SONICWALL®

EXECUTIVE BRIEF: SECURING THE NEXT WAVE OF WIRELESS

Abstract

Wireless connectivity is ubiquitous in today's mobile, global economy. Wireless devices range from smartphones and laptops to security cameras and virtual reality headsets. Businesses need to recognize and address their need for high quality, performance, and security across wireless networks and endpoints.

Today's business in a wireless world

High-speed wireless connectivity is no longer optional in today's network landscape. It's become a necessity as businesses look to increase customer value and improve employee productivity through BYOD initiatives and the growing use of bandwidth-intensive apps. Other organizations, such as schools and universities, use wireless to provide students with a more connected educational environment. From the user perspective, wireless connectivity is expected regardless of the location or device type. What's more, there is a growing trend toward the use of "wireless only" devices in the workplace, the classroom, hospitals and in everyday life.

Wireless IoT

Driving all of this are several key factors. The first is the continued proliferation of Wi-Fi-enabled devices, both personal and IT-issued. According to ABI Research, more than 20 billion Wi-Fi chipsets are expected to ship between 2016 and 2021. Furthermore, more than 95% of devices shipped in 2021 would support 5GHz. Second, the Internet of Things (IoT) has also expanded as devices not traditionally known for wireless functionality including cars, smart home devices (e.g. refrigerators, security cameras, etc.) and others are now able to connect to the Internet using wireless. Multiple analyst firms have predicted there will be 50 billion IoT devices by 2020.

Third, coupled with the increase in Wi-Fi-ready devices is the use of bandwidth-intensive applications such as HD multimedia, cloud and mobile apps, which are increasingly hosted in the network. And finally, the newest wireless standard, 802.11ac Wave 2, has gone mainstream as users look to take advantage of the promise of multi-gigabit wireless speeds. Together, this combination is driving the need for organizations to provide customers, employees and students with a high-speed wireless solution that significantly enhances the user experience.

Home on the enterprise

According to Wi-Fi Alliance, home is becoming an enterprise network. This is caused mainly due to the emergence of everyday connected things, personal assistants, and cordless virtual reality gears. Furthermore, the impact of Wi-Fi can be felt in our everyday lives not just by users but even companies like Amazon, Facebook, Netflix and major airlines. They depend on Wi-Fi to perform day-to-day operations like same-day shipping, mobile access to social media, streaming media services and even on-time airline departures. With the introductions of new standards and protocols, Wi-Fi is bound to further evolve and enhance.

Assuring wireless quality of service

While speed is always important in any network environment, so too is the quality of the wireless connection in high-density environments including outdoor locations where conditions can be harsh. In many instances multiple devices are connecting to the same access point and competing for their share of the bandwidth. This "device congestion" causes interference that can result in signal degradation and ultimately poor performance. Additional factors, including physical objects (e.g. buildings, walls, trees) and other devices that share the same frequency or channel (e.g. microwaves, cordless phones), can interfere with the wireless signal by obstructing the radio frequency transmission path. All have the potential to impact applications such as video streaming which can suffer when packets are delayed and the image quality is poor or the video is slowed due to buffering.

A growing threat to security

Underlying all of this is the need for the wireless traffic to be secured from malicious threats and vulnerabilities over the Internet. Many of today's wireless networking products offer protection from activities such as rogue access points or access point mapping, to keep intruders from gaining access to the network and ultimately critical resources. However, they often lack the ability to provide deep packet inspection scanning of encrypted traffic over the wireless LAN, putting organizations at risk. These products may also lack additional security features such as rogue access point detection and the ability to segment external user access from internal. In addition to the security risks, the products can be time-consuming to deploy, monitor and manage. They may also lack support features for auto-configuration and centralized management which are especially vital when creating and maintaining a large wireless network infrastructure.

Conclusions

What organizations require today from their wireless network is more than just faster connectivity. They need a solution that delivers greater throughput, better signal quality and an enhanced user experience from a wide variety of wireless clients in high-density environments. Not only that, it must be able to scan for and remove threats over the wireless traffic, whether unencrypted or encrypted, to secure the network while simplifying deployment and ongoing management.

Learn more. Visit www.sonicwall.com/en-us/products/firewalls/wireless-security.

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Refer to our website for additional information.
www.sonicwall.com