SonicWALL TZ Series

Herausragende Sicherheit und exzellente Leistung bei revolutionär niedrigen Gesamtbetriebskosten

Die Dell SonicWALL TZ Series Firewalls sind hochleistungsfähige Netzwerksicherheitslösungen der Enterprise-Klasse, die auf das begrenzte Budget und die eingeschränkten Ressourcen von kleinen und mittleren Unternehmen (KMUs), Remote- und Zweigniederlassungen sowie Verkaufsstandorten im Einzelhandel zugeschnitten sind.

Dank modernster Sicherheitsservices mit einer Kombination aus integrierten und cloudbasierten Funktionen für Malware-Schutz, Spyware-Schutz, Angriffsvermeidung (IPS, Intrusion Prevention System) sowie URL-Filterung bieten die SonicWALL TZ Series Firewalls umfassende Sicherheit. Da die Anzahl an Angriffen, die in verschlüsselten Paketen eingebettet sind, kontinuierlich steigt, bietet die neue SonicWALL TZ Series die Verarbeitungsleistung, die Sie benötigen, um verschlüsselte SSL-Verbindungen auf die neuesten Bedrohungen hin zu prüfen.

Über das Dell SonicWALL Global Response Intelligent Defense (GRID) Netzwerk werden SonicWALL TZ Series Systeme kontinuierlich mit Aktualisierungen versorgt und können so eine starke Verteidigungslinie gegen Cyberkriminelle um Ihr Netzwerk ziehen. Die SonicWALL TZ Series scannt jedes Byte in jedem Paket, auf allen Ports und für alle Protokolle – und das ohne jegliche Beschränkung der Dateigröße und fast ohne Latenz.

Zu ihrem Leistungsumfang gehören Gigabit-Ethernet-Ports, optionale integrierte 802.11ac-Wireless-Konnektivität, IPsec und SSL-VPN, Failover dank integrierter 3G/4G-Unterstützung, Lastausgleich und Netzwerksegmentierung. Damit gibt sie Ihnen die erweiterten Netzwerkfunktionen und modernen Sicherheitsoptionen an die Hand, die Sie heute benötigen. Für schnellen und sicheren Mobilzugriff bieten die Unified Threat Management (UTM)-Firewalls der SonicWALL TZ Series breite Unterstützung für native VPN-Clients für Remote-Zugriff – für Apple iOS, Google Android, Amazon Kindle, Windows sowie Mac OS und Linux Plattformen.

Das Dell SonicWALL Global Management System (GMS) ermöglicht die zentrale Bereitstellung und Verwaltung aller Ihrer SonicWALL TZ Series Firewalls über ein einziges System an Ihrem Hauptstandort.

Kompromisslose Sicherheit für Ihr Geschäft

Wollen KMUs wachsen, sind neue Technologien wie Mobilität und Cloud Computing unverzichtbar. Durch sie steigt aber auch das Risiko, dass die Unternehmen Opfer bösartiger Angriffe werden. Firmen jeder Größe benötigen daher vollständigen Schutz. Die SonicWALL TZ Series bietet deshalb eine integrierte Lösung, die den gesamten Netzwerkdatenverkehr überprüft, einschließlich der verschlüsselten SSL-Verbindungen.

Verwaltete Sicherheit für verteilte Umgebungen

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

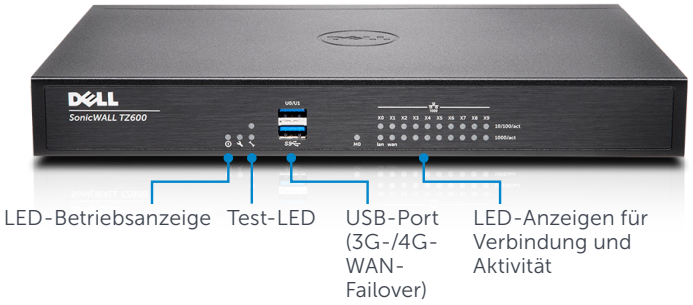
Vorteile:

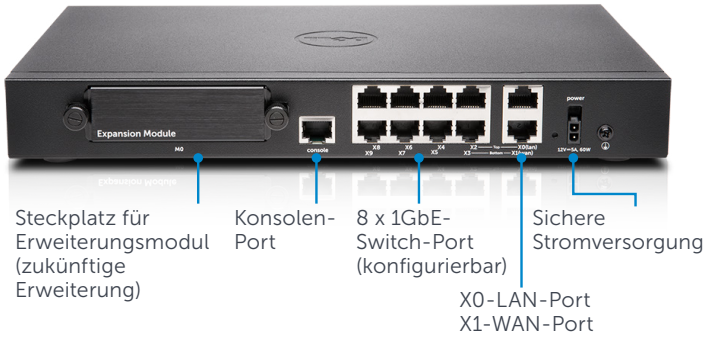
- Netzwerksicherheit der Enterprise-Klasse, die Malware-Schutz, Angriffsvermeidung, Anwendungskontrolle sowie Inhalts- und URL-Filterung umfasst
- Deep Packet Inspection für den gesamten Datenverkehr, einschließlich verschlüsselter SSL-Verbindungen – ganz ohne Einschränkungen bei Dateigröße oder Protokoll
- Sichere 802.11ac-Wireless-Konnektivität über einen integrierten Wireless-Controller oder mithilfe externer Dell SonicPoint Wireless-Zugriffspunkte
- SSL-VPN-Remote-Zugriff für Apple iOS, Google Android, Amazon Kindle, Windows, Mac OS und Linux Geräte

SonicWALL TZ600 Series

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

Technische Daten	TZ600 Series
Firewall-Datendurchsatz	1,5 Gbit/s
Datendurchsatz bei vollständiger DPI	500 Mbit/s
Datendurchsatz bei Malware-Schutz	500 Mbit/s
IPS-Datendurchsatz	1,1 Gbit/s
IMIX-Datendurchsatz	900 Mbit/s
Maximale Anzahl an DPI-Verbindungen	125.000
Neue Verbindungen/Sekunde	12.000





SonicWALL TZ500 Series

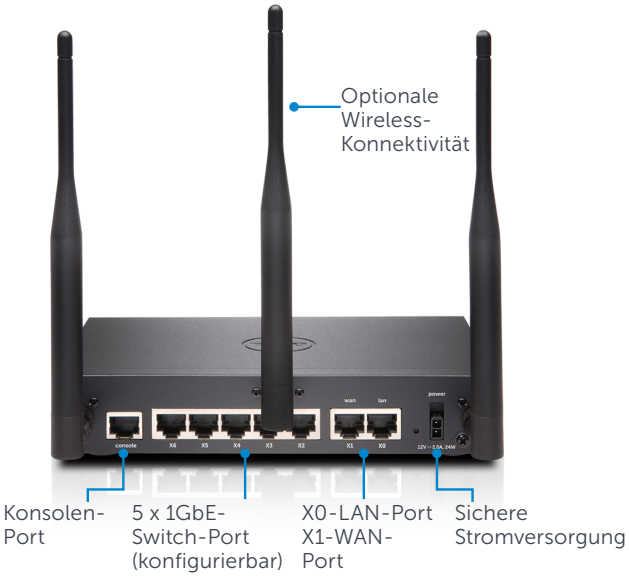
Wachsenden Zweigstellen und KMUs bietet die Dell SonicWALL TZ500 Series hoch effektiven, kompromisslosen Schutz bei hoher Netzwerkproduktivität sowie optionale integrierte Dualband-Wireless-Konnektivität gemäß dem 802.11ac-Standard.

