SonicWall TZ Series

Integrierte Threat-Prevention- und SD-WAN-Plattform für kleine bis mittelständische sowie große regional verteilte Unternehmen

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 geringer Total Cost of Ownership.

Flexible, integrierte Sicherheitslösung

Herzstück der TZ Series ist SonicOS, das funktionsreiche Betriebssystem von SonicWall. SonicOS umfasst leistungsstarke Funktionen, mit denen Organisationen ihre Unified Threat Management (UTM)-Firewalls flexibel an ihre Netzwerkanforderungen anpassen können. So vereinfachen ein integrierter drahtloser Controller, der unterstützte IEEE-802.11ac-Standard und unsere SonicWave-802.11ac-Wave-2-Access-Points allesamt die Erstellung eines sicheren drahtlosen Highspeed-Netzwerks. Die TZ300P und TZ600P 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 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

Vorteile:

Flexible, integrierte Sicherheitslösung

- Sicheres SD-WAN
- Leistungsstarkes SonicOS-Betriebssystem
- Highspeed-802.11ac WLAN
- Power over Ethernet (PoE/PoE+)
- Netzwerksegmentierung mit VLANs

Überragender Bedrohungsschutz und exzellente Performance

- Zum Patent angemeldete Real-Time Deep Memory Inspection-Technologie
- Patentierte Reassembly-Free Deep Packet Inspection-Technologie
- Integrierter und Cloud-basierter Bedrohungsschutz
- TLS-/SSL-Entschlüsselung und -Prüfung
- Effiziente, branchenweit bewährte Sicherheit
- Spezielles Capture Labs Threat Research-Team
- Endpunktsicherheit mit Capture Client

Einfache Implementierung, Einrichtung und laufende Verwaltung

- Vollautomatische Implementierung mit Zero-Touch Deployment
- Cloud-basierte und lokale zentralisierte Verwaltung
- Skalierbare Firewalls
- Geringe Total Cost of Ownership

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-Filtering 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.

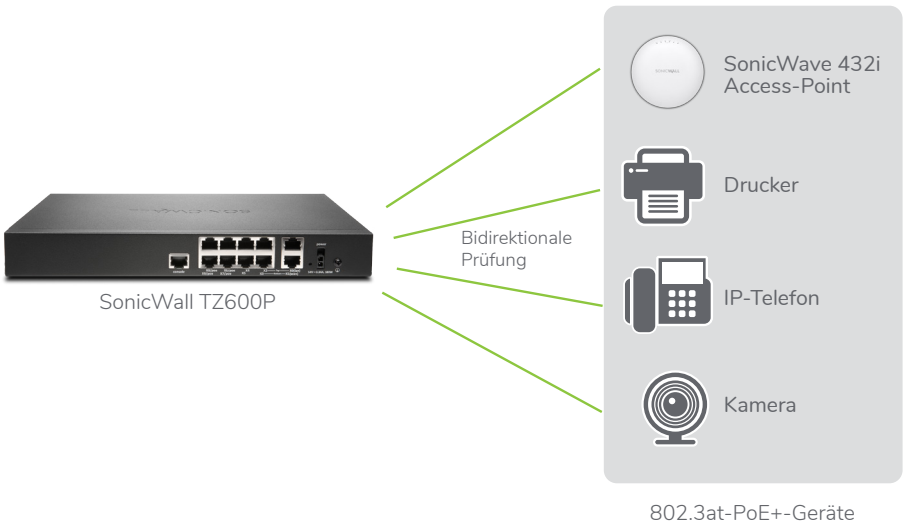
Da immer mehr Unternehmen für den Schutz von Websitzungen auf Verschlüsselung setzen, ist es extrem wichtig, dass Firewalls verschlüsselten Datenverkehr auf Bedrohungen überprüfen können. Die TZ-Firewalls bieten einen umfassenden Schutz, weil sie unabhängig von Port oder Protokoll eine vollständige Entschlüsselung 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.

