5 Tips for Securing Your Wireless Network

Balancing security, manageability and accessibility for employees and guests

In this paper, we suggest best practices that can help administrators go beyond the basics of wireless security to provide advanced security, manageability and accessibility. We will also show how Sophos UTM Wireless Protection and related products help address these issues.
5 Tips for Securing Your Wireless Network

It isn’t hard to set up security for the wireless router in your basement: change the SSID, pick a strong password and perhaps install VPN software for remote access.

But securing wireless networks in a business environment is much more demanding. Systems administrators must:

- The Basics - securing wireless access points and protecting remote and mobile employees
- Provide controlled access for guests and contractors
- Deploy and manage multiple wireless access points in central offices
- Deploy and manage wireless access in remote offices (ideally, without travel or local IT staff)
- Integrate wireless traffic into the company’s core network security infrastructure

1. The Basics - Securing Wireless Access Points and Protecting Remote and Mobile Employees

Certain security practices are essential for wireless networks of all types. These include:

**Strong encryption—preferably use WPA2.** An eavesdropper can pick up wireless signals from the street or a parking lot and break older security algorithms like WEP in minutes using tools readily available on the Web.

**Complex passwords.** Cybercriminals can use cloud computing resources to test millions of passwords in minutes, so wireless passwords should be 10 characters or longer and include numbers and special characters.

**Unique SSIDs.** SSIDs are part of the password used for WPA2 encryption. Hackers use “rainbow tables” to test common SSIDs, so administrators should pick unique network names (but not ones that identify their organization).

**VPNs for remote access.** Virtual private networks are essential to protect communications from mobile employees (who can put a VPN client on their devices) and remote offices (which can use economical, point-to-point VPN connections).

**Employee education and published policies.** Employees need to be educated on secure networking practices. In companies with bring-your-own-device (BYOD) policies, this includes acceptable uses of personal devices for company business. Organizations that publish policies and systematize training not only improve security, but also enhance their compliance posture by showing auditors that they are taking action to protect confidential information.³

---

**Watch Out!**

“I admit, one of my favorite things to do in backtrack is to crack a good ole WIFI. ... I guess it’s just thrilling, it gives me sort of a high to be in places I shouldn’t. To be able to completely exploit an entire network as a local user is definitely something that’s fun and exciting.”

BLOG POST: CRACKING WEP WITH BACKTRACK
2. Provide Controlled Access for Guests

Uncontrolled access to wireless networks is a common security issue. 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.

Some organizations address this problem by providing a separate guest network with limited access to core IT systems. This approach addresses the issue of transient guests, but it is expensive and not always useful for contractors and long-term guests.

Another approach is to find tools that restrict guest and contractor access to appropriate periods of time and place limits on their activities.

3. Manage Multiple Access Points in Central Offices

Deploying and managing wireless access points can be time-consuming. Large offices and campuses may require many access points to cover all office areas, conference rooms and meeting spaces used by employees. Multiple wireless networks for different groups and for guests can add to the work.

Not only does complex administration raise staffing costs, but it also increases the likelihood of accidental misconfigurations that cause security vulnerabilities.

Enterprises need to find tools that simplify tasks such as deploying new access points, checking on the status and settings of these devices, and changing parameters. A best-case scenario is to find tools that do not require specialized knowledge or a long learning curve, so the work can be done by network administrators rather than wireless networking specialists.
5 Tips for Securing Your Wireless Network

4. Manage Access Points in Remote Offices

Providing technical support to remote and branch offices is also 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.

5. Integrate Wireless Traffic into the Network Security Infrastructure

Cybercriminals are increasingly targeting wireless traffic as an avenue to penetrate enterprise networks. They are exploiting:

- More opportunities to find weak points because of the growing number of remote and mobile workers.
- Home computers and mobile devices that lack the endpoint protection tools found on workstations that reside in company offices.
- BYOD policies that limit the control that companies have over the selection and configuration of mobile devices (a trend amplified by the increasing number of organizations with bring-your-own-computer policies).

To prevent wireless traffic from becoming a major threat vector, enterprises 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.

Ideally, the connection should be two-way, so traffic that goes out through the wireless network must first pass through the core security infrastructure. That allows URL and content filtering tools to prevent employees from visiting websites that contain malware or are related to phishing and social engineering attacks. It may also help detect data being exfiltrated as part of an advanced persistent threat.
Security with Manageability: Sophos UTM Wireless Protection and Sophos Access Points

Sophos UTM Wireless Protection and Sophos Access Points offer full wireless security while providing flexible access for employees and guests.

Management is greatly simplified. Companies with Sophos UTM appliances get 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. A built-in wireless controller allows administrators to monitor and change security policies centrally for access points throughout the office or campus.

Plug-and-play deployment of new access points and central management of remote access points.

These tasks can be handled by the same administrator who manages the unified threat management (UTM) appliances, so no dedicated specialist or detailed training is required.

Wireless mesh networking capabilities can improve the economics and resiliency of wireless networks by using wireless LAN bridges and repeaters to link together multiple WLANs without the use of Ethernet cabling.

Sophos also greatly simplifies the management of WLANs in remote offices. A Sophos Remote Ethernet Device and a Sophos Access Point together can provide a branch office wireless network and a full set of UTM security services very economically. Travel and local IT support are not needed, because all security and wireless networking features can be managed remotely from the central office.
5 Tips for Securing Your Wireless Network

Sophos UTM Wireless Protection can provide controlled access for guests and contractors in a variety of circumstances:

- For basic compliance requirements and activity tracking, visitors can be required to accept a “Terms of Use” statement before accessing the network.
- For meetings and events with many short-term guests, visitors can be sent a “password of the day” by email.
- For longer term and more complex situations, guests can be sent vouchers that give them access to a WLAN for a specific time period, for a time quota in hours, and for data volume in megabytes.

Hotspot terms of use and an access voucher that tracks and controls guest activity on the WLAN.

Another advantage of Sophos UTM Wireless Protection is that all wireless traffic flows in both directions through the Sophos UTM appliance. The enterprise network is protected by an advanced firewall, a configurable intrusion prevention system, and antivirus and antispam engines. With URL and content filtering, employees can be blocked from visiting dangerous websites.

Administrators can enforce another wireless security best practice: the use of VPNs for mobile and remote users, including point-to-point VPN connections for remote offices.
Integration with Sophos UTM 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.

Finally, through the UTM appliance, 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. Learn more about Sophos UTM Wireless Protection.

Conclusion

Secure wireless networking for business goes far beyond SSIDs and passwords. Administrators need to manage the basics in multiple locations, efficiently and reliably. They need to be able to tailor access to different employee and guest use cases. And they need to make sure that wireless traffic is scanned just as thoroughly as any other type of Web traffic.

Ideally, these goals should be achieved economically, and without highly specialized skills or extra training.

Organizations that want these advantages should take a close look at Sophos UTM Wireless Protection and related Sophos products.

Sources

1. For more best practices, see “Hot Tips for Securing Your Wi-Fi Network.” To see short videos on cracking WEP and weak passwords, go to “WEP Encryption Isn’t Secure” and “WPA Encryption Can Be Cracked.”