoras e prestadoras de serviços de grande porte.

Por exemplo, nosso firewall multi-instância NS*sp* de ponta garante alto nível de qualidade de serviço com disponibilidade de rede ininterrupta e conectividade exigida pelas atuais empresas, agências governamentais, provedores de serviços e universidades com infraestruturas de 100/40/10 Gbps. Potencializando as inovadoras tecnologias de segurança com aprendizagem profunda na plataforma Capture Cloud da SonicWall, a série NS*sp* oferece proteção comprovada contra as ameaças mais avançadas sem diminuir o desempenho.

Política unificada com o SonicOSX 7

O recurso de gestão de políticas unificadas do SonicOSX 7 oferece a gestão integrada das políticas de acesso e segurança em determinados firewalls virtuais NS*sp* e NS*v* de ponta da SonicWall.

O recurso inclui uma nova interface web, projetada com uma abordagem radicalmente diferente. Destaca-se o design *user-first* (o usuário em primeiro lugar), que permite uma configuração mais intuitiva das políticas de segurança contextuais por meio de alertas acionáveis e com a simplicidade *point-and-click* (apontar e clicar).

Visualmente, também é mais atraente do que a interface clássica. Com uma visualização de painel único do firewall, a interface apresenta ao usuário informações sobre a eficácia de várias regras de segurança. Ela permite ao usuário alterar as regras predefinidas para antivírus, antispyware, filtragem de conteúdo, prevenção de intrusões, filtragem geo-IP e inspeção profunda de pacotes de tráfego criptografado nos gateways, sem interrupções.

Com esta nova interface de políticas unificada, a SonicWall oferece uma experiência mais ágil para controlar as alterações dinâmicas de tráfego em menos tempo, e para manter uma melhor postura global de segurança.

*Patentes nos EUA: 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

Appliance de segurança de redes da SonicWall (série NS*a*)

O appliance de segurança de redes da SonicWall (série NS*a*) é um dos NGFW mais seguros, com alto desempenho, disponíveis na classe. O sistema oferece segurança de nível empresarial, sem comprometer o desempenho, utilizando a mesma arquitetura do nosso carro-chefe, o NGFW da série NS*sp* – desenvolvido para as redes empresariais com maior demanda do mundo.

Com base em anos de pesquisa e desenvolvimento, a série NS*a* foi projetada desde o início para empresas distribuídas, empresas de médio porte, filiais, campus escolares e agências governamentais. A série NS*a* é uma combinação de arquitetura revolucionária com vários núcleos e a tecnologia de inspeção profunda de memória em tempo real (*Real-Time Deep Memory Inspection* – RTDMI), um mecanismo patenteado de prevenção de ameaças com design altamente escalável. Isto representa proteção, desempenho e escalabilidade líderes no setor, com um grande número de conexões simultâneas, baixa latência, sem limitações quanto ao tamanho dos arquivos e mais conexões por segundo, em comparação a outros fornecedores de firewalls do mercado.

Série SonicWall TZ

A série SonicWall TZ compreende firewalls altamente confiáveis, altamente seguros e gestão unificada de ameaças (*Unified threat management* – UTM), projetada para pequenas e médias empresas (PME), implementação em estabelecimentos varejistas, órgãos do governo e empresas distribuídas com unidades remotas e filiais. Ao contrário dos produtos para consumidores, a série TZ consolida recursos altamente eficazes de antimalware, prevenção de intrusões, filtragem de conteúdo/URLs e controle de aplicativos, em redes com e sem fio – juntamente com amplo suporte para plataformas móveis para notebooks, smartphones e tablets. Esta série conta com inspeção completa e aprofundada de pacotes (*Deep packet inspection* – DPI), em níveis de desempenho altíssimos, eliminando os gargalos nas redes causados por outros produtos, além de proporcionar ganhos na produtividade para as organizações.

Assim como em todos os firewalls da SonicWall, a série TZ inspeciona o arquivo inteiro, incluindo arquivos TLS/SSL criptografados, para permitir uma proteção completa. Além disso, a série TZ oferece inteligência e controle de aplicativos, análise avançada e geração de relatórios de tráfego de aplicativos, segurança de protocolos de internet (*Internet Protocol Security* – IPsec), bem como SSL VPN, failover de ISP múltiplo, balanceamento de cargas e SD-WAN. *Power over Ethernet* (PoE) integrada e rede wireless de alta velocidade 802.11ac opcionais permitem às organizações estender os limites de suas redes facilmente e em segurança. Combinados com os switches SonicWall, os firewalls da série TZ oferecem flexibilidade para expandir os negócios com segurança e com a facilidade da implantação Zero-Touch, mas sem aumentar a complexidade.

A série TZ de última geração é o primeiro firewall com configuração física para desktop que permite interfaces de multigigabits (2.5/5/10G) ou gigabits, SD-WAN segura, armazenamento interno expansível, suporte para TLS 1.3 e prontidão para 5G, ao mesmo tempo oferecendo um desempenho revolucionário. Os recursos de potência redundantes e o suporte para 802.11ac Wave 2 otimizam ainda mais os recursos dos dispositivos. Projetado para organizações de médio porte e empresas distribuídas, com unidades com SD-branch, o firewall da nova geração da série TZ oferece eficácia em segurança comprovada no setor, com a melhor relação preço-desempenho da categoria.

Série (NS*v*) virtual para segurança de redes da SonicWall

Os firewalls virtuais de segurança de redes da SonicWall (série NS*v*) ampliam a detecção e prevenção automatizada de violações em ambientes híbridos e com múltiplas nuvens, com versões virtualizadas dos firewalls com tecnologia de ponta da SonicWall. Com ferramentas e serviços com recursos completos, equivalentes a um firewall da SonicWall, o NS*v* efetivamente defende seus ambientes virtuais e em nuvens contra ataques decorrentes do mal uso dos recursos, ataques entre máquinas virtuais, ataques laterais e todas as formas de exploração e ameaças baseadas em redes.