Technische Daten	TZ500 Series
Firewall-Datendurchsatz	1,4 Gbit/s
Datendurchsatz bei vollständiger DPI	400 Mbit/s
Datendurchsatz bei Malware-Schutz	400 Mbit/s
IPS-Datendurchsatz	1 Gbit/s
IMIX-Datendurchsatz	700 Mbit/s
Maximale Anzahl an DPI-Verbindungen	100.000
Neue Verbindungen/Sekunde	8.000

SonicWALL TZ400 Series

Die Dell SonicWALL TZ400 Series bietet Schutz der Enterprise-Klasse für kleine Unternehmen, Einzelhandels- und Zweigniederlassungen. Optional ist flexible Wireless-Bereitstellung möglich, entweder über externe SonicPoint Zugriffspunkte oder die im Gerät integrierte 802.11ac-Wireless-Funktion.

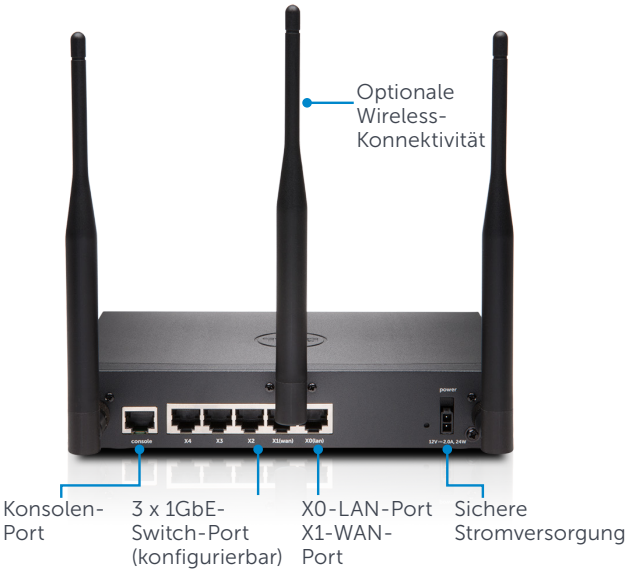
Technische Daten	TZ400 Series
Firewall-Datendurchsatz	1,3 Gbit/s
Datendurchsatz bei vollständiger DPI	300 Mbit/s
Datendurchsatz bei Malware-Schutz	300 Mbit/s
IPS-Datendurchsatz	900 Mbit/s
IMIX-Datendurchsatz	500 Mbit/s
Maximale Anzahl an DPI-Verbindungen	90.000
Neue Verbindungen/Sekunde	6.000



SonicWALL TZ300 Series

Die Dell SonicWALL TZ300 Series ist eine All-in-One-Lösung, die Netzwerke wirksam vor Angriffen schützt. Die SonicWALL TZ300 Series Firewall kombiniert effektive Funktionen für Malwareschutz, Angriffsvermeidung und Inhalts-/URL-Filterung mit optionaler integrierter 802.11ac-Wireless-Konnektivität und bietet die derzeit breiteste sichere Mobilplattformunterstützung für Notebooks, Smartphones und Tablet-PCs.

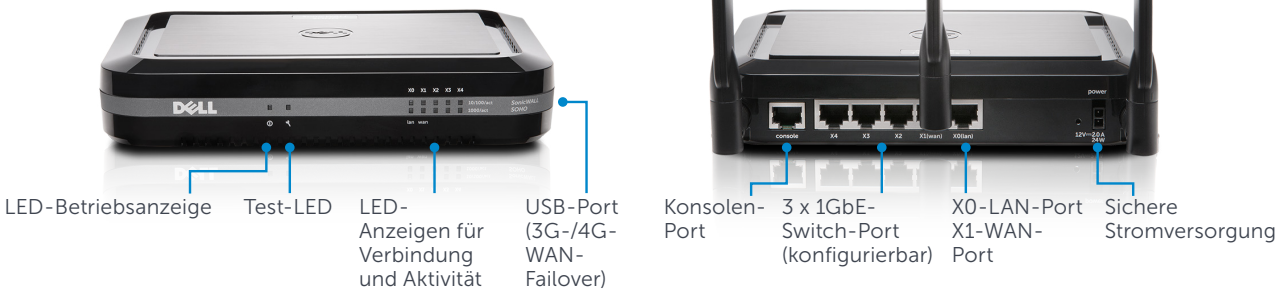
Technische Daten	TZ300 Series
Firewall-Datendurchsatz	750 Mbit/s
Datendurchsatz bei vollständiger DPI	100 Mbit/s
Datendurchsatz bei Malware-Schutz	100 Mbit/s
IPS-Datendurchsatz	300 Mbit/s
IMIX-Datendurchsatz	200 Mbit/s
Maximale Anzahl an DPI-Verbindungen	50.000
Neue Verbindungen/Sekunde	5.000



SonicWALL SOHO Series

Die Dell SonicWALL SOHO Series bietet kleinen Unternehmen und Heimbüros mit kabelgebundenen oder Wireless-Netzwerken den Schutz der Enterprise-Klasse, den auch große Organisationen benötigen – zu einem erschwinglicheren Preis.

Technische Daten	SOHO Series
Firewall-Datendurchsatz	300 Mbit/s
Datendurchsatz bei vollständiger DPI	50 Mbit/s
Datendurchsatz bei Malware-Schutz	50 Mbit/s
IPS-Datendurchsatz	100 Mbit/s
IMIX-Datendurchsatz	60 Mbit/s
Maximale Anzahl an DPI-Verbindungen	10.000
Neue Verbindungen/Sekunde	1.800

