SONICWALL

SonicWall TZ Series

Integrierter Bedrohungsschutz und SD-Plattform für kleine bis mittelständische sowie große verteilte Konzerne

Die SonicWall TZ Series bietet kleinen bis mittelständischen und regional verteilten Unternehmen die Vorteile einer integrierten Sicherheitslösung, die sämtliche Kriterien erfüllt. Mit ihrer ultraschnellen Threat-Prevention- und Software-defined-Wide-Area-Networking (SD-WAN)-Technologie, der breiten Palette an Netzwerk- und Wireless-Features, der vereinfachten Implementierung und der zentralisierten Verwaltung bietet die TZ Series eine konsolidierte Sicherheitslösung mit geringen Gesamtbetriebskosten.

Flexible, integrierte Sicherheitslösung

Herzstück der TZ Series ist SonicOS, das funktionsreiche Betriebssystem von SonicWall. Firewalls, die das neue SonicOS 7.0 OS Betriebssystem unterstützen, bieten eine Benutzeroberfläche mit modernem UI-/UX-Design, erweiterte Sicherheits- und Netzwerkfunktionen sowie ein vereinfachtes Richtlinienmanagement.

SonicOS umfasst zudem leistungsstarke Funktionen, mit denen Organisationen ihre Unified Threat Management (UTM)-Firewalls flexibel an ihre Netzwerkanforderungen anpassen können. Ein integrierter drahtloser Controller, der die IEEE-802.11-Standards unterstützt, und unsere SonicWave-802.11ac-Wave-2-Access-Points erleichtern die Erstellung eines sicheren drahtlosen Highspeed-Netzwerks. Die TZ300P, TZ600P und TZ570P bieten PoE/PoE+ und reduzieren somit die Kosten und die Komplexität, die bei der Verbindung von Highspeed-Wireless-Access-Points und anderen Power-over-Ethernet (PoE)-fähigen Geräten wie IP-Kameras, Telefonen und Druckern entstehen.

Verteilte Einzelhandelsunternehmen und Campus-Umgebungen profitieren von den Vorteilen der zahlreichen Tools in SonicOS. Zweigniederlassungen können mithilfe von Virtual Private Networking (VPN) auf sichere Weise Informationen mit der Zentrale austauschen. Virtuelle LANs (VLANs) ermöglichen die Segmentierung des Netzwerks in separate Unternehmens- und Kundengruppen mithilfe von Regeln, die das Maß an Kommunikation mit Geräten in anderen VLANs bestimmen. SD-WAN bietet eine sichere Alternative zu kostspieligen MPLS-Verbindungen und gewährleistet gleichzeitig eine konstante Anwendungsleistung und Verfügbarkeit. Dank der vollautomatischen Implementierung können TZ-Firewalls spielend leicht per Fernzugriff über die Cloud an entfernten Standorten bereitgestellt werden.

Überragender Bedrohungsschutz und exzellente Performance

Um Netzwerke in einer dynamischen Cyberbedrohungslandschaft zu schützen, setzen wir auf eine automatisierte Echtzeiterkennung und -prävention von Bedrohungen. Durch eine Kombination Cloud-basierter und integrierter Technologien bieten unsere Firewalls hocheffektive Schutzfunktionen, die bereits in unabhängigen Tests bestätigt wurden. Verdächtige Dateien werden zur Analyse an die Cloud-basierte SonicWall Multi-Engine-Sandbox Capture Advanced Threat Protection (ATP) weitergeleitet. Wesentlicher Bestandteil von Capture ATP ist unsere zum Patent angemeldete Real-Time Deep Memory Inspection (RTDMI™)-Technologie. Die RTDMI-Engine erkennt und blockiert Malware und Zero-Day-Bedrohungen, indem sie die Überprüfung direkt im Speicher vornimmt. Die RTDMI-Technologie arbeitet extrem präzise und reduziert die Anzahl von Falschmeldungen auf ein Minimum. Außerdem ist sie in der Lage, ausgeklügelte Angriffe dort zu

Vorteile:

Flexible, integrierte Sicherheitslösung

- Multigigabit-Schnittstellen in einem Desktop-Formfaktor
- Sichere SD-Branch mit SD-WAN
- Leistungsstarkes SonicOS 7.0 Betriebssystem
- Highspeed 802.11ac Wave 2 Wireless-Technologie
- Power over Ethernet (PoE/PoE+)
- 5G-/4G-/LTE-Unterstützung
- Integrierter und erweiterbarer Speicher
- Redundante Stromversorgung

Überragender Bedrohungsschutz und exzellente Performance

- Zum Patent angemeldete Real-Time Deep Memory Inspection-Technologie
- Patentierte Reassembly-Free Deep Packet Inspection-Technologie
- TLS 1.3-Unterstützung
- Effiziente, branchenweit bewährte Sicherheit

Einfache Implementierung, Einrichtung und laufende Verwaltung

- Zero-Touch-Deployment
- Cloud-basierte und lokale zentralisierte Verwaltung
- SonicExpress-App Onboarding

identifizieren und abzuwehren, wo der schädliche Malware-Mechanismus für einen winzigen Augenblick von weniger als 100 Nanosekunden offengelegt wird. Gemeinsam mit unserer patentierten Reassembly-Free Deep Packet Inspection (RFDPI)-Single-Pass-Engine lassen sich jedes einzelne Paket und jedes einzelne Byte durchleuchten. Dabei wird der ein- und ausgehende Datenverkehr direkt in der Firewall auf Bedrohungen geprüft. Neben integrierten Funktionen wie Intrusion Prevention, Anti-Malware und Web-/URL-Filterung nutzt die TZ Series auch Capture ATP mit RTDMI-Technologie in der SonicWall Capture Cloud Plattform, um Malware, Ransomware und andere Bedrohungen am Gateway zu stoppen. Bei mobilen Geräten, die sich außerhalb der Firewallgrenze befinden, wendet SonicWall Capture Client als zusätzliche Schutzschicht hoch entwickelte Threat-Protection-Technologien wie maschinelles Lernen und System-Rollback an. Darüber hinaus lässt sich durch die Installation und Verwaltung vertrauenswürdiger TLS-Zertifikate der verschlüsselte TLS-Verkehr mittels Deep Packet Inspection (DPI-SSL) auf TZ-Firewalls scannen.

Da immer mehr Unternehmen für den Schutz von Websitzungen auf Verschlüsselung setzen, ist es extrem wichtig, dass Firewalls verschlüsselten Datenverkehr auf Bedrohungen überprüfen können. Die TZ-Firewalls bieten einen umfassenden Schutz, weil sie unabhängig von Port oder Protokoll eine vollständige Entschlüsselung und Prüfung von TLS-/SSL- und SSH-verschlüsselten Verbindungen durchführen. Dabei scannt die Firewall den gesamten Verkehr auf Bedrohungen, Zero-Day-Angriffe, Eindringversuche sowie auf die Nichteinhaltung von Protokollen und sogar auf benutzerdefinierte Kriterien. Die Deep Packet Inspection-Engine erkennt und verhindert verborgene kryptografische Angriffe, blockiert verschlüsselte Malware-Downloads und verhindert die Verbreitung von Bedrohungen und Command-and-Control(C&C)-Kommunikationen sowie das Herausschleusen von Daten. Eine umfassende Kontrolle wird durch Ein- und Ausschlussregeln ermöglicht, mit denen sich festlegen lässt, welcher Verkehr entschlüsselt und geprüft werden soll, um bestimmte Compliance-Anforderungen in Organisationen und/oder rechtliche Vorgaben zu erfüllen.

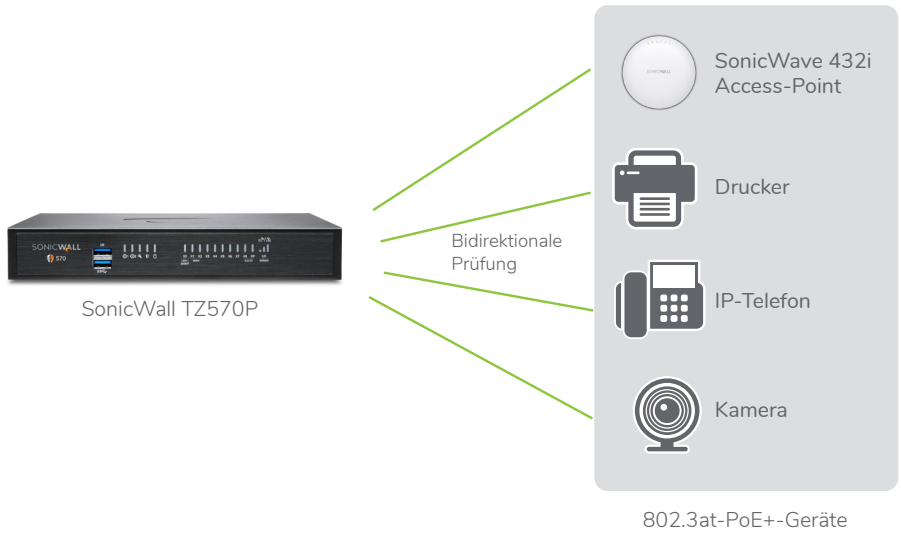
TZ670 und TZ570 bieten TLS 1.3-Unterstützung und mehrere Änderungen verbessern die Performance und Sicherheit bei gleichzeitiger Beseitigung der Komplexität.

