



SonicWALL PRO 2040

PRO SERIE

Umfassende Sicherheit und flexible Konfigurationsoptionen



- **Leistungsfähige Deep Packet Inspection Firewall**
- **Integrierte Unterstützung von Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention**
- **DDNS (Dynamic Domain Name Service)-Unterstützung**
- **Global Management und Reporting-Funktionen**
- **Spamabwehr mit Realtime Blacklist**
- **Flexibler vierter Port**
- **Integrierte WLAN Services**
- **Erweiterte Sicherheits- und Netzwerkfeatures wie DMZ, WAN/WAN-Failover und richtlinienbasiertes Routing**

Unternehmen und Organisationen bewegen heute große Mengen an geschäftskritischen Daten über weitverzweigte und oft sehr komplex strukturierte Netzwerke. Um die erforderliche Verfügbarkeit und Business Continuity zu gewährleisten, benötigen Netzwerkadministratoren eine Lösung, die gleichzeitig das Netzwerk absichert und erweiterte Features sowie hohe Performance bietet.

Die SonicWALL® PRO 2040 ist eine flexible, leistungsfähige und anwenderfreundliche Sicherheitsplattform, die Ihre Netzressourcen schützt, die Produktivität der Mitarbeiter erhöht und einen unterbrechungsfreien Geschäftsbetrieb gewährleistet. In einem kostengünstigen rack-fähigen Gerät verpackt bietet die PRO 2040 alle Vorzüge des SonicOS-Betriebssystems von SonicWALL, z.B. erweiterte Sicherheits-Features und flexible Konfigurationsoptionen speziell für Netzwerke mit bis zu 200 Nodes bzw. 50 Einzelstandorten. Die hochintegrierte Appliance vereint eine Deep Packet Inspection Firewall mit IPSec VPN-Funktionen, unterstützt Gateway-Anti-Virus, Anti-Spyware, Intrusion Prevention, Content Filtering sowie Spamschutz und sorgt so für umfassende Sicherheit.

Mit dem optionalen Upgrade auf SonicOS Enhanced verfügen Sie über eine breite Palette erweiterter Sicherheits- und Networking-Features, darunter ISP-Failover, objektbasiertes Management und richtlinienbasierte NAT. Daneben wird mit SonicOS Enhanced eine vierte Schnittstelle aktiviert, die entweder als zweiter WAN- bzw. LAN-Zugang, als DMZ-Port oder als Hardware-Failover-Port konfiguriert werden kann, um maximale Netzverfügbarkeit zu garantieren.

Funktionen und Vorteile

Leistungsfähige Deep Packet Inspection Firewall.

Bietet zuverlässigen Schutz vor böswilligen Angriffen auf der Anwendungsschicht, egal ob diese von internen oder externen Quellen stammen.

Integrierte Unterstützung von Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention.

Schützt das Netzwerk vor ständig neuen Bedrohungen wie Viren, Spyware, Würmern, Trojanern, Software-Schwachstellen (z.B. Pufferüberläufe, Peer-to-Peer- und Instant Messaging-Anwendungen, Backdoor-Angriffe) und sonstigem bösartigem Code.

DDNS (Dynamic Domain Name Service)-Unterstützung. Erlaubt die Verwendung dynamischer IP-Adressen und reduziert so die Kosten für die Bereitstellung von E-Mail-Servern, Webservern und Site-to-Site-VPN.

Ausgezeichnetes Global Management System (GMS). Beinhaltet umfassende Management- und Reporting-Tools und vereinfacht so die Konfiguration, Anwendung und Verwaltung von globalen Sicherheitsrichtlinien, VPN-Funktionen und Diensten von einer zentralen Stelle aus.

Mit SonicOS Enhanced Firmware Upgrade:

Spamabwehr mit Realtime Blacklist. Über DNS kann auf Real-Time Blacklist (RBL)-Dienste zugegriffen werden, in denen bekannte Spam- und Open-Relay-SMTP-Server erfasst sind. SMTP-Verbindungen von solchen Servern werden dann abgewiesen.

Flexibler vierter Port. Kann als zweiter WAN- bzw. LAN-Zugang, als DMZ-Port oder als Hardware-Failover-Port konfiguriert werden und garantiert so maximale Flexibilität bei der Netzwerkkonfiguration.

Integrierte WLAN Services. Die Appliance fungiert hierbei als Secure Wireless Switch und Controller. Sie erkennt und konfiguriert SonicPoints bei der Einrichtung im Netzwerk und sorgt dafür, dass Sicherheitsrichtlinien für sämtlichen kabelgebundenen und Wireless-Verkehr angewendet werden.

Erweiterte Sicherheits- und Netzwerkfeatures. Beinhalten WAN/WAN-Failover, Distributed Wireless, zonen- und objektbasierte Verwaltung, richtlinienbasiertes Routing, erweiterte NAT-Modi, QoS und vieles mehr.