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

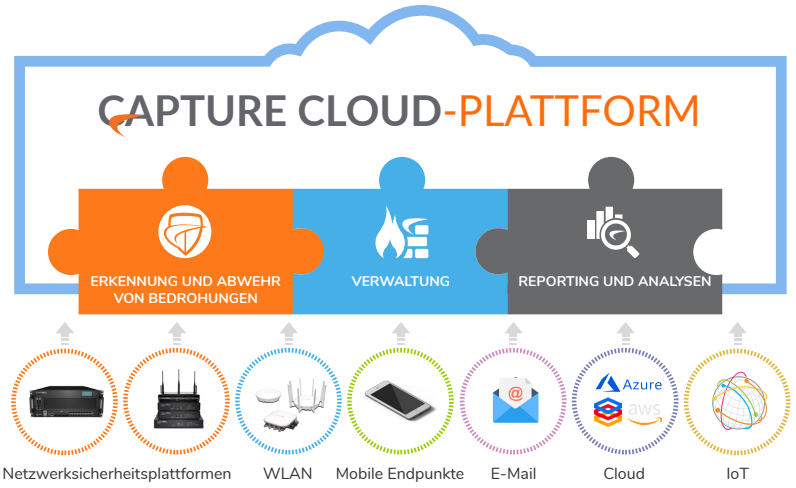
Holen Sie das Maximum aus Ihren PoE-fähigen Geräten heraus – ohne die Kosten und die Komplexität von Powerover- Ethernet-Switches oder -Injectors. TZ300P- und TZ600P-Firewalls integrieren IEEE-802.3at-Technologie für PoE- und PoE+-Geräte wie Wireless-Access-Points, Kameras, IP-Telefone usw. Die Firewalls 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.

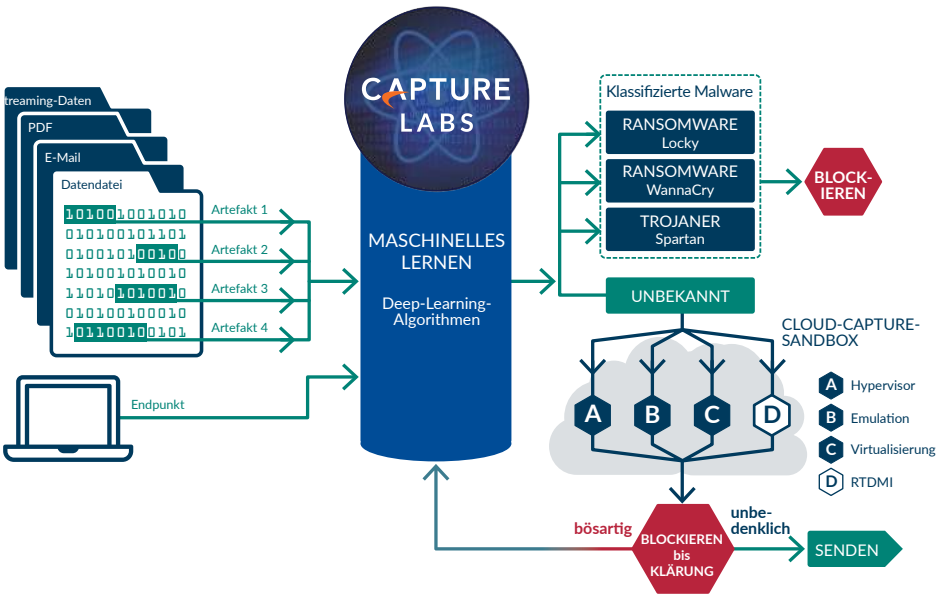


Schutz vor komplexen Bedrohungen

Herzstück der automatisierten SonicWall Lösung zur Echtzeitprävention von Sicherheitslücken ist der SonicWall Capture Advanced Threat Protection-Service, eine Cloud-basierte Multi-Engine-Sandbox, die den Firewall-Bedrohungsschutz erweitert, um Zero-Day-Bedrohungen zu erkennen und abzuwehren. Verdächtige Dateien werden zur Analyse mittels Deep-Learning-Algorithmen in die Cloud übertragen und können am Gateway gehalten werden, bis der Sicherheitsstatus geklärt ist. Die Multi-Engine-Sandbox-Plattform mit Real-Time Deep Memory Inspection-Technologie, virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus und analysiert dessen Verhalten. Als bösartig identifizierte Dateien werden blockiert und Capture ATP erstellt umgehend einen Hash. Kurz darauf erhalten die Firewalls eine Signatur, um Folgeangriffe zu verhindern.

