SONICWALL

SONICWALL SECURE MOBILE ACCESS (SMA)

Überall und jederzeit sicheren Zugriff auf Unternehmensressourcen in Multi-Cloud-Systemen basierend auf Benutzer- und Gerätidentität, Ort und bestätigter Vertrauenswürdigkeit.

SonicWall SMA ist ein einheitliches Secure Access Gateway, mit dem Organisationen jederzeit, überall und auf sämtlichen Geräten Zugang zu geschäftskritischen Unternehmensressourcen bereitstellen können. Mit ihrer Regel-Engine zur granularen Zugriffskontrolle, kontextsensibler Geräteauthentifizierung, VPN auf Anwendungsebene und einer erweiterten Authentifizierung mit Single-Sign-on unterstützt SMA moderne BYOD- und Mobilitätsstrategien in einer Multi-Cloud-Umgebung.

Mobilität und BYOD
Für Organisationen, die ihren Mitarbeitern BYOD und flexible Arbeitszeiten ermöglichen und Dritten Zugang zum Unternehmensnetzwerk bieten möchten, ist SMA die perfekte Lösung. SMA reduziert die Angriffsfläche für Bedrohungen und sorgt so für erstklassige Sicherheit. Gleichzeitig unterstützt die Lösung die neuesten Verschlüsselungsalgorithmen und Chiffrierverfahren und macht Organisationen so noch sicherer. Mit SonicWall SMA können Administratoren einen sicheren mobilen Zugriff bereitstellen und identitätsbasierte Berechtigungen definieren. Auf diese Weise erhalten Endbenutzer einen einfachen und schnellen Zugriff auf die benötigten Unternehmensanwendungen, -daten und -ressourcen. Gleichzeitig schützt die Einführung sicherer BYOD-Regeln Unternehmensnetzwerke und -daten vor unberechtigtem Zugriff und Malware.

Migration in die Cloud
Organisationen, die ihre Daten in die Cloud verlagern, bietet SMA eine Single-Sign-on (SSO)-Infrastruktur mit einem zentralen Webportal zur Authentifizierung der Anwender in einer hybriden IT-Umgebung. SMA sorgt für einen einheitlichen und nahtlosen Zugriff, ganz gleich, ob sich die Unternehmensressourcen im lokalen Netzwerk, im Web oder in einer gehosteten Cloud befinden. Für zusätzliche Sicherheit sorgt die Integration branchenweit führender Multi-Faktor-Authentifizierungstechnologien.

Managed Service-Provider
Managed Service Providern sowie Organisationen, die ihre eigene Infrastruktur hosten, bietet SMA eine sofort einsatzbereite Lösung, um ein hohes Maß an Business-Continuity und Skalierbarkeit zu gewährleisten. SMA unterstützt bis zu 20.000 gleichzeitige Verbindungen auf einer einzigen Appliance und lässt sich durch intelligentes Clustering für Hunderttausende von Anwendern nach oben skalieren. Dank Active-Active-Clustering und integriertem dynamischen Load Balancer, der den globalen Datenverkehr bedarfsgerecht dem am besten geeigneten Datencenter in Echtzeit zuweist, können Datencenter Kosten einsparen. Mit den SMA-Tools können Service Provider ihre Dienste ohne jegliche Ausfallzeiten bereitstellen und selbst anspruchsvollste SLAs erfüllen.

Mit SMA können IT-Abteilungen die Erwartungen der Anwender optimal erfüllen und den für das jeweilige Anwenderszenario sichersten Zugriff bereitstellen. Verfügbar als gehärtete, physische oder leistungsstarke virtuelle Appliance lässt sich SMA nahtlos in die bestehende On-Prem- und/oder Cloud-Infrastruktur einbinden. Organisationen können aus einer Reihe clientloser, webbasierter Secure Access-Möglichkeiten für Dritte oder Mitarbeiter mit privaten Geräten und einem konventionelleren, clientbasierten Full-Tunnel-VPN-Zugriff für Führungskräfte mit den unterschiedlichsten Geräten wählen. Egal, ob fünf Anwender auf Daten vom gleichen Standort aus oder Tausende von Anwendern auf Ressourcen in global verteilten Netzwerken zugreifen müssen – SonicWall SMA hat die passende Lösung, um einen zuverlässigen und sicheren Zugriff bereitzustellen.

Mit SonicWall SMA können Organisationen Mobilität und BYOD umsetzen und ihre Daten problemlos in die Cloud migrieren. SMA erhöht die Effizienz Ihrer Mitarbeiter und ermöglicht ihnen einen einheitlichen Zugriff.

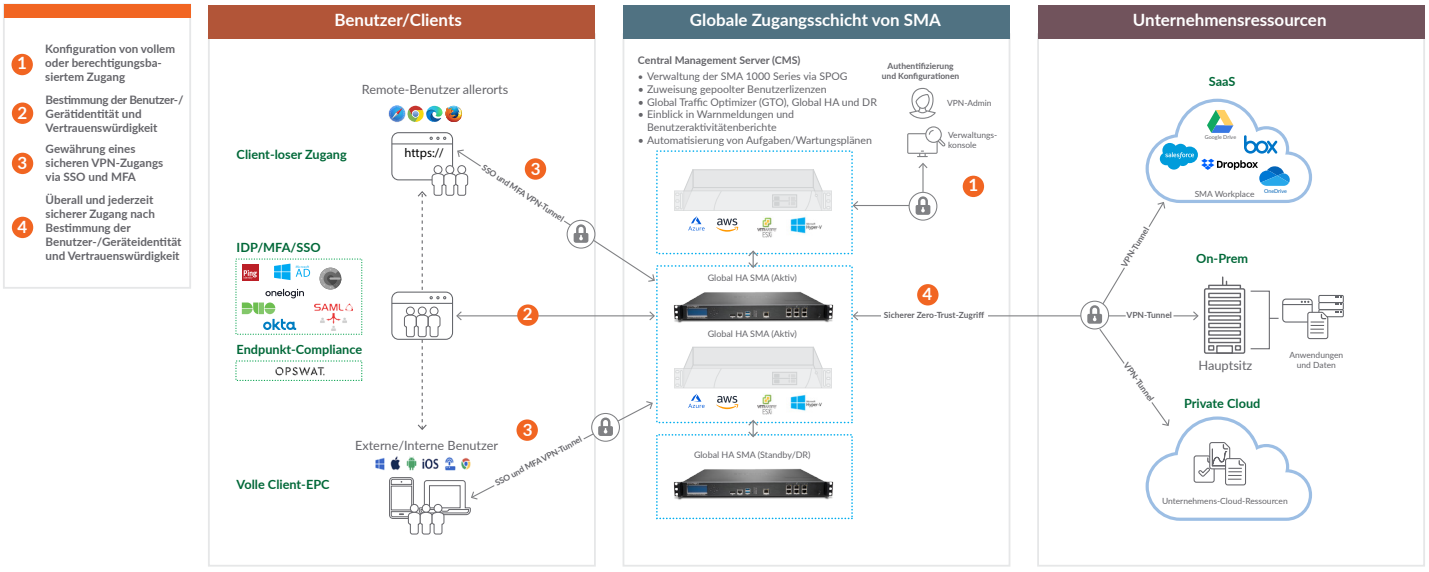
Vorteile:

