Plataforma SonicOS

A arquitetura do SonicOS está no núcleo de todo firewall físico e virtual da SonicWall, inclusive as Séries TZ, NS*a*, NSv e SuperMassive. O SonicOS utiliza nossas tecnologias Reassembly-Free Deep Packet Inspection® (RFDPI) patenteada* de passagem única e baixa latência, além da Real-Time Deep Memory Inspection™ (RTDMI) com patente pendente para fornecer eficiência de alta segurança validada pelo setor, SD-WAN, visualização em tempo real, rede privada virtual (VPN) de alta velocidade e outros recursos eficientes de segurança.

Recursos de firewall

Mecanismo Reassembly-Free Deep Packet Inspection (RFDPI)	
Recurso	Descrição
Reassembly-Free Deep Packet Inspection (RFDPI)	Esse mecanismo de inspeção patenteado, proprietário e de alto desempenho executa análise de tráfego bidirecional baseada em stream, sem proxies ou buffer, para revelar tentativas de intrusão e malware e identificar tráfego de aplicações, independentemente da porta.
Inspeção bidirecional	Verificações simultâneas de ameaças no tráfego de entrada e de saída para garantir que a rede não seja usada para distribuição de malwares e nem se torne uma plataforma de lançamento para ataques, caso uma máquina infectada seja incluída.
Inspeção baseada em fluxo	A tecnologia de inspeção com menos proxy e sem buffer oferece desempenho de latência ultrabaixa para a DPI de milhões de streamings simultâneos na rede, sem introduzir limitações quanto ao tamanho de arquivos e de streaming e podendo ser aplicada a protocolos comuns, assim como a streamings de TCP brutos.
Altamente paralelo e escalável	O design único do mecanismo RFDPI funciona com a arquitetura de vários núcleos para fornecer alta taxa de transferência de DPI e taxas extremamente altas de estabelecimento de novas sessões, permitindo a manipulação de impulsos transitórios de tráfego em redes exigentes.
Inspeção de passagem única	A arquitetura de DPI de passagem única verifica simultaneamente se há identificação de aplicações, intrusões e malware, reduzindo drasticamente a latência de DPI e garantindo que todas as informações sobre ameaças sejam correlacionadas em uma única arquitetura.
Firewall e funcionamento em rede	
Recurso	Descrição
SD-WAN segura	Uma alternativa às tecnologias mais caras, como MPLS, a SD-WAN segura permite que as organizações corporativas distribuídas criem, operem e gerenciem redes seguras de alto desempenho em localidades remotas para o propósito de compartilhamento de dados, aplicações e serviços que utilizam serviços públicos da Internet prontamente disponíveis e de baixo custo.
API REST	Permite que o firewall receba e utilize todos os feeds de inteligência proprietários, do fabricante de equipamento original e de terceiros para combater ameaças avançadas, como ameaças do tipo zero-day, internas mal-intencionadas, de credenciais comprometidas, de ransomware e advanced persistent threats.
Inspeção de pacotes com monitoramento de estado	Todo o tráfego na rede é inspecionado, analisado e colocado em conformidade com as políticas de acesso do firewall.
Alta disponibilidade/organização por clusters	Oferece suporte aos modos Ativo/Passivo (A/P) com sincronização de estado, DPI Ativo/Ativo (A/A)[2] P organização por clusters Ativo/Ativo de alta disponibilidade.[2] DPI Ativo/Ativo descarrega a carga de inspeção profunda de pacote para o appliance passivo para impulsionar a taxa de transferência.
Proteção contra ataque DDoS/DoS	A proteção contra SYN Flood fornece uma defesa contra ataques DOS por meio do uso das tecnologias de proxy da camada 3 SYN e de lista negra da camada 2 SYN. Além disso, ela protege contra DOS/DDoS por meio da proteção de UDP/ICMP flood e limitação da taxa de conexões.
Opções de implementação flexíveis	O firewall pode ser implementado nos modos com fio, NAT de tap de rede ou ponte da camada 2[2].
Balanceamento de carga WAN	Faz o balanceamento de carga de múltiplas interfaces WAN com o uso dos métodos Round Robin, Spillover ou Percentual. Roteamento baseado em políticas Cria rotas baseadas em protocolo para direcionar o tráfego a uma conexão WAN preferencial que tenha a capacidade de executar failback para uma WAN secundária, no caso de uma interrupção.
Qualidade de serviço avançada (QoS)	Garante comunicações críticas com 802.1p, marcação DSCP e remapeamento de tráfego VoIP na rede.
Suporte a gatekeeper H.323 e proxy SIP	Bloqueia chamadas de spam ao exigir que todas as chamadas recebidas sejam autorizadas e autenticadas pelo gatekeeper H.323 ou pelo proxy SIP.