Einfache Implementierung, Einrichtung und laufende Verwaltung

Die Konfiguration und Verwaltung von TZ-Firewalls und SonicWave-802.11ac-Wave-2-Access-Points ist ein Kinderspiel – unabhängig vom Implementierungsort. Verwaltung, Reporting, Lizenzierung und Analysen erfolgen zentral über unser Cloud-basiertes Capture Security Center. Dieses bietet die überlegene Transparenz, Flexibilität und Kapazität, die Sie benötigen, um Ihr gesamtes SonicWall-Sicherheitsökosystem zentral zu verwalten.

Eine wichtige Komponente des Capture Security Center ist das Zero-Touch-Deployment für die vollautomatische Implementierung. Dieses Cloud-basierte Feature vereinfacht und beschleunigt die Implementierung und Bereitstellung von Firewalls in Zweigniederlassungen und an entfernten SonicWall-Standorten. Der Prozess erfordert nur minimalen Eingriff durch die Benutzer und ist vollständig automatisiert, sodass eine große Anzahl von Firewalls in wenigen Schritten in Betrieb genommen werden kann. Dadurch werden Zeitaufwand, Kosten und Komplexität der Installation und Konfiguration erheblich reduziert, während Sicherheit und Konnektivität umgehend und automatisch gewährleistet sind. Dank der einfachen Implementierung, Einrichtung und Verwaltung können Organisationen ihre TCO senken und von einem schnellen ROI profitieren.

** 802.11ac ist derzeit für die SOHO/SOHO 250-Modelle nicht verfügbar.Die SOHO/SOHO 250-Modelle unterstützen 802.11a/b/g/n.*



Integrierte Sicherheit und Leistung für Ihre PoE-fähigen Geräte

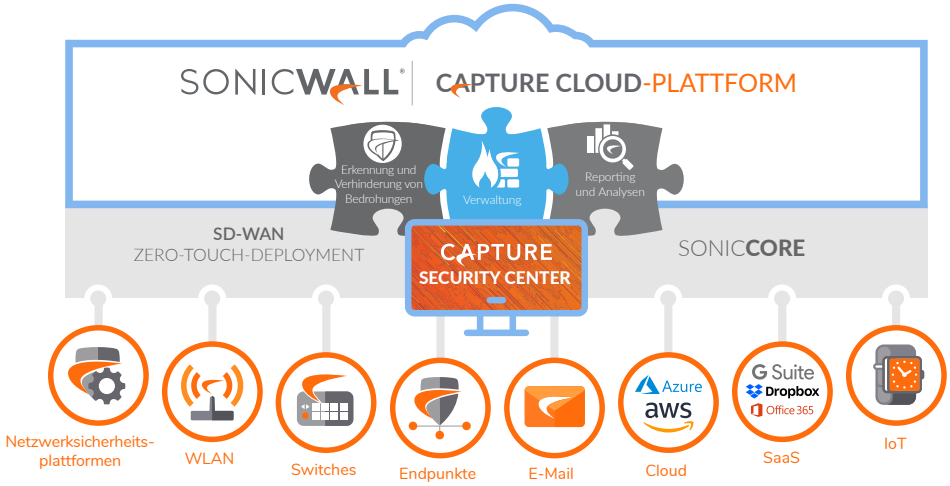
Holen Sie das Maximum aus Ihren PoE-fähigen Geräten heraus – ohne die Kosten und die Komplexität von Power-over-Ethernet-Switches oder -Injectors. TZ300P-, TZ600P- und TZ570P-Firewalls integrieren IEEE-802.3at-Technologie für PoE- und PoE+-Geräte wie Wireless-Access-Points, Kameras, IP-Telefone usw. Die Firewalls durchleuchten den gesamten ein- und ausgehenden Datenverkehr auf sämtlichen Geräten mittels Deep Packet Inspection und beseitigen anschließend gefährliche Bedrohungen wie Malware und Eindringversuche selbst bei verschlüsselten Verbindungen.

Capture Cloud-Plattform

Die Capture Cloud-Plattform von SonicWall bietet kleinen wie großen Organisationen eine Cloud-basierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen. Die Plattform konsolidiert Bedrohungsinformationen aus mehreren Quellen, zum Beispiel aus unserem prämierten Multi-Engine-Netzwerk-Sandboxing-Service Capture Advanced Threat Protection sowie aus über 1 Million SonicWall-Sensoren, die rund um den Globus verteilt sind.

Wird bei eingehenden Daten unbekannter bösartiger Code gefunden, entwickelt das dedizierte interne SonicWall Capture Labs Threat Research-Team Signaturen, die in der Datenbank der Capture Cloud-Plattform gespeichert und in die Kunden-Firewalls implementiert werden, um einen topaktuellen Schutz zu gewährleisten. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen. Die Signaturen auf der Appliance bieten Schutz vor einer großen Vielfalt an Attacken und decken Zehntausende verschiedener Bedrohungen ab. Zusätzlich zu den Abwehrmechanismen auf der Appliance haben die TZ-Firewalls auch einen kontinuierlichen Zugang zur Capture Cloud Plattform-Datenbank. Auf diese Weise wird die lokal verfügbare Signaturendatenbank um mehrere Millionen Signaturen erweitert.

Neben dem effizienten Bedrohungsschutz bietet die Capture Cloud Plattform Administratoren die Möglichkeit, über eine zentrale Stelle spielend leicht Echtzeitberichte und historische Reports zur Netzwerkaktivität zu erstellen.



Schutz vor komplexen Bedrohungen

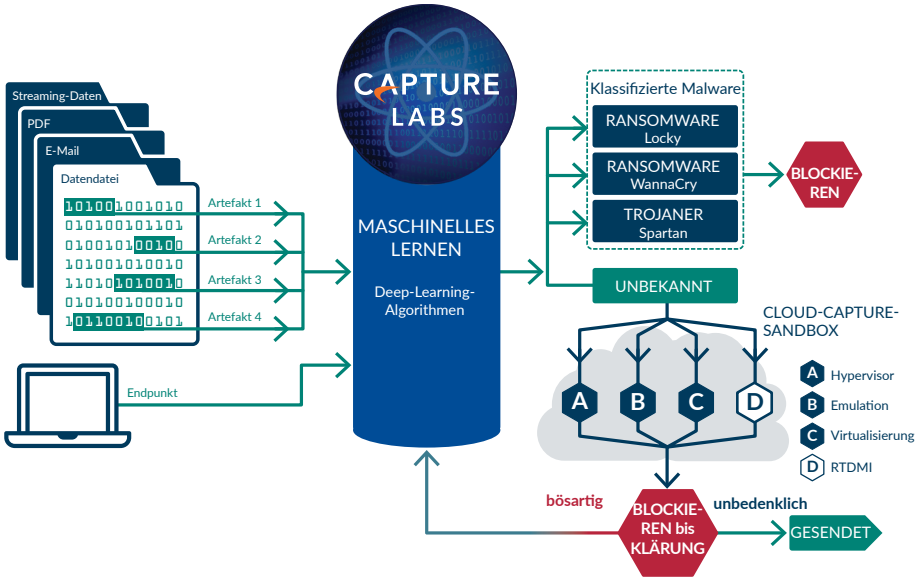
Herzstück der automatisierten SonicWall-Lösung zur Echtzeit-prävention von Sicherheitslücken sind zwei moderne Technologien für die Malware-Erkennung: Capture Advanced Threat Protection™ (Capture ATP) und Capture Security Appliance™ (CSa).

Capture ATP ist eine Cloud-basierte Multi-Engine-Sandbox-Plattform, die Real-Time Deep Memory Inspection™ (RTDMI), virtualisiertes Sandboxing, umfassende Systemsimulation und Analyse auf Hypervisor-Ebene beinhaltet. CSa ist eine On-Prem-Appliance mit RTDMI, die mithilfe von arbeitsspeicherbasierten statischen und dynamischen Verfahren schnellstens genaue Urteile erstellen kann. Beide Lösungen sorgen für einen erweiterten Bedrohungsschutz, indem sie in vielen verschiedenen SonicWall-Lösungen, z. B. in Next-Generation-Firewalls, Zero-Day-Bedrohungen erkennen und verhindern.

