SONICWALL®

TECH BRIEF

Wireless Network Security for Schools

Scan and protect Wi-Fi device traffic across schools and districts

Abstract

This brief offers IT directors and administrators at K-12 schools and school districts a deep dive into deploying Wireless Network Security solutions from SonicWall.

Introduction

K-12 school districts share student, faculty and administrative data across local networks, wide area networks and wireless networks. Districts must provide secure, high-speed wireless access for students, faculty and staff using either school-issued or personal devices — all without impeding academic performance and productivity.

Wireless network security

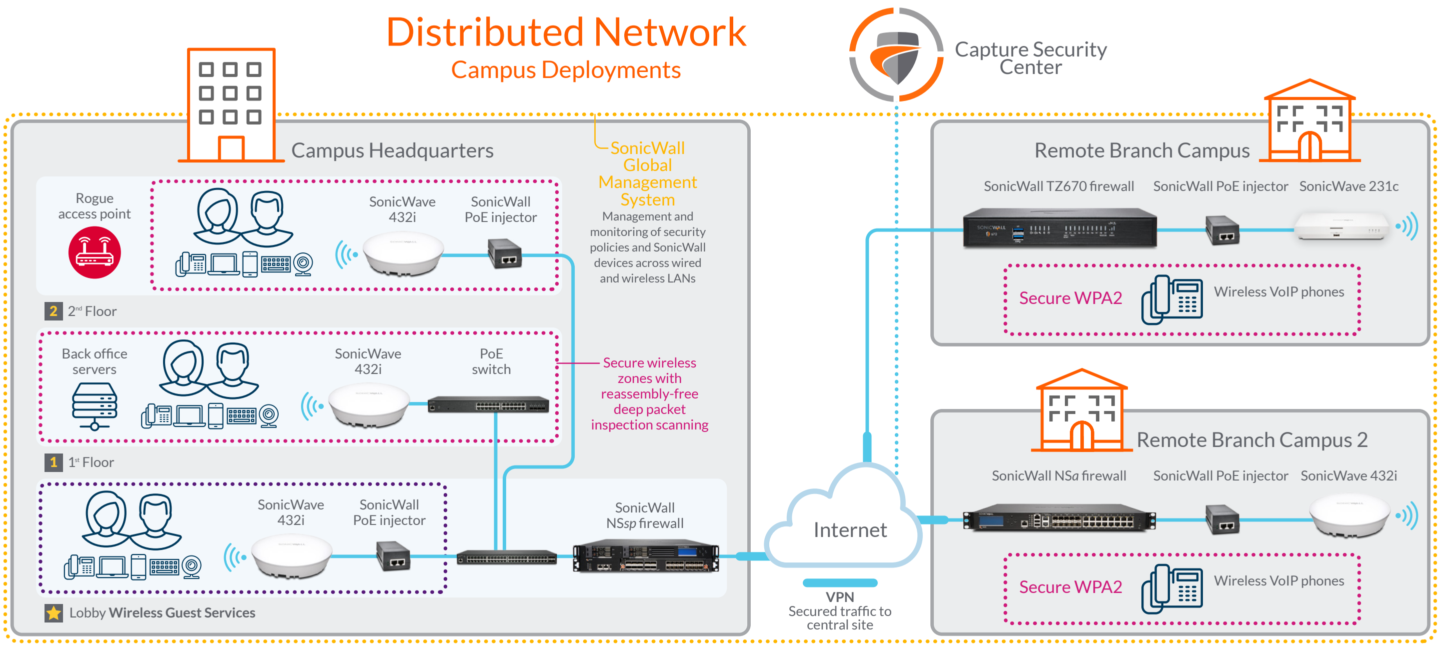
SonicWall SonicWave series wireless access points (APs) combine high-performance IEEE 802.11ac Wave 2 wireless technology with flexible deployment options.

These highly secure APs can be managed via the cloud using SonicWall Wireless Network Manager (WNM) or through SonicWall's industry-leading next-generation firewalls. The result is a solution that could be untethered from the firewall to provide a superior experience for Wi-Fi users that's as secure as any wired connection. The APs work together with SonicWall Switches for extending wired connectivity. Plus, SonicWaves have a plenum-rated chassis for safe installation in a wide variety of environments, such as air-handling spaces or above suspended ceilings.

The SonicWave series APs can achieve high data rates while maintaining higher performance levels at greater ranges, depending on environmental conditions. SonicWaves support a wide range of wireless standards and security protocols, including 802.11 a/b/g/n/ac and WPA3. This allows organizations to leverage prior investments in devices that are incapable of supporting higher encryption standards, while easing migration to 802.11ac Wave 2.

