série SonicWall TZ

prevenção de ameaças integrado e SD-Wan plataforma para organizações / pequenas e médias empresas distribuídas

A série SonicWall TZ permite que empresas de pequeno e médio porte e empresas distribuídas perceber os benefícios de uma solução de segurança integrada que verifica todas as caixas. tecnologia de software-definidas ampla área de rede (SD-WAN) prevenção de ameaças, combinando de alta velocidade e com uma extensa gama de rede e recursos sem fio além de uma instalação simplificada e gerenciamento centralizado, a série TZ oferece uma solução de segurança unificada a um baixo custo total de propriedade .

, Solução flexível de segurança integrada

A fundação da série TZ é SonicOS, sistema operacional rica em recursos da SonicWall. SonicOS inclui um poderoso conjunto de recursos que fornece às organizações a flexibilidade de ajustar essas Management (UTM) firewalls unificado de ameaças aos seus requisitos de rede específica. Por exemplo, a criação de uma rede sem fios segura de alta velocidade é simplificada através de um controlador incorporado sem fio e o suporte para o IEEE

802.11ac padrão ou adicionando nossos pontos de acesso SonicWave 802.11ac Wave 2. Para reduzir o custo ea complexidade da conexão de alta velocidade pontos de acesso wireless e outros Power over Ethernet (PoE) habilitado dispositivos como câmeras IP, telefones e impressoras, o TZ300P e TZ600P fornecer PoE / PoE + poder.

empresas de varejo distribuídas e ambientes de campus pode tirar vantagem das muitas ferramentas no SonicOS para ganhar ainda mais benefícios.

filiais são capazes de trocar informações de forma segura com o escritório central usando rede privada virtual (VPN). Criação de LANs virtuais (VLANs) permite a segmentação da rede em grupos corporativos e de clientes em separado, com regras que determinam o nível de comunicação com dispositivos em outras VLANs. SD-Wan oferece uma alternativa segura para circuitos MPLS caros ao entregar o desempenho da aplicação consistente e disponibilidade. Implantando TZ firewalls para locais remotos é fácil usando Zero-Touch implantação que permite o provisionamento do firewall remotamente através da nuvem.

prevenção de ameaças e desempenho superiores

Nossa visão para segurança de redes em constante evolução paisagem ameaça cibernética de hoje é automatizado, detecção de ameaças em tempo real e prevenção. Através de uma combinação de cloud-based e on-caixa de tecnologias que oferecem proteção aos nossos firewalls que tem sido validados por meio de testes independente de terceiros para a sua eficácia de segurança extremamente elevado. ameaças desconhecidas são enviados para captura Ameaça baseada em nuvem da SonicWall Avançada Protection (ATP) sandbox motor multi- para análise. Melhorar a Captura ATP é a nossa tecnologia de patente pendente Real-Time inspeção profunda de memória (RTDMI ™). Os detecta e blocos de motor RTDMI malware e ameaças de dia zero inspecionando diretamente na memória. tecnologia RTDMI é preciso, minimiza falsos positivos, e identifica e mitiga sofisticados

benefícios:

, Solução flexível de segurança integrada

- Seguro SD-WAN
- SonicOS poderosos do sistema operacional
- wireless 802.11ac de alta velocidade
- Power over Ethernet (PoE / PoE +)
- segmentação de rede com VLANs

prevenção de ameaças e desempenho superiores

- Patente pendente tecnologia de inspeção em tempo real memória profunda
- Tecnologia patenteada remontagem livre de inspeção profunda de pacotes
- On-caixa e prevenção contra ameaças baseada em nuvem
- TLS / descriptografia SSL e inspeção

eficácia de segurança • Indústria validado

- Captura dedicada equipe de pesquisa Labs ameaça
- segurança de endpoint com captura de cliente

Fácil implantação, configuração e gerenciamento contínuo

- Zero-Touch Deployment
- Cloud-based e no local de um gerenciamento centralizado
- linha escalável de firewalls
- Baixo custo total de propriedade

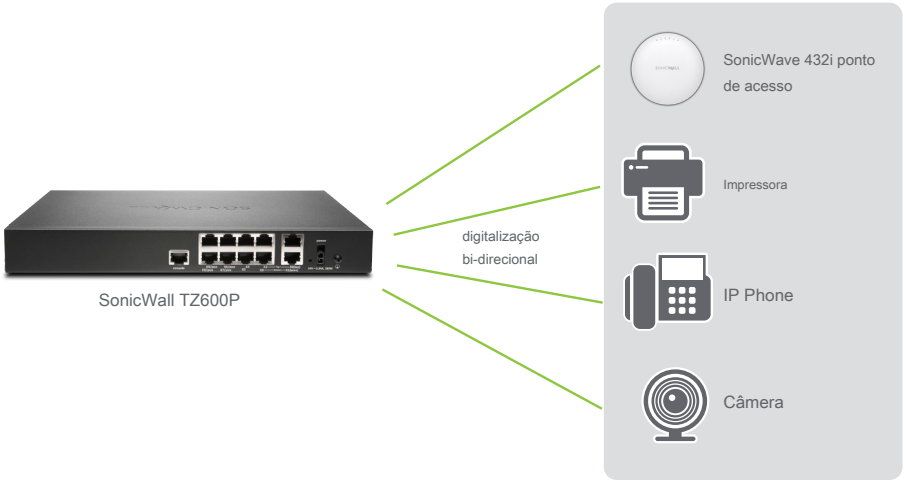
ataques onde armamento do malware é expostas por menos de 100 nanossegundos. Em combinação, o nosso patenteado single-passe remontagem-Free Deep Packet Inspection (RFDPI) motor examina cada byte de cada pacote, inspecionando o tráfego de entrada e saída diretamente no firewall. Ao alavancar Captura ATP com tecnologia RTDMI na captura SonicWall Cloud Platform, além de capacidades sobre-box, incluindo prevenção de intrusão, anti-malware e web / filtragem de URL, TZ firewalls série parada malware, ransomware e outras ameaças no gateway. Para dispositivos móveis usados fora do perímetro da firewall, SonicWall Captura de cliente fornece uma camada adicional de protecção através da aplicação de técnicas avançadas de protecção contra ameaças, tais como aprendizagem e reversão máquina sistema. Captura cliente também aproveita a profunda inspeção de tráfego criptografado TLS (DPI-SSL) em firewalls da série TZ pela instalação e gerenciamento de certificados TLS confiáveis. O crescimento contínuo no uso de criptografia para meios sessões web seguras é firewalls imperativas são capazes de verificar o tráfego criptografado para ameaças. firewalls da série TZ fornecem completa protecção através da realização de descriptografia completo e inspecção de TLS / SSL e SSH ligações encriptadas independentemente da porta ou do protocolo. As pesquisas de firewall para o não cumprimento do protocolo, ameaças, dias nulas, intrusões e critérios ainda definidos por olhando profundamente dentro de cada pacote. Os detecta mecanismo de inspeção profunda de pacotes e impede escondido ataques que a criptografia alavancagem. Ele também bloqueia criptografado de downloads de malware, cessa a propagação de infecções e bancadas de comando e controle (C & C) comunicações e dados exfiltração. regras de inclusão e exclusão permitem o controle total Para personalizar quais o tráfego é submetido a descriptografia e inspeção com base no cumprimento organizacional específica e / ou requisitos legais.

Fácil implantação, configuração e gerenciamento contínuo

SonicWall torna mais fácil de configurar e gerenciar firewalls da série TZ e SonicWave 802.11ac Onda pontos 2 acesso não importa onde você implantá-los. O gerenciamento centralizado, relatórios, licenciamento e análise são tratados através da nossa captura baseado em nuvem Security Center, que oferece o máximo em visibilidade, agilidade e capacidade de governar centralmente todo o ecossistema de segurança SonicWall a partir de um único painel de vidro.

Um componente-chave da captura Security Center é Zero-Touch implantação. Isto simplifica recursos baseados em nuvem e acelera a implantação e provisionamento de firewalls SonicWALL em locais remotos e filiais. O processo requer a intervenção mínima do usuário, e é totalmente automatizado para firewalls operacionalizar em grande escala em apenas alguns passos. Isto reduz significativamente o tempo, custo e complexidade associados com a instalação e configuração, enquanto a segurança e conectividade ocorre instantaneamente e automaticamente. Juntos, a implantação simplificada e configuração juntamente com a facilidade de gerenciamento permitem que as organizações reduzir seu custo total de propriedade e perceber um alto retorno sobre o investimento.

** 802.11ac não está disponível em SOHO / SOHO 250 modelos; SOHO / SOHO 250 modelos suportam 802.11a / b / g / n*



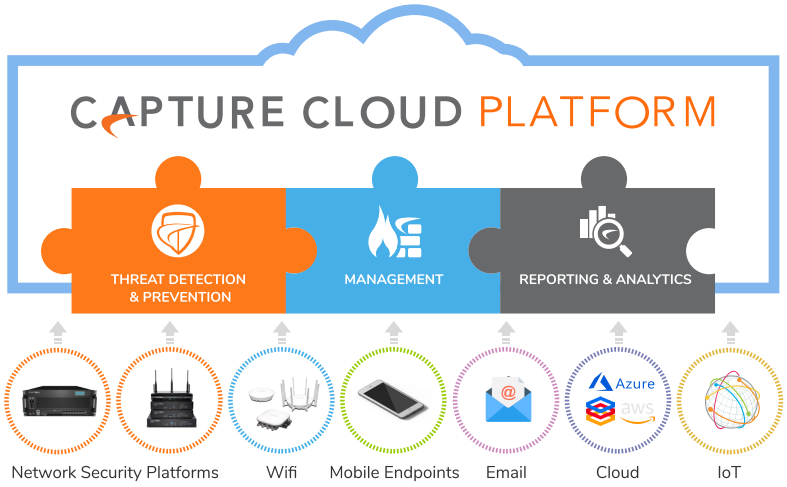
Segurança integrada e energia para seus dispositivos PoE

Fornecer energia para seus dispositivos PoE habilitados sem o custo ea complexidade de um switch Power over Ethernet ou injector. TZ300P e TZ600P firewalls integrar IEEE 802.3af tecnologia para alimentação PoE e PoE + dispositivos, tais como pontos de acesso sem fio, câmeras, telefones IP e muito mais. O firewall examina todo o tráfego vindo e indo para cada dispositivo usando a tecnologia de inspeção profunda de pacotes e, em seguida, remove ameaças nocivas, tais como malware e intrusões, até mesmo conexões mais criptografados.

