



SonicWALL TZ 170 SP-Serie

NETWORK SECURITY

Ausfallsicherheit für Geschäftsanwendungen mit VPN-Anbindung

Kein Unternehmen kann sich einen längeren Netzausfall leisten. Das gilt besonders für kleine Einzelhandelsunternehmen, die auf ihr Netzwerk angewiesen sind, um Zahlungen online abzuwickeln, Kreditkartendaten zu verarbeiten oder sensible Kundendaten zu erfassen. Wird der Informationsfluss unterbrochen, kann dies ernstzunehmende finanzielle Auswirkungen haben.

Die SonicWALL® TZ 170 SP-Serie ist die ideale Sicherheitsplattform für kleine Einzelhandels- und POS-Umgebungen, die auf verwaltete und ausfallsichere Netzwerke und VPNs angewiesen sind, um ihre kritischen Daten sicher zu übermitteln.

Die hochskalierbare TZ 170 SP-Serie gewährleistet einen hohen Investitionsschutz und bietet in einer einzigen, kostengünstigen Lösung ein integriertes Analogmodem, IPSec VPN-Funktionen sowie eine sichere Wireless-Anbindung nach 802.11b/g. Mehrere direkt in der Lösung eingebaute WAN-Redundanzfunktionen erhöhen die Verfügbarkeit und ersparen den Ärger, der normalerweise mit einem Ausfall der Internetverbindung einhergeht. Die TZ 170 SP-Serie führt ein automatisches Failover auf eine zweite bzw. auf eine dritte WAN-Verbindung durch. Sobald die ursprüngliche Verbindung wiederhergestellt ist, findet ein Failback statt, damit immer die optimale Verbindung zur Verfügung steht.

Die TZ 170 SP-Serie ist in mehreren Hardware-Konfigurationen erhältlich (z. B. TZ 170 SP und TZ 170 SP Wireless) und unterstützt die Abo-basierten Gateway Protection Services von SonicWALL, wie z. B. Anti-Virus, Anti-Spyware und Intrusion Prevention.

Funktionen und Vorteile

Integriertes und automatisiertes Failover/Failback. Garantiert maximale Netzwerkverfügbarkeit: Bei Ausfall der Erstverbindung wird automatisch auf ein Zweit-WAN oder auf das integrierte Analogmodem umgeschaltet.

Erweitertes IPSec VPN mit 3DES- und AES-Verschlüsselung. Bietet sichere Konnektivität für kritische Geschäftsanwendungen.

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

Sichere 802.11b/g WLAN-Funktionen. IPSec und WPA-Verschlüsselung im drahtlosen High-Speed-Datenverkehr.

Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention. Bietet Echtzeit-Schutz vor den neuesten Viren, Spyware-Angriffen, Software-Schwachstellen und anderem bössartigen Code.

Konfigurierbarer optionaler Port. Kann als zweiter LAN-/WAN-Port, DMZ- oder WLAN-Port für größtmögliche Flexibilität bei der Netzwerkkonfiguration eingerichtet werden.

DDNS (Dynamic Domain Name Service)-Unterstützung. Erlaubt die Verwendung dynamischer IP-Adressen an Remote-Standorten und reduziert so die Kosten für die Bereitstellung von Site-to-Site-VPNs.

- **Integriertes und automatisiertes Failover/Failback**
- **Erweitertes IPSec VPN mit 3DES- und AES-Verschlüsselung**
- **Ausgezeichnetes Global Management System (GMS)**
- **Sichere 802.11b/g WLAN-Funktionen**
- **Gateway Anti-Virus/Anti-Spyware/Intrusion Prevention**
- **Konfigurierbarer optionaler Port**
- **Dynamic Domain Name Service (DDNS)-Unterstützung**

Technische Daten

SonicWALL TZ 170 SP-Serie

Firewall

Unterstützte Nodes	10 (erweiterbar auf 25 bzw. unlimitiert)
SonicOS-Version	SonicOS Standard (TZ 170 SP) SonicOS Enhanced (TZ 170 SP Wireless)
Stateful-Durchsatz*	90 MBit/s
Deep Packet Inspection-Durchsatz	5 MBit/s
Verbindungen	6.000
Regeln	100 (SonicOS Standard/250 SonicOS Enhanced)
DoS-Angriffsschutz	22 Kategorien von DoS-, DDoS- und Scan-Angriffen

VPN

3DES/AES-Durchsatz*	Mehr als 30 MBit/s
Site-to-Site VPN Tunnel	2 (erweiterbar auf 10 mit einem Node-Upgrade)
Gebündelte Global VPN Client-Lizenzen für Remote Access	Optional
Verschlüsselung	DES, 3DES, AES (128, 192, 256-Bit)
Authentifizierung	MDS, SHA-1
Schlüsselaustausch	IKE, manueller Schlüssel, PKI (X.509)
XAUTH/RADIUS	Ja
L2TP/IPSec	Ja
Unterstützte Zertifikate	Verisign, Thawte, Baltimore, RSA Keon, Entrust und 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
Unterstützte Global VPN Client-Plattformen	Microsoft* Windows 2000, Windows XP, Vista 32-Bit (verfügbar im zweiten Halbjahr 2007)

