Datenblatt zu SonicOS 7.0 und Services

Die SonicOS-Architektur bildet den Kern der physischen und virtuellen SonicWall-Firewalls, einschließlich der TZ, NSa, NSv und NSsp Series. SonicOS nutzt unsere patentierten Reassembly-Free Deep Packet Inspection® (RFDPI) und die zum Patent angemeldete Real-Time Deep Memory Inspection™ (RTDMI) Technologie mit Single-Pass-Prüfsystem und minimaler Latenz und bietet Unternehmen branchenweit bewährte Effizienz, sicheres SD-WAN, Echtzeitvisualisierung, schnelles Virtual Private Networking (VPN) mit weiteren robusten Sicherheitsfeatures.

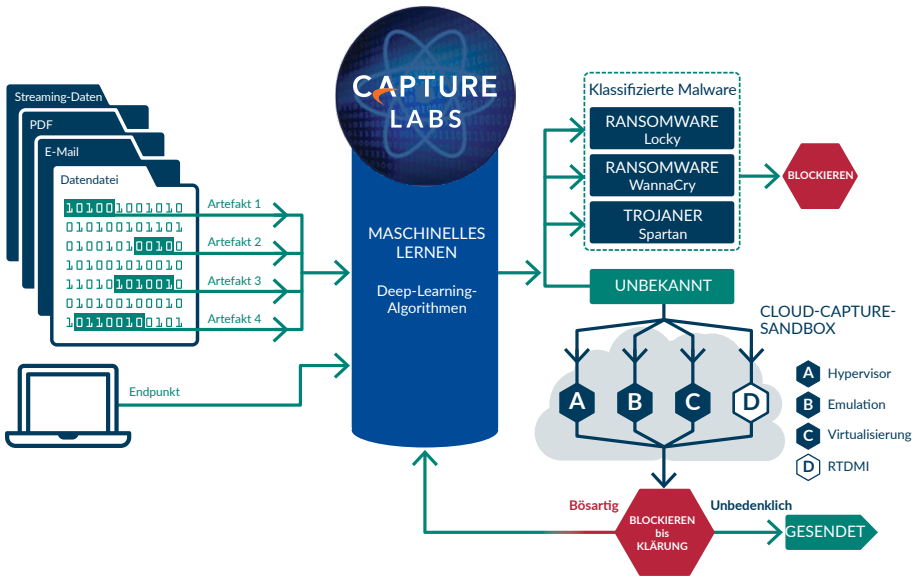
Um Netzwerke in einer dynamischen Cyberbedrohungslandschaft zu schützen, setzen wir auf eine automatisierte Echtzeiterkennung und -prävention von Bedrohungen. Durch eine Kombination Cloud-basierter und integrierter Technologien bieten unsere Firewalls hocheffektive Schutzfunktionen, die bereits in unabhängigen Tests bestätigt wurden. Verdächtige Dateien werden zur Analyse an die Cloud-basierte SonicWall Multi-Engine-Sandbox Capture Advanced Threat Protection (ATP) weitergeleitet. Ein wichtiger Bestandteil von Capture ATP ist unsere 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 RFDPI-Engine lassen sich jedes einzelne Paket und jedes einzelne Byte durchleuchten. Dabei wird der ein- und ausgehende Datenverkehr direkt in der Firewall auf Bedrohungen geprüft. Neben integrierten Funktionen wie Intrusion Prevention, Anti-Malware und Web-/URL-Filtering nutzen unsere Firewalls der nächsten Generation auch Capture ATP mit RTDMI-Technologie in der SonicWall Capture Cloud Plattform, um Malware, Ransomware und andere Bedrohungen am Gateway zu stoppen.

Mit der Einführung des brandneuen SonicOS 7.0 Betriebssystems (OS) werden die Features und Funktionen der Firewalls der nächsten Generation auf die nächste Stufe katapultiert. Das Betriebssystem integriert SD-WAN, TLS 1.3 Unterstützung, Echtzeitvisualisierung, schnelles Virtual Private Networking (VPN) und andere robuste Sicherheitsfunktionen. Das von Grund auf neu konzipierte SonicOS 7.0 Betriebssystem bietet erweiterte Sicherheitsfunktionen, ein vereinfachtes Richtlinienmanagement sowie kritische Netzwerk- und Managementfunktionen für verteilte Unternehmen mit Next-Gen SD-Branches sowie kleine und mittlere Unternehmen.

