SonicWall TZ Series

Herausragende Sicherheit und exzellente Leistung bei unglaublich niedrigen Gesamtbetriebskosten

Die SonicWall-Next-Generation-Firewalls der TZ Series eignen sich perfekt für Organisationen, die einen Enterprise-Class-Netzwerkschutz benötigen.

Dank integrierter und Cloud-basierter Funktionen wie Anti-Malware, Anti-Spyware, Anwendungskontrolle, Intrusion-Prevention-System (IPS) und URL-Filtering sorgen die erweiterten Sicherheitsservices der SonicWall TZ-Firewalls für einen umfassenden Schutz. Die SonicWall TZ Series hat die nötige Rechenpower, um verschlüsselte SSL-Verbindungen auf die neuesten Bedrohungen zu prüfen, und bietet so einen effektiven Schutz vor der zunehmenden Zahl verschlüsselter Angriffe. Zusammen mit den Switches der X-Series können ausgewählte Firewalls der TZ Series die Sicherheitseinstellungen dieser zusätzlichen Ports direkt verwalten.

Über das SonicWall Global Response Intelligent Defense(GRID)-Netzwerk wird die SonicWall TZ Series kontinuierlich mit Aktualisierungen versorgt, sodass sie das Netzwerk zuverlässig vor Cyberkriminellen schützen kann. Die SonicWall TZ Series scannt jedes Byte in jedem Paket, auf allen Ports und für alle Protokolle – ganz ohne Einschränkungen bei der Dateigröße und beinahe ohne Latenz.

Zum Leistungsumfang der SonicWall TZ Series gehören Gigabit-Ethernet-Ports, optionales integriertes 802.11ac-WLAN*, IPSec und SSL-VPN, Failover mit integrierter 3G-/4G-Unterstützung, Lastverteilung und Netzwerksegmentierung. Die UMT-Firewalls der SonicWall TZ Series bieten außerdem einen schnellen, sicheren Mobilzugriff von Apple iOS-, Google Android-, Amazon Kindle-, Windows-, MacOS- und Linux-Plattformen.

Das SonicWall Global Management System (GMS) ermöglicht die zentrale Bereitstellung und Verwaltung von SonicWall TZ-Firewalls über ein einziges System.

Verwaltete Sicherheit für verteilte Umgebungen

Schulen, Einzelhandels-, Zweig- und Remote-Niederlassungen sowie Unternehmen mit geografisch verteilten Standorten benötigen eine Lösung, die sich in die bestehende Firewall integrieren lässt. Die SonicWall TZ-Firewalls verwenden die gleiche Codebasis und die gleichen Sicherheitsfunktionen wie unser Flaggschiffprodukt – die SuperMassive-Next-Generation-Firewalls. Dies vereinfacht die Verwaltung von Remote-Standorten, da jeder Administrator mit der gleichen Benutzeroberfläche arbeitet. GMS erlaubt Netzwerkadministratoren die zentrale Konfiguration, Überwachung und Verwaltung von SonicWall-Firewalls an Remote-Standorten über eine einzige Schnittstelle. Dank Funktionen für sichere Highspeed-Wireless-Konnektivität erweitert die SonicWall TZ Series den Sicherheitsperimeter auch auf Kunden und Gäste, die Einzelhandels- oder Remote-Niederlassungen besuchen.

Vorteile:

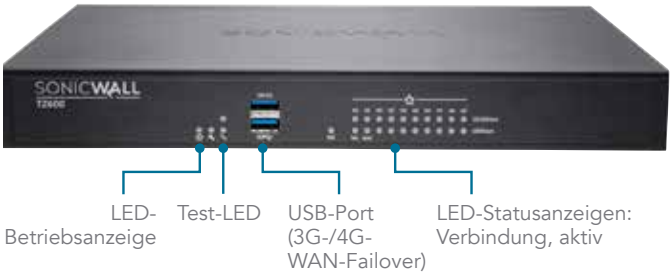
- Netzwerksicherheit der Enterprise-Klasse
- Deep Packet Inspection für den gesamten Datenverkehr ohne Einschränkungen bei Dateigröße oder Protokoll
- Sichere 802.11ac-Wireless-Konnektivität über einen integrierten Wireless-Controller oder mithilfe externer SonicPoint Wireless-Access-Points
- SSL-VPN-Mobilzugriff für Apple iOS-, Google Android-, Amazon Kindle-, Windows-, Mac OS- und Linux-Geräte
- Über 100 zusätzliche Ports lassen sich auf sichere Weise von der TZ-Konsole aus verwalten, wenn diese zusammen mit den Switches der X-Series implementiert wird

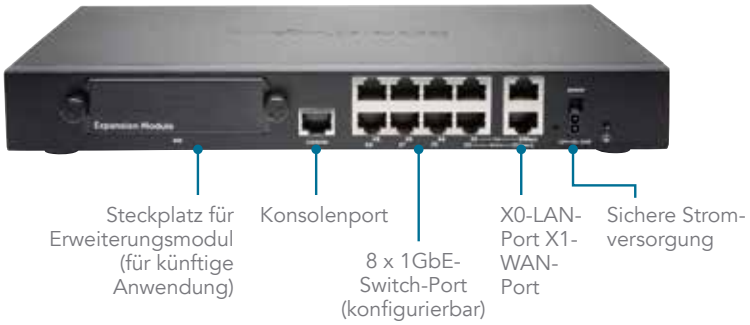
** 802.11ac ist aktuell nicht für die SOHO-Modelle verfügbar; die SOHO-Modelle unterstützen 802.11a/b/g/n.*

SonicWall TZ600 Series

Junge Unternehmen, Einzelhandelsniederlassungen und Zweigstellen suchen leistungsstarke Netzwerksicherheit zu einem erstklassigen Preis-Leistungs-Verhältnis. Die SonicWall TZ600-Next-Generation-Firewall bietet genau das – dank Funktionen der Enterprise-Klasse und kompromisslos starker Performance.

Technische Daten	TZ600 Series
Firewall-Durchsatz	1,5 GBit/s
Full-DPI-Durchsatz	500 MBit/s
Anti-Malware-Durchsatz	500 MBit/s
IPS-Durchsatz	1,1 GBit/s
IMIX-Durchsatz	900 MBit/s
Max. Anzahl an DPI-Verbindungen	125.000
Neue Verbindungen/Sekunde	12.000

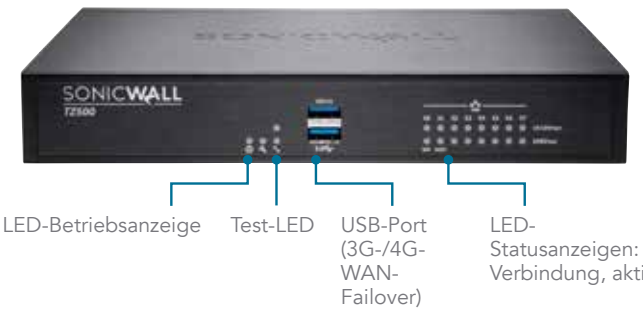




SonicWall TZ500 Series

Dynamisch wachsenden Zweigstellen und KMUs bietet die SonicWall TZ500 Series einen hocheffektiven, kompromisslosen Schutz bei hoher Netzwerkproduktivität sowie optionale integrierte Dualband-Wireless-Konnektivität gemäß dem 802.11ac-Standard.