Deep Inspection Security Services

Deep Packet Inspection Signature Service	Umfassende Signaturrendatenbank (keine Server-Unterstützung). Signaturreupdates und Überwachung von Peer-to-Peer- und Instant Messaging-Anwendungen erfolgen über die Distributed Enforcement Architecture.
Content Filtering Service (CFS) Standard Edition	Prüfung nach URLs, Schlüsselwörtern und Content, Blockieren von ActiveX, Java Applets und Cookies
Client Anti-Virus und Anti-Spyware am Gateway	HTTP/S, SMTP, POP3, IMAP und FTP, Installation von McAfee™-Clients
Gebündelte Services	Blockieren von E-Mail-Anhängen 90 Tage internationaler 8/5-Support und Services, siehe oben

Networking

DHCP	Relay, interner Server
NAT Modes	1:1, 1:many, many:1**, many:many, flexible NAT (überlappende IPs)**, PAT**, transparenter Modus
DDNS	Unterstützung für Dienste der folgenden DDNS-Provider: dyndns.org, yi.org, no-ip.com und changeip.com
Routing	Routing-Entscheidungen erfolgen nach Prüfung von Quell-IP, Ziel-IP und IP-Service-Updates**
Authentifizierung	RADIUS, Active Directory**, LDAP**, interne Benutzerdatenbank
Benutzerdatenbank	100 (SonicOS Standard)/150 (SonicOS Enhanced)
VoIP	Voll H.323v1-5-kompatibel, SIP, Gatekeeper-Unterstützung, Verwaltung der ausgehenden Bandbreite, VoIP über WLAN, Deep Inspection Security, vollständige Interoperabilität mit den meisten VoIP Gateway- und Kommunikationsgeräten

System

Zonenspezifische Sicherheitsfunktionen	Ja**
Objektbasiertes Management	Ja**
Verwaltung und Überwachung	Web-Oberfläche (HTTP, HTTPS), SNMP v2; zentrale Verwaltung mit SonicWALL GMS
Logging und Reporting	ViewPoint®, lokale Logdatei, Syslog
Failover/Failback	Ja**
WAN/WAN/Analog	Ja**
WAN/WAN	Ja**
WAN/Analog	Ja
Lastverteilung	Ja, mit prozentbasierter, Round-Robin-, und Spillover-Lastverteilung**
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS
Wireless-Standards	802.11b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS

Hardware

Schnittstellen	(7) 10/100 Ethernet (WAN, LAN-Switch mit 5 Ports, optionaler Port)
Prozessor	SonicWALL-Sicherheitsprozessor
Speicher (RAM)	64 MB
Flash-Speicher	8 MB
Integriertes Modem	v.92-Analogmodem
Antennen	Duale, externe 5 dBi Diversity-Antennen (TZ 170 SP Wireless)
Sendeleistung***	802.11b 802.11g Max. Bis zu 21 dBm/125 mW (TZ 170 SP Wireless) Max. Bis zu 19 dBm/79 mW (TZ 170 SP Wireless)
Kanäle	Kanäle 1-11 Kanäle 1-13 Kanäle 1-14 USA, Kanada, Taiwan (TZ 170 SP Wireless) EU, Korea (TZ 170 SP Wireless) Japan (TZ 170 SP Wireless)
Empfangsleistung des Senders	(-86, -78, -70, -68) dBm bei (6, 24, 48, 54) MBit/s (TZ 170 SP Wireless)
Eingangsspannung	100-240 VAC, 60-50 Hz, 6 A
Maximale Leistungsaufnahme	9,4 W (TZ 170 SP)/10,6 W (TZ 170 SP Wireless)
Wärmeabgabe	32,1 BTU (TZ 170 SP)/36,1 BTU (TZ 170 SP Wireless)
Zertifikate	ICSA IPsec VPN 1.0d ICSA Firewall 4.1, FIPS 140-2, EAL-2
Abmessungen	23,0 x 16,8 x 4,1 cm
Gewicht	0,52 kg (TZ 170 SP) 0,64 kg (TZ 170 SP Wireless)
Erfüllt folgende Standards/Normen	FCC Class B, ICES Class B, CE, C-Tick, VCCI, BSMI, MIC, UL, cUL, TÜV/GS, CB, NOM
Umgebungstemperatur	5-40 °C
MTBF	Luftfeuchtigkeit 10 - 90 % nicht kondensierend 11,7 Jahre (TZ 170 SP) 7,5 Jahre (TZ 170 SP Wireless)

* Testmethoden: Maximalleistung auf Basis von RFC 2544 (für Firewall). Die tatsächliche Leistung kann je nach Netzwerkbedingungen bzw. aktivierten Diensten variieren. Messung des VPN-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1280 Bytes pro Paket.

** Mit SonicOS Enhanced.

*** Variable Sendeleistung entsprechend den landesspezifischen Vorgaben.



SonicWALL TZ 170 SP
01-SSC-5732 (International)



SonicWALL TZ 170 SP Wireless
01-SSC-5742 (International)

Die Network Security Appliances von SonicWALL lassen sich nahtlos in eine zunehmend größere Anzahl von Security-Mehrwertdiensten einbinden und ermöglichen somit umfassende Sicherheitslösungen. Virenschutz, Spyware-Schutz, Intrusion Prevention und Content Filtering können sowohl in kabelgebundenen als auch in drahtlosen LANs implementiert werden. Weitere Informationen erhalten Sie auf unserer Website unter www.sonicwall.com/de.

SonicWALL Deutschland

Tel.: +49 89 4545 946

www.sonicwall.de

SonicWALL Schweiz

Tel.: +41 44 810 31 35

www.sonicwall.ch

SonicWALL Österreich

Tel.: +41 44 810 31 35

www.sonicwall.at