Security Serviced-Bündel

Mit SonicWall Security Services machen Sie Ihre Firewalls zu einer umfassenden Sicherheitslösung. Die Security Services werden in drei Abonnements angeboten – Essential, Advanced und Premier. (i) SonicWall Essential Protection Service Suite bietet alle wichtigen Sicherheitsdienste, die zum Schutz vor bekannten und unbekannten Bedrohungen notwendig sind. (ii) SonicWall Advanced Protection Service Suite bietet erweiterte Sicherheit für Ihr Netzwerk mit zusätzlichen für die Cloud notwendigen -Sicherheitsdiensten. (iii) SonicWall Premier Protection Service Suite* bietet umfassende Sicherheit mit zusätzlichen Sicherheitsdiensten, Sichtbarkeit in der Cloud, Analysen und Endpunktdiensten für ultimativen Schutz.



*Verfügbarkeit ausstehend

FUNKTIONEN	ESSENTIAL	ADVANCED	PREMIER*
Gateway Anti-Virus, Intrusion Prevention und Application Control	√	√	√
Content-Filtering-Service	√	√	√
Anti-Spam	√	√	√
24/7-Support	√	√	√
Netzwerktransparenz	√	√	√
Capture ATP (Multi-Engine) Sandboxing	√	√	√
RTDMI-Technologie	√	√	√
Grundlegende DNS Security	√	√	√
Cloud-Management	!	√	√
Cloud-basiertes Reporting – 7 Tage	!	√	√
Erweiterte Cloud-Analysen – Virtuell, 365 Tage Reporting	!	!	√
Erweiterte DNS Security	!	!	√
Tool für die Firewallsystemprüfung	X	X	√
Cloud App Security Startpaket	X	X	√
Capture Client Startpaket	X	X	√
Premier Support	X	!	!

√ *Im Bündel enthalten*
! *Nicht im Bündel enthalten, kann separat erworben werden*
X *Wird unter dem Bündel nicht unterstützt*
* *Verfügbarkeit ausstehend*

Erweitertes Dashboard

ERWEITERTES DASHBOARD	
Funktion	**Beschreibung**
Erweitertes Dashboard	Dashboard mit umsetzbaren Warnmeldungen.
„Optimierte Geräteansicht mit Front- und Rückansicht sowie Speicherstatistik der Hardware“	Über die Registerkarte „Start“ der Benutzeroberfläche können sich Benutzer über den Status der Vorder- und Rückseite und der Nutzungsstatistik des Speichermoduls in Echtzeit informieren. Dies vermittelt Ihnen die gleiche Erfahrung, als wenn Sie sich physisch vor der Hardware befinden würden.
System- und Bandbreitennutzung in Echtzeit	Benutzer können nun die Kern- und Bandbreitennutzung des Systems im Netzwerk in Echtzeit einsehen.
Verteilung der gesamten Verkehrslast	Verteilung der Verkehrslasten an der Firewall des Benutzers mit Echtzeit-Updates in Bezug auf die meistverwendete Anwendung.
Überblick über Top-Benutzer	Überblick über die Top-Benutzer basierend auf zulässigen oder blockierten Sitzungen; nach gesendeten und empfangenen Daten.
Überblick über aufgedeckte Bedrohungen	Überblick über Bedrohungen, wie Viren, Zero-Day-Malware, Spyware, Schwachstellen und gefährdete Anwendungen, innerhalb des Kundennetzwerks in Echtzeit.
Services im Überblick	Echtzeitstatus von aktivierten oder deaktivierten Sicherheitsdiensten, wie IPS, GAV, Anti-Spyware, Capture ATP oder DPI-SSL.
Erkenntnisse über infizierte Hosts	Anzeigen der Gesamtzahl infizierter Hostcomputer im Netzwerk in Echtzeit.
Erkenntnisse über kritische Angriffe	Anzeigen der Gesamtzahl geschäftskritischer Netzwerkangriffe in Echtzeit.
Einblicke in den verschlüsselten Verkehr	Anzeigen des gesamten verschlüsselten Netzwerkverkehrs in Echtzeit.
Überblick über Top-Anwendungen	Anzeigen der am häufigsten verwendeten Anwendungen im Netzwerk mit zusätzlichen Optionen für die Sortierung nach Sitzungen, Bytes, Blockierungen durch Zugriffsregeln, Viren, Spyware und Eindringversuchen.
Überblick über Top-Adressen	Anzeigen der am häufigsten verwendeten Adressobjekte im Netzwerk mit zusätzlichen Optionen für die Sortierung nach Sitzungen, Bytes, Blockierungen durch Zugriffsregeln, Viren, Spyware und Eindringversuchen.
Überblick über Top-Benutzer	Anzeigen der Top-Benutzer im Netzwerk mit zusätzlichen Optionen für die Sortierung nach Sitzungen, Bytes, Blockierungen durch Zugriffsregeln, Viren, Spyware und Eindringversuchen.
Überblick über Top-Website-Ratings	Zeigt die Top-Website-Ratings nach Sitzung an.
Überblick über die Top-Länderstatistiken	Anzeigen der Top-Länderstatistiken nach Sitzung, gesunkenem Datenverkehr, gesendeten oder empfangenen Bytes.
Überblick über Echtzeit-Bedrohungen	Anzeigen der größten Bedrohungen mit separaten Statistiken für Virus, Eindringversuche, Spyware und Botnet nach Sitzungen.
Erweitertes Access Point Snapshot	Anzeigen der Statistiken zum Access Point-Status in Netzwerk- und Client-Verbindungen in Echtzeit
Access Point-Verkehrsrate	Bietet Echtzeit-Bandbreitennutzung nach Access-Points.
WLAN Client Report	Bietet WLAN Client-Reporting in Echtzeit basierend auf Betriebssystemtyp, Häufigkeit und Top-Client-Diagramm