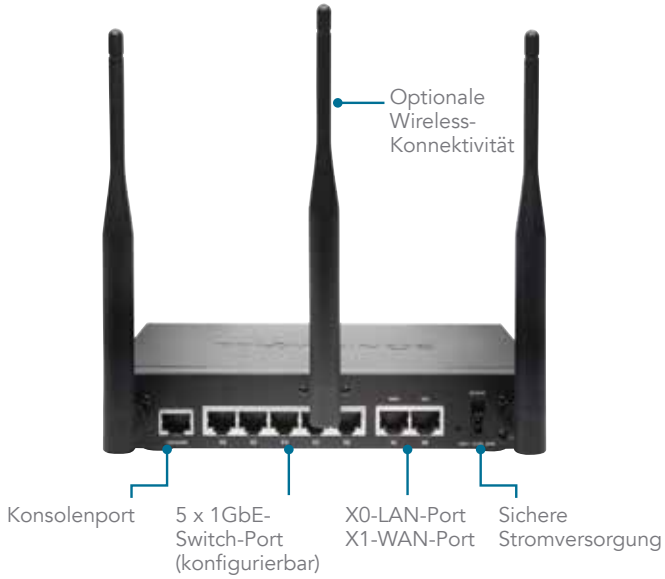
Technische Daten	TZ500 Series
Firewall-Durchsatz	1,4 GBit/s
Full-DPI-Durchsatz	400 MBit/s
Anti-Malware-Durchsatz	400 MBit/s
IPS-Durchsatz	1,0 GBit/s
IMIX-Durchsatz	700 MBit/s
Max. Anzahl an DPI-Verbindungen	100.000
Neue Verbindungen/Sekunde	8.000



SonicWall TZ400 Series

Die SonicWall TZ400 Series bietet kleinen Unternehmen sowie Einzelhandels- und Zweigniederlassungen Schutz der Enterprise-Klasse. Darüber hinaus ist eine flexible Wireless-Bereitstellung möglich, entweder über externe SonicPoint-Access-Points oder die im Gerät integrierte 802.11ac-Wireless-Funktion.

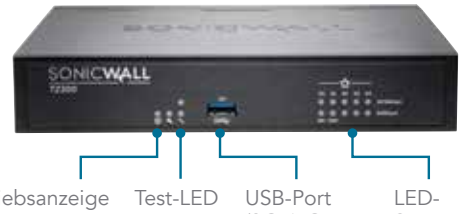
Technische Daten	TZ400 Series
Firewall-Durchsatz	1,3 GBit/s
Full-DPI-Durchsatz	300 MBit/s
Anti-Malware-Durchsatz	300 MBit/s
IPS-Durchsatz	900 MBit/s
IMIX-Durchsatz	500 MBit/s
Max. Anzahl an DPI-Verbindungen	90.000
Neue Verbindungen/Sekunde	6.000

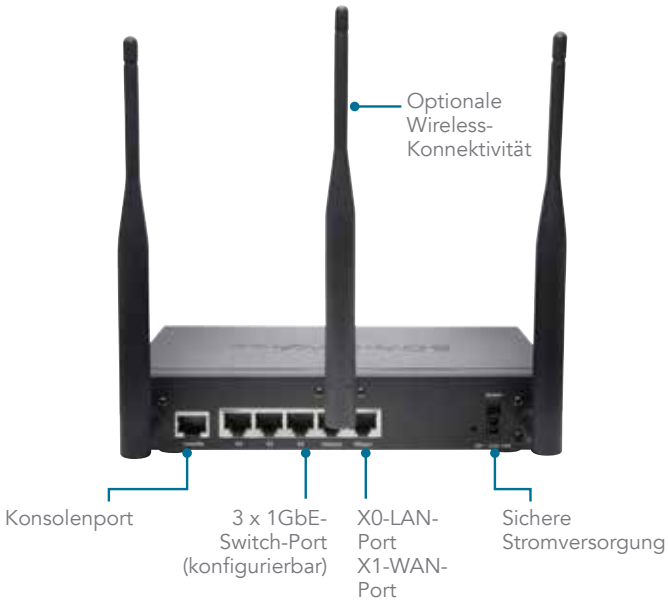


SonicWall TZ300 Series

Die SonicWall TZ300 Series ist eine All-in-one-Lösung, die Netzwerke wirksam vor Angriffen schützt. Die SonicWall TZ300-Firewall kombiniert effektive Funktionen für Malware-Schutz, Intrusion-Prevention und Inhalts-/URL-Filterung mit optionaler integrierter 802.11ac-Wireless-Konnektivität und bietet die derzeit breiteste sichere Mobilplattformunterstützung für Laptops, Smartphones und Tablet-PCs.

Technische Daten	TZ300 Series
Firewall-Durchsatz	750 MBit/s
Full-DPI-Durchsatz	100 MBit/s
Anti-Malware-Durchsatz	100 MBit/s
IPS-Durchsatz	300 MBit/s
IMIX-Durchsatz	200 MBit/s
Max. Anzahl an DPI-Verbindungen	50.000
Neue Verbindungen/Sekunde	5.000

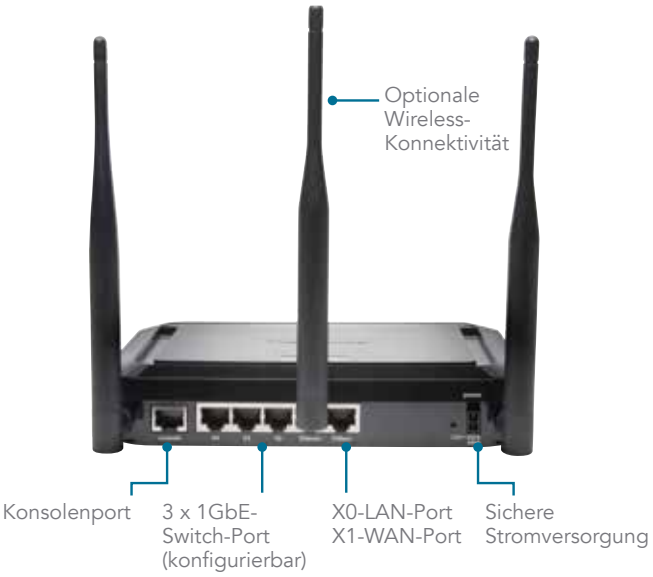




SonicWall SOHO Series

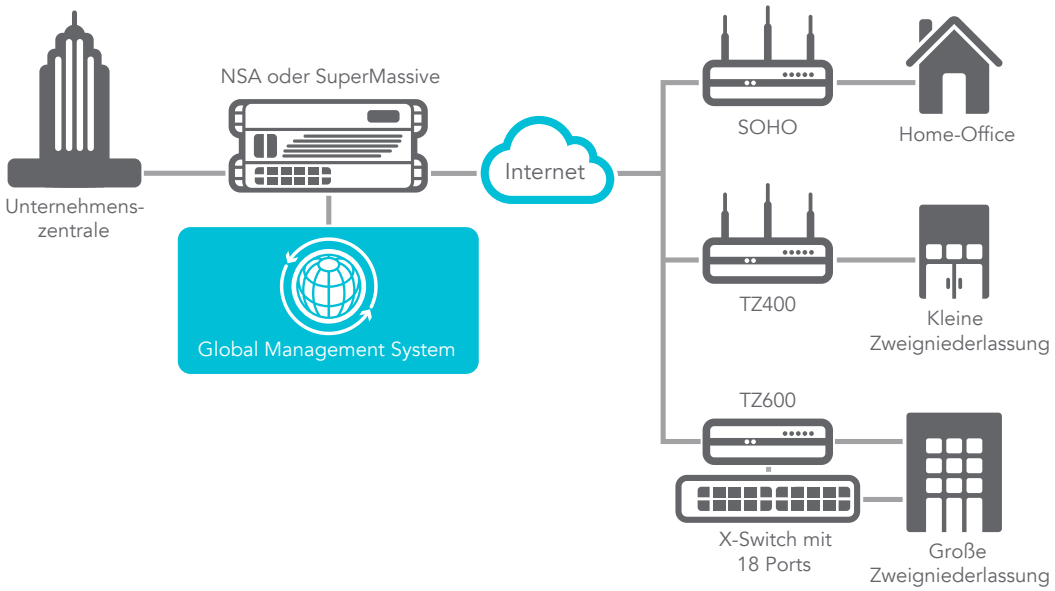
Die SonicWall SOHO Series bietet kleinen Unternehmen und Heimbüros mit kabelgebundenen oder drahtlosen Netzwerken denselben Enterprise-Class-Schutz, den auch große Organisationen benötigen – zu einem erschwinglicheren Preis.

