A série SonicWALL Network Security Appliance

SEGURANÇA DE REDE

Proteção de gerenciamento unificado de ameaças (UTM) de próxima geração

- **Segurança de próxima geração do SonicWALL**
- **Hardware escalável de vários núcleos e Reassembly-Free Deep Packet Inspection™**
- **Recursos de monitoramento de estado de alta disponibilidade e equilíbrio de carga**
- **Alto desempenho e custo total de propriedade reduzido**
- **Recursos avançados de redes e serviços de roteamento**
- **Recursos de Voz por IP (VoIP) baseados em padrões**
- **Serviços de rede local sem-fio (WLAN) seguros e distribuídos**
- **Qualidade de serviço (QoS) incorporada**

Organizações de todos os tamanhos dependem de suas redes para acessar aplicativos internos e externos com funções cruciais. Embora as empresas continuem se beneficiando enormemente dos avanços em redes, estão cada vez mais expostas a ataques sofisticados e com finalidades financeiras, projetados para interromper as comunicações, degradar o desempenho e comprometer a segurança dos dados.

Ataques maliciosos penetram firewalls de inspeção de pacotes com monitoramento de estado desatualizados através da exploração dos níveis mais altos de rede. Produtos unitarefa adicionam camadas de segurança, mas são caros, difíceis de gerenciar, limitados no que diz respeito ao controle da má-utilização da rede e ineficazes contra os ataques combinados mais recentes. A série SonicWALL® Network Security Appliance (NSA) revoluciona a segurança de rede, utilizando um projeto inovador de vários núcleos e a tecnologia patenteada Reassembly-Free Deep Packet Inspection™ (RFDPI)* que oferece proteção completa sem prejudicar o desempenho da rede. Esta plataforma foi disponibilizada pela primeira vez na série SonicWALL E-Class NSA, e agora está acessível a organizações de médio porte.

A série NSA supera as limitações das soluções de segurança existentes pela varredura integral de cada pacote em busca de ameaças atuais internas e externas em tempo real. Projetada à partir de uma plataforma de processamento de vários núcleos e alta velocidade, a série NSA permite uma inspeção profunda de pacotes sem impacto negativo no desempenho de redes e aplicativos com funções cruciais.

A série NSA aplica o gerenciamento unificado de ameaças (UTM) de próxima geração contra uma abrangente série de ataques, combinando prevenção de intrusões, antivírus e proteção contra programas espiões com o controle de nível de aplicativo do SonicWALL Application Firewall. Com roteamento avançado, alta disponibilidade de monitoramento de estado e tecnologia de IPSec e SSL VPN de alta velocidade, a série NSA acrescenta segurança, confiabilidade, funcionalidade e produtividade a sedes e filiais, e redes de empresas distribuídas de médio porte, minimizando, ao mesmo tempo, o custo e a complexidade.

Composta pelo **SonicWALL NSA 240, 2400, NSA 3500, NSA 4500 e NSA 5000**, a série NSA oferece uma variedade de soluções escaláveis, projetadas para satisfazer as necessidades de segurança de rede de qualquer organização.

Características e Vantagens

A segurança de próxima geração do SonicWALL incorpora um novo nível de gerenciamento unificado de ameaças (UTM) que integra prevenção de intrusão, antivírus e proteção contra programas espiões em portas de ligação, e destaca a suíte Application Firewall de ferramentas configuráveis para impedir o vazamento de dados e oferecer controle detalhado de aplicativos.

O hardware escalável de vários núcleos e a tecnologia Reassembly-Free Deep Packet Inspection™ fazem a varredura e eliminam ameaças de arquivos de qualquer tamanho proporcionando conexões simultâneas praticamente ilimitadas sem comprometer a velocidade. A série NSA 240 pode ser configurada através de interfaces do tipo modem primário ou secundário ou 3G sem-fio para expansibilidade futura garantida.