- Einheitlicher Zugriff auf sämtliche Netzwerk- und Cloud-Ressourcen für einen sicheren Zugriff zu jeder Zeit, mit jedem Gerät und auf jede Anwendung
- Kontrolle, wer auf welche Ressourcen zugreifen kann durch Definition granularer Regeln mit der robusten Zugriffskontroll-Engine
- Höhere Produktivität durch föderiertes Single Sign-on für sämtliche SaaS- oder lokal gehostete Anwendungen mit einer einzigen URL
- Niedrigere TCO und reduzierte Komplexität beim Zugriffsmanagement durch Konsolidierung von Infrastrukturkomponenten in einer hybriden IT-Umgebung
- Transparenz für jedes angeschlossene Gerät und Zugriff auf der Grundlage von Regeln und dem Zustand des Endpunktgeräts
- Schutz vor Malware-Angriffen durch Prüfung sämtlicher, ins Netzwerk hochgeladener Dateien mit der Capture ATP Sandbox
- Schutz vor webbasierten Angriffen und PCI-Compliance mit Web Application Firewall Add-on
- Geo IP-Erkennung und Botnet-Schutz, um DDoS- und Zombie-Angriffe zu stoppen
- Sichere, native Agenten-Funktion mit Webbrowser-basiertem, clientlosen HTML5-Zugriff, ohne dass die Agenten auf den Endpunkt-Geräten installiert und gewartet werden müssen
- Aussagekräftige Informationen dank Echtzeit-Überwachung und umfassendem Reporting, um die richtigen Entscheidungen zu treffen
- Die Lösung wird als physische Appliance oder virtuelle Appliance in privaten Clouds auf ESXi oder Hyper-V oder in AWS oder Microsoft Azure Public Cloud Umgebungen implementiert
- Dynamische Verteilung von Zugriffslizenzen basierend auf dem Echtzeit-Bedarf mit automatisierter Endpunktzuweisung zu der Verbindung mit der höchsten Performance und geringsten Latenz
- Reduzierte Investitionskosten dank integrierter Lastverteilung ohne zusätzliche Hardware oder Services sowie ohne Auswirkungen auf den Anwender beim Appliance-Failover
- Schutz vor Geschäftsunterbrechungen in lokalen oder saisonalen Ausnahmesituationen durch Skalierung der Kapazität

SMA-Implementierung

Ein gehärtetes Edge-Gateway für einen sicheren Zugriff – jederzeit, überall und mit jedem beliebigen Gerät

SMA bietet End-zu-End-Sicherheit für den Fernzugriff auf Unternehmensressourcen, die On-Prem, in der Cloud und in hybriden Datenzentren gehostet werden. Es werden identitätsbasierte, regelgesteuerte Zugangskontrollen, kontextsensible Geräteauthentifizierung und VPN auf Anwendungsebene angewendet und der Zugriff auf Daten, Ressourcen und Anwendungen wird erst gewährt, nachdem Geräteidentität, Ort und Vertrauenswürdigkeit bestätigt wurden. Die Lösung wird flexibel als gehärtete Linux-Appliance oder virtuelle Appliance in privaten Clouds auf ESXi oder Hyper-V oder in AWS oder Microsoft Azure Public Cloud Umgebungen implementiert.



SMA-Implementierung in der Cloud / On-prem

Flexible Implementierung mit physischen und virtuellen Appliances

SonicWall SMA lässt sich als gehärtete High-Performance-Appliance oder Virtual Appliance (gemeinsame Nutzung der IT-Ressourcen zur Optimierung der Auslastung, Vereinfachung der Migration und Senkung der Investitionskosten) implementieren. Die Hardware-Appliances basieren auf einer Multicore-Architektur, die dank SSL-Beschleunigung, VPN-Durchsatz und leistungsstarken Proxys eine hohe Performance zur Bereitstellung eines zuverlässigen und sicheren Zugriffs bieten. In reglementierten und staatlichen Organisationen ist SMA auch mit FIPS 140-2 Level 2-Zertifizierung verfügbar. Die virtuellen SMA-Appliances bieten den gleichen zuverlässigen und sicheren Zugriff auf gängigen virtuellen Plattformen wie Microsoft Hyper-V, VMware ESX und AWS.

Appliance-übergreifende Nutzung von User-Lizenzen

Organisationen mit global verteilten Appliances können vom schwankenden Bedarf an User-Lizenzen aufgrund unterschiedlicher Zeitzonen profitieren. Egal, ob eine Organisation Full-VPN oder einfache ActiveSync-Lizenzen nutzt: SMAs zentrale Verwaltung nimmt die Lizenzen verwalteter Appliances von Regionen, in denen es Nacht ist oder die Büros schon geschlossen haben und der Bedarf folglich gering ist, und weist sie einer anderen Region mit hohem Bedarf zu.

Netzwerktransparenz mit kontextsensiblem Geräteprofiling

Eine erstklassige kontextsensible Authentifizierung garantiert, dass nur autorisierte Benutzer und vertrauenswürdige Geräte Zugang erhalten. Auch Laptops und PCs werden auf vorhandene bzw. fehlende Sicherheitssoftware, Client-Zertifikate und Geräte-ID überprüft. Bevor Mobilgeräten der Zugriff gewährt wird, werden sie abgefragt und auf essenzielle sicherheitsrelevante Informationen überprüft, u. a. Jailbreak- bzw. Root-Status, Geräte-ID, Zertifikatsstatus und Version des Betriebssystems. Wenn ein Gerät die Regelanforderungen nicht erfüllt, wird der Zugriff auf das Netzwerk verweigert. Dem Benutzer wird die Nichteinhaltung mitgeteilt.

Einheitlicher Zugang über ein zentrales Webportal

Mit SMA ist es nicht nötig, sich viele unterschiedliche Anwendungs-URLs zu merken und unzählige Lesezeichen zu pflegen. Die Lösung bietet ein zentrales Zugriffsportal, sodass die Anwender über eine einzige URL mit einem Standard-Webbrowser auf alle geschäftskritische Anwendungen zugreifen können. Nach der Anmeldung über einen Browser bekommt der Anwender ein personalisierbares Webportal im Browserfenster angezeigt, das eine zentrale Ansicht für den Zugriff auf sämtliche SaaS- oder lokale Anwendungen bietet. Das Portal zeigt nur die Links und personalisierten Lesezeichen an, die relevant für die jeweiligen Endpunkt-Geräte, -Benutzer oder -Gruppen sind. Es ist plattformunabhängig und unterstützt alle gängigen Geräteplattformen, einschließlich Windows, Mac OS, Linux, iOS und Android sowie eine Vielzahl von Browsern.