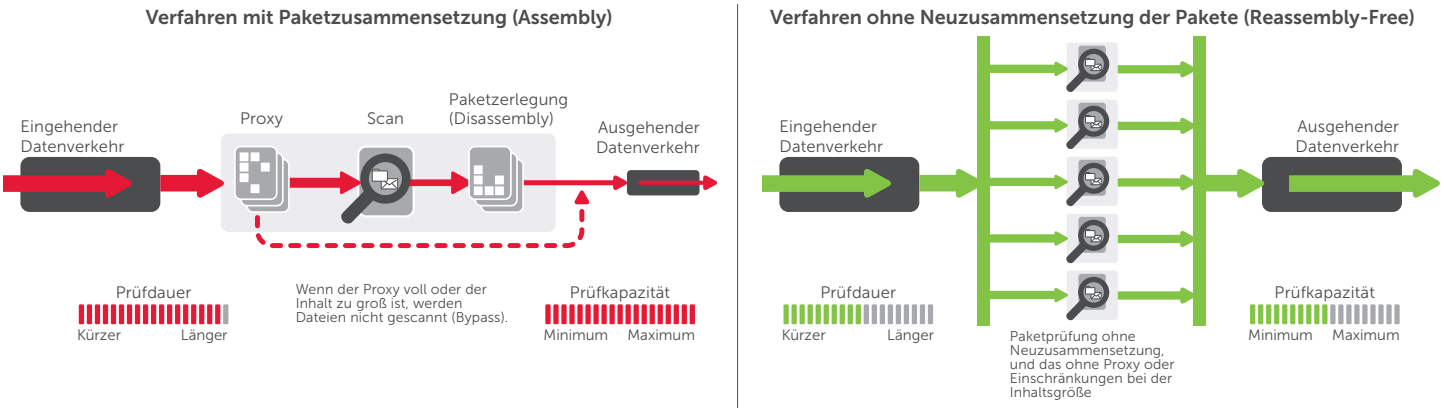


Globale Verwaltung und globales Reporting

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

Reassembly Free Deep Packet Inspection (RFDPI) Engine

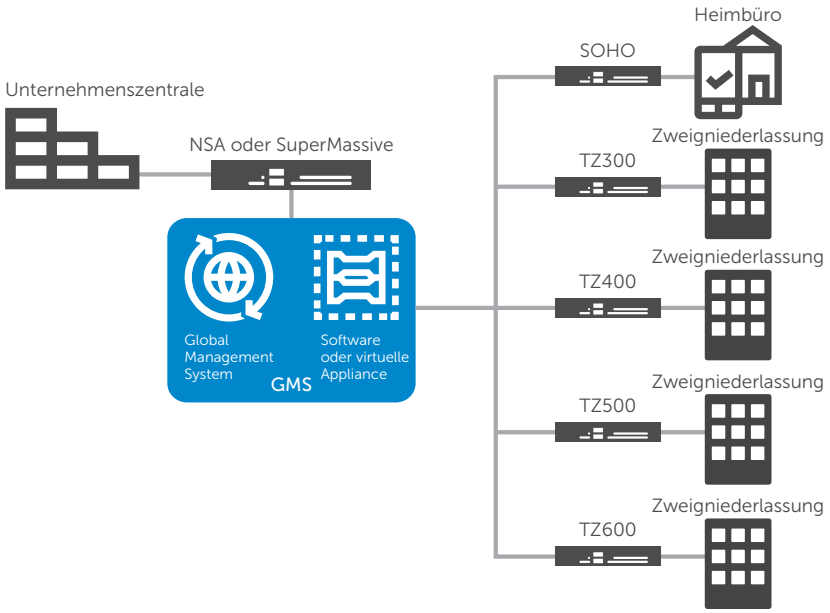
Die RFDPI Engine bietet ein herausragendes Niveau an Bedrohungsschutz und Anwendungskontrolle, ohne die Leistung zu beeinträchtigen. Dabei prüft die patentierte Engine den Daten-Stream, um Bedrohungen auf den Layern 3 bis 7 zu identifizieren. Die RFDPI Engine normalisiert und entschlüsselt den Netzwerkdatenverkehr mehrfach und umfassend. Auf diese Weise lassen sich sogenannte AET (Advanced Evasion Technique)-Attacken verhindern, die versuchen, Erkennungs-Engines durch die Kombination mehrerer Umgehungsverfahren zu verwirren und Schadcode in das Netzwerk einzuschleusen. Sobald ein Paket die erforderliche Vorverarbeitung durchlaufen hat (u. a. die SSL-Entschlüsselung), wird es mit einer einzigen, proprietären Speicherdarstellung dreier Signaturdatenbanken abgeglichen: Eindringversuche, Malware und Anwendungen. Anschließend wird der Verbindungsstatus kontinuierlich entsprechend der Position des Streams in Bezug auf diese Datenbanken angepasst, bis ein Angriff oder ein anderes Treffereignis identifiziert wird. Tritt dieser Fall ein, wird eine vordefinierte Aktion eingeleitet. Wird Malware erkannt, beendet die SonicWALL Firewall die Verbindung, bevor das Netzwerk kompromittiert werden kann, und protokolliert das Ereignis. Daneben bietet die Engine jedoch auch weitere Konfigurationsmöglichkeiten. So kann sie beispielsweise ausschließlich zur Überprüfung verwendet werden oder bei aktivierter Anwendungserkennung sofort nach Identifizierung einer Anwendung während des restlichen Anwendungs-Streams Bandbreitenverwaltungsservices auf Layer 7 bereitstellen.



Architektur von Mitbewerberlösungen | **Dell SonicWALL Architektur**

Erweiterbare Architektur für extreme Skalierbarkeit und Leistung

Die RFDPI Engine wurde von Grund auf so entwickelt, dass Sicherheitsscans bei hoher Leistung durchgeführt werden können. Damit ist sie perfekt auf den inhärent parallelen und stetig zunehmenden Datenverkehr in modernen Netzwerken abgestimmt. In Kombination mit Hardwaresystemen mit Multi-Core-Prozessoren lässt sich diese für parallele Verarbeitung optimierte Softwarearchitektur mühelos vertikal skalieren und ermöglicht so effiziente Deep Packet Inspection auch bei hoher Datenverkehrslast. Die SonicWALL TZ Series arbeitet mit Prozessoren, die – anders als x86-Plattformen – speziell auf die Verarbeitung von Paketen, verschlüsselten Daten sowie Netzwerkdatenverkehr ausgelegt sind und dabei gleichzeitig Flexibilität und Programmierbarkeit direkt am Kundenstandort garantieren. ASIC-Systeme können das nicht bieten. Diese Flexibilität ist besonders wichtig, wenn neue Code- und Verhaltens-Updates nötig sind, um sich vor neuen Angriffen zu schützen, die modernste und noch komplexere Erkennungsmethoden erfordern.