Os recursos de monitoramento de estado de alta disponibilidade e equilíbrio de carga no SonicOS 5.0 Enhanced maximizam a largura de banda total e mantêm um tempo de atividade contínua de rede, proporcionando acesso ininterrupto a recursos com funções cruciais e garantindo que os túneis de VPN e outros tipos de tráfego de rede não parem no caso de um failover.

Alto desempenho e custo total de propriedade reduzido são obtidos com a utilização do poder de processamento de vários núcleos ao mesmo tempo para aumentar de forma considerável a taxa de transferência e proporcionar recursos de inspeção simultâneos, reduzindo também o consumo de energia.

Os recursos avançados de redes e serviços de roteamento incorporam tecnologia avançada de rede e segurança, como VLANs 802.1q, failover WAN/WAN, gerenciamento baseado em zona e objeto, equilíbrio de carga, modos NAT avançados, etc..., proporcionando flexibilidade de configuração detalhada e proteção completa, definível pelo administrador.

Os recursos de Voz por IP (VoIP) baseados em padrões fornecem os mais altos níveis de segurança para cada elemento da infra-estrutura de VoIP, desde equipamentos de comunicação até dispositivos prontos para VoIP, como SIP Proxies, Gatekeepers H.323 e servidores de chamadas.

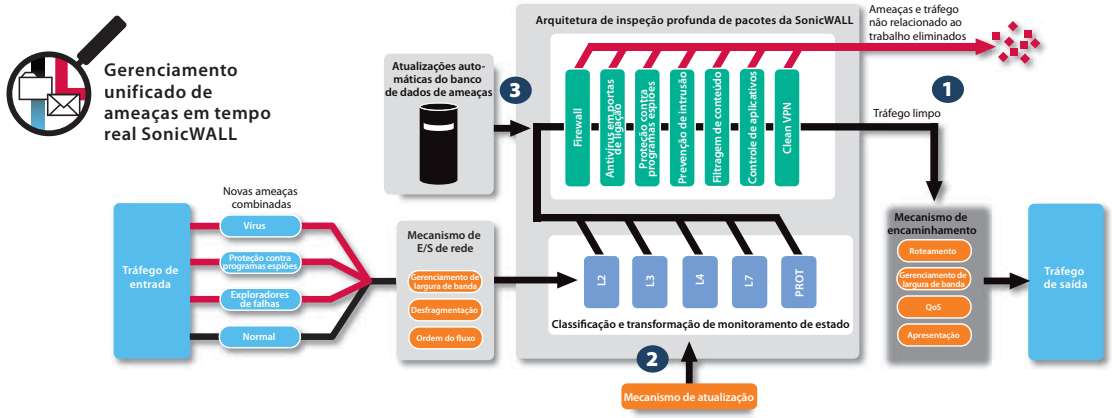
Os serviços de rede local sem-fio seguros e distribuídos permitem que o dispositivo funcione como controlador e comutador sem-fio seguro, que automaticamente detecta e configura os SonicPoints™, pontos de acesso sem-fio da SonicWALL, para o acesso remoto seguro em ambientes de rede distribuídos.

Os recursos de Qualidade de Serviço (QoS) incorporados utilizam o padrão 802.1p do setor e designações de Classe de Serviço (CoS) de pontos de código DiffSErv (DSCP) para proporcionar um gerenciamento de largura de banda potente e flexível essencial para VoIP, conteúdo multimídia e aplicativos cruciais para os negócios.

*Patente U.S. 7.310.815 – A method and apparatus for data stream analysis and blocking (método e instrumento para análise e bloqueio de fluxo de dados).

