SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

Proteja em qualquer lugar e a qualquer hora o acesso a recursos corporativos em ambientes de várias nuvens baseados na identidade, localização e confiança do usuário e do dispositivo.

O SonicWall SMA é um gateway de acesso seguro unificado que permite que os varejistas forneçam acesso a qualquer hora, em qualquer lugar e em qualquer dispositivo a recursos corporativos críticos. O mecanismo de política de controle de acesso granular do SMA, a autorização de dispositivo com reconhecimento de contexto, a VPN no nível da aplicação e a autenticação avançada com login único capacita as organizações para adotarem o BYOD e a mobilidade em um ambiente de várias nuvens.

Mobilidade e BYOD
Para as organizações que desejam adotar o BYOD, trabalho flexível ou acesso de terceiros, o SMA se torna o ponto crucial de aplicação entre todos eles. O SMA oferece a melhor segurança da categoria para minimizar as ameaças à superfície, ao mesmo tempo que torna as organizações mais seguras, sendo compatível com os algoritmos e códigos de criptografia mais recentes. Com o SMA da SonicWall, os administradores podem oferecer acesso móvel seguro e privilégios baseados em identidade para que os usuários finais tenham acesso rápido e simples aos recursos, dados e aplicações de negócios necessários. Ao mesmo tempo, as organizações podem instituir políticas de BYOD seguro para proteger suas redes e dados corporativos contra acesso não autorizado e malware.

Migração para a nuvem
Para as organizações que embarcam em uma jornada de migração para a nuvem, o SMA oferece uma infraestrutura de single sign-on (SSO) que usa um único portal da Web para autenticar os usuários em um ambiente de TI híbrido. A experiência de acesso é consistente e contínua, independentemente de o recurso corporativo estar no local, na Web ou em uma nuvem hospedada. O SMA também se integra às principais tecnologias de autenticação de vários fatores do setor para aumentar a segurança.

Fornecedores de serviços gerenciados
Para organizações que hospedam sua própria infraestrutura ou para provedores de serviços gerenciados, o SMA oferece uma solução pronta para proporcionar um alto grau de continuidade e escalabilidade dos negócios. O SMA pode comportar até 20.000 conexões simultâneas em um único appliance, com a capacidade de ajustar a escala para centenas de milhares de usuários por meio de clustering inteligente. Os datacenters podem reduzir os custos com organização por clusters ativa-ativa e um balanceador de carga dinâmico integrado, que realoca o tráfego global para o datacenter mais otimizado em tempo real com base na demanda do usuário. Os conjuntos de ferramentas do SMA permitem que os prestadores de serviços ofereçam serviços sem tempo de inatividade, para que possam atender SLAs muito exigentes.

O SMA capacita os departamentos de TI a proporcionar a melhor experiência e acesso mais seguro, dependendo do cenário do usuário. Disponível como appliances físicos protegidos ou appliances virtuais eficientes, o SMA integra-se perfeitamente à infraestrutura existente local e/ou na nuvem. As organizações podem escolher entre uma variedade de opções de acesso seguro na Web totalmente sem cliente para terceiros ou funcionários em dispositivos pessoais ou um acesso VPN com túnel completo mais tradicional baseado em cliente para executivos em todos os tipos de dispositivos. Independentemente de as organizações precisarem disponibilizar acesso seguro e confiável para cinco usuários de um único local ou escalar para milhares de usuários em redes distribuídas globalmente, o SonicWall SMA tem uma solução.

O SonicWall SMA permite que as organizações adotem a mobilidade e o BYOD sem medo e migrem para a nuvem com facilidade. O SMA capacita as forças de trabalho e proporciona uma experiência de acesso consistente.

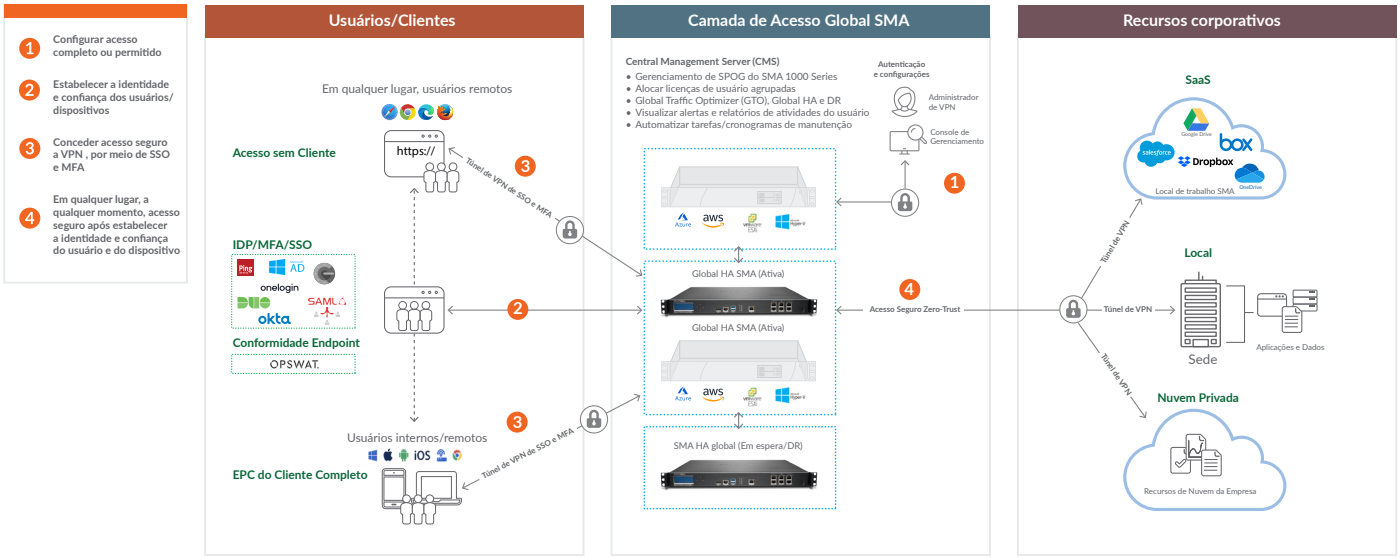
Benefícios:

