EXECUTIVE BRIEF: WHY YOU NEED COMPLETE WIRELESS AND MOBILE ACCESS SECURITY

Detect and prevent cyber attacks across wired, wireless and mobile networks

Abstract

Organizations today need to provide workers with high-speed access to resources over wired, wireless and mobile networks. However, cybercriminals are leveraging each of these vectors to initiate advanced attacks, with encrypted threats and zero-day attacks. Organizations can also lose control over data in remote team environments using wireless and mobile networks that connect to cloud services. Disruption in access leads to a loss of productivity, gives rise to shadow IT, and creates gaps in an organization's security posture.

Anywhere access to resources

Today's workers are on the go. They require 24x7 access to corporate resources using the device of their choice from anywhere. Organizations also are embracing BYOD, IoT, mobility and cloud initiatives. To stay competitive, organizations need to provide access to resources seamlessly across wired networks, wireless networks and mobile networks. Wired networks are evolving to 2.5G, 5G and 10G. Yet it's not just wired devices that are connecting to the network. Endpoints vary from desktops to laptops to tablets and smartphones. And with the increasing number of BYOD and Internet of Things (IoT) endpoints, more devices than ever are connecting to the corporate network.

Not only must access be available anywhere, anytime and on any device access, it also has to be fast and secure.

Organizations rely increasingly on high-speed wireless connectivity in their environments. And mobile and remote workers connect over VPNs from homes, branch offices, workshare offices, airports, hotels or cafés. As a result, employees have come to expect the same user experience and high-performance access not only on wired networks, but across their wireless and mobile connections as well. When employees are on the road, they require access to the same business applications they have when connected to wired networks in the office.

Cyber attacks leverage wired, wireless and mobile networks

While high-speed anywhere access and connectivity is important to users and organizations alike, so too is the security of the data that travels across the network. Ultimately, organizations need to extend comprehensive breach detection and prevention security features seamlessly across wired, wireless and mobile networks.

Over any network platform, one major challenge for combating cyber attacks is that most threats are now encrypted. The trend towards TLS/SSL encryption has been on the rise for several years. As web traffic has grown, so has encryption, from 5.3 trillion web connections in 2015 to 7.3 trillion in 2016, according to the SonicWall Capture Threat Network. The majority of web sessions that the Capture Threat Network detected throughout the year were TLS/SSL encrypted, comprising 62 percent of web traffic. That number will continue to rise as more websites use encryption to secure connections to their site.

In addition, advanced threats such as zero-day exploits and custom malware are on the rise. Organizations of every size are targeted by cybercriminals who continually seek, find and exploit holes in vulnerable software. They do this to gain access to networks, systems and data, often perpetuating serious harm within minutes. To better detect these unknown threats, security professionals are deploying advanced threat detection technologies such as virtual sandboxes, which analyze the behavior of suspicious files and uncover hidden malware. However, threats are getting smarter. Malware is now being designed to detect the presence of virtual sandboxes and then evade them. Today's sandbox environments must be as comprehensive and dynamic as the threats they seek to prevent. It is imperative today to be able to decrypt, scan and sandbox suspicious files in all traffic, whether over wired, wireless or mobile networks.

Remote team collaboration

Organizations can also lose control over data in remote team environments using wireless and mobile networks that connect to cloud services. Many organizations have remote teams that need to use collaborative tools such as SharePoint or Dropbox to share files and work collectively. Project collaborations also typically involve external stakeholders such as third-party contracts or partners. For example, both K-12 and higher education institutions provide students and faculty with wireless internet access to connect to and collaborate with others locally and across the world.

As a result, files are constantly uploaded or shared using personal (unmanaged) laptops and smartphones over mobile and wireless networks. Anywhere you provide the ability to share files, there is a risk of malware being uploaded. However, when IT departments clamp down with restrictive file sharing policies for security reasons, end users start using personal file sharing accounts, such as Google Drive, to transfer files and collaborate. These files bypass network firewalls when remote users access corporate network using full VPN access. In addition, organizations lose control of data when it goes out of the security perimeter via public cloud services like Google drive or email or USBs. This is a high security and compliance risk for organizations.

Network Performance and workforce productivity

Not only must access be available anywhere, anytime and on any device, it also has to be fast and secure. The security needed to protect against modern cyber threats can potentially impact workforce productivity, increase IT overhead and, ultimately raise the total cost of ownership for an organization.

The growing volume of traffic alone affects available bandwidth and network performance. The number of Wi-Fi-enabled devices, both personal and IT-issued, continues to increase as the use and importance of mobility grows. According to Gartner, nearly 1.5 billion smartphones alone were shipped in 2016.[1] By the end of that same year, the Wi-Fi Alliance expected Wi-Fi shipments to surpass 15 billion devices.[2] Coupled with the increase in Wi-Fi devices is the use of bandwidth intensive applications such as HD multimedia and cloud and mobile apps.

The growth of the IoT has fueled an increase in the number of wireless devices that can run bandwidth-intensive applications. The use of video and collaboration applications, such as Microsoft Lync, SharePoint and WebEx, require large amounts of available bandwidth to perform optimally. In addition, cloud computing can involve transferring large data files across the wireless network, using up valuable bandwidth.

Moreover, the growth in the number of devices has created an environment where wireless signals frequently interfere with each other due to the large number of devices sharing the same network. This includes everything from laptops, smartphones, tablets and access points to microwaves, Bluetooth devices and more. The resulting poor performance is experienced across enterprise verticals including healthcare, education, airports and shopping malls. Outdoor wireless also has become an expectation in stadiums, campuses, construction sites, industrial parks and other open-air places, where signal can be impacted by the physical environment including trees and other buildings.

Security services themselves also affect network performance. The ability to decrypt and scan encrypted traffic for threats with little or no latency is critical, as any delay slows down the flow of data through the network. Decrypting and scanning potentially thousands of encrypted web connections for threats simultaneously can be very compute-intensive. Legacy firewalls may decrypt the traffic and perform some threat detection, but not prevention. Or, they may do everything that's required, just very slowly due to a performance penalty. Organizations have resorted to even switching off key firewall services in order to maintain performance.

All this is driving the need for organizations to provide customers, employees and students with an enhanced experience across platforms.

The latest in high-speed wireless technology, 802.11ac Wave 2, provides multi-gigabit wireless throughput. However, to realize this performance potential, both the access point and connecting devices must support the 802.11ac Wave 2 wireless standard. In addition, to enable the required level of wireless throughput, most firewalls must utilize a backward-compatible 5 GbE or 10 GbE port, which is far more capacity than is required, or add switch which increases the cost.

Complicating performance and security further, most organizations have a blend of on-premises and cloud applications creating a hybrid IT environment. IT department have the overhead of maintaining multiple user directories for applications deployed in their local datacenters as well as third-party SaaS cloud applications. These directories need to be updated constantly to make sure the right people have the right access to the right applications at the right time. Users are forced to maintain and remember multiple URLs and passwords that lead to bad security practices. Any disruption in access leads to a loss of productivity, gives rise to shadow IT, and creates gaps in an organization's security posture.

Conclusion

Learn more. Find out how to provide breach detection and prevention across your wired, wireless and mobile networks. Read our Solution Brief, Best practices for wireless and mobile access security, and visit our Wireless and Mobility web page.

[1] *http://www.gartner.com/newsroom/id/3609817*

[2] *http://www.wi-fi.org/news-events/newsroom/wi-fi-device-shipments-to-surpass-15-billion-by-end-of-2016*

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.

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

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

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

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