Verdächtige Dateien werden zur Analyse mittels Deep-Learning-Algorithmen in eine dieser Lösungen übertragen und können am Gateway gehalten werden, bis der Sicherheitsstatus geklärt ist. Bei Capture ATP werden die als bösartig identifizierten Dateien blockiert und sofort mit Hash-Code in die Capture ATP-Datenbank aufgenommen, damit alle Kunden weitere Angriffe dieser Art erkennen und blockieren können. Letztendlich werden diese Signaturen zur Schaffung einer statischen Abwehr an die Firewalls weitergeleitet. Die von CSa generierten Ergebnisse werden aus Datenschutz- und Compliance-Gründen nicht außerhalb Ihrer Organisation bekanntgegeben.

Dieser Service analysiert ein breites Spektrum an Betriebssystemen sowie zahlreiche Dateitypen, einschließlich ausführbare Programme, DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK.

SonicWall Capture Client sorgt für einen umfassenden Endpunktschutz, indem Antivirentechnologien der nächsten Generation mit der Cloud-basierten Multi-Engine-Sandbox von SonicWall verbunden werden und optional in SonicWall-Firewalls integriert werden können.



Reassembly-Free Deep Packet Inspection-Engine

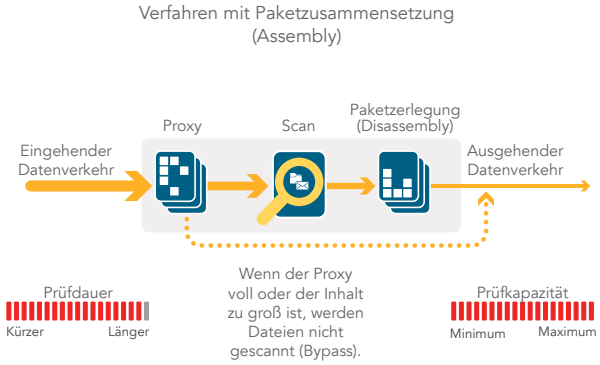
Bei der SonicWall Reassembly-Free Deep Packet Inspection (RFDPI)-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche und Malware-Downloads zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig von Port oder Protokoll und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy. Die proprietäre RFDPI-Engine prüft die Payload von Datenströmen, um Bedrohungen auf den Ebenen 3 bis 7 zu identifizieren.

Zudem wird der Netzwerkverkehr mehrfach umfassend normalisiert und entschlüsselt. Auf diese Weise lassen sich komplexe Umgehungsversuche verhindern, die darauf abzielen, Erkennungsmechanismen zu stören und bösartigen Code unbemerkt in das Netzwerk einzuschleusen.

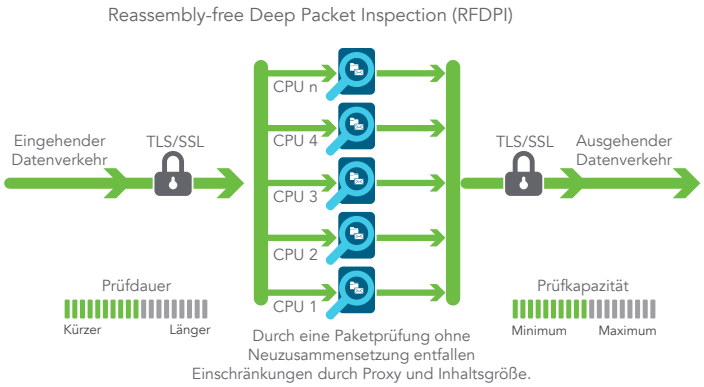
Nachdem ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. TLS-/ SSL-Entschlüsselung), wird es anhand einer einzigen proprietären Speicherdarstellung dreier Signaturendatenbanken analysiert: Eindringversuche, Malware und Anwendungen. Der Verbindungszustand wird ständig auf der Firewall 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.

In den meisten Fällen wird die Verbindung beendet und es werden entsprechende Logging- und Benachrichtigungs-Events erzeugt. Die Engine kann jedoch auch nur für Prüfungen eingerichtet werden oder bei aktivierter Anwendungserkennung kann sie so konfiguriert werden, dass für den restlichen Anwendungsverkehr Layer-7-Bandbreitenverwaltungsdienste bereitgestellt werden, sobald die Anwendung erkannt wird.



Proxybasierte Architektur von Mitbewerberlösungen



Streambasierte SonicWall-Architektur

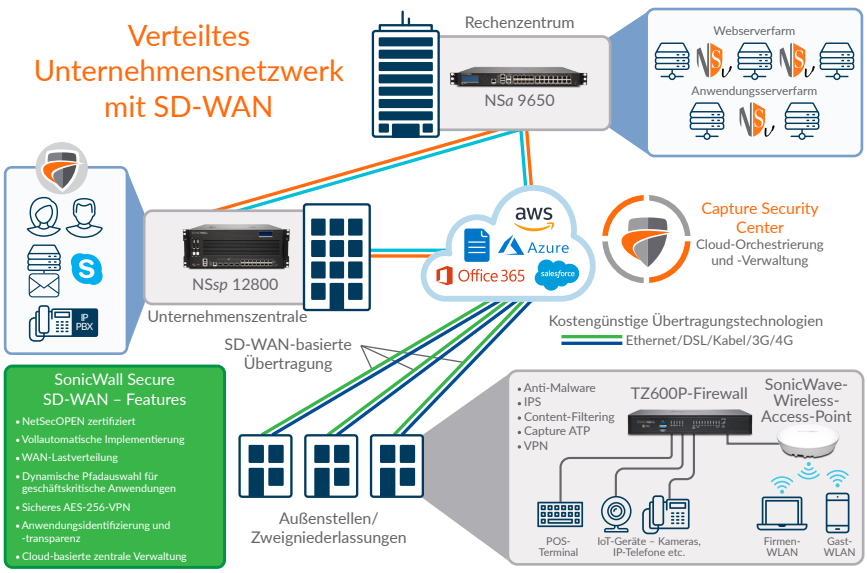
Zentralisierte Verwaltung und zentrales Reporting

Stark reglementierten Organisationen, die eine komplett aufeinander abgestimmte Security-Governance-, Compliance- und Risikomanagement-Strategie benötigen, bietet SonicWall eine einheitliche, sichere und erweiterbare Plattform, um SonicWall-Firewalls, Wireless-Access-Points und Switches der Dell N-Series und X-Series über einen korrelierten und prüfbaren Workstream-Prozess zu verwalten. So 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, Echtzeit-Ereignisüberwachung, einen Einblick in die Benutzeraktivitäten, Anwendungsidentifizierung, Datenstromanalyse und -forensik sowie Compliance- und Audit-Reporting. Dank der Workflow-Automatisierung können Unternehmen geeignete Firewall-Richtlinien flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit Compliance-Vorgaben implementieren und so alle Änderungen an ihren Firewalls effektiv verwalten. Die SonicWall Management und Reporting-Lösungen sind lokal in Form des SonicWall Global Management Systems und in der Cloud als Capture Security Center verfügbar. Damit lässt sich die Netzwerksicherheit einheitlich auf Geschäftsprozesse und Servicelevel abstimmen. Dabei zielt unsere Lösung auf Ihre gesamte Sicherheitsumgebung ab, anstatt eine gerätebasierte Strategie zu verfolgen, wodurch sich die Lebenszyklusverwaltung deutlich vereinfachen lässt.

Verteilte Netzwerke

Dank ihrer Flexibilität eignen sich TZ-Firewalls ideal sowohl für regional verteilte Unternehmen als auch für die Implementierungen an einem einzelnen Standort. In verteilten Netzwerken (z. B. im Einzelhandel) hat jeder Standort seine eigene TZ-Firewall, die oft über einen lokalen Anbieter mittels DSL-, Kabel- oder 3G-/4G-Verbindung an das Internet angeschlossen ist. Neben dem Internetzugriff nutzt jede Firewall auch eine Ethernet-Verbindung, um Pakete zwischen den Remote-Standorten und der Zentrale zu übertragen. Webservices und SaaS-Anwendungen wie etwa Office 365 und Salesforce werden über das Rechenzentrum bereitgestellt. Mithilfe der Mesh-VPN-Technologie können IT-Administratoren eine Hub-and-Spoke-Konfiguration für die sichere Übertragung von Daten zwischen sämtlichen Standorten erstellen.