- Tenha acesso unificado a todos os recursos de rede e nuvem para acesso seguro "a qualquer hora, em qualquer dispositivo e em qualquer aplicação"
- Controle quem tem acesso a quais recursos, definindo políticas detalhadas com o mecanismo eficiente de controle de acesso
- Aumente a produtividade disponibilizando um login único agrupado para aplicações SaaS ou hospedadas localmente com um único URL
- Reduza o custo total de propriedade e a complexidade do gerenciamento de acesso, consolidando os componentes da infraestrutura em um ambiente de TI híbrido
- Ganhe visibilidade de todos os dispositivos que se conectam e disponibilize o acesso com base nas políticas e na segurança do endpoint
- Evite violações de malware verificando todos os arquivos carregados na rede com o sandbox do Capture ATP
- Proteja-se contra ataques na Web e assegure a conformidade com o PCI com o complemento Web Application Firewall
- Detenha ataques de DDoS e zumbis com detecção de IP geográfico e proteção contra Botnet
- Obtenha funcionalidade segura de agente nativo usando o acesso HTML5 sem cliente baseado no navegador da Web, sem a sobrecarga de instalar e manter agentes nos dispositivos de endpoint
- Obtenha informações úteis necessárias para tomar as decisões corretas com monitoramento em tempo real e relatórios detalhados
- Implante como appliance físico ou appliance virtual em nuvens privadas no ESXi ou Hyper-V ou em ambientes de nuvem pública AWS ou Microsoft Azure
- Possibilite a emissão dinâmica de licenças de acesso com base na demanda em tempo real, com direcionamento automatizado do endpoint para a conexão de maior desempenho e menor latência
- Reduza os custos iniciais com balanceamento de carga integrado, sem hardware ou serviços adicionais, e elimine o impacto para o usuário no failover do appliance
- Evite interrupções nos negócios ou picos sazonais, aumentando a capacidade instantaneamente

Implementação do SMA

Um gateway de borda protegido para acesso seguro a qualquer hora, em qualquer lugar e em qualquer dispositivo

O SMA oferece acesso remoto seguro end-to-end abrangente para recursos corporativos hospedados em centros de dados locais, na nuvem e híbridos. Ele aplica controles de acesso baseados em identidade e com aplicação de políticas, autenticação de dispositivo com reconhecimento de contexto e VPN no nível da aplicação para disponibilizar o acesso a dados, recursos e aplicações depois de estabelecer a identidade e a confiança do usuário, do local e do dispositivo. Implantado de forma flexível como um appliance Linux protegido ou appliance virtual em nuvens privadas no ESXi ou Hyper-V ou em ambientes de nuvem pública AWS ou Microsoft Azure.



SMA Cloud/Implantação local

Implantação flexível com appliances físicos e virtuais

É possível implantar o SonicWall SMA como um appliance de alto desempenho protegido ou como um appliance virtual, empregando recursos de computação compartilhados para otimizar a utilização, facilitar a migração e reduzir os custos de capital. Os appliances de hardware são montados em uma arquitetura multi-core que oferece alto desempenho com aceleração de SSL, taxa de transferência de VPN e proxies potentes para disponibilizar acesso seguro eficiente. Para organizações reguladas e federais, o SMA também está disponível com a certificação FIPS 140-2 Nível 2. Os appliances virtuais do SMA oferecem os mesmos recursos eficientes de acesso seguro nas principais plataformas virtuais ou na nuvem, incluindo Microsoft Hyper-V, VMware ESX e AWS.

Licenças de usuário compartilhadas entre os appliances

Organizações com dispositivos distribuídos globalmente, podem se beneficiar das demandas flutuantes de licenças de usuário devido a diferenças de tempo. Se uma organização implanta licenças de VPN completas ou licenças básicas do ActiveSync, o gerenciamento central do SMA realoca as licenças para os appliances gerenciados nos quais as demandas dos usuários atingiram o pico de appliances em uma região geográfica diferente, em que o uso diminuiu por ter terminado o horário de trabalho ou iniciado o turno da noite.

Visibilidade da rede com perfil de dispositivo com reconhecimento de contexto

A melhor autenticação de reconhecimento da categoria concede acesso apenas a dispositivos confiáveis e usuários autorizados. Os laptops e PCs também são averiguados quanto à presença ou ausência de software de segurança, certificados de cliente e ID do dispositivo. Os dispositivos móveis são averiguados para obtenção de informações de segurança essenciais, como status de jailbreak ou root, ID do dispositivo, status do certificado e versões do sistema operacional anteriores à disponibilização do acesso. Os dispositivos que não cumprem os requisitos da política não recebem acesso à rede, e o usuário é notificado por não conformidade.

Experiência consistente em um único portal da Web

Os usuários não precisam se lembrar de todos os URLs de aplicações individuais e manter marcadores intermináveis. O SMA fornece um portal de acesso centralizado que fornece aos usuários um URL para acessar todas as aplicações importantes em um navegador da Web padrão. Depois de o usuário fazer login por meio de um navegador, um portal de usuário da Web personalizável é exibido na janela do navegador, com uma a visualização de um painel único de controle para acessar aplicações SaaS ou locais. O portal exibe apenas links e marcadores personalizados pertinentes ao dispositivo de endpoint, usuário ou grupo em particular. O portal é independente de plataforma e é compatível com todas as principais plataformas de dispositivos, incluindo dispositivos Windows, Mac OS, Linux, iOS e Android, com ampla compatibilidade com os navegadores em todos esses dispositivos.

Login único agrupado para aplicações SaaS e locais

Elimine a necessidade de usar várias senhas e acabe com práticas de segurança inadequadas, como a reutilização de senhas. O SMA oferece SSO agrupado para aplicações SaaS hospedadas na nuvem e aplicações hospedadas no campus. O SMA faz integração com vários servidores de autenticação, autorização e auditoria e com as principais tecnologias de autenticação de vários fatores para adicionar segurança. O SSO seguro é disponibilizado apenas a dispositivos de endpoint autorizados depois que o SMA verifica a condição e a conformidade do endpoint. O mecanismo de política de acesso garante que os usuários possam ver somente aplicações autorizadas e concede o acesso após a autenticação bem-sucedida. A solução é compatível com SSO agrupado, mesmo com o uso de clientes de VPN, proporcionando aos clientes uma experiência de autenticação uniforme, seja com acesso baseado em cliente, seja com acesso seguro sem cliente.