Föderiertes Single-Sign-on für SaaS- und lokale Anwendungen

Mit dem föderierten Single-Sign-on ist es nicht mehr notwendig, mehrere Passwörter zu haben. Außerdem werden schlechte Sicherheitspraktiken wie die Wiederverwendung von Passwörtern vermieden. SMA bietet föderiertes SSO sowohl für in der Cloud gehostete SaaS-Anwendungen als auch für lokal gehostete Anwendungen. Zusätzliche Sicherheit bietet die Integration unterschiedlicher Authentifizierungs-, Autorisierungs- und Abrechnungsserver sowie führender Multi-

Faktor-Authentifizierungstechnologien. Secure SSO wird erst dann auf autorisierten Endpunktgeräten bereitgestellt, wenn die SMA-Lösung den Health Status sowie die Einhaltung von Compliance-Vorgaben geprüft hat. Eine Regel-Engine sorgt dafür, dass der Zugriff nur auf freigegebene Anwendungen nach erfolgreicher Authentifizierung gewährt wird. Die Lösung unterstützt föderiertes SSO auch bei der Verwendung von VPN-Clients und bietet Kunden eine nahtlose Authentifizierungserfahrung, unabhängig davon, ob sie clientbasierten oder clientlosen sicheren Zugriff nutzen.

Schutz vor Sicherheitslücken und komplexen Bedrohungen

SonicWall SMA sorgt für zusätzliche Zugriffssicherheit, um Ihr Sicherheitskonzept zu verbessern und die Angriffsfläche für Bedrohungen zu reduzieren.

- SMA lässt sich mit der Cloud-basierten Multi-Engine-Sandbox SonicWall Capture ATP integrieren, um alle über unverwaltete Endpunktgeräte oder außerhalb des Unternehmensnetzwerks hochgeladenen Dateien zu prüfen. Auf diese Weise sind Anwender unterwegs genauso vor raffinierten Bedrohungen wie Ransomware oder Zero-Day Malware geschützt wie im Büro[1].
- Der SonicWall Web Application Firewall-Service bietet Unternehmen eine erschwingliche, gut integrierte Lösung für den Schutz interner, webbasierter Anwendungen. So können Sie die Vertraulichkeit Ihrer Daten sowie die Sicherheit interner Webservices gewährleisten, falls ein bösartiger oder unerlaubter Benutzerzugriff stattfindet.
- Geo-IP- und Botnet-Erkennung schützt Organisationen vor DDoS- und Zombie-Angriffen und verhindert, dass Endpunkte als Botnets missbraucht werden.

Nahtloser und sicherer Browser-basierter Zugriff ohne Client

Da SonicWall SMA ohne Client auskommt, müssen Administratoren keine Fat-Client-Komponenten manuell auf Computern installieren, die für den Remote-Zugriff eingesetzt werden. Es besteht keine Abhängigkeit von Java und die IT hat keinen zusätzlichen Aufwand, sodass sich die Nutzung des Remote-Zugriffs problemlos ausweiten lässt. Da keine Vorinstallation oder Vorkonfiguration nötig ist, können autorisierte Remote-Mitarbeiter von überall auf der Welt an beliebigen Rechnern arbeiten und sicher auf Unternehmensressourcen zugreifen. In seiner reinsten Form funktioniert der sichere Zugriff ausschließlich browserbasiert über HTML5, was den Benutzern ein nahtloses und einheitliches Erlebnis bietet.

Eine „Always-On“-Erfahrung

Für eine nahtlose Benutzererfahrung bietet SMA Always On VPN für verwaltete Windows Geräte. Administratoren können die Einstellungen so konfigurieren, dass eine VPN-Verbindung automatisch hergestellt wird, wenn ein autorisierter Endpoint-Client ein öffentliches oder nicht vertrauenswürdiges Netzwerk erkennt. Über ein einzelnes Login auf dem Windows-Gerät erhält der Benutzer eine sichere Verbindung zu den Unternehmensressourcen. Benutzer müssen sich nicht bei ihren VPN-Clients anmelden oder zusätzliche Kennwörter pflegen. Mobile Benutzer erhalten somit auf nahtlose Weise Zugriff auf geschäftskritische Ressourcen, gerade so als wären sie im Büro. Gleichzeitig werden IT-Administratoren in die Lage versetzt, die Kontrolle über verwaltete Geräte zu behalten und die Sicherheitshaltung der Organisation zu verbessern.

Intuitives Management und umfassendes Reporting

Die intuitive webbasierte Verwaltungsplattform von SonicWall, Central Management Server (CMS), sorgt für ein optimiertes Appliance-Management und bietet umfassende Reporting-Funktionen. Die benutzerfreundliche Oberfläche sorgt für Klarheit bei der Verwaltung von einzelnen oder mehreren Appliances und Regeln. Dabei lässt sich auf jeder Seite einsehen, wie die Einstellungen auf allen verwalteten Geräten konfiguriert sind. Eine einheitliche Regelverwaltung hilft Ihnen, Zugriffsregeln und -konfigurationen zu erstellen und zu überwachen. Mit einer einzigen Regel können Sie den Zugriff von Benutzern, Geräten und Anwendungen auf Daten, Server und Netzwerke kontrollieren. Die IT-Abteilung kann Routineaufgaben automatisieren und Aktivitäten planen, wodurch Sicherheitsteams von redundanten Aufgaben befreit werden und sich auf strategische Sicherheitsaufgaben, wie z. B. die Reaktion auf Vorfälle konzentrieren können. Dank benutzerfreundlichem Reporting und zentraler Anmeldung erhält die IT einen Einblick in die Zugriffstrends der Nutzer und den systemweiten Zustand.

Serviceverfügbarkeit rund um die Uhr

Organisationen müssen eine hohe Zuverlässigkeit und Verfügbarkeit ihrer Services garantieren, um jederzeit einen sicheren Zugriff auf geschäftskritische Anwendungen bereitstellen zu können. Die SMA-Appliances unterstützen konventionelle Active-Passive-Hochverfügbarkeit für Organisationen mit einem einzigen Datencenter und globale Hochverfügbarkeit mit Active-Active-Clustering für lokale oder verteilte Datencenter. Beide Hochverfügbarkeitsmodelle sorgen für ein nahtloses Anwendererlebnis mit Zero Impact Failover und Session-Persistence.

Implementierung des für Sie idealen VPN-Clients

Sie können aus einer Vielzahl von VPN-Clients wählen, um auf unterschiedlichen Endpunkten wie Laptops, Smartphones und Tablets einen regelbasierten, sicheren Remote-Zugriff bereitzustellen.

VPN-Client	Unterstütztes Betriebssystem	Unterstütztes SMA-Modell	Herausragendes Highlight
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows 10	Alle Modelle	Biometrische Authentifizierung, per App VPN und Durchsetzung von Endpunktkontrolle
Connect Tunnel (Thin-Client)	Windows, Mac OS und Linux	6200, 6210, 7200, 7210, 8200v, 9000	„In-Office“-Erlebnis mit zuverlässiger Endpunktkontrolle
NetExtender (Thin Client)	Windows und Linux	210, 410, 500v	Durchsetzung granularer Zugriffsregeln und erweiterter Netzwerkzugriff über native Clients

Geringere Investitionskosten dank integriertem Load Balancer

Die in die SMA-Appliance integrierte Lastverteilungsfunktion erreicht die Skalierbarkeit, die man von Implementierungen für mittelgroße Unternehmen und große Organisationen erwartet. Ausgewählte SMA-Appliancemodelle bieten eine dynamische Lastverteilung zur intelligenten Zuweisung von Sessionlasten und bedarfsgerechter Echtzeit-Verteilung der Benutzerlizenzen. Organisationen müssen daher nicht in externe Load Balancer investieren und können so ihre Investitionskosten reduzieren.