Technische Daten	SOHO Series
Firewall-Durchsatz	300 MBit/s
Full-DPI-Durchsatz	50 MBit/s
Anti-Malware-Durchsatz	50 MBit/s
IPS-Durchsatz	100 MBit/s
IMIX-Durchsatz	60 MBit/s
Max. Anzahl an DPI-Verbindungen	10.000
Neue Verbindungen/Sekunde	1.800



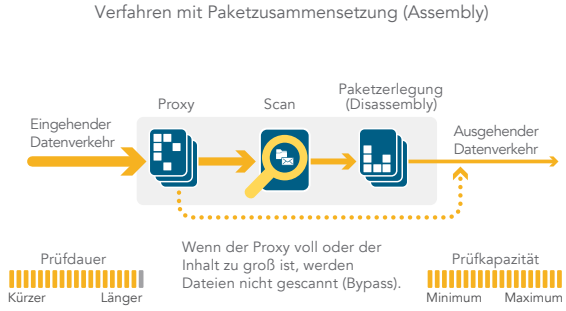
Erweiterbare Architektur für höchste Skalierbarkeit und Performance

Die Reassembly-Free Deep Packet Inspection(RFDPI)-Engine wurde von Grund auf so entwickelt, dass Sicherheitsprüfungen mit hohen Durchsatzraten durchgeführt werden können. Auf diese Weise wird den Anforderungen der parallelen Verarbeitung sowie der ständig steigenden Bandbreite Rechnung getragen. Diese Architektur ermöglicht eine parallele Verarbeitung und lässt sich in Kombination mit Multi-Core-Prozessoren optimal skalieren. Eine effektive Deep Packet Inspection-Prüfung ist so auch bei hohen Verkehrslasten gewährleistet. Die SonicWall TZ Series-Plattform arbeitet mit Prozessoren, die – im Gegensatz zum x86 – für die Verarbeitung von Paketen, verschlüsselten Daten sowie Netzwerkverkehr optimiert sind und dabei gleichzeitig Flexibilität und Programmierbarkeit vor Ort garantieren – ASIC-Systeme können da nicht mithalten. Diese Flexibilität ist besonders wichtig, wenn neue Updates zu Code und Verhalten nötig sind, um sich vor neuen Angriffen zu schützen, die innovative und technisch ausgefeiltere Erkennungsmethoden erfordern.

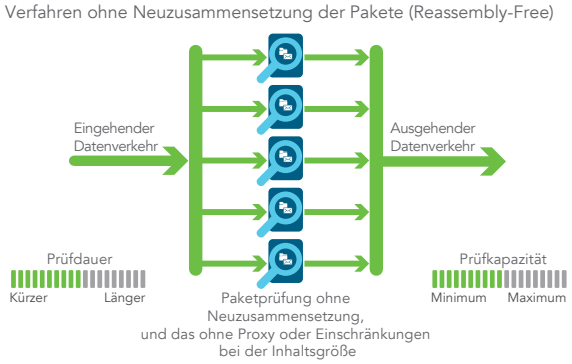


Reassembly-Free Deep Packet Inspection(RFDPI)-Engine

Die RFDPI-Engine bietet einen optimalen Schutz vor Bedrohungen und eine umfassende Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Dabei prüft die patentierte Engine den Datenstrom, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren. Durch die RFDPI-Engine wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich raffinierte Umgehungsversuche verhindern, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code in das Netzwerk einzuschleusen. Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall aktualisiert und mit diesen Datenbanken abgeglichen. Dabei wird geprüft, ob ein Angriff oder ein anderes sicherheitsrelevantes Ereignis eintritt. Ist dies der Fall, wird eine vordefinierte Aktion ausgeführt. Wird Malware erkannt, beendet die SonicWall-Firewall die Verbindung, bevor das Netzwerk kompromittiert werden kann, und protokolliert anschließend das Ereignis. Die Engine kann jedoch auch nur für Prüfungen konfiguriert werden oder – wenn die Anwendungserkennung aktiv ist – so, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.



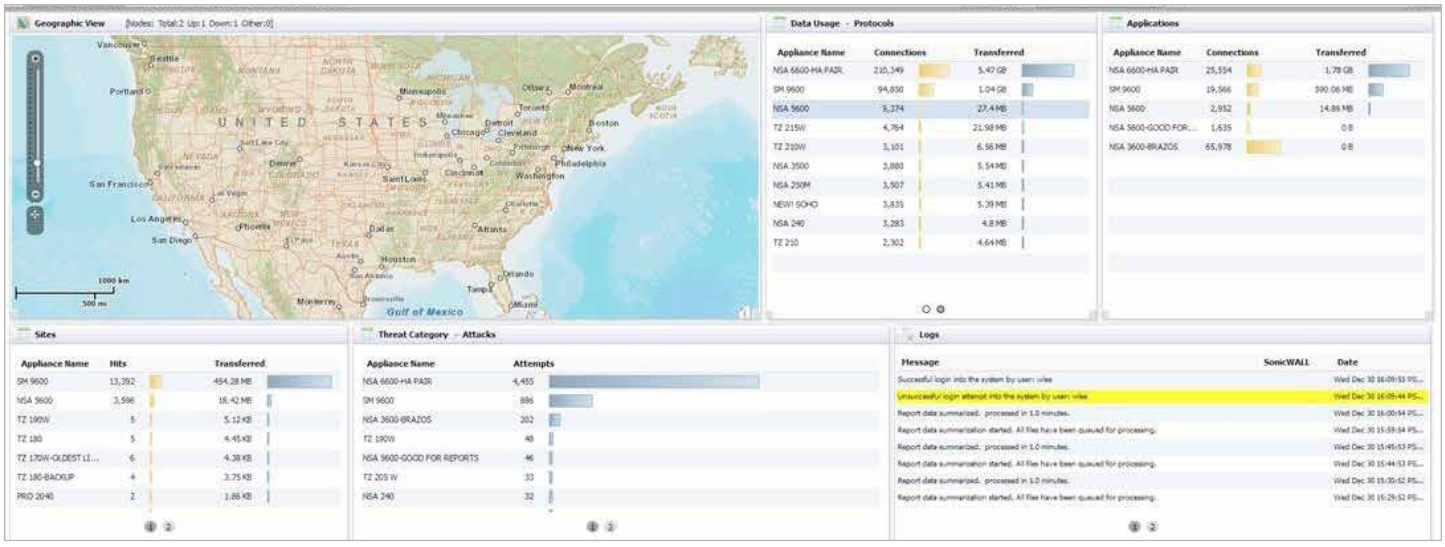
Architektur von Mitbewerberlösungen



SonicWall-Architektur

Globales Management und Reporting

In größeren, verteilten Unternehmensumgebungen bietet das optionale SonicWall Global Management System (GMS) Administratoren eine einheitliche, sichere und erweiterbare Plattform für die Verwaltung von SonicWall-Sicherheitsappliances und Switches der X-Series. Mit ihr können Unternehmen die Verwaltung ihrer Sicherheitsappliances unkompliziert konsolidieren, Administration und Fehlerbehebung vereinfachen und alle betrieblichen Aspekte der Sicherheitsinfrastruktur steuern. Unter anderem bietet die Plattform zentralisierte Richtlinienverwaltung und -durchsetzung sowie Ereignisüberwachung, -analyse und -Reporting in Echtzeit. Dank einer Funktion zur Workflow-Automatisierung können Unternehmen mit GMS zudem auch alle Änderungen an ihren Firewalls effektiv verwalten. Mit GMS können Sie die Netzwerksicherheit jetzt besser auf Ihre Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, statt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