Firewall e funcionamento em rede (continuação)	
Recurso	Descrição
Gerenciamento de switch Dell Série N e Série X simples e em cascata[2]	Gerencie configurações de segurança de portas adicionais, inclusive Portshield, HA, PoE e PoE+, em uma única tela com o uso do painel de firewall management para os switches de rede Série N e Série X da Dell.
Autenticação biométrica	Oferece suporte à autenticação de dispositivo móvel, como reconhecimento de impressão digital, que não pode ser facilmente duplicada ou compartilhada para autenticar de forma segura a identidade do usuário para acesso à rede.
Autenticação aberta e login em rede social	Permita que os usuários usem suas credenciais de serviços de redes sociais, como Facebook, Twitter ou Google+, para fazer login e acessar a Internet e outros serviços convidados por meio de zonas wireless, LAN ou DMZ de um host, com o uso da autenticação pass-through.
Autenticação em múltiplos domínios	Fornece uma maneira simples e rápida de administrar políticas de segurança em todos os domínios de rede. Gerencie uma política individual para um único domínio ou para um grupo de domínios.
Gerenciamento e relatório	
Recurso	Descrição
Gerenciamento baseado em nuvem e local	A configuração e o gerenciamento de appliances SonicWall estão disponíveis na nuvem, com o uso do SonicWall Capture Security Center, e no local, com o uso do SonicWall Global Management System (GMS).
Gerenciamento de dispositivos único e eficiente	Uma interface intuitiva baseada na Web permite uma configuração rápida e prática, além de uma ampla interface de linha de comando e suporte a SNMPv2/3.
Relatório de fluxo de aplicações IPFIX/NetFlow	Exporta dados de análise de tráfego e de uso de aplicações por meio dos protocolos IPFIX ou NetFlow para monitoramento e relatório em tempo real e histórico com ferramentas como o SonicWall Analytics ou outras ferramentas que oferecem suporte a IPFIX e NetFlow com extensões.
Rede virtual privada (VPN)	
Recurso	Descrição
VPN de provisionamento automático	Simplifica e reduz a implementação complexa distribuída de firewall a um esforço trivial ao automatizar o provisionamento inicial do gateway de VPN de local para local entre os firewalls da SonicWall, ao mesmo tempo que a segurança e a conectividade ocorrem de forma instantânea e automática.
VPN IPSec para conectividade entre locais	A VPN IPSec de alto desempenho permite que o firewall aja como um concentrador de VPN para milhares de outros locais grandes, escritórios de filiais ou escritórios residenciais.
Acesso ao cliente remoto por SSL VPN ou IPSec	Utiliza tecnologia SSL VPN sem cliente ou um cliente IPSec simples de gerenciar para acesso fácil a e-mails, arquivos, computadores, sites de intranet e aplicações a partir de diversas plataformas.
Gateway VPN redundante	Ao usar múltiplas WANs, é possível configurar uma VPN primária e secundária para permitir o failover e o failback contínuos e automáticos.
VPN baseada em rotas	A capacidade de executar o roteamento dinâmico sobre links de VPN garante tempo de atividade contínuo no caso de uma falha temporária do túnel VPN, redirecionando o tráfego de modo integrado entre os endpoints por meio de rotas alternativas.
Sensibilidade ao contexto/conteúdo	
Recurso	Descrição
Controle das atividades do usuário	A atividade e a identificação do usuário são disponibilizadas por meio da integração contínua de SSO de AD/LDAP/Citrix/serviços de terminal combinada com as informações abrangentes obtidas através de DPI.
Identificação de tráfego de país por GeoIP	Identifica e controla o tráfego na rede destinado ou proveniente de países específicos para proteger contra ataques de origens conhecidas ou suspeitas de atividade de ameaça ou para investigar tráfego suspeito originário da rede. Capacidade de criar listas personalizadas de países e botnets para substituir um rótulo de país ou de botnet incorreto associado a um endereço IP. Elimina a filtragem indesejada de endereços IP devido a uma classificação indevida.
Correspondência e filtragem de expressão regular	Evita o vazamento de dados ao identificar e controlar o conteúdo que atravessa a rede por meio da correspondência de expressões regulares.