Versicherung bei unvorhergesehenen Ereignissen

Eine umfassende Business-Continuity- und DR-Lösung muss in Ausnahmesituationen mit erheblichen Spitzen beim Remote-Datenverkehr zurechtkommen und gleichzeitig die volle Kontrolle über Sicherheit und Kosten gewährleisten. Die SonicWall Spike License Packs für SMA beinhalten Add-On-Lizenzen, mit denen verteilte Unternehmen ihre Benutzeranzahl skalieren können. Auf diese Weise erreichen sie umgehend die maximale Kapazität und ermöglichen nahtlose Business-Continuity. Die Spike-Lizenzen funktionieren wie eine Versicherung für den Fall, dass der Kapazitätsbedarf vorübergehend um mehrere Dutzend oder sogar Hunderte zusätzliche Benutzer zunimmt.

Funktionen

Erweiterte Authentifizierung

Föderiertes Single Sign-on[2]	Durch SAML 2.0-Authentifizierung ermöglicht SMA einen föderierten SSO-Zugriff über ein zentrales Portal auf On-Premise- und Cloud-Ressourcen. Für zusätzliche Sicherheit sorgt die Durchsetzung von verketteter Multifaktor-Authentifizierung.
Multifaktor-Authentifizierung	Digitale X.509 Zertifikate Server- und Client-seitige digitale Zertifikate RSA SecurID, Dell Defender, Google Authenticator, Duo Security und weitere Einmalpasswort-/Zwei-Faktor-Authentifizierungstokens Common Access Card (CAC) Dual oder verkettete Authentifizierung Captcha-Unterstützung, Benutzername/Kennwort
SAML-Authentifizierung	SMA kann als SAML Identity Provider (IdP), SAML Service Provider (SP) oder Proxy eines bestehenden On-Prem IdP konfiguriert werden, um föderiertes Single Sign-On (SSO) mittels SAML 2.0 Authentifizierung zu ermöglichen.
Authentifizierungsrepositories	SMA bietet einfache Integration mit branchenüblichen Repositories für die einfache Verwaltung von Benutzerkonten und Kennwörtern. Auf Grundlage von Authentifizierungsmethoden wie RADIUS, LDAP oder Active Directory können Benutzer Gruppen dynamisch zugeordnet werden – auch in verschachtelten Gruppen. Gemeinsame oder benutzerdefinierte LDAP-Attribute können abgefragt werden, um eine bestimmte Autorisierung oder Geräteregistrierung zu prüfen.
Layer 3-7 Anwendungsproxy	SMA bietet flexible Proxyoptionen, wie z. B. Zugriff für Servicepartner über Direct Proxy, Zugriff für Vertragspartner über Reverse Proxy und Zugriff für Mitarbeiter auf Exchange über ActiveSync.
Reverse Proxy	Der erweiterte Reverse Proxy Service mit Authentifizierung erlaubt es Administratoren, ein Application Offloading Portal und Lesezeichen zu konfigurieren, sodass Benutzer nahtlos auf Remote-Anwendungen und -Ressourcen, einschließlich RDP und HTTP, zugreifen können. Diese Funktion unterstützt alle Browser, u. a. IE, Chrome und Firefox.
Eingeschränkte Kerberos-Delegierung	SMA unterstützt die Authentifizierung anhand einer vorhandenen Kerberos-Infrastruktur, die nicht darauf angewiesen ist, dass Front-End-Services einen Dienst delegieren.

Zugriffsmanagement

Access Control Engine (ACE)	Administratoren erlauben oder verweigern den Zugriff auf der Grundlage unternehmensweiter Regeln und veranlassen Maßnahmen zur Problembehebung für unter Quarantäne gestellte Sitzungen. ACE-objektbasierte Regeln verwenden Netzwerk-, Ressourcen-, Identitäts-, Geräte-, Anwendungs-, Daten- und Zeitelemente.
End Point Control (EPC)	Mit EPC können Administratoren Regeln zur granularen Zugriffskontrolle basierend auf dem Zustand der verbundenen Geräte durchsetzen. Mit der tiefen Betriebssystem-Integration sind viele Elemente zur Typenklassifizierung und Beurteilung der Risikofaktoren kombiniert. EPC-Abfragen erleichtern die Erstellung von Geräteprofilen anhand einer vordefinierten Liste von Anti-Virus-, Anti-Spyware- und Personal Firewall-Lösungen für Windows-, Mac- und Linux-Plattformen, wobei auch die Version und Aktualität der Signaturdateien berücksichtigt werden.
App Access Control (AAC)	Administratoren können definieren, welche konkreten mobilen Anwendungen auf welche Netzwerkressourcen über eigene App-Tunnel zugreifen dürfen. AAC-Regeln werden sowohl beim Client als auch beim Server durchgesetzt und bieten so einen zuverlässigen Schutz am Netzwerkrand.

Überlegene Sicherheit

Layer 3-SSL-VPN	Die SMA Series bietet leistungsstarke Layer 3-Tunnelfunktionen für zahlreiche Clientgeräte, die in den unterschiedlichsten Umgebungen laufen.
Kryptographie-Unterstützung	Konfigurierbare Sitzungslänge Chiffrierverfahren: AES 128 + 256 Bit, Triple DES, RC4 128 Bit Hashcodes: SHA-256 Elliptic Curve Digital Signature Algorithm (ECDSA)
Erweiterte Unterstützung für Chiffrierverfahren	Dank vorkonfigurierter Chiffrierverfahren bieten die SMA-Appliances einen hohen Sicherheitsstandard zur Einhaltung von Compliance-Anforderungen. Administratoren können die vorgegebenen Einstellungen für eine optimale Performance, Sicherheit oder Kompatibilität weiter verfeinern.
Sicherheitszertifizierungen	Zertifiziert für FIPS 140-2 Level 2, ICSA SSL-TLS, in Arbeit für Common Criteria, UC-APL
Sichere Dateifreigabe	Dank automatisierter Problembehebung lassen sich unbekannte Zero-Day-Angriffe wie Ransomware am Gateway stoppen. Dateien, die Anwender von unverwalteten Endpunkten mit sicherem Zugriff in die Unternehmensnetzwerke hochladen, werden von unserer Cloud-basierten Multi-Engine Capture ATP geprüft.
Web Application Firewall (WAF)	Schutz vor Protokoll- und Web-basierten Angriffen, um Finanzdienstleistungs-, Gesundheits- und E-Commerce-Organisationen sowie andere Unternehmen bei der Einhaltung von OWASP-Top 10- und PCI-Compliance-Anforderungen zu unterstützen.
Geo IP-Erkennung und Botnet-Schutz	Mit Geo IP-Erkennung und Botnet-Schutz können Kunden mit einem Mechanismus den Benutzerzugriff von verschiedenen geografischen Standorten aus zulassen oder einschränken.
TLS 1.3 Unterstützung	Verbesserte Sicherheit und Leistung sowie geringere Komplexität im Vergleich zu den Vorgängerversionen.