Evite violações e ameaças avançadas

O SonicWall SMA acrescenta uma camada de segurança de acesso para melhorar sua postura de segurança e reduzir a área de superfície para as ameaças.

- Integra-se ao sandbox multimotor baseado em nuvem do SonicWall Capture ATP para examinar todos os arquivos enviados por usuários com endpoints não gerenciados ou por pessoas fora da rede corporativa. Assim, os usuários têm o mesmo nível de proteção contra ameaças avançadas, como ransomware ou malware zero-day, quando estão na rua e no escritório[1].
- O serviço SonicWall Web Application Firewall oferece às empresas uma solução acessível e integrada de maneira uniforme para proteger aplicações internas na Web. Dessa forma, os clientes podem garantir a confidencialidade dos dados, e os serviços internos na Web permanecem intactos no caso de um acesso de usuário autenticado mal-intencionado ou invasor.
- A detecção de IP geográfico e Botnet protege as organizações contra ataques DDoS e zumbis e endpoints comprometidos que funcionam como botnets.

Acesso sem cliente, seguro e uniforme por navegador

A natureza "sem cliente" do SonicWall SMA significa que o administrador não precisa instalar um componente de cliente de grande porte manualmente em um computador que será usado para acesso remoto. Com isso, a dependência de Java e a sobrecarga para a TI são eliminadas, expandindo amplamente o conceito de acesso remoto. Portanto, como não há necessidade de instalação ou configuração prévia, um colaborador remoto autorizado pode usar qualquer computador, em qualquer lugar do mundo, e acessar com segurança os recursos corporativos. Em sua forma mais pura, o acesso seguro é estritamente realizado em navegador usando HTML5, o que proporciona uma experiência uniforme e unificada para os usuários.

Ofereça uma experiência "Sempre Conectada"

Para obter uma experiência de usuário uniforme, o SMA disponibiliza VPN Sempre Conectada para dispositivos Windows gerenciados. Os administradores podem definir configurações para estabelecer automaticamente uma conexão VPN sempre que um cliente de endpoint autorizado detectar uma rede pública ou não confiável. Um evento de login único no dispositivo Windows fornece ao usuário uma conexão segura com os recursos corporativos. Os usuários não precisam fazer login em seus clientes de VPN ou manter senhas adicionais. Assim, os usuários móveis dispõem de uma experiência uniforme para acessar recursos importantes como se estivessem no escritório, e os administradores de TI podem manter o controle sobre os dispositivos gerenciados, melhorando a postura de segurança da organização.

Gerenciamento intuitivo e relatórios abrangentes

A SonicWall fornece uma plataforma de gerenciamento intuitiva baseada na Web, o Central Management Server (CMS), para otimizar o gerenciamento de appliances e ao mesmo tempo oferecer recursos de relatórios abrangentes. A GUI de fácil utilização traz clareza ao gerenciamento de appliances e políticas individuais ou múltiplos. Cada página mostra como as configurações são definidas em todas as máquinas no gerenciamento. O gerenciamento unificado de políticas ajuda a criar e monitorar as políticas e configurações de acesso. Uma única política pode controlar o acesso de seus usuários, dispositivos e aplicações aos dados, servidores e redes. A TI pode automatizar tarefas rotineiras e programar atividades, dispensando as equipes de segurança de tarefas repetitivas para que elas se concentrem em tarefas estratégicas de segurança, como resposta a incidentes. A TI obtém informações sobre as tendências de acesso dos usuários e sobre a integridade de todo o sistema por meio de relatórios fáceis de usar e registro centralizado.

Ofereça disponibilidade de serviço 24x7

As organizações dispõem de requisitos para manter seus serviços e seu funcionamento com um alto grau de confiabilidade para fornecer acesso seguro ininterrupto a aplicações importantes. Os appliances do SMA são compatíveis com High Availability (HA) ativa-passiva tradicional para organizações com datacenters únicos ou com AD global com organização por clusters ativa-ativa ou ativa ou em espera para datacenters locais ou distribuídos. Ambos os modelos de HA oferecem uma experiência harmoniosa para os usuários com failover de impacto zero e persistência de sessão.

Implante o cliente de VPN adequado para suas necessidades

Escolha entre uma ampla variedade de clientes de VPN para fornecer acesso remoto seguro com aplicação de política para vários endpoints, incluindo laptops, smartphones e tablets.

Cliente de VPN	SO compatível	Modelo de SMA compatível	Destaque principal
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Todos os modelos	Ofereça autenticação biométrica, VPN por aplicação e implementação de controle de endpoint
Connect Tunnel (Cliente de Pequeno Porte)	Windows, Mac OS e Linux	6200, 6210, 7200, 7210, 8200v, 9000	Ofereça uma experiência "de escritório" completa com controle eficiente de endpoint
NetExtender (Thin Client)	Windows e Linux	210, 410, 500v	Aplique políticas de acesso granular e estenda o acesso à rede com clientes nativos

Reduza os custos iniciais com balanceador de carga integrado

A funcionalidade de balanceamento de carga integrada ao appliance do SMA atinge o nível de escalabilidade esperado para implantações em empresas de médio porte e corporações. Alguns modelos de appliance do SMA oferecem balanceamento de carga dinâmico para atribuir cargas de sessão de modo inteligente e alocar licenças de usuário em tempo real conforme a demanda. As organizações não precisam investir em balanceadores de carga externos, reduzindo assim os custos iniciais.

Obtenha proteção contra eventos imprevistos

Uma solução completa de continuidade dos negócios e recuperação de desastres deve ser capaz de tratar de um aumento significativo no tráfego de acesso remoto, ao mesmo tempo que mantém os controles de segurança e custo. Os pacotes de licenças Spike da SonicWall para o SMA são licenças complementares que permitem que empresas distribuídas escalem a contagem de usuários e atinjam a capacidade máxima instantaneamente, possibilitando a continuidade uniforme dos negócios. As licenças Spike funcionam como uma apólice de seguro para picos planejados ou não planejados futuros do número de usuários atuais a dezenas ou até centenas de usuários adicionais.

