SOPHOS

Wireless network security: A how-to guide for SMBs

A Sophos Whitepaper November 2014

Wireless network security: A how-to guide for SMBs

WiFi networks are a requirement for doing business today. Employees rely on them to have constant access to their business applications to check customer data, process transactions, etc. Customers expect WiFi access for the convenience of using their mobile devices anywhere, any time – whether they are waiting for car repairs, shopping in a second-hand store or enjoying a meal at a bistro.

Unfortunately, research shows that small- and medium-business (SMB) WiFi networks represent a security risk. In a study dubbed Project Warbike, Sophos took one man, a bike, computer, GPS, two dynamos and some solar panels to the streets of London (and many other cities around the globe) to determine how many wireless networks were unsecured. Of the nearly 107,000 wireless networks surveyed, 27% had poor, or no, security. The highest density of poorly secured networks occurred along streets with a high number of small businesses.

Setting up an SMB WiFi network is deceptively simple. Install a consumer-grade access point and – voilà! – everyone has network access. However, business WiFi networks are more complex than home WiFi networks. Business networks must support visitors and contractors as well as employees – all of whom need varying levels of access. Businesses also need to enable employees to access the WiFi network with their personal devices. Without proper access controls anybody and everybody can connect to the network, putting sensitive data at risk. SMBs must have the ability to secure and manage their networks.

The problem and risks

As evidenced by Project Warbike, SMBs are neglecting WiFi security basics. Enabling strong encryption has long been a WiFi security best practice to prevent eavesdroppers from sniffing wireless traffic. But of the nearly 40% of networks using poor or weak encryption, half were using obsolete wired equivalent privacy (WEP) encryption – which can be broken in seconds. The other half wasn't using any encryption at all.

Changing the network's default public name (or service set identifier, SSID) is also a WiFi security best practice. But of all the wireless networks identified during Project Warbike, 9% were using default network names with no random element, while another 12% were using the default name with some random element per device (e.g., Default-165496). [1]

WiFi management challenges are further putting SMB WiFi networks at risk. Consumer access points are insufficient for small business needs. They have to be set up individually and often offer limited or no support for business requirements, such as virtual private networking. Businesses also risk data loss by not managing guest access. Enterprise solutions, on the other hand, are often too resource intensive. They can put undue strain on costs and staff time. In addition, many IT managers in smaller business are all-round talents, who don't necessarily have the skills to manage an enterprise wireless solution.

To further complicate matters, SMBs must understand the implications of an ever-evolving technology. The newest WiFi standard was approved in January 2014. 802.11ac supports single-link and multi-station enhancements. A throughput of at least 500 megabits per second (Mbit/s) is expected for a single link WLAN, and at least 1 gigabit per second is expected for a multi-station WLAN. These enhancements enable the simultaneous streaming of HD video to multiple clients, rapid synchronization and the backup of large data files. 802.11ac access points and routers also include a USB 3.0 interface.

[1] These figures exclude default names of obviously identifiable, intentionally open hotspots such as those in hotels and cafes.

Security requirements for small business WiFi networks

The good news is that WiFi network security doesn't have to be difficult. SMBs can easily improve their security posture starting with these five basic security principles:

1. Choose WPA2 encryption – When configuring the wireless network, select encryption using WPA2, the latest security algorithm. Attackers can break older security options like WEP with something as simple as a browser add-on or mobile phone application.

2. Create longer passwords with special characters – With code-cracking software an attacker can unlock a weak password in seconds. Create passwords that are longer than 10 characters and include special characters, numbers, and both upper- and lower-case letters.

3. Rename default SSIDs – Because WPA2 encryption includes the SSID as part of the password, hackers enter common SSIDs to crack passwords more easily.

4. Don't include business information in SSIDs – SSIDs should not identify your business or location. This helps prevent hackers from knowing that the network is worth trying to compromise.

5. Tune the range of the radio – Modern access points have multiple antennas and transmit power to help users access the network from farther away. Reducing the power of the radio controls how far from your location someone can pick up the signal, making it more difficult to compromise the network.

Beyond these WiFi security basics, SMBs need to implement business-grade security measures such as controlled guest access. Often, customers, suppliers and other office visitors are given IDs and passwords that provide perpetual access to internal networks. Stories abound of contractors whose passwords remained valid for weeks or months after they moved on to other employers. Access should be limited in time and to specific resources on the network.

SMBs also need to simplify how they manage multiple access points in central offices. Deploying and managing wireless access points can be time consuming. Complex administration raises staffing costs and increases the likelihood of accidental misconfigurations that cause security vulnerabilities.

Similarly, SMBs must address how they manage access points in remote offices. Providing technical support to remote and branch offices can be a challenge. Constant travel is rarely an option, and it is difficult to work through remote personnel, particularly if no local IT staff is available. Administrators need to find tools that allow them to deploy, monitor and update remote access points from a central console.

