DATENBLATT

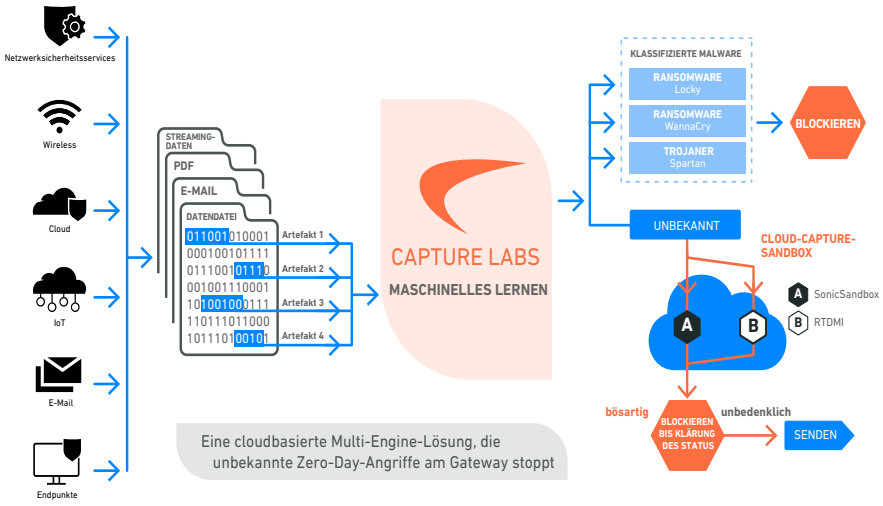
Gen 8: Architektur und Sicherheit

Robuster Schutz für eine sich ständig verändernde Bedrohungslandschaft

Die Gen-8-Produkte von SonicWall wurden für die Netzwerksicherheitsanforderungen kleiner und großer Unternehmen konzipiert, wie SOHOs (kleine Firmen, Homeoffices), KMUs (kleine und mittelständische Unternehmen) und dezentraler Unternehmen. Herzstück der Gen-8-Firewalls ist die SonicOS-Architektur.

SonicOS 8 sorgt neben Performance-Verbesserungen auch für eine konsistente und zuverlässige Netzwerksicherheit. Dieses Betriebssystem basiert auf unserer patentierten Reassembly-Free Deep Packet Inspection®(RFDPI)-Single-Pass-Engine mit niedriger Latenz und unserer ebenfalls patentierten Real-Time Deep Memory Inspection™(RTDMI)-Technologie und bietet eine hohe, bewährte Sicherheit, SD-WAN, Echtzeitvisualisierung, schnelles Virtual Private Networking (VPN) und weitere robuste Sicherheitsfunktionen.

Angesichts moderner Cyberbedrohungen, die sich ständig weiterentwickeln, stützt sich unsere Vision für die Netzwerksicherheit auf die automatisierte Echtzeiterkennung und -prävention. Eine Kombination aus cloudbasierten und integrierten Technologien ermöglicht höchste Firewall-Sicherheit, deren herausragende Effektivität von unabhängigen Drittanbietern getestet und bestätigt wurde. Verdächtige Dateien werden zur Analyse an die cloudbasierte SonicWall-Multi-Engine-Sandbox Capture Advanced Threat Protection (ATP) weitergeleitet. Wesentlicher Bestandteil von Capture ATP ist unsere RTDMI™-Technologie. Die RTDMI-Engine führt die Überprüfung direkt im Arbeitsspeicher aus und ist so in der Lage, Malware und Zero-Day-Bedrohungen zu erkennen und zu blockieren. Die Technologie arbeitet extrem präzise und reduziert die Anzahl von Falschmeldungen auf ein Minimum. Außerdem kann sie ausgeklügelte Angriffe dort identifizieren und abwehren, wo der schädliche Malware-Mechanismus für einen Augenblick von weniger als 100 Nanosekunden offengelegt wird.



Eine cloudbasierte Multi-Engine-Lösung, die unbekannte Zero-Day-Angriffe am Gateway stoppt

sonicwall.com

SONICWALL®

Gemeinsam mit unserer RFDPI-Engine lassen sich jedes einzelne Paket und jedes einzelne Byte durchleuchten. Dabei wird der ein- und ausgehende Datenverkehr in der Firewall auf Bedrohungen geprüft. Neben integrierten Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filterung verwenden unsere Next-Generation-Firewalls dabei auch Capture ATP mit RTDMI in der SonicWall Capture Cloud Platform, um Malware, Ransomware und andere Bedrohungen am Gateway zu stoppen.