Recursos

Autenticação avançada

Login único agrupado[2]	O SMA usa a autenticação SAML 2.0 para ativar o SSO agrupado com um único portal para recursos locais e na nuvem e aplica autenticação de vários fatores empilhada para aumentar a segurança.
Autenticação de vários fatores	Certificados digitais X.509 Certificados digitais do servidor e do cliente RSA SecurID, Dell Defender, Google Authenticator, Duo Security e outros tokens de senha de uso único/autenticação de dois fatores Common Access Card (CAC) Autenticação dupla ou empilhada Compatibilidade com captcha, nome de usuário/senha
Autenticação SAML	O SMA pode ser configurado como SAML Identity Provider (IdP), SAML Service Provider (SP) ou proxy em um IdP local atual para ativar o single sign-on (SSO) agrupado usando a autenticação SAML 2.0.
Repositórios de autenticação	O SMA oferece integrações simples com repositórios padrão do setor para facilitar o gerenciamento de contas e senhas de usuários. É possível preencher os grupos de usuários dinamicamente com base em repositórios de autenticação RADIUS, LDAP ou Active Directory, incluindo grupos aninhados. Os atributos de LDAP comuns ou personalizados podem ser averiguados quanto a uma autorização específica ou verificação de registro de dispositivo.
Proxy de aplicação de Camada 3-7	O SMA oferece opções flexíveis de proxy. Por exemplo, é possível viabilizar o acesso de fornecedor por proxy direto, o acesso de prestador de serviço por proxy reverso e o acesso de funcionário ao Exchange pelo ActiveSync.
Proxy reverso	O serviço de proxy reverso avançado com autenticação permite que os administradores configurem o portal de descarga de aplicações e os marcadores, de modo que os usuários possam se conectar com uniformidade a aplicações e recursos remotos, incluindo RDP e HTTP. Este recurso é compatível com todos os navegadores, incluindo IE, Chrome e Firefox.
Delegação restrita por Kerberos	O SMA fornece suporte de autenticação usando uma infraestrutura atual do Kerberos, que não precisa de serviços front-end para delegar um serviço.

Gerenciamento de acesso

Access Control Engine (ACE)	Os administradores permitem ou negam o acesso com base nas políticas organizacionais e definem ações de correção ao colocarem as sessões em quarentena. A política baseada em objeto do ACE utiliza elementos de rede, recurso, identidade, dispositivo, aplicação, dados e tempo.
End Point Control (EPC)	O EPC permite que o administrador aplique regras de controle de acesso granular conforme a condição do dispositivo que está se conectando. Com a profunda integração do sistema operacional, muitos elementos são combinados para classificação de tipo e avaliação de fatores de risco. A averiguação do EPC simplifica a configuração do perfil do dispositivo usando uma lista abrangente e predefinida de soluções antivírus, de firewall pessoal e antispyware para plataformas Windows, Mac e Linux, incluindo a versão e a aplicabilidade da atualização do arquivo de assinatura.
App Access Control (AAC)	Os administradores podem definir quais aplicações móveis específicas podem acessar quais recursos da rede por meio de túneis de aplicações individuais. As políticas do AAC são aplicadas no cliente e no servidor, protegendo o perímetro com eficiência.

Segurança superior

VPN SSL de Camada 3	A série SMA oferece recursos de tunelamento de camada 3 de alto desempenho para uma ampla variedade de dispositivos de cliente em execução em qualquer ambiente.
Compatibilidade de criptografia	Duração configurável da sessão Códigos: AES 128 + 256 bit, Triple DES, RC4 128 bit Hashes: SHA-256 Algoritmo de Assinatura Digital de Curvas Elípticas (ECDSA)
Suporte de códigos avançado	Os appliances do SMA estabelecem uma forte postura de segurança pronta para uso para conformidade, com códigos de configuração padrão. Os administradores podem aprimorar ainda mais o desempenho, a eficiência da segurança ou a compatibilidade.
Certificações de segurança	Certificado para FIPS 140-2 Nível 2, ICSA SSL-TLS, Em andamento para Common Criteria, UC-APL
Compartilhamento seguro de arquivos	Detenha ataques desconhecidos de zero-day, como ransomware, no gateway com correção automatizada. Os arquivos carregados usando endpoints não gerenciados com acesso seguro a redes corporativas são inspecionados pelo Capture ATP multimotor baseado em nuvem.
Web Application Firewall (WAF)	Impeça ataques de protocolo e baseados na Web, ajudando empresas financeiras, de saúde, de comércio eletrônico e de outras áreas a alcançarem a conformidade com o OWASP Top 10 e com o PCI.
Detecção de IP geográfico e proteção contra botnet	A Detecção de IP Geográfico e a Proteção contra Botnet dão aos clientes um mecanismo para permitir ou restringir o acesso de usuários de diversas localizações geográficas.
Suporte TLS 1.3	Fornecer segurança e melhoria de desempenho, reduzindo as complexidades em relação aos seus antecessores.

Experiência de usuário intuitiva

VPN Sempre Conectada	Estabeleça automaticamente uma conexão segura com a rede corporativa de dispositivos Windows emitidos pela empresa para melhorar a segurança, ganhar visibilidade do tráfego e manter a conformidade
Secure Network Detection (SND)	O cliente de VPN com reconhecimento de rede do SMA detecta quando o dispositivo está fora do campus e se reconecta automaticamente à VPN, desconectando-se novamente quando o dispositivo retorna a uma rede confiável.
Acesso sem cliente aos recursos	O SMA oferece acesso seguro sem cliente aos recursos por meio de agentes de navegador HTML5 que disponibilizam os protocolos RDP, ICA, VNC, SSH e Telnet.
Portal de login único	O portal WorkPlace fornece uma visualização de painel único fácil de usar e personalizável para acesso seguro com Single sign-on (SSO) a todos os recursos em um ambiente de TI híbrido. Não é necessário login adicional ou VPN.
Tunelamento de Camada 3	Os administradores podem optar pelo tunelamento dividido ou aplicar o modo Redirecionar Tudo com tunelamento SSL/TLS e fallback ESP opcional para obter desempenho máximo.
Explorador de arquivos HTML5[1]	Um navegador de arquivos moderno facilita o acesso dos usuários a compartilhamentos de arquivos em qualquer navegador da Web.
Integração de SO móvel	O Mobile Connect é compatível com todas as plataformas de sistema operacional, fornecendo aos usuários total flexibilidade na escolha de dispositivos móveis.