O NS*v* pode ser facilmente implementado e empregado em um ambiente virtual multiusuários, tipicamente entre redes virtuais (VNs). Ele estabelece medidas de controle de acesso para preservar os dados e segurança VM, ao mesmo tempo capturando o tráfego virtual entre máquinas e redes virtuais, para prevenção automatizada de violações.

Com suporte infraestrutural para implementações de alta disponibilidade (*High Availability* – HA) o NS*v* atende aos requisitos de escalabilidade e disponibilidade de centros de dados definidos por software (*Software*

Defined Data Centers – SDDC). Facilmente implementável na forma de sistema virtual em plataformas privativas em nuvem, como VMWare ESXi, Linux KVM, Nutanix or Microsoft Hyper-V, ou em ambientes em nuvens públicas AWS ou Microsoft Azure. Potencialize modelos de licenciamento flexíveis BYOL e PAYG com o NS*v* e ofereça às organizações todas as vantagens da segurança de um firewall físico, com os benefícios operacionais e econômicos da virtualização.

Determinados modelos de firewalls NS*v* oferecem o SonicOSX com Política Unificada, que proporciona uma experiência mais agilizada para controlar mudanças dinâmicas no tráfego em menos tempo, além de uma postura global de segurança melhor.

Saiba mais sobre os produtos de firewall da SonicWall no site: www.sonicwall.com/pt-br/products/firewalls/

Capture Security appliance 1000 (CSa 1000)

Para cumprir as normas e regulamentos de privacidade, você precisa de uma plataforma de análise de ameaças economicamente viável que não pode ser detectada e evitada por códigos mal-intencionados. O Capture Security appliance (CS*a*) da SonicWall é uma solução local para análise de arquivos e detecção de malware, que inclui a inspeção profunda da memória em tempo real (*Real-Time Deep Memory Inspection* – RTDMI) da SonicWall. A RTDMI permite ao CS*a* capturar mais malwares, mais rapidamente e com maior eficácia. Sua baixa taxa de falsos positivos otimiza a segurança e a experiência do usuário final.

O CS*a* permite ao usuário analisar malwares ocultos em um amplo espectro de tipos de arquivos, tamanhos de arquivos e ambientes operacionais, com uma detecção abrangente de ameaças desde o dia zero. O sistema detecta e interrompe ataques a canais secundário, por meio de inspeção da memória em tempo real. Ao forçar o malware a revelar seus recursos de invasão da memória, o CS*a* bloqueia proativamente ameaças massivas, de dia zero e desconhecidas. O CS*a* funciona em redes fechadas e pode ser utilizado com os firewalls com tecnologia de ponta mais recente da SonicWall.

A implementação do CS*a* da SonicWall é rápida e direta, e requer apenas a configuração dos parâmetros básicos das redes e relatórios e a concessão de acesso aos dispositivos. O CS*a* foi desenvolvido para ser identificável por endereços IP, portanto, pode ser implementado em qualquer lugar, desde que seja acessível por dispositivos que enviem arquivos para análise. O CS*a* também pode ser implementado em redes fechadas ou fisicamente isoladas.

Segurança de redes com fio

Os switches da SonicWall permitem comutação de alta velocidade entre redes, com desempenho e gerenciabilidade incomparáveis. Eles oferecem alta densidade de fluxo nas portas, *Power over Ethernet* (PoE) opcional e rendimento de 1 ou 10 gigabits. Ideais para PMEs e redes de unidade de negócios definidas por software (*Software-Defined Branch ou SD-Branch*), eles permitem uma transformação em empresas de todos os portes para que acompanhem o ritmo das mudanças nas redes e no panorama de segurança.

Os switches da SonicWall podem ser administrados utilizando os firewalls ou o gerenciador de redes sem fio Wireless Network Manager (WNM) da SonicWall.

O WNM integra sem contratempos a segurança de redes com ou sem fio, de ponta a ponta, para proporcionar uma postura de segurança unificada. Isto simplifica a implementação, a gestão e a solução de problemas e elimina lacunas que possam surgir com switches de terceiros. Os switches da SonicWall podem se estender rapidamente a todas as unidades distribuídas, com implementação do tipo Zero-Touch.

Segurança de redes sem fio

A SonicWall torna as redes sem fio seguras, simples e a preços acessíveis, com a inovadora solução de segurança de redes sem fio da SonicWall (*Wireless Network Security*). Os Access Points wireless de alta performance da série 802.11ax SonicWave podem ser facilmente gerenciados via Wireless Network Manager.

Além dos Access Points sem fio de alta velocidade e do painel de controle administrado em nuvem, a solução de segurança para redes sem fio da SonicWall inclui o Wi-Fi Planner, uma ferramenta avançada de pesquisa de sites que ajuda os administradores a planejar e implementar redes Wi-Fi com eficiência. A solução também inclui o aplicativo para dispositivos móveis SonicExpress, para fácil inclusão e monitoramento dos pontos de acesso, que fornece aos administradores informações em tempo real sobre o status e a segurança das redes.

Nossa solução vai além de meras soluções sem fio seguras, ela protege redes sem fio com tecnologias RTDMI e RFDPI, e oferece recursos avançados de segurança, como sandboxing multimotor, filtros de conteúdo, AV em nuvem diretamente nos pontos de acesso, sem a necessidade de um firewall. Otimize ainda mais a segurança

e o desempenho da sua rede com recursos que incluem prevenção de intrusões, descriptografia e inspeção TLS/SSL, e controle de aplicações para desempenho e proteção de nível empresarial.

Os APs do SonicWave funcionam com roaming rápido, de forma que os usuários possam navegar entre locais sem transtornos. Seu portfólio rico em recursos inclui um portal cativo, seleção automática de canais, ferramentas de análise de espectro, *air-time fairness* (redução de gargalos), gerenciamento de bandas e análise de sinais, para fins de monitoramento e solução de problemas.

A SonicWall reduz o custo total de propriedade (*Total Cost of Ownership* – TCO), ao permitir que os administradores evitem implementar e gerenciar separadamente uma solução cara específica sem fio que é executada em paralelo à rede cabeada existente.