Finally, wireless traffic should be integrated into the network security infrastructure. Cybercriminals are increasingly targeting wireless traffic as an avenue to penetrate corporate LANs. To prevent wireless traffic from becoming a major threat vector, SMBs should ensure that wireless traffic flows through the full network security infrastructure so it can be scanned for malware. Probes and attacks can also be detected.

Getting from here to there

Securing an SMB WiFi network goes far beyond configuring SSIDs and passwords. Admins need to manage the basics in multiple locations efficiently and reliably. They must be able to tailor access to different employee and guest use cases. They need to ensure that WiFi traffic is scanned and secured just as efficiently as wired LAN traffic.

Because cost is always a factor, SMBs must be able to accomplish all of this without additional staff or training. That requires simplicity, which is achieved through equipment consolidation and integration. Only a professional solution can provide the business-level WiFi security that SMBs need.

Business WiFi solutions offer a number of options for different deployment scenarios. Access points can be placed on a desktop, or wall- or ceiling-mounted, depending on what coverage is required and how the office space is set up. There are even options that are suitable for outdoor use to provide coverage for loading bays and similar areas, which may be more exposed. Alternatively, firewall or UTM appliances with a built in access point can either provide an all-in-one solution or be extended using external access points.

When evaluating a WiFi security solution, Forrester Research advises using "the five S's": [2]

> "Buying IT solutions based on the fastest access point (AP) or the cheapest 802.11ac AP is dead. However, looking for wireless solutions for a particular business can be daunting due to a dizzying array of architectures and marketing buzz. Forrester recommends that you look for the following in a solution: scalable, shared, simplified, standardized, and secure."

1.1 Evaluate Wireless LANs Using Five Simple Architectural Characteristics

Business Wireless Edge

	Vendor Terminology	I&O Technical Needs
Scalable	Flexible/ resilient	‣ Support a variety of connection environments, conditions, devices, apps, and users with a multitude of software, hardware, and protocol options ‣ Linear cost model and architecture
Shared	Unified/open/ programmable	‣ Built for multi-tenancy with differentiated user and services ‣ Shared resources with business professionals, other teams, and systems ‣ Managed a single system
Simplified	Automated	‣ Simple and intuitive interfaces ‣ Self-forming ‣ Wizards and templates for apps and business elements
Standardized	Unified/open/ programmable	‣ Standard interfaces ‣ Orchestration integration ‣ Standard processes and procedures for mobile users and administrators
Secure	Secured	‣ Integrated network and application controls, overlaid identity and data ‣ Managed as a workflow, not a single technology

115916

Source: The Forrester Wave™: Wireless Local Area Network Solutions, Q3

[2] The Forrester Wave™: Wireless Local Area Network Solutions, Q3 2014, Forrester Research, Inc., August 29, 2014.

Introduction to Sophos Wireless Protection

Sophos Wireless Protection, Sophos Access Points and Sophos SG Series appliances with integrated WiFi offer full wireless security while providing flexible access for employees and guests. As just one of the security solutions available as part of Sophos UTM, all management is through a single central console. The solution is fully scalable and can include Network, Web, Email, Web Server, Wireless and Endpoint Protection. Integration with Sophos Mobile Control provides network access control for mobile devices and integration with Sophos Endpoint, the full wealth of protection for devices both on and off the corporate network.

Scalable

Sophos offers a range of access points and appliances to provide wireless access for businesses of all sizes. Entry-level models offer a cost-effective solution for very small businesses whilst high-performance access points or even firewall appliances supporting 802.11ac offer the latest technology for the highest demands. A Sophos Remote Ethernet Device and a Sophos Access Point can economically provide a branch office wireless network and a full set of network security services.

Shared

A built-in wireless controller allows administrators to monitor and change security policies centrally for access points throughout the office or campus. These tasks can be handled by the same administrator who manages the security gateway appliance. No dedicated specialist or detailed training is needed. To ensure that no 'technical' intervention is required, the front desk or other designated person can automatically receive vouchers or codes to distribute to provide guest access for hotspots at any time.

Simplified

Sophos Wireless Protection simplifies WiFi security management through plug-and-play deployment. When new wireless access points are turned on, they appear automatically on the central console. They can be configured and placed into operation in minutes. Sophos also scales to enable the management of WLANs in remote offices.

Travel and local IT support are not needed, because all security and wireless networking features can be managed remotely from the central office.

Standardized

Integration with Sophos appliances also makes available a number of next-generation firewall capabilities for wireless traffic. For example, bandwidth and quality-of-service controls can be implemented to give priority to business-critical applications and throttle the bandwidth allocated to low-priority activities. Using the firewall appliance, authentication provided by backend systems, such as Active Directory, can be used to provide simpler access.

Secure

Another advantage of Sophos Wireless Protection is that all wireless traffic flows in both directions through the firewall appliance. The local area network is protected by an advanced firewall, a configurable intrusion-prevention system, as well as antivirus and antispam engines. Administrators and security personnel can monitor security events and react quickly to suspicious patterns. Wireless devices receive the same level of security as if they were physically connected to the LAN.

Sophos WiFi
Learn more at www.sophos.com/wireless

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

11.14.wpna.simple

SOPHOS