Resiliência

Global Traffic Optimizer (GTO)	O SMA oferece balanceamento de carga de tráfego global sem impacto para os usuários. O tráfego é roteado para o datacenter mais otimizado e com melhor desempenho.
Alta disponibilidade dinâmica[2]	O SMA aceita configuração Ativa/Passiva e oferece configuração Ativa/Ativa para alta disponibilidade, seja com implantação em um único datacenter, seja em vários datacenters geograficamente dispersos.
Persistência de sessão universal[1]	Proporcione aos usuários uma experiência harmoniosa com failover de impacto zero. Se um appliance fica off-line, a organização por clusters inteligente do SMA realoca os usuários junto com os dados da sessão, sem a necessidade de uma nova autenticação.
Desempenho escalável	Os appliances do SMA escalam o desempenho exponencialmente com a implantação de vários appliances, eliminando assim todo ponto de falha. A organização por clusters horizontal é totalmente compatível com a combinação de appliances físicos e virtuais do SMA.
Licenciamento dinâmico	Não é mais necessário aplicar as licenças de usuário a appliances individuais do SMA. É possível distribuir e realocar os usuários dinamicamente entre os appliances gerenciados conforme a demanda dos usuários.

Gerenciamento e monitoramento central

Central Management System (CMS)	O CMS fornece gerenciamento centralizado e baseado na Web para todos os recursos do SMA.
Alertas personalizados	Os alertas podem ser configurados para gerar interceptações SNMP que são monitoradas por qualquer Network Management System (NMS) da Infraestrutura de TI. Os administradores também podem configurar alertas para verificações de arquivos do Capture ATP e uso do disco para ação imediata.
Painel em Tempo Real	Um painel personalizável em tempo real permite que o administrador de TI faça o diagnóstico rápido e fácil dos problemas de acesso, obtendo informações importantes para a solução de problemas.
Integração de SIEM	A saída em tempo real para os coletores de dados centrais do SIEM permite que as equipes de segurança correlacionem atividades acionadas por eventos para entender o fluxo de trabalho completo de um usuário ou de uma aplicação em particular. Isso é fundamental durante o gerenciamento de incidentes de segurança e a análise forense.
Planejador	Com o planejador, os usuários podem planejar tarefas de manutenção, como implantação de políticas, replicação de definições de configuração e reinicialização de serviços, sem intervenção manual

Extensibilidade

APIs de gerenciamento	As APIs de gerenciamento oferecem controle administrativo programático completo sobre todos os objetos em um único ambiente SMA ou CMS global.
APIs de Usuário Final	As APIs de Usuário Final oferecem controle completo sobre todo o fluxo de trabalho de login, autenticação e endpoint.
Autenticação de dois fatores (2FA)	O SMA oferece 2FA por meio da integração com as principais soluções de senha de uso único baseadas em tempo (TOTP), como Google Authenticator, Microsoft Authenticator, Duo Security, etc.
Integração de MDM	O SMA integra-se aos principais produtos de enterprise mobile management (EMM), como Airwatch e Mobile Iron.
Integração com outros terceiros	O SMA integra-se aos principais fornecedores do setor, como OPSWAT, para fornecer proteção avançada contra ameaças

[1]*Disponível com o SMA OS 12.1 ou posterior*

[2]*Aprimorada no SMA 12.1*

Resumo dos Recursos (comparação por modelo)

Categoria	Recurso	210	410	500v	6210	7210	8200v
Implantação	Sistema operacional	SMA 10.2	SMA 10.2	SMA 10.2	SMA 12.4	SMA 12.4	SMA 12.4
	Hipervisores suportados	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	Plataformas públicas em nuvem suportadas	–	–	AWS/Azure	–	–	AWS/Azure
Taxa de transferência	Máximo de sessões de usuário simultâneas	50	250	250	2.000	10.000	5.000
	Taxa de transferência máxima de SSL/TLS	560 Mbps	844 Mbps	186 Mbps	800 Mbps	5.0 Gbps	1.58 Gbps
Acesso de cliente	Túnel de Camada 3	•	•	•	•	•	•
	Tunelamento Dividido e Redirecionar Tudo	•	•	•	•	•	•
	VPN Sempre Conectada	•	•	•	•	•	•
	Encapsulamento automático de ESP	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Detecção de Rede Segura	–	–	–	•	•	•
	Navegador de arquivos (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	Túnel por demanda	–	–	–	•	•	•
	Extensões do Chrome/Firefox	–	–	–	•	•	•
	Compatibilidade com túnel CLI	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	Net Extender (Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Acesso móvel	VPN por aplicação	–	–	–	•	•	•
	Implementação de controle de aplicação	–	–	–	•	•	•
	Validação de ID da aplicação	–	–	–	•	•	•
Portal do usuário	Imagem de Marca	•	•	•	•	•	•
	Personalização	–	–	–	•	•	•
	Localização	•	•	•	•	•	•
	Marcadores definidos pelo usuário	•	•	•	•	•	•
	Compatibilidade com URL personalizado	•	•	•	•	•	•
	Compatibilidade com aplicações SaaS	–	–	–	•	•	•
Segurança	FIPS, 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B ciphers	–	–	–	•	•	•
	Averiguação dinâmica de EPC	•	•	•	•	•	•
	Controle de Acesso Baseado em Função (RBAC)	–	–	–	•	•	•
	Registro de endpoint	•	•	•	•	•	•
	Compartilhamento Seguro de Arquivos (Capture ATP)	•	•	•	•	•	•
	Quarentena de endpoint	•	•	•	•	•	•
	Validação de OSCP e CRL	–	–	–	•	•	•
	Seleção de código	–	–	–	•	•	•
	Certificados de PKI e cliente	•	•	•	•	•	•
	Filtro de IP geográfico	•	•	•	–	–	–
	Filtro de botnet	•	•	•	–	–	–
	Proxy Web	•	•	•	•	•	•
	Proxy reverso	•	•	•	•	•	•
Serviços de autenticação e identidade	SAML 2.0	–	–	–	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	•	•	•	•	•	•
	Compatibilidade com dispositivos biométricos	•	•	•	•	•	•
	Compatibilidade com Face ID para iOS	•	•	•	•	•	•
	Autenticação de dois fatores (2FA)	•	•	•	•	•	•
	Autenticação de vários fatores (MFA)	–	–	–	•	•	•

Resumo dos Recursos (comparação por modelo, cont.)

