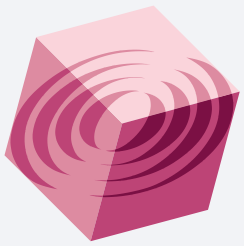


AirTight NETWORKS™

The School Has No Walls

Protecting Students from Inappropriate Content via Unauthorized Wireless LANs

339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043
www.airtightnetworks.net

The School Has No Walls

Protecting Students from Inappropriate Content via Unauthorized Wireless LANs

Many primary and secondary schools have embraced the use of networked course material and the Internet to enhance the learning experience. In concert with this, most schools have also implemented Internet filtering software to ensure that inappropriate websites are blocked from student access. This ensures that the Internet is used to enhance the learning environment and prevents minors from viewing adult content, visiting gambling or gaming sites, or downloading music files.

However, the increasing ubiquity of wireless LAN capability embedded in notebooks, smart phones and gaming devices creates a new challenge for school administrators and IT managers trying to maintain control over Internet usage. Recent studies show that wireless LAN penetration has reached 65% in the enterprise. This coupled with the millions of low cost wireless LAN access points shipped into consumer households mean that it is very likely that students will be able to access a neighboring wireless LAN from within school grounds. Another possible source of an open wireless LAN is a city-sponsored municipal Wi-Fi network. Many cities are deploying these outdoor wireless LANs with no security to encourage visitor use, with the unintended consequence that students may also tap into the network. These unsecured connections create the opportunity for:

- Unmonitored use of the Internet, potentially exposing inappropriate content (such as adult sites) to minors
- Cheating on examinations by accessing content or people over the Internet
- Inattentive classroom behavior due to social network site (i.e. MySpace.com) usage and instant messaging

The first is by far the most dangerous and impactful scenario. In addition to the negative psychological effect of adult content on young minds, lawsuits and legal fees could ensue - wasting significant personnel time and budget that otherwise could be used on educational programs. In the worst scenario, community outrage could even lead to calls for personnel changes.

A Tough Problem to Solve with Policy Changes

School administrators face several challenges in trying to curb this problem:

- as these are students' personal devices, the school cannot install software solutions or disable the wireless radios on these devices
- policies to prevent students from bringing Wi-Fi enabled devices onto the school grounds are not practical
  - Notebook usage is a standard skill that all students need to have in a competitive global economy

The Implications of the Children's Internet Protection Act

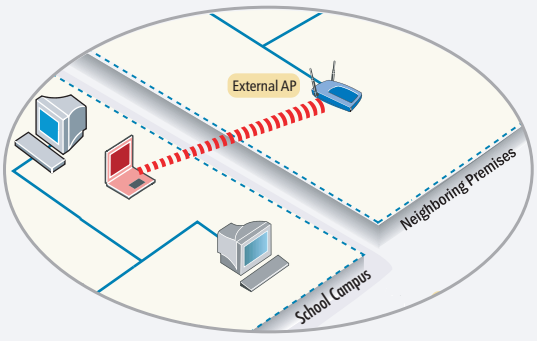
Making the situation even more difficult is the potential financial implications of failing an FCC audit of a school's compliance to the Children's Internet Protection Act (CIPA). Enacted by Congress in December 2000, the law aims to protect children from inappropriate content through school computers. Schools must certify that policies and technology protection measures are in place to prevent minors from accessing adult content. Without this certification, schools are not eligible for needed E-rate discounts on Internet access or internal communications technology.

Administrators face audit failure if school computers used by students can access the Internet over an unmonitored wireless connection. As a wireless connection will not first pass through a content filter, the computer may cause a violation of CIPA. As audits by the FCC of a school's compliance with CIPA are random, schools must carefully weigh the risks of this compliance issue coming before them and jeopardizing their funding.

Fortunately a solution does exist. Wireless intrusion prevention systems can prevent all unauthorized wireless connections, including those to neighboring wireless LANs, without requiring any client software. The next sections will describe both the threat and the solution in greater detail.

Understanding this Invisible Threat

Students accessing the Internet through an unmonitored wireless connection is a strong possibility at any school, whether or not the school has installed their own wireless LAN. The source of the problem is wireless LAN signals from neighboring businesses and homes or outdoor metro Wi-Fi networks that reach the school campus. If these wireless LANs are not secured, i.e. a user name and password is not required, then any wireless LAN client in a notebook, smart phone or gaming device can attach to these networks. This then provides the user with open, unrestricted access to any site on the Internet.



Clients can connect to neighboring wireless LANs from school property and gain unmonitored access to the Internet

Closing the Campus to Unmonitored Internet Activity

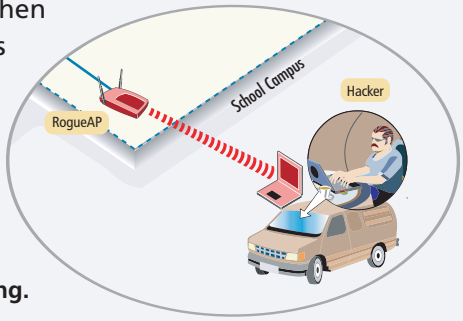
To secure the school against unmonitored Internet access and other wireless threats, AirTight Networks offers a wireless intrusion prevention and performance management solution. Traditional computer security products, such as firewalls and VPNS, only monitor wired traffic and have no visibility into the wireless traffic that is flowing in the air.