SonicOS 8 bietet erweiterte Sicherheit, vereinfachte Regelverwaltung sowie kritische Netzwerk- und Managementfunktionen für KMUs und moderne Unternehmen mit SD-Branches der nächsten Generation. Das Betriebssystem unterstützt darüber hinaus Wi-Fi 6, erweiterte DNS-Sicherheit, reputationsbasierte Content-Filterung und NAC-Integration (NAC = Netzwerkzugangskontrolle).

Die Gen-8-Firewalls sind mit Zero-Trust-Network-Access(ZTNA)-Funktionen ausgestattet. Dieser Ansatz sorgt dafür, dass die Vertrauenswürdigkeit von Benutzern und Geräten mehrfach überprüft wird, bevor ein Zugriff auf bestimmte Anwendungen gewährt wird – unabhängig von Standort und Gerätetyp.

Der Management-Plan für Gen-8-Firewalls umfasst SonicWall Unified Management. SonicWall Unified Management bietet eine zentralisierte Konsole für die Verwaltung der Cybersecurity-Lösungen von SonicWall. Speziell für MSPs und MSSPs entwickelt, führt SonicWall Unified Management den kompletten Sicherheitsstack in einer einzigen Oberfläche zusammen, um grundlegende Sicherheitsprozesse einfacher und effizienter zu gestalten. Das Firewall-Management ist in allen Gen-8-Firewalls mit aktiven Support- oder Security-Bundles enthalten.

Security-Suites und Lizenzierungsoptionen

Mit den NGFWs von SonicWall können Unternehmen aus vereinfachten Lizenzierungsoptionen wählen, die ihren Anforderungen entsprechen. Mit dem neuesten Release – Gen 8 – besteht die Option, nur die Hardware zu erwerben (Hardware only)[1] oder Security-Suites mit und ohne verwaltete Firewall-Services zu beziehen[2]. Diese vereinfachte Lizenzierung verbessert den Schutz und die operative Effizienz unserer KMU- und Enterprise-Plattformen, ohne dass dabei mühsam mehrere Lizenzen einzeln verwaltet werden müssen. Darüber hinaus können Unternehmen mit den Security-Suites von SonicWall das Risiko finanzieller Verluste durch Sicherheitsvorfälle dank einer integrierten Cybergarantie von bis zu 200.000 USD mindern.

Die SonicWall Advanced Protection Security Suite (APSS) bietet erweiterte Sicherheitsdienste, Berichte und Analysen, um Ihre Netzwerke zu schützen sowie die Sichtbarkeit und operative Effizienz zu erhöhen. Diese Lizenzoption ist für Organisationen geeignet, die keine verwalteten Firewall-Services benötigen.

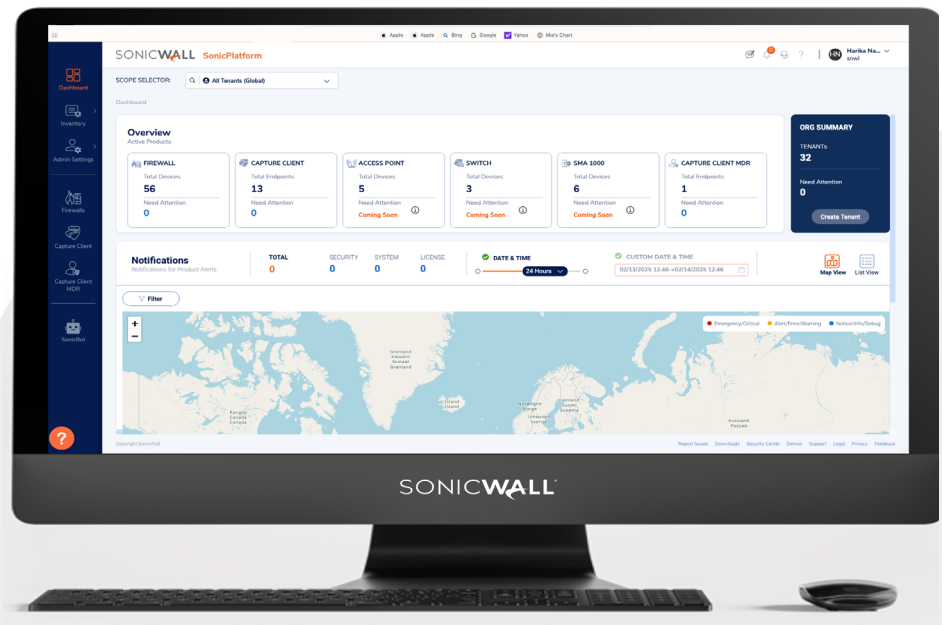
Die SonicWall Managed Protection Security Suite (MPSS) umfasst zusätzlich zu allen APSS-Diensten auch verwaltete Firewall-Services. Unser Team überwacht Ihre Firewall, informiert Sie bei Ausfällen oder lokalen Änderungen und verwaltet alle Firmware-Updates gemäß Ihrem Zeitplan.