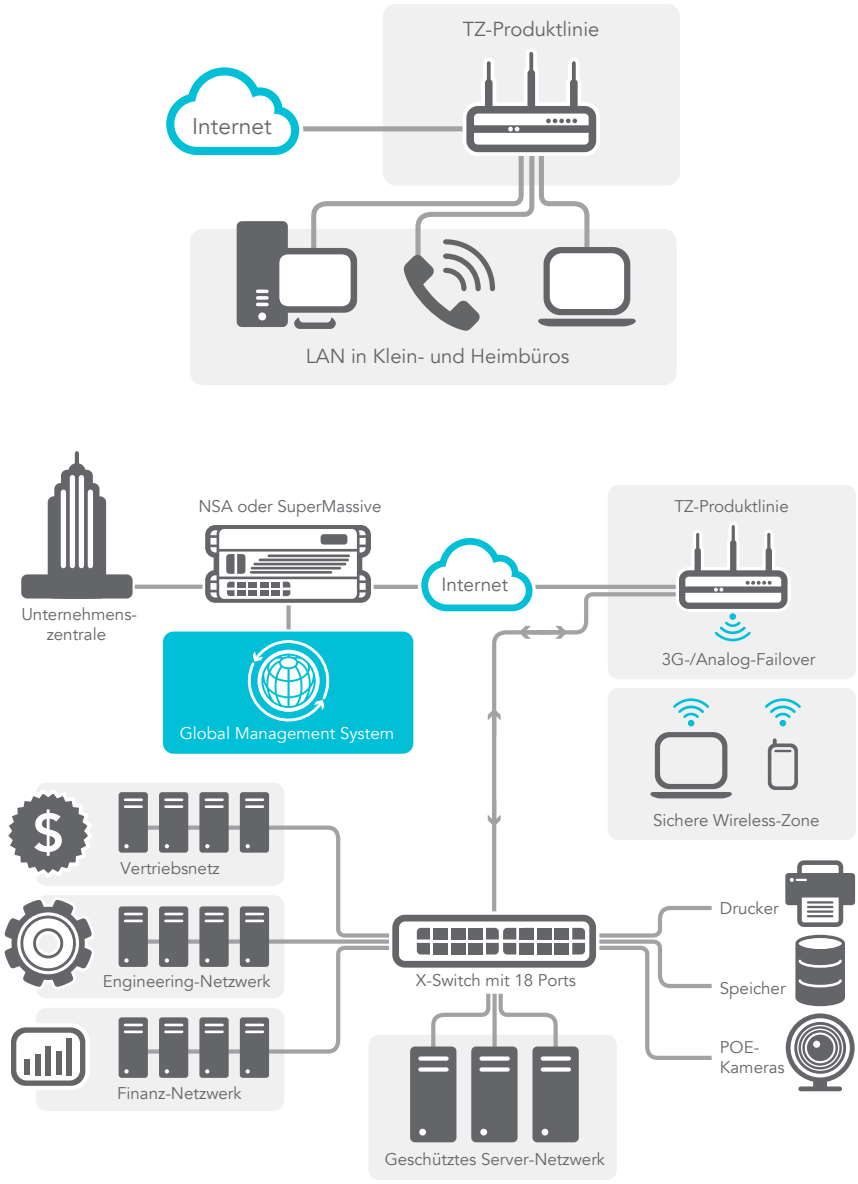


Sicherheit und Schutz

Das dedizierte interne SonicWall Threat Research-Team ist für die Erforschung und Entwicklung von Abwehrmechanismen zuständig. Diese werden in die Kunden-Firewalls implementiert, um aktuellen Schutz zu gewährleisten. Das Team nutzt weltweit über eine Million Sensoren, die Malware-Muster sammeln und Telemetriedaten zu den neuesten Bedrohungen liefern. Diese Informationen werden anschließend für wichtige Funktionen wie Intrusion-Prevention, Malware-Schutz und Anwendungserkennung eingesetzt. SonicWall-Firewall-Kunden mit aktuellen Abos erhalten rund um die Uhr Updates zu den aktuellsten Bedrohungen. Die Updates sind sofort wirksam, erfordern keine Neustarts und verursachen keinerlei Unterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer breiten Palette an Bedrohungen. Eine einzige Signatur deckt dabei bis zu mehrere Zehntausend Einzelbedrohungen ab. Zusätzlich zu den Abwehrmechanismen auf der Appliance bieten die SonicWall-Firewalls auch Zugang zum SonicWall CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um derzeit über 17 Millionen Signaturen erweitert. Die Firewall greift über ein proprietäres schlankes Protokoll auf die CloudAV-Datenbank zu, um die Prüfmöglichkeiten auf der Appliance zu erweitern. Dank effizienter Geo-IP- und Botnet-Filter-Funktionen sind die Next-Generation-Firewalls von SonicWall in der Lage, den Verkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren, um die Sicherheitsrisiken im Netzwerk zu reduzieren.

Application-Intelligence und Anwendungskontrolle

Application-Intelligence liefert detaillierte Informationen zum Anwendungsverkehr im Netzwerk. Administratoren haben so die Möglichkeit, die Anwendungskontrolle entsprechend den geschäftlichen Prioritäten zu steuern und zu planen, unproduktive Anwendungen einzuschränken und potenziell gefährliche Anwendungen zu blockieren. Auffälligkeiten im Datenverkehr werden mittels Echtzeitvisualisierung augenblicklich identifiziert. So können unverzüglich Gegenmaßnahmen eingeleitet werden, um das Netzwerk vor potenziellen ein- oder ausgehenden Angriffen zu schützen oder Performance-Engpässe zu verhindern. SonicWall Application Traffic Analytics liefert detaillierte Informationen zum Anwendungsverkehr, zur Bandbreitennutzung sowie zu Sicherheitsbedrohungen und bietet leistungsstarke Troubleshooting- und Forensik-Funktionen. Zusätzlich verbessern sichere Funktionen für die einmalige Anmeldung (Single-Sign-on, SSO) die Benutzererfahrung und Produktivität und reduzieren die Anzahl an Supportanfragen. Eine intuitive webbasierte Oberfläche vereinfacht die Verwaltung der Application-Intelligence- und Anwendungskontrollfunktionen.



Flexible und sichere Wireless-Konnektivität

Die Next-Generation-Firewall-Technologie von SonicWall lässt sich optional mit Highspeed-802.11ac-Wireless-Konnektivität* kombinieren. So entsteht eine Wireless-Netzwerksicherheitslösung, die kabelgebundenen und drahtlosen Netzwerken umfassenden Schutz bietet.

Dank dieser Wireless-Performance der Enterprise-Klasse lassen sich Wi-Fi-fähige Geräte über größere Entfernungen anbinden und bandbreitenintensive mobile Anwendungen wie beispielsweise Video- und Voice-Apps auch in Umgebungen mit höherer Dichte ohne Verschlechterung der Signalqualität ausführen.