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

Für einen umfassenden Endpunktschutz kombiniert SonicWall Capture Client Antivirentechnologien der nächsten Generation mit der Cloud-basierten Multi-Engine-Sandbox von SonicWall.



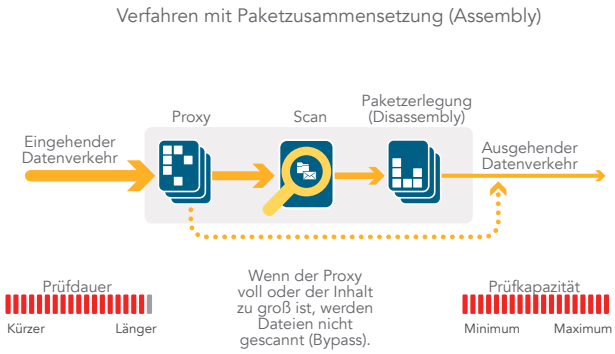
SONICWALL®

Reassembly-Free Deep Packet Inspection-Engine

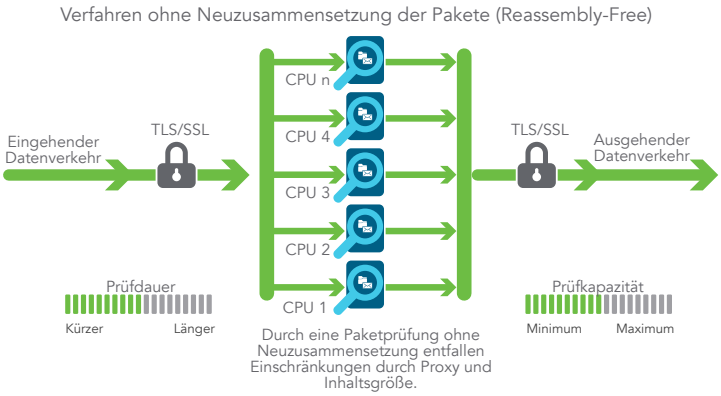
Bei der SonicWall Reassembly-Free Deep Packet Inspection (RFDPI)-Engine handelt es sich um ein Single-Pass-Prüfsystem mit niedriger Latenz, das streambasierte bidirektionale Verkehrsanalysen in Hochgeschwindigkeit durchführt, um Eindringversuche und Malware-Downloads zu erkennen und den Anwendungsverkehr 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



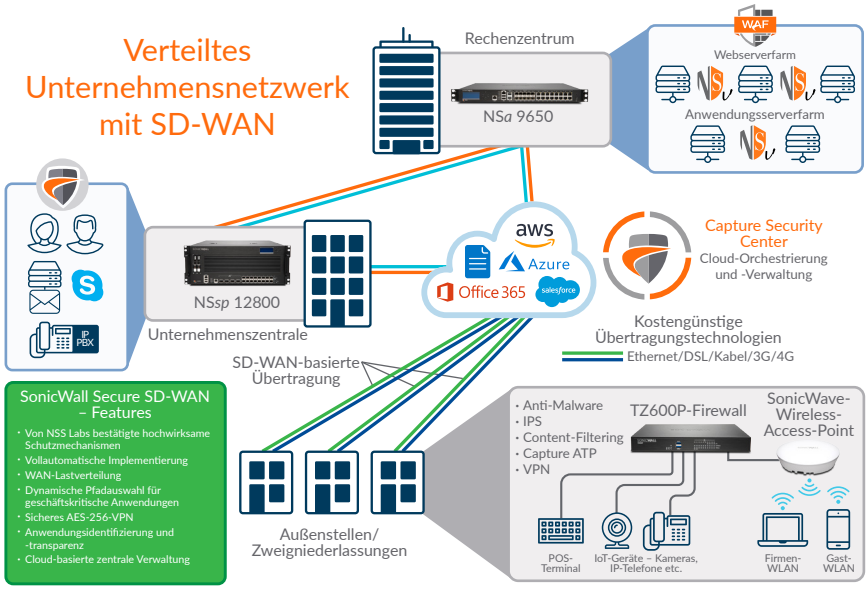
Streambasierte SonicWall Architektur

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 System 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

