



SonicWall TZ 170 Router



Features:

- **Real-Time Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention.** The TZ 170 extends security from the network core to the perimeter by integrating support for SonicWALL's Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, delivering real-time protection against the latest blended threats, including viruses, spyware, worms, Trojans, software vulnerabilities and other malicious code.¹
- **Powerful Content Filtering.** The TZ 170 supports SonicWALL's Content Filtering Service, providing an enterprise-class, scalable content filtering service that enhances productivity and security without requiring additional server or deployment costs.
- **Deep Packet Inspection Firewall.** The TZ 170 features a configurable, high performance deep packet inspection firewall for extended protection to key Internet services such as Web, e-mail, file transfer, Windows services, and DNS.
- **WorkPort.** The SonicWALL TZ 170 includes an optional port that can be configured as a WorkPort, creating an independent, isolated zone of trusted

network security that protects corporate networks from malicious attacks that can occur when telecommuters share broadband Internet access with networked home computers.

- **Comprehensive Central Management Support.** Every SonicWALL Internet security appliance can be managed using SonicWALL's award-winning Global Management System, which provides network administrators with the tools for simplified configuration, enforcement and management of global security policies, VPN, and services, all from a central location.

SonicOS Enhanced, an optional software upgrade for the SonicWALL TZ 170, adds:

- **Real-Time Blacklist Spam Filtering.** The TZ 170 provides the ability to use DNS to query Real-Time Black List (RBL) services that track well-known spam and open-relay SMTP servers, and to deny SMTP connections from servers that appear on the lists.²
- **Configurable Optional Port.** Upgrading to SonicOS Enhanced allows the optional port on the TZ 170 Wireless to be configured either as an additional LAN, WAN, DMZ or WLAN offering greater network configuration flexibility as well as internal security.
- **WAN ISP Failover and Load Balancing.** The SonicWALL TZ 170 offers the ability to configure the optional port as a secondary WAN port, delivering highly reliable network connectivity and robust performance. This secondary WAN port can be used in "active-active" load sharing or failover configuration providing a highly efficient method for maximizing total network bandwidth.
- **Object-based Management.** The SonicWALL TZ 170 provides the ability to define an object such as a user group, network address range, service or interface. When security policies change, the administrator can modify the pre-defined object and propagate the changes instantly without redefining rules, enabling businesses to implement and manage security policies easily and consistently.
- **Policy-based NAT.** In addition to standard NAT (many-to-one) functionality, the SonicWALL TZ 170 also exposes control of NAT policies to administrators for one-to-one NAT, many-to-many NAT, one-to-many NAT, inbound Port Address Translation (PAT), flexible NAT (for overlapping IP addresses), as well as NAT policies on selective source/destination/source translations. The result is greater control and flexibility to support and manage various NAT requirements.