Segurança de endpoints

A gestão e a segurança de endpoints é crítica no cenário empresarial atual. Com usuários finais entrando e saindo da rede com seus dispositivos, além das ameaças criptografadas que atingem os endpoints não verificados, algo precisa ser feito para proteger esses dispositivos. Com o crescimento dos ransomwares e das vulnerabilidades dos aplicativos, os endpoints são o campo de batalha do panorama das ameaças nos dias de hoje.

Além disso, os administradores sofrem com a visibilidade e a gestão de sua postura de segurança. Eles também enfrentam o desafio de ter de garantir de forma coerente a segurança de seus clientes, sem abrir mão de uma inteligência e relatórios de fácil utilização e acionáveis.

Os produtos de segurança de endpoints estão no mercado há muitos anos, mas os administradores têm problemas para:

- Manter os produtos de segurança atualizados
- Aplicar políticas em uma escala global
- Obter relatórios e visualizar a saúde dos usuários
- Ameaças que penetram a segurança e geram canais criptografados
- Compreender os alertas e as etapas da reparação
- Catalogar aplicativos e suas vulnerabilidades
- Interromper ameaças como ransomwares
- Ataques sem arquivos e dispositivos USB infectados se esquivando das defesas do perímetro

O SonicWall Capture Client é uma plataforma de client unificada que oferece recursos de proteção de múltiplos endpoints. Esta solução inclui um console de gerenciamento em nuvem e uma integração completa opcional, com firewalls de tecnologia de ponta da SonicWall, para proporcionar uma experiência unificada de segurança aos clientes da SonicWall. Combinado aos recursos de fiscalização, o SonicWall Capture Client pode assegurar a execução de software de segurança nos endpoints e/ou manter um certificado SSL instalado para inspeção do tráfego criptografado. Além disso, para realizar a inspeção do tráfego SSL (DPI-SSL) mais facilmente, com uma experiência melhor para o usuário final, o Capture Client permite ao administrador instalar certificados SSL nos endpoints com muito mais facilidade do que antes.

Além dessas vantagens, o Capture Client conta com um mecanismo antivírus avançado para interromper a ação dos malwares mais engenhosos, com uma opção de reversão para um estado anterior sem infecção. O Capture Client Advanced se integra à proteção avançada contra ameaças (*Capture Advanced Threat Protection* – ATP) da SonicWall para examinar arquivos suspeitos e atacá-los com mais eficiência, antes que sejam ativados.

Os administradores agora podem catalogar todas as aplicações em todos os endpoints protegidos pelo Capture Client, com a geração de relatórios sobre as vulnerabilidades conhecidas no ecossistema.

O Painel de Controle Global foi projetado para que os MSSPs vejam o número de infecções, as vulnerabilidades presentes e a versão do Capture Client instalada para cada usuário. O que e quem está sendo bloqueado com mais frequência pode ser visto pela Filtragem de conteúdo, assim como quais dispositivos estão on-line e em operação. A Política global permite aos administradores aplicar uma só política de linha de base a todos os usuários. Isto facilita o desempenho de novos usuários e cria rapidamente proteções contra novas ameaças para todos os usuários que segurem a política em questão.

Entre os recursos do SonicWall Capture Client podemos citar:

- Fiscalização da segurança
- Gestão de certificados DPI-SSL
- Monitoramento comportamental contínuo
- Determinações altamente precisas, obtidas por meio de aprendizagem de máquina
- Técnicas heurísticas em múltiplas camadas
- Inteligência em vulnerabilidade de aplicativos
- Recursos exclusivos de reversão
- Integração de sandbox de rede Capture Advanced Threat Protection
- Painel de controle global e Política hereditária global
- Pesquisa em um clique de arquivos suspeitos utilizando a base de dados inteligente de ameaças do Capture ATP, com todas as condenações e absolvições
- Filtragem de conteúdo para fiscalizar políticas da internet e bloquear endereços IPs, URLs e domínios mal-intencionados em dispositivos afastados da rede
- Controle de dispositivos baseado em políticas para bloquear dispositivos de armazenamento possivelmente infectados

Serviços de segurança avançados

Os serviços de firewall para segurança em redes da SonicWall oferecem uma proteção altamente eficaz e avançada para organizações de todos os portes, que as ajuda a se defenderem contra ameaças, obter um controle maior da segurança e otimizar sua produtividade, com custos mais baixos.

A SonicWall oferece três pacotes de assinaturas dos firewalls da série Gen 7: Threat Protection Services Suite, o Essential Protection Services Suite e o Advanced Protection Services Suite. O Threat Protection Services Suite inclui os serviços básicos de segurança necessários para assegurar que a rede está protegida contra ameaças em um pacote econômico. Adicione o pacote Essential da SonicWall para usufruir dos serviços de segurança essenciais, necessários para se proteger contra ameaças conhecidas e desconhecidas, e o pacote Advanced oferece segurança avançada que amplia a segurança da sua rede com serviços essenciais adicionais de segurança em nuvens.

O **Threat Protection Services Suite**, disponível somente nas séries TZ270/370/470, inclui Antivírus Gateway, Prevenção contra intrusões e Controle de aplicativos, serviço de Filtragem de conteúdo, inspeção profunda de pacotes de tráfego TLS/SSL criptografado (DPI-SSL) e suporte 24 horas.

O **Essential Protection Services Suite** inclui o Capture Advanced Threat Protection com tecnologia RTDMI, Antivírus Gateway, Prevenção contra intrusões e Controle de aplicativos, serviços de Filtragem de conteúdo, serviços abrangentes Antispam, inspeção profunda de pacotes de tráfego TLS/SSL criptografado (DPI-SSL) e Suporte 24 horas.

