NETFORT
know your network

Case Study

US School District Gets to the Root of its Bandwidth Problems

Executive Summary

Industry:	Education
Location:	USA
Schools:	41
Students:	25,000
Employees:	3,300

Challenge

To establish who or what is hogging all the bandwidth on the school's network

Results

- Enhanced real time visibility of network activity
- Detection of network anomalies/ bandwidth issues
- Instant drill down to see the fine grain detail
- Access to forensics data to investigate historical issues

The challenge: who or what is hogging all the bandwidth on my network?

As fast and reliable computer networks are a must for all K12 schools, and with more and more applications now being hosted in the cloud; learning material is fast moving to an on-line web-based format.

Even though, YouTube is a fantastic resource for teachers and students' alike, but it can consume huge amounts of bandwidth. As bandwidth demands grow at a massive rate, it is still expensive, and simply 'throwing more bandwidth' at the problem is not a long term solution. It is critical to always have real time visibility and at such a level that makes it really easy to understand and prove what is happening on the network.

The K-12 district with 41 schools, 25,000 students and 3,300 employees

Aiken County Public Schools is a very large K-12 school district in South Carolina, with 41 schools, 3,300 employees and more than 25,000 students.

The Network Administrators could clearly see that various links on the WAN were 100% utilized at peak times. Students and staff were continually blaming the network and the Administrators did not have the visibility and detail to completely understand the root cause. They needed instant access to readable data to enable them to go back to the school, to highlight the exact root cause and prove it was NOT the network.

> *We use LANGuardian to get a deeper look into the traffic flow across our WAN. It also allows us to clearly see who or what is hogging bandwidth on each link*

Shawn Chandler,
Network Administrator
Aiken County Public Schools

Benefits

The NetFort LANGuardian ensures K-12 school IT Administrators:

- Have real time visibility of network activity across the network
- Detect network anomalies, band-width issues before users start complaining
- Instant drill down to get to the rich detail to instantly prove what is happening and resolve the issue
- Always have access to forensics data to go back and investigate historical issues

The cause – Windows 10 clients downloading large updates

In less than one hour, with the help of a NetFort Engineer via a WebEx, the Network Administrator had downloaded the LANGuardian ISO, installed it on VMware and connected it to a SPAN port (or port mirror) so that it could see a copy of all WAN traffic for the district. It immediately identified that on this particular school WAN link, a number of Windows 10 clients were concurrently downloading large updates. Even though, they used Windows Software Update Servers (WSUS), the Windows 10 clients were still going direct to Microsoft. "I have found Windows 10 updates to be a huge data hog in our environment, even though we have WSUS servers on site. Tracking students who are using VPN's has become so much easier to put a stop to"; said, Shawn Chandler, Network Administrator at Aiken County Public Schools.

Microsoft and Apple updates were blocked for a number of hours, so staff and students could log onto cloud based applications without interruption. One of the outcomes of this, was that local update servers were deployed at some schools. The LANGuardian also identified usage of external proxies and anonymizers by some students in an attempt to access blocked sites. Access to these sites was not alone a violation of school usage policy and a security risk, but they were also consuming large amounts of bandwidth.

Getting Visibility on Encrypted Traffic

With some school districts having up to 75% of traffic encrypted at the edge, it is critical to have a tool like LANGuardian to get enough visibility and drill down in order to understand and prove what is happening on the network. Unlike other flow tools that just see IP addresses and traffic volumes, LANGuardian uniquely captures metadata from SSL certificates so it can analyze encrypted traffic - mainly HTTPS, but also encrypted sent and received email. With its ability to dissect the server's SSL certificate, it can extract the server name, critical detail in order to really understand and troubleshoot the root cause of network issues.

About NetFort LANGuardian

NetFort LANGuardian is the industry's leading deep packet inspection software for monitoring, troubleshooting, and reporting on network and user activity. It is a passive network traffic analyser, not inline, so it doesn't impact on network performance. There are no proxies, no agents or clients to install, and no special hardware appliances are needed. Visit our online demo to see LANGuardian in action:

https://demo.netfort.com