Categoria	Recurso	210	410	500v	6210	7210	8200v
Serviços de autenticação e identidade, cont.	Autenticação em cadeia	–	–	–	•	•	•
	One Time Passcode (OTP) por e-mail ou SMS	•	•	•	•	•	•
	Compatibilidade com Cartão de Acesso Comum (CAC)	–	–	–	•	•	•
	Compatibilidade com certificado X.509	•	•	•	•	•	•
	Integração de captcha	–	–	–	•	•	•
	Alteração de senha remota	•	•	•	•	•	•
	SSO baseado em formulários	•	•	•	•	•	•
	SSO agrupado	–	–	–	•	•	•
	Persistência de sessão	–	–	–	•	•	•
	Login automático	•	•	•	•	•	•
Controle de acesso	AD de grupo	•	•	•	•	•	•
	Atributos LDAP	•	•	•	•	•	•
	Políticas de localização geográfica	•	•	•	–	–	–
	Monitoramento contínuo de endpoint	•	•	•	•	•	•
Gerenciamento	Interface de gerenciamento (Ethernet)	–	–	–	•	•	•
	Interface de gerenciamento (console)	–	–	–	•	•	•
	Administração HTTPS	•	•	•	•	•	•
	Administração SSH	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog e NTP	•	•	•	•	•	•
	Monitoramento de uso	•	•	•	•	•	•
	Reversão de configuração	•	•	•	•	•	•
	Gerenciamento Centralizado	–	–	–	•	•	•
	Relatórios centralizados	–	–	–	•	•	•
	APIs REST de gerenciamento	–	–	–	•	•	•
	APIs REST de autenticação	–	–	–	•	•	•
	Auditoria RADIUS	–	–	–	•	•	•
	Tarefas programadas	–	–	–	•	•	•
	Licenciamento de sessão centralizado	–	–	–	•	•	•
	Auditoria acionada por eventos	–	–	–	•	•	•
Funcionamento em rede	IPv6	•	•	•	•	•	•
	Balanceamento de carga global	–	–	–	•	•	•
	Balanceamento de carga de servidor	•	•	•	–	–	–
	Replicação de estado do TCP	•	•	•	•	•	•
	Failover do estado de cluster	–	–	–	•	•	•
	Alta disponibilidade ativa/passiva	–	•	•	•	•	•
	Alta disponibilidade ativa/ativa	–	–	–	•	•	•
	Escalabilidade horizontal	–	–	–	•	•	•
	FQDNs únicos ou múltiplos	–	–	–	•	•	•
	Proxy de túnel inteligente de Camada 3-7	•	•	•	•	•	•
	Proxy de aplicação L7	•	•	•	•	•	•
Integração	Compatibilidade com TOTP de 2FA	•	•	•	•	•	•
	Compatibilidade com produtos de EMM e MDM	–	–	–	•	•	•
	Compatibilidade com produtos de SIEM	–	–	–	•	•	•
	Armazenamento de senhas de TPAM	–	–	–	•	•	•
	Compatibilidade com hypervisor ESX	–	–	•	–	–	•
	Compatibilidade com hypervisor Hyper-V	–	–	•	–	–	•
Opções de licenciamento	Licença baseada em assinatura	–	–	–	•	•	•
	Licença vitalícia com suporte	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	Licenciamento Spike	•	•	•	•	•	•
	Licenciamento em níveis	–	–	–	•	•	•
	Assistência virtual	•	•	•	–	–	–

** Para saber mais sobre clientes de VPN, visite: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

SONICWALL®

Benefícios da atualização para appliances de tecnologia avançada

Desempenho superior | Maior taxa de transferência | Recursos avançados | Melhor escalabilidade

Especificações do appliance

Escolha entre uma variedade de appliances de Secure Mobile Access (SMA) feitos sob medida. Disponha de opções de implantação flexíveis com appliances virtuais e físicos.

Especificações do appliance físico

Desempenho	SMA 210	SMA 410	SMA 6210	SMA 7210
Sessões/usuários simultâneos	Até 50	Até 250	Até 2.000	Até 10.000
Taxa de transferência de VPN SSL* (no máximo de usuários simultâneos)	560 Mbps	844 Mbps	Até 800 Mbps	Até 5,0 Gbps
Formato	1U	1U	1U	1U
Dimensões	16,92 x 10,23 x 1,75 pol (43 x 26 x 4,5 cm)	16,92 x 10,23 x 1,75 pol (43 x 26 x 4,5 cm)	17,0 x 16,5 x 1,75 pol (43 x 41,5x 4,5 cm)	17,0 x 16,5 x 1,75 pol (43 x 41,5x 4,5 cm)
Peso do appliance	11 lb (5 kg)	11 lb (5 kg)	17,7 lb (8 kg)	18,3 lb (8,3 kg)
Aceleração de dados de criptografia (AES-NI)	NÃO	NÃO	SIM	SIM
Porta de gerenciamento exclusiva	NÃO	NÃO	SIM	SIM
Aceleração de SSL	NÃO	NÃO	SIM	SIM
Armazenamento	4 GB (Memória Flash)	4 GB (Memória Flash)	2 x 1 TB SATA; RAID 1	2 x 1 TB SATA; RAID 1
Interfaces	(2) GB Ethernet, (2) USB, (1) console	(4) GB Ethernet, (2) USB, (1) console	(6) portas 1GE, (2) USB, (1) console	(6) portas 1GE, (2) portas 10 Gb SFP+, (2) USB, (1) console
Memória	4GB	8GB	8GB DDR4	16GB DDR4
TPM chip	NÃO	NÃO	SIM	SIM
Processador	4 núcleos	8 núcleos	4 núcleos	4 núcleos
MTBF (a 25 °C ou 77 °F) em horas	61.815	60.151	70.127	129.601
Operações e Conformidade	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Ligar	Fonte de alimentação fixa	Fonte de alimentação fixa	Fonte de alimentação fixa	Fonte de alimentação dupla, substituível em serviço
Tensão de entrada	100-240VAC, 50-60MHz	100-240VAC, 50-60MHz	100-240 VAC, 1.1 A	100-240 VAC, 1.79 A
Consumo de energia	26,9 W	31,9 W	77 W	114 W
Dissipação total de calor	92 BTU	109 BTU	264 BTU	389 BTU
Ambiental	REEE, RoHS UE, RoHS China			
Choque em modo não operacional	110 g, 2 ms			
Emissões	FCC, ICES, CE, C-Tick, VCCI; MIC			
Segurança	Esquema TUV/GS, UL, CE PSB, CCC, BSMI, CB			
Temperatura de operação	0 °C a 40 °C (32 °F a 104 °F)			
Certificação FIPS	NÃO	NÃO	FIPS 140-2 Nível 2 com proteção contra adulteração	