O **Advanced Protection Services Suite** inclui o Capture Advanced Threat Protection com tecnologia RTDMI, Antivírus Gateway, Prevenção contra intrusões e Controle de aplicativos, serviços de Filtragem de conteúdo, serviços abrangentes Antispam, inspeção profunda de pacotes de tráfego TLS/SSL criptografado (DPI-SSL), Suporte 24 horas, Gestão de nuvem, Relatórios baseados em nuvens por sete dias e o Suporte Premier opcional.

Inspeção profunda da memória

O mecanismo Real-Time Deep Memory Inspection (RTDMI) da SonicWall detecta e bloqueia proativamente malwares desconhecidos do mercado de massa por meio de inspeção profunda da memória em tempo real. Agora disponível com o serviço de sandboxing em nuvem do Capture Advanced Threat Protection (ATP) da SonicWall, o mecanismo identifica e mitiga até mesmo as ameaças modernas mais insidiosas, incluindo futuras explorações do Meltdown.

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE

Cloud App Security

A solução Cloud App Security da SonicWall protege SaaS populares, e-mails, aplicativos de colaboração e produtividade, incluindo email do Office 365, SharePoint, OneDrive, G-Suite, Dropbox e Box.

A cobertura da proteção inclui:

- Comprometimento de e-mails comerciais
- Prevenção de perda de dados (Data Loss Prevention – DLP)
- Controle de contas (Account Takeover – ATO)
- Malwares avançados e de dia zero em anexos mal-intencionados e arquivos armazenados
- Phishing direcionado
- Tentativas de fraude

O Cloud App Security utiliza definições de perfil avançadas de usuários e análise de comportamento com mais de 300 indicadores de ameaças, para determinar se contas legítimas estão sendo exploradas por criminosos cibernéticos. Com os recursos de A.M. e I.A., a solução bloqueia ataques de identidade falsa, incluindo a varredura retroativa das atividades.

Para aplicativos de SaaS e compartilhamento de arquivos como OneDrive, o Cloud App Security aplica mecanismos de sandbox multimotor do Capture ATP para detectar malwares nunca vistos antes. Ele realiza varreduras tanto históricas quanto em tempo real dos arquivos e dados, estejam eles estáticos ou sendo utilizados no ambiente de SaaS, internamente ou de nuvem para nuvem. Além disso, o recurso de DLP da solução protege os dados estáticos, limitando o acesso somente a aplicativos aprovados e impedindo o envio de dados não autorizado.

Como um serviço na modalidade SaaS, o Cloud App Security pode ser acionado e entrar em operação em poucos minutos. Com escalabilidade ilimitada, a solução ajuda organizações de qualquer porte a ampliar sua proteção imediatamente para seus usuários de aplicativos SaaS, sejam eles algumas centenas ou milhares distribuídos pelo mundo. Todos os aplicativos SaaS têm um mecanismo de políticas separado, cada qual com suas próprias regras e recursos de fiscalização. Desta forma, você pode atribuir uma política específica para cada aplicativo SaaS, com base nos seus requisitos de segurança.

Sem a necessidade de instalar e gerenciar hardware e software, o Cloud App Security elimina as despesas de capital, os custos com instalações complexas e manutenção contínua associados à implementação de uma solução alternativa local.

Saiba mais sobre o SonicWall Cloud App Security no site www.sonicwall.com/pt-br/products/cloud-security/

Cloud Edge Secure Access

Evolução da VPN tradicional para segurança Zero-Trust

Os funcionários dos dias de hoje querem a flexibilidade de trabalhar em qualquer lugar – e as organizações dos dias de hoje querem aproveitar a economia e a eficiência operacional oferecida pelas nuvens.

Porém, as soluções VPN tradicionais não foram desenvolvidas para esta nova realidade. Implementar uma solução dessas pode levar dias, até mesmo semanas. Problemas de disponibilidade de fornecimento significam que elas podem ou não estar disponíveis e, uma vez instaladas, pode ser difícil programar paralisações.

E o pior: elas podem oferecer uma porta dos fundos na sua rede, uma vez que todos os acessos concedidos representam o acesso à rede ampla e permitem a movimentação lateral na sub-rede.

E como o tráfego de usuários circula pelo concentrador de VPN local em vez de acessar a nuvem diretamente, a VPN gera uma latência que reduz a eficiência e prejudica a experiência dos usuários em nuvem.

Gartner previu que, até 2023, 60% das empresas vão eliminar a maior parte das redes privativas de acesso remoto (VPNs), substituindo-as pelo acesso à rede com zero confiança (*Zero-Trust Network Access* – ZTNA).

Segurança de redes com Zero-Trust para proteger ativos de alto valor

Com o Cloud Edge Secure Access, a SonicWall oferece uma solução ZTNA que supera esses problemas, em conjunto com uma ampla gama de outros benefícios. No núcleo do Cloud Edge Secure Access da SonicWall, há três recursos essenciais:

- Acesso com privilégio mínimo para proteger ativos corporativos
- Implementação rápida do autosserviço
- Acesso confiável diretamente à nuvem, de qualquer lugar

Como um serviço nativo em nuvem, o sistema oferece um acesso simples à rede como serviço (*Network as a Service* – NaaS), para conectividade em nuvem entre sites ou híbrida, com recursos de segurança de Zero-Trust e Privilégio Mínimo integrados.

- A verificação de postura dos dispositivos (*Device Posture Check* – DPC) concede acesso à rede somente a dispositivos autenticados e em conformidade
- Políticas de microssegmentação definidas por software efetivamente evitam a disseminação de violações
- O Controle de tráfego na rede (*Network Traffic Control* – NTC) é um tipo de firewall como serviço (*Firewall as a Service* – FwaaS) dinâmico, que oferece proteção com base em políticas, definindo quem pode acessar que recursos e de que locais

As organizações agora podem capacitar equipes de trabalho remotas e proteger ativos de alto valor da empresa ao mesmo tempo.

Serviço nativo em nuvem em todo o mundo com implementação em poucos minutos

O SonicWall Cloud Edge conta com o suporte de mais de 30 pontos de presença (*Points of Presence* – PoPs) globais.

