



Duval County Public Schools Secures the Learning Environment by Authenticating Users and Blocking Students from Anonymous Proxies

Client:

Duval County Public Schools

Web Site:

www.duvalschools.org

Number of Users:

150,000

Requirements:

Web Filtering and Reporting, Invisible Authentication, Blocking Proxies

Filtering Solutions:

M86 Web Filter and Reporter

“Authentication is a must for a safe and secure Internet environment. M86’s transparent authentication is superior to others offered in the filtering industry.”

Jim Culbert
Information Security Analyst,
Duval County Public Schools

Profile

As the 16th largest school district in the nation, Duval County Public Schools (DCPS) serves approximately 140,000 students. It is the second largest employer in Jacksonville, Florida with approximately 8,000 teachers and a similar number of staff at over 160 K-12 schools, three exceptional student centers, and two academies of technology. DCPS’s goals are to provide a safe and high-quality education for students to become productive members of the community and to ensure the academic success of every student through Internet-assisted learning.

Challenge

When DCPS’s IT administrators first met about filtering Internet content, their main concern was complying with the Children’s Internet Protection Act (CIPA). Along with the law, however, DCPS’s IT staff also faced the challenge of blocking access to pornography and other objectionable material easily accessible to students via the Internet. In particular, students were bypassing DCPS’s then-filter by accessing anonymous proxies in order to view prohibited sites, such as MySpace.com. Jim Culbert, Information Security Analyst, says, “Kids are really knowledgeable about using Web proxies, so they always find a way to get to them to access sites that are otherwise blocked by school network filters.” That was only half of the problem. In order to put a complete stop to the issue, Mr. Culbert and his team also needed a solution to locate and identify these students. He says, “The only way to get students who attempt to access bad sites is if you identify them or if they get blocked. The fastest way to identify these users is through authentication.”

Solutions

M86 was the only solution that fulfilled DCPS’s filtering needs. Says Mr. Culbert, “We looked at vendors with a large market share in content filtering and weighed that along with vendors with a large market share in educational institutions. We looked for a product that could scale to our enterprise and could be centrally located and managed. There are only two of us in the IT department, so we needed a filter that wouldn’t require constant hands-on management. We found that the M86 Web Filter and Reporter (M86 WFR) appliance had the scalability we needed and could be centrally located at our data center, without requiring individual appliances at every site. Two appliances could easily manage the Internet traffic generated by more than 160 sites and still provide full-fault tolerance. A system setup based on Windows 2003 servers and the competition’s software would have easily required twice as many servers to achieve the same level of performance and fault tolerance.”

“With all of its inclusive features, M86 is by far the best value for the school district.”

Jim Culbert
Information Security Analyst,
Duval County Public Schools

In addition, Mr. Culbert is very satisfied with M86’s invisible authentication feature. Stored on the network server, the authenticator runs as soon as a student or teacher logs into the school’s network. Because it runs locally, it provides repudiation and gets a student or teacher user’s information real-time on the workstation. Therefore, no matter where that user goes on the network, he or she is being authenticated. “Authentication is a must for a safe and secure Internet environment,” says Mr. Culbert. “It prevents kids from accessing inappropriate material whether on purpose or accidental. Even though they may not do it intentionally, kids will many times type in a wrong word or misspell a word, but authentication ensures that they are being filtered. M86’s transparent authentication is superior to others offered in the filtering industry.”

Finally, M86 is the only Internet content filtering provider that utilizes signature-based blocking in order to block peer-to-peer, instant messaging, and anonymous proxies, effectively preventing users from accessing these applications. Utilizing revolutionary Intelligent Footprint Technology™ (IFT), the M86 WFR’s unique “Proxy Pattern Blocking” feature catches requests for anonymous proxies on the fly, giving organizations zero-day protection against many open-source proxies. Therefore, if the site is not categorized as Web-Based/Anonymous Proxies in the M86 Web Filter Database, the M86 WFR will still be able to block access to the site based on the signature files in the database. Not only does the “Proxy Pattern Blocking” feature identify attempts to set up proxy tunnels and prevents these connections from being made, it keeps a record of the number of times a student tries to evade the filter in this way. After a predetermined number of attempts, the would-be tunnelers are denied Internet access. Mr. Culbert says, “M86’s Proxy Pattern Blocking feature helps us secure the network from hacker attacks and loss of private information. With all of its inclusive features, M86 is by far the best value for the school district.”

Result

“M86’s complete filtering and reporting solution has not only helped save the IT staff time, but it has proven to be a benefit to the entire DCPS community. Administrators benefit from increased production from their employees, teachers benefit from students staying on task, and students benefit by not being subjected to inappropriate material. Finally, everyone, including parents, benefit from a safer environment,” says Mr. Culbert.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Eilerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 04/05/10