

All Systems Secure

Arizona's Yavapai College deploys hardware solutions to boost server security and performance.





Bobby Cloutier, Web Systems Administrator

Patrick Burns, Interim CIO

William Earles, Systems Administrator

Yavapai College (Ariz.)

Yavapai College's IT department doesn't rest on its laurels. Even though the IT staff provides users with top-notch tech tools — from online class registration to smart multimedia classrooms with instructor computers, projection systems, DVD players and Internet access — they are always striving to find new ways to make technology work better and more cost effectively.

Last winter, interim CIO Patrick Burns and his IT team set their sights on bolstering network and server security and maximizing the performance of their servers at the five-campus community college in Arizona's Yavapai County. They specifically wanted to improve e-mail spam filtering and enhance the speed and stability of their Web servers, which have increasingly become more critical because of the growth and popularity of online classes.

When Yavapai's antispam software vendor was purchased by another security company, the IT staff noticed the quality of the software declined. With the new company in charge, the antispam software was rarely updated and couldn't stop a new breed of image-based spam, so when the college's contract with the vendor was expiring, the IT department explored its options.

Yavapai College settled on two new spam firewall appliances from Barracuda Networks, which filter out spam and viruses before they enter the e-mail servers. The antispam devices, which have options that include three years of support and maintenance, offer the college new features they previously didn't have, such as the ability for users to check a quarantine folder, where all the spam is located, so they can make sure no legitimate e-mails are caught.

"Barracuda has a big installed base, which gave us a lot of comfort," Burns says. "It also gives users the power to do what they want with their e-mail."

As for maximizing Web server performance, Yavapai's IT administrators wanted new hardware load balancers — technology that distributes users' requests for Web pages among servers to prevent individual servers from getting overtaxed — because the IT staff needed more powerful load balancers with more features, such as the ability to verify that Web servers were serving up Web pages to users.

Yavapai considered numerous models, but found that the higher-end products were too expensive, while lower-cost products from startup companies didn't offer enough features. Then the IT department discovered hardware load balancers from Coyote Point Systems, whose prices were low to mid-range, but offered features that were comparable to the higher-end products.

"People have a different tolerance for spam. Some think one message is unacceptable, while others are more tolerant and sign up for more things, such as newsletters, that some consider spam. It's almost like one person's trash is another person's treasure, and this lets people determine their tolerance."

— Patrick Burns, interim CIO, Yavapai College

"We are a public entity and are very price conscious. We always strive to get the biggest bang for our buck," Burns says. "With Coyote Point, we feel that we got really good performance and features for the price."

Network and Server Security

Yavapai College, with 15,000 students, about 100 full-time faculty members and about 300 full-time staff, is located in the mountainous central region of Arizona, with campuses and learning centers in popular tourist destinations such as Prescott and Sedona. The college, with about 30 IT staffers, operates its main data center and a backup data center out of its main campus in Prescott, as well as a secondary data center in its Verde Valley campus. ▶

Antispam Appliances and Software

Manufacturers offer security appliances and server software that protect against spam, phishing, virus and denial-of-service attacks.

Appliances:

- Barracuda Spam Firewall appliances: Model 200, the lowest-end model, supports between one to 500 users, while Model 900, the highest-end model, supports between 15,000 to 30,000 users. Model 900 can hold up to 250GB of quarantined e-mail.
- SonicWALL Email Security appliance: Models support 50 to more than 5,000 users. The SonicWALL Email Security 8000, for example, supports more than 5,000 users, and features two 3.2GHz processors, 2GB of RAM and two 146GB hard drives.

Server Software:

- CA's Secure Content Manager
- McAfee SpamKiller for Mail Servers (versions for Exchange and Domino servers)
- Symantec Brightmail Anti-Spam software
- Symantec Mail Security (versions for Exchange and Domino)
- SurfControl E-mail Filter
- Trend Micro ScanMail (versions for Exchange and Domino)

The college deploys firewalls, antivirus software and a raft of other security hardware and software products to protect the school's network and servers. A good antispam solution is also critical because it protects faculty and staff from e-mail security risks, such as phishing and worm attacks. It also allows Yavapai College staff to stay productive, so they're not wasting time deleting a deluge of unwanted e-mail.

According to Ferris Research, spam will cost U.S. enterprises \$35 billion in 2007 in lost productivity and IT costs. And of the nearly 97 billion e-mails sent daily worldwide in 2007, more than 40 billion will be spam messages, predicts analyst firm IDC.

At Yavapai College, the percentage of spam is also high. Of the more than 20,000 e-mails that faculty and staff receive on their IBM Lotus Notes and Microsoft Outlook e-mail software every day, about 92 percent are spam, Burns says.

Fighting Spam

Yavapai purchased the Barracuda Spam Firewall 600, which supports between 3,000 to 10,000 active e-mail users and uses multiple algorithms and techniques to block spam. Bayesian algorithms, for example, examine e-mail language to identify spam. Its "image analysis" feature protects against image spam, while its "intent analysis" feature looks at e-mail addresses, Web links and phone numbers in e-mails

to determine whether they are legitimate. The antispam appliance also provides virus protection and scans all attachments for spyware.

Yavapai's IT staff installed two Barracuda Spam Firewall appliances in front of its two e-mail servers in its Prescott and Verde Valley campuses in December and tested the devices with the help of all college employees. To protect itself, the college tested the Barracuda devices before the school's subscription to its previous antispam product ended, says systems administrator William Earles, who manages the e-mail system.