[1] Die Hardware-only-Option ist nicht für die TZ80 verfügbar; diese erfordert eine abobasierte Lizenz.

[2] Für die TZ80 für SOHOs und IoT kommen folgende Optionen infrage: Secure Connect Lite, Secure Connect, Advanced Protection und Managed Protection Security Suites. Weitere Informationen entnehmen Sie bitte dem TZ80-Datenblatt.

Besuchen Sie unsere Seite zu den Security-Suites für mehr Infos.

Weitere Informationen



Verbessertes Dashboard

Verbessertes Dashboard

Feature	Beschreibung
DNS-Sicherheit	Nutzt das Domain Name System, um bösartige Websites oder Anwendungen zu blockieren und schädliche oder unangemessene Inhalte zu filtern.
Integration von Network Access Control (NAC)	Ermöglicht SonicWall-Kunden eine effektive Netzwerkzugriffskontrolle durch die Integration von Aruba ClearPass. Diese Architektur verwandelt eine statische Sicherheit in eine kontextbasierte Sicherheit, was einen flexibleren und solideren Schutz sicherstellt.
Wi-Fi-6-Unterstützung	Integration und Verwaltung von SonicWave-Access-Points mit Wi-Fi 6.
Funktionserweiterung für Sekundärspeicher	Unterstützung von Paketerfassung, TSR und Korrelation von Bedrohungsinformationen im Speicher. Folgende Protokolle können im Speicher abgelegt werden: Bedrohungs-, Audit-, Anwendungsfluss- und PCAP-Protokolle.
Tokenbasierte Registrierungen	Eine Zeichenfolge, die den Benutzernamen und das Passwort für MySonicWall in der Bootstrap-Datei ersetzt, die für das NS*v*-Bootstrapping genutzt wird, um umfangreiche Bereitstellungen mit grundlegenden Konfigurationen und Lizenzinformationen zu automatisieren.
NS*v*-Bootstrapping	Leichtere Durchführung umfangreicher NS*v*-Bereitstellungen, Unterstützung für VMware, Hyper-V, AWS und Azure, einfachere Produktregistrierungen mit tokenbasierter Lizenzierung; INIT-Datei beinhaltet grundlegende Konfiguration, um die Instanz mit minimalem Aufwand einsatzbereit zu machen.
Verbessertes Dashboard	Dashboard mit praktischen Warnhinweisen.
Optimierte Geräteansicht	Auf der Startseite der Benutzeroberfläche werden die Hardware in Vorder- und Rückansicht sowie die Speicherstatistiken angezeigt.
Echtzeitdaten zur System- und Bandbreitennutzung	Benutzer können jetzt Echtzeitdaten zur Systemnutzung (CPUs und Bandbreite) im Netzwerk einsehen.
Zusammengefasste Verteilung des Datenverkehrs	Benutzerbasierte Verteilung des Datenverkehrs in der Firewall mit Echtzeitinformationen zur am häufigsten genutzten Anwendung.
Übersicht der Top-Benutzer	Übersicht der Top-Benutzer basierend auf zugelassenen oder blockierten Sitzungen und gesendeten oder empfangenen Daten.
Übersicht der erfassten Bedrohungen	Echtzeitübersicht der erfassten Bedrohungen im Kundennetzwerk, z. B. Viren, Zero-Day-Malware, Spyware, Schwachstellen und riskante Anwendungen.
Serviceübersicht	Echtzeitstatus aktivierter oder deaktivierter Sicherheitsservices wie IPS, GAV, Anti-Spyware, Capture ATP oder DPI-SSL.
Informationen zu infizierten Hosts	Anzeige der Gesamtzahl infizierter Hostcomputer im Netzwerk in Echtzeit.
Informationen zu kritischen Angriffen	Anzeige der Gesamtzahl geschäftskritischer Angriffe im Netzwerk in Echtzeit.
Informationen zu verschlüsseltem Datenverkehr	Anzeige des gesamten verschlüsselten Datenverkehrs im Netzwerk in Echtzeit.
Übersicht der Top-Anwendungen	Anzeige der am häufigsten genutzten Anwendungen im Netzwerk mit zusätzlichen Sortieroptionen (nach Sitzungen, Byte, regelbasierten Blockierungen, Virus, Spyware und Eindringversuchen).
Übersicht der Top-Adressen	Anzeige der am häufigsten genutzten Adressobjekte im Netzwerk mit zusätzlichen Sortieroptionen (nach Sitzungen, Byte, regelbasierten Blockierungen, Virus, Spyware und Eindringversuchen).
Übersicht der Top-Benutzer	Anzeige der Top-Benutzer im Netzwerk mit zusätzlichen Sortieroptionen (nach Sitzungen, Byte, regelbasierten Blockierungen, Virus, Spyware und Eindringversuchen).
Übersicht der besten Website-Ratings	Anzeige der besten Website-Ratings nach Sitzung.
Übersicht der Top-Länderstatistiken	Anzeige der Top-Länderstatistiken nach Sitzung, verworfenem Datenverkehr, gesendeten oder empfangenen Bytes.
Übersicht der Echtzeitbedrohungen	Anzeige der Top-Bedrohungen mit separaten Statistiken für Viren, Eindringversuche, Spyware und Botnets nach Sitzungen.
Verbesserte Access-Point-Informationen	Anzeige von Statistiken zum Access-Point-Status im Netzwerk und Echtzeitstatistiken zu Client-Verbindungen.
Access-Point-Datenverkehrsrate	Echtzeitinformationen zur Bandbreitennutzung nach Access-Point.
WiFi-Client-Bericht	Echtzeitbericht zum WiFi-Client basierend auf OS-Typ, Frequenz und Top-Client-Tabelle.
Echtzeitüberwachung für WiFi-Clients	Ermittlung von Hostcomputer, OS-Typ, Frequenz, Access-Point-Informationen und Datenübertragungen.
Einblicke in Capture ATP-Ergebnisse	Anzeige der Dateianalyse-Ergebnisse von Capture ATP.
Einblicke in Dateitypen	Anzeige der Dateitypen aus dem Capture ATP-Bericht.
Einblicke in Zieladressen	Anzeige der Top-Ziele von bösartigen Dateien.
Malware-Analysestatistiken	Anzeige von ausführlichen Statistiken zur dynamischen und statischen Malware-Analyse je Datei.
Standortbasierte Ursprungsanalyse für Zero-Day-Angriffe	Anzeige des Angriffsursprungs nach Land.
Capture-ATP-Statistiken	Informationen zur Gesamtzahl der übermittelten Dateien, der dynamisch analysierten Dateien, der bösartigen Dateien und zur durchschnittlichen Verarbeitungszeit mit Capture ATP.
Topologieansicht des Netzwerks	Topologieansicht mit Hosts und verbundenen Access-Points im Netzwerk des Benutzers basierend auf Gerätename, MAC- und IP-Adresse.
API-gestütztes Management	Das Management der Firewall ist API-gestützt.
SD-WAN-Assistent	Assistent zur automatischen Konfiguration der Firewall-SD-WAN-Regeln.
Benachrichtigungszentrale	Neue Benachrichtigungszentrale mit Bedrohungsübersicht, Ereignisprotokollen und Systemwarnungen.
Verbesserte Onlinehilfe	Onlinehilfe mit Links zur technischen Dokumentation für jedes Modell.
SD-WAN-Überwachung	Anzeige von Stichproben zur SD-WAN-Performance und Top-Verbindungen.
Verbessertes Dienstprogramm zur Paketüberwachung	Paketüberwachung beinhaltet jetzt auch Zugriffsregeln, NAT-Regeln und Routeninformationen.
Speichergerätekonfiguration	Konfigurationsunterstützung für Speichermodule, einschließlich erweiterter Module. Statistiken zur Modulnutzung.