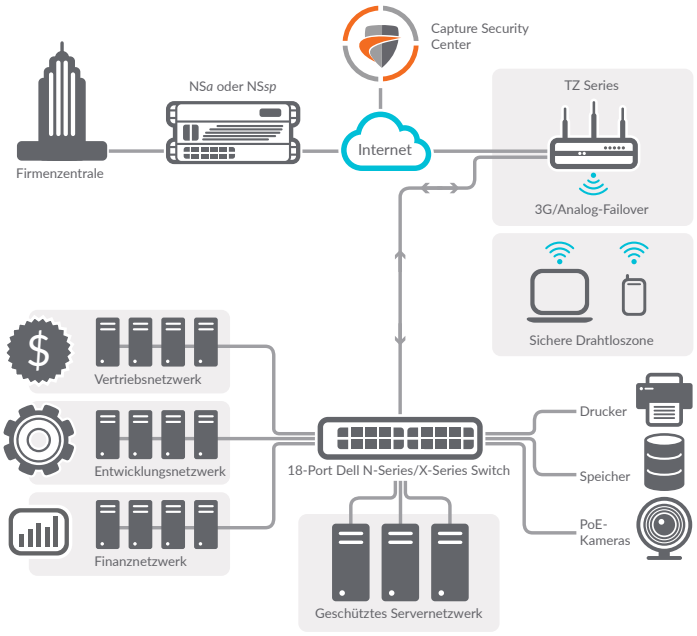
Dank ihrer Flexibilität eignen sich TZ-Firewalls ideal sowohl für regional verteilte Unternehmen als auch für die Implementierungen an einem einzelnen Standort. In verteilten Netzwerken (z. B. im Einzelhandel) hat jeder Standort seine eigene TZ-Firewall, die oft über einen lokalen Anbieter mittels DSL-, 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.



Einzelne Standorte

Für Implementierungen an einem einzigen Standort bietet eine integrierte Netzwerksicherheitslösung enorme Vorteile. TZ-Firewalls kombinieren hocheffektive Schutzfunktionen mit Optionen wie integrierter 802.11ac-Wireless-Technologie und – im Fall der TZ300P und TZ600P – PoE-/Po-E+-Unterstützung. Neben den umfangreichen SonicOS-Features nutzen wir in der TZ Series dieselbe Sicherheitsengine wie in unserer NSaSeries der Mittelklasse und unserer NSsp Serie der Spitzenklasse. Dank der intuitiven SonicOS-Benutzeroberfläche sind Konfiguration und Verwaltung wirklich ein Kinderspiel. Außerdem können Organisationen aufgrund des kompakten Formfaktors wertvolle Rackfläche einsparen.

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.

Technische Daten	TZ600 Series
Firewall-Durchsatz	1,9 GBit/s
Threat-Prevention-Durchsatz	800 MBit/s
Anti-Malware-Durchsatz	800 MBit/s
IPS-Durchsatz	1,2 GBit/s
Maximale Anzahl von Verbindungen	150.000
Neue Verbindungen/Sekunde	12.000

TZ600P

PoE-/PoE+-Ports (4 PoE/PoE+)

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

Erweiterungsmodul | Konsolenport | 8 x 1-GbE-Switch (konfigurierbar) | X0-LAN-Port X1-WAN-Port | 12V DC 2A Stromversorgung

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.

Technische Daten	TZ500 Series
Firewall-Durchsatz	1,4 GBit/s
Threat-Prevention-Durchsatz	700 MBit/s
Anti-Malware-Durchsatz	700 MBit/s
IPS-Durchsatz	1,0 GBit/s
Maximale Anzahl von Verbindungen	150.000
Neue Verbindungen/Sekunde	8.000

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

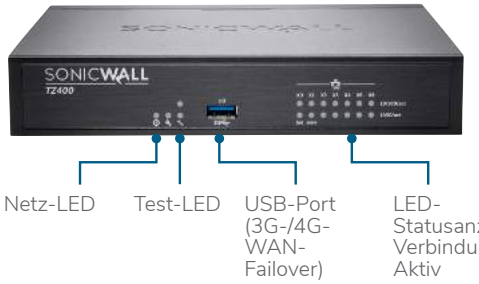
Optionale 802.11ac-Wireless-Konnektivität