Capturar Cloud Platform

Captura da SonicWall Cloud Platform oferece gerenciamento baseado em nuvem prevenção de ameaças e rede de mais relatórios e análises para organizações de qualquer tamanho. A inteligência consolida plataforma ameaça recolhidas a partir de várias fontes, incluindo o nosso premiado serviço de rede multi-motor de sandboxing, captura avançada contra ameaças de proteção, bem como mais de 1 milhão de sensores SonicWALL localizados ao redor do globo. Se os dados que entram na rede é encontrado para conter código malicioso anteriormente invisíveis, in-house de captura Labs equipe de pesquisa de ameaças dedicado da SonicWall desenvolve assinaturas que estão armazenados na captura de banco de dados Cloud Platform e implantados para firewalls de clientes para a proteção up-to-date . Novas atualizações em vigor imediatamente, sem reboots ou interrupções. O residente assinaturas no aparelho proteger contra ampla classes de ataques, cobrindo dezenas de milhares de ameaças individuais. Além das contramedidas sobre o aparelho, firewalls TZ também têm acesso contínuo à captura de banco de dados Cloud Platform que se estende a inteligência assinatura bordo com dezenas de milhões de assinaturas.

Além de fornecer prevenção de ameaças, a captura Cloud Platform oferece um único painel de gerenciamento de vidro e os administradores podem facilmente criar, tanto em tempo real e relatórios históricos sobre a atividade da rede.

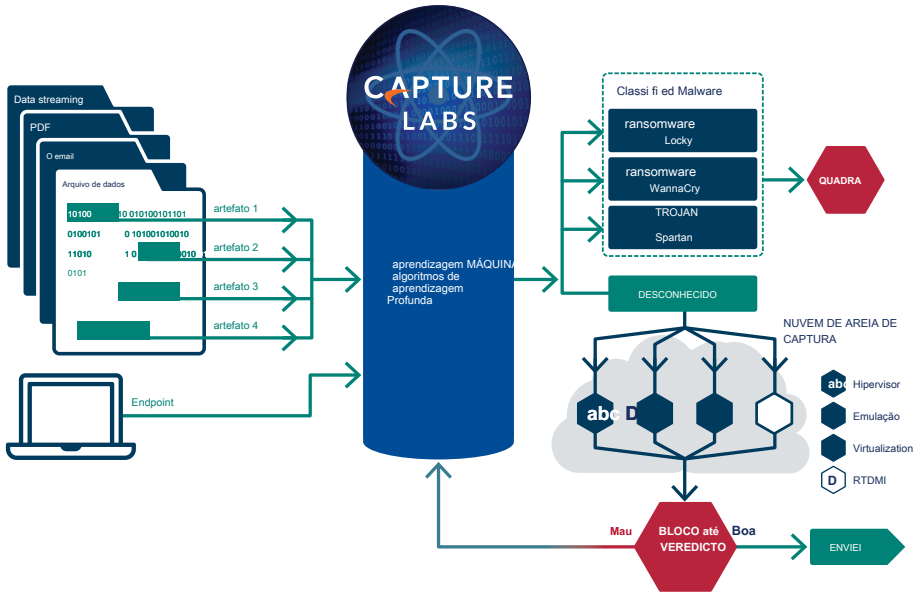


proteção avançada contra ameaças

No centro da SonicWall automatizado, prevenção de violação em tempo real é SonicWall captura avançada de serviço de proteção contra ameaças, uma caixa de areia multi-motor baseado em nuvem que se estende proteção contra ameaças firewall para detectar e prevenir ameaças dia-zero. arquivos suspeitos são enviados para a nuvem, onde são analisados usando algoritmos de aprendizagem de profundidade com a opção de mantê-los na porta de entrada até um veredicto é determinado. A plataforma sandbox motor multi-, que inclui Real-Time inspeção profunda de memória, sandboxing virtualizado, emulação completa do sistema e tecnologia de análise de nível de hypervisor, executa o código suspeito e analisa o comportamento. Quando um arquivo é identificado como malicioso, ele é bloqueado e um hash é imediatamente criado dentro Captura ATP. Logo depois, uma assinatura é enviado para firewalls para evitar follow-on ataques.

O serviço analisa uma ampla gama de sistemas operacionais e tipos de arquivos, incluindo programas executáveis, DLL, PDFs, documentos do MS Office, arquivos JAR e APK.

Para a proteção completa endpoint, a SonicWALL combina a captura de cliente de próxima geração de tecnologia anti-vírus com caixa de areia multi-motor baseado em nuvem da SonicWall.



SONICWALL®

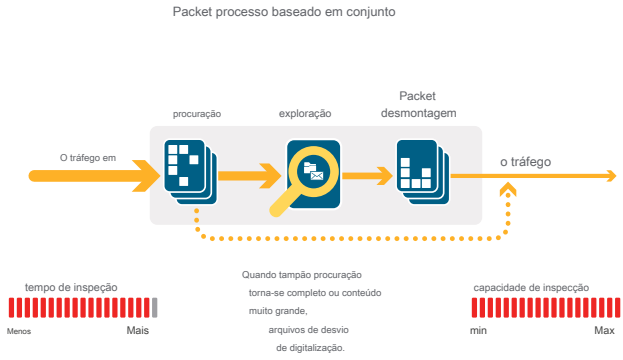
Remontagem-Free motor de Deep Packet Inspection

A SonicWall remontagem-Free Deep Packet Inspection (RFDPI) é uma passagem única, o sistema de inspecção latência baixo que executa córrego baseada-, bi-direccional análise de tráfego a alta velocidade sem proxy ou de tamponamento para tentativas de intrusão efectivamente exposto e descargas de aplicação maliciosos, identificando tráfego independentemente da porta e de protocolo. Este motor de propriedade depende de streaming de inspeção de carga de tráfego para detectar ameaças nas camadas 3-7, e leva

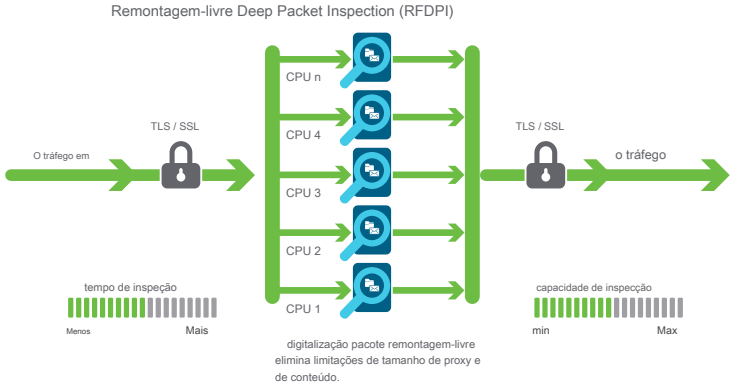
rede córregos através da normalização e descriptografia extenso e repetido, a fim de neutralizar técnicas de evasão avançados que buscam mecanismos de detecção confundir e esgueirar código malicioso na rede.

Uma vez que um pacote sofre o pré-processamento necessário, incluindo TLS / descriptografia SSL, é analisado contra uma única representação de memória, proprietária de três bancos de dados de assinatura: ataques de intrusão, malware e aplicações. O estado de ligação é então avançado para representar a posição do fluxo

em relação a esses bancos de dados até encontrar um estado de ataque, ou outro evento "match", altura em que uma ação pré-definida é tomada. Na maioria dos casos, a conexão é encerrada e eventos de registro e notificação adequados são criados. No entanto, o motor também pode ser configurado apenas de controlo ou, em caso de detecção de aplicação, para fornecer serviços de gestão de Camada 7 de largura de banda para o restante da corrente aplicação, logo que a aplicação é identificada.



arquitetura baseada em proxy competitiva



SonicWall arquitetura baseada em fluxo

gestão e relatórios centralizados

Para organizações altamente regulados querer alcançar uma estratégia de governança de segurança, compliance e gestão de risco totalmente coordenada, SonicWall oferece aos administradores de um sistema unificado, seguro e plataforma extensível para gerenciar firewalls SonicWALL, pontos de acesso sem fio e N-Series Dell e X-Series alterna através de um correlacionada e fluxo de trabalho auditável

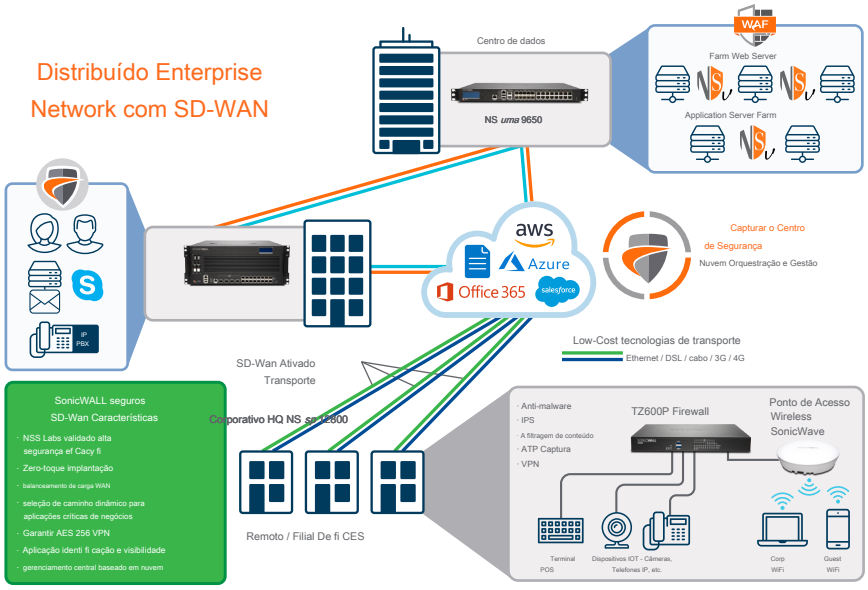
processo. As empresas podem facilmente consolidar a gestão de dispositivos de segurança, reduzir complexidades administrativas e solução de problemas, e governar todos os aspectos operacionais da infra-estrutura de segurança, incluindo gerenciamento centralizado de políticas e execução; monitoramento de eventos em tempo real; actividades do utilizador; identificações de aplicação; fluxo de análise forense e; conformidade e auditoria de relatórios; e mais. Além disso, as empresas atender aos requisitos de gerenciamento de mudanças do firewall por meio da automação de fluxo de trabalho que proporciona a agilidade e confiança para implantar as políticas de firewall certas no momento certo e em conformidade com normas de conformidade. Disponível nas instalações como SonicWall Sistema de Gestão Global e na nuvem como Captura Security Center,

gestão SonicWall e soluções de relatórios fornecem uma maneira coerente para gerir a segurança da rede de processos de negócios e níveis de serviço, simplificando drasticamente a gestão de ciclo de vida de seus ambientes de segurança global em comparação com a gestão de forma dispositivo-a-dispositivo.