Capture Threat Assessment	Der Bericht unterstützt eine neue Berichtsvorlage mit Anpassungsoptionen wie Logo, Name und Bereichen. Unterstützung für Datei- und Malware-Analyse. Unternehmensstatistiken mit Branchen- und globalem Durchschnitt für jeden Bereich. Separate Vorlage für Führungskräfte mit Empfehlungen.
Download von Systemprotokollen	Systemprotokolle enthalten Konsolenprotokolle, die aus dem Diagnosebereich heruntergeladen werden können. Dadurch muss der Benutzer keine Verbindung zum Konsolenport herstellen, um diese Protokolle zu erfassen. Das vereinfacht das Debugging und beschleunigt die Fehlerbehebung.
SSH-Terminal in der Benutzeroberfläche	Das SSH-Terminal kann über die Web-UI aufgerufen werden.
Dienstprogramm zur GRID-Überprüfung	Dieses Dienstprogramm ermöglicht die Überprüfung der IP-Adresse der GRID-IP zu Diagnosezwecken.
Debugging-Utility	Benutzer können den Debug-Modus in derselben Firmware aktivieren und Debug-Befehle im SSH-Terminal über die UI ausführen.
Systemdiagnosetools	Unterstützung für weitere Diagnosetools wie GDB, HTOP und Linux perf.
Switch-Netzwerkübersicht	SonicWall-Switch-Ansicht wie physische Ansicht, Listenansicht und VLAN-Ansicht.
Bandbreitennutzung je Switch-Port	SonicWall-Switch-Informationen enthalten Daten zur Bandbreitennutzung je Port.
WWAN-Status	Anzeige des WWAN-Modem- und Netzwerkstatus.