Die in SonicOS enthaltene SD-WAN-Technologie ist eine perfekte Ergänzung für TZ-Firewalls, die

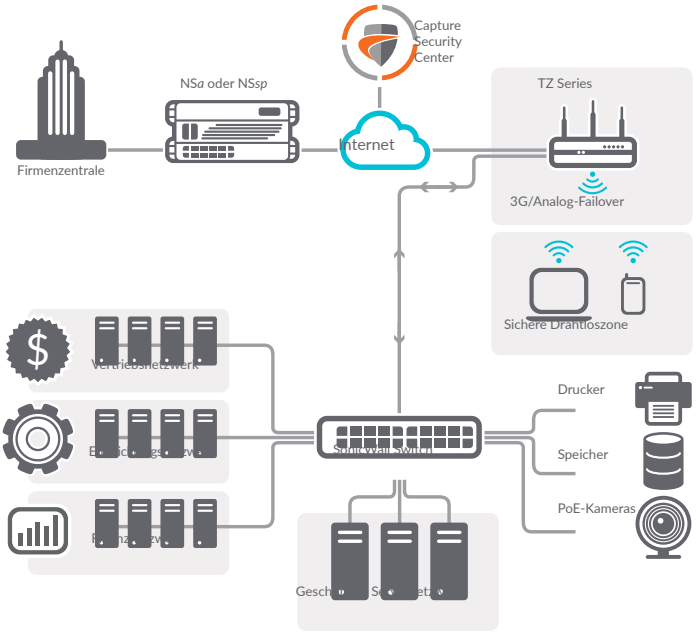


an Remote-Standorten und Zweigniederlassungen implementiert sind. Im Gegensatz zu kostspieligeren veralteten Technologien wie MPLS und T1 können Organisationen mit SD-WAN erschwinglichere öffentliche Internetdienste wählen und gleichzeitig eine hohe Anwendungsverfügbarkeit und eine vorhersehbare Performance sicherstellen.

Capture Security Center

Verbunden wird das verteilte Netzwerk durch das Cloud-basierte Capture Security Center (CSC) von SonicWall, das die Implementierung, die laufende Verwaltung und Echtzeitanalysen der TZ-Firewalls zentralisiert. Ein wesentliches CSC-Feature ist die vollautomatische Implementierung mit Zero-Touch-Deployment. Die Konfiguration und Implementierung von Firewalls an mehreren Standorten ist nicht nur zeitaufwendig, sondern erfordert normalerweise auch Personal vor Ort. Nicht bei SonicWall: Unsere vollautomatische Implementierung ermöglicht eine einfachere und schnellere Remote-Bereitstellung der SonicWall-Firewalls über die Cloud. Gleichzeitig vereinfacht CSC die laufende Verwaltung dank einer zentralen Cloud-basierten Verwaltung der SonicWall-Geräte im Netzwerk. Darüber hinaus bietet SonicWall Analytics einen zentralisierten, umfassenden, situativ angepassten Überblick über alle Aktivitäten in der Netzwerksicherheitsumgebung. So können Organisationen einen tieferen Einblick in die Anwendungsnutzung und -performance gewinnen und gleichzeitig die Bildung einer parallelen Schatten-IT verhindern.

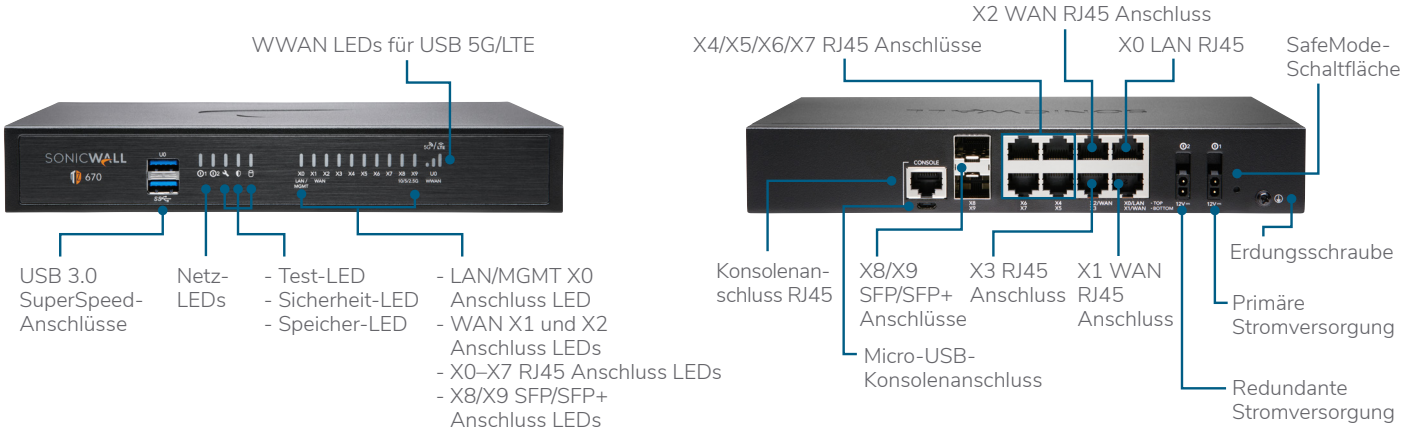
SonicWall Network Security Manager (NSM) ist ein zentralisierter Firewall-Manager für mehrere Mandanten und ermöglicht durch den Einsatz von



auditierbaren Arbeitsabläufen eine fehlerfreie zentrale Verwaltung aller Firewall-Funktionen. Er ist Teil des CSC. Die native Analyse-Engine sorgt für zentrale Transparenz und ermöglicht eine effektive Überwachung und Aufdeckung von Bedrohungen durch Vereinheitlichung und Korrelation der Protokolle über alle Firewalls hinweg. Der NSM unterstützt auch die Aufrechterhaltung der Konformität, da für alle Konfigurationsänderungen ein kompletter Audit-Trail und granulare Berichte erstellt werden. Der NSM lässt sich problemlos für jede Unternehmensgröße skalieren – von kleinen Organisationen bis hin zu Netzwerken mit Tausenden von Firewall-Appliances an zahlreichen Standorten.

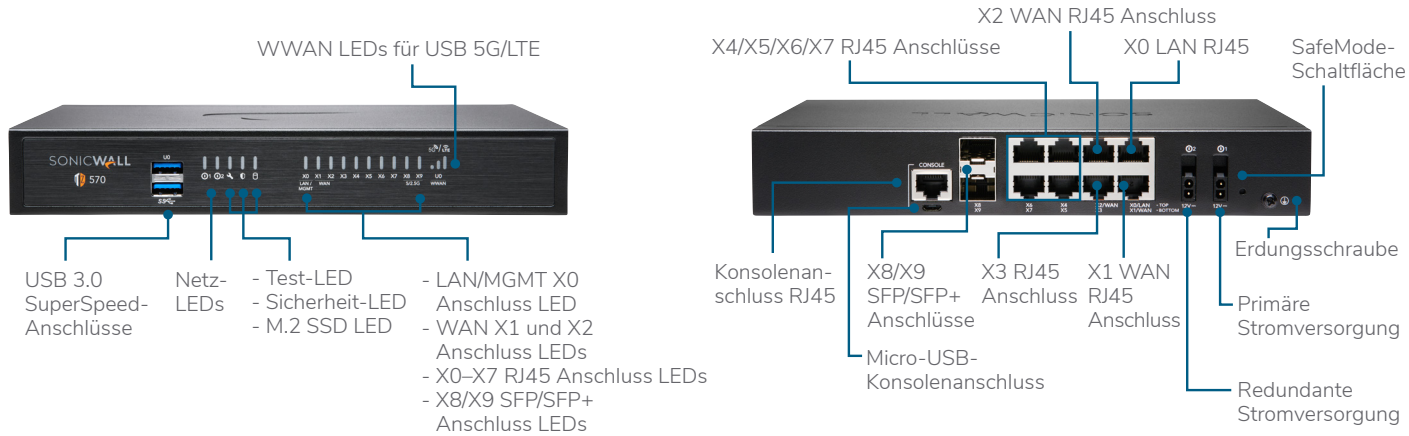
SonicWall TZ670 Series

TZ670 Firewalls sind für mittelgroße Unternehmen und verteilte Großunternehmen mit SD-Branch-Standorten bestimmt und verbinden branchenweit bewährte wirksame Sicherheit mit unübertroffener Preisperformance.



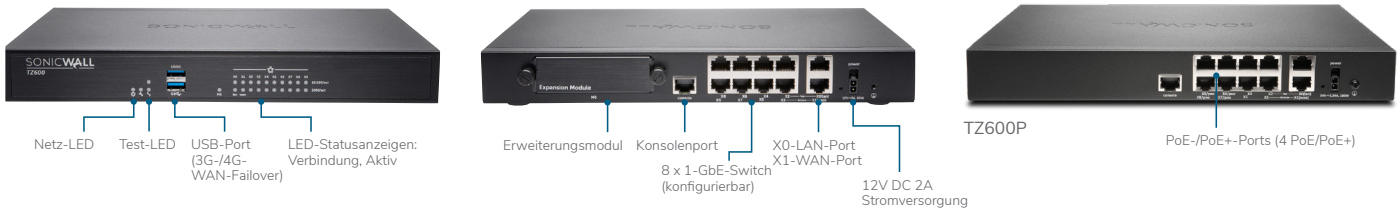
SonicWall TZ570 Series

TZ570 Firewalls sind für kleine bis mittelgroße Unternehmen und verteilte Großunternehmen mit SD-Branch-Standorten bestimmt und verbinden branchenweit bewährte wirksame Sicherheit mit unübertroffener Preisperformance.