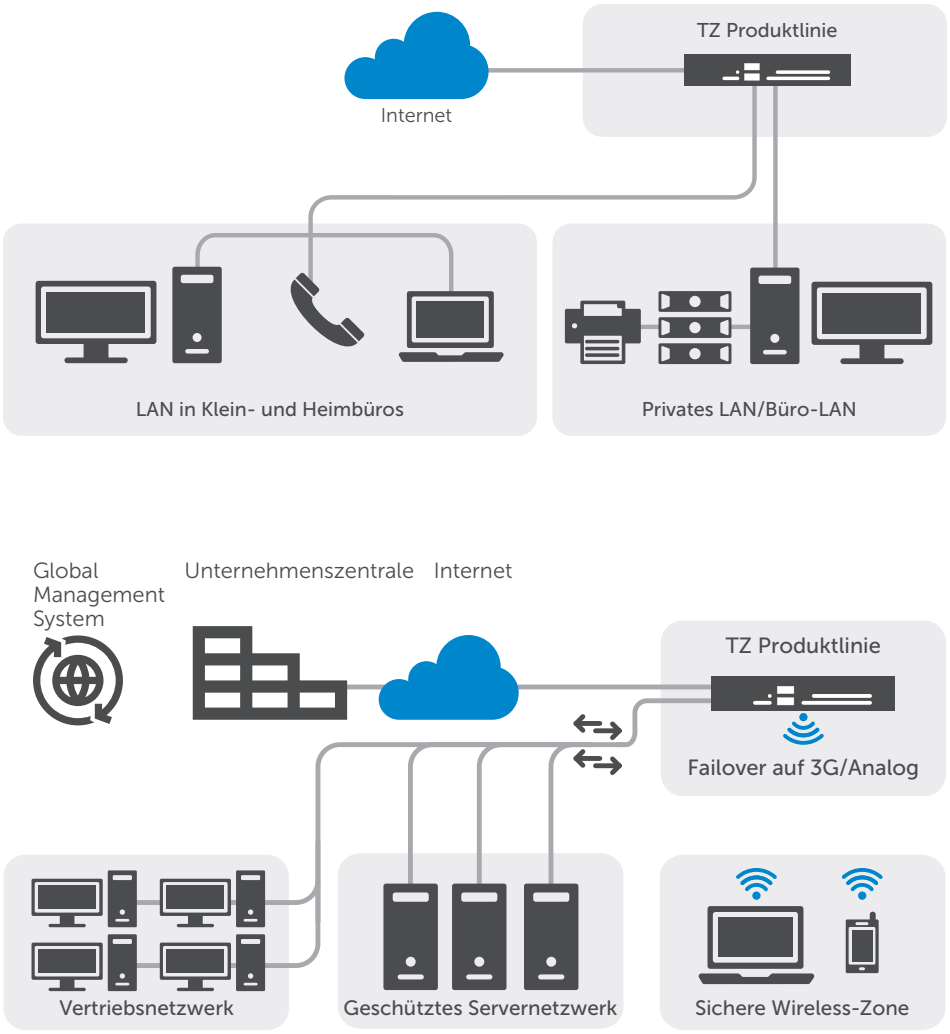


Sicherheit und Schutz

Das dedizierte interne Dell SonicWALL Threat Research Team ist für die Erforschung und Entwicklung von Abwehrmechanismen zuständig. Diese werden für die vor Ort bei unseren Kunden installierten Firewalls bereitgestellt, um jederzeit topaktuellen Schutz zu gewährleisten. Das Team greift dabei auf mehr als eine Million weltweit verteilte Sensoren zurück, die Malware-Muster und Telemetriedaten zu den neuesten Bedrohungen erfassen. Diese Informationen werden anschließend in die Systeme für Angriffsvermeidung, Malware-Schutz und Anwendungserkennung eingespeist. Kunden, die Dell SonicWALL Firewalls mit gültigen Abonnements einsetzen, erhalten rund um die Uhr aktualisierten Bedrohungsschutz. Neue Updates werden sofort implementiert – ohne Neustarts oder Betriebsunterbrechungen. Die Signaturen auf den Appliances bieten Schutz vor einer breiten Palette an Bedrohungen. Eine einzige Signatur deckt dabei bis zu mehrere Zehntausend Einzelbedrohungen ab. Zusätzlich zu den Abwehrmechanismen auf der Appliance selbst bieten alle Dell SonicWALL Firewalls auch Zugang zum Dell SonicWALL CloudAV Service. Auf diese Weise wird die lokal verfügbare Signaturdatenbank um einen kontinuierlich wachsenden Pool mit derzeit über 17 Millionen Signaturen erweitert. Der Firewall-Zugriff auf die CloudAV Datenbank erfolgt über ein schlankes, proprietäres Protokoll und ist eine leistungsstarke Ergänzung der Überprüfungsfunktionen der Appliance. Dank effizienter Funktionen für Geo-IP- und Botnet-Filterung sind die Dell SonicWALL Firewalls der nächsten Generation in der Lage, Datenverkehr aus gefährlichen Domänen oder ganzen Regionen zu blockieren, und können so die Sicherheitsrisiken im Netzwerk reduzieren.

Anwendungserkennung und -kontrolle

Über die Anwendungserkennung stehen Administratoren detaillierte Informationen zum Anwendungsdatenverkehr im Netzwerk zur Verfügung. So können sie die Anwendungskontrolle an den jeweils aktuellen Geschäftsprioritäten ausrichten, nicht produktive Anwendungen drosseln und potenziell gefährliche Anwendungen blockieren. Auffälligkeiten im Datenverkehr lassen sich dank Echtzeitvisualisierung augenblicklich identifizieren. So können unverzüglich Gegenmaßnahmen



eingeleitet werden, um das Netzwerk vor potenziellen Angriffen über ein- und ausgehenden Datenverkehr zu schützen oder Leistungsengpässe zu verhindern. Dell SonicWALL Application Traffic Analytics erlaubt granulare Einblicke in den Anwendungsdatenverkehr, die Bandbreitennutzung sowie etwaige Sicherheitsbedrohungen und bietet leistungsstarke Fehlerbehebungs- und Forensikfunktionen. Zusätzlich verbessern sichere Funktionen für die einmalige Anmeldung (Single Sign-On, SSO) die Benutzererfahrung und Produktivität und reduzieren die Anzahl an Support-Anfragen. Für eine vereinfachte Verwaltung der gesamten Anwendungserkennung und -kontrolle steht Ihnen eine intuitive, webbasierte Oberfläche zur Verfügung.

Flexible und sichere Wireless-Konnektivität

Die Dell SonicWALL Firewall-Technologie der nächsten Generation lässt sich optional mit High-Speed-Wireless-Technologie gemäß 802.11ac kombinieren. So entsteht eine Wireless-Netzwerksicherheitslösung, die umfassenden Schutz für kabellose und Wireless-Netzwerke bietet.

