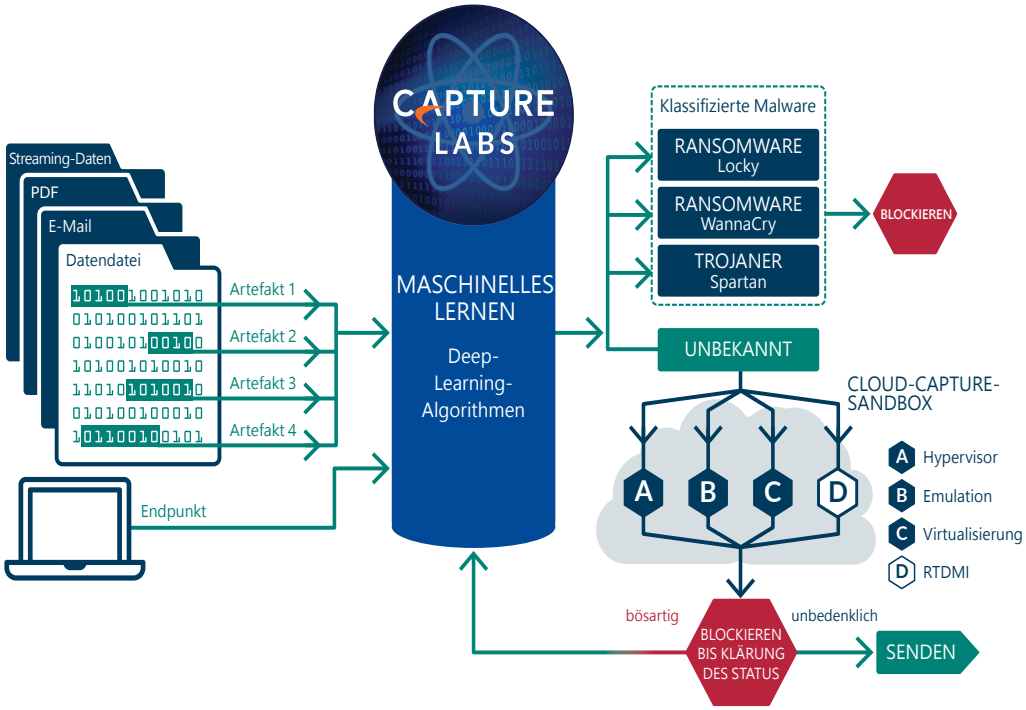
SonicOS 7 und Services

Die SonicOS-Architektur bildet das Herzstück jeder physischen und virtuellen SonicWall-Firewall, einschließlich der TZ, NS*a*, NS*v* und NS*sp Series*. SonicOS basiert auf unseren patentierten RFDPI- (Reassembly-Free Deep Packet Inspection®) und RTDMI-Technologien (Real-Time Deep Memory Inspection™) mit Single-Pass-Engine und niedriger Latenz 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 Multi-Engine-Sandbox Capture Advanced Threat Protection (ATP) von SonicWall 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.



DATENBLATT

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-Filtering 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.

Die Einführung des Betriebssystems SonicOS 7.1.1 hebt die Features und Funktionen der Gen-7-Firewall aufs nächste Level. SonicOS 7.1.1 bietet erweiterte Sicherheit, vereinfachte Regelverwaltung sowie kritische Netzwerk- und Managementfunktionen für kleine und mittlere Firmen sowie dezentrale Unternehmen mit SD-Branches der nächsten Generation. Das Betriebssystem wartet mit neuen oder verbesserten Features in puncto Wi-Fi 6-Support, DNS-Sicherheit, reputationsbasiertes Content-Filtering und Integration von Network Access Control (NAC) auf.

Security-Service-Bundles

Mit SonicWall Security Services wird die Firewall zu einer ganzheitlichen Sicherheitslösung. Security Services werden in drei Abo-Bundles angeboten: Threat Protection, Essential Protection und Advanced Protection. (i) Die SonicWall Threat Protection Service Suite beinhaltet grundlegende Sicherheitsservices in einem kostengünstigen Paket, mit denen der Schutz des Netzwerks vor Bedrohungen sichergestellt werden kann. (ii) Die SonicWall Essential Protection Service Suite bietet alle erforderlichen Sicherheitsservices für den Schutz vor bekannten und unbekannten Bedrohungen. (iii) Die SonicWall Advanced Protection Service Suite bietet erweiterte Sicherheit, um den Schutz Ihres Netzwerks mit unverzichtbaren Cloud-Security-Services auszuweiten.

Funktion	Threat Protection	Essential Protection	Advanced Protection
Gateway-Anti-Virus, Intrusion-Prevention, Anwendungskontrolle	✓	✓	✓
Content Filtering Service	✓	✓	✓
Anti-Spam	!	✓	✓
24/7-Support	✓	✓	✓
Netzwerktransparenz	✓	✓	✓
Capture ATP (Multi-Engine-Sandbox)	!	✓	✓
RTDMI-Technologie	!	✓	✓
DNS-Sicherheit	✓	✓	✓
Cloud-Management	!	!	✓
Cloudbasierte Berichte – 7 Tage	!	!	✓