SONICWALL®

redes distribuídas

Devido à sua flexibilidade, firewalls da série TZ são ideais tanto para empresas distribuídas e implementações de local único. Em redes distribuídas como os encontrados em organizações de varejo, cada site tem seu próprio firewall TZ que se conecta à Internet muitas vezes através de um provedor local usando uma conexão DSL, cabo ou conexão 3G / 4G. Além de acesso à Internet, cada firewall utiliza uma conexão Ethernet para pacotes de transporte entre locais remotos e as sedes centrais. aplicações de serviços e de SaaS Web como o Office

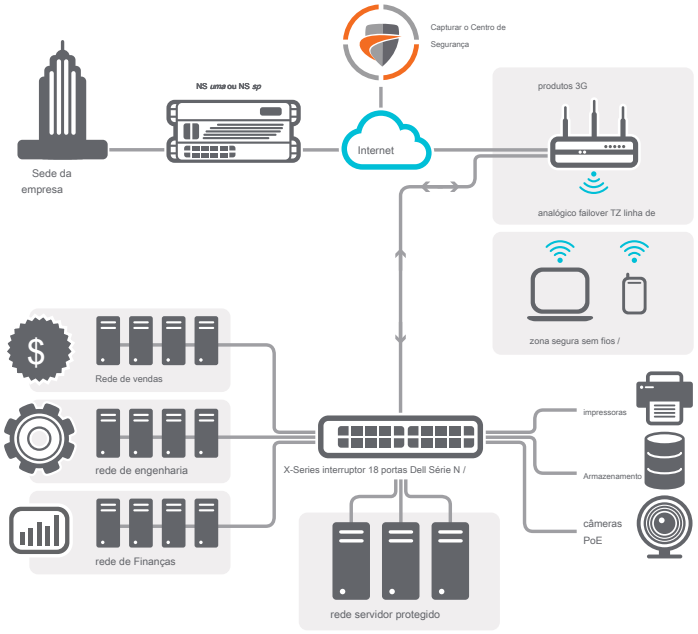


365, Salesforce e outros são servidos a partir do centro de dados. Através de malha tecnologia VPN, os administradores de TI podem criar um hub e falou de configuração para o transporte seguro de dados entre todos os locais.

A tecnologia SD-WAN em SonicOS é um complemento perfeito para firewalls TZ implantado em locais remotos e filiais. Em vez de depender mais tecnologias legadas caros, como MPLS e T1, organizações que usam SD-WAN pode escolher os serviços de Internet pública de custo mais baixo, continuando a alcançar um elevado nível de disponibilidade de aplicações e desempenho previsível.

Capturar o Centro de Segurança

Amarrando o conjunto rede distribuída é a captura baseado em nuvem da SonicWALL Security Center (CSC) que centraliza a implantação, o gerenciamento contínuo e análise em tempo real dos firewalls TZ. Uma característica fundamental do CSC é Zero-implantação Touch. Configuração e implementação de firewalls em vários sites é demorado e requer pessoal no local. No entanto Zero- Toque implantação remove esses desafios, simplificando e acelerando a implantação e provisionamento de firewalls SonicWALL remotamente através da nuvem. Da mesma forma, CSC facilita o gerenciamento contínuo ao fornecer gerenciamento baseado em nuvem único painel-de-vidro para dispositivos SonicWALL na rede. Para a consciência situacional completa do ambiente de segurança de rede, SonicWall Analytics oferece uma vista de painel único para todas as atividades que ocorrem dentro da rede.



Sites individuais

Para implantações de local único, com uma solução de segurança de rede integrada é altamente benéfico. firewalls da série TZ combinar eficácia de alta segurança com opções como built-in wireless 802.11ac e, no caso do TZ300P e TZ600P, PoE / PoE + suporte. o **mesmo motor segurança em nossas NS mid-range *uma* NS série e de gama alta *sp* series é destaque em firewall série** TZ, juntamente com o amplo conjunto de recursos do SonicOS. Configuração e gerenciamento é fácil usando o SonicOS interface intuitiva. Organizações economizar espaço valioso de rack devido ao fator de forma de desktop compacto.

série SonicWall TZ600

Para as empresas emergentes, escritórios de varejo e filiais à procura de segurança, desempenho e opções como 802.3at PoE + suporte a um preço acessível, as redes da SonicWall TZ600 protege com recursos de classe empresarial e desempenho intransigente.

Especificação	série TZ600
transferência de firewall	1.9 Gbps
Ameaça rendimento Prevenção	800 Mbps
rendimento antimalware	800 Mbps
IPS rendimento	1,2 Gbps
máximo de conexões	150.000
Novas ligações / seg	12.000

TZ600P

PoE / PoE + portas (4 PoE / PoE +)

Power LED LED de teste

porta USB (3G / 4G WAN failover)

LEDs indicadores de link e de atividade

módulo de expansão

(configurável)

interruptor 6x1-Gigabit

X0 porta LAN

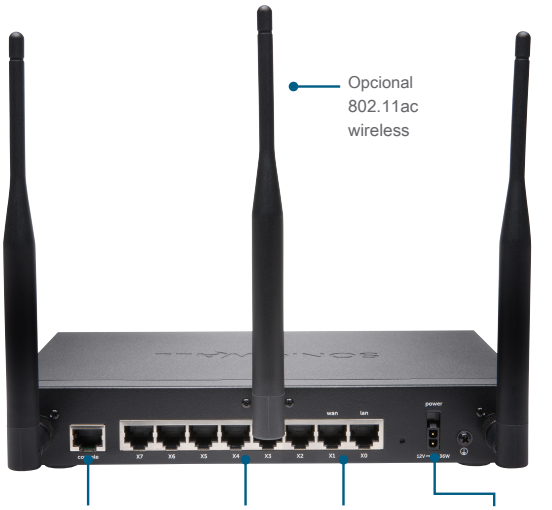
porta X1 WAN

12V DC 2A

série SonicWall TZ500

Para o cultivo de filiais e SMBs, a série SonicWall TZ500 oferece, proteção sem compromisso altamente eficaz com a produtividade da rede e opcional 802.11ac integrada de banda dupla sem fio.

Especificação	série TZ500
transferência de firewall	1,4 Gbps
Ameaça rendimento Prevenção	700 Mbps
rendimento antimalware	700 Mbps
IPS rendimento	1.0 Gbps
máximo de conexões	150.000
Novas ligações / seg	8.000



Opcional 802.11ac wireless

Power LED LED de teste

porta USB (3G / 4G WAN failover)

LEDs indicadores de link e de atividade

Ethernet a porta do painel (configurável)

interruptor 6x1-Gigabit

X0 porta LAN

porta X1 WAN

12V DC 2A

série SonicWall TZ400

Para os pequenos locais de negócios, varejo e escritórios remotos, a série SonicWall TZ400 oferece proteção de classe empresarial. implantação sem fio e flexível está disponível com 802.11ac opcional de banda dupla sem fio integrado ao firewall.

Especificação	série TZ400
transferência de firewall	1.3 Gbps
Ameaça rendimento Prevenção	600 Mbps
rendimento antimalware	600 Mbps
IPS rendimento	900 Mbps
máximo de conexões	150.000
Novas ligações / seg	6.000

Power LED LED de teste | porta USB (3G / 4G WAN failover) | LEDs indicadores de link e de atividade

Opcional 802.11ac wireless

interruptor 5x1-Gigabit Ethernet a porta do painel (configurável) | X0 porta LAN porta X1 WAN | 12V DC 2A

SonicWall TZ350 / TZ300 série

A SonicWall TZ300 e TZ350 série oferecer uma solução tudo-em-um que protege as redes contra ataques avançados. Ao contrário dos produtos voltados ao consumidor, esses firewalls UTM combinam prevenção de intrusão de alta velocidade, anti-malware e conteúdo / URL filtragem além de suporte acesso móvel ampla seguro para laptops, smartphones e tablets, juntamente com opcional wireless 802.11ac integrado. Além disso, os TZ300 ofertas opcionais 802.3at PoE + para poder dispositivos PoE habilitados.

