Customer

uniserver

Industry

Managed Hosting, Cloud Hosting

Challenges

- Managing extensive traffic
- Cost effective DDoS mitigation
- Fully established service to customers
- Cooperation with the Dutch national scrubbing center NaWaS

Solution Benefits

- Complete traffic visibility with possibility to drill down to any communication
- Fast and cost effective way to combat DDoS attacks
- Deep understanding of attack characteristics
- Full range of methods for successful mitigation

Deployed Products

- Flowmon DDoS Defender
- Flowmon VA Collector

Contact

www.uniserver.nl

Uniserver Internet

Uniserver Internet is a leading cloud hosting provider on the Dutch market. It has over 8 000 customers and runs datacentres in Amsterdam and Maastricht Airport. Its staff consists of carefully selected specialist responsible for more than thousand successfully delivered cloud projects.

Situation

The Uniserver network provides managed hosting, shared hosting and infrastructure as a service (IaaS) offerings. In all these, the Uniserver network and its availability are crucial for their 8 000+ customers. From Uniserver's datacenters, multiple connections towards public peers, private peers as well as transit providers are available. To ensure business continuity, Uniserver was looking for an anti-DDoS solution to protect its infrastructure and customers.

Flowmon Solution Deployment

To support its goals, Uniserver has implemented Flowmon DDoS Defender. Using Flowmon DDoS Defender with adaptive baselining options, Uniserver is able to automatically detect DDoS traffic without the need of manually configuring thresholds. Flowmon also allows to zoom in on both actual and historical traffic characteristics. Along with automated reporting capabilities Uniserver is now updated on traffic and attack status and progress.

DDoS Defender allows Uniserver to initiate the scrubbing of incoming DDoS traffic through the NaWaS, the Dutch non-profit DDoS Scrubbing Centre. Sample data is collected from inbound traffic on all transit connection via sFlow and sent to the Flowmon Collector. The Flowmon DDoS Defender module analyses the sFlow information and generates dynamic baselines for traffic flows. If traffic flows deviate too much from normal behavior, Flowmon can trigger based on manual and adaptive thresholds after which traffic is rerouted via the NaWaS scrubbing center. DDoS defender does this by propagating more-specific prefix to a route server. This route server propagate this route to the NaWaS.

As soon as the NaWaS receives such a more-specific prefix it propagates this to the Internet via their transits to attacked traffic. The scrubbing center filters out DDoS traffic and sends "clean" traffic via the existing NL-IX Internet Exchange infrastructure to Uniserver's network.

Customer Review

Chango Eersel, Director of Operations at Uniserver Internet, summarizes the Flowmon deployment:

"There are a number of reasons why we are very pleased to work with Flowmon Networks. The ease of deployment and use allows us to effectively monitor our network traffic and take actions promptly. With dynamic baselines being used, the amount of work required to maintain the deployment is limited while highly effective. This gives both Uniserver and its customers peace of mind allowing more focus on their business."