** 802.11ac ist aktuell nicht für die SOHO-Modelle verfügbar; die SOHO-Modelle unterstützen 802.11a/b/g/n.*

Funktionen

RFDPI-Engine	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection	Diese hochleistungsfähige, proprietäre und patentierte Prüf-Engine führt eine streambasierte bidirektionale Verkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Der ein- und ausgehende Datenverkehr wird gleichzeitig auf Bedrohungen geprüft, um zu verhindern, dass ein infizierter Computer das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe nutzt.
Single-Pass-Inspection	Eine Single-Pass-DPI-Architektur prüft den Verkehr auf Malware und Eindringversuche und sorgt gleichzeitig für die Erkennung von Anwendungen. Dadurch werden DPI-bedingte Latenzzeiten drastisch verkürzt. Außerdem wird sichergestellt, dass sämtliche Informationen zu Bedrohungen innerhalb einer einheitlichen Architektur verarbeitet werden.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxys stattfindet, können für mehrere Datenströme gleichzeitig leistungsstarke Deep Packet Inspection-Prüfungen durchgeführt werden – bei minimalen Latenzzeiten und ohne Einschränkungen bei Datenvolumen oder Dateigrößen. Dies funktioniert sowohl bei gängigen Protokollen als auch bei Raw-TCP-Streams.
Deep Packet Inspection of Secure Socket Shell (DPI-SSH)	Diese Funktion erkennt und verhindert raffinierte verschlüsselte Angriffe, die SSH nutzen, blockiert verschlüsselte Malware-Downloads und verhindert die Verbreitung von Bedrohungen, Command-and-Control-Kommunikationen und das Herausschleusen von Daten.
Capture Advanced Threat Protection	
Funktion	Beschreibung
Multi-Engine-Sandbox	Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht bösartige Aktivitäten transparent.
Analyse unterschiedlichster Dateitypen	Der Service unterstützt die Analyse unterschiedlichster Dateitypen, darunter ausführbare Programme (PE), DLL, PDFs, MS Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme wie Windows, Android, Mac OSX und Multi-Browser-Umgebungen.
Schnelle Implementierung von Signaturen	Wird eine Datei als bösartig identifiziert, so wird innerhalb von 48 Stunden eine Signatur auf Firewalls mit SonicWall Capture-Abos aufgespielt und in die GRID-Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt.
Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus	Um zu verhindern, dass potenziell bösartige Dateien in das Netzwerk eindringen, können die zur Analyse in die Cloud gesendeten Dateien am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist.
Schutz vor verschlüsselten Bedrohungen	
Funktion	Beschreibung
TLS-/SSL-Entschlüsselung und -Prüfung	Blitzschnelle, proxylose Entschlüsselung und Prüfung von SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im TLS-/SSL-verschlüsselten Verkehr lauern. Dieser Service ist bei allen Modellen außer der SOHO in den Sicherheitsabos inbegriffen. Für die SOHO ist er in Form einer separaten Lizenz verfügbar.
SSH-Prüfung	Durch die Deep Packet Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen.
Intrusion-Prevention	
Funktion	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion-Prevention-System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signatur-Updates	Das SonicWall Threat Research-Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Verbesserter Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion-Prevention. Dies verhindert, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten.
Erkennen und Blockieren von Command-and-Control(CnC)-Aktivitäten durch Botnets	Erkennen und Blockieren von Command-and-Control-Verkehr, der von Bots im lokalen Netzwerk ausgeht und an IPs und Domänen geleitet wird, die nachweislich Malware verbreiten oder bekannte CnC-Punkte sind.
Protokollmissbrauch/-anomalien	Erkennen und Verhindern von Angriffen, die Protokolle missbrauchen, um unbemerkt am IPS vorbeizukommen.
Zero-Day-Schutz	Ständige Updates zu den neuesten Exploit-Techniken und -Methoden decken Tausende verschiedener Exploits ab und schützen das Netzwerk vor Zero-Day-Angriffen.
Umgehungsschutz	Umfassende Normalisierungs- und Entschlüsselungsmethoden sowie weitere Maßnahmen verhindern, dass Bedrohungen Umgehungstechniken auf den Schichten 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.
Bedrohungsschutz	
Funktion	Beschreibung
Malware-Schutz am Gateway	Die RFDPI-Engine prüft den gesamten Verkehr auf Viren, Trojaner, Keylogger und andere Malware in Dateien unbegrenzter Größe und über alle Ports und TCP-Streams hinweg. Die Prüfung erfolgt sowohl in ein- als auch ausgehender Richtung sowie innerhalb von Zonen.

Bedrohungsschutz (Fortsetzung)	
Funktion	Beschreibung
CloudAV-Malware-Schutz	Eine kontinuierlich aktualisierte Datenbank mit über 17 Millionen Bedrohungssignaturen auf den SonicWall-Cloud-Servern ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Engine eine größtmögliche Anzahl an Bedrohungen abdeckt.
Sicherheitsupdates rund um die Uhr	Neue Updates zu Bedrohungen werden automatisch an Firewalls vor Ort mit aktivierten Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne dass Neustarts nötig sind oder andere Unterbrechungen verursacht werden.
SSL-Entschlüsselung und -Prüfung	SSL-Datenverkehr wird in Echtzeit und ohne Umweg über einen Proxy entschlüsselt und auf Malware, Eindringversuche und Datenlecks überprüft. Gleichzeitig werden Richtlinien für Anwendungs-, URL- und Inhaltskontrolle angewendet, um das Netzwerk gegen versteckte Bedrohungen in SSL-verschlüsseltem Datenverkehr abzusichern. Dieser Service ist bei allen Modellen außer der SOHO in den Sicherheitsabos inbegriffen. Für die SOHO ist er in Form einer separaten Lizenz verfügbar.
Bidirektionale Raw-TCP-Prüfung	Die RFDPI-Engine ist in der Lage, Raw-TCP-Streams bidirektional auf sämtlichen Ports zu prüfen. So lassen sich Angriffe verhindern, bei denen veraltete Sicherheitssysteme umgangen werden, die sich lediglich auf ein paar bekannte Ports konzentrieren.
Unterstützung zahlreicher Protokolle	Identifizierung gängiger Protokolle wie HTTP/S, FTP, SMTP, SMBv1/v2 und andere, bei denen Daten nicht in Raw-TCP-Paketen gesendet werden. Payloads werden für die Malware-Prüfung entschlüsselt, auch wenn sie keine bekannten Standardports nutzen.
Application-Intelligence und Anwendungskontrolle	
Funktion	Beschreibung
Anwendungskontrolle	Die RFDPI-Engine nutzt eine kontinuierlich erweiterte Datenbank mit über 3.500 Anwendungssignaturen, um Anwendungen oder einzelne Anwendungsfunktionen zu identifizieren und zu kontrollieren. Dadurch lassen sich Netzwerksicherheit und -produktivität erhöhen.
Identifizierung benutzerdefinierter Anwendungen	Die Lösung erstellt Signaturen auf der Grundlage bestimmter Parameter oder Muster, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen. So lassen sich benutzerdefinierte Anwendungen kontrollieren und eine erweiterte Kontrolle über das Netzwerk erreichen.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenkapazität kann für kritische Anwendungen oder Anwendungskategorien granular zugewiesen und reguliert werden. Gleichzeitig lässt sich jedweder nicht notwendiger Anwendungsverkehr unterbinden.
Granulare Kontrolle	Kontrolle von Anwendungen oder bestimmten Anwendungskomponenten auf der Grundlage von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten mit voller SSO-Benutzeridentifizierung durch LDAP-/AD-/Terminaldienst-/Citrix-Integration.
Content-Filtering	
Funktion	Beschreibung
Internes/Externes Content-Filtering	Über den Content Filtering Service lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und Websites mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren. Mit dem Content Filtering Client kann die Richtliniendurchsetzung zudem erweitert werden, um Internetinhalte auch auf Geräten außerhalb der Firewallgrenze zu blockieren.
Gezielte Kontrollmöglichkeiten	Inhalte lassen sich auf Basis der bereits vordefinierten Kategorien oder einer beliebigen Kombination an Kategorien blockieren. Die Filter können für eine bestimmte Tageszeit aktiviert werden, z. B. während Unterrichts- oder Geschäftszeiten, und auf einzelne Benutzer oder Gruppen beschränkt werden.
YouTube für Schulen	Lehrkräften stehen auf YouTube EDU Hunderttausende kostenlose Lernvideos zur Verfügung, die nach Themen und Bildungsstufe sortiert sind und allgemeinen Unterrichtsstandards entsprechen.
Web-Caching	URL-Bewertungen werden lokal auf der SonicWall-Firewall zwischengespeichert, sodass jeder weitere Zugriff auf häufig besuchte Websites nur den Bruchteil einer Sekunde dauert.
Durchsetzung von Viren- und Spyware-Schutz	
Funktion	Beschreibung
Mehrstufiger Schutz	Die Firewall ist die erste Verteidigungsstufe am Netzwerkrand. Zusammen mit dem Endpunktschutz verhindert sie das Eindringen von Viren über Laptops, USB-Sticks und andere ungeschützte Systeme.
Option für automatisierte Durchsetzung	Es wird sichergestellt, dass auf jedem Computer, der auf das Netzwerk zugreift, die neueste Version der Signaturen für Viren- und Spyware-Schutz installiert und aktiviert ist. Somit entfallen die Kosten, die typischerweise für die Verwaltung von Desktop-Lösungen für Viren- und Spyware-Schutz entstehen.
Option für automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz werden automatisch und netzwerkweit auf jedem Rechner installiert und bereitgestellt, sodass der administrative Mehraufwand minimiert wird.
Ständig aktiver, automatischer Virenschutz	Der Viren- und Spyware-Schutz wird häufig aktualisiert und transparent auf allen Desktop-PCs und Dateiservern bereitgestellt. Das sorgt für höhere Endbenutzerproduktivität und reduziert den Aufwand für die Sicherheitsverwaltung.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt den eingehenden Verkehr und blockiert die Installation zahlreicher Spyware-Programme auf Desktop-PCs und Laptops, bevor vertrauliche Daten übertragen werden können. Auf diese Weise werden die Sicherheit und die Performance von Desktops erhöht.

