SonicWall Secure Mobile Access (SMA)

Einheitliches Secure Access Gateway zur optimalen Umsetzung von Mobilität, BYOD und Cloud-Migraton

SonicWall SMA ist ein einheitliches Secure Access Gateway, mit dem Organisationen jederzeit, überall und auf sämtlichen Geräten Zugang zu geschäftskritischen Unternehmensressourcen bereitstellen können. Dank Regel-Engine zur granularen Zugriffskontrolle, kontextsensibler Geräteauthentifizierung, VPN auf Anwendungsebene und einer erweiterten Authentifizierung mit Singe-Sign-on ermöglicht SMA die Umsetzung von BYOD und Mobilität in einer hybriden IT-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 rollenbasierte 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 Anwender 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 anspruchvollste 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 bestehende IT-Infrastrukturen 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 Anwender auf Ressourcen in global verteilten Datencentern 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.

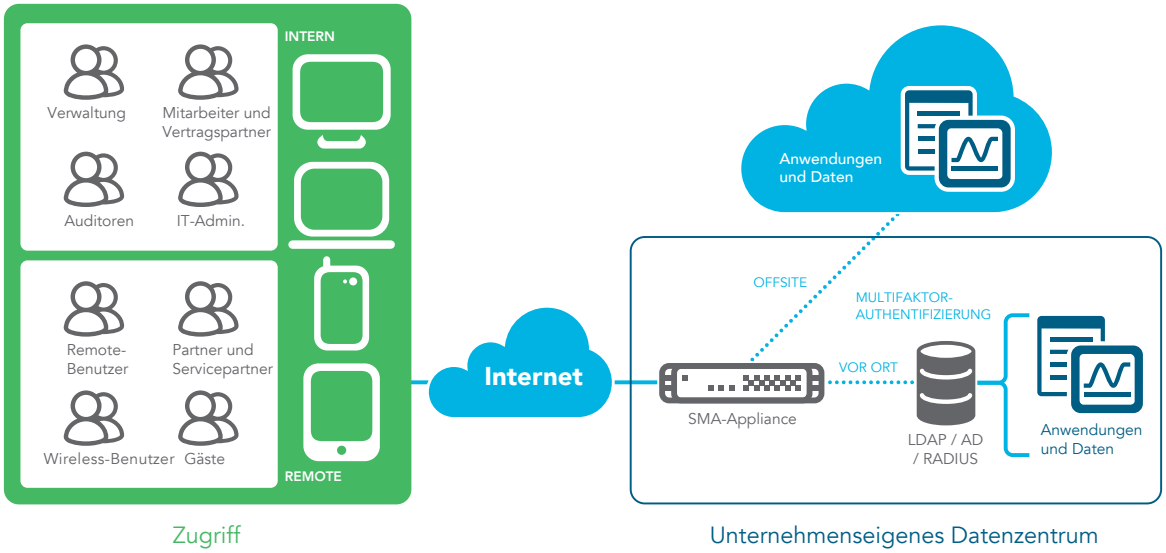
Vorteile:

- 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 Definieren granularer Regeln mit der robusten Zugriffskontroll-Engine
- Höhere Produktivität durch Federated 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 DoS- und Zombie-Angriffe zu stoppen
- Sichere, native Agentfunktion mit Webbrowser-basiertem, clientlosen HTML5-Zugriff, ohne dass die Agents auf den Endpunkt-Geräten installiert und gewartet werden müssen
- Aussagekräftige Informationen dank Echtzeit-Überwachung und umfassendem Reporting, um die richtigen Entscheidungen zu treffen
- Einfache Implementierung mit flexiblen virtuellen und physischen Appliances je nach geschäftlichen Anforderungen
- 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 umgehende Skalierung der Kapazität

SMA-Appliance und Implementierung

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

Bei SMA handelt es sich um ein Advanced Access Security Gateway, das einen sicheren Zugriff auf Netzwerk- und Cloud-Ressourcen von sämtlichen Geräten aus ermöglicht. Mit ihrer gehärteten Linux-basierten Appliance bietet die SMA-Lösung einen zentralen, granularen und regelbasierten Sicherheitsmechanismus für den Remote- und Mobilzugriff auf sämtliche Unternehmensressourcen. Verfügbar als gehärtete physische oder leistungsstarke virtuelle Appliance lässt sich SMA nahtlos in jede bestehende IT-Infrastruktur einbinden.