Intuitive Benutzererfahrung

Always-On VPN	Durch die automatische Herstellung einer sicheren Verbindung zum Unternehmensnetzwerk auf den vom Unternehmen ausgegebenen Windows-Geräten wird für erhöhte Sicherheit, Verkehrstransparenz und Compliance gesorgt.
Sichere Netzwerkerkennung (SND)	Der VPN-Client mit Network Aware-Modus von SMA erkennt, wenn sich das Gerät außerhalb des Firmengeländes befindet und verbindet sich automatisch mit dem VPN. Ist das Gerät wieder in einem vertrauenswürdigen Netzwerk, wird die VPN-Verbindung getrennt.
Clientloser Zugriff auf Ressourcen	SMA bietet einen sicheren Zugriff ohne Client mit HTML5-Browseragents, die RDP-, ICA-, VNC-, SSH- und Telnet-Protokolle bereitstellen.
Single-Sign-On Portal	Das WorkPlace-Portal bietet eine benutzerfreundliche, personalisierbare zentrale Ansicht für einen sicheren Zugriff mit Single Sign-on (SSO) auf sämtliche Ressourcen in einer hybriden IT-Umgebung. Es ist keine zusätzliche Anmeldung oder VPN erforderlich.
Layer 3-Tunneling	Administratoren können sich zwischen Split-Tunnel oder dem Modus „Alles weiterleiten“ mit SSL/TLS-Tunneling und optionalem ESP-Fallback für maximale Performance entscheiden.
HTML5-Datei-Explorer[1]	Mit modernen Dateibrowsern können Benutzer ganz einfach über beliebige Webbrowser auf Dateifreigaben zugreifen.
Integration von Mobilbetriebssystemen	Mobile Connect wird auf allen Betriebssystem-Plattformen unterstützt, sodass die Anwender bei der Auswahl ihrer Mobilgeräte flexibel sind.

Ausfallsicherheit

Global Traffic Optimizer (GTO)	SMA bietet eine globale Lastverteilung des Datenverkehrs ohne jegliche Auswirkungen auf die Anwender. Der Verkehr wird an den am besten geeigneten Datencenter mit der höchsten Performance geleitet.
Dynamische Hochverfügbarkeit[2]	SMA unterstützt Active/Passive und bietet eine Active/Active-Konfiguration für Hochverfügbarkeit, egal ob in einem einzigen Datenzentrum oder über mehrere geografisch verteilte Datenzentren hinweg implementiert.
Universal Session Persistence[1]	Bietet Anwendern ein reibungsloses Erlebnis mit Zero Impact Failover. Geht eine Appliance offline, verteilt die intelligente Clusteringfunktion der SMA-Lösung die Anwender mit ihren Sitzungsdaten um, ohne dass sie sich neu authentifizieren müssen.
Skalierbare Performance	Die SMA-Appliances erlauben eine exponentielle Performance-Skalierung durch die Implementierung mehrerer Appliances. Auf diese Weise werden einzelne Ausfallpunkte eliminiert. Horizontales Clustering ermöglicht die uneingeschränkte Kombination aus physischen und virtuellen SMA-Appliances.
Dynamische Lizenzierung	Benutzer-Lizenzen sind nicht mehr an einzelne SMA-Appliances gebunden. Anwender können dynamisch und bedarfsgerecht auf die verwalteten Appliances verteilt und neu zugeordnet werden.

Zentrale Verwaltung und Überwachung

Central Management System (CMS)	CMS bietet eine zentralisierte, webbasierte Verwaltung für alle SMA Funktionen.
Konfigurierbare Warnmeldungen	Warnmeldungen lassen sich so konfigurieren, dass sie SNMP-Traps erzeugen, die von jedem beliebigen Network Management System (NMS) in der IT-Infrastruktur überwacht werden können. Administratoren können auch Warnmeldungen für Capture ATP-Dateiscans und Festplattennutzung für einen sofortigen Eingriff konfigurieren.
Echtzeit-Dashboard	Ein konfigurierbares Echtzeit-Dashboard ermöglicht es dem IT-Administrator, Zugangsprobleme schnell und einfach zu diagnostizieren und wertvolle Erkenntnisse für die Fehlerbehebung zu gewinnen.
SIEM-Integration	Echtzeit-Ausgabe an zentrale SIEM-Datenkollektoren erlaubt den Sicherheitsteams die Korrelierung ereignisgesteuerter Aktivitäten, um Einblick in den Ende-zu-Ende-Workflow eines bestimmten Benutzers oder einer bestimmten Anwendung zu erhalten. Das ist für das Security Incident Management und forensische Analysen wichtig.
Scheduler	Der Scheduler ermöglicht die Planung von Wartungsaufgaben wie die Implementierung von Regeln, die Replizierung von Konfigurationseinstellungen und den Neustart von Services, ohne dass ein manuelles Eingreifen nötig ist.

Erweiterungsmöglichkeiten

Management-APIs	Management-APIs erlauben eine vollständig programmatische Verwaltungskontrolle über sämtliche Objekte innerhalb einer einzigen SMA oder globalen CMS-Umgebung.
Endbenutzer-APIs	Endbenutzer-APIs bieten eine umfassende Kontrolle über die gesamte Anmeldung, Authentifizierung und den Endpunkt-Workflow.
Zwei-Faktor-Authentifizierung (2FA)	SMA bietet 2FA durch Integration mit führenden Lösungen für zeitbasierte Einmalpasswörter (TOTP) wie Google Authenticator, Microsoft Authenticator, Duo Security etc.
MDM-Integration	SMA lässt sich mit führenden Enterprise Mobile Management (EMM)-Produkten wie Airwatch und MobileIron integrieren.
Integration mit weiteren Drittanbieterprodukten	SMA erlaubt die Integration von Produkten führender Anbieter wie OPSWAT, um einen erweiterten Bedrohungsschutz zu gewährleisten.

[1]*Verfügbar mit SMA OS 12.1 oder höher*

[2] *Erweitert in SMA 12.1*

Die Funktionen im Überblick (Vergleich nach Modell)

