SonicOS-Plattform

Die SonicOS-Architektur bildet das Herzstück jeder physischen und virtuellen SonicWall-Firewall, einschließlich der TZ, NS*a*, NSv und SuperMassive Series. SonicOS basiert auf unserer patentierten* Reassembly-Free Deep Packet Inspection® (RFDPI)-Single-Pass-Engine mit niedriger Latenz und unserer zum Patent angemeldeten Real-Time Deep Memory Inspection™ (RTDMI)-Technologie und bietet eine hohe, bewährte Sicherheit, SD-WAN, Echtzeitvisualisierung, schnelles Virtual Private Networking (VPN) und andere robuste Sicherheitsfunktionen.

Firewall-Funktionen

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 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/Clustering	Unterstützung der Hochverfügbarkeitsmodi Active/Passive (A/P) mit State-Synchronisierung, Active/Active(A/A)-DPI[2] und Active/Active-Clustering[2]. 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-, Netzwerk-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 sorgt für das Erstellen von protokollbasierten Routen für die Umleitung des Datenverkehrs zu einer bevorzugten 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.

Firewall und Netzwerk (Fortsetzung)	
Funktion	Beschreibung
Verwaltung einzelner und hintereinandergeschalteter Switches der Dell N-Series und X-Series[2]	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 Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird.
Offene Authentifizierung und Social Login	Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.
Authentifzierung für mehrere Domänen	Erlaubt eine einfache und schnelle Verwaltung von Sicherheitsregeln über sämtliche Netzwerkdomänen hinweg. Verwaltung individueller Regeln für einzelne Domänen oder Domänengruppen.
Management und Reporting	
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.
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 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.
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 innerhalb von 48 Stunden 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 Modellen außer der SOHO in den Sicherheitsabos inbegriffen. Für die SOHO ist er in Form einer separaten Lizenz verfügbar.
SSH-Prüfung	Durch die Deep Packet Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen.
Intrusion-Prevention[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.
Enforced Content Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewallgrenze 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.
Virenschutz der nächsten Generation	Capture Client nutzt eine statische Artificial-Intelligence(AI)-Engine, um Bedrohungen zu identifizieren, bevor sie ausgeführt werden. Darüber hinaus ermöglicht Capture Client ein Rollback auf einen Zustand vor der Infizierung.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt den eingehenden Verkehr und blockiert die Installation zahlreicher Spyware-Programme auf Desktop-PCs und Laptops, bevor vertrauliche Daten übertragen werden können. Auf diese Weise werden die Sicherheit und die Performance von Desktops erhöht.

[1] Erfordert zusätzliches Abo.
[2] Wird nicht auf Firewalls der NSv Series unterstützt.

Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können. Für weitere Informationen besuchen Sie **www.sonicwall.com** oder folgen uns auf Twitter, LinkedIn, Facebook und Instagram.

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

Die SonicOS-Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- REST-APIs

TLS-/SSL-/SSH-Entschlüsselung und -Prüfung[2]

- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Granulare DPI-SSL-Steuerung nach Zone oder Regel

Capture Advanced Threat Protection[2]

- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Übermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention[2]

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüf-Engine
- Granulare IPS-Regeln
- GeoIP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]

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

Anwendungsidentifizierung[2]

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[2]

- URL-Filtering
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN

- Sicheres SD-WAN
- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (RIP/OSPF/BGP)

Netzwerk

- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung (NS*a* 2650 und höher)
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller[1]
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation[1] (statisch und dynamisch)
- Port-Redundanz[1]
- Hochverfügbarkeitsmodus A/P mit State-Sync
- A/A-Clustering[1]
- Lastausgleich für ein- und ausgehenden Datenverkehr
- L2-Bridge-[1], Wire-/Virtual-Wire-, Tap-, NAT-Modus
- 3G-/4G-WAN-Failover[1]
- Asymmetrisches Routing
- Common Access Card (CAC)-Unterstützung

VoIP

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

Verwaltung und Überwachung

- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mit dem SonicWall Global Management System (GMS)[2]
- Logging
- NetFlow-/IPFIX-Export
- Cloudbasiertes Konfigurationsbackup
- BlueCoat Security Analytics Platform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- Externes Reporting (Scrutinizer)
- LCD-Bildschirm[1]
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinandergeschalteten Switches[1]

Wireless-Bereich[1]

- WIDS/WIPS
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- Automatische Kanalauswahl
- Analyse des HF-Spektrums
- Floor Plan View
- Topology View
- Bandsteering
- Beamforming
- AirTime-Fairness
- MiFi-Extender
- Zyklische Quote für Gastbenutzer
- LHM-Gast-Portal

Integrierte Wireless-Konnektivität (nur TZ Series)

- Dualband (2,4 GHz und 5,0 GHz)
- Wireless-Standards 802.11 a/b/g/n/ac
- Erkennung und Vermeidung von Wireless-Angriffen
- Wireless Guest Services
- Lightweight Hotspot Messaging
- Segmentierung mithilfe virtueller Access-Points
- Captive Portal
- Cloud-Zugriffssteuerungsliste

[1] Wird nicht auf Firewalls der NSv Series unterstützt.
[2] Erfordert zusätzliches Abo.

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

Datasheet-SonicOSplatform-US-VG-MKTG4136

SONICWALL®