Serviços de assinatura de prevenção contra violação

Capture advanced threat protection[1]	
Recurso	Descrição
Sandboxing com múltiplos mecanismos	A plataforma de sandbox com múltiplos mecanismos, que inclui sandboxing virtualizado, emulação completa do sistema e tecnologia de análise no nível do hypervisor, executa código suspeito e analisa o comportamento, o que fornece uma visibilidade abrangente da atividade mal-intencionada.
Bloqueio até o veredito	Para evitar que arquivos potencialmente mal-intencionados entrem na rede, os arquivos enviados ao serviço de nuvem para análise podem ser retidos no gateway até que um veredito seja determinado.
Análise de uma ampla variedade de tipos de arquivo	Oferece suporte à análise de uma ampla variedade de tipos de arquivos, inclusive programas executáveis (PE), DLL, PDFs, documentos MS Office, arquivos, JAR e APK, além de múltiplos sistemas operacionais, inclusive Windows, Android, Mac OS e ambientes com múltiplos navegadores.
Implementação rápida de assinaturas	Quando um arquivo é identificado como mal-intencionado, uma assinatura é implementada imediatamente nos firewalls com SonicWALL Capture, nos bancos de dados de assinaturas de antivírus de gateway e de IPS e nos bancos de dados de reputação de URL, de IP e de domínio no prazo de 48 horas.
Capture Client	O Capture Client usa um mecanismo estático de inteligência artificial (AI) para determinar as ameaças antes que elas possam ser executadas e reverter a um estado anterior não infectado.
Prevenção contra ameaças criptografadas	
Recurso	Descrição
Descriptografia e inspeção de TLS/SSL	Descriptografa e inspeciona o tráfego TLS/SSL criptografado rapidamente, sem uso de proxy, em busca de malware, intrusões e vazamento de dados, além de aplicar políticas de controle de aplicações, URL e conteúdo para proteger contra ameaças ocultas no tráfego criptografado. Incluídas nas assinaturas de segurança para todos os modelos, exceto SOHO. Vendido como uma licença separada no SOHO.
Inspeção de SSH	A Inspeção detalhada de pacote SSH (DPI-SSH) descriptografa e inspeciona dados que atravessam túneis SSH para evitar ataques que utilizam SSH.
Prevenção contra intrusões[1]	
Recurso	Descrição
Proteção baseada em contramedidas	A alta integração do sistema de prevenção contra intrusões (IPS) utiliza assinaturas e outras contramedidas para verificar o payload de pacotes quanto a vulnerabilidades e exploits, abrangendo um amplo espectro de ataques e vulnerabilidades.
Atualizações automáticas de assinatura	A equipe de pesquisa de ameaças da SonicWall pesquisa e implementa atualizações de forma contínua em uma lista extensiva de contramedidas de IPS que abrange mais de 50 categorias de ataques. As novas atualizações entram em vigor imediatamente, sem a necessidade de reinicialização ou interrupção do serviço.
Proteção do IPS dentro da zona	Impulsiona a segurança interna ao segmentar a rede em múltiplas zonas de segurança com prevenção contra intrusões, o que impede que as ameaças se propaguem para além dos limites da zona.
Detecção e bloqueio de comando e controle (CnC) de botnet	Identifica e bloqueia o tráfego de comando e controle originário de bots na rede local para IPs e domínios que são identificados como propagadores de malware ou são pontos de CnC conhecidos.
Abuso/anomalia de protocolo	Identifica e bloqueia ataques que abusam de protocolos na tentativa de enganar o IPS.
Proteção zero-day	Protege a rede contra ataques de zero day, com constantes atualizações contra os mais recentes métodos e técnicas de exploit, que abrangem milhares de explorações individuais.
Tecnologia contra evasão	A normalização e a decodificação amplas de stream, além de outras técnicas, garantem que as ameaças não passem despercebidas pela rede com o uso de técnicas de evasão nas camadas 2-7.
Prevenção contra ameaças[1]	
Recurso	Descrição
Gateway anti-malware	O mecanismo RFDPI verifica todo o tráfego de entrada, saída e dentro da zona quanto à existência de vírus, cavalos de Troia, keyloggers e outros malwares em arquivos de comprimento e tamanho ilimitados em todas as portas e streams de TCP.
Proteção contra malware no Capture Cloud	Um banco de dados continuamente atualizado de mais de dezenas de milhões de assinaturas de ameaças reside nos servidores em nuvem da SonicWall e é consultado para ampliar os recursos do banco de dados integrado de assinaturas, o que fornece o RFDPI com uma cobertura abrangente de ameaças.
Atualizações de segurança constantes	Atualizações sobre novas ameaças são automaticamente transferidas para firewalls no campo que estejam com os serviços de segurança ativados e entram em vigor imediatamente, sem reinicializações ou interrupções.
Inspeção bidirecional de TCP bruto	O mecanismo RFDPI verifica streams brutos de TCP em qualquer porta e bidirecionalmente para detectar e evitar ameaças de entrada e saída.
Amplo suporte a protocolos	Identifica protocolos comuns, como HTTP/S, FTP, SMTP, SMBv1/v2, entre outros, que não enviam dados em TCP bruto. Decodifica os payloads para a inspeção de malware, mesmo se eles não operarem em portas padrão conhecidas.