** O desempenho da taxa de transferência pode variar de acordo com a implantação e conectividade. Os números publicados baseiam-se nas condições internas do laboratório*

Especificações do appliance virtual

Especificações	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Sessões simultâneas	Até 250 usuários	Até 5000
Taxa de transferência de VPN SSL* (no máximo de usuários simultâneos)	Até 186 Mbps	Até 1,58 Gbps
Memória alocada	2GB	8 GB
Processador	1 núcleo	4 núcleos
Aceleração de SSL	NÃO	SIM
Tamanho do disco aplicado	2GB	64 GB (padrão)
Sistema operacional instalado	Linux	Linux Protegido
Porta de gerenciamento exclusiva	NÃO	SIM

** O desempenho da taxa de transferência pode variar de acordo com a implantação e conectividade. Os números publicados baseiam-se nas condições internas do laboratório. O SMA 8200v no Hyper-V pode ser escalado para até 5.000 sessões simultâneas e oferece uma taxa de transferência de VPN SSL de até 1,58 Gbps quando executa o SMA OS 12.1 com Windows Server 2016*

Informações de Pedidos

SKU	APPLIANCE DO SONICWALL SECURE MOBILE ACCESS (SMA)
02-SSC-2800	SMA 210 com licença para 5 usuários
02-SSC-2801	SMA 410 com licença para 25 usuários
01-SSC-8469	SMA 500v com licença para 5 usuários
02-SSC-0978	SMA 7210 com licença de teste de administrador
02-SSC-0976	SMA 6210 com licença de teste de administrador
01-SSC-8468	SMA 8200v (appliance virtual)
SKU	**LICENÇAS DE USUÁRIO DO SONICWALL SMA**
01-SSC-9182	SMA 500V com acréscimo de 5 usuários (também disponível para SMA 210)
01-SSC-2414	SMA 500V com acréscimo de 100 usuários (também disponível para SMA 410)
01-SSC-7856	Licença para 5 usuários do SMA - empilhável para 6210, 7210, 8200v
01-SSC-7860	Licença para 100 usuários do SMA - empilhável para 6210, 7210, 8200v
01-SSC-7865	Licença do SMA para 5.000 usuários - empilhável para 7210, 8200v
SKU	**CONTRATO DE SUPORTE DO SONICWALL SMA**
01-SSC-9191	Suporte 24X7 para SMA 500V com até 25 usuários por 1 ano (também disponível para SMA 210 e 410)
01-SSC-2326	Suporte 24X7 para SMA 6210 com 100 usuários por 1 ano - empilhável
01-SSC-2350	Suporte 24X7 para SMA 7210 com 500 usuários por 1 ano - empilhável
01-SSC-8434	Suporte 24X7 para SMA 8200V com 5 usuários por 1 ano - empilhável (também disponível para SMA 6210 e 7210)
01-SSC-8446	Suporte 24X7 para SMA 8200V com 100 usuários por 1 ano - empilhável (também disponível para SMA 6210 e 7210)
01-SSC-7913	Suporte 24X7 para SMA 8200V com 5000 usuários por 1 ano - empilhável (também disponível para SMA 6210 e 7210)
SKU	**GERENCIAMENTO CENTRAL PARA 6210, 7210, 8200V**
Licença de appliance do CMS	
01-SSC-8535	Licença básica do CMS + 3 appliances (Gratuita para avaliações e uso com licenças de usuário por assinatura)
01-SSC-8536	Licença do CMS para 100 appliances por 1 ano (para uso com licenças de usuário por assinatura)
01-SSC-3369	CMS básico + 3 appliances (Gratuito para uso com licenças de usuário vitalícias)
01-SSC-3402	Licença do CMS para 100 appliances por 1 ano (para uso com licenças de usuário vitalícias)
Licenças de usuário centrais (assinatura)	
01-SSC-2298	Licença coletiva do CMS para 10 usuários por 1 ano
01-SSC-8539	Licença coletiva do CMS para 1000 usuários por 1 ano
01-SSC-5339	Licença coletiva do CMS para 50000 usuários por 1 ano
Licenças de usuário centrais (vitalícias)	
01-SSC-2053	Licença do CMS vitalícia para 10 usuários
01-SSC-2058	Licença do CMS vitalícia para 1000 usuários
01-SSC-2063	Licença do CMS vitalícia para 50000 usuários
Suporte para licenças de usuário centrais (vitalício)	
01-SSC-2065	Suporte para CMS 24x7 por 1 ano para 10 usuários
01-SSC-2070	Suporte para CMS 24x7 por 1 ano para 1000 usuários
01-SSC-2075	Suporte para CMS 24x7 por 1 ano para 50000 usuários
Licenças Centrais do ActiveSync (assinatura)	
01-SSC-2088	Licença coletiva de e-mail do CMS para 10 usuários por 1 ano
01-SSC-2093	Licença coletiva de e-mail do CMS para 1000 usuários por 1 ano
01-SSC-2087	Licença coletiva de e-mail do CMS para 50000 usuários por 1 ano

Informações de Pedidos, cont.