Die SMA-Lösungen sorgen für einen sicheren Zugriff für alle Anwender, Geräte und Anwendungen.

Flexible Implementierung mit physischer und virtueller Appliance

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 und VMware ESX.

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 geschäftskritischen 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.

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

Mit Federated Single-Sign-on ist es nicht mehr notwendig, mehrere Passwörter zu haben. Außerdem werden schlechte Sicherheitspraktiken wie die Wiederverwendung von Passwörtern vermieden. SMA bietet Federated SSO sowohl für in der Clould 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.

Schutz vor Sicherheitslücken und raffinierten 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 Anwenderzugriff 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.

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.

Intuitives Management und umfassendes Reporting

SonicWall bietet eine intuitive webbasierte Verwaltungsplattform, um das Appliance-Management zu optimieren, und stellt umfassende Reporting-Funktionen bereit. 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.

Geringere Investitionskosten dank integriertem Load-Balancer

Die in die SMA-Appliance integrierte Lastverteilungskfunktion 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 Licenses funktionieren wie eine Versicherung für den Fall, dass der Kapazitätsbedarf vorübergehend um mehrere Dutzend oder sogar hunderte zusätzliche Benutzer zunimmt.

VPN-Client	Unterstütztes Betriebssystem	Unterstütztes SMA-Modell	Herausragendes Highlight
Mobile Connect	iOS, OS X, Android, Chrome OS, Windows (8,1 oder höher) und Kindle Fire	Alle Modelle	Biometrische Authentifizierung per App-VPN und Durchsetzung von Endpunktkontrolle
Connect-Tunnel (Thin Client)	Windows, Mac OS und Linux	6200, 7200, 8200v	„In-Office"-Erlebnis mit zuverlässiger Endpunktkontrolle
NetExtender (Thin Client)	Windows und Linux	200, 400, 500v	Durchsetzung granularer Zugriffsregeln und erweiterter Neztwerkzugriff über native Clients

Features

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 Signaturendateien 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 1000 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: MD5, SHA-256, SHA-1 Elliptic Curve Digital Signature Algorithm (ECDSA)
Erweiterte Unterstützung für Chiffrierverfahren	Dank vorkonfigurierter Chiffrierverfahren bieten die SMA 1000-Lösungen 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
Sichere Dateifreigabe[1]	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-basierte Multi-Engine Capture ATP geprüft.
Web Application Firewall	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	Kunden können den Zugriff von bestimmten geografischen Regionen aus erlauben oder einschränken.

Erweiterte Authentifizierung

Cloud-Single-Sign-on[2]	Der SMA SAML IdP Proxy ermöglicht SSO-Zugriff über ein zentrales Portal auf SaaS-Cloud- sowie konventionelle AD-Ressourcen mit Benutzername/Kennwort. Für zusätzliche Sicherheit sorgt die Durchsetzung von Stacked Multifactor Authentication.
Multifaktor-Authentifizierung	Digitale X.509-Zertifikate Server- und Client-seitige digitale Zertifikate RSA SecurID, Dell Defender und weitere Einmalpasswort-/Zwei-Faktor-Authentifizierungstokens mit RADIUS-Protokoll Common Access Card (CAC) Dual oder Stacked Authentication Captcha-Unterstützung, Benutzername/Kennwort
SAML-Gatekeeper-Unterstützung[2]	SMA bietet Air Gap-Sicherheit für Ihren lokal gehosteten SAML-IdP mittels Technologien zum Ändern der Anmeldedaten in der FIPS-zertifizierten Edge Point Appliance.
Authentifizierungsmethoden	SMA bietet eine einfache Integration mit Standardmethoden zur unkomplizierten Verwaltung von Benutzeraccounts und -passwörtern. 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. Dieses Feature 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.

