

PRODUKTE

Intelligente High-Performance-Lösungen für kosteneffiziente Netzwerksicherheit

SONICWALL[®]

PROTECTION AT THE SPEED OF BUSINESS[®]

Überblick	2
Network Security-Lösungen	
Überblick über Netzwerksicherheitslösungen.....	3
E-Class-Lösungen	4
Lösungen für KMUs und Niederlassungen	5
Wireless-Geräte.....	11
Abo-services, Lizenzen und Firmware.....	12
Secure Remote Access-Lösungen	
Überblick über Secure Remote Access-Lösungen	13
E-Class-Lösungen	13
Add-On-Features	14
SSL VPN-Lösungen für KMUs und Niederlassungen	15
Add-On-Features	16
Anti-Spam/Email- und Web Security-Lösungen	
Überblick über E-Mail-Sicherheitslösungen	17
E-Class-Lösungen	17
KMU-Lösungen	18
Abo-services	18
Web-Lösungen	19
Backup- und Recovery-Lösungen	
Überblick über Backup- und Recovery-Lösungen	20
KMU-Lösungen	20
Abo-services.....	21
Policy- und Management-Lösungen	
Global Management System.....	22
SonicWALL ViewPoint	22
MySonicWALL.....	22
Global Support Services	
Dynamic 8/5- und 24/7-Support.....	23
Comprehensive Global Management System	23

Deep Protection SonicWALL® arbeitet ständig daran, die Kosten und die Komplexität von sicheren High-Performance-Netzwerken zu senken und hilft Unternehmen so, ihre Ressourcen produktiver einzusetzen. Als anerkannter Innovationsführer entwickelt SonicWALL intelligente Lösungen, die dynamischen High-Performance-Schutz gewährleisten und gleichzeitig die Anschaffungs-, Implementierungs- und Verwaltungskosten senken. Die hochskalierbaren appliancebasierten Lösungen und Abo-Services von SonicWALL sind leicht zu handhaben und zu verwalten und unterstützen Unternehmen dabei, ihre Produktivität und Performance zu steigern – egal ob es sich dabei um staatliche Einrichtungen, Einzelhandelsfirmen, Organisationen im Gesundheitswesen oder Service Provider handelt. SonicWALL schützt Netzwerke – und Unternehmen – mit einem umfassenden Portfolio an skalierbaren und interoperablen Lösungen, die ein effizientes Threat Management, sichere Mobilität, Business Continuity und die Einhaltung von gesetzlichen Vorschriften gewährleisten.

Threat Management Internetbedrohungen sind heute mehr als nur ein lästiges Ärgernis. Ihre zunehmende Komplexität macht sie zu einer ernstzunehmenden Gefahr, die einen enormen wirtschaftlichen Schaden anrichten kann. SonicWALL sorgt für eine nahtlose Integration von Netzwerk- sowie Web- und E-Mail-Sicherheitslösungen und bietet umfassenden Schutz vor den immer raffinierteren dynamischen Bedrohungen. Mit SonicWALL Network Security sind Unternehmen umfassend vor Viren, Würmern, Trojanern, Spyware und Eindringlingen geschützt und profitieren gleichzeitig von einer exzellenten Netzwerkperformance auch unter Lastbedingungen. SonicWALL Web Security bietet bessere Kontrollmöglichkeiten, um den Zugriff auf anstößige, illegale oder gefährliche Webinhalte zu verhindern und den Zugriff auf Instant Messaging- und Peer-to-Peer-Anwendungen zu überwachen. Die Email Security-Lösungen runden das Angebot von SonicWALL ab und schützen effizient vor Spam und Phishing-Angriffen, so dass Mitarbeiter nur reguläre E-Mails erhalten und nicht mit fingierten Mails überschwemmt werden. Mit den All-in-One-Sicherheitslösungen von SonicWALL lassen sich lokale, remote verfügbare und mobile Netzwerkdienste erheblich einfacher verwalten. Zudem können wichtige Daten und Kommunikationsressourcen günstig geschützt werden.

Mobility Mit der zunehmenden Verbreitung von Mobiltechnologien, der wachsenden Zahl mobiler Mitarbeiter und der steigenden Nachfrage nach Business Continuity-Lösungen gewinnt das Thema Mobilität für Unternehmen immer mehr an Bedeutung. SonicWALL bietet intelligente Mobilitätslösungen mit Breitband-, Wireless- oder DFÜ-Konnektivität für Organisationen jeder Größenordnung. Die Netzwerksicherheitslösungen von SonicWALL mit integriertem SonicWALL Unified Threat Management-Schutz gewährleisten dank IPSec VPN sichere Site-to-Site-Verbindungen. In Kombination mit den sich selbst konfigurierenden SonicPoints gewährleisten diese Appliances eine sichere Wireless-Hotspot-Konnektivität in temporär genutzten Netzwerken. Mit der SonicWALL TZ 190 lassen sich für temporäre Standorte so gut wie überall und innerhalb kürzester Zeit sichere 3G Wireless-Breitbandnetze einrichten, ohne dass ein Festnetzanschluss erforderlich ist. Darüber hinaus ist mit den SonicWALL SSL VPNs ein sicherer Zugriff über Standard-Webbrowser oder mobile Geräte wie z. B. drahtlose PDAs und Smartphones an fast allen Remote-Standorten möglich. Zudem bieten die SonicWALL SSL VPNs unübertroffene Kontrollmöglichkeiten.

Business Continuity Größere Katastrophen, Stromausfälle oder andere unerwartete Ereignisse, die den normalen Geschäftsbetrieb stören, können dazu führen, dass Unternehmen wichtige Geschäftschancen verpassen, Umsätze verlieren oder dass ihr Ruf beschädigt wird. SonicWALL bietet Business Continuity- und Recovery-Lösungen für große und kleine Unternehmen. Mit den SonicWALL SSL VPN-Lösungen können Mitarbeiter in Ausnahmesituationen von zuhause oder von temporären Ausweichstandorten aus genauso produktiv arbeiten wie in ihrem Büro. Die komfortablen und diskbasierten SonicWALL Backup- und Recovery-Lösungen bieten automatische Echtzeit-Backups für Server, Laptops und PCs. Mit den Appliances der Continuous Data Protection (CDP)-Serie werden die Daten sowohl lokal als auch offsite gesichert, damit Dateien von jedem beliebigen Zeitpunkt sofort wiederhergestellt werden können.

Compliance Sicherheitsbedrohungen gibt es nicht nur außerhalb, sondern auch innerhalb eines Firmennetzwerks. Zum Beispiel kann es vorkommen, dass Mitarbeiter – absichtlich oder versehentlich – ungeeignete Inhalte, geschütztes geistiges Eigentum oder vertrauliche Daten übermitteln. Dies kann Unternehmen enorm schaden bzw. Branchenstandards und gesetzliche Vorgaben verletzen. Werden solche Vorgaben nicht eingehalten, müssen Unternehmen mit Geldbußen, Haftungsproblemen oder einem Verlust ihrer Glaubwürdigkeit rechnen. Mit seiner führenden Verschlüsselungstechnologie und der Deep Packet Inspection-Funktion, die eine „Clean VPN“-Konnektivität sicherstellt, kann SonicWALL Organisationen dabei unterstützen, wichtige Vorschriften einzuhalten. Die SonicWALL SSL VPN-Lösungen bieten Datenverschlüsselung und -authentifizierung, granulare Zugangskontrollen, Regelverwaltung, Logging-Funktionen und eine flexible Authentifizierungsarchitektur. Mit SonicWALL Email Security lassen sich Regeln für den ausgehenden Datenverkehr einfach erstellen und nicht regelkonforme E-Mails auf intelligente Weise erkennen. Außerdem gibt es zuverlässige Überwachungs- und Reporting-Tools sowie zahlreiche Optionen zur Problembehebung. Die SonicWALL Content Security Appliances schützen Ihr Netzwerk vor illegalen oder nicht arbeitsrelevanten Webinhalten. Das mehrfach ausgezeichnete Global Management System (GMS) bietet Audit-Trails mit zentraler Echtzeit-Überwachung sowie ein umfassendes Regel- und Compliance-Reporting.

**Die SonicWALL E-Class
Network Security
Appliances (NSA) für
große Unternehmen
arbeiten mit einem
Multi-Core-
Mikroprozessor, der
leistungsstarke Deep
Packet Inspection
bietet, ohne den
Netzwerkdurchsatz
zu beeinträchtigen.**

SonicWALL Network Security

Die Sicherheitslösungen anderer Anbieter sind nicht selten überteuert, technisch unzulänglich oder umständlich in der Implementierung und Handhabung. Mit den Netzwerksicherheitslösungen von SonicWALL gehören diese Probleme der Vergangenheit an: SonicWALL steht für Lösungen, die einen sicheren Betrieb von High-Performance-Infrastrukturen ermöglichen und dabei die Kosten senken und die Komplexität reduzieren. Das schafft Freiräume im Unternehmen und ermöglicht produktiveres Arbeiten. In den SonicWALL Network Security-Lösungen kommen mehrere Sicherheitstechnologien in einer einzigen Plattform zum Einsatz, die nicht nur extrem schnellen Schutz und zuverlässige Kommunikation, sondern auch niedrige TCO und flexible Verbindungsoptionen gewährleisten.

SonicWALL *E*CLASS

SonicWALL Enterprise-Lösungen: Die E-Class NSA-Serie im Überblick

Mit der Network Security Appliance (NSA)-Serie präsentiert SonicWALL® eine Branchenneuheit: Durch die Kombination einer Reassembly-Free Deep Packet Inspection-Engine mit einem Multi-Core-Mikroprozessor bieten die Appliances extrem leistungsfähige Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention, ohne dass die Netzwerk-Performance beeinträchtigt wird. Der Einsatz einer leistungsstarken Deep Packet Inspection Firewall mit mehrstufigen Schutzmechanismen und zahlreichen Hochverfügbarkeitsfunktionen macht die NSA-Serie zur idealen Lösung für die verschiedensten Infrastrukturen wie etwa verteilte Netzwerke, Campus-Netzwerke und Rechenzentren.