O serviço global permite aos gerentes de TI que se conectem a uma unidade de negócios e implementem o serviço em 15 minutos. E os usuários finais podem instalar o client do SonicWall Cloud Edge e se tornar produtivos em 5 minutos.

A infraestrutura é desenvolvida sob uma arquitetura de perímetro definido pelo software (*Software-Defined Perimeter* – SDP), que separa o controlador centralizado do gateway que atua na análise do nível de confiança.

Ao distribuir os gateways do SDP, o Cloud Edge Secure Access pode se ampliar rapidamente, manter o alto desempenho e proporcionar a melhor atuação possível em nuvem.

Além disso, a separação das funções também torna o Cloud Edge Secure Access impenetrável para as ameaças cibernéticas comuns, como DDoS, exploits do Log4j, sequestro de redes Wi-Fi públicas, SYN flood e Slowloris.

Benefícios adicionais:

- A solução de segurança para empresas distribuídas e com mão de obra remota
- Acesso instantâneo e seguro a sites físicos e recursos em nuvens híbridas
- Escala de 10 usuários a milhares de usuários
- Compatível com acesso à rede sem client, com qualquer dispositivo público
- Criptografia WireGuard de alta performance
- Integração de provedor de identidade em nuvem e SIEM
- Moderna integração SSO e MFA
- Integração SIEM
- Recursos multiusuários para MSSPs
- O Controle de tráfego na rede (*Network Traffic Control* – NTC) permite a proteção em nível de firewall, definindo quem pode acessar que recursos e de que locais
- A verificação de postura dos dispositivos (*Device Posture Check* – DPC) concede acesso à rede somente a dispositivos autenticados e em conformidade.
- Disponível nos EUA, na Europa, no Oriente Médio e na Ásia

Saiba mais sobre o Cloud Edge Secure Access da SonicWall no site www.sonicwall.com/pt-br/products/cloud-edge-secure-access/

Secure Mobile Access

A série da SonicWall de acesso móvel seguro (*Secure Mobile Access* – SMA) é o gateway de acesso seguro unificado para organizações que enfrentam desafios de mobilidade, trabalho em casa, BYOD e migração para nuvem. A solução permite que a organização forneça acesso a qualquer hora, em qualquer lugar e de qualquer dispositivo, a recursos corporativos críticos para a missão. O mecanismo da política de controle de acesso granular, a autorização de dispositivos sensíveis ao contexto, VPN em nível de aplicativo e autenticação avançada do SMA, com um único acesso, capacita as organizações a permitirem o BYOD e a mobilidade em um ambiente de TI híbrido.

Além disso, o SMA reduz a superfície das ameaças, oferecendo recursos como detecção de Geo IP e Botnet, firewall para aplicativos de internet e integração de sandbox do Capture ATP.

Mobilidade e BYOD

Para organizações que pretendem adotar o BYOD, trabalho flexível ou desenvolvimento internacional, o SMA se torna o ponto central de fiscalização em todos esses nichos. O SMA oferece a melhor segurança da categoria, para minimizar a superfície das ameaças, ao mesmo tempo tornando as organizações mais seguras com o suporte aos algoritmos de criptografia e cifras mais recentes. O SMA da SonicWall permite aos administradores oferecer acesso seguro para dispositivos móveis e privilégios baseados na função do usuário, de forma que os usuários finais tenham acesso rápido e simples aos aplicativos, dados e recursos da empresa. Ao mesmo tempo, as organizações podem instituir políticas de BYOD seguro para proteger suas redes e dados corporativos contra o acesso de criminosos e malwares.

Mudança para a nuvem

Para organizações que estão embarcando em uma jornada de migração para as nuvens, o SMA oferece uma só infraestrutura de registro (*Single Sign-on* – SSO), que utiliza um único portal da internet para autenticar usuários em um ambiente de TI híbrido. Seja o recurso corporativo instalado localmente, na internet ou em uma nuvem, a experiência de acesso será consistente e sem transtornos. Os usuários não precisam se lembrar de todas as URLs dos aplicativos individuais e manter marcadores em excesso. Com o Workplace, um portal de acesso centralizado, você gera para os usuários uma URL para acessar todos os aplicativos críticos para a missão, a partir de um navegador comum da internet. O SMA funciona com SSO federado tanto para aplicativos SaaS hospedados em nuvem, que usam SAML 2.0, quanto para os hospedados em campus, que utilizam RADIUS ou Kerberos. O SMA integra-se a vários servidores de autenticação, autorização e contabilidade e tecnologias líderes de autenticação multifator (MFA) para oferecer segurança adicional. O SSO seguro é disponibilizado apenas em dispositivos endpoint autorizados, depois de verificações de status de saúde e conformidade.

Prestadores de serviços gerenciados

Para organizações com centros de dados ou prestadores de serviços gerenciados, o SMA é uma solução pronta para o uso, que proporciona um alto grau de continuidade e escalabilidade dos negócios. O SonicWall SMA pode suportar até 20.000 conexões simultâneas em um único dispositivo, com a capacidade de escalar mais de um milhão de usuários por meio de agrupamentos inteligentes. Reduza os custos nos centros de dados com agrupamentos HA ativo-ativo (alta disponibilidade global) e balanceamento de carga dinâmico embutido (otimizador de tráfego global), que realoca o tráfego global para o centro de dados mais otimizado, em tempo real, com base na demanda do usuário. O SMA capacita os proprietários dos serviços com uma série de ferramentas que prestam serviços com zero paralisação, e permite que SLAs muito agressivos sejam cumpridos.

Sistemas SMA

O SMA da SonicWall pode ser implementado como um hardware de alto desempenho, ou como um sistema virtual que potencializa recursos de computação compartilhados para otimizar a utilização, facilitar a migração e reduzir os custos de capital. Os hardwares são construídos com arquitetura multinuclear, que oferece alto desempenho com aceleração de SSL, rendimento de VPN e proxies poderosos para oferecer acesso seguro e robusto. Para organizações regulamentadas e federais, o SMA está disponível com certificação FIPS 140-2 Nível 2. O sistema virtual SMA oferece os mesmos recursos de acesso robusto e seguro das principais plataformas virtuais e em nuvem, como Hyper-V, VMWare ESX/ESXi, KVM, AWS e Azure. Se você optar pela implementação de sistemas físicos, virtuais ou uma combinação dos dois, o SMA se enquadra sem contratempos à sua infraestrutura de TI instalada.

