



East Grand Rapids Schools Find Security and Economy with the TippingPoint X505

The Challenge: To continue a tradition of academic excellence dating back to 1841, East Grand Rapids Public Schools uses technology to enhance “student learning at all levels.” Comprised of three elementary schools, a middle school and a high school in western Michigan, the district empowers its 2,800 students with robust 3Com networking solutions. Using 3Com Gigabit core switches, 10/100 SuperStack® edge switches, and XRN (eXpandable Resilient Networking) technology, which interconnects 3Com core devices for extraordinary availability, students access a spate of learning applications as well as the Web and streaming video for research.

As powerful as these technologies are, however, they still posed security risks to the suburban Grand Rapids school system. Administrators, in particular, feared that a virus, worm or spyware could penetrate the district’s network from the Internet and alter or access confidential school records. They also worried that a student using a laptop computer might unwittingly unleash harmful software that could paralyze mission-critical online learning and administrative services.

Additionally, the district needs to comply with the Children’s Internet Protection Act (CIPA), which demands that schools block students from accessing inappropriate Web sites. Moreover, it wanted to deter students from improperly using instant messaging to communicate with their peers via the Internet, while retaining it for teachers to connect with each other on school matters.

Initially, the district used a legacy firewall and deployed an open source Snort intrusion

detection system to detect suspicious traffic. These solutions, however, had limitations. The firewall blocked access to inappropriate Web sites, but consumed significant bandwidth, undermining networking performance. It also required constant manual updates to keep abreast of objectionable sites. The Snort solution was reactive and only detected intrusions, requiring administrators, if they were on duty, to take preventative measures manually and typically after the attack had already successfully penetrated the network.

“We would have loved a comprehensive enterprise-class, intrusion prevention system from TippingPoint to proactively safeguard our applications and data, but we figured it was too costly for a school district of our size,” said Jeff Crawford, manager of networking and security for East Grand Rapids Public Schools.

The district also wanted to use virtual LANs (VLANs) to create a public network that contains

“The TippingPoint X505 is a perfect solution because it gave us the most robust security available at an affordable price point.”

Jeff Crawford
Manager of Networking
and Security
East Grand Rapids
Public Schools

school information freely accessible by parents and others, and a secure internal network only for students, teachers, and administrators. Its firewall, however, did not support virtual private networks (VPNs), which would permit authorized users to safely access the private network via the Internet.

“To comply with CIPA and protect our students, we wanted to do many things— deter hackers and viruses 24/7, provide more efficient Web content filtering, support VPNs and throttle specific traffic,” said Crawford.

“But we needed to accomplish these goals in a way that was economical and easy to maintain to avoid draining our budget.”

Why_TippingPoint

East Grand Rapids Public Schools began examining firewalls from Cisco, WatchGuard, and 3Com when administrators learned of the innovative, high-value TippingPoint X505 platform from TippingPoint, a division of 3Com.

The TippingPoint X505 is a multi-function security solution that integrates intrusion prevention, firewall, IPSec VPN and WAN routing features in a single system. The device features the industry-leading capabilities of the TippingPoint Intrusion Prevention System (IPS), which proactively protects networks from such malicious traffic as worms, viruses, Trojans, phishing, spyware, and VoIP threats. It also supports VLANs and includes Web content filtering and policybased traffic shaping, permitting bandwidth control for both inbound and outbound packets.

“The TippingPoint X505 is a perfect solution because it gave us the most robust security available at an affordable price point,” said Crawford. “Moreover, this single platform eliminated our need for VPN-enabled firewalls, our Snort IDS system, and a switch that supports VLANs, all at a fraction of what these multiple boxes would have cost.”

In October 2005, the school district deployed the TippingPoint X505 at the Internet portal of its network, creating private and public segments

using VLANs. The solution inspects the traffic entering the network’s public segment as well as all VPN communications to the private segment. The platform also examines traffic exiting the private segment, ensuring no malicious software emanates from any of the schools.

The district will rely on the Digital Vaccine® service of its TippingPoint solution to protect against the latest threats, often in advance of attacks. The service automatically updates the TippingPoint X505—weekly and more often when needed—without any IT intervention. In addition, the Digital Vaccine Gold service for the TippingPoint X505 also has the option to update the list of Web sites for Web content filtering so that school children cannot access sites with inappropriate Web content rated as violent, crude or sexual.

“In addition to providing attack-specific protection, the TippingPoint filters also guard against exploitation of vulnerabilities through vulnerability-based protection, deterring future attacks, both known and unknown” said Crawford. “Now, we’ll always have preemptive protection against threats.”

The TippingPoint X505 provides administrators with real-time reports of Web access by students. “We can monitor each desktop and detect policy infractions as they happen,” said Crawford. “Moreover, our content filtering no longer diminishes our network’s performance.”

Furthermore, administrators use the TippingPoint X505 to manage bandwidth usage. While allowing faculty to use instant messaging on the private network, they are prohibiting the use of the application over the Internet, helping to ensure that students stay focused on their studies. “We’ll restrict students’ use of our Internet portal to only the Web sites they require for their work, eliminating any future abuses and saving bandwidth for more appropriate uses,” added Crawford.

The_Benefits

By integrating IPS, routing, VPNs, and firewall capabilities, the TippingPoint X505 is bolstering East Grand Rapids students’ education securely,

productively, and economically. The solution's IPS functionality is not only detecting, but also preemptively preventing malicious or suspicious traffic from either entering or exiting the district's networking infrastructure. It even protects the district's servers from Denial of Service attacks that can incapacitate the network.

"With the TippingPoint X505, 3Com has made IPS security affordable for educators like us and many other mid-size organizations," said Crawford. "Security is all about stopping bad things from happening, not just detecting them when they occur. Everyday, our TippingPoint X505 blocks malicious packets from entering our network."

The highly efficient content filtering of the TippingPoint X505 ensures that the district complies with CIPA. Student will use the Web

only for educational purposes, eliminating the concern that they will access inappropriate sites. Additionally, the district's Web access will be responsive because the TippingPoint X505 is throttling unauthorized traffic from traversing its Internet portal.

"The TippingPoint X505 combines the latest TippingPoint security technology with the reliability, affordability, and ease of use common to all 3Com products," said Crawford. "Rather than operate a handful of discrete security devices, we only administer one, providing us with unified threat management. As result, the system delivers great value and substantially reduced ownership costs."

Corporate_Headquarters: 7501B North Capital of Texas Hwy. > Austin, Texas 78731 USA > +1 512 681 8000 > +1 888 TRUE IPS
European_Headquarters: Herengracht 466, 2nd Floor > 1017 CA Amsterdam, The Netherlands > +31 20 521 0450
Asia_Pacific_Headquarters: 47 Scotts Road #11-03 Goldbell Towers > Singapore 228233 > +65 6213 5999