SONICWALL®

Arquitetura e gerenciamento dinâmicos de segurança

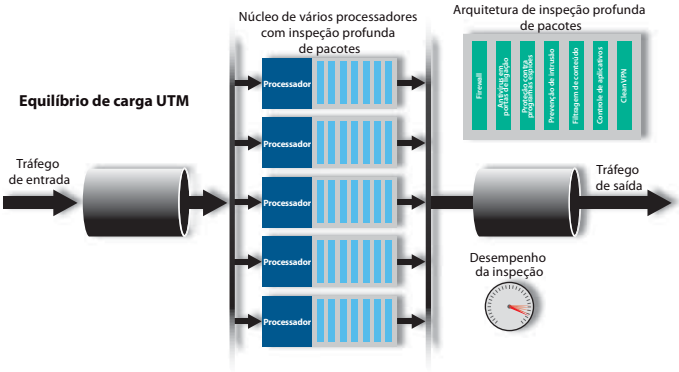


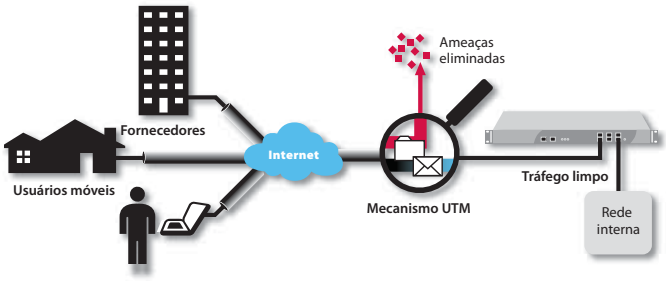
A melhor proteção contra ameaças da categoria

1. A inspeção profunda de pacotes da SonicWALL protege contra riscos de rede, como vírus, vermes, cavalos-de-Tróia, programas espiões, ataques de phishing, novas ameaças e utilizaçãão imprópria da Internet. O Application Firewall acrescenta controles altamente configuráveis para prevenir o vazamento de dados e gerenciar a largura de banda em nível de aplicativo.
2. A tecnologia SonicWALL Reaseembly-Free Deep Packet Inspection (RFDPI) utiliza a arquitetura de vários núcleos da SonicWALL para fazer a varredura de pacotes em tempo real sem estagnar tráfego na memória. Graças a esta funcionalidade, as ameaças são identificadas e eliminadas em arquivos de qualquer tamanho e em um número ilimitado de conexões simultâneas, sem interrupção.
3. A série Network Security Appliance oferece segurança de rede dinâmica através de atualizações de segurança contínuas e automatizadas que protegem contra ameaças novas e em evolução, sem a necessidade de intervenção do administrador.

Equilíbrio de carga UTM

Os projetos com um único processador que incluem várias tecnologias de proteção são severamente limitados por este único processador centralizado. O equilíbrio de carga UTM da SonicWALL integra uma inspeção profunda de pacotes de alta velocidade em um mecanismo de classificação de tráfego em vários núcleos de segurança, inspecionando aplicativos, arquivos e tráfego com base em conteúdo, em tempo real e sem impacto significativo ao desempenho e à escalabilidade. Isto permite a varredura e o controle de ameaças à rede com aplicativos de alto consumo de largura de banda e sensíveis a latências.





SonicWALL Clean VPN™

A série Network Security Appliance inclui a inovadora tecnologia SonicWALL Clean VPN™ que elimina vulnerabilidades e códigos maliciosos de tráfego de filiais e usuários móveis remotos antes que eles penetrem na rede da empresa, e sem a intervenção de usuários.