SonicWall TZ600 Series

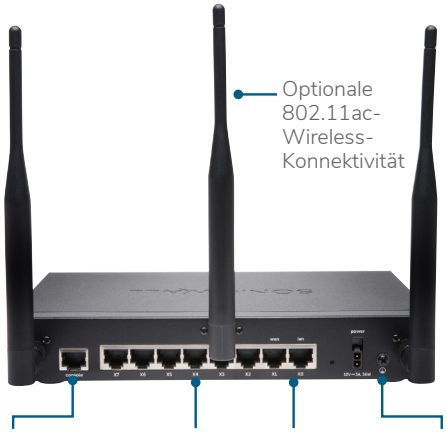
Für aufstrebende Unternehmen, Läden und Zweigstellen, die leistungsstarke Netzwerksicherheit und Optionen wie 802.3at-PoE+-Unterstützung zu einem erstklassigen Preis-Leistungs-Verhältnis benötigen, ist die SonicWall TZ600 mit ihren Enterprise-Class-Funktionen und ihrer kompromisslosen Performance genau das Richtige.



SonicWall TZ500 Series

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

Netz-LED | Test-LED | USB-Port (3G-/4G-WAN-Failover) | LED-Statusanzeigen: Verbindung, Aktiv



Konsolenport | 6 x 1-GbE-Switch (konfigurierbar) | X0-LAN-Port X1-WAN-Port | 12V DC 2A Stromversorgung

SonicWall TZ400 Series

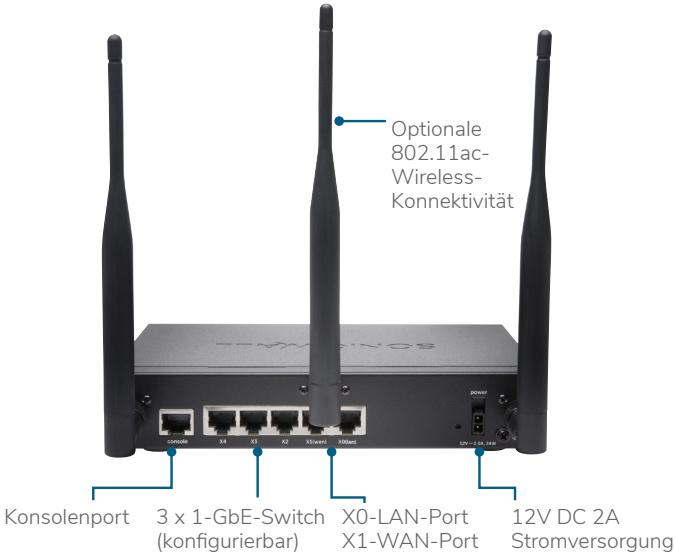
Die SonicWall TZ400 Series bietet kleinen Unternehmen sowie Einzelhandels- und Zweigniederlassungen Schutz der Enterprise-Klasse. Mit optional im Gerät integrierter Dualband-Wireless-Konnektivität gemäß dem 802.11ac-Standard ist eine flexible Wireless-Implementierung möglich.

Netz-LED | Test-LED | USB-Port (3G-/4G-WAN-Failover) | LED-Statusanzeigen: Verbindung, Aktiv

Konsolenport | 5 x 1-GbE-Switch (konfigurierbar) | X0-LAN-Port X1-WAN-Port | 12V DC 2A Stromversorgung

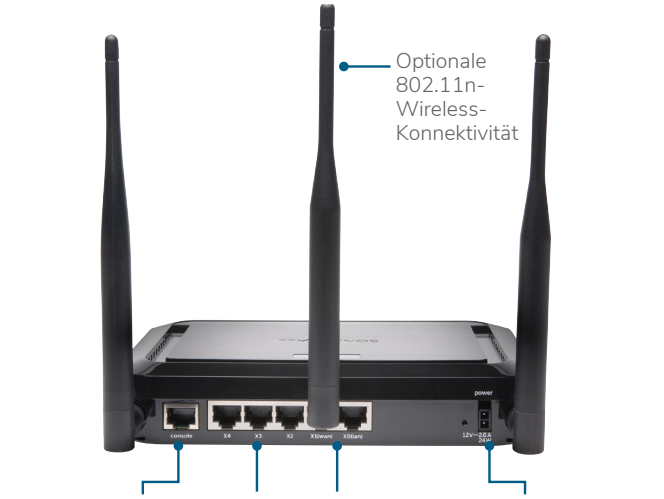
SonicWall TZ350/TZ300 Series

Die SonicWall TZ300/TZ350 Series ist eine All-in-One-Lösung, die Netzwerke wirksam vor Angriffen schützt. Im Unterschied zu Produkten aus dem Verbrauchermarkt kombinieren diese UTM-Firewalls schnelle Intrusion-Prevention, Malware-Schutz, Inhalts-/URL-Filterung mit optionaler integrierter 802.11ac-Wireless-Konnektivität. Gleichzeitig unterstützt sie einen umfassenden und sicheren mobilen Zugriff für Laptops, Smartphones und Tablets. Darüber hinaus bietet die TZ 300 optionale 802.3at PoE+-Konnektivität für die Versorgung PoE-fähiger Geräte.



SonicWall SOHO 250/SOHO Series

Die SonicWall SOHO 250 und 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. Mit der optionalen 802.11n-Wireless-Konnektivität können auch Mitarbeiter, Kunden und Gäste eine sichere WLAN-Verbindung nutzen.



Partner Enabled Services

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

Die SonicOS 7.0 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
- Umfassende API-Unterstützung
- SonicWall Switch-Integration
- SD-WAN-Skalierbarkeit
- SD-WAN Usability-Assistent[1]
- SonicCoreX und SonicOS Containerisierung[1]
- Skalierbarkeit von Verbindungen (SPI, DPI, DPI SSL)

Erweitertes Dashboard[1]
- Optimierte Geräteansicht
- Überblick über Top-Verkehr und -Benutzer
- Einblick in Bedrohungen
- Benachrichtigungszentrum

TSL/SSL/SSH-Entschlüsselung und -Prüfung
- TLS 1.3 mit verbesserter Sicherheit[1]
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Erweiterungen für DPI-SSL mit CFS
- Granulare DPI-SSL-Kontrollen nach Zone oder Regel

Capture Advanced Threat Protection[2]
- Real-Time Deep Memory Inspection
- Cloud-basierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention[2]
- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- GeoIP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]
- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloud-basierte Malware-Datenbank

Anwendungsidentifizierung[2]
- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturendatenbank

Visualisierung und Analyse des Datenverkehrs
- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloud-basierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[2]
- URL-Filterung
- Vermeidung von Proxys
- Blockieren mithilfe von Schlüsselwörtern
- Richtlinienbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN
- Sicheres SD-WAN
- 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, BGP)

Netzwerk
- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Port Mirroring (NSa 2650 und höher)
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Hochverfügbarkeitsmodus A/P mit State-Sync
- Lastausgleich für ein- und ausgehenden Datenverkehr
- Hochverfügbarkeit - Active/Standby mit State-Sync
- L2-Bridge, Wire/Virtual Wire-Modus, Tap-Modus, NAT-Modus
- Asymmetrisches Routing
- Common Access Card (CAC)-Unterstützung

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

Management, Überwachung und Support
- Capture Security Appliance (CSa) Support
- Capture Threat Assessment (CTA) v2.0
  - Neues Design oder neue Vorlage
  - Vergleich des Branchen- und globalen Durchschnitts
- Neue Benutzeroberfläche und Nutzererfahrung (UI/UX), intuitives Layout[1]
  - Dashboard
  - Geräteinformationen, Anwendungen, Bedrohungen
  - Topology-Ansicht
  - Vereinfachte Erstellung und Verwaltung von Richtlinien
- Regeln/Objekte Nutzungsstatistik[1]
  - Verwendet ggü. nicht verwendet
  - Aktiv ggü. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung[1]
- Interne und externe Speicherverwaltung[1]
- WWAN USB-Kartenunterstützung (5G/LTE/4G/3G)
- Network Security Manager (NSM)-Unterstützung
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Registrierung und Bereitstellung mittels Zero-Touch-Deployment
- Einfaches Reporting im CSC[1]
- Support für mobile SonicExpress-Apps
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mittels SonicWall Global Management System (GMS)[2]
- Logging
- NetFlow-/IPFIX-Export
- Cloud-basiertes Konfigurationsbackup
- BlueCoat Security Analytics Plattform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- CD Management-Anzeige
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinandergeschalteten Switches