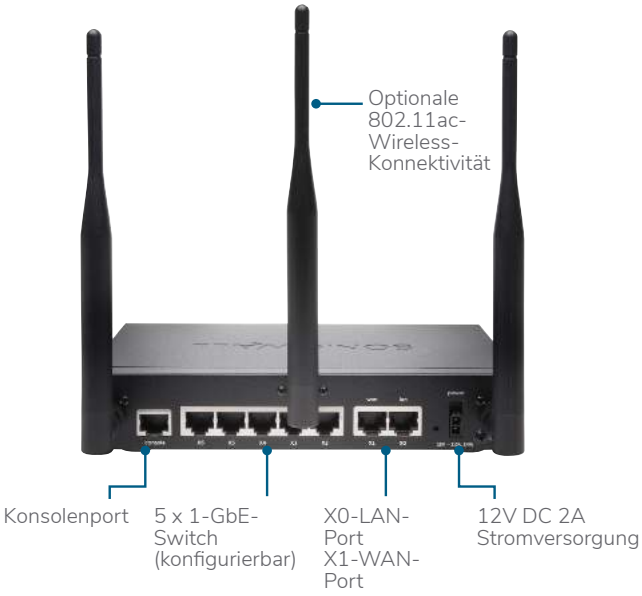
Konsolenport | 6 x 1-GbE-Switch (konfigurierbar) | X0-LAN-Port X1-WAN-Port | 12V DC 2A Stromversorgung

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.

Technische Daten	TZ400 Series
Firewall-Durchsatz	1,3 GBit/s
Threat-Prevention-Durchsatz	600 MBit/s
Anti-Malware-Durchsatz	600 MBit/s
IPS-Durchsatz	900 MBit/s
Maximale Anzahl von Verbindungen	150.000
Neue Verbindungen/Sekunde	6.000

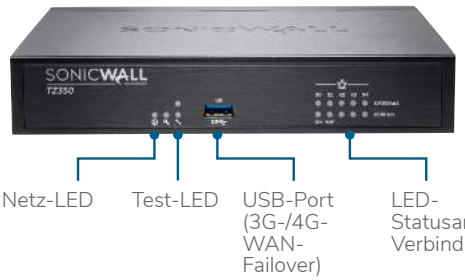


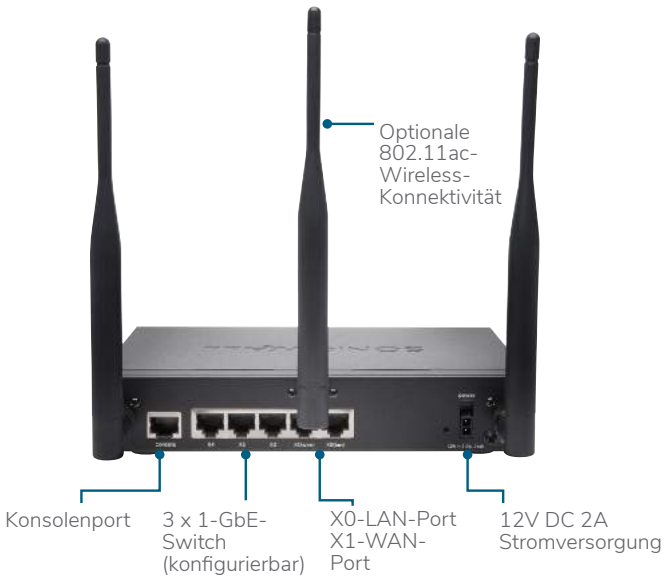


SonicWall TZ350/TZ300 Series

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.

Technische Daten	TZ350 Series	TZ300 Series
Firewall-Durchsatz	1,0 GBit/s	750 MBit/s
Threat-Prevention-Durchsatz	335 MBit/s	235 MBit/s
Anti-Malware-Durchsatz	300 MBit/s	200 MBit/s
IPS-Durchsatz	400 MBit/s	300 MBit/s
Maximale Anzahl von Verbindungen	100.000	100.000
Neue Verbindungen/Sekunde	6.000	5.000





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.