Als hochskalierbare, leistungsstarke und zuverlässige multifunktionale Lösung entwickelt, sind die E-Class NSA-Appliances den anderen Lösungen ihrer Klasse weit überlegen. Dem Administrator erschließen sich mit der Funktion Application Firewall völlig neue Dimensionen in puncto Schutz und Steuerung: Eine Reihe individuell anpassbarer Sicherheitstools ermöglicht eine detaillierte Kontrolle und Überwachung des Netzwerkverkehrs. Für Enterprise-Netzwerke ist es wichtig, dass ein zuverlässiger Betrieb gewährleistet ist. Um Ausfallzeiten auf ein Minimum zu reduzieren und den Netzwerkschutz zu verbessern, ist die E-Class NSA-Serie mit verschiedenen Hochverfügbarkeitsfunktionen auf Hardware- und Systemebene ausgestattet. Die E-Class NSA-Serie erleichtert die Verwaltung mit einer großen Auswahl ausgereifter Konfigurationsoptionen, die eine einfache Integration und flexible Einsatzmöglichkeiten bieten. Daher ist die NSA-Serie ideal für Organisationen geeignet, die sichere High-Performance-Netzwerke für die unterschiedlichsten Umgebungen benötigen. Die E-Class NSA-Serie bietet:

- Enterprise-Class Deep Packet Inspection (DPI) und Application Firewall für jedes Datenpaket, jedes Protokoll und jede Schnittstelle
- Bahnbrechende Multi-Core-Performance mit bis zu 16 Prozessorkernen für extrem schnellen, mehrschichtigen Schutz in externen und internen Netzwerken
- Höchste Skalierbarkeit bei der Neutralisierung von Sicherheitsbedrohungen mit unbegrenzter Dateigröße und unbegrenzter Anzahl gleichzeitiger Downloads dank einer Reassembly-Free Deep Packet Inspection Engine
- Dynamisch aktualisierbare und personalisierbare Sicherheitsabwehr-Mechanismen
- Robuster Schutz dank leistungsfähiger Business Continuity- und Hochverfügbarkeitsfunktionen



SonicWALL ECLASS

Network Security-Lösungen – SonicWALL E-Class NSA-Serie

SonicWALL NSA E7500

Die SonicWALL E-Class Network Security Appliance (NSA) E7500 ist das Flaggschiff der E-Class NSA-Serie. Als hochskalierbare, leistungsstarke und zuverlässige Threat Appliance konzipiert, bietet die NSA E7500 weit mehr als vergleichbare Lösungen ihrer Klasse. Sie schützt Unternehmensnetze nicht nur umfassend vor einer Vielzahl von Bedrohungen, sondern bietet gleichzeitig eine außergewöhnlich hohe Geschwindigkeit und Zuverlässigkeit. Möglich wird dies durch eine 16-Core-Architektur, bei der die Prozessorkerne parallel arbeiten und so ultraschnellen Schutz und größtmögliche Skalierbarkeit gewährleisten. Dem Administrator erschließen sich mit der Funktion Application Firewall völlig neue Dimensionen in puncto Schutz und Steuerung: Eine Reihe individuell anpassbarer Sicherheitstools ermöglicht eine detaillierte Kontrolle und Überwachung des Netzwerkverkehrs. Die NSA E7500 verfügt standardmäßig über vier Gigabit Kupfer-Ethernet-Ports, vier erweiterbare SFP-Ports für unterschiedliche Implementierungsoptionen und einen LCD-Bildschirm, der einen sofortigen Zugriff auf die Systemkonfiguration ermöglicht. Verschiedene Hochverfügbarkeitsfunktionen auf der Hardware-Ebene, zwei Stromversorgungen und Lüfter sowie Stateful Failover auf System-Ebene sorgen für einen zuverlässigen Betrieb und reduzieren Ausfallzeiten auf ein Minimum. Darüber hinaus bietet die NSA E7500 Unternehmenskunden eine große Auswahl an ausgereiften und flexiblen Implementierungsoptionen für den Einsatz in großen Enterprise-Netzwerken.



SonicWALL NSA E6500

Als leistungsstarke, skalierbare und multifunktionale Threat Prevention Appliance eignet sich die SonicWALL E-Class Network Security Appliance (NSA) E6500 für wachsende Unternehmensnetze. Die Appliance nutzt dabei eine Multi-Core-Technologie mit spezialisierten Prozessorkernen, die in Verbindung mit der Reassembly-Free Deep Packet Inspection Engine von SonicWALL eine parallele Verarbeitung des Netzwerkverkehrs erlaubt. Mit der NSA E6500 verfügen IT-Administratoren über eine High-Performance-Sicherheitsplattform, um dynamische Bedrohungen effizient auszuschalten. Die Application Firewall ermöglicht es Netzwerkadministratoren mithilfe einer Reihe individuell anpassbarer Sicherheitstools den Netzwerkverkehr gezielt zu kontrollieren und zu überwachen. Die NSA E6500 verfügt standardmäßig über acht Gigabit Kupfer Ethernet-Ports für flexible Einsatzmöglichkeiten und über einen LCD-Bildschirm, der die Implementierung vereinfacht.



SonicWALL NSA E5500

Die SonicWALL E-Class Network Security Appliance (NSA) E5500 ist eine leistungsstarke Multi Service-Sicherheitsplattform, die als robustes Arbeitsgerät für Enterprise-Netzwerkumgebungen konzipiert wurde. Neben der Reassembly-Free Deep Packet Inspection Engine von SonicWALL bietet die NSA E5500 eine 8-Core-Prozessortechnologie zur parallelen Verarbeitung des Netzwerkverkehrs und ermöglicht so eine außergewöhnlich leistungsfähige Deep Packet Inspection für Unternehmensnetze. Die NSA E5500 kommt standardmäßig mit acht Gigabit Kupfer-Ethernet-Ports für flexible Einsatzmöglichkeiten und verfügt über einen LCD-Bildschirm, der die Implementierung vereinfacht. Die Lösung enthält umfangreiche Funktionen für eine unkomplizierte Verwaltung von Enterprise-Netzwerkumgebungen und bietet ein unschlagbares Preis-Leistungs-Verhältnis.



SonicWALL-Lösungen für KMUs und Niederlassungen: Die NSA-Serie im Überblick
SonicWALL Network Security Appliance 5000

Die SonicWALL Network Security Appliance (NSA) 5000 ist die Top-Appliance der NSA-Serie und wurde als Unified Threat Management (UTM)-Firewall für anspruchsvolle Campus-Netzwerke und verteilte Netzwerkumgebungen entwickelt. Dank ihrer bahnbrechenden 8-Core-Hardware-Plattform bietet die NSA 5000 Echtzeit-Schutz vor internen und externen Netzwerkbedrohungen, ohne die Netzwerkperformance zu beeinträchtigen. Die NSA 5000 verfügt über High-Speed-Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten, leistungsstarke Application Firewall-Kontrollmöglichkeiten sowie zahlreiche erweiterte und flexible Netzwerk-, Hochverfügbarkeits- und Konfigurationsfeatures für anspruchsvolle Netzwerkumgebungen. Ausgestattet mit 6 konfigurierbaren Gigabit Ethernet (GE)-Ports sowie der SonicWALL Clean VPN™-Technologie und integrierten Secure WLAN-Funktionen, bildet die NSA 5000 die ideale Lösung für verschiedenste Anwendungsszenarien in kabelgebundenen oder drahtlosen Umgebungen, die einen High-Speed-Zugang und eine starke Segmentierung von Arbeitsgruppen erfordern. Außerdem unterstützt die NSA 5000 Virtual Local Area Networks (VLANs), Enterprise-Class-Routing- und QoS-Features und optimiert damit die Sicherheit und Performance im gesamten Netzwerk.



SonicWALL Network Security Appliance 4500

Die SonicWALL Network Security Appliance (NSA) 4500 wurde als Unified Threat Management (UTM)-Firewall der nächsten Generation für Firmenzentralen und größere verteilte Netzwerkumgebungen entwickelt. Mit ihrer bahnbrechenden 8-Core-Hardwareplattform bietet die Appliance Echtzeit-Schutz vor internen und externen Bedrohungen, ohne die Performance zu beeinträchtigen. Die NSA 4500 kombiniert High-Speed-Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten und leistungsstarke Application Firewall-Kontrollmöglichkeiten mit zahlreichen erweiterten und flexiblen Netzwerk-, Hochverfügbarkeits- und Konfigurationsfeatures. Ausgestattet mit 6 konfigurierbaren Gigabit Ethernet (GE)-Ports sowie der SonicWALL Clean VPN™-Technologie ist die NSA 4500 die ideale Lösung, um zuverlässigen Schutz am Netzwerkrand sowie eine sichere Remote-Konnektivität zu gewährleisten. Außerdem unterstützt die NSA 4500 Virtual Local Area Networks (VLANs), Enterprise-Class-Routing- und QoS-Features und optimiert damit die Sicherheit und Performance im gesamten Netzwerk.



SonicWALL Network Security Appliance 3500

Die SonicWALL Network Security Appliance (NSA) 3500 wurde als Unified Threat Management-Firewall der nächsten Generation für die Netzwerkumgebungen von Unternehmen, Zweigniederlassungen und verteilten Organisationen entwickelt. Dank dem bahnbrechenden Multi-Core-Hardware-Design mit 4 Prozessorkernen und 6 Gigabit Ethernet (GE)-Ports sorgt die NSA 3500 für Echtzeit-Schutz vor internen und externen Netzwerkbedrohungen, ohne die Performance zu beeinträchtigen. Die NSA 3500 vereint High-Speed-Intrusion Prevention, Funktionen zur Prüfung von Dateien und Dateiinhalten sowie leistungsstarke Application Firewall-Kontrollmöglichkeiten mit zahlreichen erweiterten Netzwerk- und Konfigurationsfeatures in einer komfortablen und erschwinglichen Plattform, die sich in den unterschiedlichsten Netzwerkumgebungen leicht implementieren und verwalten lässt. Die intuitive webbasierte Verwaltungsoberfläche und die anwenderfreundlichen Konfigurationsassistenten erleichtern die Installation und Konfiguration der NSA 3500. Außerdem unterstützt die NSA 3500 Virtual Local Area Networks (VLANs), Enterprise-Class-Routing- und QoS-Features und optimiert damit die Sicherheit und Performance im gesamten Netzwerk.

**Umfassender
Unified Threat
Management-Schutz
in Echtzeit
für KMUs und
Niederlassungen**



Lösungen für KMUs und Niederlassungen: Die SonicWALL PRO-Serie im Überblick

Als Multi Service-Sicherheitsplattform ist die SonicWALL PRO-Serie für Unternehmen gedacht, die einen robusten Netzwerkschutz und einen schnellen, sicheren VPN-Zugang für Mitarbeiter im Home Office benötigen. Dank der innovativen Deep Packet Inspection-Architektur von SonicWALL bietet die PRO-Serie nicht nur Gateway Anti-Virus-, Anti-Spyware-, Intrusion Prevention-, Anti-Spam-, Content Filtering- und sichere Wireless-Funktionen, sondern sorgt mit IPSec VPN und einer Deep Packet Inspection Firewall für gezielten Echtzeit-Schutz gegen böswillige Angriffe über die Anwendungsebene. Mit der PRO-Serie stehen sechs Security Appliances zur Verfügung, um unterschiedlichste Anforderungen rasch wachsender Netzwerke in puncto Skalierbarkeit und Performance zu erfüllen.

In Form von kostengünstigen rackfähigen Appliances bietet die PRO-Serie alle Vorzüge des SonicOS-Betriebssystems von SonicWALL, wie z. B. Enterprise Class-Performance, erweiterte Funktionen sowie flexible Konfigurationsoptionen. SonicWALL SonicOS Enhanced gehört bei der PRO 4060, PRO 4100 und PRO 5060 zum Lieferumfang und bietet als optionales Upgrade für die PRO 1260, PRO 2040 und PRO 3060 zahlreiche Funktionen, wie z. B. Verwaltungs-, Redundanz- und WLAN-Features, die bis vor kurzem nur in hochpreisigen Appliances erhältlich waren. Zu den vielen erweiterten Funktionen von SonicOS Enhanced gehören unter anderem QoS (Quality of Service), ISP Failover, WAN-Redundanz, Lastverteilung, objekt- und zonenbasiertes Management, regelbasierte NAT und Wireless Guest Services.

Die ICSA-zertifizierten Geräte der PRO-Serie lassen sich per Web-Oberfläche oder mithilfe des innovativen Global Management Systems (GMS) von SonicWALL innerhalb einer IT-Umgebung mit mehreren Firewalls und VPN-Verbindungen einfach fernwarten.

SonicWALL PRO 5060

Die PRO 5060 ist das Flaggschiff der SonicWALL PRO-Serie. Als Multi-Service-, Enterprise Class-Sicherheitsplattform für Gigabit-Netzwerke schützt die PRO 5060 Benutzer und geschäftskritische Netzwerk-Ressourcen wirkungsvoll vor den immer komplexeren Internet-Bedrohungen. In den beiden erhältlichen Ausführungen mit 10/100/1000 Kupfer- bzw. Kupfer/Glasfaser-Schnittstellen bietet die PRO 5060 erweiterte Netzwerk- und Sicherheitsfunktionen, wie z. B. VLAN nach 802.1q, QoS (Quality of Service) sowie dynamisches RIP- und OSPF-Routing, und ist damit die ideale Lösung für datenintensive Netzwerkkumgebungen. Zum Lieferumfang der PRO 5060 gehören die ViewPoint® Reporting-Software, eine 1-Jahres lizenz für Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention Service sowie 2.000 Global VPN Client-Lizenzen für einen sicheren Remote-Zugang.