SKU	GERENCIAMENTO CENTRAL PARA 6210, 7210, 8200V
Licenças centrais de Spike	
01-SSC-2111	Spike do CMS para 1.000 usuários por 5 dias
01-SSC-2115	Spike do CMS para 50000 usuários por 5 dias
Complemento do Capture (assinatura)	
Entre em contato com o revendedor ** As licenças por assinatura têm suporte 24X7*	
SKU	**COMPLEMENTOS DO SONICWALL SMA**
01-SSC-2406	Complemento SMA 7210 FIPS
01-SSC-2405	Complemento SMA 6210 FIPS
01-SSC-9185	Web Application Firewall para SMA 500V por 1 ano (também disponível para SMA 210 e 410)
SKU	**SONICWALL SMA SECURE UPGRADE**
02-SSC-2794	SMA 210 Secure Upgrade Plus, pacote para 5 usuários com suporte 24X7 para até 25 usuários por 1 ano
02-SSC-2795	SMA 210 Secure Upgrade Plus, pacote para 5 usuários com suporte 24X7 para até 25 usuários por 3 anos
02-SSC-2798	SMA 410 Secure Upgrade Plus, pacote para 25 usuários com suporte 24X7 para até 100 usuários por 1 ano
02-SSC-2799	SMA 410 Secure Upgrade Plus, pacote para 25 usuários com suporte 24X7 para até 100 usuários por 3 anos
02-SSC-2893	SMA 6210 Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 1 ano
02-SSC-2894	SMA 6210 Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 3 anos
02-SSC-2895	SMA 7210 Secure Upgrade Plus, suporte 24X7 para até 250 usuários por 1 ano
02-SSC-2896	SMA 7210 Secure Upgrade Plus, suporte 24X7 para até 250 usuários por 3 anos
02-SSC-0860	SMA 8200V Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 1 ano
02-SSC-0862	SMA 8200V Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 3 anos
02-SSC-2807	SMA 500V Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 1 ano
02-SSC-2808	SMA 500V Secure Upgrade Plus, suporte 24X7 para até 100 usuários por 3 anos
SKU	**LICENÇA DE SPIKE PARA SMA (ADICIONAL NECESSÁRIO PARA ATINGIR A CAPACIDADE)**
01-SSC-2240	Licença de Spike do SMA 210 por 10 dias para 50 usuários (também disponível para SMA 410 e 500v)
01-SSC-7873	Licença de Spike do SMA 8200v por 10 dias para 5 a 2.500 usuários (também disponível para SMA 6210 e 7210)
02-SSC-4490	LICENÇA DE SPIKE DO SMA 500V PARA 250 USUÁRIOS POR 30 DIAS
02-SSC-4489	LICENÇA DE SPIKE DO SMA 500V PARA 250 USUÁRIOS POR 60 DIAS
02-SSC-4488	LICENÇA DE SPIKE DO SMA 200/210 PARA 50 USUÁRIOS POR 30 DIAS
02-SSC-4487	LICENÇA DE SPIKE DO SMA 200/210 PARA 50 USUÁRIOS POR 60 DIAS
02-SSC-4486	LICENÇA DE SPIKE DO SMA 400/410 PARA 250 USUÁRIOS POR 30 DIAS
02-SSC-4485	LICENÇA DE SPIKE DO SMA 400/410 PARA 250 USUÁRIOS POR 60 DIAS
02-SSC-4471	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 100 USUÁRIOS POR 63 DIAS
02-SSC-4473	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 500 USUÁRIOS POR 63 DIAS
02-SSC-4475	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 1.000 USUÁRIOS POR 30 DIAS
02-SSC-4477	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 5.000 USUÁRIOS POR 63 DIAS
02-SSC-4479	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 10.000 USUÁRIOS POR 63 DIAS
02-SSC-4481	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 25.000 USUÁRIOS POR 30 DIAS
02-SSC-4483	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 50.000 USUÁRIOS POR 63 DIAS
02-SSC-4472	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 100 USUÁRIOS POR 60 DIAS
02-SSC-4474	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 500 USUÁRIOS POR 60 DIAS
02-SSC-4476	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 1.000 USUÁRIOS POR 60 DIAS

Informações de Pedidos, cont.

SKU	LICENÇA DE SPIKE PARA SMA (ADICIONAL NECESSÁRIO PARA ATINGIR A CAPACIDADE)
02-SSC-4478	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 5.000 USUÁRIOS POR 60 DIAS
02-SSC-4480	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 10.000 USUÁRIOS POR 60 DIAS
02-SSC-4482	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 25.000 USUÁRIOS POR 60 DIAS
02-SSC-4484	COMPLEMENTO DE LICENÇA DE SPIKE DO SMA CMS PARA 50.000 USUÁRIOS POR 60 DIAS

** Contratos de suporte para vários anos e SKUs disponíveis. Entre em contato com o revendedor ou com a equipe de vendas para obter uma lista completa de SKUs*

Serviços Disponibilizados por Parceiros

Precisa de ajuda para planejar, implantar ou otimizar sua solução da SonicWall? Os Parceiros de Serviços Avançados da SonicWall são treinados para prestar serviços profissionais de nível mundial. Saiba mais em www.sonicwall.com/PES.

Sobre a SonicWall

A SonicWall vem lutando contra a indústria do crime cibernético há mais de 27 anos, defendendo empresas de pequeno e médio portes, grandes corporações e órgãos governamentais no mundo todo. Respaldadas pela pesquisa do SonicWall Capture Labs, nossas premiadas soluções de detecção e prevenção de violações em tempo real protegem mais de um milhão de redes e seus e-mails, aplicações e dados em mais de 215 países e territórios. Essas organizações operam com mais eficácia e com menos receios quanto à segurança. Para obter mais informações, visite www.sonicwall.com ou siga-nos no Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/

Datasheet-SecureMobileAccess-US-VG-1834