Fehlersuche und Diagnose
- Erweiterte Paketüberwachung
- SSH-Terminal auf der Benutzeroberfläche

Wireless
- SonicWave AP Cloud-Management
- WIDS/WIPS
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- 802.11s Mesh-Networking
- Automatische Kanalauswahl
- RF-Spektrumanalyse
- Floor Plan View
- Topology-Ansicht
- Band Steering
- Beamforming
- AirTime-Fairness
- Bluetooth Low Energy
- MiFi-Extender
- Optimierte Funkfrequenzen (RF) und Verbesserungen
- Zyklische Quote für Gastbenutzer

Integrierte Wireless-Modelle
- 802.11ac Wave 2 Wireless-Technologie (TZ570W)
- Dualband (2,4 GHz und 5 GHz)
- 802.11 a/b/g/n/ac Wireless-Standards
- Erkennung und Vermeidung von Wireless-Angriffen
- Wireless Guest Services
- Lightweight Hotspot Messaging
- Segmentierung mithilfe virtueller Access Points
- Captive Portal
- Cloud-Zugriffssteuerungsliste

[1] *Neue Funktion, für SonicOS 7.0 verfügbar.*
[2] *Erfordert zusätzliches Abo.*

SONICWALL®

SonicWall TZ Series Systemddaten — SOHO, SOHO 250, TZ300 und TZ350

FIREWALL ALLGEMEIN	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Betriebssystem	SonicOS			
Schnittstellen	5 x 1-GbE, 1 USB, 1 Konsole		5 x 1-GbE, 1 USB, 1 Konsole	5 x 1-GbE, 1 USB, 1 Konsole
Power-over-Ethernet(PoE)-Unterstützung	—	—	TZ300P – 2 Ports (2 PoE oder 1 PoE+)	—
Erweiterung	USB			
Verwaltung	CLI, SSH, Web-UI, Capture Security Center, GMS, REST-APIs			
Single-Sign-on(SSO)-Benutzer	250	350	500	500
VLAN-Schnittstellen	25			
(Maximal) unterstützte Access-Points	2	4	8	8
FIREWALL/VPN-PERFORMANCE	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Firewall-Inspection-Durchsatz[1]	300 MBit/s	600 MBit/s	750 MBit/s	1,0 GBit/s
Threat-Prevention-Durchsatz[2]	150 MBit/s	200 MBit/s	235 MBit/s	335 MBit/s
Application-Inspection-Durchsatz[2]	—	275 MBit/s	375 MBit/s	600 MBit/s
IPS-Durchsatz[2]	200 MBit/s	250 MBit/s	300 MBit/s	400 MBit/s
Anti-Malware-Inspection-Durchsatz[2]	150 MBit/s	200 MBit/s	235 MBit/s	335 MBit/s
Durchsatz bei TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	30 MBit/s	50 MBit/s	60 MBit/s	65 MBit/s
IPSec-VPN-Durchsatz[3]	150 MBit/s	200 MBit/s	300 MBit/s	430 MBit/s
Verbindungen pro Sekunde	1.800	3.000	5.000	6.000
Maximale Anzahl von Verbindungen (SPI)	10.000	50.000	100.000	100.000
Maximale Anzahl von Verbindungen (DPI)	10.000	50.000	90.000	90.000
Maximale Anzahl von Verbindungen (DPI-SSL)	250	25.000	25.000	25.000
VPN	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Site-to-Site-VPN-Tunnel	10	10	10	15
IPSec-VPN-Clients (max.)	1 (5)	1 (5)	1 (10)	2 (10)
SSL-VPN-Lizenzen (max.)	1 (10)	1 (25)	1 (50)	1 (75)
Gebündelt mit Virtual Assist (max.)	—	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, 14v			
Routenbasiertes VPN	RIP, OSPF, BGP[4]			
VPN-Funktionen	Dead Peer Detection, DHCP Over 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 (integriert)			
SECURITY SERVICES	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
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			
Comprehensive Anti-Spam Service	unterstützt			
Anwendungsvisualisierung	Nein	Ja	Ja	Ja
Anwendungskontrolle	Ja	Ja	Ja	Ja
Capture Advanced Threat Protection	Nein	Ja	Ja	Ja
NETZWERK	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
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			
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)			

SonicWall TZ Series Systemdaten (Fortsetzung) — SOHO, SOHO 250, TZ300 und TZ350

NETZWERK (FORTSETZUNG)	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
Authentifizierung	LDAP (mehrere Domänen), XAUTH/ RADIUS, SSO, Novell, interne Benutzerdatenbank		LDAP (mehrere Domains), XAUTH/ RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)	
Lokale Benutzerdatenbank	150			
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			
Zertifizierungen[5]	FIPS 140-2 (mit Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus, Common Criteria NDPP (Firewall und IPS)			
Common Access Card (CAC)	unterstützt			
Hochverfügbarkeit	Nein		Active/Standby	
HARDWARE	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Formfaktor	Desktop			
Netzteil	24 W (extern)		24 W (extern) 65 W (extern) (nur TZ300P)	24 W (extern)
Maximaler Stromverbrauch (W)	6,4/11,3	6,9/11,3	6,9/12,0	6,9/12,0
Eingangsspannung	100–240 V AC, 50–60 Hz, 1 A			
Gesamtwärmeabgabe	21,8/38,7 BTU	23,5/38,7 BTU	23,5/40,9 BTU	23,5/40,9 BTU
Abmessungen	3,6 x 14,1 x 19 cm 1,42 x 5,55 x 7,48 Zoll		3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 Zoll	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 Zoll
Gewicht	0,34 kg 0,48 kg		0,73 kg 0,84 kg	0,73 kg 0,84 kg
WEEE-Gewicht	0,80 kg 0,94 kg		1,15 kg 1,26 kg	1,15 kg 1,26 kg
Versandgewicht	1,20 kg 1,34 kg		1,37 kg 1,48 kg	1,37 kg 1,48 kg
MTBF (in Jahren)	58,9/56,1 (Wireless)	56,1	56,1	56,1
Umgebung (Betrieb/Lagerung)	0 bis 40 °C/-40 bis 70 °C			
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend			
RICHTLINIEN	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Konformität mit wichtigen Normen (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, ANATEL		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, ANATEL	
Konformität mit wichtigen Normen (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (RES, 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 (RES, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	
INTEGRIERTE WIRELESS-OPTIONEN	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
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[6]	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		802.11a: 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	

SonicWall TZ Series Systemdaten (Fortsetzung) — SOHO, SOHO 250, TZ300 und TZ350

INTEGRIERTE WIRELESS-OPTIONEN	SOHO SERIES	SOHO 250 SERIES	TZ300 SERIES	TZ350 SERIES
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			
Steuerung der Sendeleistung	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, 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, 866,7 MBit/s pro Kanal	
Modulationstechnologie/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 zukünftiges Release.

[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 Threat-Prevention-/Gateway-AV-/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. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen.*