SonicWALL PRO 4100

Als leistungsfähige Unified Threat Management-Plattform bietet die PRO 4100 wirksamen Echtzeitschutz vor internen und externen Sicherheitsbedrohungen in Unternehmensnetzen, verteilten Netzwerken oder Rechenzentren. Die benutzerfreundliche und kostengünstige Appliance kombiniert leistungsstarke Deep Packet Inspection-Technologien mit schnellen Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention Services sowie zahlreichen flexiblen Netzwerk- und Konfigurationsfunktionen in einer einzigen komfortablen Plattform. Ausgestattet mit zehn konfigurierbaren Gigabit Ethernet-Ports sowie der SonicWALL Clean VPN-Technologie und integrierten Secure WLAN-Funktionen bildet die PRO 4100 die ideale Lösung für verschiedenste Anwendungsszenarien in kabelgebundenen oder drahtlosen Umgebungen, die einen High-Speed-Zugang und eine starke Segmentierung von Arbeitsgruppen erfordern. Zum Lieferumfang der PRO 4100 gehören die SonicWALL ViewPoint Reporting-Software sowie 1.000 Global VPN Client-Lizenzen für einen sicheren Remote-Zugang.

SonicWALL PRO 4060

Die PRO 4060 von SonicWALL wurde als leistungsfähige Multi-Service-Sicherheitsplattform entwickelt und sorgt in kleinen bis mittelgroßen Netzwerken für unterbrechungsfreie Geschäftsabläufe. Hardwarebeschleunigte VPN-Performance mit 190 MBit/s, erweiterte VPN-Funktionen und 1.000 Global VPN Client-Lizenzen machen die PRO 4060 zur idealen Lösung selbst für komplexe Remote-Umgebungen. Für Flexibilität beim Netzwerkaufbau sorgen sechs konfigurierbare 10/100 Ethernet-Ports, mit denen sich mehrere LANs, WANs, WLANs, DMZs sowie speziell definierte Zonen einrichten lassen. Zum Lieferumfang der PRO 4060 gehören die ViewPoint Reporting-Software sowie 1.000 Global VPN Client-Lizenzen für einen sicheren Remote-Zugang.

SonicWALL PRO 3060

Die PRO 3060 von SonicWALL wurde als leistungsfähige Sicherheitsplattform entwickelt und sorgt in kleinen bis mittelgroßen Netzwerken für unterbrechungsfreie Geschäftsabläufe. Ausgestattet mit dem zukunftsweisenden Betriebssystem SonicOS von SonicWALL stellt die PRO 3060 leistungsstarke Firewall-Performance und 3DES/AES VPN-Konzentration zur Verfügung. Das optionale Upgrade auf SonicOS Enhanced erweitert die Funktionspalette der PRO 3060 um wichtige Redundanz-Funktionen, wie beispielsweise Hardware Failover, WAN ISP Failover sowie Failover-Möglichkeiten auf ein zweites VPN-Gateway, und garantiert so maximale Netzverfügbarkeit. Für Flexibilität beim Netzwerkaufbau sorgen sechs konfigurierbare 10/100 Ethernet-Ports, mit denen sich mehrere LANs, WANs, WLANs, DMZs sowie speziell definierte Zonen einrichten lassen.



SonicWALL PRO 2040

Die ausgezeichnete SonicWALL PRO 2040 wurde als Sicherheitsplattform entwickelt und sorgt in kleinen bis mittelgroßen Netzwerken für unterbrechungsfreie Geschäftsabläufe. Die PRO 2040 stellt leistungsstarke Firewall-Performance und 3DES/AES VPN-Konzentration zur Verfügung, speziell für Netzwerke mit bis zu 200 Nodes bzw. 50 Einzelstandorten. Das optionale Upgrade auf SonicOS Enhanced erweitert die Funktionspalette der PRO 2040 um Hardware Failover, WAN ISP Failover sowie Failover-Möglichkeiten auf ein zweites VPN-Gateway und garantiert so maximale Netzverfügbarkeit. Für Flexibilität beim Netzwerkaufbau sorgen vier konfigurierbare 10/100 Ethernet-Ports, mit denen sich mehrere LANs, WANs, WLANs, DMZs sowie speziell definierte Zonen einrichten lassen.

SonicWALL PRO 1260

Als umfassende Sicherheitsplattform mit LAN Switching-Option für kleine Netzwerkanwendungen bietet die PRO 1260 nicht nur eine Deep Packet Inspection Firewall und leistungsfähige IPSec VPN-Funktionen, sondern auch einen intelligenten Autosensing-MDIX-Switch mit 24 Ports und Wire Speed-Durchsatz. Die PRO 1260 kombiniert Netzwerksicherheit mit LAN Switching in einem einzigen Gerät und kann entweder mit der standardmäßigen Switch-Funktion unter SonicOS Standard oder als administrierbare LAN Switching-Plattform mit der leistungsstarken SonicWALL PortShield-Architektur unter SonicOS Enhanced eingerichtet werden. Dank der innovativen PortShield-Architektur kann jeder der 24 Ports individuell als spezielle Sicherheitszone (PortShield-Gruppe) konfiguriert werden, wobei jeder Zone eine eigene „virtuelle Firewall“ zugewiesen wird. Für jede Schnittstelle kann darüber hinaus der maximale Durchsatz stufenweise festgelegt werden.

Funktion	PRO 1260	PRO 2040	PRO 3060	PRO 4060	PRO 4100	PRO 5060
Nodes			Unlimitiert			
Schnittstellen	27 Ethernet	3/4* Ethernet	3/6* Ethernet	6 Ethernet	10 Gigabit	6 Gigabit
SonicOS Standard/Enhanced	Standard	Standard	Standard	Enhanced	Enhanced	Enhanced
Upgrade auf SonicOS Enhanced	Ja	Ja	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Stateful-Durchsatz ¹	90 MBit/s	200 MBit/s	300 MBit/s	Mehr als 300 MBit/s	800 MBit/s	2,4 GBit/s
Gateway Anti-Virus-Durchsatz ²	8 MBit/s	40 MBit/s	99 MBit/s	182 MBit/s	300 MBit/s	339 MBit/s
Intrusion Prevention-Durchsatz ²	8 MBit/s	39 MBit/s	98 MBit/s	170 MBit/s	300 MBit/s	279 MBit/s
Verbindungen	6.140	32.000	128.000	500.000	600.000	750.000
Regeln	150/300*	150/1.000*	300/3.000*	5.000	10.000	15.000
3DES/AES-Durchsatz ³	Mehr als 30 MBit/s	50 MBit/s	75 MBit/s	190 MBit/s	350 MBit/s	700 MBit/s
Site-to-Site-VPN-Tunnel	25	50	500/1.000*	3.000	3.500	4.000
Remote Access-VPN-Tunnel (max.)	50	100	500	3.000	4.500	6.000
Remote Access-VPN-Tunnel (inklusive)	5	10	25	1.000	1.500	2.000
Zonenspezifische Sicherheitsfunktionen	Ja*	Ja*	Ja*	Ja	Ja	Ja
Objektbasiertes Management	Ja*	Ja*	Ja*	Ja	Ja	Ja
Regelbasierte NAT	Ja*	Ja*	Ja*	Ja	Ja	Ja
WAN/WAN Failover	Ja*	Ja*	Ja*	Ja	Ja	Ja
Lastverteilung	Ja*	Ja*	Ja*	Ja	Ja	Ja
Hardware Failover	Nein	Ja*	Ja*	Ja	Ja	Ja
Stateful Hardware Failover	Nein	Nein	Ja**	Ja**	Ja**	Ja**
Integrierter Wireless Switch und Controller	Ja*	Ja*	Ja*	Ja	Ja	Ja
Spamschutz	Ja*	Ja*	Ja*	Ja	Ja	Ja
Voice over IP (VoIP)	Ja	Ja	Ja	Ja	Ja	Ja
IKEv2 VPN	Ja*	Ja*	Ja*	Ja	Ja	Ja
Secure Remote Management (SSHv2-Unterstützung)	Ja*	Ja*	Ja*	Ja	Ja	Ja
Multi-SSIDs mit VAP	Nein	Ja**	Ja**	Ja**	Ja**	Ja**
Dynamische Adressobjekte	Ja**	Ja**	Ja**	Ja**	Ja**	Ja**
Layer 2 Bridge-Modus	Nein	Ja**	Ja**	Ja**	Ja**	Ja**
VLAN nach 802.1q	Nein ⁴	Ja*	Ja*	Ja	Ja	Ja
RIPv2- und OSPF-Routing	Ja*	Ja*	Ja*	Ja	Ja	Ja
Single Sign On (SSO)	Ja**	Ja**	Ja**	Ja**	Ja**	Ja**
Application Firewall	Nein	Nein	Ja**	Ja**	Ja**	Ja**
SSL Control	Ja**	Ja**	Ja**	Ja**	Ja**	Ja**

*Bei Upgrade auf SonicOS Enhanced

**4.0.0.0 Enhanced erforderlich

¹Messung des Firewall-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1518 Bytes pro Paket

²Messung des Gateway AV/Anti-Spyware/IPS-Durchsatzes mit HTTP-Verkehr

³Messung des VPN-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1280 Bytes pro Paket

⁴Die PRO 1260 unterstützt die PortShield-Technologie

**Die TZ-Serie
ist die ideale
All-in-One-
Sicherheitsplattform
für kleine
Netzwerke mit
Außenstellen,
Zweigniederlassungen
und Verkaufsfilialen.**



Lösungen für KMUs und Niederlassungen: Die SonicWALL TZ-Serie im Überblick

Als umfassende Sicherheitslösung für Mitarbeiter im Home Office, kleine Betriebe, Außenstellen und Niederlassungen kombiniert die SonicWALL TZ-Serie anwenderfreundliche Bedienung für kleinere Netzwerke mit einem hohen Maß an Flexibilität für komplexere Infrastrukturen. Die hochskalierbare Plattform gewährleistet einen hohen Investitionsschutz und integriert in einer einzigen, kostengünstigen Lösung eine Vielzahl leistungsfähiger Features wie Deep Packet Inspection Firewall, sichere Wireless-Anbindung nach 802.11b/g, Failover/Failback, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Content Filtering und IPSec VPN-Funktionen. Die unterschiedlichen Modelle der TZ-Serie bieten eine große Auswahl an Hardware- und Node-Konfigurationen und lassen sich flexibel um zusätzliche Funktionen erweitern, sobald diese im Netzwerk benötigt werden.

In Form von kostengünstigen Desktop Appliances bietet die TZ-Serie alle Vorzüge des SonicOS-Betriebssystems von SonicWALL, wie z. B. Business Class-Performance, erweiterte Funktionen sowie flexible Konfigurationsoptionen. SonicOS Enhanced von SonicWALL gehört bei der TZ 190-Serie und der TZ 170 SP Wireless zum Lieferumfang und bietet als optionales Upgrade für die übrigen Appliances der TZ 170 SP- und TZ 180-Serie zahlreiche Funktionen, wie z. B. Verwaltungs-, Redundanz- und WLAN-Features, die bis vor kurzem nur in hochpreisigen Appliances erhältlich waren.