Inteligência e controle de aplicações[1]	
Recurso	Descrição
Controle de aplicações	Controla aplicações ou recursos de aplicações individuais que são identificados pelo mecanismo RFDPI em relação a um banco de dados em contínua expansão de milhares de assinaturas de aplicação. Isso aumenta a segurança e a produtividade da rede.
Identificação de aplicações personalizadas	Controla aplicações personalizadas ao criar assinaturas com base em parâmetros específicos ou padrões exclusivos de uma aplicação em suas comunicações de rede. Isso ajuda a obter controle adicional sobre a rede.
Gerenciamento da largura de banda de aplicações	O gerenciamento de largura de banda de aplicações aloca e regula de forma granular a largura de banda disponível para aplicações (ou categorias de aplicações), ao mesmo tempo que inibe o tráfego de aplicações não essenciais.
Controle granular	Controla aplicações (ou componentes específicos de uma aplicação) com base em agendamentos, grupos de usuários, listas de exclusão e uma gama de ações com identificação de usuário de SSO completa por meio da integração de Protocolo LDAP/AD/Serviços de terminal/Citrix.
Filtragem de conteúdo[1]	
Recurso	Descrição
Filtragem de conteúdo interno/externo	Aplique políticas de uso aceitável e bloqueie o acesso a sites HTTP/HTTPS que contêm informações ou imagens ofensivas ou improdutivas com o Content Filtering Service e o Content Filtering Client.
Content Filtering Client aplicado	Estende a aplicação de política para bloquear conteúdo da Internet para dispositivos Windows, Mac OS, Android e Chrome localizados fora do perímetro do firewall.
Controles granulares	Bloqueia conteúdo com o uso de qualquer combinação de categorias. A filtragem pode ser programada pela hora do dia, como durante o horário escolar ou comercial, e aplicada a usuários individuais ou grupos.
Web caching	As classificações de URL são armazenadas em cache localmente no firewall SonicWall para que o tempo de resposta de um acesso posterior a sites acessados com frequência seja apenas uma fração de segundo.
Local CFS Responder	O Local CFS Responder pode ser implementado como um appliance virtual em nuvens privadas com base no VMWare ou Microsoft Hyper-V. Isso fornece a opção de flexibilidade de implementação (VM leve) de banco de dados de classificações de CFS em vários casos de uso de rede de clientes que requerem uma solução local dedicada que acelere os tempos de solicitação e resposta de classificações de CFS, ofereça suporte a um grande número de URLs permitidas/travadas (mais de 100 mil) e adicione até 1.000 firewalls da SonicWall para consultas de classificações de CFS.
Antivírus e antispyware aplicados[1]	
Recurso	Descrição
Proteção em várias camadas	Utiliza os recursos de firewall como a primeira camada de defesa no perímetro, juntamente com proteção de endpoint para bloquear a entrada de vírus na rede por meio de notebooks, pen drives e outros sistemas não protegidos.
Opção de aplicação automatizada	Assegure que todo computador que acesse a rede tenha o software antivírus apropriado e/ou o certificado DPI-SSL instalado e ativo, o que elimina os custos comumente associados ao gerenciamento de antivírus de desktop.
Opção de implementação e instalação automatizada	A instalação e implementação máquina a máquina dos clientes de antivírus e antispyware é automática na rede, o que minimiza a sobrecarga administrativa.
Antivírus de última geração	O Capture Client usa um mecanismo estático de inteligência artificial (AI) para determinar as ameaças antes que elas possam ser executadas e reverter a um estado anterior não infectado.
Proteção contra spyware	A eficiente proteção contra spyware verifica e bloqueia a instalação de uma ampla matriz de programas de spyware em desktops e notebooks antes que eles transmitam dados confidenciais, o que proporciona maior segurança e desempenho de desktop.

