Secure campus network

Because of their accessibility, school networks are often the targets of malicious attacks and intrusions by viruses or botnets. It is therefore essential for network equipment to offer some form of automated security control to mitigate threats and to reduce the work load on faculty. It is also the top priority to provide content filtering of improper websites to ensure academic quality and safety for K-12 education.

Loop Guard

One of the most common problems inhibiting network performance in schools is the network loop. A loop occurs when inexperienced network administrators like teachers, other faculty, and even students mismanage connected devices. The loop guard feature on Zyxel switches can proactively detect when and where a loop occurs and respond with an alert, intelligently preventing it from hampering network performance.

Access Privilege Management

The foundation of a secure school network is making sure that all school resources are only accessible by authorized clients. Whether via wired or wireless connections, clients accessing the network should be identified and authorized with specific access privileges through Ethernet switches or wireless devices. Zyxel switches and WLAN APs can work with RADIUS servers to enforce authorized access.

IP Source Guard

The ability to manage and control of network usage is never more critical than in education. In network world, each IP address represents an individual. That's why ensuring proper use of IP addresses is critical to network security. IP source guard (IPSG) provides that assurance by enabling Zyxel switches to prevent IP spoofing. Whenever it becomes necessary to locate and identify improper use of a network, IPSG helps you find the right one.

Content Filter

Security threats and attacks are continually increasing in complexity, number, and type. Students, teachers, and administrators who access malicious sites inadvertently through public Wi-Fi may infect their devices with malware, which can then spread to school networks when their devices connect. The Zyxel USG Series features Content Filtering 2.0, which leverages a cloud database to continuously analyze and track URLs. This real-time detection provides school networks with the highest level of security protection. To extend filtering coverage, Content Filtering 2.0 blocks inappropriate content, images, and videos efficiently by supporting SafeSearch, which is a service offered by search engines such as Yahoo, Google, Bing, and Yandex.

SSL Inspection

Secure Sockets Layer (SSL) encryption is widely used by almost every website. Popular websites on campus such as Facebook, Gmail, and Dropbox are examples of sites which utilize SSL encryption. However, SSL encrypted connections can also create potential security blind spots as attacks, intrusions, or malware can hide in SSL-encrypted connections to avoid inspection and influence network performance and efficiency. Zyxel Content Filtering 2.0 supports deeper policy enforcement, inspecting traffic in SSL-encrypted connections while blocking threats.

Application Intelligence

When it comes to bringing malicious software onto campus, new network applications are often the primary culprit. This unwanted software — particularly instant messaging (IM) and peer-to-peer (P2P) applications — can consume excessive bandwidth or even cause system damage. With application patrol and bandwidth management features, IT administrators have full control over traffic inspection and rate limit settings. Popular IM and P2P applications can be controlled to restrict client access within the predefined time frame. The table below illustrates typical applications whose control is critical in the school environment.