Firewall und Networking	
Funktion	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall-Zugriffsregeln erfüllt werden.
Schutz vor DDoS-/DoS-Angriffen	Dank SYN-Flood-Schutz lassen sich DoS-Angriffe mit Layer-3-SYN-Proxy- und Layer-2-SYN-Blacklisting-Technologien abwehren. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
Flexible Implementierungsoptionen	Die SonicWall TZ Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
IPv6-Unterstützung	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) hat gerade erst begonnen. Mit der neuesten SonicOS-Version unterstützt die Hardware die Implementierung von Filterfunktionen.
Biometrische Authentifizierung für den Remote-Zugriff	Unterstützung von Authentifizierungsmethoden für Mobilgeräte, bei denen eine Duplizierung oder Weitergabe nicht ohne Weiteres möglich ist, wie z. B. bei der Fingerabdruckerkennung. So lässt sich die Identität des Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird.
Integration von Switches der X-Series	Verwaltung der Sicherheitseinstellungen zusätzlicher Ports (einschließlich POE und POE+) über eine einzige Konsole mithilfe des TZ-Dashboards mit X-Switch (nicht für das SOHO-Modell verfügbar)
Hochverfügbarkeit	Die SonicWall TZ500- und SonicWall TZ600-Modelle unterstützen Hochverfügbarkeit mit Active/Standby und State-Synchronisierung. Die SonicWall TZ300- und SonicWall TZ400-Modelle unterstützen Hochverfügbarkeit ohne Active-/Standby-Synchronisierung. Auf den SonicWall SOHO-Modellen wird Hochverfügbarkeit nicht unterstützt.
API gegen Bedrohungen	Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Auf diese Weise kann sie raffinierte Bedrohungen wie Zero-Day-Angriffe, Insider-Bedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv bekämpfen.
Sicherheit für Wireless-Netzwerke	Die Wireless-Technologie nach dem IEEE 802.11ac-Standard stellt einen Wireless-Durchsatz von bis zu 1,3 GBit/s mit größerer Signalreichweite und höherer Zuverlässigkeit bereit. Sie ist für die SonicWall-Modelle TZ600 bis TZ300 verfügbar. Auf den SonicWall SOHO-Modellen ist optional 802.11a/b/g/n verfügbar.
Management und Reporting	
Funktion	Beschreibung
Global Management System	Das SonicWall GMS ermöglicht es, über eine einzige Verwaltungsschnittstelle mit intuitiver Oberfläche mehrere SonicWall-Appliances und Switches der X-Series zu überwachen und zu konfigurieren und Berichte darüber zu erstellen. Dies reduziert nicht nur die Kosten, sondern auch die Komplexität bei der Verwaltung.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive, webbasierte Oberfläche ermöglicht eine schnelle und bequeme Konfiguration. Die Lösung stellt Ihnen außerdem eine umfassende Befehlsschnittstelle zur Verfügung und unterstützt SNMPv2/3.
Berichte zum IPFIX-/NetFlow-Datenstrom	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Unterstützt wird auch die Berichterstellung mit Tools wie SonicWall GMSFlow-Server oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.
Virtual Private Networking	
Funktion	Beschreibung
Auto-Provisioning für VPNs	Durch Automatisierung der Site-to-Site-VPN-Gateway-Erstausstattung zwischen den SonicWall-Firewalls ist die Implementierung komplexer verteilter Firewalls ein Kinderspiel. Funktionen für Sicherheit und Konnektivität werden umgehend und automatisch ausgeführt.
IPSec-VPN für Site-to-Site-Konnektivität	Dank eines hochleistungsfähigen IPSec-VPNs kann die SonicWall TZ Series als VPN-Konzentrator für Tausende anderer großer Standorte, Zweigstellen oder Heimbüros genutzt werden.
Remote-Zugriff per SSL-VPN- oder IPSec-Client	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mails, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.
Redundantes VPN-Gateway	Mit mehreren WANs lässt sich ein primäres und sekundäres VPN konfigurieren, um ein einfaches automatisches Failover und Failback für alle VPN-Sitzungen zu ermöglichen.
Routenbasiertes VPN	Bei Ausfall eines temporären VPN-Tunnels wird der Datenverkehr reibungslos über alternative Verbindungen zwischen Endgeräten umgeleitet. Dieses dynamische Routing über VPN-Links sorgt für eine hohe Ausfallsicherheit.
Content- bzw. kontextorientierte Sicherheitsfunktionen	
Funktion	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Dank nahtloser SSO-Integration von AD-/LDAP-/Citrix1-/Terminaldiensten und umfassenden DPI-Daten können Benutzer identifiziert und Benutzeraktivitäten nachverfolgt werden.
Identifizierung des Datenverkehrs nach Ländern mittels Geo-IP	Identifizierung und Kontrolle des Netzwerkverkehrs aus oder in bestimmte Länder. Schützt das Netzwerk vor Angriffen bzw. Sicherheitsbedrohungen bekannten oder verdächtigen Ursprungs. Zudem kann verdächtiger Verkehr, der vom Netzwerk ausgeht, analysiert werden.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern.

