North American City School System Thwarts DDoS Attacks with Cloud DDoS Services

THE CHALLENGES

The school district began experiencing a series of DDoS attacks, potentially from students, which would take down the network for hours, resulting in delayed testing.

THE SOLUTION

Radware's Cloud DDoS Service was implemented in an always-on model during the eight-month testing period and changed to on-demand during nontesting months.

WHY RADWARE

Radware was selected over Prolexic and AT&T because Radware satisfied all of the school district's requirements and offered a flexible solution at a competitive price.

BENEFITS

Radware's solutions have stopped an array of attacks, including network and UDP Floods, Lightweight Directory Access Protocol (LDAP) reflective and TCP attacks, ensuring network availability for testing

This North American Midwestern school district serves about 36,000 students (from preschool to 12th grade) in 63 schools. Three of its high schools are ranked among the top 1,000 public high schools in the United States, according to national magazines.

THE CHALLENGES

This school district is responsible for administering the national student assessment program for students K–12, which runs for eight months a year. This program includes a series of standard tests that must be completed within certain time frames, or funding for the school can be cancelled. The tests are administrated online and delivered via the district's network.

The school district began experiencing a series of DDoS attacks, potentially from students, which would take the network down for hours, resulting in delayed testing. The DDoS attacks occurred regularly around testing time and became more than the district's internet service provider (ISP) could handle. The ISP had difficulty identifying the attacks in a timely fashion using packet captures. They tried several methods to mitigate the attacks, including "blackholing" traffic. Although this stopped the attacks, it caused good traffic to be dropped, so the school district lost several testing days.

Because the school district couldn't administer the required tests, government funding was withdrawn, the school district's reputation was negatively impacted, and the Director of IT was forced to present to the school board regarding how the problem would be addressed.

THE SOLUTION

The customer issued an RFP for which their ISP's technical solutions group brought in Radware to help with the solution. The customer compared services from Radware, Prolexic and AT&T.

The school district had several core requirements for the solution:

- Network availability
- A seamless installation of the solution by July of the following school year
- An automated solution that would not require additional management resources
- Vendor monitoring and management

Prolexic and AT&T proposed standard configurations, including an always-on cloud-based DDoS deployment. This provided the required network protection during testing but was too expensive for the school district during the nontesting period. They also proposed an on-demand cloud DDoS option, which required the customer to constantly manage the service when it was enabled or disabled.

Ultimately, the school district selected Radware's fully managed Cloud DDoS Service because it satisfied all of the school district's requirements and offered a flexible solution at a competitive price. The service was deployed in an always-on model during the eight-month testing period to ensure network availability and changed to on-demand during nontesting months.

Radware was able to expedite installation to make the July deadline. Radware's professional services helped the customer implement automated DDoS attack management policies, and Radware's 24x7 Emergency Response Team (ERT) provided full management and monitoring, relieving the load from the ISP.

BENEFITS

Since installation, Radware's solution has stopped many types of DDoS attacks against the school district, including network and UDP Floods, LDAP reflective and TCP attacks. Most recently, the school district was hit by a 380,000-instance/570 Mbs Memcached reflective attack, which is a DDoS attack that overloads the caching database. The attacks were mitigated, and the school's network was protected.