the JOURNAL

Highlights from a recent webcast on HP TippingPoint

NEXT GENERATION FIREWALL ENABLES SECURE ONLINE TESTING

Enhanced management capabilities protect test environments and minimize bandwidth issues

With Common Core-driving the migration of standardized testing online, network managers and other tech workers in the schools are challenged with the need to keep the testing environment secure, distributing reliable bandwidth to end points and protecting the network. Mike Kunz, director of technology for the Collinsville (Illinois) Unit 10 School District and T.J. Alldridge, HP TippingPoint Enterprise Security Products marketing manager, discussed these issues in a May 29 webcast titled "Top 3 Tips for Keeping Your Testing Environment Secure."

Forty-four states and the District of Columbia have adopted Common Core standards. Most of these states have moved to standardized online testing using either the Smarter Balanced Assessment Consortium (Smarter Balanced) or Partnership for Assessment of Readiness for College and Careers (PARCC) testing platforms. Even among the states that haven't adopted Common Core, many are currently using or are expected to move to online standardized testing.

According to Alldridge, the move toward online testing is "the right move for the children, but it does present a lot of testing difficulties. These difficulties are across the end point, the network, as well as security." Although just about every state is moving to online standardized tests regardless of Common Core adoption, there is rarely funding earmarked for building the robust environments required to ensure the integrity of the tests.

Bandwidth is a major, and highly critical, concern to educators. Kunz explains that his district recently upgraded its leased fiber network connecting all district facilities from 42 Mbps to 200 Mbps throughput. The increased bandwidth "has allowed us to do many more things than we ever thought we could do before," he says. As the grade levels in the schools are taking the online tests it is critical to ensure they have ample bandwidth available by setting rate limits for those classes not testing.

Even with the increased capacity, Kunz explains that his staff must be able to manipulate bandwidth use. This is where a next-generation firewall becomes critical. "We must be able to see what is using our bandwidth, which application is our bandwidth 'hog'. Be it YouTube video streaming or any other application that may not

3 TIPS FOR KEEPING THE NETWORK, AND THE TESTING ENVIRONMENT, SECURE

1 Application control at the perimeter
This is a critical aspect of maintaining test environment integrity. Device-level application control is relatively easy for students to circumvent, often simply by rebooting the endpoint. Additionally, configuring and testing individual endpoints is extremely time consuming for staff, and with BYOD policies, can be impractical. Perimeter-based application control is set through a next-generation firewall that can be configured for multiple (BYOD) device types and is immune to unauthorized endpoint reboots and other local attempts to disable security.

2 Choosing and configuring endpoints
Setting endpoint security policies and requiring devices connecting to the network to meet those policies in order to gain access. Next-generation firewalls can monitor and grant appropriate access for a wide variety of devices and platforms.

3 Practical and year-round protection
Although standardized testing periods are critical, network security must be a constant, year-round process to ensure integrity. With complex systems, and restricted budgets in the K12 environment, practical, easy-to-maintain security and monitoring systems are essential.

LISTEN/LEARN:

For a replay of the webcast, go to: thejournal.com/HPTippingPoint

"The most important device you have to protect your network environment is your firewall. When you look at the threats, it's not just what's outside. We've found that many of our threats are internal."

—Mike Kunz, director of technology for the Collinsville (Illinois) Unit 10 School District

be needed as critically during the testing period. My job is to ensure that the most critical needs are met. No matter how much bandwidth you give them, they will take it all."

"We're able to determine how much bandwidth is available for certain applications, and that has been huge. We've maxed out our 200 Mbps more than once. We like to know what is going on with our bandwidth at all times, and a next-generation firewall allows us to do that," explained Kunz.

Keeping bandwidth dedicated to the testing platforms is only one challenge. Placing security controls on the user devices is untenably expensive and a major logistical challenge for district staff, it is also easily defeated. According to an HP business whitepaper, 1:1 and Common Core Online Testing, Best Practices Guide for Network Infrastructures: "Personal devices can be temporarily 'locked down' to prevent access to non-test applications. Bluetooth connections, Internet access, social media tools, etc., but many personal systems become 'unlocked' after a reboot. Students understand this and are very likely to reboot a 'locked down' device in less than two minutes, which could place all test results for the school under suspicion."

A next-generation firewall, such as the HP TippingPoint Next-Generation Firewall, enables network managers to control security and access features at the perimeter, rather than at the end-user level. Application control enables administrators to limit or deny high-bandwidth, or keep non-approved applications from running, regardless of individual device settings. Unauthorized reboots will not affect the system policies, maintaining the test environment integrity. At the same time, internal network threats can be controlled at the perimeter, ensuring that your network doesn't become a broadcast source of malware which can lead to having your domain blacklisted by e-mail servers and other networks.

Keeping the entire network secure every day is critical and complicated by the increase in BYOD as well as the multiple device types connecting to the network both during testing periods and general curriculum usage. "The most important device you have to protect your network environment is your firewall. When you look at the threats, it's not just what's outside. We've found that many of our threats are internal," said Kunz.

With BYOD allowed at the high school level in his district, Kunz is aware of the potential security problems. "When someone brings their device from home, they aren't going to come to us (IT staff) and ask us to put protection on it," he explained. "That doesn't happen." But, he continued, with strong intrusion protection at the firewall level, not only are end-users' devices protected while on the network, the network is protected from any malicious applications that they may be carrying.

Kunz heavily relies on his HP TippingPoint Next-Generation Firewall to protect his district from malicious intrusions. Automatic and frequent updates to the firewall are crucial. "We have more than 1,200 XP machines and XP has been discontinued by Microsoft for any updates," he said. "Having a firewall that can protect us is crucial to our well being while we keep some of these legacy systems in operation."

Alldridge explains that the HP TippingPoint Next-Generation Firewall offers digital vaccines, "We're still able to provide a level of protection for them (legacy systems) by providing virtual patches to the vulnerabilities."

HP'S TIPPINGPOINT NEXT-GENERATION FIREWALL

HP's TippingPoint Next-Generation Firewall (NGFW) is designed to be a "bump in the line" device, meaning that it simply plugs into your existing network infrastructure and begins protecting your systems from intrusion while providing application control management capabilities through a variety of at-a-glance monitors. There are hundreds of application filters, enabling IT staff to monitor and control end-user behaviors.

TippingPoint NGFW solutions range from 500 Mb/sec (model S1050F) to as much as 10 Gb/sec (S8010F) firewall bandwidth. Models can support between 250,000 and 10,000,000 concurrent sessions. Most models also include dual hot-swappable redundant power supplies.