Firewall-Funktionen und -Services

Reassembly-Free Deep Packet Inspection(RFDPI)-Engine

Feature	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	Dank ihres einzigartigen Designs und der Multi-Core-Architektur erreicht die RFDPI-Engine einen hohen DPI-Durchsatz und kann extrem viele neue Sitzungen pro Sekunde aufbauen. Verkehrsspitzen in anspruchsvollen Netzwerken lassen sich so souverän 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 Bedrohungsinformationen innerhalb einer einheitlichen Architektur verarbeitet werden.

Firewall und Networking

Feature	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. So können Daten, Anwendungen und Services mithilfe leicht zugänglicher und erschwinglicher öffentlicher Internetdienste bereitgestellt werden.
REST-API	Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Diese nutzt sie, um raffinierte 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 eingehalten werden.
Hochverfügbarkeit	Unterstützung von Active/Passive (A/P) mit Zustandssynchronisierung.
Schutz vor DDoS-/ DoS-Angriffen	Dank SYN-Flood-Schutz lassen sich DoS-Angriffe mit Layer-3-SYN-Proxy- und Layer-2-SYN-Blacklisting-Technologien abwehren. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
Flexible Implementierungsoptionen	Die Firewall lässt sich im Wire-, Netzwerk-Tap-NAT- oder Layer-2-Bridge-Modus implementieren.
WAN-Lastverteilung	Die Lösung ermöglicht die Lastverteilung über mehrere WAN-Schnittstellen hinweg. Zur Verfügung stehen verschiedene Optionen, wie Round Robin, Spillover und prozentbasierte Methoden. Regelbasiertes Routing sorgt für die Erstellung von protokollbasierten Routen für die Umleitung des Datenverkehrs auf eine bevorzugte WAN-Verbindung mit Failback-Möglichkeit auf ein sekundäres WAN bei einem Stromausfall.
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-Unterstützung	Alle eingehenden Anrufe müssen durch den H.323-Gatekeeper oder den SIP-Proxy autorisiert und authentifiziert werden. So werden Spam-Anrufe blockiert.
SonicWall-Switch-Integration	SonicWall-Switches lassen sich nahtlos in Firewalls integrieren und ermöglichen so eine zentrale Verwaltung und transparente Einblicke in das Netzwerk.

Verwaltung einzelner und hintereinandergeschalteter Switches der Dell N-Series und X-Series	Verwaltung der Sicherheitseinstellungen zusätzlicher Ports, einschließlich PortShield, HA, PoE und PoE+ über eine einzige Konsole mithilfe des Firewall-Management-Dashboards für Dells Netzwerk-Switches der N-Series und X-Series.
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 Benutzers 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.
Authentifizierung für mehrere Domänen	Erlaubt eine einfache und schnelle Verwaltung von Sicherheitsregeln über sämtliche Netzwerkdomänen hinweg. Verwaltung individueller Regeln für einzelne Domänen oder Domänengruppen.
Umfassende API-Unterstützung	Lückenlose API-Unterstützung für jeden Bereich der Firewall-UI.
SD-WAN-Skalierbarkeit	Skalierbare Tunnelschnittstellen für verteilte Unternehmen.

Management, Reporting und Unterstützung

Feature	Beschreibung
Cloudbasierte und lokale Verwaltung	Die SonicWall-Appliances lassen sich über den SonicWall Network Security Manager (NSM) on premises oder via Cloud konfigurieren und verwalten (verfügbar über SonicWall Unified Management).
Leistungsstarke Verwaltung einzelner Geräte	Neben einer umfassenden Befehlszeilenschnittstelle und SNMPv2/3-Unterstützung ermöglicht die intuitive webbasierte Oberfläche eine schnellere und einfachere Konfiguration.
IPFIX-/NetFlow-Berichte zum Anwendungsdatenverkehr	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Unterstützt wird auch die Berichterstellung mit SonicWall Analytics sowie anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.
Compliancebasierte Malware-Erkennung	Analyse verdächtiger Dateien in Ihrer eigenen Umgebung, ohne Dateien oder Ergebnisse in eine Drittanbieter-Cloud zu senden.

Virtual Private Networking (VPN)

Feature	Beschreibung
Auto-Provisioning für VPNs	Durch die Automatisierung der Erstkonfiguration des Site-to-Site-VPN-Gateways zwischen den SonicWall-Firewalls wird die Implementierung komplexer verteilter Firewalls zum Kinderspiel. Funktionen für Sicherheit und Konnektivität werden umgehend und automatisch ausgeführt.
IPsec-VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPsec-VPN kann die Firewall als VPN-Konzentrator für Tausende großer Standorte, Filialen oder Homeoffices 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 zu ermöglichen.
Routenbasiertes VPN	Dank dynamischem Routing über VPN-Links lässt sich auch bei einem temporären Ausfall eines VPN-Tunnels ein unterbrechungsfreier Betrieb gewährleisten. Der Datenverkehr zwischen den betroffenen Endpunkten wird nahtlos über alternative Routen geleitet.