Technische Daten	SOHO 250 Series	SOHO Series
Firewall-Durchsatz	600 MBit/s	300 MBit/s
Threat-Prevention-Durchsatz	200 MBit/s	150 MBit/s
Anti-Malware-Durchsatz	100 MBit/s	50 MBit/s
IPS-Durchsatz	250 MBit/s	100 MBit/s
Maximale Anzahl von Verbindungen	50.000	10.000
Neue Verbindungen/Sekunde	3.000	1.800

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

Optionale 802.11n-Wireless-Konnektivität

Konsolenport | 3 x 1-GbE-Switch (konfigurierbar) | X0-LAN-Port X1-WAN-Port | 12V DC 2A Stromversorgung

Partner Enabled Services

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

Features

RFDPI-ENGINE	
Funktion	Beschreibung
Reassembly-Free Deep Packet Inspection (RFDPI)	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.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxys stattfindet, lassen sich Millionen gleichzeitiger Datenströme mit der DPI-Technologie bei minimalen Latenzzeiten scannen, ohne dabei das Datenvolumen oder die Dateigrößen einzuschränken. Dies funktioniert sowohl bei gängigen Protokollen als auch bei Raw-TCP-Streams.
Hohe Parallelität und Skalierbarkeit	Gemeinsam mit der Multicore-Architektur ermöglicht das einzigartige Design der RFDPI-Engine einen hohen DPI-Durchsatz sowie extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen. Verkehrsspitzen in anspruchsvollen Netzwerken lassen sich so besser bewältigen.
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.

FIREWALL UND NETZWERK	
Funktion	Beschreibung
Sicheres SD-WAN	Mit einem sicheren SD-WAN können verteilte Unternehmen geschützte, leistungsstarke Netzwerke über Remote-Standorte hinweg aufbauen, betreiben und verwalten, ohne auf kostspieligere Technologien wie MPLS zurückgreifen zu müssen. Auf diese Weise können sie Daten, Anwendungen und Services mithilfe einfach verfügbarer und erschwinglicher öffentlicher Internetdienste bereitstellen.
REST-APIs	Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Diese nutzt diese, um komplexe Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv zu bekämpfen.
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall-Zugriffsregeln erfüllt werden.
Hochverfügbarkeit/Clustering	Die SonicWall TZ500- und TZ600-Modelle unterstützen Hochverfügbarkeit mit Active/Standby und State-Synchronisierung. Die SonicWall TZ300- und TZ400-Modelle unterstützen Hochverfügbarkeit ohne Active-/Standby-Synchronisierung. Auf den SonicWall SOHO-Modellen wird Hochverfügbarkeit nicht unterstützt.
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.
IPv6-Unterstützung	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) ist noch nicht abgeschlossen. Mit SonicOS unterstützt die Hardware Filtering- und Wire-Implementierungsmodi.
Flexible Implementierungsoptionen	Die TZ Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden.
Verbesserte QoS (Quality of Service)	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
H.323-Gatekeeper- und SIP-Proxy-Support	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom H.323-Gatekeeper oder SIP-Proxy autorisiert und authentifiziert werden müssen.
Verwaltung einzelner und hintereinander geschalteter Switches der Dell N-Series und X-Series	Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich Portshield, HA, PoE und PoE+ über eine zentrale Stelle mithilfe des Firewall-Management-Dashboards für Dells Netzwerk-Switches der N-Series und X-Series (nicht für SOHO-Modelle verfügbar).
Biometrische Authentifizierung	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.
Offene Authentifizierung und Social Login	Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.
Sicherheit für Wireless-Netzwerke	Als integrierte Option für SonicWall TZ300- bis TZ500-Firewalls stellt die Wireless-Technologie nach dem IEEE-802.11ac-Standard einen Wireless-Durchsatz von bis zu 1,3 GBit/s mit größerer Signalreichweite und höherer Zuverlässigkeit sicher. Auf den SonicWall SOHO-Modellen ist optional 802.11a/b/g/n verfügbar.