Die SonicOS-Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- API gegen Bedrohungen

SSL-/SSH-Entschlüsselung und -Prüfung[1]

- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Kontrolle

Capture Advanced Threat Protection[1]

- Cloud-basierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Übermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Automatische Blockierung

Intrusion-Prevention[1]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granulare IPS-Regeln
- GeoIP-/Botnet-Filtering[2]
- Abgleich regulärer Ausdrücke

Malware-Schutz[1]

- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloud-basierte Malware-Datenbank

Anwendungsidentifizierung[1]

- Anwendungskontrolle
- Anwendungsvisualisierung[2]
- Blockieren von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Nachverfolgung der Benutzeraktivitäten (SSO)
- Umfassende Anwendungs-signaturendatenbank

Filterung von Webinhalten[1]

- URL-Filtering
- Anti-Proxy-Technologie
- Blockieren mithilfe von Schlüsselwörtern
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN

- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (OSPF, RIP)

Networking

- PortShield
- Erweiterte Protokollierung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing
- SonicPoint Wireless Controller
- Regelbasiertes Routing
- Asymmetrisches Routing
- DHCP-Server
- NAT
- Bandbreitenverwaltung
- Hochverfügbarkeit – Active/Standby mit State-Sync[3]
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge-Modus, NAT-Modus
- 3G-/4G-WAN-Failover
- Common Access Card(CAC)-Unterstützung

VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Support

Verwaltung und Überwachung

- Web-Oberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mit SonicWall GMS
- Logging
- NetFlow-/IPFIX-Export
- Single-Sign-on (SSO)
- Unterstützung für Terminaldienste/Citrix
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- Dell X-Series-Switch-Verwaltung

IPv6

- IPv6-Filterung
- 6rd (schnelle Bereitstellung)
- DHCP-Präfixdelegierung
- BGP

Wireless

- Dualband (2,4 GHz und 5 GHz)
- 802.11 a/b/g/n/ac-Wireless-Standards[2]
- Erkennung und Vermeidung von Wireless-Angriffen
- Wireless Guest Services
- Lightweight Hotspot Messaging
- Segmentierung mithilfe virtueller Access-Points
- Captive Portal
- Cloud-Zugriffssteuerungsliste

[1] Erfordert zusätzliches Abo.
[2] Nicht für die SOHO Series verfügbar.
[3] Hochverfügbarkeit mit State-Sync nur für die Modelle SonicWall TZ500 und SonicWall TZ600 erhältlich.

SonicWall TZ Series – Systemdaten

Hardware	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
Betriebssystem	SonicOS				
Security-Prozessor-Cores	2 x 400 MHz / 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1,4 GHz
Schnittstellen	5x 1-GbE, 1 USB, 1 Konsole	5x 1-GbE, 1 USB, 1 Konsole	7x 1-GbE, 1 USB, 1 Konsole	8x 1-GbE, 2 USB, 1 Konsole	10x 1-GbE, 2 USB, 1 Konsole, 1 Erweiterungssteckplatz
Speicher (RAM)	512 MB/1GB	1 GB	1 GB	1 GB	1 GB
Flash-Speicher	32 MB/64 MB	64 MB	64 MB	64 MB	64 MB
Erweiterung	USB	USB	USB	2 USB	Erweiterungssteckplatz (Rückseite)*, 2 USB
Single-Sign-on(SSO)-Benutzer	250	500	500	500	500
VLAN-Schnittstellen	25	25	50	50	50
Unterstützte SonicPoints (max.)	2	8	16	16	24
Unterstützung für Switch-Modelle der X-Series	Nicht verfügbar	X1008/P, X1018/P, X1026/P, X1052/P, X4012			
Firewall-/VPN-Performance	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Firewall-Inspection-Durchsatz[1]	300 MBit/s	750 MBit/s	1.300 MBit/s	1.400 MBit/s	1.500 MBit/s
Full-DPI-Durchsatz[2]	50 MBit/s	100 MBit/s	300 MBit/s	400 MBit/s	500 MBit/s
Application-Inspection-Durchsatz[2]	-	300 MBit/s	900 MBit/s	1.000 MBit/s	1.100 MBit/s
IPS-Durchsatz[2]	100 MBit/s	300 MBit/s	900 MBit/s	1.000 MBit/s	1.100 MBit/s
Anti-Malware-Inspection-Durchsatz[2]	50 MBit/s	100 MBit/s	300 MBit/s	400 MBit/s	500 MBit/s
IMIX-Durchsatz[3]	60 MBit/s	200 MBit/s	500 MBit/s	700 MBit/s	900 MBit/s
Durchsatz bei SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	15 MBit/s	45 MBit/s	100 MBit/s	150 MBit/s	200 MBit/s
IPSec-VPN-Durchsatz[3]	100 MBit/s	300 MBit/s	900 MBit/s	1.000 MBit/s	1.100 MBit/s
Verbindungen pro Sekunde	1.800	5.000	6.000	8.000	12.000
Maximale Anzahl von Verbindungen (SPI)	10.000	50.000	100.000	125.000	150.000
Maximale Anzahl von Verbindungen (DPI)	10.000	50.000	90.000	100.000	125.000
Maximale Anzahl von Verbindungen (DPI SSL)	100	500	500	750	750
VPN	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Site-to-Site-VPN-Tunnel	10	10	20	25	50
IPSec-VPN-Clients (max.)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL-VPN-Lizenzen (max.)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Gebündelt mit Virtual Assist (max.)	-	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit), MD5, SHA-1, Suite B Cryptography				
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14				
Routenbasiertes VPN	RIP, OSPF				
Unterstützte Zertifikate	Verisign, Thawte, Cybertrust, RSA Keon, Entrust und Microsoft CA für SonicWall-to-SonicWall-VPN, SCEP				
VPN-Funktionen	Dead Peer Detection, DHCP über VPN, IPSec NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN				
Unterstützte globale VPN-Client-Plattformen	Microsoft® Windows Vista (32/64 Bit), Windows 7 (32/64 Bit), Windows 8.0 (32/64 Bit), Windows 8.1 (32/64 Bit), Windows 10				
NetExtender	Microsoft Windows Vista (32/64 Bit), Windows 7, Windows 8.0 (32/64 Bit), Windows 8.1 (32/64 Bit), Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE				
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)				
Sicherheitsservices	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Deep Packet Inspection-Services	Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention, DPI-SSL				
Content Filtering Service (CFS)	Prüfung nach HTTP-URL, HTTPS-IP, Schlüsselwörtern und Inhalt, umfassende Filterung anhand von Dateitypen wie ActiveX, Java, Cookies für Datenschutz, Freigabe- und Sperrlisten				
Enforced Client Anti-Virus and Anti-Spyware	McAfee®				
Comprehensive Anti-Spam Service	unterstützt				
Anwendungsvisualisierung	Nein	Ja	Ja	Ja	Ja
Anwendungskontrolle	Ja	Ja	Ja	Ja	Ja
Capture Advanced Threat Protection	Nein	Ja	Ja	Ja	Ja

SONICWALL™

SonicWall TZ Series – Systemdaten (Fortsetzung)

Networking	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus				
Routing-Protokolle[4]	BGP[4], OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing, Multicast				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)				
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix			
Lokale Benutzerdatenbank	150			250	
VoIP	Volle Unterstützung für H.323v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Zertifikate	FIPS 140-2 (mit Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus				
Zertifikate (ausstehend)	Common Criteria NDPP				
Common Access Card (CAC)	unterstützt				
Hochverfügbarkeit	Nein	Active/Standby	Active/Standby	Active/Standby mit Stateful-Synchronisierung	Active/Standby mit Stateful-Synchronisierung
Hardware	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Formfaktor	Desktop				
Stromversorgung (W)	24 W (extern)	24 W (extern)	24 W (extern)	36 W (extern)	60 W (extern)
Maximaler Stromverbrauch (W)	6,4/11,3	6,9/12,0	9,2/13,8	13,4/17,7	16,1
Eingangsspannung	100–240 VAC, 50–60 Hz, 1 A				
Gesamtwärmeabgabe	21,8/38,7 BTU	23,5/40,9 BTU	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Abmessungen	3,6 x 14,1 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Gewicht	0,34 kg 0,48 kg	0,73 kg 0,84 kg	0,73 kg 0,84 kg	0,92 kg 1,05 kg	1,47 kg
WEEE-Gewicht	0,80 kg 0,94 kg	1,15 kg 1,26 kg	1,15 kg 1,26 kg	1,34 kg 1,48 kg	1,89 kg
Versandgewicht	1,2 kg 1,34 kg	1,37 kg 1,48 kg	1,37 kg 1,48 kg	1,93 kg 2,07 kg	2,48 kg
MTBF (Jahre)	58,9/56,1 (Wireless)	56,1	54,0	40,8	18,4
Umgebungstemperatur	0–40 °C				
Luftfeuchtigkeit	5–95 %, nicht kondensierend				
Richtlinien	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600**
Vorschriftenmodell (kabelgebunden)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Einhaltung wichtiger gesetzlicher Vorschriften (kabelgebundene Modelle)	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, BSMI, KCC/MSIP	FCC Klasse A, ICES Klasse A, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse A, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP
Vorschriftenmodell (drahtlos)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	-
Einhaltung wichtiger gesetzlicher Vorschriften (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	-