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

Funktionen und Merkmale

RFDPI Engine	
Funktion/Merkmal	Beschreibung
Reassembly-Free Deep Packet Inspection	Diese hochleistungsfähige proprietäre und patentierte Prüf-Engine führt eine streambasierte, bidirektionale Datenverkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsdatenverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Ein- und ausgehender Datenverkehr wird simultan auf Bedrohungen geprüft, um zu verhindern, dass das Netzwerk für die Verteilung von Malware oder als Ausgangspunkt für Angriffe genutzt wird, sollte ein infizierter Computer in die Umgebung gelangen.
Single-Pass-Inspection	Die Single-Pass-DPI-Architektur prüft den Datenverkehr simultan auf Malware und Eindringversuche und stellt Anwendungserkennung bereit. Dadurch werden DPI-bedingte Latenzzeiten deutlich verkürzt. Außerdem wird sichergestellt, dass sämtliche Bedrohungsdaten innerhalb einer einzigen Architektur verarbeitet werden.
Streambasierte Prüfung	Da die Prüfung ohne Proxys und Zwischenspeicherung stattfindet, können für mehrere Netzwerk-Streams gleichzeitig leistungsstarke DPI-Scans durchgeführt werden – bei ultraniedriger Latenz und ohne Einschränkungen bei Datei- oder Stream-Größe. Dabei kann die Engine nicht nur mit gängigen Protokollen, sondern auch mit reinen TCP-Streams umgehen.
Angriffsvermeidung	
Funktion/Merkmal	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes System zur Angriffsvermeidung (Intrusion Prevention System, IPS) nutzt Signaturen und andere Abwehrmechanismen, um den Paket-Payload auf Schwachstellen und Exploits zu prüfen. Dabei wird ein breites Spektrum an Angriffen und Schwachstellen abgedeckt.
Automatische Signatur-Updates	Das Dell SonicWALL Threat Research Team analysiert kontinuierlich Bedrohungen und aktualisiert fortlaufend unsere umfassende Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Neue Updates sind sofort wirksam und erfordern keine Neustarts oder sonstigen Serviceunterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Eine Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Angriffsvermeidung steigert die interne Sicherheit und verhindert, dass Bedrohungen sich über Zonengrenzen hinweg ausbreiten.
Erkennung und Blockierung von Command-and-Control-Aktivitäten (CnC) durch Botnets	Die Lösung identifiziert und blockiert Command-and-Control-Datenverkehr, der von Bots im lokalen Netzwerk zu IP-Adressen und Domänen gesendet wird, die als Malware-Quellen oder bekannte CnC-Punkte identifiziert wurden.
Protokollmissbrauch/-anomalien	Angriffe, bei denen versucht wird, das IPS durch Protokollmissbrauch zu umgehen, werden identifiziert und blockiert.
Zero-Day-Schutz	Dank kontinuierlicher Updates zu den neuesten Exploit-Methoden und -Techniken wird das Netzwerk effektiv gegen Zero-Day-Attacken geschützt. Dabei werden Tausende Einzel-Exploits abgedeckt.
Umgehungsschutztechnologie	Umfassende Stream-Normalisierung und -Entschlüsselung sowie weitere Maßnahmen verhindern, dass Angreifer Umgehungstechniken auf den Layern 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.
Bedrohungsabwehr	
Funktion/Merkmal	Beschreibung
Malware-Schutz am Gateway	Die RFDPI Engine prüft den gesamten Datenverkehr auf Viren, Trojaner, Keylogger und andere Malware – ohne Einschränkungen bei Dateilänge oder -größe und über alle Ports und TCP-Streams hinweg. Dabei wird sämtlicher eingehender und ausgehender Datenverkehr sowie sämtlicher Datenverkehr zwischen den verschiedenen Zonen untersucht.
CloudAV Malware-Schutz	Auf den Dell SonicWALL Cloud-Servern steht eine kontinuierlich aktualisierte Datenbank mit über 17 Millionen Bedrohungssignaturen bereit, die als Ergänzung zur integrierten Signaturdatenbank genutzt wird. So bietet die RFDPI Engine umfassenden Schutz vor einer breiten Palette an Bedrohungen.
Sicherheits-Updates rund um die Uhr	Neue Bedrohungs-Updates werden automatisch an Kunden-Firewalls mit aktiven Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne Neustart oder Betriebsunterbrechungen.
SSL-Entschlüsselung und -Prüfung	SSL-Datenverkehr wird in Echtzeit und ohne Umweg über einen Proxy entschlüsselt und auf Malware, Eindringversuche und Datenlecks überprüft. Gleichzeitig werden Richtlinien für Anwendungs-, URL- und Inhaltskontrolle angewendet, um das Netzwerk gegen versteckte Bedrohungen in SSL-verschlüsseltem Datenverkehr abzusichern. Dieser Service ist bei allen Modellen außer der SOHO in den Sicherheits-Abonnements inbegriffen. Für die SOHO ist er in Form einer separaten Lizenz verfügbar.
Bidirektionale Prüfung von reinem TCP-Datenverkehr	Die RFDPI Engine kann reine TCP-Streams auf jedem beliebigen Port bidirektional scannen. So werden Angriffe abgewehrt, die auf veraltete Sicherheitssysteme ausgelegt sind, bei denen nur einige weithin bekannte Ports abgesichert werden.
Unterstützung für zahlreiche Protokolle	Unsere Lösung identifiziert gängige Protokolle wie HTTP/S, FTP, SMTP, SMBv1/v2 und andere, die Daten nicht als reines TCP senden, und entschlüsselt die Payloads für die Malware-Prüfung – auch dann, wenn sie nicht über weithin bekannte Standardports laufen.
Anwendungserkennung und -kontrolle	
Funktion/Merkmal	Beschreibung
Anwendungskontrolle	Die RFDPI Engine nutzt eine kontinuierlich wachsende Datenbank mit über 3.500 Anwendungssignaturen, um Anwendungen oder einzelne Anwendungsfunktionen zu identifizieren und zu kontrollieren. Das steigert die Netzwerksicherheit und erhöht die Netzwerkproduktivität.
Identifizierung benutzerdefinierter Anwendungen	Die Lösung erstellt Signaturen für benutzerdefinierte Anwendungen, um die Kontrolle im Netzwerk weiter zu verstärken. Hierfür nutzt sie spezifische Parameter oder Muster, die für den Netzwerkdatenverkehr der betreffenden Anwendung charakteristisch sind.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenkapazität kann für kritische Anwendungen oder Anwendungskategorien granular zugewiesen und reguliert werden. Gleichzeitig lässt sich jedweder nicht absolut notwendiger Anwendungsdatenverkehr unterbinden.
Granulare Kontrolle	Die Lösung kontrolliert Anwendungen oder spezifische Anwendungskomponenten auf Basis von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten. Dank Integration mit LDAP/AD/Terminaldiensten/Citrix ist eine vollständige SSO-Benutzeridentifizierung möglich.
Inhaltsfilterung	
Funktion/Merkmal	Beschreibung
Interne/externe Inhaltsfilterung	Über den Content Filtering Service lassen sich Richtlinien zu Nutzungseinschränkungen effektiv erzwingen und Webseiten mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren. Mit dem Content Filtering Client kann die Richtlinienerzwingung zudem erweitert werden, um Internetinhalte auch auf Geräten außerhalb des Firewall-Perimeters zu blockieren.