Especificação	série TZ350	série TZ300
transferência de firewall	1.0 Gbps	750 Mbps
Ameaça rendimento Prevenção	335 Mbps	235 Mbps
rendimento antimalware	300 Mbps	200 Mbps
IPS rendimento	400 Mbps	300 Mbps
máximo de conexões	100.000	100.000
Novas ligações / seg	6.000	5.000

TZ300P | PoE / PoE + portas (2 PoE ou um PoE +)

Power LED LED de teste | porta USB (3G / 4G WAN failover) | LEDs indicadores de link e de atividade

Opcional 802.11ac wireless

porta de console | interruptor 3x1-Gigabit Ethernet (configurável) | X0 porta LAN porta X1 WAN | 12V DC 2A

SonicWall SOHO 250 / série SOHO

Para ambientes de pequenos escritórios e casas com e sem fios, a SonicWall SOHO 250 e série SOHO oferecer a mesma proteção classe média alta grandes organizações exigem a um preço mais acessível. Adicionar wireless 802.11n opcional para fornecer funcionários, clientes e convidados com conectividade sem fio segura.

Especificação	SOHO 250 série	série SOHO
transferência de firewall	600 Mbps	300 Mbps
Ameaça Prevenção throughput 200 Mbps		150 Mbps
rendimento antimalware	100 Mbps	50 Mbps
IPS rendimento	250 Mbps	100 Mbps
máximo de conexões	50.000	10.000
Novas ligações / seg	3.000	1.800

Power LED LED de teste

LEDs indicadores de link e de atividade

porta USB (3G / 4G WAN failover)

Ethernet a porta do painel (configurável)

interruptor 3x1-Gigabit

X0 porta LAN porta X1 WAN

12V DC 2A

Parceiros Ativado Serviços

Precisa de ajuda para planejar, implantar ou otimizar sua solução SonicWall? SonicWALL serviços avançados de Parceiros são treinados para lhe fornecer serviços profissionais de classe mundial. Saiba mais em www.sonicwall.com/PES.

Recursos

RFDPI MOTOR	
Característica	Descrição
Remontagem-Free Deep Packet Inspection (RFDPI)	Este alto desempenho, executa motor inspecção patenteadas baseado sequência, análise de tráfego bidireccional, sem proxy ou de tamponamento, a tentativas de intrusão Revelar e software malicioso e para identificar o tráfego aplicação independentemente da porta.
inspecção bi-direccional	Varreduras para ameaças em tráfego de entrada e saída simultaneamente para garantir que a rede não é usada para distribuir malware e não se tornar uma plataforma de lançamento para ataques no caso de uma máquina infectada é trazido para dentro.
inspecção baseada no fluxo	tecnologia de inspeção Proxy-less e não-buffering fornece desempenho ultra-baixa latência para DPI de milhões de rede simultânea córregos sem a introdução de limitações de arquivo e de fluxo de tamanho, e pode ser aplicado em protocolos comuns, bem como fluxos TCP matérias.
Altamente paralela e escalável	O design exclusivo do motor funciona RFDPI com a arquitetura multi-core para proporcionar alta DPI rendimento e extremamente elevadas novas taxas de estabelecimento de sessão para lidar com picos de tráfego em exigentes redes.
inspecção de passagem única	Uma arquitectura de DPI-passe único verifica simultaneamente para maliciosos, intrusões e identificação da aplicação, reduzindo drasticamente a latência DPI e assegurar que toda a informação ameaça é correlacionada numa única arquitectura.

FIREWALL E NETWORKING	
Característica	Descrição
Seguro SD-WAN	Uma alternativa para tecnologias mais caros, como MPLS, Secure SD-WAN permite distribuída organizações empresariais para construir, operar e gerenciar redes seguras e de alto desempenho em locais remotos para fins de compartilhamento de dados, aplicações e serviços que utilizam prontamente disponíveis, de baixa custam os serviços de internet públicas.
APIs de REST	Permite que o firewall para receber e aproveitar toda e qualquer proprietário, fabricante de equipamento original e de terceiros alimentações de inteligência para combater as ameaças avançadas, tais como zero-day, insider malicioso, credenciais comprometidas, ransomware e ameaças persistentes avançadas.
inspeção de pacotes	Todo o tráfego de rede é inspecionado, analisados e postos em conformidade com as políticas de acesso de firewall.
Alta disponibilidade / Cluster	SonicWall TZ500 e TZ600 modelos suportam alta disponibilidade com o Active / Standby com a sincronização do estado. SonicWall TZ300 e TZ400 modelos suportam alta disponibilidade sem sincronização Ativo / Standby. Não há alta disponibilidade em modelos SonicWall SOHO.
protecção ataque DDoS / DoS	SYN proteção contra inundações fornece uma defesa contra ataques DoS usando tanto Layer 3 SYN proxy e Camada 2 SYN tecnologias lista negra. Além disso, ele protege contra DoS / DDoS através de UDP / ICMP protecção contra cheias e taxa de conexão limitante.
suporte IPv6	Internet Protocol versão 6 (IPv6) está em seus estágios iniciais para substituir o IPv4. Com SonicOS, o hardware vai apoiar a filtragem e implementações do modo de fio.
opções flexíveis de implantação	A série TZ pode ser implantado em NAT tradicional, ponte de camada 2, de arame e torneira rede modos.
balanceamento de carga WAN	Load-equilibra várias interfaces WAN usando Round Robin, Spillover ou métodos percentuais.
qualidade avançada de serviço (QoS)	Garante comunicações críticas com 802.1p, marcação DSCP, e remapeamento do tráfego VoIP na rede.
H.323 gatekeeper e SIP suporte a proxy	Bloqueia spam chamadas, exigindo que todas as chamadas recebidas são autorizados e autenticados pelo H.323 gatekeeper ou proxy SIP.
Único e em cascata N-Series Dell e X-Series gerenciamento de comutador	Gerenciar as configurações de portas adicionais, incluindo PortShield, HA, PoE e PoE + segurança, sob um único painel de vidro usando o painel de gerenciamento de firewall para switch de rede N-Series e X-Series da Dell (não disponível no modelo SOHO).
A autenticação biométrica	Suporta a autenticação de dispositivos móveis, tais como reconhecimento de impressões digitais que não podem ser facilmente duplicado ou compartilhado para autenticar com segurança a identidade do usuário para acesso à rede.
Autenticação aberta e login sociais	Permitir que os usuários de hóspedes a usar suas credenciais de serviços de redes sociais como Facebook, Twitter, ou Google+ para fazer login e acessar a Internet e outros serviços ao cliente através de zonas sem fio, LAN ou DMZ um hospedeiro usando pass-through autenticação.
Segurança de rede sem fio	Disponível como uma opção integrada na SonicWall TZ300 através TZ500, a tecnologia sem fio IEEE 802.11ac pode fornecer até 1,3 Gbps de taxa de transferência sem fio com maior alcance e confiabilidade. Opcional 802.11 a / b / g / n é disponível em modelos SonicWall SOHO.

GESTÃO E RELATÓRIO	
Característica	Descrição
Cloud-based e no local de gerenciamento	Configuração e gerenciamento de dispositivos SonicWALL está disponível através da nuvem através da SonicWall Captura Centro de Segurança e on-instalações que utilizam SonicWall Global Management System (GMS).
gerenciamento de dispositivo único e poderoso	Uma interface intuitiva baseada na web permite a configuração rápida e conveniente, além de uma interface de linha de comando abrangente e suporte para SNMPv2 / 3.
IPFIX / NetFlow relatórios de fluxo de aplicação	Exportações análise de tráfego de aplicativos e dados de uso através IPFIX ou NetFlow protocolos para em tempo real e monitoramento histórico e relatórios com ferramentas que suportam IPFIX e NetFlow com extensões.

Rede privada virtual	
Característica	Descrição
VPN-provision Auto	Simplifica e reduz complexo baixo firewall implantação distribuída a um esforço trivial, automatizando o site site-to-inicial VPN gateway de provisionamento entre firewalls SonicWALL enquanto a segurança e conectividade ocorre instantaneamente e automaticamente.
VPN IPSec para IPSec VPN site-to-site de conectividade de alto desempenho permite que a série TZ para agir como um concentrador VPN para milhares de outros grandes sites, filiais ou escritórios domésticos.	
SSL VPN ou cliente de acesso Utiliza clientless SSL VPN remoto tecnologia IPSec ou um fácil de gerenciar cliente IPSec para acesso fácil a e-mail, arquivos, computadores, sites de intranet e aplicativos de uma variedade de plataformas.	
Redundant Gateway de VPN	Ao utilizar múltiplos WANs, uma VPN primário e secundário pode ser configurado para permitir que sem costura, failover automático e failback de todas as sessões VPN.
VPN baseada em rota	A capacidade de realizar o encaminhamento dinâmico através de ligações VPN assegura o tempo de funcionamento contínuo no caso de uma falha temporária túnel VPN, por perfeitamente re-encaminhamento do tráfego entre os terminais através de vias alternativas.
CONTEÚDO / sensibilidade ao contexto	
Característica	Descrição
rastreamento de atividade do usuário	identificação do utilizador e actividade são disponibilizados por meio de emenda AD integração / LDAP / Citrix1 / Terminal Services1 SSO combinado com extensa informação obtida através do DPI.
GeoIP identificação tráfego país	Identifica e controla o tráfego de rede vai ou proveniente de países específicos, quer se proteger contra ataques de origens conhecidas ou suspeitas de atividade ameaça, ou para investigar o tráfego suspeito proveniente da rede. Fornece a capacidade de criar do país do costume e listas de botnets para substituir um país incorreta ou tag Botnet associado a um endereço IP. Elimina filtragem indesejada de endereços IP, devido à má classificação.
filtragem DPI expressão regular	dados impede a fuga através da identificação e controlo do teor de atravessar a rede através de expressões regulares. Fornece a capacidade de criar do país do costume e listas de botnets para substituir um país incorreta ou tag Botnet associado a um endereço IP.
CAPTURA DE PROTECÇÃO ADVANCE AMEAÇA	
Característica	Descrição
Multi-motor sandboxing	A plataforma sandbox multi-motor, que inclui sandboxing virtualizado, emulação completa do sistema e tecnologia de análise de nível de hypervisor, executa o código suspeito e analisa o comportamento, fornecendo visibilidade abrangente para atividades maliciosas.
Inspeção profunda de memória Real-Time (RTDMI)	Esta patente pendente detecta tecnologia baseada em nuvem e bloqueia malware que não apresentam qualquer comportamento malicioso e esconde seu armamento através de criptografia. Ao forçar malwares para revelar seu armamento na memória, o motor RTDMI proativamente detecta e bloqueia o mercado de massa, ameaças de dia zero e malware desconhecido.
Bloco até veredicto	Para evitar arquivos potencialmente maliciosos entrem na rede, arquivos enviados para a nuvem para análise pode ser realizada no gateway até um veredicto é determinado.
Broad tipo de arquivo e análise de tamanho	análise de suportes de uma ampla gama de tipos de arquivos, individualmente ou como um grupo, incluindo programas executáveis (PE), DLL, PDFs, documentos do MS Office, arquivos JAR e APK além de vários sistemas operacionais, incluindo Windows, Android, Mac OS X e ambientes multi-navegador.
rápida implantação de assinaturas	Quando um arquivo é identificado como malicioso, uma assinatura é imediatamente implantado para firewalls com assinaturas SonicWall captura ATP e antivírus de gateway e bancos de dados de assinaturas IPS e o URL, IP e bancos de dados de reputação de domínio dentro de 48 horas.
captura de cliente	Captura de Client é uma plataforma cliente unificada que oferece vários recursos de proteção de endpoint, incluindo proteção contra malware avançado e suporte para visibilidade para o tráfego criptografado. Ele aproveita tecnologias de proteção em camadas, relatórios abrangentes e aplicação da proteção de endpoint.
ENCRIPTADA prevenção de ameaças	
Característica	Descrição
TLS / descriptografia SSL e inspeção	Descriptografa e inspeciona TLS / SSL criptografado tráfego em tempo real, sem proxy, por malware, intrusões e vazamento de dados, e aplica-se a aplicação, URL e políticas de controle de conteúdo, a fim de proteger contra ameaças escondidas em tráfego criptografado. Incluído com assinaturas de segurança para todos os modelos da série TZ, exceto SOHO. Vendido como uma licença separada no SOHO.
inspeção SSH	inspeção profunda de pacotes de SSH (DPI-SSH) decifra e inspecionar os dados atravessando ao longo do túnel SSH para prevenir ataques que SSH alavancagem.
Intrusion Prevention	
Característica	Descrição
proteção baseada em contramedida	sistema de prevenção de intrusão totalmente integrado (IPS) aproveita assinaturas e outras contramedidas para cargas de pacotes de digitalização para vulnerabilidades e explorações, abrangendo um amplo espectro de ataques e vulnerabilidades.
atualizações automáticas	A ameaça SonicWall Research Team investiga continuamente e atualizações implanta a uma extensa lista de IPs contramedidas que cobre mais de 50 categorias de ataque. As novas atualizações tenham efeito imediato, sem qualquer reinicialização ou interrupção do serviço requerido.