[1] Requer assinatura adicional
[2] Série de firewall NSv sem suporte

Sobre nós

A SonicWall tem combatido o setor de crime cibernético há mais de 27 anos, ao defender pequenas, médias e grandes empresas em todo o mundo. Nossa combinação de produtos e parceiros possibilitou uma solução automatizada de detecção e prevenção de violação em tempo real ajustada às necessidades específicas de mais de 500.000 organizações em mais de 215 países e territórios, o que permite que você faça mais negócio com menos preocupações. Para obter mais informações, acesse www.sonicwall.com ou siga-nos no Twitter, no LinkedIn, no Facebook e no Instagram.

Serviços ativados por parceiros

Precisa de ajuda para planejar, implementar ou otimizar sua solução SonicWall? Os Parceiros de serviços avançados da SonicWall são treinados para fornecerem a você serviços profissionais de nível mundial. Saiba mais em www.sonicwall.com/PES.

SONICWALL®

Resumo dos recursos do SonicOS

Firewall
- Inspeção de pacotes com monitoramento de estado
- Reassembly-Free Deep Packet Inspection
- Proteção contra ataque de DDoS (UDP/ICMP/SYN flood)
- Suporte a IPv4/IPv6
- Autenticação biométrica para acesso remoto
- Proxy DNS
- APIs REST

Descriptografia e inspeção de TLS/SSL/SSH[2]
- Inspeção detalhada de pacotes para TLS/SSL/SSH
- Inclusão/exclusão de objetos, grupos ou nomes de hosts
- Controle de SSL
- Controles granulares de DPI SSL por zona ou regra

Capture Advanced Threat Protection[2]
- Real-Time Deep Memory Inspection
- Análise de múltiplos mecanismos baseada em nuvem
- Sandboxing virtualizado
- Análise no nível do hypervisor
- Emulação completa de sistemas
- Análise de uma ampla variedade de tipos de arquivo
- Envio automatizado e manual
- Atualizações de threat intelligence em tempo real
- Bloqueio até o veredito
- Capture Client

Prevenção contra intrusões[2]
- Verificação baseada em assinatura
- Atualizações automáticas de assinatura
- Mecanismo de inspeção bidirecional
- Capacidade de regras granulares de IPS
- Aplicação de GeoIP
- Filtragem de botnet com lista dinâmica
- Correspondência de expressão regular