Intuitive Benutzererfahrung

Sichere Netzwerkerkennung	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	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 „Alle weiterleiten" mit SSL/TLS-Tunneling und optionalem ESP-Failback für maximale Performance entscheiden.
HTML5-Datei-Explorer[1]	Mit modernen Dateibrowsern können Benutzer ganz einfach über beliebige Webbrowser auf Dateifreigaben zugreifen.
Mobilbetriebssystem-Integration	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/Active und bietet eine Active/Active-Konfiguration für Hochverfügbarkeit, egal ob in einem einzigen Datencenter oder über mehrere geografisch verteilte Datencenter hinweg implementiert.
Universelle 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 1000-Appliances erlauben eine exponentielle Performance-Skalierung durch die Implementierung mehrerer Appliances. Auf diese Weise werden einzelne Points of Failure 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 (GMS)	CMS bietet eine zentrale, webbasierte Verwaltung für alle SMA-Funktionen.
Personalisierbare 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.
SONAR-Überwachung	SonicWall SONAR erlaubt IT-Administratoren eine schnelle und einfache Diagnose von Zugriffsproblemen und steuert wertvolle Informationen zur Problembehebung bei.
SIEM-Integration	Echtzeit-Ausgabe an zentrale SIEM-Datenkollektoren erlaubt den Sicherheitsteams die Korrelierung ereignisgesteuerter Aktivitäten, um Einblick in den End-to-End-Workflow eines bestimmten Benutzers oder einer bestimmten Anwendung zu erhalten. Das ist für das Security Incident Management und forensische Analysen wichtig.
Scheduler	Der Scheduler erlaubt 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.
MDM-Integration	SMA lässt sich mit führenden Enterprise Mobile Management (EMM)-Produkten wie Airwatch und MobileIron integrieren.
Integration mit weiteren Fremdanbieterprodukten	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	200	400	500v	6200	7200	9000	8200v
Durchsatz	Max. Anzahl gleichzeitiger Sitzungen	50	250	250	2.000	10.000	20.000	5.000
	Max. SSL-/TLS-Durchsatz	100 MBit/s	368 MBit/s	186 MBit/s	400 MBit/s	3,75 GBit/s	3,75 GBit/s	1,58 GBit/s
Client-Zugriff	Layer3-Tunnel	•	•	•	•	•	•	•
	Split-Tunnel und „Alle weiterleiten“	•	•	•	•	•	•	•
	Auto-ESP-Encapsulation	–	–	–	•	•	•	•
	HTML5 (RDP/VNC/ICA/SSH/Telnet)	•	•	•	•	•	•	•
	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)	•	•	•	•	•	•	•
	NetExtender (Windows, Linux)	•	•	•	–	–	–	–
	Connect Tunnel (Windows, Mac OSX und Linux)	–	–	–	•	•	•	•
Mobiler Zugriff	Per-App-VPN	–	–	–	•	•	•	•
	Durchsetzung von Anwendungskontrolle	–	–	–	•	•	•	•
	App-ID-Prüfung	–	–	–	•	•	•	•
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	•	•	•	•	•	•	•
	Capture Malware-Schutz	–	–	–	•	•	•	•
	Endpunkt-Quarantäne	•	•	•	•	•	•	•
	OSCP CRL-Prüfung	–	–	–	•	•	•	•
	Auswahl von Chiffrierverfahren	–	–	–	•	•	•	•
	PKI und Client-Zertifikate	•	•	•	•	•	•	•
	Geo IP-Filter	•	•	•	–	–	–	–
	Botnet-Filter	•	•	•	–	–	–	–
	Forward Proxy	•	•	•	•	•	•	•
	Reverse Proxy	•	•	•	•	•	•	•
Authentifizierung und Identitätsservices	SAML 2.0	–	–	–	•	•	•	•
	LDAP, RADIUS	•	•	•	•	•	•	•
	Kerberos (KDC)	•	•	•	•	•	•	•
	NTLM	•	•	•	•	•	•	•
	SAML IdP-Gatekeeper	–	–	–	•	•	•	•
	Unterstützung für biometrische Geräte	•	•	•	•	•	•	•
	Zwei-Faktor-Authentifizierung (2FA)	•	•	•	•	•	•	•
	Multi-Faktor-Authentifizierung (MFA)	–	–	–	•	•	•	•
	Chained-Authentifizierung	–	–	–	•	•	•	•
	Ausgabe von Einmalpasswörtern	–	–	–	•	•	•	•