Zu den vielen erweiterten Funktionen in SonicOS Enhanced gehören unter anderem auch ISP Failover, Lastverteilung, objekt- und zonenbasiertes Management, regelbasierte NAT und Wireless Guest Services. Die ICSA-zertifizierten Geräte der TZ-Serie lassen sich per Web-Oberfläche oder mithilfe des innovativen Global Management Systems (GMS) von SonicWALL innerhalb einer IT-Umgebung mit mehreren Firewalls und VPN-Verbindungen einfach fernwarten.

Jede Appliance der TZ-Serie ist auch als komfortable und erschwingliche SonicWALL® TotalSecure™-Lösung verfügbar, die neben der Hardware alle erforderlichen Services bereitstellt, um Netzwerke zuverlässig vor unterschiedlichen Bedrohungen wie z. B. Viren, Spyware, Würmern, Trojanern, Keyloggern und anderen böswärtigen Angriffen zu schützen. Gemeinsam bilden diese Komponenten eine Unified Threat Management (UTM)-Lösung, die ein außergewöhnlich hohes Maß an Sicherheit gewährleistet.

SonicWALL TZ 190-Serie

Die TZ 190-Serie wurde für eine leistungsstarke Unified Threat Management (UTM)-Performance optimiert und bietet Organisationen die Möglichkeit, in kürzester Zeit sichere 3G Wireless-Breitbandverbindungen zu Netzwerken herzustellen, ohne dabei auf einen Festnetzanschluss angewiesen zu sein. Neben einer Deep Packet Inspection-Firewall und automatisierten Failover- und Failback-Funktionen bietet die Multi-Layer-Netzwerksicherheitsplattform mit ihrem modularen Design auch Unterstützung für 3G- und Analogmodem-PC-Karten* für den Einsatz als primäre oder sekundäre WAN-Verbindung sowie einen optionalen 802.11b/g WLAN-Zugang. Mit dem leistungsstarken SonicWALL-Betriebssystem SonicOS Enhanced ausgestattet, bietet die TZ 190-Serie außerdem erweiterte Business Continuity- und Netzwerkfunktionen wie ISP Failover, regelbasierte NAT, objektbasiertes Management und DDNS. Integrierte Echtzeitfunktionen für Viren-, Spam- und Spyware-Schutz sowie Intrusion Prevention am Gateway sorgen für erhöhte Sicherheit und gewährleisten umfassenden Schutz vor böswärtigen Bedrohungen aus dem Internet oder aus dem eigenen Netzwerk.

**Karte nicht enthalten. Informationen zu den unterstützten 3G PCMCIA Type II- und Analogmodem-PCMCIA-Karten unter: <http://www.sonicwall.com/us/products/tz190cards.html>*

SonicWALL TZ 180-Serie

Als umfassende Unified Threat Management (UTM)-Plattform bietet die TZ 180-Serie dank ihrer Deep Packet Inspection-Firewall und sicherer Wireless-Konnektivität gemäß 802.11b/g Home Offices, kleinen Betrieben, Außenstellen und Niederlassungen Business Class-Sicherheit für kabelgebundene und drahtlose Netzwerkumgebungen in einer kosteneffizienten und benutzerfreundlichen Lösung. Das kompakte Gerät verfügt über einen Ethernet WAN-Port und einen Auto-MDIX LAN Switch mit fünf Ports, über die mehrere Geräte sicher an das Netzwerk angeschlossen werden können. Netzwerkadministratoren können mit der TZ 180 Wireless mehrere Sicherheitszonen für den drahtlosen/drahtgebundenen Netzwerkzugang von Mitarbeitern bzw. drahtlosen Netzwerkzugang für Gastbenutzer einrichten, ohne die Sicherheit des Firmennetzes zu beeinträchtigen. Erweiterte Funktionen wie VPN-Verschlüsselung im WLAN sowie Wireless Intrusion Detection und die Erkennung unberechtigter Access Points sorgen für maximale Wireless-Sicherheit. Bei einem Upgrade auf SonicOS Enhanced lässt sich der optionale Port als WorkPort für Home Offices, als zweiter WAN-Zugang für ISP Failover und Lastverteilung, oder als zweiter LAN-Zugang bzw. als zusätzliche benutzerdefinierte Zone z. B. für Wireless-Anbindungen konfigurieren.



SonicWALL TZ 170 SP Wireless

Die TZ 170 SP Wireless ist eine umfassende Sicherheitsplattform für kabelgebundene und drahtlose Netzwerke, die mit ihren automatisierten Failover- und Failback-Funktionen für maximale Netzverfügbarkeit sorgt. Mit zwei Breitband-WAN-Verbindungen plus integriertem Analogmodem und sicherer Wireless-Konnektivität gemäß 802.11b/g stellt die TZ 170 SP Wireless als erste Appliance automatisierte WAN-Redundanz für Breitband- und Analogverbindungen für höchste Netzverfügbarkeit in kabelgebundenen wie drahtlosen Netzwerken zur Verfügung. Die SonicOS Enhanced Firmware von SonicWALL gehört bei der TZ 170 SP Wireless zum Lieferumfang und umfasst unter anderem erweiterte Netzwerk- und Sicherheitsfunktionen wie ISP Failover, zonen- und objektbasiertes Management, regelbasiertes Routing, NAT und Spamschutz.

SonicWALL TZ 170 SP

Als umfassende Sicherheitsplattform für Firmen mit Mitarbeitern im Home Office und Handelsunternehmen gewährleistet die TZ 170 SP mit ihren integrierten und automatisierten Failover- und Failback-Funktionen maximale Netzverfügbarkeit für die sichere Übertragung kritischer Daten. Dank eines integrierten Analogmodems und eines optionalen Ports, der über SonicOS Enhanced als zweiter WAN-Port eingerichtet werden kann, bietet die TZ 170 SP automatisierte Breitband-Breitband-Analog-WAN-Redundanz für höchste Netzverfügbarkeit.

SonicWALL TZ 150 Series

Die TZ 150-Serie integriert eine Deep Packet Inspection Firewall und einen sicheren WLAN-Zugang nach 802.11b/g in einer anwenderfreundlichen und kostengünstigen Plattform und bietet Mitarbeitern in Home Offices und kleinen Betrieben umfassenden Netzwerkschutz. Das kompakte Gerät umfasst einen Ethernet WAN-Port und einen Auto-MDIX LAN Switch mit vier Ports, über die mehrere Geräte sicher an das Netzwerk angeschlossen werden können. Die TZ 150 Wireless verfügt über erweiterte Funktionen wie VPN-Verschlüsselung im WLAN sowie Wireless Intrusion Detection und Prevention für maximale WLAN-Sicherheit. Mit der Wireless Guest Service-Funktion können Netzwerk-Administratoren mehrere Sicherheitszonen für den drahtlosen/drahtgebundenen Netzwerkzugang von Mitarbeitern und Gastbenutzern einrichten, ohne die Sicherheit des Firmennetzes zu beeinträchtigen. Die TZ 150-Serie unterstützt hardwarebeschleunigte IPSec 3DES/AES-Verschlüsselung sowie SonicWALL Global VPN Client-Updates für einen sicheren Remote-Zugriff auf geschäftskritische Netzwerk-Ressourcen.

Funktion	TZ 150-Serie	TZ 170 SP	TZ 170 SP Wireless	TZ 180-Serie	TZ 190-Serie
Nodes	10	10	10	10/25	Unlimitiert
Schnittstellen	5 Ethernet	7 Ethernet	7 Ethernet	7 Ethernet	10 Ethernet
SonicOS Standard/Enhanced	Standard	Standard	Enhanced	Standard	Enhanced
Upgrade auf SonicOS Enhanced	Nein	Ja	Nicht zutreffend	Ja	Nicht zutreffend
Stateful-Durchsatz ¹	30 MBit/s	90 MBit/s	90 MBit/s	90 MBit/s	90 MBit/s
Gateway Anti-Virus-Durchsatz ²	8 MBit/s	8 MBit/s	8 MBit/s	10 MBit/s	10 MBit/s
Intrusion Prevention-Durchsatz ²	8 MBit/s	8 MBit/s	8 MBit/s	8 MBit/s	8 MBit/s
Gateway Anti-Spyware-Durchsatz	5 MBit/s	5 MBit/s	5 MBit/s	6 MBit/s	6 MBit/s
Verbindungen	2.000	6.000	6.000	6.000	6.000
Regeln	20	100/250*	100/250*	100/250*	250
3DES/AES-Durchsatz ³	Mehr als 10+ MBit/s	Mehr als 30 MBit/s	Mehr als 30 MBit/s	Mehr als 30 MBit/s	Mehr als 30 MBit/s
Site-to-Site-VPN-Tunnel	2	2	2	2/10	15
Remote Access-VPN-Tunnel (max.)	2	5	5	5/50	25
Remote Access-VPN-Tunnel (inklusive)	Optionales Upgrade	Optionales Upgrade	Optionales Upgrade	Optionales Upgrade/1	2
Zonenspezifische Sicherheitsfunktionen	Nein	Ja*	Ja	Ja*	Ja
Objektbasiertes Management	Nein	Ja*	Ja	Ja*	Ja
Regelbasierte NAT	Nein	Ja*	Ja	Ja*	Ja
WAN/WAN Failover	Nein	Ja*	Ja	Ja*	Ja
ISP Failover	Nein	Ja*	Ja	Ja*	Ja
Lastverteilung	Nein	Ja*	Ja	Ja*	Ja
Wireless Switch und Controller	Nein	Ja*	Ja	Ja*	Ja
Integrierter Access Point	Optional	Nein	Ja	Optional	Optional
Stromversorgung über Ethernet (PoE)	Nein	Nein	Ja	Nein	Nein
Integriertes Analogmodem	Nein	Ja	Ja	Nein	Nein
Optionaler Port	Nein	Ja	Ja	Ja	Ja
Spamschutz	Nein	Ja*	Ja	Ja*	Ja
Voice over IP (VoIP)	Ja	Ja	Ja	Ja	Ja
PortShield-Architektur	Nein	Nein	Nein	Ja*	Ja
3G Wireless-Technologie	Nein	Nein	Nein	Nein	Ja
Modularer PC-Karten-Steckplatz	Nein	Nein	Nein	Nein	Ja
Bandbreitenverwaltung	Nein	Ja*	Ja	Ja*	Ja

*Bei Upgrade auf SonicOS Enhanced

¹Messung des Firewall-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1518 Bytes pro Paket

²Messung des Gateway AV/Anti-Spyware/IPS-Durchsatzes mit HTTP-Verkehr

³Messung des VPN-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1280 Bytes pro Paket



SonicWALL Secure Distributed Wireless Solution

Die SonicWALL Secure Distributed Wireless Solution vereint als erste Lösung 802.11a/b/g WLAN-Management- und Sicherheitsfunktionen mit einer Enterprise Class-Firewall und VPN-Appliance. Durch die Platzierung von SonicPoints an geeigneten Stellen lässt sich die innovative Secure Distributed Wireless-Lösung von SonicWALL flexibel für unterschiedliche Netzwerk-Infrastrukturen einsetzen. SonicPoint Access Points sind in zwei Varianten für IEEE 802.11a/b/g bzw. 802.11b/g erhältlich und stellen nahtlose und sichere WLAN-Verbindungen sowie eine Vielzahl erweiterter Funktionen und Services bereit. Mittels 802.3af-kompatibler Power over Ethernet (PoE)-Stromversorgung lassen sich die SonicPoints von SonicWALL unkompliziert in jedem beliebigen Netzwerk einrichten. Die Secure Wireless Distributed Solution basiert auf den ausgezeichneten Network Security Appliances der TZ-, PRO- und NSA-Serie (mit SonicOS Enhanced), die als sichere Wireless-Switches und Überwachungsstationen fungieren. Sie erkennen und konfigurieren SonicPoints automatisch, sobald diese an das Netzwerk angeschlossen werden, und sorgen dafür, dass die Sicherheitsregeln auf den gesamten drahtlosen und kabelgebundenen Netzwerkverkehr angewendet werden.