VERWALTUNG UND REPORTING	
Funktion	Beschreibung
Cloud-basierte und lokale Verwaltung	Die SonicWall Appliances lassen sich über die Cloud durch das SonicWall Capture Security Center sowie lokal durch das SonicWall Global Management System (GMS) konfigurieren und verwalten.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende Befehlszeilenschnittstelle und bietet Support für 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 sowie die Berichterstellung mit Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, zu ermöglichen.

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 leistungsstarkem IPSec-VPN kann die TZ Series als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home-Offices eingesetzt 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	Bereitstellung von Informationen zur Benutzerkennung und -aktivität, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix1/Terminal Services1 sowie umfassenden DPI-Daten basieren.
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. Es besteht die Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben. Eliminiert unerwünschtes Filtering von IP-Adressen aufgrund einer Fehlklassifikation.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern. Es besteht die Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben.
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.
Real-Time Deep Memory Inspection (RTDMI)	Diese zum Patent angemeldete Cloud-basierte Technologie ist in der Lage, Malware, die kein bösartiges Verhalten zeigt oder ihre Mechanismen durch Verschlüsselungsmethoden verschleiert, zu identifizieren und zu blockieren. Die RTDMI-Engine zwingt Malware dazu, ihre Wirkmechanismen im Speicher offenzulegen. So ist sie imstande, die in großer Zahl vorkommenden Zero-Day-Bedrohungen sowie unbekannte Malware aufzudecken und abzuwehren.
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.
Analyse unterschiedlichster Dateitypen und- größen	Der Service unterstützt die Analyse unterschiedlichster Dateitypen (entweder einzeln oder als Gruppe), darunter ausführbare Programme (PE), DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme wie Windows, Android, Mac OS X 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 ATP-Abos aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt.
Capture Client	Capture Client ist eine einheitliche Client-Plattform mit mehreren Funktionen für die Endpunktsicherheit, darunter einem hoch entwickelten Malware-Schutz und einem umfassenden Einblick in den verschlüsselten Datenverkehr. Die Plattform bietet mehrschichtige Sicherheitstechnologien, umfassendes Reporting und einen zuverlässigen Endpunktschutz.
SCHUTZ VOR VERSCHLÜSSELTEN BEDROHUNGEN	
Funktion	Beschreibung
TLS-/SSL-Entschlüsselung und -Prüfung	Proxylose On-the-Fly-Entschlüsselung und -Prüfung von TLS-/SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im verschlüsselten Verkehr lauern. Dieser Service ist bei allen TZ-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.

INTRUSION-PREVENTION (FORTSETZUNG)	
Funktion	Beschreibung
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.
Malware-Schutz durch Capture Cloud	Eine kontinuierlich aktualisierte Datenbank mit mehreren 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.
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 Tausenden von 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 sämtlicher nicht notwendige 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 und Content Filtering Client lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und HTTP-/HTTPS-Websites mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren.
Enforced Content Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewallgrenze zu blockieren.
Granulare Kontrolle	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.
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, geeignete Antivirensoftware und/oder DPI-SSL-Zertifikate installiert und aktiviert sind. Somit entfallen die Kosten, die typischerweise für die Verwaltung desktopbasierter Virenschutzlösungen 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.
Virenschutz der nächsten Generation	Capture Client nutzt eine statische Artificial-Intelligence(AI)-Engine, um Bedrohungen zu identifizieren, bevor sie ausgeführt werden. Darüber hinaus ermöglicht Capture Client ein Rollback auf einen Zustand vor der Infizierung.
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.

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
- REST-APIs

SSL-/SSH-Entschlüsselung und -Prüfung[1]
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- TLS-/SSL-Kontrolle
- Granulare DPI-SSL-Kontrollen nach Zone oder Regel

Capture Advanced Threat Protection[1,2]
- 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[1]
- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- GeoIP-/Botnet-Filtering[2]
- Abgleich regulärer Ausdrücke

Anti-Malware[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
- 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[1]
- URL-Filterung
- Anti-Proxy-Technologie
- 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
- 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
- Sicheres SD-WAN
- PortShield
- Erweiterte Protokollierung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- 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
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mit SonicWall GMS und Capture Security Center
- Logging
- NetFlow-/IPFIX-Export
- Cloud-basiertes Konfigurationsbackup
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinander geschalteten Switches[2]