ERWEITERTES DASHBOARD (FORTSETZUNG)	
WLAN Client Monitor in Echtzeit	Bestimmt den Hostcomputer, Betriebssystemtyp, die Frequenz, Access-Point-Informationen und Datenübertragung.
Erkenntnisse über Capture ATP-Urteile	Zeigt die von Capture ATP ermittelten Urteile für die Dateianalyse an.
Einblick in Dateitypen	Zeigt den Dateityp an, der auf dem Capture-ATP-Report basiert.
Erkenntnisse über Zieladressen	Zeigt die am häufigsten von bösartigen Dateien verwendeten Ziele an.
Statistiken zur Malware-Analyse	Zeigt detaillierte Statistiken über dynamische und statische Malware-Analysen pro Datei an.
Analyse des Ursprungs von standortbasierten Zero-Day-Attacken	Zeigt den Ursprung des Angriffs nach Ländern an.
Capture ATP-Statistiken	Gewährt Einblick in alle eingereichten Dateien, dynamisch analysierte Dateien, bösartige Dateien und die durchschnittliche Bearbeitungszeit mit Capture ATP.
Netzwerktopologie-Ansicht	In der Topologie-Ansicht werden Hosts sowie mit dem Benutzernetzwerk verbundene Access Points basierend auf Gerätenamen, Mac-Adresse und IP-Adresse angezeigt
API-gesteuertes Management	Das Firewall-Management wird über die API gesteuert
SD-WAN-Assistent	Assistent zur automatischen Konfiguration der SD-WAN-Richtlinie in der Firewall
Benachrichtigungszentrum	Ein neues Benachrichtigungszentrum mit Bedrohungsübersicht, Ereignisprotokollen und Systemalarm.
Optimierte Online-Hilfe	Online-Hilfe mit Links zur technischen Dokumentation zu jedem Modell.
SD-WAN-Überwachung	Zeigt die SD-WAN Leistungssensoren und optionalen Verbindungen an.
Erweitertes Packet-Monitor Dienstprogramm	Das erweiterte Packet Monitor Dienstprogramm umfasst jetzt auch Zugriffsregel, NAT-Regel und Routeninformationen.
Konfiguration des Speichergeräts	Konfigurationsunterstützung für Speichermodule, einschließlich erweiterter Module. Nutzungsstatistik des Moduls
Capture Threat Assessment (CTA) 2.0	Neuer CTA 2.0 Report unterstützt die neue Berichtsvorlage und bietet Personalisierungsoptionen wie Logo, Name und Abschnitte. Unterstützt Datei- und Malware-Analysen. Unternehmensstatistik mit Industrie- und Global-Mittelwert für jeden Abschnitt. Separate Executive-Vorlage mit Empfehlungen.
Systemprotokoll-Downloads	Systemprotokolle und auch Konsolenprotokolle können vom Diagnoseabschnitt heruntergeladen werden, ohne dass der Rechner mit dem Konsolenanschluss verbunden werden muss. Das vereinfacht die Fehlerbehebung und verkürzt die Zeit für die Fehlersuche.
SSH-Terminal auf der Benutzeroberfläche	SSH-Terminal ist über die Web-Benutzeroberfläche zugänglich.
Dienstprogramm für Grid-Prüfung	Dieses Dienstprogramm ermöglicht die Überprüfung der IP-Adresse der Grid-IP zur Diagnose.
Dienstprogramm für die Fehlersuche	Benutzer können den Debug-Modus innerhalb der gleichen Firmware aktivieren und Debugbefehle vom SSH-Terminal innerhalb der Benutzeroberfläche ausführen.
Systemdiagnose-Tools	Unterstützung für weitere Diagnosetools, wie GDB, HTOP und das Linux Perf Tool.
Switch Netzwerküberblick	SonicWall Switch-Ansicht wie physische Ansicht, Listenansicht und VLAN-Ansicht.
Bandbreitennutzung pro Switch-Port	SonicWall Switch Info zeigt die Bandbreitennutzung pro Port an.
WWAN-Status	Anzeige des WWAN Modem- und Netzwerkstatus.