Erweiterte Security Services für Network Security Appliances

SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service und Application Firewall

Der Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention Service von SonicWALL bietet umfassenden Echtzeit-Netzwerkschutz gegen eine Vielzahl von dynamischen Bedrohungen, einschließlich Viren, Spyware, Würmer, Trojaner, Softwareschwachstellen wie beispielsweise Pufferüberläufe, sowie Backdoor Exploits und anderen bösartigen Code. Mit einer zusätzlichen Sicherheitsschicht schützt diese leistungsstarke Lösung sowohl vor externen als auch vor internen Angriffen über die Anwendungsebene. Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention Service von SonicWALL überwacht zahlreiche E-Mail-, Web-, Dateitransfer- und Streaming-Protokolle sowie Instant Messaging (IM) und Peer-to-Peer (P2P)-Anwendungen und schließt damit mögliche Sicherheitslücken. Die Application Firewall bietet eine Reihe konfigurierbarer Tools, mit denen sich Anwendungen gezielt überwachen lassen und die Weitergabe vertraulicher Informationen verhindert werden kann.



SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) bietet Unternehmen und Bildungseinrichtungen umfassende Funktionen, um privates Surfen am Arbeitsplatz transparent zu kontrollieren und den Zugriff auf anstößige, illegale oder gefährliche Webinhalte zu verhindern. Die dynamische Rating- und Caching-Architektur blockiert unerwünschte Webseiten nach Kategorien und garantiert 100 % Schutz dank flexibler Kontrollmechanismen.



SonicWALL Enforced Client Anti-Virus and Anti-Spyware und SonicWALL Client/Server Anti-Virus Suite

SonicWALL Enforced Client Anti-Virus and Anti-Spyware schützt Ihr Netzwerk umfassend vor Viren und Spyware und reduziert den Verwaltungsaufwand. Gemeinsam mit McAfee® entwickelt, bietet die Lösung effizienten Endpoint-Schutz durch die automatische Aktualisierung von Virensignaturen im gesamten Netzwerk. Die SonicWALL Client/Server Anti-Virus Suite erweitert die Enforced Client-Lösung um zusätzliche Serverschutzkomponenten und nutzt die ausgezeichneten McAfee-Anwendungen VirusScan Enterprise für Windows® und GroupShield für Exchange für Windows-basierte Datei-, Druck-, Mail- und Exchange-Server. Gleichzeitig verringern die Anti-Virus-Lösungen von SonicWALL den Aufwand für die Verwaltung von Antivirenregeln im gesamten Netzwerk.



Firmware für Network Security Appliances

SonicOS Enhanced Firmware

Das leistungsstarke SonicWALL-Betriebssystem der nächsten Generation enthält zahlreiche Business Continuity-Funktionen und flexible Konfigurationsoptionen für den Betrieb komplexer Netzwerke und holt so mehr aus Ihrer SonicWALL Appliance heraus. SonicOS Enhanced ist als optionales Upgrade für die PRO 3060, PRO 2040, PRO 1260, TZ 180, TZ 180 Wireless, TZ 170 SP erhältlich und ist bei der NSA-Serie sowie der PRO 5060, PRO 4100, PRO 4060, PRO 1260 Enhanced, TZ 190 und der TZ 170 SP Wireless werksseitig installiert.

**SonicWALL Secure
Remote Access
erlaubt eine gezielte
Zugriffskontrolle
auf Unternehmens-
ressourcen
– bei einfacher
Bedienung und
Verwaltung.**



Secure Remote Access-Lösungen von SonicWALL

Das traditionelle Firmen-LAN entwickelt sich immer mehr zu einem verteilten globalen Netzwerk, das Mitarbeiter, Partner und Kunden über verschiedene Internet-, Intranet-, Extranet- und VoIP-Kanäle verbindet. Mobile Mitarbeiter verlangen heute vielfältige Lösungen für einen sicheren Zugriff auf die unterschiedlichsten Ressourcen – und das von den verschiedensten Geräten und Plattformen aus. SonicWALL bietet skalierbare Secure Remote Access-Lösungen für jede Art von Organisation: von kleinen bis mittelgroßen Betrieben bis hin zu großen internationalen Unternehmen. Mit den SonicWALL Aventail E-Class SSL VPNs und SonicWALL SSL VPNs stehen dabei flexible Lösungen für den sicheren Remote-Zugriff, Disaster Recovery, Wireless-Netzwerke und sicheres Extranet zur Verfügung.

SonicWALL ^ECLASS

Die SonicWALL Aventail E-Class SSL VPN-Serie im Überblick

Die SonicWALL Aventail E-Class SSL VPNs sorgen dank unkomplizierter Zugriffsmöglichkeiten für erhöhte Produktivität. Gleichzeitig bieten sie granulare Kontrollmöglichkeiten und eine einfache Verwaltung und reduzieren so den IT-Aufwand. Die SSL VPNs von SonicWALL Aventail wurden mehrfach ausgezeichnet und von Top-Analysten als führende Branchenlösungen eingestuft. In der zunehmend auf Mobilität ausgerichteten Unternehmenswelt liefern sie die perfekte Antwort auf das Bedürfnis nach einem sicheren Remote-Zugriff. Als einheitliches, zentral verwaltetes Gateway, über das der Zugriff auf Netzwerkressourcen gesteuert wird, bieten die SonicWALL Aventail SSL VPNs zuverlässige Lösungen mit den folgenden Funktionen:

- Sicherer Remote-Zugriff auf geschäftskritische Anwendungen und Ressourcen von zahlreichen Endgeräteplattformen, darunter Mac OS X, Linux, Microsoft® Vista und Microsoft® Windows Mobile
- Einfacher Zugriff per Browser oder über einen webbasierten Thin Client, der für ein echtes „In-Office“-Erlebnis sorgt
- Business Continuity und Disaster Recovery bei unerwarteten Betriebsunterbrechungen
- Zentrale Zugangssteuerung für drahtlose Netzwerke mit Unterstützung verschiedener Geräteplattformen
- Sicherer Zugriff auf Partner-Extranets zur Verbesserung der Zusammenarbeit und Steigerung der Produktivität
- Gezielte Zugangssteuerung durch Anwendung von Regeln an verschiedenen Zugangspunkten
- Solide, zukunftssichere Grundlage für Network Access Control (NAC)
- Erweiterte Sicherheitsfunktionen, die Endpunkte vor der Authentifizierung auf bestehende Risiken untersuchen, Ressourcen anhand von granularen Regeln für verschiedene Benutzer und Endpunkte schützen und Benutzer nur mit freigegebenen Ressourcen verbinden
- Unübertroffene Kontrollmöglichkeiten, bei denen der Zugang entsprechend der Vertrauenswürdigkeit des Benutzers und des verwendeten Gerätes sowie in Abhängigkeit von den benötigten Anwendungen freigegeben wird

Secure Remote Access-Lösungen – SonicWALL Aventail E-Class SSL VPN-Serie

SonicWALL Aventail E-Class EX-2500

Bei der SonicWALL® Aventail E-Class EX-2500 handelt es sich um eine clientlose SSL VPN-Lösung, die mobilen Unternehmen eine sichere und leicht zu verwaltende Option zur Remote-Zugriffskontrolle bietet. Eine einzelne Appliance unterstützt dabei bis zu 2.000 gleichzeitige Benutzer. Die EX-2500 erhöht die Produktivität der Benutzer und verbessert die Kontrollmöglichkeiten von IT-Administratoren, indem sie den autorisierten Zugriff auf sämtliche Anwendungen über eine breite Palette von plattformübergreifenden Geräten ermöglicht.

SonicWALL Aventail E-Class EX-1600

Mittelgroßen Betrieben und Unternehmensabteilungen mit bis zu 250 gleichzeitigen Benutzern steht mit der SonicWALL® Aventail E-Class EX-1600 eine clientlose SSL VPN-Lösung zu Verfügung, die eine sichere und leicht zu verwaltende Option zur Remote-Zugriffskontrolle bietet. Die EX-1600 ermöglicht einen unkomplizierten sicheren Zugriff auf zahlreiche Anwendungen von einer Vielzahl von Geräten und Standorten. Ein einheitliches Gateway erleichtert die Steuerung und senkt die Kosten für Implementierung und Verwaltung.

SonicWALL Aventail E-Class EX-750

Die SonicWALL® Aventail E-Class EX-750 ist eine clientlose SSL VPN-Lösung mit komplettem Funktionsumfang und bietet Organisationen mit bis zu 50 gleichzeitigen Benutzern eine sichere und leicht zu verwaltende Option zur Remote-Zugriffskontrolle. Organisationen können so mobilen Mitarbeitern und Partnern von einer Vielzahl von Endgeräten und von jedem beliebigen Ort aus Zugriff auf ihre Ressourcen gewähren und dabei den Zugang gezielt kontrollieren.



SonicWALL Aventail E-Class – Optionale Add-On-Features

SonicWALL Aventail Advanced End Point Control (EPC)™

Advanced EPC verbindet eine präzise Endpunkterkennung mit erweiterter Datensicherheit.



SonicWALL Aventail Advanced Reporting™

Advanced Reporting bietet umfassende Auswertungen der Remote-Zugriffe auf eigene Ressourcen.



SonicWALL Aventail Connect Mobile™

Connect Mobile sorgt bei PDA-Geräten für ein echtes „In-Office“-Erlebnis.



SonicWALL Aventail Connect Tunnel™

Connect Tunnel bietet Benutzern von Geräten, die von der IT-Abteilung verwaltet werden, ein umfassendes „In-Office“-Erlebnis.



SonicWALL Aventail Host Access Modules™

Die Host Access Modules unterstützen die führende Terminalemulation über SSL VPN.



SonicWALL Aventail Native Access Modules™

Die Funktion Native Access Modules erlaubt den Zugriff auf serverbasierte Anwendungen über native Protokolle.



SonicWALL Aventail Spike License™

Spike License ist Ihre Disaster Recovery-„Versicherungspolice“ für den Fall, dass die Zahl der Remote-Benutzer stark ansteigt.

Funktion	EX-750	EX-1600	EX-2500
Lizenz für gleichzeitige Benutzer	10 bis 50	25 bis 250	50 bis 2.000
Einfache End Point Control (EPC)-Abfragen	Enthalten	Enthalten	Enthalten
Advanced EPC (Anti-Virus, Personal Firewall, Anti-Spyware)	Add-On	Add-On	Enthalten
Aventail Secure Desktop	Add-On	Add-On	Enthalten
Freigabe-, Sperr- oder Quarantänezonen auf der Basis von EPC-Abfragen	Enthalten	Enthalten	Enthalten
Gezielte Zugriffssteuerung (Benutzer u. Gruppe, Quell-IP, Dienst/Port, Ziel-URL, Hostname/IP-Adresse, IP-Bereich, Subnet, Domäne)	Enthalten	Enthalten	Enthalten
Advanced Reporting	Add-On	Add-On	Add-On
WorkPlace Portal	Enthalten	Enthalten	Enthalten
WorkPlace Mobile (für Mobiltelefon-Browser optimiertes Portal)	Enthalten	Enthalten	Enthalten
Native Access Modules (Citrix und Windows Terminal Services)	Add-On	Add-On	Enthalten
Host Access Modules (Zugriff über Terminalemulation)	Add-On	Add-On	Add-On
Connect Tunnel (Zugriff von Windows-, Mac- und Linux-Systemen auf TCP- oder UDP-basierte Anwendungen)	Add-On	Enthalten	Enthalten
Connect Mobile (Windows Mobile)	Add-On	Add-On	Enthalten

SonicWALL SSL VPN

**bietet einen
erschwinglichen,
benutzerfreundlichen
und
leicht zu verwaltenden
Secure Remote Access.**


**Lösungen für KMUs und Niederlassungen:
Die SonicWALL SSL VPN-Produkte im Überblick**

Die SonicWALL SSL VPN-Serie bietet Unternehmen jeder Größenordnung eine kostengünstige, anwenderfreundliche, leicht zu verwaltende und sichere Lösung für den Remote-Zugriff auf Netzwerke und Anwendungen, die ganz ohne vorinstallierte Client-Software auskommt. Benutzer können über einen Standard-Webbrowser von jedem beliebigen Punkt aus einfach und sicher auf E-Mail, Dateien, Intranet-Sites, Anwendungen, Remote-Desktops, Server und andere Ressourcen im Firmen-LAN zugreifen. SonicWALL SSL VPN lässt sich nahtlos in nahezu jede kabelgebundene oder drahtlose Netzwerk-Topologie einbinden. Die kostengünstige und dabei leistungsfähige Lösung wächst mit Ihrem Netzwerk mit und sorgt für einen sicheren Remote-Zugriff auf unternehmenseigene Ressourcen.