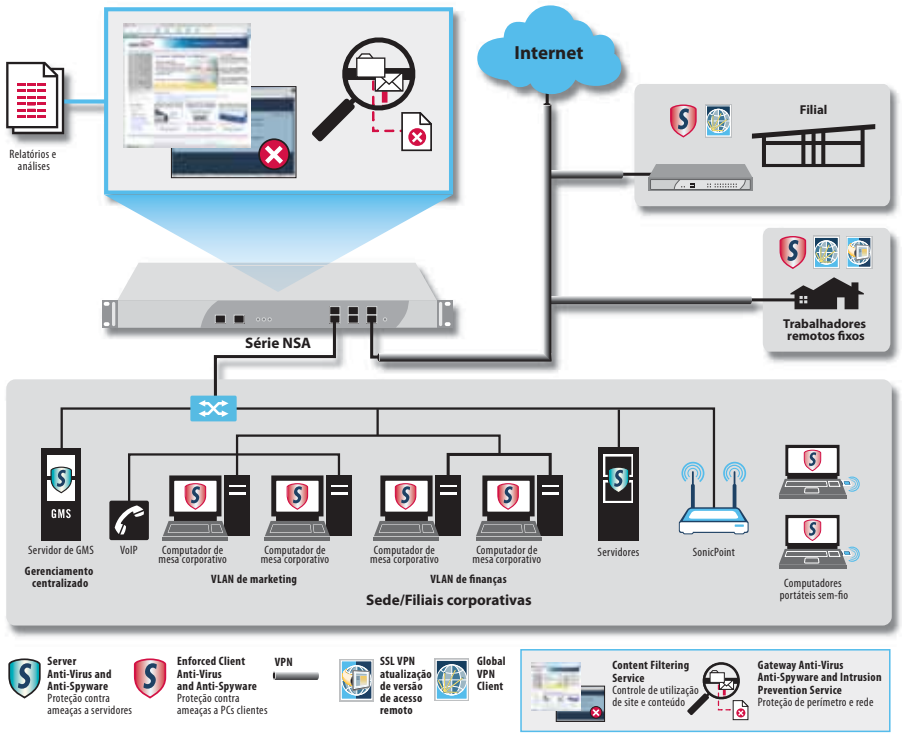
Gerenciamento centralizado de políticas

A série Network Security Appliance pode ser gerenciada através do SonicWALL Global Management System (GMS), que proporciona ferramentas flexíveis, poderosas e intuitivas para gerenciar configurações de forma centralizada, visualizar indicadores de monitoramento em tempo real e integrar relatórios de políticas e conformidade.

Opções de implantação flexíveis e personalizáveis: uma rápida apresentação da série NSA

Todas as soluções SonicWALL Network Security Appliance fornecem proteção de gerenciamento unificado de ameaças de próxima geração, utilizando um inovador projeto de hardware de vários núcleos e a tecnologia Reassembly-Free Deep Packet Inspection para a proteção interna e externa da rede sem comprometer o desempenho. Os produtos da série NSA combinam prevenção de intrusão de alta velocidade, inspeção de arquivos e conteúdo e os poderosos controles do Application Firewall com uma ampla gama de recursos avançados de rede e configuração flexível. A série NSA é uma plataforma acessível e econômica, fácil de implantar e gerenciar em uma grande variedade de ambientes de rede: corporativa, de filiais e distribuídas.

- O SonicWALL **NSA 5000** é o topo de linha, ideal para os mais exigentes ambientes de rede campus e distribuída
- O SonicWALL **NSA 4500** é ideal para sedes corporativas e grandes ambientes distribuídos, que exigem capacidade e desempenho elevados de taxa de transferência
- O SonicWALL **NSA 3500** é ideal para ambientes distribuídos, corporativos e de filiais, que exigem capacidade e desempenho significativos de taxa de transferência
- O SonicWALL **NSA 2400** é ideal para ambientes corporativos de pequeno e médio portes e filiais que precisam de uma boa capacidade e desempenho de taxa de transferência
- O SonicWALL **NSA 240** é ideal para pequenas e médias empresas e filiais.



Serviços de segurança e atualizações de versão

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service e Application Firewall – oferece proteção de segurança de rede inteligente e em tempo real contra ataques sofisticados em nível de aplicativo e baseados em conteúdo, incluindo vírus, programas espiões, vermes, cavalos-de-Tróia e vulnerabilidades de software (como estouros de buffer). O Application Firewall oferece uma suíte de ferramentas configuráveis projetadas para impedir o vazamento de dados, o que fornece controles detalhados em nível de aplicativo.