Firewall — Features und Services

REASSEMBLY-FREE DEEP PACKET INSPECTION (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 API	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 effizient zu bekämpfen.
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall- Zugriffsregeln erfüllt werden.
Hochverfügbarkeit/Clustering	Unterstützt die Hochverfügbarkeitsmodi Active/Passive (A/P) mit State-Synchronisierung, Active/Active (A/A)-DPI[2] und Active/Active-Clustering. Beim Active/Active-DPI-Modus wird die Deep Packet Inspection-Last an die passive Appliance weitergegeben, um den Durchsatz zu erhöhen.
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-, Netzwek-Tap-NAT- oder Layer-2-Bridge-[2] -Modus implementieren.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden. Regelbasiertes Routing erstellt Routen auf Basis des Protokolls, um den Verkehr an eine bevorzugte WAN-Verbindung zu leiten, während bei einem Ausfall jederzeit ein Failback auf ein sekundäres WAN möglich ist.
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.
SonicWall Switch-Integration	Die ersten Switches von SonicWall lassen sich nahtlos in Firewalls integrieren und ermöglichen die Verwaltung und Sichtbarkeit Ihres Netzwerks über eine zentrale Benutzeroberfläche
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.
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 ihrem Google Account und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.
Multi-Domain-Authentifizierung	Ermöglicht eine einfache und schnelle Verwaltung von Sicherheitsrichtlinien für alle Netzwerkdomänen. Verwaltung einzelner Richtlinien für eine Domäne oder eine Gruppe von Domänen.
Umfassende API-Unterstützung	Umfassende API-Unterstützung für jeden Abschnitt der Firewall-Benutzeroberfläche.
SD-WAN-Skalierbarkeit	Skalierbare Tunnelschnittstellen für verteilte Unternehmen.

MANAGEMENT, REPORTING UND SUPPORT

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.
IPFIX-/NetFlow Application Flow-Berichte	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.
Compliance-zentrische Malware-Erkennung	Analysiert verdächtige Dateien in Ihrem eigenen Umfeld, ohne die Dateien oder Ergebnisse in die Cloud eines Drittanbieters zu setzen.

VIRTUAL PRIVATE NETWORKING (VPN)	
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 Firewall 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.
Optimiertes Objekt-Matching	Match Object unterstützt das Hinzufügen von Anwendungen und bietet eine verbesserte Benutzererfahrung.
Profilbasierte Objekte	Profilobjekte für Endpunktsicherheit, Bandbreitenmanagement, QoS-Marking, Content-Filter, DHCP Option und AWS VPN.
Aktionsbasierte Objekte	Aktionsobjekt für Anwendungsregel und Content Filtering Regel.
Verbesserte Zugriffsregeln	Verbesserte Regelanzeige für eine intuitive Benutzererfahrung
Anpassbare Grid-Einstellungen	Anpassbare und bewegliche Spalten innerhalb der Zugriffs-, NAT- und Routing-Regeln.
Aktive und inaktive Regelanzeige	Zeigt die Regeln an, die aktiviert oder deaktiviert sind.
Übersicht über angewandte und nicht angewandte Regeln	Zeigt die Regeln, die aktiv angewandt oder nicht angewandt werden.
Export der Zugriffsregeln	Exportiert alle Zugriffsregeln in eine CSV-Datei.
Live Counter für Zugriffsregeln	Ermöglicht die Erfassung von Live-Statistiken zu den Zugriffsregeln.
Regeldiagramm	Grafische Darstellung einer bestimmten Zugriffsregel, NAT- und Routing-Regel, was bei der Suche nach Echtzeit-Statistiken hilft.
Sicherheitsprofil innerhalb einer Zugriffsregel	Möglichkeit, ein Sicherheitsprofil innerhalb einer Regel hinzuzufügen, um DPI, DPI-SSL, Botnet und Geo-IP zu erlauben oder zu blockieren.
Endpunktsicherheitsregel	Möglichkeit zum Hinzufügen von Sicherheitsregeln für die Endpunktsicherheit mit Capture Client.
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/Citrix/Terminaldienste 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. 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 unerwünschte Filterung von IP-Adressen aufgrund einer Fehlklassifikation.
Abgleich regulärer Ausdrücke und Filterung	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern.