- Die uneingeschränkte Anzahl gleichzeitiger Tunnelverbindungen (anstelle einer Lizenzierung pro Tunnel) senkt die Kosten für die Implementierung einer skalierbaren und sicheren Remote Access-Lösung.
- Konnektivität ohne Clients macht vorinstallierte VPN-Clients (Fat Clients) überflüssig. Damit erübrigt sich auch die aufwändige Installation und Aktualisierung der Clients auf einzelnen PCs.
- Durch die nahtlose Integration mit nahezu allen Firewalls können Unternehmen die bestehende Netzwerkinfrastruktur weiter nutzen, ohne zusätzliche Hardware erwerben zu müssen.
- Gezielte Kontrolle bei der Regelkonfiguration ermöglicht es Netzwerkadministratoren, Benutzern anhand von Regeln festgelegte Anwendungen/Ressourcen zuzuordnen und den unberechtigten Zugriff auf bestimmte Netzwerkressourcen zu sperren.
- Zwei-Faktor-Authentifizierung ohne Token bietet erweiterten Schutz vor Keyloggern. Die SSL VPN-Appliance generiert ein Einmalpasswort, das an das mobile Gerät oder an die E-Mail-Adresse eines Remote-Benutzers gesendet und mit dem Netzwerknamen und dem Passwort des Benutzers kombiniert wird.
- Die Kombination mit einer SonicWALL Network Security Appliance sorgt für erweiterte Sicherheit auf allen Netzwerkebenen. Der Datenverkehr wird dabei von der Appliance mithilfe der Deep Packet Inspection-Technologie auf Sicherheitsbedrohungen wie Viren, Würmer, Trojaner und Spyware gescannt.

SonicWALL SSL-VPN 4000

Die SonicWALL SSL-VPN 4000 bietet mittleren bis großen Organisationen eine solide, leistungsstarke und flexible Remote Access-Lösung.

SonicWALL SSL-VPN 2000

Die SonicWALL SSL-VPN 2000 ist eine leistungsstarke, benutzerfreundliche und kostengünstige Secure Remote Access-Lösung für mittelgroße Unternehmen, die keine vorinstallierte Client-Software benötigt.

SonicWALL SSL-VPN 200

Die SonicWALL SSL-VPN 200 bietet kleinen Organisationen eine günstige Secure Remote Access-Lösung, die sich leicht implementieren und verwalten lässt und keine vorinstallierte Client-Software benötigt.



SSL VPN – Optionale Add-On Features

SonicWALL Virtual Assist

SonicWALL® Virtual Assist ist ein clientloses Remote Support-Tool für IT-Techniker, mit dem sie Zugriff auf die PCs oder Laptops von Kunden erhalten können, um Remote-Support zu leisten. Mit der Erlaubnis des Kunden können Techniker so innerhalb kürzester Zeit über einen Webbrowser auf den Computer zugreifen und Probleme remote identifizieren und beheben, ohne dass ein vorinstallierter „Fat Client“ erforderlich ist. Durch die Nutzung bestehender Netzwerk- und Authentifizierungsinfrastrukturen ist mit SonicWALL Virtual Assist außerdem eine enge Integration möglich.

Implementierung	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Typ und Größe der Implementierungsumgebung	Kleine Organisationen mit bis zu 50 Mitarbeitern	Mittlere Organisationen mit bis zu 500 Mitarbeitern	Mittlere Organisationen mit mehr als 500 Mitarbeitern
Empfohlene Höchstzahl gleichzeitiger Benutzer	10	50	200
Lizenz für gleichzeitige Benutzer	Unlimitiert	Unlimitiert	Unlimitiert

Funktion	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Zwei-Faktor-Authentifizierung ohne Token	Enthalten	Enthalten	Enthalten
Vasco-Unterstützung	Enthalten	Enthalten	Enthalten
RSA-Unterstützung	—	Enthalten	Enthalten
Citrix (ICA)-Unterstützung	—	Enthalten	Enthalten
NetExtender: Unterstützung für mehrere IP-Bereiche und -Routen	—	Enthalten	Enthalten
Optionale Client Certificate-Unterstützung	—	Enthalten	Enthalten
Grafische Darstellung der Nutzung	—	Enthalten	Enthalten
Reverse Proxy: OWA-Premiumversion und Lotus Domino Access	—	Enthalten	Enthalten
RADIUS-Testfunktion	—	Enthalten	Enthalten
Unterstützung für Virtual Host/Domännennamen	—	Enthalten	Enthalten
FileShares Java Applet	—	Enthalten	Enthalten
Diagnosetools: DNS Lookup und Traceroute	—	Enthalten	Enthalten
SonicWALL Virtual Assist	—	Add-On	Add-On
ViewPoint	—	Add-On	Add-On

**Effizienter und
benutzerfreundlicher
Schutz vor
E-Mail-Bedrohungen**

SonicWALL Email Security

Organisationen jeder Art müssen sich vor eingehenden E-Mail-Bedrohungen wie Spam, Phishing-Angriffen, Viren oder Zombies schützen und verhindern, dass Compliance-Vorgaben durch ausgehende E-Mails verletzt werden. Mit der äußerst leistungsfähigen und benutzerfreundlichen SonicWALL Email Security-Lösung für 10 bis 100.000 Postfächer können Sie Zeit und Kosten für den Kauf und die Verwaltung einer E-Mail-Security-Lösung deutlich senken.

SonicWALL Email Security bietet maximalen Schutz vor ein- und ausgehenden E-Mail-Bedrohungen. Dank unseren weltweit einzigartigen Methoden zur Identifizierung von Angriffen und unserem umfassenden Überwachungsnetzwerk, dem SonicWALL Global Response Intelligent Defense (GRID), sowie unseren innovativen Sicherheitstechnologien, die laufend weiterentwickelt werden, sind wir schon heute in der Lage, die Angriffe von morgen abzuwehren. Zu unseren Sicherheitsfunktionen zählen Anti-Spam-, Anti-Phishing-, Anti-Virus- und Time-Zero-Technologien (reaktiv und prädiktiv), Regelverwaltung, Verbindungsverwaltung, Zombie-Erkennung, Compliance und Content Filtering entsprechend gesetzlicher Vorgaben und interner Richtlinien sowie die Überprüfung von E-Mails.

Mit SonicWALL Email Security dauert die Verwaltung weniger als 10 Minuten pro Woche. Es müssen keine Regeln oder Spam-Scores festgelegt und keine E-Mails aus der Quarantäne aussortiert werden. Die benutzerfreundliche E-Mail-Sicherheitslösung von SonicWALL lässt sich von Administratoren genauso wie von Endbenutzern intuitiv bedienen. Für ein besonders unkompliziertes Handling sorgen folgende Vorteile: Spam-Verwaltung durch Endbenutzer, schnelle Konfiguration, nahtlose LDAP-Integration, umfassende Berichte, automatische Software- und Sicherheits-Updates sowie eine intuitive und effiziente Schnittstelle.

Dank seinem exklusiven Mail Transfer Agent (MTA) zur präventiven Prüfung von E-Mails und seinen umfassenden Funktionen zur Verbindungsverwaltung gewährleistet SonicWALL Email Security eine hohe Performance und maximalen Durchsatz. Auf diese Weise setzt SonicWALL neue Maßstäbe bei der Analyse des E-Mail-Verkehrs und ist wesentlich schneller als die Lösungen anderer Anbieter.

SonicWALL Email Security ist als Appliance- oder als Windows-Softwarelösung erhältlich. Jede Appliance verfügt über effiziente Sicherheitsfunktionen zum Schutz vor ein- und ausgehenden Bedrohungen.

SonicWALL ECLASS

SonicWALL E-Class Email Security-Lösungen im Überblick

E-Class Email Security Appliance:

SonicWALL Email Security 6000 und 8000-Serie

Die SonicWALL Email Security Appliances der E-Class-Serie bieten umfassenden, effektiven und skalierbaren E-Mail-Schutz für Unternehmensumgebungen. Neben Anti-Spam-, Anti-Virus- und Anti-Phishing-Funktionen sowie Content Filtering bietet diese leistungsstarke, aber gleichzeitig leicht verwaltbare Lösung auch Managementoptionen für ausgehende E-Mails. Außerdem wird verhindert, dass vertrauliche Informationen nach außen dringen und gesetzliche Vorschriften verletzt werden. Der exklusive Mail Transfer Agent (MTA) von SonicWALL setzt neue Maßstäbe bei der präventiven Prüfung und Analyse des E-Mail-Verkehrs und hebt sich durch seine schnellen Zustellzeiten ab. Gleichzeitig gewährleistet er hohe Performance und Skalierbarkeit.

E-Class Email Security Software:

SonicWALL Email Security Software – Enterprise

Die Email Security-Software von SonicWALL bietet Unternehmen, die standardmäßig eine bestimmte Hardware einsetzen, die bereits Backup- und Überwachungssysteme implementiert haben, oder die möglichst flexibel bleiben möchten, alle Funktionen der SonicWALL Email Security Appliances der 6000er und 8000er Serie in Form einer Software-Plattform. Dabei kombiniert die E-Mail-Sicherheitslösung optimalen Schutz mit unkomplizierter Kontrolle und hoher Performance.





SonicWALL Anti-Spam Email Security-KMU-Lösungen im Überblick
KMU-Appliance-Lösungen: SonicWALL Email Security Appliances der 200er, 300er, 400er und 500er-Serie

Diese leicht installierbaren Email Security Appliances von SonicWALL eignen sich ideal für kleine und mittelgroße Unternehmen und blockieren äußerst effektiv sämtliche E-Mail-Bedrohungen am SMTP-Gateway. Die leistungsstarken Lösungen bieten Organisationen umfassenden Schutz vor Spam, Phishing-Angriffen, Viren, DoS- und DHA-Angriffen sowie vor Zombie-Rechnern. Außerdem bieten sie zuverlässige Managementoptionen, um die Einhaltung von Regeln und gesetzlichen Vorschriften bei ausgehenden E-Mails sicherzustellen. Die Plug&Play-Appliances basieren auf dem optimierten SonicWALL OS Betriebssystem und lassen sich in weniger als einer Stunde installieren.