SonicWall TZ Series – Systemdaten (Fortsetzung)

Integrierte Wireless-Optionen	SOHO Series	TZ300, TZ400, TZ500 Series	TZ600
Standards	802.11 a/b/g/n	802.11a/b/g/n/ac (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS)	-
Frequenzbänder[5]	802.11a: 5,180–5,825 GHz; 802.11b/g: 2,412–2,472 GHz; 802.11n: 2,412–2,472 GHz, 5,180 bis 5,825 GHz	802.11a: 5,180–5,825 GHz; 802.11b/g: 2,412–2,472 GHz; 802.11n: 2,412–2,472 GHz, 5,180–5,825 GHz; 802.11ac: 2,412–2,472 GHz, 5,180–5,825 GHz	-
Verwendete Kanäle	802.11a: USA und Kanada 12, Europa 11, Japan 4, Singapur 4, Taiwan 4; 802.11b/g: USA und Kanada 1–11, Europa 1–13, Japan 1–14 (Kanal 14 nur nach 802.11b-Standard); 802.11n (2,4 GHz): USA und Kanada 1–11, Europa 1–13, Japan 1–13; 802.11n (5 GHz): USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64	802.11a: USA und Kanada 12, Europa 11, Japan 4, Singapur 4, Taiwan 4; 802.11b/g: USA und Kanada 1–11, Europa 1–13, Japan 1–14 (Kanal 14 nur nach 802.11b-Standard); 802.11n (2,4 GHz): USA und Kanada 1–11, Europa 1–13, Japan 1–13; 802.11n (5 GHz): USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64; 802.11ac: USA und Kanada 36–48/149–165, Europa 36–48, Japan 36–48, Spanien 36–48/52–64	-
Sendeleistung	Basierend auf dem vom Systemadministrator angegebenen Geltungsbereich	Basierend auf dem vom Systemadministrator angegebenen Geltungsbereich	-
Steuerung der Sendeleistung	unterstützt	unterstützt	-
Unterstützte Datenübertragungsraten	802.11a: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 802.11b: 1, 2, 5,5 und 11 MBit/s pro Kanal; 802.11g: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135 und 150 MBit/s pro Kanal	802.11a: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 802.11b: 1, 2, 5,5 und 11 MBit/s pro Kanal; 802.11g: 6, 9, 12, 18, 24, 36, 48 und 54 MBit/s pro Kanal; 802.11n: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 15, 30, 45, 60, 90, 120, 135 und 150 MBit/s pro Kanal; 802.11ac: 7,2, 14,4, 21,7, 28,9, 43,3, 57,8, 65, 72,2, 86,7, 96,3, 15, 30, 45, 60, 90, 120, 135, 150, 180, 200, 32,5, 65, 97,5, 130, 195, 260, 292,5, 325, 390, 433,3, 65, 130, 195, 260, 390, 520, 585, 650, 780 und 866,7 MBit/s pro Kanal	-
Modulations-technologie/ Frequenzspreizung	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM)	802.11a: Orthogonal Frequency Division Multiplexing (OFDM); 802.11b: Direct Sequence Spread Spectrum (DSSS); 802.11g: Orthogonal Frequency Division Multiplexing (OFDM)/Direct Sequence Spread Spectrum (DSSS); 802.11n: Orthogonal Frequency Division Multiplexing (OFDM); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	-

**Für künftige Anwendung.*

[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren.

[2] Der Full-DPI-/GatewayAV-/Anti-Spyware-/IPS-Durchsatz wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia Testtools nach Branchenstandard gemessen. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren.

[3] Der VPN-Durchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.

[4] BGP ist nur für die SonicWall TZ400, TZ500 und TZ600 verfügbar.

[5] Alle TZ-Modelle mit integrierten Wireless-Optionen unterstützen entweder das 2,4-GHz- oder 5-GHz-Band. Wenn Sie eine Dual-Band-Unterstützung wünschen, nutzen Sie bitte die Wireless-Access-Point-Produkte von SonicWall (SonicPoints).

SonicWall TZ Series – Bestellinformationen

Produkt	Artikelnummer
SonicWall SOHO mit TotalSecure (1 Jahr)	01-SSC-0651
SonicWall SOHO Wireless-N mit TotalSecure (1 Jahr)	01-SSC-0653
SonicWall TZ300 mit TotalSecure (1 Jahr)	01-SSC-0581
SonicWall TZ300 Wireless-AC mit TotalSecure (1 Jahr)	01-SSC-0583
SonicWall TZ400 mit TotalSecure (1 Jahr)	01-SSC-0514
SonicWall TZ400 Wireless-AC mit TotalSecure (1 Jahr)	01-SSC-0516
SonicWall TZ500 mit TotalSecure (1 Jahr)	01-SSC-0445
SonicWall TZ500 Wireless-AC mit TotalSecure (1 Jahr)	01-SSC-0446
SonicWall TZ600 mit TotalSecure (1 Jahr)	01-SSC-0219
Optionen für Hochverfügbarkeit (nur Geräte gleichen Modells)	
SonicWall TZ500 High Availability	01-SSC-0439
SonicWall TZ600 High Availability	01-SSC-0220

SonicWall TZ Series – Bestellinformationen (Fortsetzung)

Dienstleistungen	Artikelnummer
Für SonicWall SOHO	
Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0670
Content Filtering Service (1 Jahr)	01-SSC-0676
Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0682
24/7-Support 1 (Jahr)	01-SSC-0700
Für SonicWall TZ300	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für TZ300 (1 Jahr)	01-SSC-1430
Capture Advanced Threat Protection für TZ300 (1 Jahr)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0602
Content Filtering Service (1 Jahr)	01-SSC-0608
Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0632
24/7-Support 1 (Jahr)	01-SSC-0620
Für SonicWall TZ400	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für TZ400 (1 Jahr)	01-SSC-1440
Capture Advanced Threat Protection für TZ400 (1 Jahr)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0534
Content Filtering Service (1 Jahr)	01-SSC-0540
Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0561
24/7-Support 1 (Jahr)	01-SSC-0552
Für SonicWall TZ500	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für TZ500 (1 Jahr)	01-SSC-1450
Capture Advanced Threat Protection für TZ500 (1 Jahr)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0458
Content Filtering Service (1 Jahr)	01-SSC-0464
Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0482
24/7-Support 1 (Jahr)	01-SSC-0476
Für SonicWall TZ600	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering und 24/7-Support für TZ600 (1 Jahr)	01-SSC-1460
Capture Advanced Threat Protection für TZ600 (1 Jahr)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0228
Content Filtering Service (1 Jahr)	01-SSC-0234
Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0252
24/7-Support 1 (Jahr)	01-SSC-0246

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-SonicWall-TZ Series-US-VG-27321

SONICWALL™