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

[4] *BGP ist nur für die SonicWall TZ350, TZ400, TZ500 und TZ600 verfügbar.*

[5] *Ausstehende FIPS- und ICSA-Genehmigung für SOHO 250 und TZ350.*

[6] *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.*

SonicWall TZ Series Systemdaten — TZ400, TZ500 und TZ600

FIREWALL ALLGEMEIN	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Betriebssystem		SonicOS	
Schnittstellen	7 x 1-GbE, 1 USB, 1 Konsole	8 x 1-GbE, 2 USB, 1 Konsole	10 x 1-GbE, 2 USB, 1 Konsole, 1 Erweiterungssteckplatz
Power-over-Ethernet(PoE)-Unterstützung	—	—	TZ600P - 4 Anschlüsse (4 PoE oder 4 PoE+)
Erweiterung	USB	2 USB	Erweiterungssteckplatz (Rückseite)*, 2 USB
Verwaltung	CLI, SSH, Web-UI, Capture Security Center, GMS, REST-APIs		
Single-Sign-on(SSO)-Benutzer	500	500	500
VLAN-Schnittstellen	50	50	50
(Maximal) unterstützte Access-Points	16	16	24
FIREWALL/VPN-PERFORMANCE	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Firewall-Inspection-Durchsatz[1]	1,3 GBit/s	1,4 GBit/s	1,9 GBit/s
Threat-Prevention-Durchsatz[2]	600 MBit/s	700 MBit/s	800 MBit/s
Application-Inspection-Durchsatz[2]	1,2 GBit/s	1,3 GBit/s	1,8 GBit/s
IPS-Durchsatz[2]	900 MBit/s	1,0 GBit/s	1,2 GBit/s
Anti-Malware-Inspection-Durchsatz[2]	600 MBit/s	700 MBit/s	800 MBit/s
Durchsatz bei TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	180 MBit/s	225 MBit/s	300 MBit/s
IPSec-VPN-Durchsatz[3]	900 MBit/s	1,0 GBit/s	1,1 GBit/s
Verbindungen pro Sekunde	6.000	8.000	12.000
Maximale Anzahl von Verbindungen (SPI)	150.000	150.000	150.000
Maximale Anzahl von Verbindungen (DPI)	125.000	125.000	125.000
Maximale Anzahl von Verbindungen (DPI-SSL)	25.000	25.000	25.000
VPN	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Site-to-Site-VPN-Tunnel	20	25	50
IPSec-VPN-Clients (max.)	2 (25)	2 (25)	2 (25)
SSL-VPN-Lizenzen (max.)	2 (100)	2 (150)	2 (200)
Gebündelt mit Virtual Assist (max.)	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, 14v		
Routenbasiertes VPN	RIP, OSPF, BGP		
VPN-Funktionen	Dead Peer Detection, DHCP Over 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 (integriert)		
SECURITY SERVICES	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
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		
Comprehensive Anti-Spam Service	unterstützt		
Anwendungsvisualisierung	Ja	Ja	Ja
Anwendungskontrolle	Ja	Ja	Ja
Capture Advanced Threat Protection	Ja	Ja	Ja
NETZWERK	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
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		
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)		

SonicWall TZ Series Systemdaten (Fortsetzung) — TZ400, TZ500 and TZ600

NETZWERK	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Authentifizierung	LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)		
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		
Zertifizierungen	FIPS 140-2 (mit Suite B) Level 2, UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus, Common Criteria NDPP (Firewall und IPS)		
Common Access Card (CAC)	unterstützt		
Hochverfügbarkeit	Active/Standby	Active/Standby mit Stateful-Synchronisierung	
HARDWARE	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Formfaktor	Desktop		
Netzteil	24W (extern)	36W (extern)	60W (extern) 180W (extern) (nur TZ600P)
Maximaler Stromverbrauch (W)	9,2/13,8	13,4/17,7	16,1
Eingangsspannung	100–240 V AC, 50–60 Hz, 1 A		
Gesamtwärmeabgabe	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Abmessungen	3,5 x 13,4 x 19 cm 1,38 x 5,28 x 7,48 Zoll	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,86 Zoll	3,5 x 18 x 28 cm 1,38 x 7,09 x 11,02 Zoll
Gewicht	0,73 kg 0,84 kg	0,92 kg 1,05 kg	1,47 kg
WEEE-Gewicht	1,15 kg 1,26 kg	1,34 kg 1,48 kg	1,89 kg
Versandgewicht	1,37 kg 1,48 kg	1,93 kg 2,07 kg	2,48 kg
MTBF (in Jahren)	54,0	40,8	18,4
Umgebung (Betrieb/Lagerung)	0 bis 40 °C/-40 bis 70 °C		
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend		
RICHTLINIEN	**TZ400 SERIES**	**TZ500 SERIES**	**TZ600 SERIES**
Konformität mit wichtigen Normen (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, ANATEL	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, ANATEL	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, ANATEL
Konformität mit wichtigen Normen (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (RES, 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 (RES, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/ GS, CB, Mexiko CoC nach UL, WEEE, REACH	—

SonicWall TZ Series Systemdaten (Fortsetzung) — TZ400, TZ500 and TZ600

INTEGRIERTE WIRELESS-OPTIONEN	TZ400 SERIES	TZ500 SERIES	TZ600 SERIES
Standards	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, 5,180–5,825 GHz; 802.11ac: 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 (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		—
Steuerung der Sendeleistung	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; 802.11ac: 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, 866,7 MBit/s pro Kanal		—
Modulationstechnologie/ 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); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)		—

SonicWall TZ Series Technische Daten — TZ500 und TZ670

FIREWALL ALLGEMEIN	TZ570 SERIES	TZ670 SERIES
Betriebssystem	SonicOS 7.0	
Schnittstellen	8x1GbE, 2x5GbE, 2 USB 3.0, 1 Konsole	8x1GbE, 2x10GbE, 2 USB 3.0, 1 Konsole
Power-over-Ethernet(PoE)-Unterstützung	TZ570P (5 PoE oder 3PoE+)	—
Erweiterung	Speichererweiterungssteckplatz (bis zu 256 GB)	Speichererweiterungssteckplatz (bis zu 256 GB) (32 GB im Lieferumfang enthalten)
Verwaltung	Network Security Manager, CLI, SSH, Web UI, GMS, REST APIs	
Single-Sign-on(SSO)-Benutzer	2.500	2.500
VLAN-Schnittstellen	256	256
(Maximal) unterstützte Access-Points	32	32
FIREWALL/VPN-PERFORMANCE	**TZ570 SERIES**	**TZ670 SERIES**
Firewall-Inspection-Durchsatz[1]	4,00 GBit/s	5,00 GBit/s
Threat-Prevention-Durchsatz[2]	2,00 GBit/s	2,50 GBit/s
Application-Inspection-Durchsatz[2]	2,5 GBit/s	3,0 GBit/s
IPS-Durchsatz[2]	2,5 GBit/s	3,0 GBit/s
Anti-Malware-Inspection-Durchsatz[2]	2,00 GBit/s	2,50 GBit/s
Durchsatz bei TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	750 MBit/s	800 MBit/s
IPSec-VPN-Durchsatz[3]	1,80 GBit/s	2,10 GBit/s
Verbindungen pro Sekunde	16.000	25.000
Maximale Anzahl von Verbindungen (SPI)	1.250.000	1.500.000
Maximale Anzahl von Verbindungen (DPI)	400.000	500.000
Maximale Anzahl von Verbindungen (DPI-SSL)	30.000	30.000
VPN	**TZ570 SERIES**	**TZ670 SERIES**
Site-to-Site-VPN-Tunnel	200	250
IPSec-VPN-Clients (max.)	10 (500)	10 (500)
SSL-VPN-Lizenzen (max.)	2 (200)	2 (250)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography	
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v	
Routenbasiertes VPN	RIP, OSPF, BGP	
VPN-Funktionen	Dead Peer Detection, DHCP über VPN, IPSec-NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN	
Unterstützte globale VPN-Client-Plattformen	Microsoft® Windows 10	
NetExtender	Microsoft® Windows 10, Linux	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 10	
SECURITY SERVICES	**TZ570 SERIES**	**TZ670 SERIES**
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	
Comprehensive Anti-Spam Service	Ja	
Anwendungsvisualisierung	Ja	
Anwendungskontrolle	Ja	
Capture Advanced Threat Protection	Ja	
DNS-Sicherheit	Ja	

SonicWall TZ Series Technische Daten (Fortsetzung) — TZ570 and TZ670

NETZWERK	TZ570 SERIES	TZ670 SERIES
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	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)	
Authentifizierung	LDAP (mehrere Domänen), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)	
Lokale Benutzerdatenbank	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 a802.3	
Zertifikate (ausstehend)	FIPS 140-2 (mit Suite B) Level 2, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus, Common Criteria NDPP (Firewall und IPS)	

HARDWARE	TZ570 SERIES	TZ670 SERIES
Formfaktor	Desktop[5]	
Netzteil	60W (extern) 180W (extern) (nur TZ570P)	60W (extern)
Maximaler Stromverbrauch (W)	13,1	13,1
Eingangsspannung und Frequenz	100–240 V AC, 50–60 Hz	100–240 V AC, 50–60 Hz
Gesamtwärmeabgabe	45,9/60,5 BTU	55,1 BTU
Abmessungen	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,85 Zoll	3,5 x 15 x 22,5 cm 1,38 x 5,91 x 8,85 Zoll
Gewicht	0,97 kg	0,97 kg
WEEE-Gewicht	1,42 kg	1,42 kg
Versandgewicht	1,93 kg	1,93 kg
MTBF bei 25 °C in Jahren	26,1	43,9
Umgebung (Betrieb/Lagerung)	0 bis 40 °C/-40 bis 70 °C	
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend	