Firewall para aplicações web do SMA

O firewall para aplicativos via internet da série SMA100 da SonicWall (*Web Application Firewall* – WAF) permite uma estratégia de defesa aprofundada, aumentando a segurança do perímetro para proteger seus aplicativos via internet em execução em ambiente privado, público ou híbrido. O WAF da série SMA100 oferece proteção de aplicativos da web e proteção de divulgação de informações, ao mesmo tempo que acelera os recursos de entrega de aplicativos da Web que permitem balanceamento de carga com reconhecimento de aplicativos, descarregamento de SSL para resiliência e um envolvimento e experiência digital aprimorados.

Alguns benefícios adicionais:

- Proteção contra vulnerabilidades conhecidas e de dia zero, com reparos virtuais e regras personalizadas

- Defesa contra as vulnerabilidades mais recentes e ameaças delineadas pelo OWASP, incluindo injeção SQL e geração de scripts entre sites (XSS)
- Funciona com acesso com zero confiança, utilizando um navegador da internet para a utilização mais conveniente com qualquer dispositivo público.
- Gerenciamento de sessões e requisitos de autenticação poderosos, como OTP, 2FA e SSO
- Garantia de proteção da alta disponibilidade dos servidores contra ataques de aplicativos DoS/DDoS

Gerenciamento e geração de relatórios

A SonicWall fornece uma plataforma intuitiva de gestão via internet para agilizar o gerenciamento de sistemas, ao mesmo tempo oferecendo recursos extensivos de geração de relatórios. A GUI de fácil utilização representa clareza para a administração de várias máquinas. A gestão unificada de políticas ajuda você a criar e monitorar políticas e configurações de acesso. A configuração com uma única política pode gerenciar seus usuários, dispositivos, aplicativos, dados e redes. Automatize tarefas de rotina e atividades de programação, liberando as equipes de segurança de tarefas repetitivas, para se concentrarem em tarefas estratégicas para a segurança, como a resposta a incidentes.

Qualifique seu departamento de TI para proporcionar a melhor experiência e o acesso mais seguro, conforme o panorama dos usuários. Escolha entre uma série de acessos seguros sem clientes e baseados na internet, para fornecedores e contratados terceirizados, ou um acesso mais tradicional, baseado em clientes e um túnel VPN completo para executivos. Seja para conceder acesso confiável e seguro a 5 usuários a partir de um único centro de dados ou para escalar o acesso a milhares de usuários a partir de centros de dados distribuídos globalmente, o SMA da SonicWall tem uma solução para você.

Saiba mais sobre os produtos de segurança móvel da SonicWall no site: www.sonicwall.com/pt-br/products/remote-access/

Segurança de e-mails

E-mails são fundamentais para as comunicações na sua empresa, mas também são o principal vetor de ataques para ameaças como ransomwares, phishing, comprometimento de e-mails corporativos, bisbilhotagem, spam e vírus. E mais: as normas governamentais agora responsabilizam a sua empresa pela proteção da dados confidenciais e pela garantia da ausência de vazamentos e de que e-mails contendo dados sigilosos ou pessoais sejam intercambiados em total segurança. Seja sua empresa de pequeno ou médio porte, em processo de crescimento, ou um empreendimento de grande porte distribuído, ou ainda um prestador de serviços gerenciados (*Managed Service Provider* – MSP), você precisa de uma maneira econômica de implementar a segurança e criptografia dos e-mails, bem como a escalabilidade para aumentar facilmente sua capacidade – e delegar o gerenciamento em toda a empresa – para unidades de negócios e domínios.

Para gerenciar os custos e recursos, as organizações também estão adotando o Microsoft Office 365 e o Google G Suite. Embora esses produtos possuam funcionalidades de segurança embutidas para combater ameaças avançadas a e-mails, as organizações exigem uma solução de segurança com tecnologia de próxima geração que se integre sem contratempos ao Office 365 e ao G Suíte, para protegê-las contra as ameaças avançadas da atualidade.

Sistemas de segurança de e-mails da SonicWall

Fácil de se instalar e administrar, o SonicWall Email Security foi projetado para se expandir com economia de 10 para 100.000 caixas de e-mail. Ele pode ser implementado como um sistema físico, como um sistema virtual potencializando recursos de computação compartilhados, ou como software – incluindo software otimizado para servidores Microsoft Windows ou servidores de empresas de pequeno porte. Os sistemas físicos de segurança de e-mails da SonicWall são ideais para organizações que precisam de uma solução local dedicada. Nossa solução em múltiplas camadas oferece proteção abrangente para itens recebidos e enviados. Disponível em uma ampla gama de opções de sistemas de hardware que funcionam com até 10.000 usuários por sistema. O SonicWall Email Security também está disponível como sistema virtual ou como um aplicativo de software. É ideal para organizações que requerem a flexibilidade e agilidade que faz parte da virtualização. A solução pode ser configurada para alta disponibilidade de modo subdividido, para gerenciar de forma centralizada e confiável implementações de grande porte.

A solução SonicWall Email Security utiliza tecnologias como a aprendizagem de máquina, heurística, análise de reputação e conteúdo, proteção de URL no momento do clique, e sandboxing para anexos e URLs, proporcionando proteção abrangente para itens recebidos e enviados.

A solução também inclui poderosas normas de autenticação de e-mails para impedir ataques de bisbilhotagem e fraudes em e-mails. Isto inclui uma estrutura de políticas de remetentes (*Sender Policy Framework* – SPF); Mensagens identificadas por chaves de domínios (*Domain Keys Identified Mail* – DKIM); e autenticação de mensagens, relatórios e conformidade com base no domínio (*Domain-based Message Authentication, Reporting and Conformance* – DMARC).

