Case Study

University of Glasgow Scales its Intrusion Detection System to Support 30,000 Users

“The cyber criminals will keep upping their game and it’s up to us to keep pace with them.”

–Chris Edwards, *Information Security Coordinator, the University of Glasgow*

Customer Benefits

- Monitor all of the traffic coming across its 10Gb Internet links
- Detect compromised PC’s before damage is done – helping identify users with a virus and taking remedial action
- Operate its IDS systems on a cluster of commodity servers, saving cost
- Repurpose existing network monitoring and measuring equipment

Gigamon Solution

- Gigamon Visibility Platform

Challenges

Like all large institutions, the University of Glasgow must protect itself against the ever increasing rise in IT security threats. The university uses an Intrusion Detection System (IDS) system to alert it to potential threats but with 30,000 users it is faced with a huge problem of scale.

Chris Edwards, Information Security Coordinator at the university, said, “The cyber criminals will keep upping their game and it’s up to us to keep pace with them. Using IDS to monitor our network traffic is similar in many ways to using an antivirus program on a PC. But we have to be able to do this concurrently for 30,000 users. This means we have to monitor huge volumes of Internet traffic.” The university had been using a mirrored port on one of its Internet gateway routers, which fed its IDS system, but it was limited to 1Gb of traffic. As Internet traffic grew to tens of gigabits per second, this port was only able to monitor a fraction of the overall capacity, and it became less and less probable that the system would identify malware or cyber attacks.

The problem couldn’t be resolved simply by adding multiple mirrored router ports, because the algorithms within the routers only allowed traffic to be mirrored to a single port, rather than spread across several ports. That meant the only way to scale the existing IDS system would be to mirror all the traffic to a single port running faster than 10Gb. Even if this had been viable, by putting in expensive new gateway routers for example, the IDS servers could only support 1Gb interfaces so they couldn’t have received information at this higher rate.

Selection Criteria

The University of Glasgow looked at a wide range of possible solutions, before being introduced to Gigamon’s technology by a systems integrator, Synetix Solutions. The university was impressed by a number of characteristics of the Gigamon solution:

- It’s 10Gb capability was key for delivering the solution the university needed, and it also had plenty of headroom for the future
- The granularity of Gigamon’s hardware-based filtering would allow it to select only the traffic it needed to send to the IDS systems
- It was cost-effective, and included platforms at the right scale

Solution

The university selected the Gigamon solution to enable it to scale its IDS infrastructure. All external Internet traffic is mirrored using Gigamon's optical traffic splitters, which duplicate all the traffic passing over the 10Gb links. The system then uses Gigamon's hardware-based patented Flow Mapping technology to isolate the traffic that needs to be sent to the IDS systems.

Edwards added, "For example, we might be sending some massive data files from the Large Hadron Collider project – which we know we can trust and might be too large for our IDS servers to analyze. We can use the Gigamon systems to filter this traffic out, based on source and destination addresses, and significantly reduce the load on the IDS servers. When new sources come online, it's an easy process to exclude the ones we aren't interested in."

The Gigamon platform also performs a load balancing function to share the traffic across multiple 1Gb ports on the intrusion detection servers, using IP addressing to share the load evenly. This means the university can spread the IDS function across multiple cost-effective Linux servers, rather than having to invest in new high-end, higher bandwidth hardware.

Results

The University of Glasgow can now monitor all of the traffic coming across its 10Gb Internet links.

Chris Edwards said, "The Gigamon technology has solved our scale issues. Now we can detect compromised PC's before damage is done in a way we couldn't do earlier – helping identify users with a virus and taking remedial action. It enables us to split the traffic load across multiple monitor ports, minimising packet loss, so we can operate a cluster of multiple IDS boxes, comprised of cheap commodity hardware, each of which 'watche over' a portion of our campus."

As the system is fed from an optical splitter, the original mirror port on the router has been freed up for other purposes. And because the Gigamon systems can pre-filter the traffic that the existing tools are exposed to, it has been possible to reuse existing network monitoring and measuring equipment.

Chris Edwards was positive about his experience of working with Gigamon. He said, "We had direct contact with Gigamon from the outset. They lent us a trial system and provided engineering support. Once they'd explained how the system worked, we had a good understanding and could configure it ourselves – saving us a lot of time. We tend to use the CLI rather than the web GUI, which is nice and simple and we can't fault it."

Now that the Gigamon systems are installed, the university also sees other potential uses for them, such as testing the effectiveness of new firewalls by replicating some or all of the Internet traffic into the test firewall without disturbing the operational systems.

Next Steps and Lessons Learned

The university's network continues to grow, and now has 40Gb speeds running in its core. Like many educational establishments, it is also seeing a surge in demand for BYOD (Bring Your Own Device), increasing the potential exposure to malware even further. Despite this, the university believes the Gigamon solution will perform well into the foreseeable future.

Chris Edwards concluded, "The network traffic continues to grow, but now we can detect malware and attacks even better than we could before. I'd advise anyone in a similar position to talk to other similar organizations to see how they've solved this problem. We'll certainly be sharing our experiences around other UK universities."

About University of Glasgow

Founded in 1451, the University of Glasgow is the fourth oldest university in the English speaking world. Today it is a broad-based, research led institution with campuses in Glasgow and its suburbs as well as in several Glasgow teaching hospitals. The university has over 20,000 students and 6,000 members of staff. As one of the UK's leading research centres and a member of the prestigious Russell Group of UK research universities, it contributes to research programs with a global impact, in fields that range from the rapid detection of malaria to the biggest particle physics experiment in the world: the Large Hadron Collider.

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Platform and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network and application performance management solutions in enterprise, government and service provider networks operate more efficiently and effectively. See more at **www.gigamon.com**, the **Gigamon Blog**, or follow Gigamon on **Twitter**, **LinkedIn** or **Facebook**.

3105-02 06/17