Antimalware[2]
- Verificação de malware baseada em stream
- Gateway anti-virus
- Gateway anti-spyware
- Inspeção bidirecional
- Sem limitação de tamanho de arquivo
- Banco de dados de malware em nuvem

Identificação de aplicações[2]
- Controle de aplicações
- Gerenciamento da largura de banda de aplicações
- Criação de assinatura de aplicação personalizada
- Prevenção contra vazamento de dados
- Relatórios de aplicação por NetFlow/IPFIX
- Banco de dados de assinaturas de aplicações abrangente

Visualização e análise de tráfego
- Atividade do usuário
- Uso de aplicações/largura de banda/ameaças
- Análise baseada em nuvem

Filtragem de conteúdo da Web HTTP/HTTPS[2]
- Filtragem de URL
- Evasão de proxy
- Bloqueio de palavra-chave
- Filtragem baseada em política (exclusão/inclusão)
- Inserção de cabeçalho HTTP
- Categorias de classificação de CFS de gerenciamento de largura de banda
- Modelo de política unificado com controle de aplicações
- Content Filtering Client

VPN
- SD-WAN segura
- VPN de provisionamento automático
- VPN IPSec para conectividade entre locais
- Acesso remoto ao cliente IPSec e SSL VPN
- Gateway VPN redundante
- Mobile Connect para iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN baseada em rotas (RIP/OSPF/BGP)

Networking
- PortShield
- Jumbo frames
- Path MTU discovery
- Registro em log aprimorado
- Tronco VLAN
- Espelhamento de porta (NS*a* 2650 e acima)
- Layer-2 QoS
- Segurança de portas
- Roteamento dinâmico (RIP/OSPF/BGP)
- Controlador wireless da SonicWall[1]
- Roteamento baseado em políticas (ToS/métrica e ECMP)
- NAT
- Servidor DHCP
- Gerenciamento da largura de banda
- Agregação de links[1] (estática e dinâmica)
- Redundância de porta[1]
- Alta disponibilidade A/P com sincronização de estado
- Organização por clusters A/A[1]
- Balanceamento de carga de entrada/saída
- Ponte de L2,[1] modo com fio/com fio virtual, modo tap e modo NAT
- Failover de WAN 3G/4G[1]
- Roteamento assimétrico
- Common Access Card (CAC)

VoIP
- Controle de QoS granular
- Gerenciamento da largura de banda
- Tráfego de DPI para VoIP
- Suporte a gatekeeper H.323 e proxy SIP

Gerenciamento e monitoramento
- Web GUI
- Command-line interface (CLI)
- SNMPv2/v3
- Gerenciamento centralizado e relatório com o SonicWall Global Management System (GMS)[2]
- Registro
- Exportação de NetFlow/IPFix
- Backup de configuração baseada em nuvem
- Plataforma de análise de segurança BlueCoat
- Visualizador de aplicação e de largura de banda
- Gestão de IPv4 e IPv6
- Relatório off-box (Scrutinizer)
- Tela LCD de gerenciamento[1]
- Gerenciamento de switch Dell Série N e Série X, inclusive switches em cascata[1]

Wireless[1]
- WIDS/WIPS
- Prevenção contra APs invasores
- Roaming rápido (802.11 k/r/v)
- Seleção automática de canal
- Análise do espectro RF
- Visualização de planta
- Visualização de topologia
- Direcionamento de banda
- Beamforming
- Imparcialidade no tempo de transmissão
- Extensor de MiFi
- Cota cíclica de convidados
- Portal LHM de convidados

Wireless integrado (somente na Série TZ)
- Banda dupla (2,4 GHz e 5,0 GHz)
- Padrões wireless 802.11 a/b/g/n/ac
- Prevenção e detecção de intrusão wireless
- Serviços wireless para VM
- Mensagens de pontos de acesso leves
- Segmentação de ponto de acesso virtual
- Portal cativo
- ACL em nuvem

[1] *Sem suporte em firewalls Série NSv*
[2] *Requer assinatura adicional.*

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

Datasheet-SonicOSplatform-US-VG-MKTG4136

SONICWALL®