Funktionen und Merkmale

Inhaltsfilterung	
Funktion/Merkmal	Beschreibung
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.
YouTube für Schulen	Lehrkräften stehen auf YouTube EDU Hunderttausende kostenlose Lernvideos zur Verfügung, die nach Themen und Bildungsstufe sortiert sind und allgemeinen Unterrichtsstandards entsprechen.
Webcaching	URL-Bewertungen werden lokal in der Dell SonicWALL Firewall zwischengespeichert, sodass die Reaktionszeiten bei erneuten Aufrufen häufig besuchter Webseiten nur Sekundenbruchteile betragen.
Erzwingung von Viren- und Spyware-Schutz	
Funktion/Merkmal	Beschreibung
Mehrstufiger Schutz	Die Firewall ist die erste Verteidigungsstufe am Netzwerkperimeter. Zusammen mit dem Endpunktschutz verhindert sie das Eindringen von Viren über Notebooks, USB-Sticks und andere ungeschützte Systeme.
Option für automatisierte Erzwingung	Es wird sichergestellt, dass auf jedem Computer, der auf das Netzwerk zugreift, die neueste Version der Signaturen für Viren- und Spyware-Schutz installiert und aktiviert ist. Das eliminiert die Kosten, die typischerweise für die Verwaltung von Desktop-Lösungen für Viren- und Spyware-Schutz entstehen.
Option für automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz müssen nicht auf jedem Rechner separat bereitgestellt und installiert werden. Bereitstellung und Installation werden automatisch und netzwerkweit durchgeführt, sodass der administrative Mehraufwand minimiert wird.
Unterbrechungsfreier und automatischer Virenschutz	Der Viren- und Spyware-Schutz wird häufig aktualisiert und transparent auf allen Desktop-PCs und Dateiservern bereitgestellt. Das sorgt für höhere Endbenutzerproduktivität und reduziert den Aufwand für die Sicherheitsverwaltung.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt Desktop-PCs und Notebooks auf eine umfangreiche Palette an Spyware-Programmen und blockiert deren Installation – bevor sie vertrauliche Daten übertragen können. Das steigert die Sicherheit und Leistung Ihrer Desktop-Umgebung.
Firewall und Netzwerkbetrieb	
Funktion/Merkmal	Beschreibung
Stateful Packet Inspection	Der gesamte Netzwerkdatenverkehr wird geprüft und analysiert. Dabei wird sichergestellt, dass Firewall-Zugriffsrichtlinien eingehalten werden.
Schutz vor DDoS-/DoS-Angriffen	Eine Kombination aus SYN-Proxy-Technologie auf Layer 3 und SYN-Blacklisting auf Layer 2 sorgt für SYN-Flood-Schutz und wehrt DOS-Angriffe ab. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
Flexible Bereitstellungsoptionen	Die SonicWALL TZ Series lässt sich im konventionellen NAT-Modus, als Layer 2-Bridge, im Wire-Modus oder im Network Tap-Modus bereitstellen.
IPv6-Unterstützung	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) hat gerade erst begonnen. Mit der neuesten Version des SonicOS Betriebssystems unterstützt die Hardware Implementierungen für Filterung.
Hochverfügbarkeit	Die SonicWALL TZ500 und SonicWALL TZ600 Firewalls unterstützen Hochverfügbarkeit mit Active/Standby und Zustandssynchronisierung. Die SonicWALL TZ300 und SonicWALL TZ400 Firewalls unterstützen Hochverfügbarkeit ohne Active/Standby-Synchronisierung. Auf den SonicWALL SOHO Modellen wird Hochverfügbarkeit nicht unterstützt.
Sicherheit für Wireless-Netzwerke	Die Wireless-Technologie nach IEEE 802.11ac-Standard stellt einen Wireless-Datendurchsatz von bis zu 1,3 Gbit/s mit größerer Signalreichweite und höherer Zuverlässigkeit bereit. Sie ist für die SonicWALL Modelle TZ600 bis TZ300 verfügbar. Auf den SonicWALL SOHO Modellen ist optional 802.11a/b/g/n verfügbar.
Verwaltung und Reporting	
Funktion/Merkmal	Beschreibung
Global Management System	Dell SonicWALL GMS gibt Ihnen eine einzige Verwaltungskonsole mit intuitiver Oberfläche an die Hand, mit der Sie mehrere Dell SonicWALL Appliances in Ihrem Netzwerk zentral überwachen und konfigurieren sowie Berichte erstellen können. Die Verwaltung wird kostengünstiger und einfacher.
Leistungsstarke Verwaltung auf Geräteebene	Eine intuitive, webbasierte Oberfläche ermöglicht eine schnelle und bequeme Konfiguration. Die Lösung stellt Ihnen außerdem eine umfassende Befehlsschnittstelle zur Verfügung und unterstützt SNMPv2/3.
IPFIX/NetFlow Berichte zum Anwendungsdatenverkehr	Analysedaten zum Anwendungsdatenverkehr und Daten zur Anwendungsnutzung lassen sich per IPFIX- oder NetFlow-Protokoll exportieren. Anschließend können sie von Tools wie Dell SonicWALL Scrutinizer und anderen Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, für Überwachung und Reporting genutzt werden – wahlweise in Echtzeit oder verlaufsbasiert.
VPNs (virtuelle private Netzwerke)	
Funktion/Merkmal	Beschreibung
IPsec-VPN für Site-to-Site-Konnektivität	Dank eines hochleistungsfähigen IPsec-VPNs kann die SonicWALL TZ Series als VPN-Konzentrator für Tausende anderer großer Standorte, Zweigstellen oder Heimbüros genutzt werden.
Remote-Zugriff per SSL-VPN oder IPsec-Client	Benutzer können mithilfe der clientlosen SSL-VPN-Technologie oder eines einfach zu verwaltenden IPsec-Clients unkompliziert auf E-Mails, Dateien, Computer, Intranetseiten und Anwendungen zugreifen, und das über eine Vielzahl verschiedener Plattformen.
Redundantes VPN-Gateway	Wenn Sie mit mehreren WANs arbeiten, können Sie ein primäres und ein sekundäres VPN konfigurieren und so für alle VPN-Sitzungen nahtloses automatisches Failover und Failback gewährleisten.
Routenbasiertes VPN	Dank dynamischem Routing über VPN-Links lässt sich auch beim temporären Ausfall eines VPN-Tunnels unterbrechungsfreier Betrieb gewährleisten. Der Datenverkehr zwischen den betroffenen Endpunkten wird nahtlos über alternative Routen geleitet.
Inhalts-/Kontextsensitivität	
Funktion/Merkmal	Beschreibung
Nachverfolgung von Benutzeraktivitäten	Dank nahtloser SSO-Integration von AD/LDAP/Citrix1/Terminaldiensten und umfassenden DPI-Daten können Benutzer identifiziert und Benutzeraktivitäten nachverfolgt werden.
Datenverkehrsidentifizierung nach Herkunftsland mittels Geo-IP	Die Lösung kann in bestimmte Länder gesendeten oder aus bestimmten Ländern stammenden Datenverkehr identifizieren und kontrollieren. So schützen Sie Ihr Netzwerk gegen Angriffe aus bekannten oder vermuteten Bedrohungsquellen und können verdächtigen Datenverkehr aus Ihrem Netzwerk analysieren.
DPI-Filterung mit regulären Ausdrücken	Alle Inhalte, die das Netzwerk passieren, können mithilfe regulärer Ausdrücke identifiziert und kontrolliert werden, um Datenlecks vorzubeugen.