Enforced Client e Server Anti-Virus and Anti-Spyware – proporciona uma proteção abrangente contra vírus e programas espiões para laptops, desktops e servidores, utilizando um único cliente integrado e também oferece fiscalização automática em âmbito de rede de políticas, definições e atualizações de softwares antivírus e de proteção contra programas espiões.

Content Filtering Service – fiscaliza o cumprimento de políticas de proteção e produtividade através do emprego de uma arquitetura de classificação inovadora, utilizando um banco de dados dinâmico para o bloqueio de até 56 categorias de conteúdo questionável da Web.

ViewPoint Reporting – fornece recursos fáceis de usar e baseados na Web que proporcionam aos administradores uma percepção abrangente e instantânea do desempenho e da segurança da rede. Composto por uma série de relatórios históricos que utilizam painéis de controle e resumos detalhados, o ViewPoint ajuda organizações de todos os portes a controlarem a utilização da Internet, cumprirem requisitos de conformidade normativa e monitorarem o estado de segurança da rede.

Serviços de suporte dinâmico – disponíveis em horário comercial (8 horas por dia, 5 dias por semana) ou ininterruptamente (24 horas por dia, 7 dias por semana), dependendo das necessidades do cliente. Os recursos incluem suporte técnico de categoria internacional, atualizações e atualizações de versão essenciais de firmware, acesso a ferramentas eletrônicas abrangentes e substituição de hardware de forma tempestiva, para ajudar as organizações a obterem o maior retorno possível dos seus investimentos nas soluções da SonicWALL.

As atualizações de versão do Global VPN Client – utilizam um software cliente instalado em computadores Windows e aumentam a produtividade da força de trabalho através do fornecimento do acesso seguro a e-mails, arquivos, intranets e aplicativos para usuários remotos. As licenças para atualização de versão estão disponíveis em uma variedade de números de usuários, o que permite que a solução cresça junto com a organização.

As atualizações de versão de acesso remoto SSL VPN – oferecem acesso remoto sem cliente em nível de rede para sistemas PC (Windows), Mac e Linux. Com a tecnologia integrada SSL VPN, os dispositivos da SonicWALL para gerenciamento unificado de ameaças permitem o acesso remoto de forma contínua e segura a e-mails, arquivos, intranets e aplicativos de uma variedade de plataformas de cliente via NetExtender, um cliente leve instalado na máquina do usuário. O NetExtender é instalado e configurado automaticamente, sem a necessidade de interação com o usuário.

Especificações

Network Security Appliance 5000
01-SSC-7042

Network Security Appliance 4500
01-SSC-7012

NSA 4500 TotalSecure (1 ano)
01-SC-7032

Network Security Appliance 3500
01-SSC-7016

NSA 3500 TotalSecure (1 ano)
01-SC-7033

Network Security Appliance 2400
01-SSC-7020

NSA 2400 TotalSecure (1 ano)
01-SC-7035

Network Security Appliance 240
TotalSecure (1 ano)
01-SSC-8760

Adaptador SonicWALL de placa para ExpressCard (para NSA 240)
01-SSC-2887

Certificações

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

Para obter mais informações sobre as soluções de segurança de rede SonicWALL, visite **www.sonicwall.com**.