Breach Prevention-Aboservices

CAPTURE ADVANCED THREAT PROTECTION[1]	
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™)	Die zum Patent angemeldete RTDMI-Technologie von SonicWall umfasst ein Verfahren, das von der SonicWall Capture Cloud zur Erkennung und Entschärfung selbst der heimtückischsten modernen Bedrohungen eingesetzt wird, einschließlich künftiger Meltdown Exploits. Sie erkennt und blockiert sogar Schadcode, der kein schädliches Verhalten zeigt und seine zerstörerische Kraft durch Verschlüsselung verbirgt.
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	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 sofort 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.
Capture Client	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.

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 im verschlüsselten Verkehr zu schützen. 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.
TLS 1.3 Unterstützung	Unterstützung für TLS 1.3, um die Sicherheit der Firewall insgesamt zu verbessern. Dies ist im Firewall Management, SSL VPN und DPI implementiert.

INTRUSION-PREVENTION[1]

Funktion	Beschreibung
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion-Prevention-System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signatur-Updates	Das SonicWall Threat Research-Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Verbesserter Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion Prevention. Dies verhindert, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten.
Erkennen und Blockieren von Command-and-Control(CnC)-Aktivitäten durch Botnets	Erkennen und Blockieren von Command-and-Control-Verkehr, der von Bots im lokalen Netzwerk ausgeht und an IPs und Domänen geleitet wird, die nachweislich Malware verbreiten oder bekannte CnC-Punkte sind.
Protokollmissbrauch/-anomalien	Erkennen und Verhindern von Angriffen, die Protokolle missbrauchen, um unbemerkt am IPS vorbeizukommen.
Zero-Day-Schutz	Ständige Updates zu den neuesten Exploit-Techniken und -Methoden decken Tausende verschiedener Exploits ab und schützen das Netzwerk vor Zero-Day-Angriffen.
Umgehungsschutz	Umfassende Normalisierungs- und Entschlüsselungsmethoden sowie weitere Maßnahmen verhindern, dass Bedrohungen Umgehungstechniken auf den Schichten 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

BEDROHUNGSSCHUTZ[1]

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 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 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[1]

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	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 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[1]	
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.
Durchsetzung des Content-Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewallgrenzen zu blockieren.
Granulare Kontrolle	Blockiert Inhalte auf Basis einer beliebigen Kombination von Kategorien. 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, die eine dedizierte On-Premise-Lösung erfordern, die CFS-Rating-Abfrage- und Antwortzeiten verkürzen, eine große Anzahl eine große Anzahl an URL-Freigabe-/Sperrlisten unterstützen (über 100.000) und bis zu 1.000 SonicWall-Firewalls für CFS-Rating-Lookups hinzufügen.

DURCHSETZUNG VON VIREN- UND SPYWARE-SCHUTZ[1]	
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 Engine mit statischer Künstlicher Intelligenz, 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.

ERWEITERTE SICHERHEIT	
Funktion	**Beschreibung**
Erweiterte DNS Security	DNS Security sorgt für eine schnellere Erkennung von Angriffen (TTD, Time to Detect) und reduziert die Gesamtbetriebskosten (TCO, Total Cost of Ownership). DNS Security überprüft DNS-Felder, um bösartige Domänen zu identifizieren und blockiert so die Verbindung in einem sehr frühen Stadium der Verbindungsherstellung. SonicWall verfügt über Petabyte an Bedrohungsdaten, um Domänen als bösartig zu klassifizieren und falsch-positive Ergebnisse zu reduzieren.
Tool für die Firewallsystemprüfung	Risiken identifizieren und Compliance und Sicherheit verbessern. Das Heath Check Tool ist auf der Firewall-Benutzeroberfläche verfügbar und überwacht konstant die Sicherheitsinfrastruktur, Gateways, Technologien, Richtlinien und Konfigurationseinstellungen in Echtzeit.
Netzwerktransparenz	Sorgt für granulare Visualisierung der Netzwerktopologie sowie der Host-Informationen
Cloud-Management	Verwaltung von Firewalls in der Cloud durch die Network Security Manager-Kachel im Capture Security Center
Cloud-basiertes Reporting	Umfasst sieben Tage Cloud-basiertes Reporting

[1] *Erfordert zusätzliches Abo.*

Partner Enabled Services

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

Über SonicWall

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

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

Datasheet-SonicOSplatform-COG-2584

SONICWALL®