Intrusion Prevention continuação	
Característica	Descrição
Intra-zona de protecção IPS	Reforça a segurança interna por segmentar a rede em várias zonas de segurança com prevenção de intrusão, evitando que as ameaças se propaguem para além das fronteiras da zona.
comando de rede de bots e de detecção de controlo (CNC) e bloqueando	Identifica e blocos de comando e controle de tráfego proveniente de bots na rede local para IPs e domínios que são identificados como malware propagação ou são conhecidos pontos CNC.
abuso Protocol / anomalia	Identifica e bloqueia ataques que abusam de protocolos em uma tentativa de sneak após os IPS.
protecção de dia zero	Protege a rede contra ataques de dia zero com atualizações constantes contra as últimas explorar métodos e técnicas que cobrem milhares de explorações individuais.
tecnologia anti-evasão	normalização fluxo extensa, decodificação e outras técnicas de garantir que as ameaças não entrar na rede sem ser detectado através da utilização de técnicas de evasão nas camadas 2-7.
prevenção de ameaças	
Característica	Descrição
Gateway anti-malware	O motor RFDPI verifica todos os inbound, outbound e tráfego intra-zona em busca de vírus, trojans, keyloggers e outros malwares em arquivos de comprimento e tamanho ilimitado em todos os portos e TCP córregos.
Captura Nuvem proteção contra malware	Um banco de dados continuamente atualizado de dezenas de milhões de assinaturas de ameaças reside nos servidores SonicWall nuvem e é referenciado para aumentar as capacidades do banco de dados de assinatura a bordo, proporcionando RFDPI com extensa cobertura de ameaças.
atualizações de segurança em torno do relógio	Novas atualizações de ameaças são automaticamente empurrado para firewalls no campo com os serviços de segurança activa, e entram em vigor imediatamente, sem reboots ou interrupções.
inspeção TCP raw Bi-direcional	O motor RFDPI é capaz de digitalizar fluxos TCP matérias em qualquer porta bi-direcional prevenção de ataques que a esgueirar-se por sistemas de segurança desatualizadas que o foco em garantir algumas portas conhecidas.
apoio extenso protocolo	Identifica protocolos comuns, como HTTP / S, FTP, SMTP, SMBv1 / v2 e outros, que não enviam dados em TCP raw e descodifica cargas úteis para a inspeção de malware, mesmo se eles não correr, portas padrão bem conhecidos.
APLICAÇÃO DE INTELIGÊNCIA E CONTROLE	
Característica	Descrição
controle de aplicativos	aplicações de controle ou recursos de aplicativos individuais, que são identificados pelo motor RFDPI contra um banco de dados em expansão contínua de mais de milhares de assinaturas de aplicativos, para aumentar a segurança da rede e aumentar a produtividade da rede.
identificação aplicativo personalizado	aplicações personalizadas de controle através da criação de assinaturas com base em parâmetros ou padrões únicos para uma aplicação em suas comunicações de rede específicos, a fim de ganhar mais controle sobre a rede.
gerenciamento de banda aplicação	Granular alocar e regular largura de banda disponível para aplicações críticas ou categorias de aplicativos enquanto inibir o tráfego de aplicativos não essencial.
controle granular	aplicações de controlo, ou componentes específicos de uma aplicação, com base em tabelas, grupos de utilizadores, listas de exclusão e uma gama de acções de identificação do utilizador com total de SSO através LDAP / AD / integração de serviços de terminal / Citrix.
A filtragem de conteúdo	
Característica	Descrição
Inside / filtragem de conteúdo fora	Aplicar políticas de uso aceitável e bloquear o acesso a sites HTTP / HTTPS que contenham informações ou imagens que são questionáveis ou improdutiva com Service Filtragem de Conteúdo e Filtragem de Conteúdo do cliente.
Content Filtering aplicadas Cliente	Estender a aplicação de políticas para o conteúdo internet bloco para Windows, Mac OS, Android e dispositivos Chrome localizados fora do perímetro firewall.
controles granulares	Bloquear conteúdo usando as categorias predefinidas ou qualquer combinação de categorias. A filtragem pode ser agendada por hora do dia, como durante escolares ou de negócios horas, e aplicado a usuários individuais ou grupos.
caching web	classificações de URL são armazenadas localmente no SonicWall firewall de modo que o tempo de resposta para posterior acesso a sites frequentemente visitados é apenas uma fração de segundo.
EXECUTADA antivírus e anti-spyware	
Característica	Descrição
protecção multi-camadas	Utilizar as capacidades de firewall como a primeira camada de defesa no perímetro, acoplados com protecção terminal de bloco, os vírus que entram através da rede de computadores portáteis, unidades de polegar e outros sistemas desprotegidos.
opção de execução automática	Certifique-se de cada computador acessar a rede tem o software antivírus apropriado e / ou certificado DPI- SSL instalado e ativo, eliminando os custos normalmente associados com a gestão de antivírus desktop.
implantação automatizada e opção de instalação	Máquina-a-máquina de implantação e instalação de clientes de antivírus e anti-spyware é automática através da rede, minimizando a sobrecarga administrativa.
antivírus de última geração	Captura de cliente usa um motor estática inteligência artificial (AI) para determinar as ameaças antes que possam executar e reverter a um estado não infectado anterior.
proteção contra spyware	varreduras e bloqueia a instalação de uma ampla gama de programas de spyware em desktops e laptops poderosos de proteção contra spyware antes que eles transmitir dados confidenciais, proporcionando maior segurança de desktop e desempenho.

SonicOS resumo recurso

firewall

- inspeção de pacotes
- Remontagem-Free Deep Packet Inspection
- DDoS protecção de ataque (UDP / ICMP / SYN floods)
- apoio IPv4 / IPv6
- A autenticação biométrica para acesso remoto
- proxy DNS
- APIs de REST

SSL / SSH descriptografia e inspection1

- inspeção profunda de pacotes para TLS / SSL / SSH
- Inclusão / exclusão de objetos, grupos ou nomes de host
- controle TLS / SSL
- Granular DPI SSL controla por zona ou regra

Captura de proteção avançada contra ameaças[1]

- Tempo real-inspeção profunda de memória
- análise multi-motor baseado em nuvem
- sandboxing virtualizado
- análise de nível de hypervisor
- emulação completa do sistema
- Broad exame tipo de arquivo
- Automatizado e manual apresentação
- atualizações ameaça de inteligência em tempo real
- Bloco até veredicto
- captura de cliente

prevenção de intrusão[1]

- Verificação baseada em assinaturas
- atualizações automáticas
- inspeção bidirecional
- Granular IPS capacidade regra
- GeoIP / Botnet filtragem[2]
- correspondência de expressão regular

Anti-malware[1]

- verificação de malware baseada em fluxo
- Gateway anti-vírus
- Gateway anti-spyware
- inspecção bi-direccional
- Sem limitação de tamanho de arquivo
- Nuvem de banco de dados de malware

identificação aplicativo[1]

- controle de aplicativos
- gerenciamento de banda aplicação
- criação de assinaturas de aplicativos personalizados
- prevenção de fugas de dados
- relatórios de aplicação sobre NetFlow / IPFIX
- banco de dados de assinatura de aplicação abrangente

visualização de tráfego e análises

- Atividade do usuário
- / Uso de banda / ameaça de aplicação
- analytics baseados em nuvem