- Interrompa ameaças avançadas antes que cheguem à sua caixa de entrada
- Proteja-se contra fraudes por e-mail e ataques de phishing direcionados
- Obtenha segurança atualizada com inteligência em ameaças em tempo real
- A segurança do seu serviço de e-mails em nuvem (Office 365, G-Suíte)
- Habilite a prevenção de perda de dados e a conformidade dos e-mails
- Fácil gerenciamento e geração de relatórios
- Opções de implementação flexíveis

A administração do E-mail Security é intuitiva, rápida e simples. Você pode delegar o gerenciamento de spam em segurança para o usuário final, ao mesmo tempo mantendo o controle final da fiscalização de segurança. Você também pode gerenciar facilmente contas de usuários e grupos com sincronização multi-LDAP sem contratempos.

A solução também permite a fácil integração ao Office 365 e G-Suite, para defesa contra ameaças avançadas em e-mails.

Para ambientes distribuídos de grande porte, o suporte multiusuários permite a delegação de sub-administradores para gerenciar as configurações de várias unidades organizacionais (como divisões de empresas ou clientes MSP) em uma mesma implementação de segurança de e-mails.

Serviço de segurança de e-mail hospedado da SonicWall

Você pode confiar nos serviços hospedados de rápida implementação e fácil administração para proteger sua organização contra ameaças por e-mail, como ransomwares, ameaças de dia zero, spear phishing e BEC, ao mesmo tempo atendendo aos requisitos legais e de conformidade. Mantenha o mesmo nível de proteção avançada em e-mails com a nossa solução hospedada, que oferece paridade de recursos com sistemas físicos e virtuais. A solução também permite a continuidade de e-mails, para assegurar que os e-mails sejam sempre entregues e a produtividade não seja afetada em caso de quedas de energia ou paralisações programadas dos servidores de e-mail locais ou provedores em nuvem, como o Office 365 e o G-Suite.

A segurança de e-mails hospedada da SonicWall oferece proteção superior, operando em nuvem, contra ameaças recebidas e enviadas, a um preço acessível, previsível, com assinaturas mensais ou anuais flexíveis. Você pode minimizar o tempo e o custo de implementação desde o início, bem como as despesas administrativas, sem comprometer a segurança.

A SonicWall oferece a VARs e MSPs mais oportunidades de concorrência e aumento da receita, ao mesmo tempo minimizando riscos, custos diretos e indiretos. A segurança de e-mails hospedada da SonicWall inclui recursos utilizáveis por MSPs, como sistemas multiusuários robustos, gestão centralizada de múltiplos assinantes, integração ao Office 365, opções de compra flexíveis e automatização.

Saiba mais sobre os produtos de segurança de e-mails da SonicWall no site www.sonicwall.com/pt-br/products/secure-email/cloud-email-security/.

Gestão, geração de relatórios e análises

A SonicWall acredita que uma abordagem conectada para gestão da segurança é fundamental para uma boa prática de segurança preventiva. Essa abordagem também compõe a base para uma governança unificada da segurança, estratégias de conformidade e gestão de riscos. Com as soluções de gerenciamento, relatórios e análises da SonicWall, as organizações obtêm uma plataforma integrada, segura e expansível para estabelecer uma estratégia de resposta e defesa de segurança robusta e uniforme em suas redes com fio, sem fio e multinuvem. Além disso, a adoção integral desta plataforma comum oferece às organizações uma visão profunda de segurança para tomar decisões de segurança informadas e mover-se rapidamente para impulsionar a colaboração, a comunicação e o conhecimento por toda a estrutura de segurança compartilhada.

Gestão de segurança de redes da SonicWall

O SonicWall Network Security Manager (NSM) oferece à sua organização tudo o que ela precisa para ter um sistema de gestão de firewalls unificado. O sistema oferece visibilidade em nível de usuário, controle de dispositivos com base em grupos, e escala ilimitada para gerenciar e prestar serviços de forma centralizada em suas operações de segurança de redes com a SonicWall.

Essas operações incluem a implementação e administração dos todos os dispositivos, grupos de dispositivos e usuários protegidos pelos firewalls, organizando e fiscalizando configurações e políticas de segurança coerentes em todos os ambientes de SD-Branch, SD-WAN, monitorando tudo a partir de um painel de controle dinâmico, com relatórios e análises detalhados. O NSM permite tudo isso em um único console intuitivo nativo em nuvem, que pode ser acessado a partir de qualquer local, com um dispositivo com navegador habilitado.

Para prestadores de serviços, o NSM oferece gerenciamento completo multi-tenant e isolamento do controle de políticas independentes para todos os tenants administrados. Essa separação abrange todos os recursos e funções do gerenciamento via NSM, que determinam a operação dos firewalls de cada usuário. Consequentemente, torna-se possível para cada tenant manter seu próprio grupo de usuários e as respectivas funções, para realizar a administração de grupos de dispositivos, a organização de políticas, e todas as demais tarefas administrativas no âmbito das contas dos tenants designados. Isto abre oportunidades para os MSP/MSSPs aumentarem a agilidade dos serviços de segurança, ao mesmo tempo reduzindo as despesas operacionais e as complexidades do suporte a uma única infraestrutura própria.

SonicWall Analytics

O SonicWall Analytics transforma dados em decisões e decisões em ações que solucionam problemas de segurança e evitam sua recorrência.

Trata-se de um robusto sistema de monitoramento tráfego e serviço de análises, que proporciona uma visão panorâmica do ambiente de segurança de redes. O mecanismo analítico baseado em inteligência agrega, normaliza e contextualiza dados de segurança, incluindo o tráfego nas redes e as atividades dos usuários que fluem pelo firewall e pontos de acesso sem fio, fornecendo ao administrador uma linha de visão da inteligência em ameaças em suas redes e dos usuários em tempo quase real.

