

Asian National Ministry of Education

Allot Security Solution Keeps Asian National Education Network Safe

About National Ministry of Education

A Ministry of Education in Asia operates a national network through which it provides IT services such as remote learning, school administration and research. The network connects schools in 35,000 locations to datacenters and the Internet. As part of a broader national digital initiative, the schools are also connected to other Ministry of Education networks, such as the national university network. Millions of users leverage the applications and connectivity provided by the Ministry of Education for the advancement of the country's education.

Challenge

The Ministry of educational wanted to be secure, reliable and fast, but posed the unique challenge of serving a very wide variety of user groups, from the students and their parents, to the school faculties and administration. Many of the users would often connect to the network with their own devices, which was another security risk.

Key requirements included blocking access to inappropriate content for the schoolchildren, as well as blocking access to malware infected web sites and malware downloads. A high level of service availability was also a requirement, the importance of which was emphasized after a massive DDoS attack the previous year. The attack affected several government websites including the Ministry of Education rendering the network services impossible to access for a period of time.

The challenge was to deliver a versatile, simple and scalable security solution that would be centrally deployed and managed. The solution needed to support multiple types of end-devices (desktops, laptops and tablets, for example), operating systems and user-profiles, and HTTPS traffic. Transparent and frequent updates would be required, and easy maintenance was essential.



Vertical | Enterprise
Industry | Education
Region | APAC
Solution | DDoS Protection

Challenge

- Block access to inappropriate content for children
- Protect network from malware infected web sites and malware downloads
- Need for a scalable solution that supported multiple types of endpoints

Solution

Our solution for the Ministry of Education consisted of three major pieces. First, an Allot Service Gateway Tera was deployed on the network to act as a central hub for visibility, security and control from a centralized portal. Then, Allot DDoS Secure was activated within the Tera, providing DDoS protection and service continuity to the network. Finally, an Allot WebSafe Business license was implemented to provide safe browsing, anti-malware, mail security and ad blocking.

Benefits

- Single solution for a network of thousands of sites and users
- Assures comprehensive security and consistent QoS
- Easy to manage, scalable solution that reduces costs and TCO
- Provides customer and user satisfaction

Solution

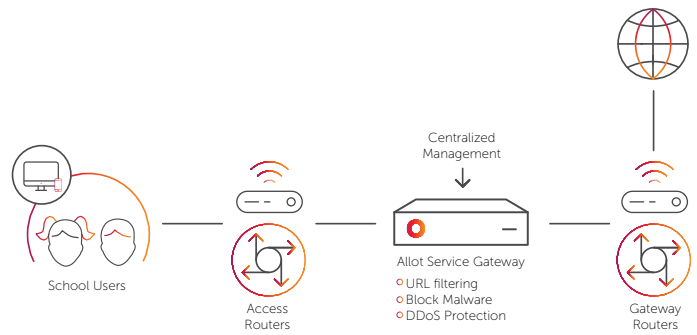
Allot implemented a centralized network-based solution consisting of three main components. Allot Service Gateway (SG) Tera, our flagship multi-service delivery platform, was deployed to act as a central hub for the Ministry of Education to achieve a high level of visibility, security and control. With the Tera as the basis of the solution, the Ministry activated Allot WebSafe Business to provide safe browsing via web (URL) filtering, anti-malware, application control, mail security and ads blocking services, which enable the network's users to use internet resources safely and productively.

“Being able to solve multiple challenges with Allot's unified DDoS Secure solution has made integration and network management so much easier.”

Director of Network Infrastructure,
Ministry of Education

Finally, our DDoS protection solution which is fully integrated in the SG Tera, was also activated. DDoS Secure prevents DDoS attacks from external sources by identifying, mitigating and reporting them. It also reinforces service continuity by identifying and blocking Bot infected endpoints that originate attacks from inside the network. The license was initially activated in monitoring mode, and shortly afterwards, the Ministry of Education experienced an attack. Without hesitation DDoS Secure was shifted to prevention mode, contained the attack and restored service.

By strategically deploying at a network level and providing central management, the Allot solution ensures comprehensive security for the network's multiple branches. Delivered by the network, the solution provides a shared security infrastructure that is multi-tenanted and scalable, offering the capacity for expansion to handle expected traffic growth and simultaneously reducing TCO.



Benefits

By deploying Allot Service Gateway Tera with Allot DDoS Secure and Allot WebSafe Business, the Ministry of Education can:

- Protect the information of many tens of thousands of students and staff countrywide from malware attacks
- Mitigate and avoid risk to the network simultaneously, without compromising the performance of the network
- Free bandwidth by the detection and mitigation of malware and inappropriate content.

This combination of security and assured performance makes the network as fast and efficient as possible. The network is also available to users on any device and operating system, thereby ensuring reliable access protection for all users and a consistently high quality of experience (QoE).

Resources

[About Allot Secure Service Gateway](#)

[About DDoS Protection](#)

[Frost & Sullivan DDoS Mitigation Whitepaper](#)

Learn more about
Allot's Solutions »