Die Funktionen im Überblick (Vergleich nach Modell – fortg.)

Kategorie	Funktion	200	400	500v	6200	7200	9000	8200v
Authentifizierung und Identitätsservices (Fortsetzung)	Common Access Card(CAC)-Unterstützung	–	–	–	•	•	•	•
	Unterstützung für X.509-Zertifikat	•	•	•	•	•	•	•
	Captcha-Integration	–	–	–	•	•	•	•
	Remote-Passwort-Änderungen	•	•	•	•	•	•	•
	Formularbasiertes SSO	•	•	•	•	•	•	•
	Federated SSO	–	–	–	•	•	•	•
	Session Persistence	–	–	–	•	•	•	•
	Automatische Anmeldung	•	•	•	•	•	•	•
Zugriffskontrolle	Gruppen-AD	•	•	•	•	•	•	•
	LDAP-Attribute	•	•	•	•	•	•	•
	Geolocation-Regeln	•	•	•	–	–	–	–
	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-Abrechnung	–	–	–	•	•	•	•
	Aufgabenplanung	–	–	–	•	•	•	•
	Zentralisierte Sessionlizenzierung	–	–	–	•	•	•	•
	Ereignisgesteuertes Auditing	–	–	–	•	•	•	•
Networking	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 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 Infos zu VPN-Clients erhalten Sie unter:*
https://www.sonicwall.com/en-us/products/remote-access/vpn-client