Munidas de análises e relatórios criteriosos, as organizações têm a inteligência e a capacidade de identificar e solucionar problemas operacionais com mais eficiência. Os recursos de análise detalhada permitem às equipes de segurança a investigação, análise e

[1] Os SaaS do NSM incluem recursos de geração de relatórios e análises.

[2] O NSM On-Prem requer uma instalação e uma licença separadas do SonicWall Analytics On-Prem para os recursos de geração de relatórios e análises.

ações com base em evidências contra atividades suspeitas ou de risco, bem como do comportamento dos usuários, com maior visibilidade, precisão e velocidade. Também permite que concentrem seu valioso tempo e seus esforços na administração de uma resposta rápida e ações de reparação de danos contra os riscos à segurança mais importantes, em vez de reagirem a todos os eventos.

Além disso, a inclusão de Análises no processo comercial ajuda a operacionalizar as análises, automatizando alertas acionáveis em tempo real; organizando as políticas e os controles de segurança de forma proativa e automatizada; e monitorando os resultados para garantir a segurança.

SonicWall Wireless Network Manager

O SonicWall Wireless Network Manager (WNM) integra globalmente a gestão do SonicWave Access Points e do SonicWall Switches. Como parte do ecossistema do SonicWall Capture Security, o sistema permite visibilidade e gestão unificadas em todas as redes com ou sem fio.

O WNM em nuvem e intuitivo simplifica o acesso, o controle e a solução de problemas em um único painel de controle visual. Cria políticas exclusivas em nível de usuáUsando WNM, os administradores podem criar políticas exclusivas em nível de tenant e implementá-las em diversas localidades e zonas ou fazer drill down em dispositivos gerenciados para dados granulares. O WNM é altamente escalável, capaz de gerenciar desde um único site até redes corporativas globais, com dezenas de milhares de dispositivos gerenciados.

Antes da implementação dos pontos de acesso, um levantamento de locais com redes sem fio pode ajudar a assegurar o desempenho e a produtividade. A ferramenta integrada WNM Wi-Fi Planner ajuda a implementar estrategicamente os pontos de acesso, para otimizar a experiência dos usuários das redes Wi-Fi e evitar erros dispendiosos.

O SonicWave Access Points e SonicWall Switches utilizam Implementação com zero toque, para instalação automática em poucos minutos, utilizando o aplicativo móvel SonicExpress. A prestação do serviço é simples e pode ser feita remotamente, poupando tempo e dinheiro.

Atualizações automáticas de firmware e segurança mantêm os dispositivos gerenciados atualizados. Em caso de queda da conexão com a internet, os pontos de acesso e os switches podem continuar funcionando sem o WNM, assegurando a continuidade dos negócios.

Saiba mais sobre os produtos de gerenciamento e geração de relatórios da SonicWall no site www.sonicwall.com/pt-br/products/management-and-reporting/.

Serviços e Suporte profissionais

Aproveite ao máximo sua solução de segurança de rede da SonicWall e obtenha o suporte que você precisa, quando você precisar. Com o suporte para empresas e os serviços profissionais da SonicWall, você agrega mais valor em longo prazo para a sua solução.

Serviços globais de suporte

Receba o suporte adequado para manter seu negócio fluindo sem transtornos:

Assistência técnica

- **8x5** – De segunda a sexta-feira, das 8:00 h às 17:00 h para ambientes não críticos.
- **7x24** – Suporte 24 horas, inclusive nos fins de semana e feriados, para ambientes críticos para os negócios.

Suporte agregador de valor

- **O Premier Support** oferece às empresas ambientes com um Gerente Técnico de Contas (*Technical Account Manager* - TAM) dedicado. Seu TAM atua em seu nome como um consultor de sua confiança, que trabalha com seu pessoal para ajudar a minimizar paralisações não planejadas, otimizar processos de TI, gerar relatórios operacionais para estimular a eficiência, e será seu único ponto de responsabilidade, para uma experiência de suporte sem transtornos.
- **O engenheiro de suporte dedicado (*Dedicated Support Engineer* - DSE)** representa um recurso de engenharia designado para prestar suporte à conta da sua empresa. Seu DSE conhece e compreende seu ambiente, suas políticas e seus objetivos de TI, para oferecer a você uma solução técnica rápida quando você precisar de suporte.

Serviços profissionais globais

Precisa de ajuda para determinar a melhor solução de segurança para sua empresa, bem como para configurá-la na sua infraestrutura existente? Deixe-nos cuidar disto. Com os Serviços profissionais globais, você terá um único ponto de contato para atender a todas as suas necessidades em termos de implementação e integração. Você recebe serviços desenvolvidos para o seu ambiente exclusivo e assistência com:

- **Planejamento:** Definição de escopo e compreensão dos requisitos dos seus firewalls.
- **Implementação/entrada em operação:** Avaliação e implementação da sua solução.
- **Transferência de conhecimentos:** Uso, administração e manutenção do seu dispositivo.
- **Migração:** Minimização de distúrbios e garantia da continuidade dos negócios.

Os serviços empresariais da SonicWall estão disponíveis nos produtos da série NS*sp*/NS*a*/Série TZ/SMA/Segurança de e-mails/GMS.

Saiba mais:
www.sonicwall.com/pt-br/support/

Conclusão

Conheça os produtos de segurança da SonicWall

Integre seu hardware, software e seus serviços ao melhor sistema de segurança da categoria. Saiba mais no site www.sonicwall.com. Conheça as opções de aquisição e atualização no site www.sonicwall.com/how-to-buy. Experimente as soluções da SonicWall: www.sonicwall.com/trials.

Sobre a SonicWall

A SonicWall fornece segurança cibernética sem limites na era da hiperdistribuição, em uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao conhecer o desconhecido, oferecer visibilidade em tempo real e possibilitar economia disruptiva, a SonicWall preenche as lacunas de cibersegurança para grandes empresas, governos e PMEs em todo o mundo. Para mais informações, visite www.sonicwall.com

Se tiver dúvidas em relação à possível utilização deste material, entre em contato:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Consulte nosso site para obter mais informações:
www.sonicwall.com