RICHTLINIEN	TZ570 SERIES	TZ670 SERIES
Konformität mit wichtigen Normen (kabelgebundene Modelle - TZ670, TZ570)	FCC Klasse B, FCC, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL/cUL, TÜV/GS, CB, Mexico DGN Notification nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	FCC Klasse B, FCC, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL/cUL, TÜV/GS, CB, Mexico DGN Notification nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL
Konformität mit wichtigen Normen (Wireless-Modelle - TZ570W)	FCC Klasse B, FCC P15C, FCC P15E, ICES Klasse B, ISED/IC, CE (RES, RoHS), C-Tick, VCCI Klasse B, Japan Wireless, UL/cUL, TÜV/GS, CB, Mexico DGN Notification nach UL, WEEE, REACH, BSMI, NCC (TW) KCC/MSIP, SRRC, ANATEL	—
Konformität mit wichtigen Normen (PoE-Modelle - TZ570P)	FCC Klasse A, ICES Klasse A, CE (EMC, LVD, RoHS), C-Tick, VCCI Klasse A, UL/cUL, TÜV/GS, CB, Mexico DGN Notification nach UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL	—

SonicWall TZ Series Technische Daten (Fortsetzung) — TZ570 and TZ670

INTEGRIERTE WIRELESS-OPTIONEN	TZ570 SERIES	TZ670 SERIES
Standards	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, 5,180–5,825 GHz; 802.11ac: 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 (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	—
Steuerung der Sendeleistung	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; 802.11ac: 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, 866,7 MBit/s pro Kanal	—
Modulationstechnologie/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); 802.11ac: Orthogonal Frequency Division Multiplexing (OFDM)	—

[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 Threat-Prevention-/Gateway-AV-/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. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen.*
[3] *VPN-Durchsatz gemäß RFC 2544 unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte gemessen. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.*
[4] *Für Rackmontage, separates Rackmontagekit erhältlich.*
[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.*

Produkt	Artikelnummer
SOHO 250 mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-1815
SOHO 250 Wireless-AC mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-1824
TZ300 mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1702
TZ300 Wireless-AC mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1703
TZ300P mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-0602
TZ350 mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-1843
TZ350 Wireless-AC mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-1851
TZ400 mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1705
TZ400 Wireless-AC mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1706
TZ500 mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1708
TZ500 Wireless-AC mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1709
TZ570 mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-5651
TZ570W mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-5649
TZ570P mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-5653
TZ600 mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1711
TZ600P mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-0600
TZ670 mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-5640
Optionen für Hochverfügbarkeit (nur Geräte des gleichen Modells)	
TZ500 High Availability	01-SSC-0439
TZ570 High Availability	02-SSC-5694
TZ570P High Availability	02-SSC-5655
TZ600 High Availability	01-SSC-0220
TZ670 High Availability	02-SSC-5654

Dienste	Artikelnummer
Für die SonicWall SOHO 250 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	02-SSC-1726
Capture Advanced Threat Protection für SOHO 250 (1 Jahr)	02-SSC-1732
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-1750
Content Filtering Service (1 Jahr)	02-SSC-1744
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-1823
24/7-Support (1 Jahr)	02-SSC-1720
Für die SonicWall TZ300 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	01-SSC-1430
Capture Advanced Threat Protection für TZ300 (1 Jahr)	01-SSC-1435
Gateway Anti-Virus, Intrusion Prevention und 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 die SonicWall TZ350 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	02-SSC-1773
Capture Advanced Threat Protection für TZ350 (1 Jahr)	02-SSC-1779
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-1797
Content Filtering Service (1 Jahr)	02-SSC-1791
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-1809
24/7-Support (1 Jahr)	02-SSC-1767

SonicWall TZ Series – Bestellinformationen

Für die SonicWall TZ400 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	01-SSC-1440
Capture Advanced Threat Protection für TZ400 (1 Jahr)	01-SSC-1445
Gateway Anti-Virus, Intrusion Prevention und 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 die SonicWall TZ500 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	01-SSC-1450
Capture Advanced Threat Protection für TZ500 (1 Jahr)	01-SSC-1455
Gateway Anti-Virus, Intrusion Prevention und 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 die SonicWall TZ600 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention und 24/7-Support (1 Jahr)	01-SSC-1460
Capture Advanced Threat Protection für TZ600 (1 Jahr)	01-SSC-1465
Gateway Anti-Virus, Intrusion Prevention und 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
Für die SonicWall TZ670 Series	
Essential Protection Service Suite – Capture ATP, Threat Prevention, Content Filtering, Anti-Spam und 24/7-Support (1 Jahr)	02-SSC-5053
Capture Advanced Threat Protection für TZ670 (1 Jahr)	02-SSC-5035
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-5059
Content Filtering Service (1 Jahr)	02-SSC-5047
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-5041
24/7-Support (1 Jahr)	02-SSC-5029
Für die SonicWall TZ570 Series (TZ570)	
Essential Protection Service Suite – Capture ATP, Threat Prevention, Content Filtering, Anti-Spam und 24/7-Support (1 Jahr)	02-SSC-5137
Capture Advanced Threat Protection für TZ570 (1 Jahr)	02-SSC-5083
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-5155
Content Filtering Service (1 Jahr)	02-SSC-5119
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-5101
24/7-Support (1 Jahr)	02-SSC-5065
Für die SonicWall TZ570 Series (TZ570W)	
Essential Protection Service Suite – Capture ATP, Threat Prevention, Content Filtering, Anti-Spam und 24/7-Support (1 Jahr)	02-SSC-5149
Capture Advanced Threat Protection für TZ570W (1 Jahr)	02-SSC-5095
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-5167
Content Filtering Service (1 Jahr)	02-SSC-5131
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-5113
24/7-Support (1 Jahr)	02-SSC-5077
Für die SonicWall TZ570 Series (TZ570P)	
Essential Protection Service Suite – Capture ATP, Threat Prevention, Content Filtering, Anti-Spam und 24/7-Support (1 Jahr)	02-SSC-5143
Capture Advanced Threat Protection für TZ570P (1 Jahr)	02-SSC-5089
Gateway Anti-Virus, Intrusion Prevention und Application Control (1 Jahr)	02-SSC-5161
Content Filtering Service (1 Jahr)	02-SSC-5125
Comprehensive Anti-Spam Service (1 Jahr)	02-SSC-5107
24/7-Support (1 Jahr)	02-SSC-5071

Zubehör	Artikelnummer
TZ670/570 Series	
SonicWall TZ670/570 Series FRU Stromversorgung	02-SSC-3078
SonicWall TZ670/570 Series Rackmontagekit	02-SSC-3112
SonicWall 32GB Speichermodul für die TZ670/570 Series	02-SSC-3114
SonicWall 64GB Speichermodul für die TZ670/570 Series	02-SSC-3115
SonicWall 128GB Speichermodul für die TZ670/570 Series	02-SSC-3116
SonicWall 256GB Speichermodul für die TZ670/570 Series	02-SSC-3117
SonicWall Micro-USB-Konsolenkabel für die TZ670/570 Series	02-SSC-5173
TZ600/500/400/350/300, SOHO 250 Series	
SonicWall TZ600 Rackmontagekitt	01-SSC-0225
SonicWall TZ600 Series FRU Stromversorgung	01-SSC-0280
SonicWall TZ500 Series Rackmontagekit	01-SSC-0438
SonicWall TZ500 Series FRU Stromversorgung	01-SSC-0437
SonicWall TZ400 Series Rackmontagekit	01-SSC-0525
SonicWall TZ350, TZ300 Series Rackmontagekit	01-SSC-0742
SonicWall TZ400, TZ350, TZ300, SOHO 250, SOHO Series FRU Stromversorgung	01-SSC-0709
SonicWall TZ300 PoE FRU Stromversorgung	02-SSC-0613
SonicWall SFP/SFP+ Module	
10GB-SR SFP+ Kurzstrecken-Fasermodul Multi-Mode ohne Kabel	01-SSC-9785
10GB-LR SFP+ Langstrecken-Fasermodul Multi-Mode ohne Kabel	01-SSC-9786
10GB SFP+ Kupfer mit 1m Twinax-Kabel	01-SSC-9787
10GB SFP+ Kupfer mit 3m Twinax-Kabel	01-SSC-9788
1GB-SX SFP Nahverkehr-Fasermodul Multi-Mode ohne Kabel	01-SSC-9789
1GB-LX SFP Fernverkehr-Fasermodul Multi-Mode ohne Kabel	01-SSC-9790
1GB-RJ45 SFP Kupfermodul ohne Kabel	01-SSC-9791
SONICWALL SFP+ 10GBASE-T Transceiver Kupfer RJ45-Modul	02-SSC-1874

Modellnummern (Zulassung)

SOHO/SOHO Wireless	APL31-0B9/APL41-0BA
SOHO 250/SOHO 250 Wireless	APL41-0D6/APL41-0BA
TZ300/TZ300 Wireless/TZ300P	APL28-0B4/APL28-0B5/APL47-0D2
TZ350/TZ350 Wireless	APL28-0B4/APL28-0B5
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3
TZ670	APL62-0F7
TZ570/TZ570W/TZ570P	APL62-0F7/APL62-0F8/APL63-0F9

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

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

Datasheet-TZSeries-US-KJ-2126

SONICWALL®