	NSA 240	NSA 2400	NSA 3500	NSA 4500	NSA 5000
Firewall					
Versão do SonicOS	SonicOS Enhanced 5.0 (ou superior)				
Taxa de transferência com monitoramento de estado[1]	600 Mbps	775 Mbps	1,5 Gbps	2,75 Gbps	3,5 Gbps
Desempenho GAV[1]	115 Mbps	160 Mbps	350 Mbps	690 MBps	800 Mbps
Desempenho IPS[1]	195 Mbps	275 Mbps	750 Mbps	1,4 Gbps	1,7 Gbps
Desempenho UTM[1]	110 Mbps	150 Mbps	240 Mbps	600 Mbps	800 Mbps
Desempenho IMIX	195 Mbps	235 Mbps	580 Mbps	700 Mbps	950 Mbps
Máximo de conexões[3]	25.000/35.000[2]	48.000	128.000	450.000	600.000
Novas conexões/segundo	2.000	4.000	7.000	10.000	12.000
Máximo de nós	Ilimitado				
Prevenção de ataques de negação de serviço (DoS)	22 classes de ataques de DoS, DDoS e varredura				
Máximo de SonicPoints	16	32	32	64	64
VPN					
Taxa de transferência 3DES/AES[1]	150 Mbps	300 Mbps	625 Mbps	1,0 Gbps	1,5 Gbps
Túneis VPN entre locais	25/50[2]	75	800	1.500	2.500
Licenças de Global VPN Client em pacote (Máximo)	2 (25)	10 (250)	50 (1.000)	500 (3.000)	1.000 (3.500)
Licenças de SSL VPN em pacote (Máximo)	2 (15)	2 (25)	2 (30)	2 (30)	2 (30)
Criptografia/Autenticação	DES, 3DES, AES (128, 192, 256 bits), MD5, SHA-1				
Troca de chaves	Troca de chaves IKE, IKEv2, chave manual, PKI (X.509)				
L2TP/IPSec	Sim				
Suporte a certificado	Verisign, Thawte, Cybertrust, RSA Keon, Entrust e Microsoft CA para SonicWALL a SonicWALL VPN				
Dead Peer Detection	Sim				
DHCP por VPN	Sim				
IPSec NAT Traversal	Sim, NAT_Tv00 e v03				
Porta de ligação VPN redundante	Sim				
Plataformas Global VPN Client compatíveis	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32 bits				
Plataformas SSL VPN compatíveis	Microsoft® Windows 2000 / XP / Vista 32/64 bits, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
Serviços de segurança de inspeção profunda de pacotes					
Serviço de assinatura de inspeção profunda de pacotes	Banco de dados de assinaturas completo. Controle de mensagens instantâneas e ponto a ponto, e atualizações de assinaturas por meio de arquitetura de fiscalização distribuída				
Content Filtering Service (CFS) Premium Edition	HTTP URL, HTTPS IP, varredura de palavras-chave e conteúdo, e bloqueio de ActiveX, Java Applet e cookies				
Enforced Client Anti-Virus and Anti-Spyware para portas de ligação	HTTP/S, SMTP, POP3, IMAP e FTP, Enforced McAfee™ Clients e bloqueio de anexos de e-mail				
Application Firewall	Proporciona controle de largura de banda e fiscalização em nível de aplicativo, regula tráfego da Web, e-mails, anexos de e-mail e transferência de arquivos, faz a varredura e restringe documentos e arquivos com base em frases e palavras chaves				
Redes					
Atribuição de endereço IP	Estática, (cliente DHCP, PPPoE, L2TP e PPTP), servidor DHCP interno, relay de DHCP				
Modos NAT	1 para 1, 1 para muitos, muitos para 1, muitos para muitos, NAT flexível (IPs sobrepostos), PAT, modo transparente				
Interfaces VLAN (802.1q)	10/25[2]	25	50	200	256
Roteamento	OSPF, RIPv1/v2, rotas estáticas, roteamento baseado em políticas, multicast				
QoS	Prioridade de largura de banda, largura de banda máxima, largura de banda garantida, marcação DSCP, 802.1p				
IPv6	Pronto para IPv6				
Autenticação	XAUTH/RADIUS, Active Directory, SSO, LDAP, banco de dados de usuários interno				