✓ Im Bundle enthalten ! Nicht im Bundle enthalten, aber separat erhältlich

VERBESSERTES DASHBOARD

Verbessertes Dashboard	
Funktion	**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)	Bietet SonicWall-Kunden Network Access Control durch die Integration von Aruba ClearPass. Diese Architektur verwandelt statische in kontextbezogene Sicherheit, um einen flexibleren und moderneren Schutz bereitzustellen.
Wi-Fi 6-Support	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.
Token-basierte 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 grundlegender Konfiguration und Lizenzinformationen zu automatisieren.
NS*v*-Bootstrapping	Leichtere Durchführung umfangreicher NS*v*-Bereitstellungen, Unterstützung in VMware, Hyper-V, AWS und Azure, einfachere Produktregistrierungen mit Token-basierter Lizenzierung, INIT-Datei beinhaltet grundlegende Konfiguration, um die Instanz einsatzbereit zu machen.
Verbessertes Dashboard	Dashboard mit praktischen Warnhinweisen.
Optimierte Geräteansicht mit Anzeige der Front- und Rückblende sowie Speicherstatistiken zur Hardware	Über die Start-Registerkarte der UI können Benutzer den Echtzeitstatus der Front- und Rückblende sowie Nutzungsstatistiken des Speichermoduls abrufen, als hätten sie die Hardware direkt vor sich.
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 besten Länderstatistiken	Anzeige der besten Länderstatistiken nach Sitzung, verworfenem Datenverkehr, gesendeten oder empfangenen Bytes.
Übersicht der Echtzeitbedrohungen	Anzeige der Top-Bedrohungen mit separaten Statistiken für Viren, Eindringversuche, Spyware und Botnet nach Sitzungen.
Verbesserte Access-Point-Informationen	Anzeige von Statistiken zum Access-Point-Status im Netzwerk und Echtzeitstatistiken zu Clientverbindungen.
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.
SDWAN-Assistent	Assistent zur automatischen Konfiguration der Firewall-SDWAN-Regeln.
Benachrichtigungszentrale	Neue Benachrichtigungszentrale mit Bedrohungsübersicht, Ereignisprotokollen und Systemwarnungen.

Verbesserte Onlinehilfe	Onlinehilfe mit Links zur technischen Dokumentation für jedes Modell.
SDWAN-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 (CTA) 2.0	Neuer CTA 2.0-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 SwitchPort	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

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 Networking

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. 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 erfüllt werden.
Hochverfügbarkeit/Clustering	Unterstützung der Hochverfügbarkeitsmodi Active/Passive (A/P) mit State-Synchronisierung, Active/Active (A/A)-DPI2 und Active/Active-Clustering. Beim Active/Active-DPI-Modus wird die Deep-Packet-Inspection-Last an eine 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-, Netzwerk-Tap-NAT- oder Layer 2 Bridge-Modus implementieren.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten 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	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom H.323-Gatekeeper oder SIP-Proxy autorisiert und authentifiziert werden müssen.
SonicWall-Switch-Integration	SonicWall-Switches lassen sich nahtlos in Firewalls integrieren und ermöglichen so eine zentrale Verwaltung und 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.
SDWAN-Skalierbarkeit	Skalierbare Tunnelschnittstellen für verteilte Unternehmen.

Management, Reporting und Unterstützung

Funktion	Beschreibung
Cloudbasierte und lokale Verwaltung	Die SonicWall-Appliances lassen sich über die Cloud durch das SonicWall Capture Security Center sowie lokal durch das SonicWall Global Management System (GMS) konfigurieren und verwalten.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende Befehlszeilenschnittstelle und bietet Support für SNMPv2/3.
Berichte zum IPFIX-/NetFlow-Datenstrom	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Unterstützt wird auch die Berichterstellung mit SonicWall Analytics sowie anderen Tools, die IPFIX und NetFlow mit Erweiterungen erlauben.
Compliance-basierte Malware-Erkennung	Analyse verdächtiger Dateien in Ihrer eigenen Umgebung, ohne Dateien oder Ergebnisse in eine Drittanbieter-Cloud zu senden.

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.

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 unerwünschtes Filtering 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. So können Datenlecks verhindert werden.

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™)	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

Funktion	Beschreibung
Endpunktschutz	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.
DPI-SSL-Enforcement	Bereitstellung von DPI-SSL-Zertifikaten und Prüfung von verschlüsseltem Datenverkehr mittels Deep Packet Inspection (DPI-SSL) auf Endgeräten.
Endpoint Enforcement	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.

Schutz vor verschlüsselten Bedrohungen

Funktion	Beschreibung
TLS-/SSL-Entschlüsselung und -Inspektion	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 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. Dies ist in 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 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-Filtering[1]

Funktion	Beschreibung
Reputationsbasiertes Content-Filtering	Beschränkung und Kontrolle der Webinhalte, auf die Internetbenutzer zugreifen können. Beim reputationsbasierten Content-Filtering wird ein Reputation-Score ausgegeben, der das Sicherheitsrisiko einer URL bewertet.
Internes/Externes Content-Filtering	Über den Content Filtering Service und Content Filtering Client lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und HTTP-/HTTPS-Websites mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren.
Enforced Content Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewall-Grenze zu blockieren.
Gezielte Kontrollmöglichkeiten	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[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 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

Funktion	Beschreibung
Netzwerktransparenz	Granulare Einblicke in die Netzwerktopologie und Hostinformationen.
Cloud-Management	Cloudbasiertes Firewall-Management über die Network Security Manager-Kachel in Capture Security Center.
Cloudbasierte Berichte	Mit cloudbasiertem 7-Tage-Reporting.

[1] Erfordert zusätzliches Abo

PARTNER ENABLED SERVICES

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

Weitere Informationen: **www.sonicwall.com/PES**

Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

SONICWALL

© 2023 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 deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Datasheet-SonicOS7andServices-JK-9883