

Industry: Higher Education

Customer



Challenges

To increase visibility and traffic inspection, respect student privacy and keep costs down. The university was hampered by existing firewall technology and embedded IDS/IPS that could only inspect a portion of network traffic and did not provide visibility into GLR's high-speed internal and virtual network.

Solution



- ▶ StealthWatch Xe for sFlow
- ▶ StealthWatch FlowSensor VE
- ▶ StealthWatch IDentity
- ▶ StealthWatch Management Console

StealthWatch Benefits

StealthWatch delivers:

- ▶ visibility into GLR's Internet gateway traffic without requiring hardware upgrades
- ▶ visibility across GLR's high speed internal and virtual network
- ▶ faster time to resolution
- ▶ automated mitigation
- ▶ 75% cost savings compared to internal monitoring technologies
- ▶ minimal administrative burden

CASE STUDY: GRAFISCH LYCEUM ROTTERDAM

StealthWatch leverages sFlow to deliver end-to-end network visibility at 10G speeds for Grafisch Lyceum Rotterdam

Background

The Grafisch Lyceum Rotterdam (GLR) is the largest specialized college for media, design and technique in the Netherlands. More than 4,000 students attend GLR to study 40 different programs, including interactive media and graphic design, animation, games, video, stage and theatre technique, media management, media technology and printing and finishing. To support its world-class programs, GLR maintains an extensive computer network with more than 2,200 advanced workstations, specialized digital equipment and 4,000 ports.

Overview

Like many academic institutions, GLR's network team struggles to balance network traffic monitoring with protecting students online privacy. According to Mark Pleunes, Network Manager for GLR, "The best way to protect our environment and maintain high availability is to have a clear view of what is happening on the network." But, GLR's existing firewalls with embedded IDS/IPS could only inspect traffic up to a certain throughput. As a result, a portion of GLR's high-speed Internet traffic was not being monitored, inspected or captured for troubleshooting. In addition, GLR had no means of monitoring virtual machine (VM) host's activity on its VMware ESX servers.

To increase visibility across the physical and virtual network, GLR selected the StealthWatch System™ for network performance and security monitoring.

StealthWatch leverages sFlow® data from GLR's Brocade® routers and switches to provide detailed

insight into network traffic patterns, link utilization and overall network performance at speeds up to or above 10G. StealthWatch also provides deep virtual monitoring down to individual VM instances and the appliance that resides within. StealthWatch directly links individual users to specific network events for greater user accountability and faster, more immediate insight into unexpected network events. StealthWatch helps GLR maintain a high level of visibility and enable proactive troubleshooting that does not infringe on student privacy.

"StealthWatch has made our network team more productive. It automates many of the tedious analysis...offers more visibility and remains on duty 24/7."

StealthWatch Speeds Network Troubleshooting, Streamlines Workflow

Prior to deploying StealthWatch, initial efforts to identify worm activity were tedious and often inconclusive. “To confirm worm activity, we used to examine firewall logs, analyze traffic volumes and make conclusions,” said Pleunes.

If worm or other unwanted network activity was spotted, the team engaged in a repetitive, costly and time-consuming exercise of traveling to different geographic network locations and shutting down switch ports to try to pinpoint the responsible host. For confirmation, the network team had to rely on multiple disparate technologies, such as firewall, sniffers and mirror ports, for any data still available for packet analysis.

StealthWatch streamlines the troubleshooting and greatly increases the network traffic visibility available to the GLR team. The System alerts the team to worm activity, providing a network-wide view that includes point of origination, infected hosts and propagation. With its host-centric view of the network, StealthWatch can enable automated mitigation responses using GLR’s Brocade infrastructure. As a result, StealthWatch removes the travel, guesswork, packet analysis and sweeping mitigation responses involved in GLR’s previous incident investigations.

“Flow-based Network Behavior Analysis is the only way to monitor your network.”

According to Pleunes, “Flow-based Network Behavior Analysis is the only way to monitor your network. The time of using a mirror port with a packet analyzer is over. StealthWatch automates network actions if the traffic meets certain criteria. The Worm Tracker feature demonstrates StealthWatch’s ability to detect a worm even without knowing its signature.”

StealthWatch Improves Virtual Network Performance and Security

GLR relies on StealthWatch as its primary monitoring and mitigation solution for both its physical and virtual network. Before StealthWatch, GLR had no means of monitoring VM hosts that reside on the same VMware ESX server because intra-host traffic did not leave the virtual switch. In some cases, performance issues with VM hosts on the ESX server were inaccurately attributed to network problems.

With StealthWatch operating as the eyes and ears of the network, GLR was able to verify that the network load of its ESX servers was not the root cause. Furthermore, GLR discovered that its VMware VMotion was aggressively configured. With complete insight into activity on ESX servers, GLR regained visibility into the uncharted, unknown parts of its VMs. This insight was critical in driving forth GLR’s VM Migration Program. Within three months Pleunes and his team added 60% more VMs per ESX server without compromising virtual performance.

StealthWatch Eliminates Expensive Hardware Upgrades

In the past, GLR could only monitor a subset of traffic because of IDS throughput limitations. The team often relied on manual firewall log analysis and had no way to precisely mitigate specific IPs involved in unwanted network behavior. Achieving greater visibility of all Internet gateway traffic using the existing firewall/IDS/IPS solution would have required hardware upgrades on all uplinks—a cost-prohibitive option calculated at more than USD \$240,000.

By selecting StealthWatch, GLR leverages sFlow data from its existing Brocade routers and switches, resulting in 75% hardware, software and maintenance cost savings.

StealthWatch Monitors User Activity Without Violating Policy

Academic institutions are encouraged to limit packet analysis due to concerns about students' online privacy. Pleunes explains, "Only when we have evidence of unwanted behavior, can we take action against the person(s) responsible. That's why StealthWatch is so useful to our team. Although we don't capture the actual data that crosses the wire, StealthWatch provides tremendous visibility and maintains weeks of host activity that we can use to identify patterns of unwanted behavior—without infringing on students' privacy."

Under the previous setup, GLR could only retain packet data for one-day, thereby severely limiting forensic investigations. But, StealthWatch monitors host conversations and maintains weeks of historical user activity for GLR's network. StealthWatch immediately identifies IPs and users involved in incidents, and its historical data supports much broader forensic investigations. The GLR team ultimately relies on StealthWatch to identify network abuse and enforce compliance with network and security policies.

"By leveraging sFlow data from our Brocade routers and switches, StealthWatch offers tremendous visibility into the network core, generates valuable network performance reports and performs automated actions on network devices."

About Lancope, Inc.

Lancope®, Inc. is a leading provider of flow-based monitoring to ensure high-performing and secure networks for global enterprises. Unifying critical network performance and security information for borderless network visibility, Lancope provides actionable insight that reduces the time between problem identification and resolution. Enterprises rely on Lancope to make better network decisions, respond faster to network problem areas and avoid costly outages and downtime — at a fraction of the cost of conventional network monitoring solutions.

Lancope Headquarters

3650 Brookside Parkway
Suite 400
Alpharetta, GA 30022

U.S. Sales

+1.770.225.6500
888.419.1462

International Sales

+44 (0)560 344 8075

Website: www.lancope.com

E-mail: sales@lancope.com

©2011 Lancope, Inc. All rights reserved. Lancope, StealthWatch and other trademarks are registered or unregistered trademarks of Lancope, Inc. All other trademarks are properties of their respective owners.

MB08102010