



Hurricane Stress Tests Firewall

The Challenge: As Hurricane Isabel drifted toward with the East Coast for days, finally landing during work hours on September 18, people did what they always do: they checked the weather. Frequently. At Weather.com, the on-line sister of The Weather Channel, visitors racked up 55 million page views per day, making it briefly the most visited site on the Web. By the time the hurricane petered out (to the tune of \$10 billion in damages), the site had a daily record of 7.4 million users. For the month, total unique visitors, according to Nielsen/NetRatings, grew from 20.1 million (in July) to 22.4 million.

While advertisers might love those numbers, they tend to complicate two important criteria: availability and security. The two are frequently interconnected. If security appliances can't handle the load, they fail, and if they fail ungracefully, they take security off-line as well.

At the time of the hurricanes, there was another wrinkle, recounts Dan Agronow, vice president of technology for Weather.com. He just happened to be testing a deep-packet-inspection TippingPoint Intrusion Prevention Appliance—a new firewall from TippingPoint.

"It was a test by fire," he notes, which was exactly what he wanted. "During severe weather events, site traffic can dramatically increase, and we want to make sure any network or infrastructure equipment we put in can scale to handle that load."

Agronow has a simple criterion for his technology; it's a lot like a weather report. "It's something that people expect to be there all the time," he notes. Yet given the load on the Web site, maintaining service availability and security at the same time isn't necessarily easy.

First, some background. Weather.com has what some might call an aggressive approach to technology. "Purely for cost reasons," says Agronow, "we went from an all Sun shop to an Intel Linux platform, and we have reduced our IT expenses close to 50 percent over the past three years, while our growth has outpaced the Internet. Everything we've done is to focus on increased capacity, increased scalability, and to reduce expenses, and open source has been less expensive for us."

Certain kinds of security, however, didn't always fit into that paradigm. "When we looked at firewalls several years ago, we couldn't find one that was scalable enough for us and able to handle two-gigabyte links," he notes. He wasn't willing to risk losing a two-gigabyte connection, so Weather.com opted to not use firewalls. Instead, it used access control lists attached to each server.

As the company grew, however, such an approach became unwieldy. So the company reexamined firewalls from Cisco, Crossbeam Systems, and TippingPoint.

"It was a test by fire. During severe weather events, site traffic can dramatically increase, and we want to make sure any network or infrastructure equipment we put in can scale to handle that load "

Dan Agronow
V.P. of Technology
Weather.com

All firewalls were put through similar tests. “We didn’t have any special training,” notes Agronow. While the vendor verified IT personnel installed the devices properly, after that it was vendor-hands-off. “We wanted to see if our staff could support it,” he says. “I don’t want to be surprised.”

After testing, Weather.com had capacity concerns about the Cisco and Crossbeam Systems, but TippingPoint worked, then passed the hurricane test to boot. “I don’t have any horror stories to tell you. This is why we chose them—there weren’t any surprises, it worked as expected, it handled our load, and it’s a competitive price,” says Agronow.

Another draw was how the device would fail, if it came to that. “The device is able to fail open. You don’t want it to fail, but in the worst case [if it does] you lose some protection but you don’t lose your link. The other devices, they failed, and we lost the network link. It was not a graceful degradation.”

To sum it up, he says, “Finding a firewall that can handle [our] capacity at a price we can afford is great. If you can throw money at the solution, great, but we can’t.”

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