SpectraGuard Enterprise is a complete wireless intrusion detection and prevention solution which continuously scans the airwaves and provides automatic protection against any unauthorized wireless activities. With SpectraGuard, the school can institute a complete "no wireless" policy preventing all wireless LAN activity. Or, if the school wants to install its own wireless LAN on campus, SpectraGuard Enterprise can prevent wireless connections to external, neighboring APs while allowing authorized use of the school wireless network. In either case, SpectraGuard Enterprise eliminates the risk of inappropriate Internet sites being viewed over an unmonitored wireless connection while doing no harm to authorized internal WLANs or neighboring WLANs.

SpectraGuard Enterprise also prevents two other wireless threats that endanger school security; rogue access points and ad hoc wireless connections.

- rogue access points: APs that students or others install, often without malice, to create their own local wireless network.
- Ad hoc networks: peer-to-peer wireless connections that avoid security monitoring by centralized infrastructure

If the school does not have its own WLAN, students or faculty members may try to create their own. This is simply done by plugging a consumer-grade access point into any available Ethernet jack. If the Ethernet jack is behind the firewall, then anyone within range of the wireless signal may gain access to the school's network. This could lead to release of confidential student or faculty information, or a malicious attempt to cause havoc on the school network through release of malware.



Access points installed without authorization by the IT department can leave a school network open to malicious hacking.

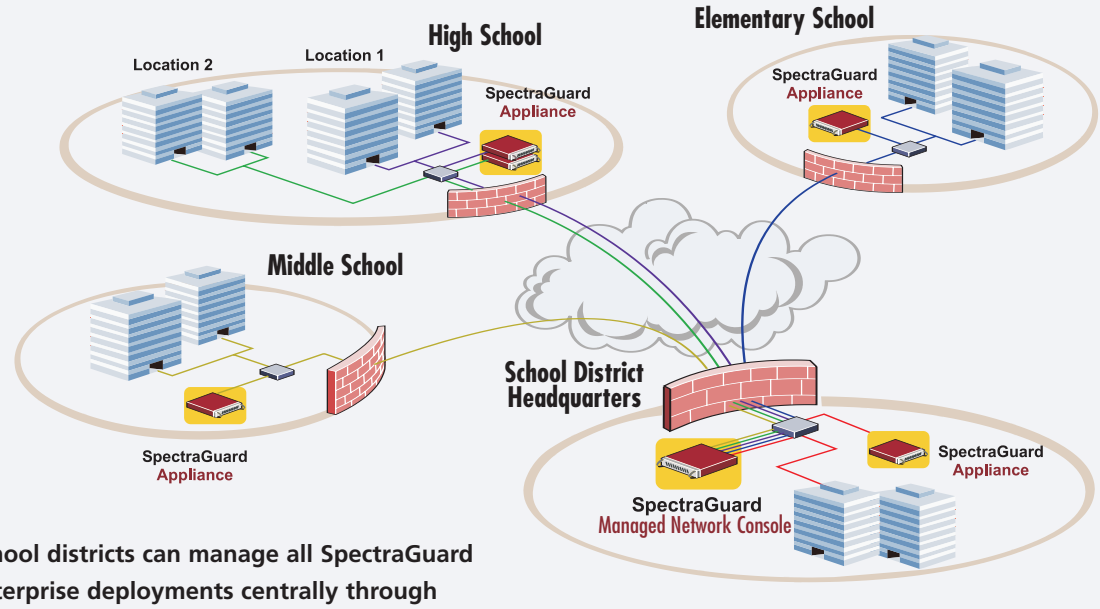
Ad hoc wireless networks may also create a security breach or lead to inappropriate student behavior. An ad hoc wireless network is formed when two laptop computers form a direct wireless connection to each other. This is very easy to do, as Microsoft has designed this functionality explicitly into Windows. If one of the computers is also plugged into the wired Ethernet infrastructure at the same time, the other wireless client has full access to the school network.

So, as an example, a student (at his or her desk) can set up an ad-hoc connection to a teacher's laptop that is attached to the school network, and see everything on the school network that the teacher can see. This may expose confidential information or allow malicious behavior. Or, ad hoc networks might be used by students attempting to cheat on exams through instant messaging or other information sources.

SpectraGuard Enterprise stops both rogue access points and ad hoc wireless networks, ensur-

ing the school network and confidential information remain secure. SpectraGuard Enterprise automatically identifies unauthorized wireless behavior and takes immediate action to prevent it. This means that schools do not need a local IT manager to initiate prevention; SpectraGuard Enterprise allows administrators to set policies that take effect automatically.

For districts with centralized IT resources, SpectraGuard Managed Network Console allows remote management of all SpectraGuard Enterprise deployments, no matter where they are. Centralized policies can be pushed to all schools, and each site can be independently monitored, down to each individual Wi-Fi client.



School districts can manage all SpectraGuard Enterprise deployments centrally through the SpectraGuard Managed Network Console.

Conclusion

While wireless LANs are a boon to schools helping to provide Internet or network access to each classroom, they also can pose a threat. Because wireless LAN signals travel outside of walls, neighboring homes and businesses' WLAN signals can reach the school campus. Municipal Wi-Fi networks may also reach school grounds. When these networks are open, students using their own personal laptops or other devices with wireless capabilities may be able to access the Internet and view inappropriate material. Rogue access points and ad hoc networks may also pose a threat to school network integrity and lead to release of confidential student or faculty information. To counter these invisible threats, schools should deploy a wireless intrusion prevention system (WIPS). SpectraGuard Enterprise is a leading solution that allows school administrators to regain control of their airwaves without requiring on site IT management, nor client software. SpectraGuard Enterprise blocks all unauthorized wireless activity, providing peace of mind for administrators and the community alike.