Zero-Trust-Network-Access (ZTNA)

Feature	Beschreibung
Konnektor für Secure Private Access (SPA)	Über bestehende SonicWall-Firewalls und durch die Integration mit Cloud Secure Edge lässt sich ein Zero-Trust-Network-Zugriff auf private Apps hinter der Firewall ermöglichen.

Content- bzw. kontextorientierte Sicherheitsfunktionen

Feature	Beschreibung
Nachverfolgung der Benutzeraktivitäten	Dank nahtloser SSO-Integration für AD/LDAP/Citrix/Terminaldienste und umfassender DPI-Daten lassen sich Nutzer identifizieren und ihr Verhalten nachvollziehen.
Identifizierung des Datenverkehrs nach Ländern mittels Geo-IP	Die Lösung kann Datenverkehr in oder aus spezifischen Ländern identifizieren und kontrollieren. So schützen Sie Ihr Netzwerk gegen Angriffe aus bekannten oder vermuteten Bedrohungsquellen und können verdächtigen Datenverkehr aus Ihrem Netzwerk analysieren. 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. Eine unerwünschte Filterung von IP-Adressen aufgrund einer Fehlklassifikation wird so verhindert.
Abgleich regulärer Ausdrücke und Filterung	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren. So können Datenlecks verhindert werden.

Aboservices zur Prävention von Sicherheitslücken

Capture Advanced Threat Protection[1]

Feature	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™)	SonicWall RTDMI ist eine patentierte Technologie, die von SonicWall Capture Cloud genutzt wird, um selbst die gefährlichsten modernen Bedrohungen einschließlich künftiger Meltdown-Exploits zu identifizieren und abzuwehren. Die Technologie ist in der Lage, Malware zu identifizieren und zu blockieren, die kein bösartiges Verhalten zeigt und ihre Wirkmechanismen durch Verschlüsselungsmethoden verschleiert.
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	Der Service unterstützt die Analyse unterschiedlichster Dateitypen, darunter ausführbare Programme (PE), DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK, sowie unterschiedliche Betriebssysteme, wie Windows, Android, Mac OS und Multi-Browser-Umgebungen.
Schnelle Implementierung von Signaturen	Wird eine Datei als bösartig identifiziert, so wird unmittelbar eine Signatur auf Firewalls mit SonicWall-Capture-Abos aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt.

Endpoint-Security

Feature	Beschreibung
Schutz von Endgeräten	Capture Client nutzt einen verhaltensbasierten Schutz vor ausgeklügelten Bedrohungen auf Basis von SentinelOne-EDR-Funktionen der nächsten Generation. Die Integration mit Capture ATP sorgt für einen effektiveren Schutz, kürzere Reaktionszeiten und geringere Gesamtbetriebskosten.
Anwendung von DPI-SSL	Bereitstellung von DPI-SSL-Zertifikaten und Prüfung von verschlüsseltem Datenverkehr mittels Deep Packet Inspection (DPI-SSL) auf Endgeräten.
Umsetzung von Regeln auf Endgeräten	Weiterleitung ungeschützter Benutzer zur Capture-Client-Downloadseite, bevor sie hinter einer Firewall auf das Internet zugreifen können.
SSO-Anmeldung	Ermöglicht die Nutzung von Benutzerinformationen von Endgeräten für SSO-Richtlinien.
SAML-Single-Sign-on[1]	Zugriff auf mehrere Apps über einen einzigen Satz Anmeldedaten für eine einfachere Authentifizierung.[1]

Schutz vor verschlüsselten Bedrohungen

Feature	Beschreibung
TLS-/SSL-Entschlüsselung und -Prüfung	Proxylose On-the-Fly-Entschlüsselung und -Prüfung von TLS-/SSL-verschlüsseltem Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen im verschlüsselten Verkehr zu schützen. Dieser Service ist bei allen Modellen außer der SOHO in den Sicherheitsabos inbegriffen. Für die SOHO ist er in Form einer separaten Lizenz verfügbar.
SSH-Prüfung	Durch die Deep-Packet-Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen.
TLS-1.3-Unterstützung	Unterstützung für TLS 1.3 zur Erhöhung der allgemeinen Firewall-Sicherheit. Verfügbar für Firewall-Management, SSL-VPN und DPI.