Kategorie	Funktion	210	410	500v	6210	7210	8200v
Implementierung	Betriebssystem	Ab v9.0	Ab v9.0	Ab v9.0	Ab v12.1	Ab v12.1	Ab v12.1
	Unterstützte Hypervisors	–	–	VMware ESXi / Microsoft Hyper-V	–	–	VMware ESXi / Microsoft Hyper-V
	Unterstützte Public-Cloud-Plattformen	–	–	AWS/Azure	–	–	AWS/Azure
Durchsatz	Max. Anzahl gleichzeitiger Sitzungen	200	400	250	2.000	10.000	5.000
	Max. SSL/TLS-Durchsatz	560 MBit/s	844 MBit/s	265 MBit/s	1,3 GBit/s	5,0 GBit/s	1,58 GBit/s
Client-Zugriff	Layer-3-Tunnel	•	•	•	•	•	•
	Split-Tunnel und „Alles weiterleiten“	•	•	•	•	•	•
	Always-On VPN	•	•	•	•	•	•
	Automatische ESP-Encapsulation	–	–	–	•	•	•
	HTML5 (RDP, VNC, ICA, SSH, Telnet, Network Explorer)	•	•	•	•	•	•
	Sichere Netzwerkerkennung	–	–	–	•	•	•
	Dateibrowser (CIFS/NFS)	•	•	•	•	•	•
	Citrix XenDesktop/XenApp	•	•	•	•	•	•
	VMware View	–	–	–	•	•	•
	On-Demand-Tunnel	–	–	–	•	•	•
	Chrome/Firefox-Erweiterungen	–	–	–	•	•	•
	CLI-Tunnel-Unterstützung	–	–	–	•	•	•
	Mobile Connect (iOS, Android, Chrome, Win 10, Mac OSX)	•	•	•	•	•	•
	NetExtender (Windows, Linux)	•	•	•	–	–	–
	Connect Tunnel (Windows, Mac OSX, Linux)	–	–	–	•	•	•
	Exchange ActiveSync	•	•	•	•	•	•
Mobiler Zugriff	Pro-App-VPN	–	–	–	•	•	•
	Durchsetzung von Anwendungskontrolle	–	–	–	•	•	•
	App-ID-Validierung	–	–	–	•	•	•
Benutzerportal	Branding	•	•	•	•	•	•
	Personalisierung	–	–	–	•	•	•
	Lokalisierung	•	•	•	•	•	•
	Benutzerdefinierte Lesezeichen	•	•	•	•	•	•
	Benutzerdefinierte URL-Unterstützung	•	•	•	•	•	•
	Unterstützung von SaaS-Anwendungen	–	–	–	•	•	•
Sicherheit	FIPS 140-2	–	–	–	•	•	–
	ICSA SSL-TLS	•	•	•	•	•	•
	Suite B-Cipher	–	–	–	•	•	•
	Dynamische EPC-Abfragen	•	•	•	•	•	•
	Role Based Access Control (RBAC)	–	–	–	•	•	•
	Endpunkt-Registrierung	•	•	•	•	•	•
	Sichere Dateifreigabe (Capture ATP)	•	•	•	•	•	•
	Endpunkt-Quarantäne	•	•	•	•	•	•
	OSCP CRL-Validierung	–	–	–	•	•	•
	Auswahl von Chiffrierverfahren	–	–	–	•	•	•
	PCI- und Client-Zertifikate	•	•	•	•	•	•
	Geo IP-Filter	•	•	•	–	–	–
	Botnet-Filter	•	•	•	–	–	–
	Forward Proxy	•	•	•	•	•	•
	Reverse Proxy	•	•	•	•	•	•
Authentifizierungs- und Identitätsdienste	SAML 2.0	•	•	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•
	SAML Identity Provider (IdP)	•	•	•	•	•	•
	Unterstützung für biometrische Geräte	•	•	•	•	•	•
	Face ID-Unterstützung für iOS	•	•	•	•	•	•
	Zwei-Faktor-Authentifizierung (2FA)	•	•	•	•	•	•
	Multi-Faktor-Authentifizierung (MFA)	–	–	–	•	•	•

Die Funktionen im Überblick (Vergleich nach Modell, Forts.)

Kategorie	Funktion	210	410	500v	6210	7210	8200v
Authentifizierungs- und Identitätsdienste, Forts.	Verkettete Authentifizierung	–	–	–	•	•	•
	Ausgabe von Einmalpasswörtern (OTP) per E-Mail oder SMS	•	•	•	•	•	•
	Common Access Card (CAC)-Unterstützung	–	–	–	•	•	•
	Unterstützung für X.509-Zertifikat	•	•	•	•	•	•
	Captcha-Integration	–	–	–	•	•	•
	Remote-Passwort-Änderungen	•	•	•	•	•	•
	Formularbasiertes SSO	•	•	•	•	•	•
	Föderiertes SSO	–	–	–	•	•	•
	Session Persistence	–	–	–	•	•	•
	Automatische Anmeldung	•	•	•	•	•	•
Zugriffskontrolle	Gruppen-AD	•	•	•	•	•	•
	LDAP-Attribute	•	•	•	•	•	•
	Geolokalisierungsregeln	•	•	•	–	–	–
	Kontinuierliche Endpunktüberwachung	•	•	•	•	•	•
Verwaltung	Verwaltungsschnittstelle (Ethernet)	–	–	–	•	•	•
	Verwaltungsschnittstelle (Konsole)	–	–	–	•	•	•
	HTTPS-Verwaltung	•	•	•	•	•	•
	SSH-Verwaltung	–	–	–	•	•	•
	SNMP MIBS	•	•	•	•	•	•
	Syslog und NTP	•	•	•	•	•	•
	Nutzungskontrolle	•	•	•	•	•	•
	Konfigurations-Rollback	•	•	•	•	•	•
	Zentrale Verwaltung	–	–	–	•	•	•
	Zentrales Reporting	–	–	–	•	•	•
	REST-APIs zur Verwaltung	–	–	–	•	•	•
	REST-APIs zur Authentifizierung	–	–	–	•	•	•
	RADIUS Accounting	–	–	–	•	•	•
	Aufgabenplanung	–	–	–	•	•	•
	Zentralisierte Sessionlizenzierung	–	–	–	•	•	•
	Ereignisgesteuertes Auditing	–	–	–	•	•	•
Netzwerk	IPv6	•	•	•	•	•	•
	Globale Lastverteilung	–	–	–	•	•	•
	Server-Lastverteilung	•	•	•	–	–	–
	TCP-Status-Replikation	•	•	•	•	•	•
	Cluster State-Failover	–	–	–	•	•	•
	Active/Passive-Hochverfügbarkeit	–	•	•	•	•	•
	Active/Active-Hochverfügbarkeit	–	–	–	•	•	•
	Horizontale Skalierbarkeit	–	–	–	•	•	•
	Einzelne oder mehrere FQDNs	–	–	–	•	•	•
	L3-7 Smart-Tunnel-Proxy	•	•	•	•	•	•
	L7 Anwendungsproxy	•	•	•	•	•	•
Integration	Unterstützung für 2FA-TOTP	•	•	•	•	•	•
	Unterstützung für EMM- und MDM-Produkte	–	–	–	•	•	•
	Unterstützung für SIEM-Produkte	–	–	–	•	•	•
	TPAM-Password-Vault	–	–	–	•	•	•
	Unterstützung für ESX Hypervisor	–	–	•	–	–	•
	Unterstützung für Hyper-V Hypervisor	–	–	•	–	–	•
Lizenzierungs-optionen	Abo-basierte Lizenzen	–	–	–	•	•	•
	Unbefristete Lizenzen mit Support	•	•	•	•	•	•
	Web Application Firewall (WAF)	•	•	•	–	–	–
	Spike-Lizenzierung	•	•	•	•	•	•
	Abgestufte Lizenzierung	–	–	–	•	•	•
	Virtual Assist	•	•	•	–	–	–

** Weitere Informationen zu VPN-Clients erhalten Sie unter: https://www.sonicwall.com/en-us/products/remote-access/vpn-client*

Upgrades auf High-End-Appliances bringen viele Vorteile

Höhere Performance | Mehr Durchsatz | Erweiterte Funktionen | Verbesserte Skalierbarkeit

Appliance - Technische Daten

Sie können aus einer Reihe speziell entwickelter Secure Mobile Access (SMA)-Appliances wählen. Profitieren Sie von den flexiblen Implementierungsoptionen mit virtuellen und physischen Appliances.