The 802.11ac standard operates in the 5 GHz frequency band, which has fewer wireless devices competing for airspace and is therefore less prone to signal interference. In addition, 802.11ac Wave 2 uses wider 160 MHz channels and has more non-overlapping channels. All of these features combined yield a higher quality signal. The increase in bandwidth capacity and greater number of spatial streams, combined with MU-MIMO and the improved processing offered by 802.11ac Wave 2, result in more reliable wireless coverage.

SonicWaves also support AirTime Fairness and FairNet, which guarantees a minimum amount of bandwidth to each wireless client to prevent disproportionate bandwidth consumption by a single user. In combination, SonicWaves support auto-channel assignment that prevents interference on a best-effort basis. Furthermore, fast roaming on the SonicWave access points enables users to roam from one location to another without dropping connectivity.



Intuitive cloud management

SonicWall WNM provides an intuitive user interface to manage all SonicWave APs from a single pane of glass via SonicWall Capture Security Center (CSC). Additionally, the dashboard offers integrated SonicWall Switch management, providing centralized management of switches and APs. Easily monitor and manage networks with alerts and rich analytics updated in real-time. Always stay up-to-date with the current features and enhancements from the latest firmware. Updates are pushed automatically to APs, eliminating manual updates and chances of human error.

Simplified firewall management

SonicWaves are automatically detected, provisioned and updated by the wireless controller in the managing SonicWall NS*sp*, NS*a*, or TZ Series firewall. WLAN administration is also handled directly from the managing firewall, simplifying setup and centralizing ongoing management. Ongoing management and monitoring of SonicWaves and security are handled centrally through the firewall or through the SonicWall GMS, providing administrators with a single pane of glass from which to manage all aspects of the network — both wired and wireless.

SonicWaves are powered by SonicWall IEEE 802.11ac Power over Ethernet (PoE) Injector or SonicWall Switches. In addition, SonicWaves enable both radios to enter sleep mode for power saving when no clients are actively connected. The AP will exit sleep mode once a client attempts to associate with it. With dimmable LEDs (excluding power), SonicWaves fit perfectly into environments that need discreet wireless coverage.

Multi-RADIUS Authentication provides enterprise-class redundancy by enabling organizations to deploy multiple RADIUS servers in active/passive mode for high availability. Should the primary RADIUS server fail, the managing SonicWall firewall discovers the failure and switches to the secondary server, ensuring wireless devices can continue to authenticate.

Further, multi-RADIUS authentication can be supported on each virtual access point and configured for WPA-Enterprise, WPA2-Enterprise, or WPA2-Auto-Enterprise mode. Administrators can create up to eight SSIDs on the same access point, each with its own dedicated authentication and privacy settings. This provides logical segmentation of secure wireless network traffic and secure customer access.

Wireless guest services enable administrators to provide internet-only access for guest users. This access is separate from internal access and requires guest users to securely authenticate to a virtual access point before access is granted. Lightweight hotspot messaging extends the SonicWall wireless guest services model of differentiated internet access for guest users, enabling extensive customization of the authentication interface and the use of any kind of authentication scheme. The captive portal forces a user's device to view a page and provide authentication through a web browser before internet access is granted.

SonicWall NGFWs scan all inbound and outbound traffic on wired and wireless networks and eliminate intrusions, spyware, viruses and other threats before they enter the network. The same set of security policies can be enforced over both wired and wireless networks. Cloud ACL (an extension to local ACL) is deployed and managed from a centralized RADIUS server in the cloud. This eliminates local ACL scalability issues, enabling organizations to configure authentication accounts based on their specific requirements. In addition, MAC authentication can be enforced on all Wi-Fi-enabled devices, even if they are not capable of 802.1x support. This adds another layer of protection to the wireless network.

For increased flexibility, most SonicWaves even allow for the dedication of one radio for wireless intrusion detection and prevention scanning to meet compliance mandates, while the other two continue to serve clients. Wireless intrusion detection and prevention scans the wireless network for unauthorized (rogue) access points and the managing firewall automatically takes countermeasures, such as preventing any connections to the device.

In addition to intrusion prevention, SSL decryption and inspection, application control, and content filtering, the wireless network security solution also integrates additional security-related features, including wireless intrusion detection and prevention, virtual access points, wireless guest services, cloud access control list, and more.

Conclusion

SonicWall wireless network security extends network protection to provide secure, high-speed wireless access for students, faculty and staff, using either school-issued or personal devices.

Learn more at www.sonicwall.com/K12.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for schools, universities, enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.