SONICWALL®

Upgrades auf High-End-Appliances bieten viele Vorteile
Höhere Performance | Mehr Durchsatz | Erweiterte Features | 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 200	SMA 400	SMA 6200	SMA 7200	SRA EX9000
Gleichzeitige Sitzungen/User	Bis zu 50	Bis zu 250	Bis zu 2.000	Bis zu 10.000	Bis zu 20.000
SSL-VPN-Durchsatz* (bei max. CCU)	Bis zu 100 MBit/s	Bis zu 368 MBit/s	Bis zu 400 MBit/s	Bis zu 3,75 GBit/s	Bis zu 3,75 GBit/s
Formfaktor	1 HE	1 HE	1 HE	1 HE	2 HE
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	68,6 x 48,2 x 8,8 cm
Gewicht	5 kg	5 kg	7,3 kg	8,3 kg	22,3 kg
Beschleunigung von Verschlüsselungsdaten (AES-NI)	NEIN	NEIN	JA	JA	JA
Spezieller Management-Port	NEIN	NEIN	JA	JA	JA
SSL-Beschleunigung	NEIN	NEIN	JA	JA	JA
Speicher	2 GB (Flashspeicher)	2 GB (Flashspeicher)	2 X 500 GB SATA	2 X 500 GB SATA	2 X 2TB SATA
Schnittstellen	(2) GB Ethernet, (2) USB, (1) Konsole	(4) GB Ethernet, (2) USB, (1) Konsole	6 (6-Port 1 GE)	8 (6-Port 1 GE + 2-Port 10 Gigabit SFP+)	12 (8-Port 1 GE + 4-Port 10 Gigabit SFP+)
Speicher	2 GB	4GB	8 GB DDR3	16 GB DDR3	32 GB DDR3
TPM-Chip	NEIN	NEIN	JA	JA	NEIN
Prozessor	2 Kerne	4 Kerne	4 Kerne	4 Kerne	2 x 4 Kerne
MTBF (bei 25 °C) in Stunden	61.815	60.151	200.064	233.892	129.489
Betrieb und Compliance	**SMA 200**	**SMA 400**	**SMA 6200**	**SMA 7200**	**SRA EX9000**
Stromversorgung	Feste Stromversorgung	Feste Stromversorgung	Feste Stromversorgung	Duale Stromversorgung, hot-swappable	Duale Stromversorgung, hot-swappable
Eingangsnennwerte	100-240 VAC, 50-60 MHz	100-240 VAC, 50-60 MHz	100-240 VAC, 1,1 A	100-240 VAC, 1,79 A	100-240 VAC, 2,85 A
Leistungsaufnahme	26,9 W	31,9 W	78 W	127 W	320 W
Gesamtwärmeabgabe	92 BTU	109 BTU	266 BTU	432 BTU	1091 BTU
Umgebungsbedingungen	WEEE, EU RoHS, China RoHS				
Erschütterung (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 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)	SMA 8200v (ESX/ESXI)	SMA 8200v (Hyper-V)
Gleichzeitige Sitzungen	Bis zu 250 Benutzer	Bis zu 5000	Bis zu 250
SSL-VPN-Durchsatz* (bei max. CCU)	Bis zu 186 MBit/s	Bis zu 1,58 GBit/s	Bis zu 1,2 GBit/s
Zugewiesener Speicher	2 GB	8 GB	
Prozessor	1 Kern	4 Kerne	
WAN-Beschleunigung	NEIN	JA	
Benötigter Festplattenspeicher	2 GB	64 GB (Standard)	Von Administrator konfigurierbar
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
01-SSC-2231	SMA 200 mit 5 User-Lizenz
01-SSC-2243	SMA 400 mit 25 User-Lizenz
01-SSC-8469	SMA 500v mit 5 User-Lizenz
01-SSC-2301	SMA 7200 mit Administrator-Testlizenz
01-SSC-2300	SMA 6200 mit Administrator-Testlizenz
01-SSC-9574	SRA EX9000 Basis-Appliance
01-SSC-8468	SMA 8200v (virtuelle Appliance)
ARTIKELNUMMER	**SONICWALL SMA USER-LIZENZEN**
01-SSC-9182	SMA 500V Zusätzlich 5 User (Auch verfügbar für SMA 200)
01-SSC-2414	SMA 500V Zusätzlich 100 User (Auch verfügbar für SMA 400)
01-SSC-7856	SMA 5 User-Lizenz – kombinierbar mit 6200, 7200, EX9000, 8200v
01-SSC-7860	SMA 100 User-Lizenz – kombinierbar mit 6200, 7200, EX9000, 8200v
01-SSC-7865	SMA 5.000 User Lizenz – kombinierbar mit 7200, EX9000, 8200v
01-SSC-5286	SMA 5 User HA-Lizenz – kombinierbar mit 6200, 7200, EX9000
01-SSC-5290	SMA 100 User HA-Lizenz – kombinierbar mit 6200, 7200, EX9000
01-SSC-5295	SMA 5.000 User-HA-Lizenz – kombinierbar mit 7200, EX9000
ARTIKELNUMMER	**SONICWALL SMA-SUPPORTVERTRAG**
01-SSC-9188	8/5-Support für SMA 500V bis zu 25 User 1 Jahr (Auch verfügbar für SMA 200 und 400)
01-SSC-9191	24/7-Support für SMA 500V bis zu 25 User 1 Jahr (Auch verfügbar für SMA 200 und 400)
01-SSC-8434	24/7-Support für SMA 8200V 5 User 1 Jahr – kombinierbar (Auch verfügbar für SMA 6200, 7200 und EX9000)
01-SSC-8446	24/7-Support für SMA 8200V 100 User 1 Jahr – kombinierbar (Auch verfügbar für SMA 6200, 7200 und EX9000)
01-SSC-7913	24/7-Support für SMA 8200V 5.000 User 1 Jahr – kombinierbar (Auch verfügbar für SMA 6200, 7200 und EX9000)
ARTIKELNUMMER	**ZENTRALE VERWALTUNG FÜR 6200,7200,EX900, 8200V**
Lizenz für CMS Appliance	
01-SSC-8535	Lizenz für CMS-Basis + 3 Appliances (kostenlos)
01-SSC-8536	CMS Lizenz für 100 Appliances 1 Jahr
Zentrale User-Lizenzen (Abo)	
01-SSC-2298	CMS Gepoolte Lizenz 10 User 1 Jahr
01-SSC-8539	CMS Gepoolte Lizenz 1000 User 1 Jahr
01-SSC-5339	CMS Gepoolte Lizenz 50.000 User 1 Jahr
Zentrale User-Lizenzen (unbefristet)	
01-SSC-2053	CMS Unbefristete Lizenz 10 User
01-SSC-2058	CMS Unbefristete Lizenz 1.000 User
01-SSC-2063	CMS Unbefristete Lizenz 50.000 User
Support für zentrale User-Lizenzen (unbefristet)	
01-SSC-2065	CMS 24/7-Support 1 Jahr 10 User
01-SSC-2070	CMS 24/7-Support 1 Jahr 1.000 User
01-SSC-2075	CMS 24/7-Support 1 Jahr 50.000 User
Zentrale ActiveSync-Lizenzen (Abo)	
01-SSC-2088	CMS Gepoolte E-Mail-Lizenz 10 User 1 Jahr
01-SSC-2093	CMS Gepoolte E-Mail-Lizenz 1.000 User 1 Jahr
01-SSC-2087	CMS Gepoolte E-Mail-Lizenz 50.000 User 1 Jahr