Integrierte Wireless-Optionen
- Dualband (2,4 GHz und 5 GHz)
- 802.11 a/b/g/n/ac-Wireless-Standards[2]
- WIDS/WIPS
- Wireless Guest Services
- Lightweight Hotspot Messaging
- Segmentierung mithilfe virtueller Access-Points
- Captive Portal
- Cloud ACL

[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

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]	100 MBit/s	250 MBit/s	300 MBit/s	400 MBit/s
Anti-Malware-Inspection-Durchsatz[2]	50 MBit/s	100 MBit/s	200 MBit/s	300 MBit/s
Durchsatz bei TLS/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	30 MBit/s	40 MBit/s	50 MBit/s	65 MBit/s
IPSec-VPN-Durchsatz[3]	100 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)	1 (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			
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 (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)

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			
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 (Firewall und IPS)			
Common Access Card (CAC)	unterstützt			
Hochverfügbarkeit	Nein		Active/Standby	
HARDWARE	**SOHO SERIES**	**SOHO 250 SERIES**	**TZ300 SERIES**	**TZ350 SERIES**
Formfaktor	Desktop			
Stromversorgung	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		3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm
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	1,2 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			
KONFORMITÄT	**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		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	
Konformität mit wichtigen Normen (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMV, 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, EMV, LVD, 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[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		802.11a: 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)

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 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	
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 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 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 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.

SonicWall TZ Series – Systemdaten (Fortsetzung)

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 Ports (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]	150 MBit/s	200 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		
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 (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)

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		
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 (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		
Stromversorgung	24 W (extern)	36 W (extern)	60 W (extern) 180 W (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	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
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		
KONFORMITÄT	**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	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
Konformität mit wichtigen Normen (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMV, 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, EMV, 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	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: 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; 802.11ac: 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 und 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)		—

Produkt	Artikelnummer
SOHO mit TotalSecure (1 Jahr)	01-SSC-0651
SOHO Wireless-N mit TotalSecure (1 Jahr)	01-SSC-0653
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
TZ600 mit TotalSecure Advanced Edition (1 Jahr)	01-SSC-1711
TZ600P mit TotalSecure Advanced Edition (1 Jahr)	02-SSC-0600
Optionen für Hochverfügbarkeit (nur Geräte des gleichen Modells)	
TZ500 High Availability	01-SSC-0439
TZ600 High Availability	01-SSC-0220

Dienste	Artikelnummer
Für die SonicWall SOHO Series	
Comprehensive Gateway Security Suite - Threat Prevention, Content Filtering und 24/7 Support (1 Jahr)	01-SSC-0688
Gateway Anti-Virus, Intrusion Prevention und 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 die SonicWall SOHO 250 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering 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, Content Filtering 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, Content Filtering 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
Für die SonicWall TZ400 Series	
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering 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, Content Filtering 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, Content Filtering 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

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
TZ400/TZ400 Wireless	APL28-0B4/APL28-0B5
TZ500/TZ500 Wireless	APL28-0B4/APL28-0B5
TZ350/TZ350 Wireless	APL29-0B6/APL29-0B7
TZ600/TZ600P	APL30-0B8/APL48-0D3

Über SonicWall

SonicWall kämpft seit über 27 Jahren gegen Cyberkriminalität und verteidigt kleine und mittelständische Betriebe, größere Unternehmen und Regierungsbehörden weltweit. Unsere preisgekrönten Lösungen zur Erkennung und Prävention von Datenschutzverletzungen in Echtzeit bauen auf der Forschung aus den SonicWall Capture Labs auf und sichern mehr als eine Million Netzwerke sowie E-Mails, Anwendungen und Daten in mehr als 215 Ländern und Gebieten. Die betreffenden Organisationen können sich besser auf ihr Geschäft konzentrieren und müssen sich weniger um ihre Sicherheit sorgen. Weitere Informationen finden Sie auf www.sonicwall.com oder folgen Sie uns auf Twitter, LinkedIn, Facebook und Instagram.

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

Datasheet-TZ Series-US-VG-MKTG5144