"We set it up and tested the routing to make sure it worked correctly, and if there was a problem or we were not satisfied, we could switch back," Earles explains.

To test the new equipment, Earles let all e-mails, including spam, go into people's inboxes, but he made the Barracuda appliances flag all e-mails that they considered spam. So if Barracuda deemed an e-mail was spam, users would see an e-mail marked as "SPAM." Earles asked everyone to send him feedback on whether the product was correctly or incorrectly identifying spam.

"It was in production for everybody; and it works in our favor because letting everything get through tells our users how much spam we block, and it makes them more appreciative," he says.

More than 100 users gave Earles feedback on the product's accuracy, telling him how many legitimate e-mails were flagged incorrectly as spam and how many spam e-mails were missed and considered legitimate. Based on the feedback, he made adjustments to the sensitivity of the spam filter, from conservative to more aggressive, until he found a happy medium.

"It took us a good month of tweaking until we were happy with it," Burns says.

Another advantage of Barracuda is the ability to give users more control over their e-mail, Earles says. Users can log in, and through a Web interface, check their quarantined e-mail. If Barracuda wrongly flags an e-mail as spam, a user can recover the e-mail. The user also can approve the sender and put him on a "whitelist," so all future e-mails from that sender will arrive in the user's inbox unimpeded, Earles explains. The device also can allow users to create their own "blacklists," which is a list of e-mail addresses they want to block.

The spam in the quarantine box automatically deletes if users don't touch them after a certain period.

While IT administrators have set a standard spam filter sensitivity level for every user, the IT staff can individualize the sensitivity level for those who want it adjusted, Burns adds.

"People have a different tolerance for spam," Burns says. "Some think one message is unacceptable, while others are more tolerant and sign up for more things, such as newsletters, that some consider spam. It's almost like one person's trash is another person's treasure, and this lets people determine their tolerance."

Maximizing Servers

Because Yavapai County is rural, many students are choosing to take online classes because they may have to commute a long way to one of the college's five campuses, Burns says. In

Antispam Do's and Don'ts

Ferris Research analyst Richi Jennings shares his tips on what to look for and what to avoid when purchasing an antispam filter:

- **Accuracy:** When choosing a solution, accuracy rates for filtering spam is important, but also look at “false positive” rates, which is the amount of legitimate e-mail that gets filtered out as spam. For e-mail users, a false positive is much worse than letting some spam e-mail get through to inboxes.
- **Avoid challenge-response systems,** an antispam feature that blocks questionable e-mails, sends an e-mail to the questionable e-mail sender and forces the senders to prove they are legitimate by performing a simple task, such as responding to a question over e-mail. The problem is most spammers spoof legitimate e-mail addresses when they send spam, so there's a high probability that challenge-response systems will send these messages to an innocent third party.

“At best, you will annoy this person and paint your brand in a bad light. And at worst, you will get painted as spam and they will complain to your service provider and you will get blacklisted,” Jennings says.
- **Another antispam feature to avoid is sending suspected spammers an automated nondelivery notification to make the spammers think your e-mail address is invalid.** Because many spammers forge e-mail addresses, many innocent people can receive your nondelivery message.
- **Look for antispam solutions that don't put every spam into quarantine boxes.** Some antispam filters automatically delete e-mails that are clearly spam, then put e-mails they are not sure of into the quarantine box. That will save users time because it reduces the amount of e-mails they will have to look through in their quarantine boxes.

addition, many of Yavapai College's students work full time, and online classes offer greater flexibility and convenience. This semester, more than 2,400 students are taking 129 online classes. “Online classes get more popular every day. It's a growing trend with no end in sight,” he says.

But the e-learning system was notorious for not being stable, so the IT department decided to install hardware load balancers to improve the reliability, stability and speed of the Web servers, says Bobby Cloutier, the college's Web systems administrator.

Yavapai College purchased two Coyote Point Equalizer E450si load balancers, which can support 800 megabits per second of throughput, 50,000 Layer 7 requests per second, and up to 128 servers in a cluster. The college installed the two load balancers in front of its five most critical Web servers that house the campus' critical online applications, such as online class registration and online courses.

“They take a load off the Web servers and do a lot of the processing up front,” Burns explains.

Cloutier says two features on Coyote Point's products improve Web server performance. One is “active content checking,” which simulates a user requesting access to a Web page and can check to see that the site is not only up but also serving the Web content the way the college wants it to.

Another feature is Secure Sockets Layer (SSL) acceleration. The load balancers house a dedicated card to handle SSL transactions, so they don't bog down the Web servers.

“SSL takes up a lot of processing power, so by offloading it on the load balancers, the Web servers can focus on content,” Cloutier explains.

The technology, which is managed and configured with Web-based software, was easy to implement, he says. Coyote Point says it takes less than an hour to install and configure.

“We were pretty much able to do it with zero downtime,” Cloutier says.

A Helping Hand

In choosing the Barracuda spam firewalls and Coyote Point load balancers, the Yavapai IT department did their own research and settled on purchasing the devices. When they called CDW•G, account manager Paul Cardamone and CDW•G network engineer Mike Tomasello helped them narrow down the different choices that Barracuda and Coyote Point offered.

“These guys are savvy,” Cardamone says. “They only needed a little bit of guidance on models and specs. We got on a conference call and hashed it out on both those deals.”

Yavapai's IT staff regularly checks in with Cardamone on product availability and price before making a decision.

“Paul's been great and has gone out of his way to try to offer the lowest price,” Earles says. ■

To find technology products related to this article on server security, please see pages 2 and 3 in this catalog or visit CDWG.com/security.