Bestellinformationen (Fortsetzung)

Zentrale Spike-Lizenzen	
01-SSC-2111	CMS Spike 1.000 User 5 Tage
01-SSC-2115	CMS Spike 50.000 User 5 Tage
Capture-Add-on (Abo)	
01-SSC-2116	CMS Capture-Testversion 1 Jahr für SMA
** Abolizenzen mit 24/7-Support inklusive*	
ARTIKELNUMMER	**SONICWALL SMA ADD-ONS**
01-SSC-2406	SMA 7200 FIPS Add-on
01-SSC-2405	SMA 6200 FIPS Add-on
01-SSC-9185	SMA 500V Web Application Firewall 1 Jahr (Auch verfügbar für SMA 200 und 400)
ARTIKELNUMMER	**SONICWALL SMA ADD-ONS**
01-SSC-5967	Virtual Assist bis zu 1 gleichzeitiger Techniker (SMA 200, 400, 500v)
01-SSC-5971	Virtual Assist bis zu 10 gleichzeitige Techniker (SMA 200, 400, 500v)
ARTIKELNUMMER	**SPIKE LICENSE FÜR SMA (ABSTUFUNG ERFORDERLICH, UM KAPAZITÄT ZU ERREICHEN)**
01-SSC-2240	SMA 200 10 Tage 50 User Spike-Lizenz (Auch verfügbar für SMA 400 und 500v)
01-SSC-7873	SMA 8200v 10 Tage 5-2.500 User Spike-Lizenz (Auch verfügbar für SMA 6200, 7200 und EX9000)

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

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara,
Kalifornien 95054, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-SecureMobileAccess-US-VG-MKTG482