Physische Appliance - Technische Daten

Leistung	SMA 210	SMA 410	SMA 6210	SMA 7210
Gleichzeitige Sitzungen/Benutzer	Bis zu 200	Bis zu 400	Bis zu 2.000	Bis zu 10.000
SSL VPN-Durchsatz* (bei max. CCU)	560 MBit/s	844 MBit/s	Bis zu 800 MBit/s	Bis zu 5,0 GBit/s
Formfaktor	1U	1U	1U	1U
Abmessungen	43 x 26 x 4,5 cm	43 x 26 x 4,5 cm	43 x 41,5 x 4,5 cm	43 x 41,5 x 4,5 cm
Gewicht	5 kg	5 kg	8 kg	8,3 kg
Beschleunigung von Verschlüsselungsdaten (AES-NI)	NEIN	NEIN	JA	JA
Spezieller Management-Port	NEIN	NEIN	JA	JA
SSL-Beschleunigung	NEIN	NEIN	JA	JA
Speicher	4 GB (Flash-Speicher)	4 GB (Flash-Speicher)	2 x 1 TB SATA; RAID 1	2 x 1 TB SATA; RAID 1
Schnittstellen	(2) GB Ethernet, (2) USB, (1) Konsole	(4) GB Ethernet, (2) USB, (1) Konsole	(6)-Port 1GE, (2) USB, (1) Konsole	(6)-Port 1GE, (2)-Port 10 Gigabit SFP+, (2) USB, (1) Konsole
Speicher	4 GB	8 GB	8 GB DDR4	16 GB DDR4
TPM-Chip	NEIN	NEIN	JA	JA
Prozessor	4 Kerne	8 Kerne	4 Kerne	4 Kerne
MTBF (bei 25 °C) in Stunden	61.815	60.151	70.127	129.601
Betrieb und Compliance	**SMA 210**	**SMA 410**	**SMA 6210**	**SMA 7210**
Stromversorgung	Feste Stromversorgung	Feste Stromversorgung	Feste Stromversorgung	Duale Stromversorgung, hot-swappable
Eingangsnennwerte	100-240 V AC, 50-60 MHz	100-240 V AC, 50-60 MHz	100–240 V AC, 1,1 A	100–240 V AC, 1,79 A
Leistungsaufnahme	26,9 W	31,9 W	77 W	114 W
Gesamtwärmeabgabe	92 BTU	109 BTU	264 BTU	389 BTU
Umweltvorschriften	WEEE, EU RoHS, China RoHS			
Erschütterungen (außer Betrieb)	110 g, 2 ms			
Emissionen	FCC, ICES, CE, C-Tick, VCCI; MIC			
Sicherheit	TÜV/GS, UL, CE PSB, CCC, BSMI, CB Scheme			
Betriebstemperatur	0 °C bis 40 °C			
FIPS-Zertifizierung	NEIN	NEIN	FIPS 140-2 Level 2 mit Manipulationsschutz	

** Der Durchsatz kann je nach Implementierung und Konnektivität variieren. Die veröffentlichten Werte entsprechen unseren internen Laborbedingungen.*

Virtuelle Appliance - Technische Daten

Technische Daten	SMA 500v (ESX/ESXi/Hyper-V)	SMA 8200v (ESX/ESXi/Hyper-V)
Gleichzeitige Sitzungen	Bis zu 250 Benutzer	Bis zu 5000
SSL-VPN-Durchsatz* (bei max. CCU)	Bis zu 186 MBit/s	Bis zu 1,58 GBit/s
Zugewiesener Speicher	2 GB	8 GB
Prozessor	1 Kern	4 Kerne
SSL-Beschleunigung	NEIN	JA
Benötigter Festplattenspeicher	2 GB	64 GB (Standard)
Installiertes Betriebssystem	Linux	Gehärtetes Linux
Spezieller Management-Port	NEIN	JA

** Der Durchsatz kann je nach Implementierung und Konnektivität variieren. Die veröffentlichten Werte entsprechen unseren internen Laborbedingungen. SMA 8200v auf Hyper-V für bis zu 5.000 gleichzeitige Sessions skalierbar mit bis zu 1,58 GBit/s SSL-VPN-Durchsatz unter SMA OS 12.1 mit Windows Server 2016*

Bestellinformationen

ARTIKELNUMMER	SONICWALL SECURE MOBILE ACCESS (SMA) APPLIANCE
02-SSC-2800	SMA 210 mit Lizenz für 5 Benutzer
02-SSC-2801	SMA 410 mit Lizenz für 25 Benutzer
01-SSC-8469	SMA 500v mit Lizenz für 5 Benutzer
02-SSC-0978	SMA 7210 mit Administrator-Testlizenz
02-SSC-0976	SMA 6210 mit Administrator-Testlizenz
01-SSC-8468	SMA 8200v (virtuelle Appliance)
ARTIKELNUMMER	**SONICWALL SMA BENUTZERLIZENZEN**
01-SSC-9182	SMA 500V Zusätzlich 5 Benutzer (auch für SMA 210 verfügbar)
01-SSC-2414	SMA 500V Zusätzlich 100 Benutzer (auch für SMA 410 verfügbar)
01-SSC-7856	SMA Lizenz für 5 Benutzer - kombinierbar mit 6210, 7210, 8200v
01-SSC-7860	SMA Lizenz für 100 Benutzer - kombinierbar mit 6210, 7210, 8200v
01-SSC-7865	SMA Lizenz für 5000 Benutzer - kombinierbar mit 7210, 8200v
ARTIKELNUMMER	**SONICWALL SMA SUPPORTVERTRAG**
01-SSC-9191	24/7 Support für SMA 500V bis zu 25 Benutzer 1 Jahr (auch verfügbar für SMA 210 und 410)
01-SSC-2326	24/7 Support für SMA 6210 100 Benutzer 1 Jahr - kombinierbar
01-SSC-2350	24/7 Support für SMA 7210 500 Benutzer 1 Jahr - kombinierbar
01-SSC-8434	24/7 Support für SMA 8200V 5 Benutzer 1 Jahr - kombinierbar (auch verfügbar für SMA 6210, 7210)
01-SSC-8446	24/7 Support für SMA 8200V 100 Benutzer 1 Jahr - kombinierbar (auch verfügbar für SMA 6210, 7210)
01-SSC-7913	24/7 Support für SMA 8200V 5000 Benutzer 1 Jahr - kombinierbar (auch verfügbar für SMA 6210, 7210)
ARTIKELNUMMER	**ZENTRALE VERWALTUNG FÜR 6210, 7210, 8200V**
Lizenz für CMS-Appliance	
01-SSC-8535	CMS-Basislizenz + 3 Appliances (kostenlos - für Testzwecke und Nutzung mit Abo-Benutzerlizenzen)
01-SSC-8536	CMS-Lizenz für 100 Appliances 1 Jahr (zur Nutzung mit Abo-Benutzerlizenzen)
01-SSC-3369	CMS-Basislizenz + 3 Appliances (kostenlos - zur Nutzung mit unbefristeten Benutzerlizenzen)
01-SSC-3402	CMS-Lizenz für 100 Appliances 1 Jahr (zur Nutzung mit unbefristeten Benutzerlizenzen)
Zentrale Benutzerlizenzen (Abo)	
01-SSC-2298	CMS Gepoolte Lizenz 10 Benutzer 1 Jahr
01-SSC-8539	CMS Gepoolte Lizenz 1000 Benutzer 1 Jahr
01-SSC-5339	CMS Gepoolte Lizenz 50000 Benutzer 1 Jahr
Zentrale Benutzerlizenzen (unbefristet)	
01-SSC-2053	CMS Unbefristete Lizenz 10 Benutzer
01-SSC-2058	CMS Unbefristete Lizenz 1000 Benutzer
01-SSC-2063	CMS Unbefristete Lizenz 50000 Benutzer
Support für zentrale Benutzerlizenzen (unbefristet)	
01-SSC-2065	CMS 24/7 Support 1 Jahr 10 Benutzer
01-SSC-2070	CMS 24/7 Support 1 Jahr 1000 Benutzer
01-SSC-2075	CMS 24/7 Support 1 Jahr 50000 Benutzer
Zentrale ActiveSync-Lizenzen (Abo)	
01-SSC-2088	CMS Gepoolte E-Mail-Lizenz 10 Benutzer 1 Jahr
01-SSC-2093	CMS Gepoolte E-Mail-Lizenz 1000 Benutzer 1 Jahr
01-SSC-2087	CMS Gepoolte E-Mail-Lizenz 50000 Benutzer 1 Jahr

Bestellinformationen Forts.

