State Government Launches Comprehensive Solution Against DDoS

About the Organization

State Department of Administrative Services

A group of state and regional educational organizations covering over 900 public and private school districts share a common network. The architecture includes 28 regional Information Technology Centers (ITCs) and a fiber-optic backbone of more than 1,850 miles, which helps the department lower broadband access costs.

The combined network supports over 1.4 million students and school internet access. A critical service conducted over the network is high stakes online testing, such as PARCC, AIR, and MAP[1]. It also support integrated Education Management Information Systems with student data reporting, student information systems, and state fiscal software applications. The fiber-optic backbone also extends to state health-care, public broadcasting and local government constituencies.

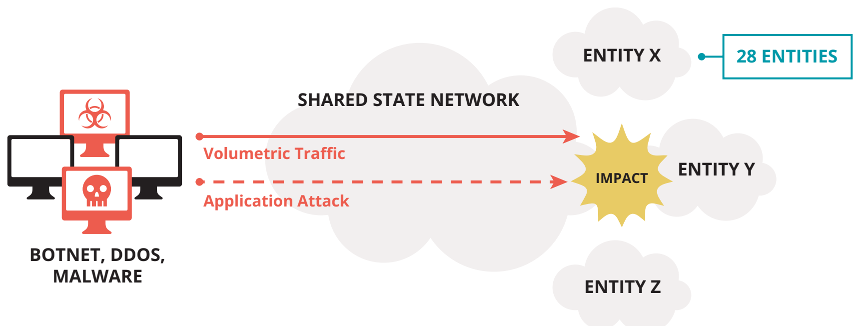
[1] *"Kansas math, Reading Tests Results Might not Go Public because of Cyberattacks,"* Kansas City Star, April 14, 2014.

[2] *"DDoS Attacks on Schools are on the Rise: Is Your District Prepared?"* The Modern Network, October 22, 2014.

The Security Division of NETSCOUT

The Challenge

The shared network was experiencing an increasing number of distributed denial of service (DDoS) attacks. During one period a single ITC reported 28 attacks in 28 days. In this case, the average duration of the attacks was 23 minutes, and the average size of the attacks was 2.3 gigabytes per second. What also was of concern was not all the attacks throughout the network were detected or reported. Administrators were aware of "low and slow" DDoS tactics targeting applications with lesser volumes of traffic that were very difficult to identify.



System managers were also aware of other attacks on specific educational networks. In fact, according to Gartner and other researchers, DDoS attacks on schools are not only increasing, but are more highly targeted, sophisticated, and difficult to detect. These DDoS attacks are targeting more back-end system weaknesses, are more difficult to fend off and expensive to recover from[2].

The Decision Process

The state department of education was granted funds to investigate a layered DDoS protection solution that would encompass all the different entities, with vouchers for each organization that participated in the joint project to purchase their own on premise solution components.

The department of education established a team of regional representatives to develop the process and criteria by which to evaluate solutions. Based largely on a review of Gartner's Security report for DDOS that recommends a layered approach, the team came up with short list of five vendors. The agreed upon set of criteria were:

- A hybrid solution with both cloud and on premise components
- The ability to support multiple carriers
- Mitigation support for at least 10 gigabytes
- The willingness to meet the team's timeline—including a proof of concept
- And deliver the highest level of service

Ultimately only two vendors were invited to provide proof of concepts, in what amounted to a head-to-head comparison at one of the regional ITC's.

Looking Ahead

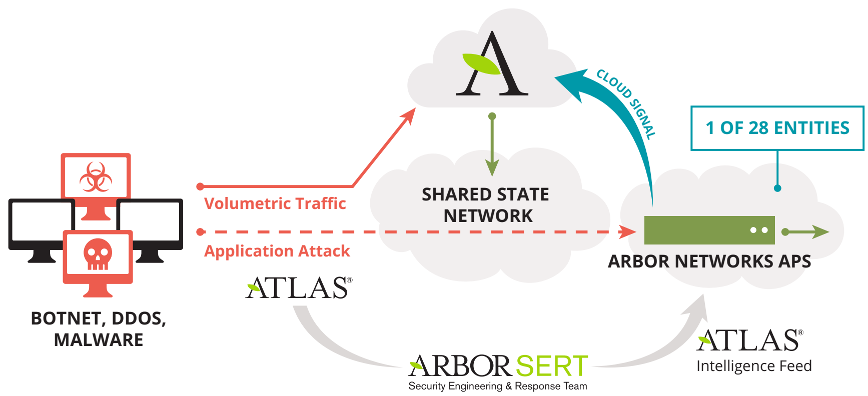
As the statewide network continues to add participants and other government departments become involved, they to will be able to take advantage of the flexible DDoS protection solutions established by Arbor. They'll be able to choose from a combination of products and services to design the the specific DDoS protection that best meets the needs of each organization:

- Mitigation platforms and capacities ranging from 2U appliances (1 Gbps-40 Gbps) to virtual (sub 1 Gbps)
- Managed APS (mAPS) for organizations that want to outsource DDoS protection. mAPS service can be used for on premise only deployments, or as part of a fully managed Arbor Cloud DDoS Protection solution
- Global Scrubbing centers provide up to 2Tbps of on-demand mitigation capacity

The Solution

Following the PoC the team unanimously chose Arbor's DDoS Protection Solution. Every participating organization utilizing the statewide network now enjoys multi-layer DDoS defense, with always on, in-line protection from in-bound DDoS attacks through an on premise Availability Protection Systems (APS) that can also stop outbound activity from compromised hosts, and up to 2 Tbps of on-demand mitigation capacity from Arbor Cloud's global, cloud-based scrubbing centers.

In fact, one of the strengths of the comprehensive Arbor DDoS solution is the seamless integration between the scalable, Arbor Cloud DDoS protection service and Arbor's on premise APS. If an APS detects a volumetric DDoS attack that may overwhelm the organization the APS can automatically redirect traffic to the fully managed Arbor Cloud DDoS protection service. This Cloud Signaling feature is unique to Arbor's DDoS Protection Solution.



The team was especially impressed by Arbor's superior ease of installation (under one hour) and the interface easily used by non-security staff. Faster detection and mitigation is enabled with actionable threat intelligence derived from ATLAS, hundreds of terabits per second of anonymous traffic data from more than 330 ISP customers. This traffic data is analyzed by ASERT, a team of industry experts who conduct threat research, help customers mitigate DDoS attacks and create ATLAS Intelligence Feeds to continuously inform both Arbor Cloud services and the on premise APS.

The flexibility of an integrated APS and Arbor Cloud met all the criteria established by the team – and then some. Armed with ATLAS Intelligence Feeds, the Arbor DDoS Protection Solution helps protect the state-wide network against the full spectrum of DDoS attacks, from amplification/reflection volumetric attacks to state-exhaustion techniques, e.g. targeting firewall/IPS, to "low and slow" application-layer attacks.

Benefits

Since deploying Arbor's DDoS Protection Solution, state and regional educational organizations have experienced a reduction in DDoS attacks—and faster mitigation. They have effectively removed the threat of botnets, and set connection limits on application servers to prevent "unintentional" DDoS. They were also pleasantly surprised to recover 5-6% of inbound bandwidth and reduced their average firewall utilization. The success of the Department of Education's DDoS protection initiative is causing other state agencies to engage Arbor.

What problems can the Arbor DDoS Protection Solution help you solve? Visit www.arbornetworks.com/products/ddos-protection-products for more.

The Security Division of NETSCOUT

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

SB/GOVSTUDY/EN/1115-LETTER