SonicOS Funktions- und Merkmalsübersicht

Firewall
- Reassembly-Free Deep Packet Inspection
- Deep Packet Inspection für SSL
- Stateful Packet Inspection
- Stealth-Modus
- Unterstützung für Common Access Cards (CACs)
- Schutz vor DoS-Angriffen
- UDP-/ICMP-/SYN-Flood-Schutz
- SSL-Entschlüsselung
- IPv6-Sicherheit

Angriffsvermeidung
- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granulare IPS-Regeln
- Filterung auf Basis von Geo-IP und Reputation
- Abgleich mit regulären Ausdrücken

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

Anwendungskontrolle
- Anwendungskontrolle
- Blockierung von Anwendungskomponenten
- Bandbreitenverwaltung auf Anwendungsebene
- Signaturerstellung für benutzerdefinierte Anwendungen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Nachverfolgung der Benutzeraktivitäten (SSO)
- Umfassende Datenbank mit Anwendungssignaturen

Filterung von Webinhalten
- URL-Filterung
- Anti-Proxy-Technologie
- Schlüsselwortblockierung
- Bandbreitenverwaltung anhand von CFS Bewertungskategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- 57 Kategorien für die Inhaltsfilterung
- Content Filtering Service Client

VPN
- IPsec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPsec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS und Android™
- Routenbasiertes VPN (OSPF, RIP)

Netzwerk
- PortShield
- Layer 2-Netzwerkerkennung
- IPv6
- Erweiterte Protokollierung
- Portspiegelung
- Layer 2-QoS
- Portsicherheit
- Dynamisches Routing
- Richtlinienbasiertes Routing
- Asymmetrisches Routing
- DHCP-Server
- Bandbreitenverwaltung
- Active/Standby-Hochverfügbarkeitsmodus mit Zustandssynchronisierung*
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge, DDNS im NAT-Modus
- 3G-/4G-WAN-Failover

VoIP
- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- Unterstützung für H.323-Gatekeeper und SIP-Proxys

Verwaltung und Überwachung
- Webbasierte grafische Benutzeroberfläche
- Befehlsschnittstelle
- SNMPv2/v3
- Externes Reporting (Scrutinizer)
- Zentralisierte Verwaltung und zentrales Reporting
- Protokollierung
- NetFlow-/IPFIX-Export
- Visualisierung des Anwendungsdatenverkehrs
- Zentralisierte Richtlinienverwaltung
- Einmalige Anmeldung (Single Sign-On, SSO)
- Unterstützung für Terminaldienste/Citrix
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung

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

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

* Hochverfügbarkeit mit Zustandssynchronisierung nur für die Modelle SonicWALL TZ500 und SonicWALL TZ600 verfügbar

Systemspezifikationen SonicWALL TZ Series

Leistungsübersicht	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
Betriebssystem	SonicOS 5.9x/6.2.x	SonicOS 6.2.x			
Sicherheitsprozessor	2 x 400 MHz/ 2 x 800 MHz	2 x 800 MHz	4 x 800 MHz	4 x 1 GHz	4 x 1,4 GHz
Arbeitsspeicher (RAM)	512 MB/1 GB	1 GB	1 GB	1 GB	1 GB
Flash-Speicher	32 MB/64 MB	64 MB	64 MB	64 MB	64 MB
1GbE-Kupferschnittstellen	5	5	7	8	10
Erweiterung	USB	USB	USB	2 x USB	Erweiterungssteck-platz (hinten)*, 2 x USB
Datendurchsatz bei Firewall-Überprüfung[1]	300 Mbit/s	750 Mbit/s	1.300 Mbit/s	1.400 Mbit/s	1.500 Mbit/s
Datendurchsatz bei vollständiger DPI[2]	50 Mbit/s	100 Mbit/s	300 Mbit/s	400 Mbit/s	500 Mbit/s
Datendurchsatz bei Anwendungsüberprüfung[2]	–	300 Mbit/s	900 Mbit/s	1.000 Mbit/s	1.100 Mbit/s
IPS-Datendurchsatz[2]	100 Mbit/s	300 Mbit/s	900 Mbit/s	1.000 Mbit/s	1.100 Mbit/s
Datendurchsatz bei Malware-Überprüfung[2]	50 Mbit/s	100 Mbit/s	300 Mbit/s	400 Mbit/s	500 Mbit/s
IMIX-Datendurchsatz[3]	60 Mbit/s	200 Mbit/s	500 Mbit/s	700 Mbit/s	900 Mbit/s
Datendurchsatz bei SSL-Prüfung und -Entschlüsselung (DPI SSL)[2]	15 Mbit/s	45 Mbit/s	100 Mbit/s	150 Mbit/s	200 Mbit/s
IPsec-VPN-Datendurchsatz[3]	100 Mbit/s	300 Mbit/s	900 Mbit/s	1.000 Mbit/s	1.100 Mbit/s
Verbindungen pro Sekunde	1.800	5.000	6.000	8.000	12.000
Maximale Anzahl an Verbindungen (SPI)	10.000	50.000	100.000	125.000	150.000
Maximale Anzahl an Verbindungen (DPI)	10.000	50.000	90.000	100.000	125.000
Single Sign-On (SSO)-Benutzer	250	500	500	500	500
VLAN-Schnittstellen	25	25	50	50	50
Unterstützte SonicPoints (Maximum)	2	8	16	16	24
VPN	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600 Series**
Site-to-Site-VPN-Tunnel	10	10	20	25	50
IPsec-VPN-Clients (Maximum)	1 (5)	1 (10)	2 (25)	2 (25)	2 (25)
SSL-VPN-Lizenzen (Maximum)	1 (10)	1 (50)	2 (100)	2 (150)	2 (200)
Gebündelt mit Virtual Assist (Maximum)	–	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)	1 (30-Tage-Testversion)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit), MD5, SHA-1, Suite B Cryptography				
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14				
Routenbasiertes VPN	RIP, OSPF				
Unterstützte Zertifikate	Verisign, Thawte, CyberTrust, RSA Keon, Entrust und Microsoft Zertifizierungsstelle für Dell SonicWALL-zu-Dell SonicWALL-VPNs, SCEP				
VPN-Funktionen	Dead Peer Detection, DHCP über VPN, IPsec-NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN				
Unterstützte globale VPN-Clientplattformen	Microsoft® Windows Vista (32/64 Bit), Windows 7 (32/64 Bit), Windows 8.0 (32/64 Bit), Windows 8.1 (32/64 Bit)				
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, Windows 8.1 (Embedded)				
Sicherheitsservices	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600 Series**
Deep Packet Inspection-Services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	Prüfung auf HTTP-URLs, HTTPS-IPs, Schlüsselwörter und Inhalte, umfassende Filterung anhand von Dateitypen wie ActiveX, Java Applets und Cookies (für Datenschutz), individuelle Freigabe- und Sperrlisten				
Enforced Client Anti-Virus and Anti-Spyware	McAfee®				
Comprehensive Anti-Spam Service	Unterstützt				
Anwendungsvisualisierung	Nein	Ja	Ja	Ja	Ja
Anwendungskontrolle	Ja	Ja	Ja	Ja	Ja