Intrusion-Prevention[2]

Feature	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 aktualisiert fortlaufend eine umfassende Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Eine Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion-Prevention steigert die interne Sicherheit und verhindert, dass Bedrohungen sich über Zonengrenzen hinweg 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 Domains 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	Dank kontinuierlicher Updates zu den neuesten Exploit-Methoden und -Techniken wird das Netzwerk effektiv vor Zero-Day-Attacken geschützt. Dabei werden Tausende verschiedene Exploits abgedeckt.
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.
Umfassende Liste von IPS-Signaturen	Über 10.000 IPS-Signaturen zum Schutz vor Exploits, die auf Software-Schwachstellen abzielen.*

Bedrohungsschutz[2]

Feature	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.

* Einige Signaturen zum Schutz vor Exploits, die auf Software-Schwachstellen abzielen, stehen im Rahmen von GAV- und Anti-Spyware-Services zur Verfügung.

[1] SAML-Single-Sign-on ist für das demnächst erscheinende SonicOS-8.1-Release verfügbar.

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 prüft Raw-TCP-Streams bidirektional und auf sämtlichen Ports, um Bedrohungen in ein- und ausgehendem Datenverkehr zu erkennen und abzuwehren.
Unterstützung zahlreicher Protokolle	Identifizierung gängiger Protokolle wie z. B. HTTP/S, FTP, SMTP und SMB v1/v2, 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[2]

Feature	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	Erstellung von Signaturen auf der Grundlage bestimmter Parameter oder Muster, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen. Auf diese Weise lässt sich eine erweiterte Kontrolle über das Netzwerk erreichen.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenkapazität kann für kritische Anwendungen (oder Anwendungskategorien) granular zugewiesen und reguliert werden. Gleichzeitig lässt sich jedweder nicht notwendiger Anwendungsverkehr unterbinden.
Granulare Kontrolle	Kontrolle von Anwendungen (oder bestimmten Anwendungskomponenten) auf der Grundlage von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten mit voller SSO-Benutzeridentifizierung durch LDAP-/AD-/Terminaldienst-/Citrix-Integration.

Content-Filterung[2]

Feature	Beschreibung
Reputationsbasierte Content-Filterung	Beschränkung und Kontrolle der Webinhalte, auf die Internetbenutzer zugreifen können. Bei der reputationsbasierten Content-Filterung wird ein Reputation-Score ausgegeben, der das Sicherheitsrisiko einer URL bewertet.
Filterung interner/externer Inhalte	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 Firewall-Grenze zu blockieren.
Granulare Kontrolle	Inhalte lassen sich auf Basis 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.
Local CFS Responder	Local CFS Responder lässt sich als virtuelle Appliance in Private Clouds auf Grundlage von VMware oder Microsoft Hyper-V implementieren. Dies ermöglicht flexible Implementierungsoptionen (schlanke VM) für CFS-Rating-Datenbanken in verschiedenen Kundennetzwerk-Szenarien, bei denen eine spezielle lokale Lösung erforderlich ist, die CFS-Rating-Abfrage- und Antwortzeiten verkürzt, eine große Anzahl an URL-Freigabe-/Sperrlisten unterstützt (über 100.000) und bis zu 1.000 SonicWall-Firewalls für CFS-Rating-Lookups hinzufügt.

Durchsetzung von Viren- und Spyware-Schutz[2]

Feature	Beschreibung
Mehrstufiger Schutz	Die Firewall ist die erste Verteidigungsstufe am Netzwerkrand. Zusammen mit Endpoint-Security-Funktionen verhindert sie, dass Viren über Laptops, USB-Sticks und andere ungeschützte Systeme ins Netzwerk eindringen.
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 von desktopbasierten 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.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt den eingehenden Datenverkehr 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 der Geräte erhöht.

Erweiterte Sicherheit

Feature	Beschreibung
Netzwerktransparenz	Granulare Einblicke in die Netzwerktopologie und Hostinformationen.
Cloud-Management	Cloudbasiertes Firewall-Management über die Network-Security-Manager-Kachel in SonicWall Unified Management.