ARTIKELNUMMER	ZENTRALE VERWALTUNG FÜR 6210, 7210, 8200V
Zentrale Spike-Lizenzen	
01-SSC-2111	CMS Spike 1000 Benutzer 5 Tage
01-SSC-2115	CMS Spike 50000 Benutzer 5 Tage
Capture-Add-on (Abo)	
Wenden Sie sich an Ihren Wiederverkäufer ** Abolizenzen inklusive 24/7-Support*	
ARTIKELNUMMER	**SONICWALL SMA ADD-ONS**
01-SSC-2406	SMA 7210 FIPS Add-on
01-SSC-2405	SMA 6210 FIPS Add-on
01-SSC-9185	SMA 500V Web Application Firewall 1 Jahr (auch verfügbar für SMA 210 und 410)
ARTIKELNUMMER	**SONICWALL SMA SECURE UPGRADE**
02-SSC-2794	SMA 210 Secure Upgrade Plus, 5 Benutzer Bündel mit 24/7 Support bis zu 25 Benutzer 1 Jahr
02-SSC-2795	SMA 210 Secure Upgrade Plus, 5 Benutzer Bündel mit 24/7 Support bis zu 25 Benutzer 3 Jahre
02-SSC-2798	SMA 410 Secure Upgrade Plus, 25 Benutzer Bündel mit 24/7 Support bis zu 100 Benutzer 1 Jahr
02-SSC-2799	SMA 410 Secure Upgrade Plus, 25 Benutzer Bündel mit 24/7 Support bis zu 100 Benutzer 3 Jahre
02-SSC-2893	SMA 6210 Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 1 Jahr
02-SSC-2894	SMA 6210 Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 3 Jahre
02-SSC-2895	SMA 7210 Secure Upgrade Plus, 24/7 Support bis zu 250 Benutzer 1 Jahr
02-SSC-2896	SMA 7210 Secure Upgrade Plus, 24/7 Support bis zu 250 Benutzer 3 Jahre
02-SSC-0860	SMA 8200V Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 1 Jahr
02-SSC-0862	SMA 8200V Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 3 Jahre
02-SSC-2807	SMA 500V Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 1 Jahr
02-SSC-2808	SMA 500V Secure Upgrade Plus, 24/7 Support bis zu 100 Benutzer 3 Jahre
ARTIKELNUMMER	**SPIKE-LIZENZ FÜR SMA (ABSTUFUNG ERFORDERLICH, UM KAPAZITÄT ZU ERREICHEN)**
01-SSC-2240	SMA 210 10 Tage 50 Benutzer Spike-Lizenz (auch verfügbar für SMA 410 und 500v)
01-SSC-7873	SMA 8200v 10 Tage 5 - 2500 Benutzer Spike-Lizenz (auch verfügbar für SMA 6210, 7210)
02-SSC-4490	SMA 500V 30 TAGE 250 BENUTZER SPIKE-LIZENZ
02-SSC-4489	SMA 500V 60 TAGE 250 BENUTZER SPIKE-LIZENZ
02-SSC-4488	SMA 200/210 30 TAGE 50 BENUTZER SPIKE-LIZENZ
02-SSC-4487	SMA 200/210 60 TAGE 50 BENUTZER SPIKE-LIZENZ
02-SSC-4486	SMA 400/410 30 TAGE 250 BENUTZER SPIKE-LIZENZ
02-SSC-4485	SMA 400/410 60 TAGE 250 BENUTZER SPIKE-LIZENZ
02-SSC-4471	SMA CMS SPIKE ZUSATZLIZENZ 100 BENUTZER 30 TAGE
02-SSC-4473	SMA CMS SPIKE ZUSATZLIZENZ 500 BENUTZER 30 TAGE
02-SSC-4475	MA CMS SPIKE-ZUSATZLIZENZ 1.000 BENUTZER 30 TAGE
02-SSC-4477	SMA CMS SPIKE ZUSATZLIZENZ 5.000 BENUTZER 30 TAGE
02-SSC-4479	SMA CMS SPIKE ZUSATZLIZENZ 10.000 BENUTZER 30 TAGE
02-SSC-4481	MA CMS SPIKE-ZUSATZLIZENZ 25.000 BENUTZER 30 TAGE
02-SSC-4483	SMA CMS SPIKE ZUSATZLIZENZ 50.000 BENUTZER 30 TAGE
02-SSC-4472	SMA CMS SPIKE ZUSATZLIZENZ 100 BENUTZER 60 TAGE
02-SSC-4474	SMA CMS SPIKE ZUSATZLIZENZ 500 BENUTZER 60 TAGE
02-SSC-4476	SMA CMS SPIKE ZUSATZLIZENZ 1.000 BENUTZER 60 TAGE

Bestellinformationen Forts.

ARTIKELNUMMER	SPIKE-LIZENZ FÜR SMA (ABSTUFUNG ERFORDERLICH, UM KAPAZITÄT ZU ERREICHEN)
02-SSC-4478	SMA CMS SPIKE ZUSATZLIZENZ 5.000 BENUTZER 60 TAGE
02-SSC-4480	SMA CMS SPIKE ZUSATZLIZENZ 10.000 BENUTZER 60 TAGE
02-SSC-4482	SMA CMS SPIKE ZUSATZLIZENZ 25.000 BENUTZER 60 TAGE
02-SSC-4484	SMA CMS SPIKE ZUSATZLIZENZ 50.000 BENUTZER 60 TAGE

** Artikel und Supportverträge sind auch für mehrere Jahre erhältlich. Eine Liste mit allen Artikelnummern erhalten Sie bei Ihrem Händler oder Ansprechpartner*

Partner Enabled Services

Brauchen Sie Hilfe bei der Planung, Einbindung oder Optimierung Ihrer SonicWall-Lösung? SonicWall Advanced Services Partner sind umfassend ausgebildet, um Ihnen erstklassigen professionellen Service zu bieten. Weitere Informationen finden Sie auf www.sonicwall.com/PES.

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. SonicWall schützt Organisationen bei der Mobilisierung für die neue Geschäftsnormalität mit nahtlosem Schutz, der die raffiniertesten Cyberangriffe an den durch eine zunehmend grenzenlose Remote-, Mobil- und Cloud-fähige Belegschaft entstehenden Schwachstellen stoppt. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035 USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

SONICWALL®