Systemspezifikationen SonicWALL TZ Series

Netzwerk	SOHO Series	TZ300 Series	TZ400 Series	TZ500 Series	TZ600 Series
IP-Adresszuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, 1:n, n:1, n:n, flexible NAT (überlappende IPs), PAT, transparenter Modus				
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, richtlinienbasiertes Routing, Multicast				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)				
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix				
Lokale Benutzerdatenbank	150			250	
VoIP	Volle Unterstützung für H.323v1-5, SIP				
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPsec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Zertifizierungen	VPNC, IPv6 (Phase 2)				
Ausstehende Zertifizierungen	Common Criteria NDPP, FIPS 140-2 (mit Suite B) Level 2, ICSA Firewall, ICSA Anti-Virus, UC APL				
Common Access Card (CAC)	Unterstützt				
Hochverfügbarkeit	Nein	Active/Standby	Active/Standby	Active/Standby mit Stateful-Synchronisierung	Active/Standby mit Stateful-Synchronisierung
Hardware	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600 Series**
Formfaktor	Desktop				
Netzteil (W)	24 W (extern)	24 W (extern)	24 W (extern)	36 W (extern)	60 W (extern)
Maximaler Stromverbrauch (W)	6,4/11,3	6,9/12	9,2/13,8	13,4/17,7	16,1
Eingangsleistung	100 bis 240 V Wechselstrom, 50 bis 60 Hz, 1 A				
Gesamtwärmeabgabe	21,8/38,7 BTU	23,5/40,9 BTU	31,3/47,1 BTU	45,9/60,5 BTU	55,1 BTU
Abmessungen	3,6 x 14,1 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 13,4 x 19 cm	3,5 x 15 x 22,5 cm	3,5 x 18 x 28 cm
Gewicht	0,34 kg/0,75 lb 0,48 kg/1,06 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,73 kg/1,61 lb 0,84 kg/1,85 lb	0,92 kg/2,03 lb 1,05 kg/2,31 lb	1,47 kg/3,24 lb
WEEE-Gewicht	0,80 kg/1,76 lb 0,94 kg/2,07 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,15 kg/2,53 lb 1,26 kg/2,78 lb	1,34 kg/2,95 lb 1,48 kg/3,26 lb	1,89 kg/4,16 lb
Versandgewicht	1,2 kg/2,64 lb 1,34 kg/2,95 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,37 kg/3,02 lb 1,48 kg/3,26 lb	1,93 kg/4,25 lb 2,07 kg/4,56 lb	2,48 kg/5,47 lb
MTBF (Jahre)	30/15	28/14	27/13	20/12	18
Umgebung	0 bis 40 °C (40 bis 105 °F)				
Luftfeuchtigkeit	5 bis 95% (nicht kondensierend)				
Gesetzliche Vorschriften	**SOHO Series**	**TZ300 Series**	**TZ400 Series**	**TZ500 Series**	**TZ600 Series**
Vorschriftenmodell (kabelgebunden)	APL31-0B9	APL28-0B4	APL28-0B4	APL29-0B6	APL30-0B8
Einhaltung wichtiger gesetzlicher Vorschriften (kabelgebundene-Modelle)	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP	FCC Klasse B, ICES Klasse B, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse B, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, BSMI, KCC/MSIP	FCC Klasse A, ICES Klasse A, CE (EMV, LVD, RoHS), C-Tick, VCCI Klasse A, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH, KCC/MSIP
Vorschriftenmodell (drahtlos)	APL41-0BA	APL28-0B5	APL28-0B5	APL29-0B7	–
Einhaltung wichtiger gesetzlicher Vorschriften (Wireless-Modelle)	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	FCC Klasse B, FFC RF ICES Klasse B, IC RF CE (R&TTE, EMC, LVD, RoHS), RCM, VCCI Klasse B, MIC/TELEC, UL, cUL, TÜV/GS, CB, Mexiko CoC nach UL, WEEE, REACH	–

Systemspezifikationen SonicWALL TZ Series

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

* Zukünftige Nutzung
[1] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Netzwerkbedingungen und aktivierten Services variieren.
[2] Der Datendurchsatz bei vollständiger DPI/Virenschutz am Gateway/Spyware-Schutz/IPS wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia Testtools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt.
[3] Der VPN-Datendurchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.280 Byte. Änderungen von Spezifikationen, Funktionen und Verfügbarkeit vorbehalten.
[4] Nur für die Modelle SonicWALL TZ300, TZ400, TZ500 und TZ600 verfügbar

Bestellinformationen SonicWALL TZ Series

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

Services	SKU
Für die Dell SonicWALL SOHO	
• Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0688
• Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0670
• Content Filtering Service (1 Jahr)	01-SSC-0676
• Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0682
• Rund-um-die-Uhr-Support (1 Jahr)	01-SSC-0700
Für die Dell SonicWALL TZ300	
• Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0638
• Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0602
• Content Filtering Service (1 Jahr)	01-SSC-0608
• Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0632
• Rund-um-die-Uhr-Support (1 Jahr)	01-SSC-0620
Für die Dell SonicWALL TZ400	
• Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0567
• Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0534
• Content Filtering Service (1 Jahr)	01-SSC-0540
• Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0561
• Rund-um-die-Uhr-Support (1 Jahr)	01-SSC-0552
Für die Dell SonicWALL TZ500	
• Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0488
• Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0458
• Content Filtering Service (1 Jahr)	01-SSC-0464
• Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0482
• Rund-um-die-Uhr-Support (1 Jahr)	01-SSC-0476
Für die Dell SonicWALL TZ600	
• Comprehensive Gateway Security Suite (1 Jahr)	01-SSC-0258
• Gateway Anti-Virus, Intrusion Prevention and Application Control (1 Jahr)	01-SSC-0228
• Content Filtering Service (1 Jahr)	01-SSC-0234
• Comprehensive Anti-Spam Service (1 Jahr)	01-SSC-0252
• Rund-um-die-Uhr-Support (1 Jahr)	01-SSC-0246

Datasheet-SonicWALL-TZ Series-US-KS-26675