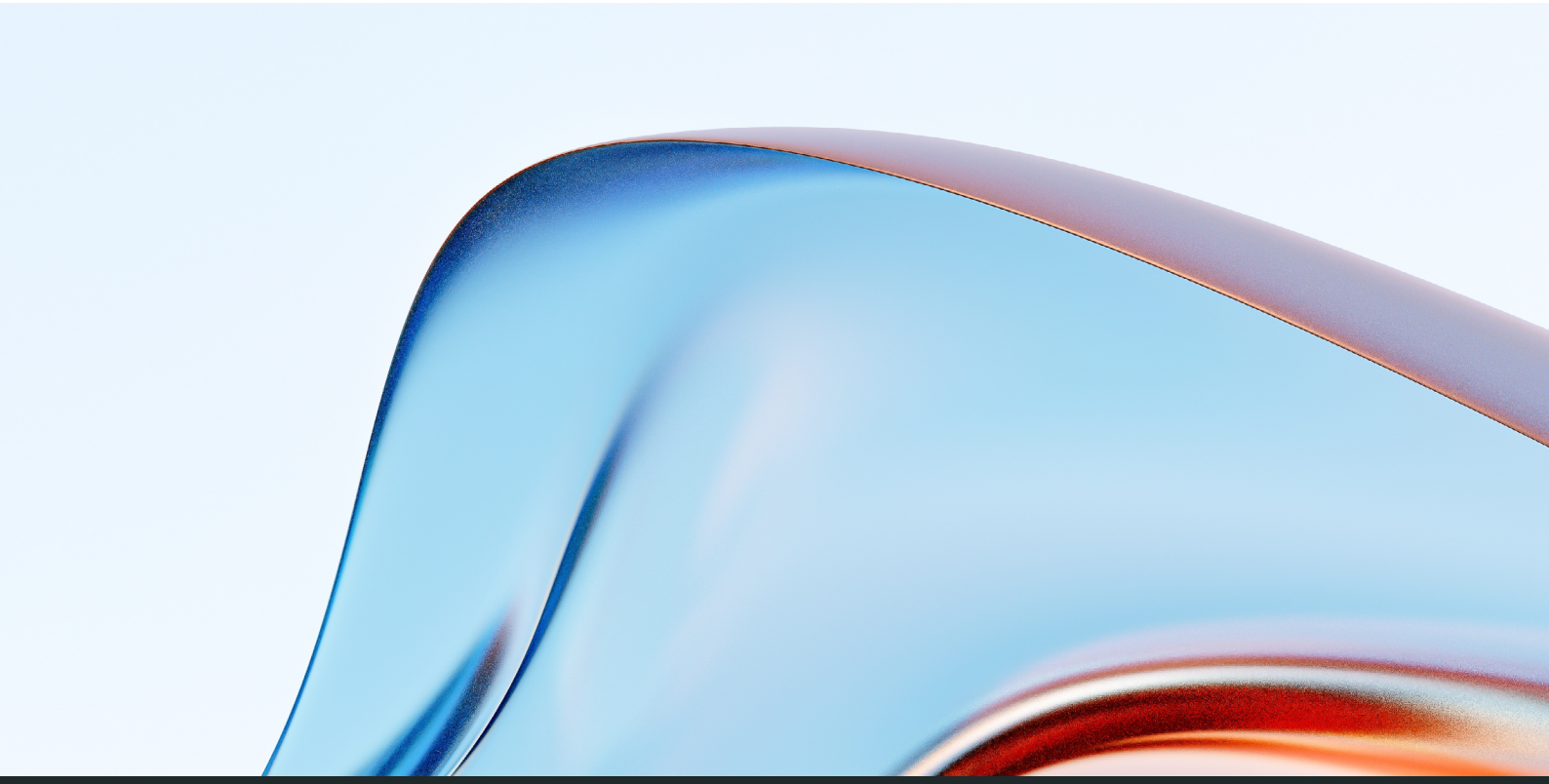
[2] Erfordert zusätzliches Abo.

SONICWALL

PARTNER ENABLED SERVICES

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Die SonicWall-Advanced-Services-Partner unterstützen Sie mit erstklassigen Professional Services.

Weitere Informationen:
www.sonicwall.com/PES



SonicWall Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA | Weitere Informationen erhalten Sie auf unserer Website.

© 2025 SonicWall Inc. ALLE RECHTE VORBEHALTEN.
SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Haftung und keinerlei ausdrückliche, stillschweigende oder gesetzliche Gewährleistung für deren Produkte, einschließlich, aber nicht beschränkt auf die stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck und die Nichtverletzung von Rechten Dritter, soweit sie nicht in den Bestimmungen der Lizenzvereinbarung für dieses Produkt niedergelegt sind. SonicWall und/oder dessen Tochtergesellschaften haften nicht für irgendwelche unmittelbaren, mittelbaren, strafrechtlichen, speziellen, zufälligen oder Folgeschäden (einschließlich, aber nicht beschränkt auf Schäden aus entgangenem Gewinn, Geschäftsunterbrechung oder Verlust von Information), die aus der Verwendung oder der Unmöglichkeit der Verwendung dieses Dokuments entstehen, selbst wenn SonicWall und/oder dessen Tochtergesellschaften auf die Möglichkeit solcher Schäden hingewiesen wurden. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder Tochtergesellschaften von SonicWall Inc. übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Datasheet - Gen 8 Architecture & Security

sonicwall.com

SONICWALL®