HTTP / HTTPS filtragem de conteúdo Web[1]

filtragem • URL

- tecnologia anti-proxy
- bloqueio de palavras-chave
- Com base em políticas de filtragem (exclusão / inclusão)
- Cabeçalho HTTP inserção
- Bandwidth gerenciar CFS categorias de classificação
- modelo de política unificada com controle de aplicativo
- Filtragem de Conteúdo do Cliente

VPN

- VPN-provision Auto
- VPN IPSec para conectividade site-to-site de
- SSL VPN IPSec e acesso remoto cliente
- Redundant Gateway de VPN
- Mobile Connect para iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- baseada em rota VPN (OSPF, RIP, BGP)

Networking

- Seguro SD-WAN

• PortShield

- logging reforçada

• camada 2 QoS

segurança • Porto

- Roteamento dinâmico (RIP / OSPF / BGP)
- controlador sem fio SonicWall
- roteamento baseado em políticas (TOS / métrica e ECMP)
- roteamento assimétrico

• Servidor DHCP

• NAT

gestão • Bandwidth

- Alta disponibilidade - Ativo / Standby com sincronização estado[3]
- Inbound / balanceamento de carga de saída
- Modo de ponte L2, o modo de NAT

failover WAN • 3G / 4G

- Cartão de Acesso Comum de apoio (CAC)

VoIP

controle • Granular QoS

gestão • Bandwidth

• DPI para o tráfego VoIP

- H.323 gatekeeper e SIP suporte a proxy

Gestão e monitorização

• Web GUI

- Comando interface de linha (CLI)

• SNMPv2 / v3

- gestão e relatórios centralizados com captura de Centro de Segurança SonicWall GMS e

• Exploração

• Netflow / IPFIX exportação

- backup de configuração baseado em nuvem
- Aplicação e visualização largura de banda
- gestão de IPv4 e IPv6
- N-Series Dell e gestão interruptor X-Series incluindo switches em cascata[2]

integrada sem fio

- Dual-band (2,4 GHz e 5,0 GHz)
- 802.11 a / b / g / n / ac padrões wireless[2]

• WIDS / WIPS

• serviços ao cliente sem fio

- Leve hotspot de mensagens
- segmentação de ponto de acesso virtual

• Captive portal

• ACL Nuvem

[1] Requer assinatura adicionada
[2] Não disponível no SOHO / SOHO sem fio
[3] alta disponibilidade estado de sincronização apenas em SonicWall TZ500 e modelos SonicWall TZ600

especificações do sistema série SonicWall TZ

FIREWALL GERAL	SÉRIE SOHO	SOHO 250 SERIES	SÉRIE TZ300	SÉRIE TZ350
Sistema operacional	SonicOS			
Interfaces	5x1GbE, 1 USB, 1 Console		5x1GbE, 1 USB, 1 Console	5x1GbE, 1 USB, 1 Console
Power over Ethernet (PoE) apoio	-	-	TZ300P - 2 portas (2 PoE ou um PoE +)	-
Expansão	USB			
Gestão	CLI, SSH, Web UI, Captura Security Center, GMS, APIs de REST			
Sign-On (SSO) Usuários individuais	250	350	500	500
interfaces de VLAN	25			
Os pontos de acesso suportados (máximo)	2	4	8	8
Performance de firewall / VPN	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
rendimento inspecção firewall[1]	300 Mbps	600 Mbps	750 Mbps	1.0 Gbps
Ameaça rendimento Prevenção[2]	150 Mbps	200 Mbps	235 Mbps	335 Mbps
rendimento inspecção aplicação[2]	-	275 Mbps	375 Mbps	600 Mbps
IPS rendimento[2]	100 Mbps	250 Mbps	300 Mbps	400 Mbps
rendimento inspecção antimalware[2]	50 Mbps	100 Mbps	200 Mbps	300 Mbps
TLS inspecção / SSL e rendimento descodificação (DPI SSL)[2]	30 Mbps	40 Mbps	50 Mbps	65 Mbps
rendimento VPN IPsec[3]	100 Mbps	200 Mbps	300 Mbps	430 Mbps
Conexões por segundo	1.800	3.000	5.000	6.000
Máximo de ligações (SPI)	10.000	50.000	100.000	100.000
Máximo de ligações (DPI)	10.000	50.000	90.000	90.000
Máximo de ligações (DPI SSL)	250	25.000	25.000	25.000
VPN	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
Site-to-site VPN túneis	10	10	10	15
VPN IPSec clientes (máximo)	1 (5)	1 (5)	1 (10)	1 (10)
SSL VPN licenças (máximo)	1 (10)	1 (25)	1 (50)	1 (75)
Virtual Assist empacotado (máximo)	-	1 (teste de 30 dias)	1 (teste de 30 dias)	1 (teste de 30 dias)
Criptografia / autenticação	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1, Suite B Criptografia			
troca de chaves	Diffie Hellman grupos 1, 2, 5, 14v			
VPN baseada em rota	RIP, OSPF, BGP			
apoio certificado	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA para SonicWall-to-SonicWall VPN, SCEP			
recursos de VPN	Detecção mortos Peer, DHCP Ao longo VPN, IPSec NAT Traversal, VPN, baseada em rota redundante Gateway de VPN			
plataformas de cliente VPN Global suportado	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, o Windows 8.1 32/64-bit, Windows 10			
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, o Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3 + / Ubuntu 7 + / OpenSUSE			
mobile Connect	maçã® iOS, Mac OS X, Google® androide™, Kindle Fire, Chrome, O Windows 8.1 (embutido)			
SERVIÇOS DE SEGURANÇA	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
serviços Deep Packet Inspection	Gateway Anti-Virus, Anti-Spyware, Prevenção de Intrusão, DPI SSL			
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, palavra-chave e varredura de conteúdo, Comprehensive filtragem baseada sobre os tipos de arquivo, como ActiveX, Java, Cookies de privacidade, permitir / proibir listas			
Comprehensive Anti-Spam Serviço	suportado			
Visualization aplicação	Não	sim	sim	sim
Controle de aplicação	sim	sim	sim	sim
Captura de proteção avançada contra ameaças	Não	sim	sim	sim
NETWORKING	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
atribuição de endereço IP	Estática, (DHCP, PPPoE, L2TP e cliente PPTP), servidor DHCP interno, relé DHCP			
modos NAT	1: 1, 1: muitos, muitos: 1, muitos: muitos, NAT flexível (sobreposição IPs), PAT, o modo transparente			
protocolos de roteamento[4]	BGP4, OSPF, RIPv1 / v2, rotas estáticas, roteamento baseado em políticas			
QoS	prioridade da largura de banda, largura de banda máxima, largura de banda garantida, marcação DSCP, 802.1e (WMM)			

SONICWALL®

Especificações da série SonicWall TZ continuação

NETWORKING CONT	SÉRIE SOHO	SOHO 250 SERIES	SÉRIE TZ300	SÉRIE TZ350
Autenticação	LDAP (vários domínios), XAUTH / RADIUS, SSO, Novell, base de dados do usuário interno		LDAP (vários domínios), XAUTH / RADIUS, SSO, Novell, base de dados do usuário interno, de serviços de terminal, Citrix Cartão de Acesso Comum (CAC)	
banco de dados de usuário local	150			
VoIP	Completa H.323v1-5, SIP			
Padrões	TCP / IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP / IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
certificações	FIPS 140-2 (com Suite B) Nível 2, UC APL, VPNC, IPv6 (Fase 2), ICSA de rede Firewall, ICSA Anti-vírus			
certificações pendentes	Critérios Comuns NDPP (firewall e IPS)			
Cartão de Acesso Comum (CAC)	suportado			
Alta disponibilidade	Não		Ativo / standby	
HARDWARE	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
Fator de forma	Área de Trabalho			
Fonte de energia	24W externa		24W 65W externo externo (TZ300P única)	24W externa
consumo de potência máxima (W)	6,4 / 11,3	6,9 / 11,3	6,9 / 12,0	6,9 / 12,0
Potência de entrada	100 a 240 VAC, 50-60 Hz, 1 A			
dissipação de calor total	21,8 / 38,7 BTU	23,5 / 38,7 BTU	23,5 / 40,9 BTU	23,5 / 40,9 BTU
dimensões	3,6 x 14,1 x 19 centímetros 1,42 x 5,55 x 7,48 em		3,5 x 13,4 x 19 centímetros 1,38 x 5,28 x 7,48 em 3,5 x 13,4 x 19 centímetros	1,38 x 5,28 x 7,48 em
Peso	0,34 kg / 0,75 lbs 0,48 kg / 1,06 lbs		0,73 kg / 1,61 lbs 0,84 kg / 1,85 lbs	0,73 kg / 1,61 lbs 0,84 kg / 1,85 lbs
peso de REEE	0,80 kg / 1,76 lbs 0,94 kg / 2,07 lbs		1,15 kg / 2,53 lbs 1,26 kg / 2,78 lbs	1,15 kg / 2,53 lbs 1,26 kg / 2,78 lbs
Peso	1,20 kg / 2,64 lbs 1,34 kg / 2,95 lbs		1,37 kg / 3,02 lbs 1,48 kg / 3,26 lbs	1,37 kg / 3,02 lbs 1,48 kg / 3,26 lbs
MTBF (em anos)	58,9 / 56,1 (sem fios)	56,1	56,1	56,1
Ambiente (/ Armazenamento Operacional)	32 ° -105 ° F (0 ° -40 ° C) / - 40 ° a 158 ° F (-40 ° a 70 ° C)			
Umidade	5-95% de não-condensação			
REGULAMENTAÇÃO	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
Maior conformidade regulamentar (modelos com fio)	FCC Classe B, Classe CIEM B, CE (EMC, LVD, RSP), C-Tick, VCCI Classe B, UL, CUL, TUV / GS, CB, México CdC pela UL, REEE, REACH, KCC / MSIP		FCC Classe B, Classe CIEM B, CE (EMC, LVD, RSP), C-Tick, VCCI Classe B, UL, CUL, TUV / GS, CB, México CdC pela UL, REEE, REACH, KCC / MSIP	
Maior conformidade regulamentar (modelos sem fio)	FCC Classe B, FCC RF CIEM Classe B, IC RF CE (R & TTE, EMC, LVD, RSP), RCM, VCCI Classe B, MIC / TELEC, UL, CUL, TUV / GS, CB, México CoC pela UL, WEEE, REACH		FCC Classe B, FCC RF CIEM Classe B, IC RF CE (R & TTE, EMC, LVD, RoHS), RCM, VCCI Classe B, MIC / TELEC, UL, CUL, TUV / GS, CB, México CdC pela UL, REEE, ALCANCE	
INTEGRADO WIRELESS	**SÉRIE SOHO**	**SOHO 250 SERIES**	**SÉRIE TZ300**	**SÉRIE TZ350**
Padrões	802.11 a / b / g / n		802.11a / b / g / n / ac (WEP, WPA, WPA2 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS	
bandas de frequência.	802.11a: 5,180-5,825 GHz; 802.11b / g: 2,412-2,472 GHz; 802.11n: 2,412-2,472 GHz, 5,180-5,825 GHz		802.11a: 5,180-5,825 GHz; 802.11b / g: 2,412-2,472 GHz; 802.11n: 2,412-2,472 GHz, 5,180-5,825 GHz; 802.11ac: 2.412-2.472 GHz, 5,180-5,825 GHz	