Technische Daten

SonicWALL PRO 2040

Firewall

Unterstützte Nodes	Unlimitiert
Stateful-Durchsatz	200 MBit/s*
Deep Packet Inspection	Schutz vor Viren, Spyware, Würmern, Trojanern und Angriffen auf der Anwendungsschicht. Erfordert Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention Service für die Aktualisierung von Signaturen
Gateway Anti-Virus-Durchsatz	40 MBit/s**
Gleichz. Verbindungen	32.000
Richtlinien	1.000 (SonicOS Enhanced)
Angriffsschutz	Schutz vor diversen DoS, DDoS- und Scan-Angriffen

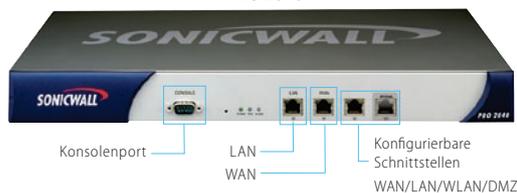
VPN

3DES/AES-Durchsatz	50 MBit/s*
Site-to-Site VPN	Max. 50 Tunnel
Remote Access VPN	Max. 100 Tunnel (10 Clients enthalten)
Verschlüsselung	DES, 3DES, AES (128, 192, 256-Bit)
Authentifizierung	MDS, SHA-1
Schlüsselaustausch	Manueller Schlüssel, PKI (X.509), IKE
XAUTH/RADIUS	Ja
L2TP/IPSec	Ja
Unterstützte Zertifikate	Verisign®, Thawte, Baltimore, RSA Keon, Entrust* sowie Microsoft® CA für SonicWALL-to-SonicWALL VPN
Dead Peer Detection	Ja
DHCP über VPN	Ja
IPSec NAT-Traversal	Ja, NAT_Tv00 und v03
Redundantes VPN-Gateway	Ja
Single Arm VPN	Ja (SonicOS Standard)
Topologien	Hub-and-Spoke, Full Mesh

Deep Inspection Security Services

Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention	Umfangreiche Signaturrendatenbank. Die Kontrolle von Peer-to-Peer- und Instant Messaging-Anwendungen sowie die Aktualisierung von Signaturen zwischen allen Schnittstellen und Zonen erfolgt über die Distributed Enforcement-Architektur. ¹
Content Filtering Service (CFS) Premium Edition	Prüfung nach URLs, Schlüsselwörtern und Content. Blockieren von ActiveX®, Java Applets und Cookies ²
Network Anti-Virus	HTTP/S, SMTP, POP3, IMAP und FTP; Installation von McAfee™-Clients; ³ Blockieren von E-Mail-Anhängen
Integrierte Features	8/5 International-Support in den ersten 90 Tagen, Global VPN Clients und Services siehe oben

PRO 2040



Security-Mehrwertdienste von SonicWALL

Die Internet Security Appliances von SonicWALL lassen sich nahtlos in eine zunehmend größere Anzahl von Security-Mehrwertdiensten einbinden und ermöglichen somit umfassende Sicherheitslösungen. Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention und Content Filtering können über das kabelgebundene und drahtlose LAN angewendet werden.

Networking

DHCP	Relay, interner Server
WAN-Modi	NAT- und transparenter Modus mit statischer oder dynamischer Adressierung
DDNS	Unterstützung für Dienste der folgenden DDNS-Provider: dyndns.org, yi.org, no-ip.com und changeip.com
Authentifizierung	RADIUS, interne Benutzerdatenbank, LDAP, Active Directory (SonicOS Enhanced)
Benutzerdatenbank	250 intern
VoIP	Voll H.323v1-5-kompatibel, SIP, Gatekeeper-Unterstützung, Verwaltung der ein- und ausgehenden Bandbreite, Anrufverfolgung und -überwachung, volle Kompatibilität mit den meisten VoIP Gateway- und Kommunikationsgeräten

System

Verwaltung und Überwachung	Lokale CLI, Web-Oberfläche (HTTP, HTTPS), SNMP v2, zentrale Verwaltung mit SonicWALL GMS
Logging und Reporting	ViewPoint®, lokale Logdatei, Syslog
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS

Hardware

Ports	4 10/100 Auto-Sensing Ethernet 1 serieller Anschluss
Prozessoren	800 MHz x86 Hauptprozessor, Verschlüsselungsbeschleunigung
Speicher (RAM)	128 MB
Flashspeicher	64 MB
Netzspannung	100-240 Volt, 60-50 Hz, 4 A
Leistungsaufnahme (max.)	65 W
Wärmeabgabe	241 BTU
Zertifikate Ausstehend	ICSA IPSec VPN 1.0d ICSA Firewall 4.1, EAL-2, FIPS 140-2
Abmessungen	43,2 x 25,4 x 4,5 cm
Gewicht	3,86 kg
Erfüllt folgende Standards/Normen	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, BSMI Class A, MIC, NOM, UL, cUL, TÜV/GS, CB
Umgebungstemperatur	5-40 °C; Luftfeuchtigkeit 10-90% nicht kondensierend
MTBF	11,2 Jahre

* Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren.

- 1) mit 30 Tagen Service
- 2) mit 30 Tagen Service
- 3) mit 30 Tagen Service für 10 User

** Messung des Durchsatzes anhand der HTTP-Dateidownloads



SonicWALL PRO 2040

- SonicWALL PRO 2040 (International) 01-SSC-5701
- SonicWALL SonicOS Enhanced Firmware Upgrade mit 8/5-Support für PRO 2040 01-SSC-5705
- SonicWALL Gateway Anti-Virus, Anti-Spyware und Intrusion Prevention Service für PRO 2040 01-SSC-5757
- SonicWALL Content Filtering Premium Business Edition für PRO 2040 01-SSC-5652
- SonicWALL Content Filtering Premium Gov/Ed Edition für PRO 2040 01-SSC-5662
- SonicWALL Global Security Client (25-User-Lizenz) 01-SSC-5252
- SonicWALL SonicPoint (International) 01-SSC-5523
- SonicWALL Support 8/5 für PRO 2040 01-SSC-5706
- SonicWALL Support 24/7 für PRO 2040 01-SSC-5707

SonicWALL Deutschland
SonicWALL Schweiz
SonicWALL Österreich

Tel.: +49-89-4545-946
Tel.: +41-44-308-3777
Tel.: +41-44-308-3777

www.sonicwall.de
www.sonicwall.ch
www.sonicwall.at