Software-Lösungen: SonicWALL Email Security-Software für KMUs

Die SonicWALL Email Security-Software eignet sich ideal für kleine und mittelgroße Organisationen, die eine E-Mail-Sicherheitslösung auf ihrer bestehenden Hardware implementieren möchten. Die Software enthält alle Funktionen der KMU-Appliances und bietet mit ihrer benutzerfreundlichen webbasierten Verwaltungsoberfläche umfassenden Schutz für alle ein- und ausgehenden E-Mails.



SonicWALL Email Security Services

SonicWALL Email Protection-Abo und Dynamic Support (8/5 oder 24/7)

Für die Email Security Appliances und -Software von SonicWALL ist das Email Protection-Abo mit Dynamic Support erforderlich. Der Abo-Service bietet Echtzeit-Anti-Spam- und Anti-Phishing-sowie Software- und Firmware-Updates und ergänzt die Email Security-Lösung, um Netzwerke umfassend vor E-Mail-Bedrohungen zu schützen. Außerdem bietet das Email Protection-Abo technischen Support (8/5 oder 24/7) mit Vorabaustausch-Service für die Appliance (Advanced RMA) und eine Garantie für die Reparatur bzw. den Austausch von defekten Geräten aufgrund von Produktionsfehlern.



SonicWALL Email Anti-Virus-Abo

Das SonicWALL Email Anti-Virus-Abo schützt Netzwerke mit der SonicWALL Time Zero-Technologie in der kritischen Phase zwischen dem Virenausbruch und der Bereitstellung eines neuen Signaturen-Updates. SonicWALL arbeitet bei der Aktualisierung von Signaturen mit den führenden Virenschutz-Anbietern McAfee™ und Kaspersky Lab™ zusammen, und bietet so eine zusätzliche Sicherheitsschicht.



SonicWALL Email Compliance-Abo

Das SonicWALL Email Compliance-Abo unterstützt Organisationen bei der Einhaltung von gesetzlichen Vorschriften und bei der Einführung von bewährten Standards für den E-Mail-Verkehr. Zu den im Email Compliance-Abo enthaltenen Funktionen zählen Compliance-Wörterbücher, Scannen von E-Mail-Anhängen, Approval-Ordner, Suche nach spezifischen Daten, Verschlüsselungsrouting, E-Mail-Archivierung, vordefinierte Regeln und Konformitäts-Reports. Mit SonicWALL können Organisationen E-Mails identifizieren, die gegen Richtlinien verstoßen, Probleme überwachen und melden und entsprechende Maßnahmen durchführen.

Email Security Appliances	KMU				E-Class	
	200	300	400	500	6000	8000
Lizenzierte User	50	250	750	2.000	5.000	Über 5.000
Rackoptimiertes Gehäuse	1 HE, Mini	1 HE, Mini	1 HE, Mini	1 HE, Mini	1 HE, Mini	1 HE, Maximalgröße
CPU	2,66 GHz	2,66 GHz	2,66 GHz	2,66 GHz	3,2 GHz	2 x 3,2 GHz
RAM	1 GB	1 GB	1 GB	1 GB	2 GB	2 GB
Festplatte	80 GB	80 GB	2 x 80 GB	2 x 80 GB	2 x 160 GB	2 x 146 GB
Redundant Disk Array (RAID)	Nein	Nein	Ja	Ja	Ja	Ja
Hot-swappable Laufwerke	Nein	Nein	Nein	Nein	Nein	Ja
Redundante Stromversorgung	Nein	Nein	Nein	Nein	Nein	Ja
Email Security Software						
Lizenzierte User	25	50	250	750	2.000	5.000
Software-Plattformen	Windows 2000 Server, Windows 2003 Server					

SonicWALL Content Security Manager-Serie im Überblick

Mit der SonicWALL Content Security Manager (CSM)-Serie vereint SonicWALL Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und erweitertes Content Filtering in Echtzeit und gewährleistet so maximalen Netzwerkschutz vor den immer komplexeren webbasierten Bedrohungen. Als kostengünstige, appliancebasierte Lösung bietet die CSM-Lösung kombinierte Funktionen zur Kontrolle von Internetnutzung und dynamischen Sicherheitsbedrohungen. Damit erhöht die CSM-Appliance nicht nur Ihre Netzwerksicherheit, sondern steigert auch die Produktivität Ihrer Mitarbeiter, optimiert Netzwerkressourcen und beugt rechtlichen Haftungsproblemen vor. Diese einzigartige Lösung lässt sich nahtlos in nahezu jede Netzwerk-Topologie integrieren und bietet so leistungsstarken, skalierbaren und kostengünstigen Schutz vor Sicherheitsbedrohungen.

- Gezielte Kontrollmöglichkeiten, um den Zugriff auf Websites mit nicht arbeitsrelevanten oder möglicherweise illegalen Webinhalten zu steuern.
- Wehrt ständig neue Bedrohungen wie Viren, Würmer, Trojaner, Spyware, Keylogging- und Phishing-Angriffe sowie Malicious Mobile Code (MMC) ab.
- Kontrollmechanismen für Instant Messaging, Peer-to-Peer- und Multimedia-Anwendungen für eine bessere Bandbreitennutzung.
- Dynamisch aktualisierte Signaturen- und Rating-Datenbanken garantieren, dass Sicherheitslücken rechtzeitig geschlossen werden.
- Leistungsfähiges Reporting- und Analyse-Tool bietet über individuell anpassbare Reports detaillierte Einblicke in die Netzwerknutzung.

SonicWALL CSM 3200

Die SonicWALL Content Security Manager 3200 bietet Schutz vor ein- und ausgehenden webbasierten Bedrohungen und ist für Netzwerke mit bis zu 1.000 Benutzern ausgelegt.

SonicWALL CSM 2200

Die SonicWALL Content Security Manager 2200 bietet Schutz vor ein- und ausgehenden webbasierten Bedrohungen und eignet sich für Netzwerke mit bis zu 250 Benutzern.



SonicWALL Continuous Data Protection (CDP)-Serie

Die SonicWALL CDP (Continuous Data Protection)-Serie bietet Unternehmen und Niederlassungen umfassende Datensicherheit in Form einer diskbasierten Backup- und Recovery-Lösung. Damit lassen sich Ausfallzeiten von Tagen und Stunden auf Minuten und Sekunden reduzieren, so dass Unternehmen selbst strenge RTO-(Recovery Time Objectives)- und RPO (Recovery Point Objectives)-Vorgaben einhalten können. Durch die Kombination einer unmittelbaren Datenwiederherstellung (lokale diskbasierte Datensicherung) mit einer externen Datensicherung im Katastrophenfall (Offsite-Backup) handelt es sich bei der CDP-Serie um die erste Backup- und Recovery-Lösung, die das Datenverlustrisiko nicht nur reduziert, sondern vollständig ausschaltet. Dank zentralem Management und Remote-Verwaltungsfunktionen können IT-Administratoren die Unternehmensdaten effektiver sichern.



SonicWALL Backup- und Recovery-Lösungen im Überblick

SonicWALL CDP 4440i

Bei der CDP 4440i handelt es sich um eine robuste rackoptimierte Backup- und Recovery-Lösung für Filialen und mittelgroße Organisationen. Die 2 HE-Appliance bietet 1,2 TB Kapazität für komprimierte Daten, RAID 5 sowie beschleunigten Durchsatz und AES 256-Bit-Verschlüsselung für die Offsite-Datensicherung. Zusätzlich zum Funktionsumfang der CDP 3440i bietet die CDP 4440i kontinuierliche Backups in Echtzeit für Server, Laptops, PCs, Datenbanken und Geschäftsanwendungen. IT-Administratoren profitieren von einer zentralen Verwaltung und können die an die SonicWALL CDP-Appliance angeschlossenen Client-Computer bis auf die Dateiebene einsehen. Somit lassen sich Backup-Regeln konsequent anwenden und Kontrollfunktionen bis auf Endbenutzer-Ebene einrichten.

SonicWALL CDP 3440i

Die CDP 3440i sorgt für höchste Datensicherheit in kleinen bis mittelgroßen Organisationen und Niederlassungen. Die ultra-leistungsstarke 1 HE-Appliance ist für 75 Benutzer und 5 Server ausgelegt und bietet 600 GB Kapazität für komprimierte Daten, RAID 1, beschleunigten Durchsatz und AES 256-Bit-Verschlüsselung für die Offsite-Datensicherung. Mithilfe von regelbasierten Backups, zentraler Verwaltung und Backups von geöffneten Dateien bietet die CDP 3440i kontinuierliche Echtzeit-Datensicherheit für Server, Laptops und PCs. Die Appliance unterstützt außerdem native Backups von Microsoft® Exchange, Outlook, SQL und Active Directory.

SonicWALL CDP 2440i

Die CDP 2440i ist ideal für kleine Organisationen und Niederlassungen geeignet. Neben 300 GB Kapazität für komprimierte Daten sowie Standard-Durchsatz und AES 256-Bit-Verschlüsselung für die Offsite-Datensicherung bietet die Appliance kontinuierliche Echtzeit-Backups für Server, Laptops und PCs. Die CDP 2440i unterstützt gängige Datenbanken und Anwendungen wie SQL-Server und Microsoft Exchange, ohne dass weitere Software-Pakete installiert werden müssen, und hebt sich dadurch von den Produkten der meisten Mitbewerber ab.

SonicWALL CDP 1440i

Die diskbasierte Backup- und Recovery Appliance CDP 1440i bietet kleinen Organisationen durchgängige Echtzeit-Datensicherheit sowie spezielle Funktionen zur unmittelbaren Datenwiederherstellung und zur zentralen Verwaltung. Die Appliance unterstützt Server, PCs und Laptops in kleinen Unternehmensnetzwerken mit bis zu 15 Benutzern. Darüber hinaus bietet sie 192 GB Kapazität für komprimierte Daten und AES 256-Bit-Verschlüsselung für die Offsite-Datensicherung.



SonicWALL Backup- und Recovery-Lizenzen und -Services

Mit den automatisierten Offsite Backup- und Recovery-Lösungen von SonicWALL können Daten entweder an ein externes Datacenter oder an eine verwaltete CDP-Appliance übertragen werden, so dass Unternehmen nach einem Katastrophenfall den Betrieb schnell wieder aufnehmen können. Alle Daten werden mit einem AES 256-Bit-Chiffrierschlüssel, den nur der Endbenutzer kennt, übermittelt und gespeichert. Die Daten können direkt in einer CDP-Appliance mit Point&Click-Oberfläche wiederhergestellt werden. Außerdem steht Ihnen der Support von SonicWALL jederzeit bei der Wiederherstellung Ihrer Daten zur Seite.

SonicWALL CDP Offsite-Datenbackup-Service

Der SonicWALL CDP Offsite-Datenbackup-Service bietet eine vollverwaltete Offsite-Lösung für eine unkomplizierte Datensicherung im Katastrophenfall. Dabei werden die Daten direkt in einer CDP-Appliance mit Point&Click-Funktion wiederhergestellt. Die Datacenter verfügen über eine unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselgeneratoren, Schutz vor Erdbeben und Überschwemmungen, redundanten Brandschutz, HVAC und 24-Stunden-Überwachung.

SonicWALL CDP Site-to-Site-Backup

Das SonicWALL CDP Site-to-Site-Backup ist für Kunden und Händler ausgelegt, die ihre Katastrophen-Sicherheitslösung verwalten möchten. Dank Site-to-Site-Backup können sämtliche CDP Appliances für das Offsite-Backup eingesetzt werden. Auf diese Weise kann eine einzige Offsite Appliance Katastrophensicherheit für mehrere nachgeschaltete CDP-Appliances gewährleisten. Im Katastrophenfall können Daten mit der Enterprise Manager-Software von SonicWALL schnell auf einer neuen CDP Appliance wiederhergestellt werden.