INTEGRADO WIRELESS	SÉRIE SOHO	SOHO 250 SERIES	SÉRIE TZ300	SÉRIE TZ350
Canais operacionais	802.11a: EUA e Canadá 12, a Europa 11, Japão 4, Singapura 4, Taiwan 4; 802.11b / g: EUA e Canadá 1-11, 1-13 Europa, Japão 1-14 (14-802.11b apenas); 802.11n (2,4 GHz): EUA e Canadá 1-11, 1-13 Europa, Japão 1-13; 802.11n (5 GHz): EUA e Canadá 36-48 / 149-165, Europa 36-48, Japão 36-48, Espanha 36-48 / 52-64;		802.11a: EUA e Canadá 12, a Europa 11, Japan 4, Singapura 4, Taiwan 4; 802.11b / g: EUA e Canadá 1-11, 1-13 Europa, Japão 1-14 (14-802.11b apenas); 802.11n (2,4 GHz): EUA e Canadá 1-11, 1-13 Europa, Japão 1-13; 802.11n (5 GHz): EUA e Canadá 36-48 / 149-165, Europa 36-48, Japão 36-48, Espanha 36-48 / 52-64; 802.11ac: EUA e Canadá 36- 48 / 149-165, Europa 36-48, Japão 36-48, Espanha 36-48 / 52-64	
potência de saída de transmissão	Com base no domínio regulamentar especificado pelo administrador do sistema			
controle de potência de transmissão	suportado			
As taxas de dados suportadas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps per canal		802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps por canal; 802.11ac: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 86,7, 96,3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32,5, 65, 97,5, 130, 195, 260, 292,5, 325, 390, 433,3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866,7 Mbps por canal	
espectro de tecnologia de modulação	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Espalhamento directo Sequência Espectro (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM) / Espectro de Espalhamento directo Sequência (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)		802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Espalhamento directo Sequência Espectro (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM) / Espectro de Espalhamento directo Sequência (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	

** Uso futuro.*

[1] Metodologias de testes: desempenho máximo com base no RFC 2544 (para firewall). O desempenho real pode variar dependendo das condições da rede e dos serviços ativados.

[2] Ameaça Prevenção / GatewayAV / Anti-Spyware / IPS rendimento medido utilizando padrão da indústria Spirent WebAvalanche HTTP teste de desempenho e ferramentas de teste Ixia. Testes feitos com vários fluxos através de múltiplos pares de porta. Ameaça Prevenção de fluxo medido com gateway AV, Anti-Spyware, IPS e de controlo de aplicação activado.

[3] VPN fluxo medido usando o tráfego de UDP em 1280 bytes tamanho do pacote aderindo a RFC 2544. Todas as especificações, características e disponibilidade estão sujeitas a mudanças.

[4] BGP é disponível apenas em SonicWall TZ400, TZ500 e TZ600.

[5] Todos TZ integrado modelos sem fio pode suportar 2,4 GHz ou banda de 5GHz. Para suporte dual-band, utilize produtos de ponto de acesso sem fio da SonicWALL

especificações do sistema série SonicWall TZ continuação

FIREWALL GERAL	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Sistema operacional		SonicOS	
Interfaces	7x1GbE, 1 USB, 1 Console	8x1GbE, 2 USB, 1 Console	10x1GbE, 2 USB, 1 Console, Slot 1 de expansão
Power over Ethernet (PoE) apoio	-	-	TZ600P - 4 portas (4 PoE ou 4 PoE +)
Expansão	USB	2 USB	Slot de expansão (traseira) *, 2 USB
Gestão	CLI, SSH, Web UI, Captura Security Center, GMS, APIs de REST		
Sign-On (SSO) Usuários individuais	500	500	500
interfaces de VLAN	50	50	50
Os pontos de acesso suportados (máximo)	16	16	24
Performance de firewall / VPN	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
rendimento inspecção firewall[1]	1.3 Gbps	1,4 Gbps	1.9 Gbps
Ameaça rendimento Prevenção[2]	600 Mbps	700 Mbps	800 Mbps
rendimento inspecção aplicação[2]	1,2 Gbps	1.3 Gbps	1.8 Gbps
IPS rendimento[2]	900 Mbps	1.0 Gbps	1,2 Gbps
rendimento inspecção antimalware[2]	600 Mbps	700 Mbps	800 Mbps
TLS inspecção / SSL e rendimento descodificação (DPI SSL)[2]	150 Mbps	200 Mbps	300 Mbps
rendimento VPN IPsec[3]	900 Mbps	1.0 Gbps	1.1 Gbps
Conexões por segundo	6.000	8.000	12.000
Máximo de ligações (SPI)	150.000	150.000	150.000
Máximo de ligações (DPI)	125.000	125.000	125.000
Máximo de ligações (DPI SSL)	25.000	25.000	25.000
VPN	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Site-to-site VPN túneis	20	25	50
VPN IPSec clientes (máximo)	2 (25)	2 (25)	2 (25)
SSL VPN licenças (máximo)	2 (100)	2 (150)	2 (200)
Virtual Assist empacotado (máximo)	1 (teste de 30 dias)	1 (teste de 30 dias)	1 (teste de 30 dias)
Criptografia / autenticação	DES, 3DES, AES (128, 192, 256 bits) / MD5, SHA-1, Suite B Criptografia		
troca de chaves	Diffie Hellman grupos 1, 2, 5, 14v		
VPN baseada em rota	RIP, OSPF, BGP		
apoio certificado	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA para SonicWall-to- SonicWall VPN, SCEP		
recursos de VPN	Detecção mortos Peer, DHCP Ao longo VPN, IPSec NAT Traversal, VPN, baseada em rota redundante Gateway de VPN		
plataformas de cliente VPN Global suportado	Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, o Windows 8.1 32/64-bit, Windows 10		
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, o Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3 + / Ubuntu 7 + / OpenSUSE		
mobile Connect	maçã® iOS, Mac OS X, Google® Android ™, Kindle Fire, o Chrome, o Windows 8.1 (embutido)		
SERVIÇOS DE SEGURANÇA	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
serviços Deep Packet Inspection	Gateway Anti-Virus, Anti-Spyware, Prevenção de Intrusão, DPI SSL		
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, palavra-chave e varredura de conteúdo, Comprehensive filtragem baseada em tipos de arquivo tais como ActiveX, Java, Cookies de privacidade, permitir / proibir listas		
Comprehensive Anti-Spam Serviço	suportado		
Visualization aplicação	sim	sim	sim
Controle de aplicação	sim	sim	sim
Captura de proteção avançada contra ameaças	sim	sim	sim
NETWORKING	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
atribuição de endereço IP	Estática, (DHCP, PPPoE, L2TP e cliente PPTP), servidor DHCP interno, relé DHCP		
modos NAT	1: 1, 1: muitos, muitos: 1, muitos: muitos, NAT flexível (sobreposição IPs), PAT, o modo transparente		
protocolos de roteamento[4]	BGP[4], OSPF, RIPv1 / v2, rotas estáticas, roteamento baseado em políticas		
QoS	prioridade da largura de banda, largura de banda máxima, largura de banda garantida, marcação DSCP, 802.1e (WMM)		

