CASE STUDY

EMEA-based Internet and Communications Provider Secures Schools' Networks Using Infoblox

SUMMARY

A large national research institute, this EMEA-based Internet and communications provider is responsible for ensuring Internet security and providing telecommunication services to academic institutions. It was chosen to build a large-scale national education network to provide safe Internet connectivity for **25,000** primary and secondary schools.

The provider was able to offer students a secure and clean browsing experience through Infoblox subscriber services, which included malware mitigation and DNS-based content filtering capabilities. In a cost-effective manner, the Infoblox solution provided foundational and scalable security services that enabled the provider to protect **4.5 million children** using **700,000 school computers** from going to inappropriate sites.

The Challenge

The provider wanted to make sure that network connections and the user experience were not only stable, but also secure, especially because the users were schoolchildren. In addition, it wanted to make sure these children did not go to inappropriate sites or inadvertently download malware. For such an extensive project, implementing secure web gateways (SWGs) alone for content filtering was a high risk. No one had done such a large implementation of SWGs before. (The estimated download traffic is over 1Tbps, which requires around 200 appliances from main SWG vendors.) In the event that something went wrong, the Internet provider wanted a way to augment SWGs. However, the provider did not want to rely on SaaS-based security solutions. Instead it needed its security implementations to be on-premises because it was building its own networks, cloud and data centers.

The Situation

The massive private network the provider was building called for 100-megabit links with routers for each of the 25,000 schools. The project was divided into three phases: delivery of the links, delivery of the networking equipment and security. Security was implemented in two stages. The first involved foundational security using DNS, application delivery controllers (ADCs) and firewalls. The second entailed the deployment of web gateways.

The Solution

Infoblox assessed the announced schools project and suggested that DNS-based foundational security should be considered as a first step to protecting the school networks. Although SaaS vendors also approached the company, it never really considered them because it wanted something that could be deployed on the internal private network it was building for schools. Most service providers build their own infrastructure and for that reason will not use a SaaS-based service. Several additional factors led the provider to select Infoblox over other competitors:

- Infoblox offered **differentiated functionality**, such as Threat Insight, which can detect malware command and control traffic hidden in DNS queries. It can also detect the presence of DNS tunneling, a common method that some students can potentially use to bypass SWG security policy limitations.

- The provider felt that Infoblox was a **better technical partner** by way of its local technical expertise, something that other competitors could not match because they did not have technical experts in the region.
- Infoblox provided references of many other service providers and similar deployments that use Infoblox technology.

As part of its discussions, Infoblox held an in-depth security workshop that covered different examples of malware and how they use DNS for command and control. In addtiton, a basic malware mitigation discussion with Infoblox soon became a broader discussion that included:

- How **content categorization using DNS** can cost-effectively bolster the performance of secure web gateways.
- How DNS-level traffic inspection can provide stable, scalable augmentation for SWGs. For example, through Infoblox the provider was now able to prevent students from accessing obviously inappropriate content, such as adult web sites, by blocking traffic at the DNS level. More nebulous sites were filtered based on URLs using SWGs (Fig. 1).
- How this combined approach limits the amount of malicious traffic that SWGs must handle and brings down the total cost of threat defense.

The Result

During the first, limited-scale deployment, an Infoblox partner implemented the DNS solution in just seven days for two of the service provider locations. This deployment showed that the Infoblox solution was **easy to implement and stable**, giving the provider confidence that the solution would work for large-scale deployments. Implementation for the rest of 16 locations is ongoing as of June 2019. The provider has already noticed several benefits, including central security policy management on DNS firewalls and mitigation of temporary problems with traffic control on ADC and SWG thanks to content filtering on Infoblox DNS servers, which has proven to be a valuable augmentation and offloading solution. Through Infoblox, the provider was thus able to provide a **safe, secure and clean browsing experience for students throughout the region.**

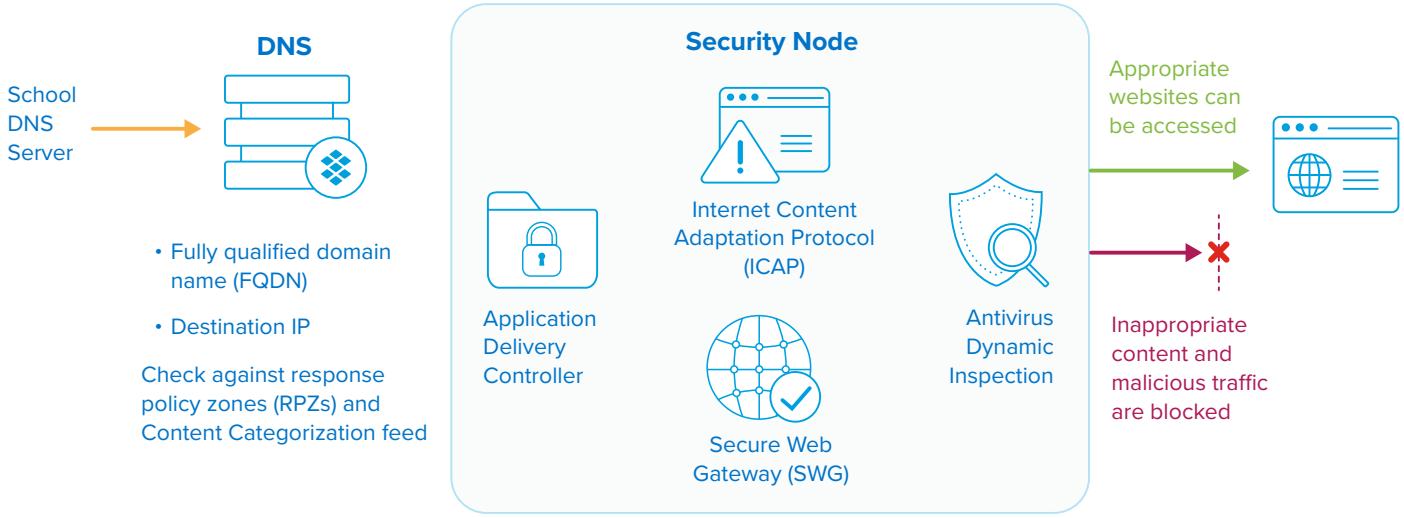

Figure 1: The Infoblox solution uses DNS-based content categorization and inspection to augment SWGs in filtering content.