SonicWALL CDP Bare Metal Recovery/Local Archiving

Die Bare Metal Recovery (BMR)-Software erstellt ein exaktes Abbild des gesamten Servers oder der gesamten Workstation, einschließlich der Betriebssystem-Dateien, Programme, Datenbanken und Einstellungen. So lässt sich das komplette System innerhalb von nur wenigen Minuten über eine anwenderfreundliche grafische Benutzeroberfläche mithilfe eines Assistenten wiederherstellen. Die BMR-Software enthält lokale Archivierungsfunktionen, mit denen Unternehmen Snapshots ihrer Daten über lange Zeiträume hinweg speichern können, um die Einhaltung von Branchenstandards und gesetzlichen Vorschriften zu unterstützen.

Funktion	CDP 1440i	CDP 2440i	CDP 3440i	CDP 4440i
Core Compression-Technologie	Standard	Standard	Erweitert	Erweitert
Verschlüsselung	AES 256-Bit	AES 256-Bit	AES 256-Bit	AES 256-Bit
Durchsatz	Standard	Standard	Beschleunigt	Beschleunigt
Benutzer (empfohlen)	Maximal 15	Maximal 30	Maximal 75	Maximal 100
Server (empfohlen)	1-2	2-3	Maximal 5	Maximal 5
Grundkapazität¹	160 GB	250 GB	400 GB	600 GB
Kapazität mit Komprimierung²	192 GB	300 GB	800 GB	1,2 TB
Gehäuse	Mini	Mini	1 HE-Rack	2 HE-Rack
RAID	Nicht zutreffend	Nicht zutreffend	RAID 1	RAID 5
Schnittstelle	1 x 10/100 Base-T Ethernet	1 x 10/100 Base-T Ethernet	10/100/1000 GIG LAN	10/100/1000 GIG LAN
Continuous Data Protection	Ja	Ja	Ja	Ja
Datei-Versionen	Ja	Ja	Ja	Ja
Zentrale Verwaltung	Ja	Ja	Ja	Ja
Desktop-, Laptop-, Server-Backup	Ja	Ja	Ja	Ja
Remote-Verwaltung	Ja	Ja	Ja	Ja
Backup geöffneter Dateien	Ja	Ja	Ja	Ja
Regelbasiertes Backup	Ja	Ja	Ja	Ja
Active Directory Backup	Nein	Ja	Ja	Ja
SQL Server-Unterstützung	Nein	Ja	Ja	Ja
MS Exchange Server-Unterstützung	Nein	Ja	Ja	Ja
Bare Metal Recovery/Local Archiving - Workstation	Ja (inklusive 1 Lizenz)	Ja (inklusive 2 Lizenzen)	Ja (inklusive 5 Lizenzen)	Ja (inklusive 10 Lizenzen)
Bare Metal Recovery/Local Archiving - Server	Nein	Nein	Ja (inklusive 1 Lizenz)	Ja (inklusive 2 Lizenzen)

¹Angabe der produktspezifischen Kapazität in Gigabyte (GB) bzw. Terabyte (TB). Dabei entspricht 1 GB 1.000.000.000 Bytes und 1 TB 1.000.000.000.000 Bytes.
²Bei der Kapazität mit Komprimierung wird ein Verhältnis von 1,2:1 für die Standard-Datenkompression und 2:1 für die erweiterte Datenkompression zugrunde gelegt. Die tatsächliche Kapazität kann abhängig von den zu sichernden Daten variieren.



Global Management System (GMS)

SonicWALL Global Management System (GMS) bietet Organisationen, Service-Anbietern und Unternehmen mit verteilten Netzwerken ein flexibles, leistungsstarkes und intuitives Tool, um SonicWALL Appliances und Sicherheitsregeln zentral zu verwalten und schnell zu implementieren. Auf diese Weise lassen sich Anwendungen wie Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Content Filtering inklusive aller Detailinformationen von einer einzigen Konsole aus global verwalten. SonicWALL GMS verringert so den Bedarf an IT-Personal und reduziert Kosten- sowie Zeitaufwand bei der Implementierung einer Internet Security-Infrastruktur.

- Vereinfachte Konfiguration und komfortable Anwendung globaler Sicherheits- und VPN-Regeln
- Zentrales Reporting und Überwachung von Security Appliances und Benutzer-Aktivitäten
- Skalierbare Lösung für wachsende Infrastrukturen



SonicWALL ViewPoint

Mit seinem komfortablen webbasierten Reporting stellt SonicWALL ViewPoint™ eine ideale Ergänzung zu den übrigen Sicherheitsprodukten und Services von SonicWALL dar. Durch die benutzerdefinierte Übersichtsanzeige und eine Vielzahl unterschiedlicher historischer Reports erhalten Administratoren mit SonicWALL ViewPoint einen detaillierten Überblick über den Zustand des Netzwerks, inklusive Netzwerkauslastung, Security-Aktivitäten und Internetnutzung.

- Übersichtliche grafische Reports zu Netzwerk- und Security-Aktivitäten
- Geringerer Verwaltungsaufwand dank On-Demand-Reporting
- Schnelle Implementierung und einfacher Zugriff (lokal oder remote) dank Web-Oberfläche



MySonicWALL

Mit MySonicWALL können IT-Manager alle SonicWALL Netzwerk- und Datensicherheits-Appliances sowie die dazugehörigen Services komfortabel und zentral registrieren bzw. verwalten. MySonicWALL ist ein benutzerfreundliches Online-Kundenportal, das die zentrale Verwaltung aller SonicWALL-Produkte ermöglicht. Vielbeschäftigte IT-Manager können mit MySonicWALL alle Firmware-Versionen, Software-Lizenzen oder Abos für Sicherheitsservices einsehen und auf diese Weise viel Zeit bei der Verwaltung sparen.

- MySonicWALL verhindert, dass Abos für Sicherheitsservices unbemerkt ablaufen, was den Geschäftsbetrieb lahm legen und zu kostspieligen Sicherheitsschwachstellen führen kann.
- Mit MySonicWALL können IT-Manager ganz unkompliziert bestehende Sicherheitsservices verlängern und Abos für zusätzliche Netzwerk- und Datensicherheitsservices beziehen.
- Außerdem können Kunden mit MySonicWALL die Installation mehrerer Einzelprodukte, wie z. B. Network Security Appliances, Email Security Appliances und Datenbackup- und Recovery-Lösungen verwalten, die über das gesamte Unternehmen hinweg verteilt sind.



SonicWALL Global Support Services

Mit einem starken Portfolio an Global Support Services sorgt SonicWALL dafür, dass Ihre Netzwerksicherheit und Ihre Datenbackup- und Recovery-Infrastruktur immer auf dem neuesten Stand bleiben und mögliche Probleme in kürzester Zeit gelöst werden. Für einen umfassenden Netzwerkschutz jedoch braucht es heutzutage mehr. Unsere Support Services beinhalten daher auch wichtige Updates und Upgrades, kompetenten technischen Support, den Zugang zu zahlreichen elektronischen Tools, einen schnellen Hardware-Austausch sowie Zugriff auf eine breite Palette elektronischer Tools.

SonicWALL E-Class 24/7-Support

Der E-Class 24/7-Support wurde für Kunden mit E-Class-Lösungen konzipiert und bietet die Servicequalität und die Support-Funktionen, die Geschäftskunden für einen reibungslosen und effizienten Netzwerkbetrieb benötigen.

- Telefonischer und webbasierter technischer Support rund um die Uhr, an 365 Tagen im Jahr und direkter Kontakt mit einem Team hervorragend ausgebildeter und erfahrener Support-Ingenieure
- Abo auf Firmware-Updates und -Upgrades
- Vorabaustausch von Hardware im Fehlerfall

Dynamic 8/5- und 24/7-Support

Dieses Servicepaket wurde für Kunden entwickelt, die einen kontinuierlichen Service in Form von regelmäßigen Firmware-Updates und intensivem technischem Support benötigen. SonicWALL Dynamic Support ist je nach Bedarf entweder während der üblichen Geschäftszeiten oder rund um die Uhr (24/7) verfügbar. Die Services im Überblick:

- Abo für Firmware-Updates und -Upgrades
- Telefonischer und webbasierter Support bei der Basis-Konfiguration und Fehlerbehebung
- Vorabaustausch von Hardware im Fehlerfall

Comprehensive Global Management System (GMS)

Für Kunden, die ihre verteilten Netzwerke mit SonicWALL Global Management System (GMS) verwalten, stellt SonicWALL den Support-Service Comprehensive GMS zur Verfügung. Dieser Service bietet für alle Appliances, die mit SonicWALL GMS verwaltet werden, die gleichen Vorteile wie ein 8/5- oder 24/7-Supportvertrag. Im Einzelnen bietet Comprehensive GMS:

- Alle Services und Vorteile eines 8/5- oder 24/7-Supportvertrags
- Support und Software-Updates für die GMS-Anwendung selbst
- Vereinfachte Verwaltung durch gemeinsames Ablaufdatum für alle SonicWALL-Produkte

SonicWALL – führender Anbieter von Sicherheitslösungen

SonicWALL, Inc. wurde 1991 gegründet und entwickelt seitdem Lösungen für Unternehmen und Organisationen in aller Welt. Wir sind der Meinung, dass Sicherheitslösungen mehrere Funktionen erfüllen sollten – vor allem, wenn sie direkt am Gateway eingesetzt werden. So waren wir auch die Ersten, die Zusatzfunktionen wie VPN und Content Filtering in Firewall Appliances integriert haben.

Heute gehören wir zu den Marktführern im Bereich Netzwerkschutz, Secure Remote Access, Web und Email Security sowie Backup und Recovery. Zu den weltweit führenden Produkten von SonicWALL gehören z. B. unsere Unified Threat Management-Lösungen. Diese appliancebasierten Produkte und Services integrieren Anti-Virus- und Anti-Spyware-Schutz sowie Intrusion Prevention in einem einzigen umfassenden Paket und eignen sich für drahtlose und kabelgebundene Netzwerke jeder Größe. Mit über einer Million verkaufter Network Security- und Data Protection-Lösungen bietet SonicWALL Millionen von Benutzern in kleinen, mittleren und verteilten Netzwerken zuverlässigen Schutz vor Sicherheitsbedrohungen sowie eine optimale Netzwerkproduktivität. Davon profitieren nicht nur Unternehmen wie E-Commerce-Anbieter oder Handelsfirmen, sondern auch öffentliche Einrichtungen und Organisationen aus den Bereichen Bildung und Gesundheitswesen.

SonicWALLs Engagement reicht weit über die Herstellung von Produkten hinaus. Unsere Mission sehen wir darin, bei der Entwicklung zuverlässiger Netzwerk- und Datensicherheitslösungen gegen aktuelle und künftige Internet-Sicherheitsbedrohungen immer den entscheidenden Schritt voraus zu sein. Zu unseren strategischen Partnern gehören daher einige der stärksten Unternehmen der IT-Branche. Das weltweite SonicWALL Händler- und Distributoren-Netzwerk zählt mehr als 15.000 hochqualifizierte Experten. SonicWALL bietet seinen Kunden außerdem umfassenden technischen Support und baut auf die besten Security- und Datensicherheitsspezialisten der Welt – nur so können wir unser Ziel erreichen: die kontinuierliche Weiterentwicklung innovativer Komplettlösungen in den Bereichen Netzwerksicherheit, Secure Remote Access, Web- und Email Security, Backup und Recovery, sowie Policy und Management-Lösungen.

SonicWALL Deutschland

Tel.: +49 89 4545 946
www.sonicwall.de

SonicWALL Schweiz

Tel.: +41 44 810 31 35
www.sonicwall.ch

SonicWALL Österreich

Tel.: +41 44 810 31 35
www.sonicwall.at