Banco de dados de usuários	100 usuários	250 usuários	500 usuários	1.000 usuários	1.500 usuários
VoIP	H.323v1-5 VoIP total, SIP, suporte a gatekeeper, gerenciamento de largura de banda de saída, VoIP por WLAN, segurança de inspeção profunda, interoperabilidade integral com a maioria dos dispositivos de comunicação e portas de ligação VoIP				
Sistema					
Segurança de zona	Sim				
Programações	Sim				
Gerenciamento baseado em objeto/grupo	Sim				
DDNS	Sim				
Gerenciamento e monitoramento	Interface gráfica Web (HTTP, HTTPS), Linha de comando (SSH, Console), SNMP v2: Gerenciamento global com SonicWALL GMS				
Logs e relatórios	ViewPoint,® Local Log, Syslog				
Alta disponibilidade	Ativa/passiva com State Sync (opcional)[2]	Ativa/passiva com State Sync (opcional)		Ativa/passiva com State Sync	
Equilíbrio de carga	Sim (de saída, com percentual, round robin e spill-over); (de entrada, com round robin, distribuição aleatória, sticky IP, remapeamento de bloqueio e remapeamento simétrico)				
Padrões	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS				
Padrões sem-fio	802.11 a/b/g, WPAD, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
Hardware					
Interfaces	(3) portas GE Gigabit + (6) 10/100, 2 USB para uso futuro, slot para placa PC (modem analógico/3G opcional), 1 interface de console	(6) portas 10/100/1.000 Gigabit de cobre, 1 interface de console, 2 USB (uso futuro)			
Memória (RAM)	256 MB	512 MB	512 MB	512 MB	1 GB
Memória Flash	32 MB Compact Flash	512 MB Compact Flash			
Fonte de alimentação	36 W Externa	Fonte de alimentação única de 180 W ATX			
Ventoinhas	Sem ventoinha	2 ventoinhas			
Tensão de entrada	10-240 V, 50-60 Hz	100-240 Vac, 60-50 Hz			
Consumo energético (máximo)	15 W	42 W	64 W	66 W	66 W
Dissipação de calor total	51,1 BTU	144 BTU	219 BTU	225 BTU	225 BTU
Certificações	VPNC		EAL4+, FIPS 140-2 Level 2, VPNC		
Certificações pendentes	ICSA Firewall 4.1, EAL-4+, FIPS 140-2		ICSA Firewall 4.1		
Formato e dimensões	18,1 x 3,8 x 26,7 cm/ 7,1 x 1,5 x 10,5 pol	Montagem em rack 1U 43,2 x 26 x 4,4 cm/ 17 x 10,3 x 18 pol		Montagem em rack 1U 43,2 x 33,7 x 4,4 cm/ 17 x 13,3 x 1,8 pol	
Peso	1,16 kg/2,55 lb	3,65 kg/8,05 lb		5,14 kg/11,30 lb	
Peso WEEE	1,43 kg/3,15 lb	3,65 kg/8,05 lb		5,14 kg/11,30 lb	
Principais normas	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE				
Ambiente	0-40 °C, 32-105 °F	5-40 °C, 40-105 °F			
MTBF	A definir	16,0 anos	14,3 anos	14,1 anos	14,1 anos
Umidade	0-95% sem condensação	10-90% sem condensação			

[1] Metodologias de teste: Desempenho máximo baseado em RFC 2544 (para firewall). O desempenho real pode variar de acordo com as condições de rede e os serviços ativados. Taxa de transferência de VPN com tráfego UDP e pacotes de 1.418 bytes, conforme a RFC 2544. O desempenho UTM baseia-se em testes HTTP executados no Spirent Avalanche/Reflector. Testes feitos com vários fluxos através de diversos pares de portas.
[2] Apenas com o Stateful HA (monitoramento de estado de alta disponibilidade) e a atualização de expansão da série NSA 240.
[3] Os números reais máximos de conexões são menores quando os serviços UTM estão ativados.

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale CA 94089-1306
T +1 408.745.9600
F +1 408.745.9300
www.sonicwall.com

SONICWALL®