

## Overview:

The SonicWall TZ series enables small to mid-size organizations and distributed enterprises realize the benefits of an integrated security solution that checks all the boxes. Combining high-speed threat prevention and software-defined wide area networking (SD-WAN) technology with an extensive range of networking and wireless features plus simplified deployment and centralized management, the TZ series provides a unified security solution at a low total cost of ownership.

### Flexible, integrated security solution

The foundation of the TZ series is SonicOS, SonicWall's feature-rich operating system. SonicOS includes a powerful set of capabilities that provides organizations with the flexibility to tune these Unified Threat Management (UTM) firewalls to their specific network requirements. For example, creating a secure high-speed wireless network is simplified through a built-in wireless controller and support for the IEEE 802.11ac standard or by adding our SonicWave 802.11ac Wave 2 access points. To reduce the cost and complexity of connecting high-speed wireless access points and other Power over Ethernet (PoE)-enabled devices such as IP cameras, phones and printers, the TZ300P and TZ600P provide PoE/PoE+ power.

Distributed retail businesses and campus environments can take advantage of the many tools in SonicOS to gain even greater benefits. Branch locations are able to exchange information securely with the central office using virtual private networking (VPN). Creating virtual LANs (VLANs) enables segmentation of the network into separate corporate and customer groups with rules that determine the level of communication with devices on other VLANs. SD-WAN offers a secure alternative to costly MPLS circuits while delivering consistent application performance and availability. Deploying TZ firewalls to remote locations is easy using Zero-Touch Deployment which enables provisioning of the firewall remotely through the cloud.

### Superior threat prevention and performance

Our vision for securing networks in today's continually-evolving cyber threat landscape is automated, realtime threat detection and prevention. Through a combination of cloud-based and on-box technologies we deliver protection to our firewalls that's been validated by independent third-party testing for its extremely high security effectiveness. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine detects and blocks malware and zero-day threats by inspecting directly in memory. RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, our patented single-pass Reassembly-Free Deep Packet Inspection (RFDPI) engine examines every byte of every packet, inspecting both inbound and outbound traffic directly on the firewall. By leveraging Capture ATP with RTDMI technology in the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, anti-malware and web/ URL filtering, TZ series firewalls stop malware, ransomware and other threats at the gateway. For mobile devices used outside the firewall perimeter, SonicWall Capture Client provides an added layer of protection by applying advanced threat protection techniques such as machine learning and system rollback. Capture Client also leverages the deep inspection of encrypted TLS traffic (DPI-SSL) on TZ series firewalls by installing and managing trusted TLS certificates.

The continued growth in the use of encryption to secure web sessions means it is imperative firewalls are able to scan encrypted traffic for threats. TZ series firewalls provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. The firewall searches for protocol non-compliance, threats, zerodays, intrusions, and even defined criteria by looking deep inside every packet. The deep packet inspection engine detects and prevents hidden attacks that leverage cryptography. It also blocks encrypted malware downloads, ceases the spread of infections and thwarts command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.

### Easy deployment, setup and ongoing management

SonicWall makes it easy to configure and manage TZ series firewalls and SonicWave 802.11ac Wave 2 access points no matter where you deploy them. Centralized management, reporting, licensing and analytics are handled through our cloud-based Capture Security Center which offers the ultimate in visibility, agility and capacity to centrally govern the entire SonicWall security ecosystem from a single pane of glass.

A key component of the Capture Security Center is Zero-Touch Deployment. This cloud-based feature simplifies and speeds the deployment and provisioning of SonicWall firewalls at remote and branch office locations. The process requires minimal user intervention, and is fully automated to operationalize firewalls at scale in just a few steps. This significantly reduces the time, cost and complexity associated with installation and configuration,

while security and connectivity occurs instantly and automatically. Together, the simplified deployment and setup along with the ease of management enable organizations to lower their total cost of ownership and realize a high return on investment.

\* 802.11ac currently not available on SOHO/SOHO 250 models; SOHO/SOHO 250 models support 802.11a/b/g/n

Benefits:

### **Flexible, integrated security solution**

- Secure SD-WAN
- Powerful SonicOS operating system
- High-speed 802.11ac wireless
- Power over Ethernet (PoE/PoE+)
- Network segmentation with VLANs

### **Superior threat prevention and performance**

- Patent-pending real-time deep memory inspection technology
- Patented reassembly-free deep packet inspection technology
- On-box and cloud-based threat prevention
- TLS/SSL decryption and inspection
- Industry-validated security effectiveness
- Dedicated Capture Labs threat research team
- Endpoint security with Capture Client

### **Easy deployment, setup and ongoing management**

- Zero-Touch Deployment
- Cloud-based and on-premises centralized management
- Scalable line of firewalls
- Low total cost of ownership