SONICWALL®

especificações do sistema série SonicWall TZ continuação

NETWORKING	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Autenticação	LDAP (vários domínios), XAUTH / RADIUS, SSO, Novell, base de dados do usuário interno, Terminal Services, Citrix, Cartão de Acesso Comum (CAC)		
banco de dados de usuário local	150		250
VoIP	Completa H.323v1-5, SIP		
Padrões	TCP / IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP / IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3		
certificações	FIPS 140-2 (com Suite B) Nível 2, UC APL, VPNC, IPv6 (Fase 2), ICSA de rede Firewall, ICSA Anti-vírus		
certificações pendentes	Critérios Comuns NDPP (firewall e IPS)		
Cartão de Acesso Comum (CAC)	suportado		
Alta disponibilidade	Ativo / standby	Ativo / Standby com a sincronização com estado	
HARDWARE	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Fator de forma	Área de Trabalho		
Fonte de energia	24W externa	36W externa	60W externo 180W externo (TZ600P única)
consumo de potência máxima (W)	9,2 / 13,8	13,4 / 17,7	16,1
Potência de entrada	100-240 VAC, 50-60 Hz, 1 A		
dissipação de calor total	31,3 / 47,1 BTU	45,9 / 60,5 BTU	55,1 BTU
dimensões	3,5 x 13,4 x 19 centímetros 1,38 x 5,28 x 7,48 em	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,86 em	3,5 x 18 x 28 cm 1,38 x 7,09 x 11,02 em
Peso	0,73 kg / 1,61 lbs 0,84 kg / 1,85 lbs	0,92 kg / 2,03 lbs 1,05 kg / 2,31 lbs	1,47 kg / 3,24 lbs
peso de REEE	1,15 kg / 2,53 lbs 1,26 kg / 2,78 lbs	1,34 kg / 2,95 lbs 1,48 kg / 3,26 lbs	1,89 kg /4.16 lbs
Peso	1,37 kg / 3,02 lbs 1,48 kg / 3,26 lbs	1,93 kg / 4,25 lbs 2,07 kg / 4,56 lbs	2,48 kg / 5,47 lbs
MTBF (em anos)	54,0	40,8	18,4
Ambiente (/ Armazenamento Operacional)	32 ° -105 ° F (0 ° -40 ° C) / - 40 ° a 158 ° F (-40 ° a 70 ° C)		
Umidade	5-95% de não-condensação		
REGULAMENTAÇÃO	**SÉRIE TZ400**	**SÉRIE TZ500**	**SÉRIE TZ600**
Maior conformidade regulamentar (modelos com fio)	FCC Classe B, Classe CIEM B, CE (EMC, LVD, RSP), C-Tick, VCCI Classe B, UL, CUL, TUV / GS, CB, México CdC pela UL, REEE, ALCANCE, KCC / MSIP	FCC Classe B, Classe CIEM B, CE (EMC, LVD, RSP), C-Tick, VCCI Classe B, UL, CUL, TUV / GS, CB, México CdC pela UL, REEE, ALCANCE, BSMI, KCC / MSIP	FCC classe A, classe CIEM A, CE (EMC, LVD, RSP), C-Tick, VCCI Classe A, UL cUL, TUV / GS, CB, México CdC pela UL, REEE, REACH, KCC / MSIP
Maior conformidade regulamentar (modelos sem fio)	FCC Classe B, FCC RF CIEM Classe B, IC RF CE (R & TTE, EMC, LVD, RSP), RCM, VCCI Classe B, MIC / TELEC, UL, CUL, TUV / GS, CB, México CdC pela UL, WEEE, REACH	FCC Classe B, FCC RF CIEM Classe B, IC RF CE (R & TTE, EMC, LVD, RSP), RCM, VCCI Classe B, MIC / TELEC, UL, CUL, TUV / GS, CB, México CdC pela UL, WEEE, REACH	-

SONICWALL®

INTEGRADO WIRELESS	SÉRIE TZ400	SÉRIE TZ500	SÉRIE TZ600
Padrões	802.11a / b / g / n / ac (WEP, WPA, WPA2, 802,11, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS		-
bandas de frequência[4]	802.11a: 5,180-5,825 GHz; 802.11b / g: 2,412-2,472 GHz; 802.11n: 2,412-2,472 GHz, 5,180-5,825 GHz; 802.11ac: 2.412-2.472 GHz, 5,180-5,825 GHz		-
Canais operacionais	802.11a: EUA e Canadá 12, a Europa 11, Japão 4, Singapura 4, Taiwan 4; 802.11b / g: EUA e Canadá 1-11, 1-13 Europa, Japão 1-14 (14-802.11b apenas); 802.11n (2,4 GHz): EUA e Canadá 1-11, 1-13 Europa, Japão 1-13; 802.11n (5 GHz): EUA e Canadá 36-48 / 149-165, Europa 36-48, Japão 36-48, Espanha 36-48 / 52-64; 802.11ac: EUA e Canadá 36-48 / 149-165, Europa 36-48, Japão 36-48, Espanha 36-48 / 52-64		-
potência de saída de transmissão	Com base no domínio de regulação especificada pelo sistema administrador		-
controle de potência de transmissão	suportado		-
As taxas de dados suportadas	802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11b: 1, 2, 5,5, 11 Mbps por canal; 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps por canal; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135, 150 Mbps por canal; 802.11ac: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 86,7, 96,3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32,5, 65, 97,5, 130, 195, 260, 292,5, 325, 390, 433,3, 65, 130, 195, 260, 390, 520, 585, 650, 780, 866,7 Mbps por canal		-
espectro de tecnologia de modulação	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Espalhamento directo Sequência Espectro (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM) / Espectro de Espalhamento directo Sequência (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)		-

produtos	SKU
SOHO com TotalSecure 1 ano	01-SSC-0651
SOHO Wireless-N com TotalSecure 1 ano	01-SSC-0653
SOHO 250 com 1 ano TotalSecure Advanced Edition	02-SSC-1815
SOHO 250 Wireless-AC com 1 ano TotalSecure Advanced Edition	02-SSC-1824
TZ300 com 1 ano TotalSecure Advanced Edition	01-SSC-1702
TZ300 Wireless-AC com 1 ano TotalSecure Advanced Edition	01-SSC-1703
TZ300P com 1 ano TotalSecure Advanced Edition	02-SSC-0602
TZ350 com 1 ano TotalSecure Advanced Edition	02-SSC-1843
TZ350 Wireless-AC com 1 ano TotalSecure Advanced Edition	02-SSC-1851
TZ400 com 1 ano TotalSecure Advanced Edition	01-SSC-1705
TZ400 Wireless-AC com 1 ano TotalSecure Advanced Edition	01-SSC-1706
TZ500 com 1 ano TotalSecure Advanced Edition	01-SSC-1708
TZ500 Wireless-AC com 1 ano TotalSecure Advanced Edition	01-SSC-1709
TZ600 com 1 ano TotalSecure Advanced Edition	01-SSC-1711
TZ600P com 1 ano TotalSecure Advanced Edition	02-SSC-0600
opções de alta disponibilidade (cada unidade deve ser do mesmo modelo)	
TZ500 High Availability	01-SSC-0439
TZ600 High Availability	01-SSC-0220

Serviços	SKU
Para SonicWall Series SOHO	
Comprehensive Gateway Security Suite - Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	01-SSC-0688
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	01-SSC-0670
Content Filtering Service (1 ano)	01-SSC-0676
Comprehensive Anti-Spam de Serviços (1-year)	01-SSC-0682
Suporte 24x7 (1 ano)	01-SSC-0700
Para SonicWall SOHO Series 250	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	02-SSC-1726
Captura avançada proteção contra ameaças para SOHO 250 (1-year)	02-SSC-1732
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	02-SSC-1750
Content Filtering Service (1 ano)	02-SSC-1744
Comprehensive Anti-Spam de Serviços (1-year)	02-SSC-1823
Suporte 24x7 (1 ano)	02-SSC-1720
Para SonicWall Series TZ300	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	01-SSC-1430
Captura Ameaça Avançada Proteção para TZ300 (1 ano)	01-SSC-1435
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	01-SSC-0602
Content Filtering Service (1 ano)	01-SSC-0608
Comprehensive Anti-Spam de Serviços (1-year)	01-SSC-0632
Suporte 24x7 (1 ano)	01-SSC-0620

informações sobre pedidos SonicWall TZ Series

Para SonicWall Series TZ350	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	02-SSC-1773
Captura Ameaça Avançada Proteção para TZ350 (1 ano)	02-SSC-1779
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	02-SSC-1797
Content Filtering Service (1 ano)	02-SSC-1791
Comprehensive Anti-Spam de Serviços (1-year)	02-SSC-1809
Suporte 24x7 (1 ano)	02-SSC-1767
Para SonicWall Series TZ400	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	01-SSC-1440
Captura Ameaça Avançada Proteção para TZ400 (1 ano)	01-SSC-1445
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	01-SSC-0534
Content Filtering Service (1 ano)	01-SSC-0540
Comprehensive Anti-Spam de Serviços (1-year)	01-SSC-0561
Suporte 24x7 (1 ano)	01-SSC-0552
Para SonicWall Series TZ500	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	01-SSC-1450
Captura Ameaça Avançada Proteção para TZ500 (1 ano)	01-SSC-1455
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	01-SSC-0458
Content Filtering Service (1 ano)	01-SSC-0464
Comprehensive Anti-Spam de Serviços (1-year)	01-SSC-0482
Suporte 24x7 (1 ano)	01-SSC-0476
Para SonicWall Series TZ600	
Avançada Gateway Security Suite - Captura ATP, Threat Prevention, Filtragem de Conteúdo e 24x7 Support (1 ano)	01-SSC-1460
Captura Ameaça Avançada Proteção para TZ600 (1 ano)	01-SSC-1465
Gateway Anti-Virus, Prevenção de Intrusão e Controle de Aplicação (1 ano)	01-SSC-0228
Content Filtering Service (1 ano)	01-SSC-0234
Comprehensive Anti-Spam de Serviços (1-year)	01-SSC-0252
Suporte 24x7 (1 ano)	01-SSC-0246

números de modelo de regulamentação

SOHO / SOHO sem fio	APL31-0B9 / APL41-0BA
SOHO 250 / SOHO 250 sem fio	APL41-0D6 / APL41-0BA
TZ300 / TZ300 Wireless / TZ300P	APL28-0B4 / APL28-0B5 / APL47-0D2
TZ350 / TZ350 sem fio	APL28-0B4 / APL28-0B5
TZ400 / TZ400 sem fio	APL28-0B4 / APL28-0B5
TZ500 / TZ500 sem fio	APL29-0B6 / APL29-0B7
TZ600 / TZ600P	APL30-0B8 / APL48-0D3

Sobre SonicWall

SonicWall tem vindo a lutar a indústria cibercriminoso por mais de 27 anos defendendo pequenas e médias empresas, empresas e agências governamentais em todo o mundo. Apoiada por pesquisa da SonicWall captura Labs, nossa premiada, detecção de violação em tempo real e soluções de prevenção de garantir mais de um milhão de redes e seus e-mails, aplicativos e dados, em mais de 215 países e territórios. Estas organizações executar de forma mais eficaz e temer menos sobre segurança. Para mais informações visite www.sonicwall.com ou siga-nos no Twitter , LinkedIn , Facebook e Instagram.

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