AFR-IX telecom

The African network operator AFR-IX chose the joint solution from Flowmon & F5 to protect their infrastructure against volumetric DDoS attacks. Flow-based detection by Flowmon and mitigation capabilities of F5 together ensure reliable protection in a fully automated workflow.

Area of activity

Telecommunication services

Challenges

High service quality standards

Fully automated and cost-efficient DDoS protection

Lack of detailed visibility into network traffic

Solution benefits

Near real-time DDoS attacks detection

Out-of-path mitigation via F5 BIG-IP

Comprehensive solution covering DDoS Protection and Network Performance Monitoring

Ease of use, professional maintenance and support

Deployed products

Flowmon Collector VA

Flowmon DDoS Defender

F5 BIG-IP AFM

CUSTOMER REQUIREMENTS

As a leading provider of high-speed Internet connection in West and Central Africa, AFR-IX Telecom sought to ensure high quality of their service by setting up DDoS attack protection. The company required a complex and fully automated out-of-band solution that would effectively protect their extensive infrastructure, including West and Central African backbone and marine cables.

AFR-IX preferred a solution that would make use of their existing Cisco infrastructure that featured flow export capabilities and BGP Flowspec. The desired solution was expected to collect, store and analyze NetFlow data from border routers and use them to detect volumetric DDoS attacks on specific subnets or Autonomous Systems (AS).

Should an attack occur, the solution was required to automatically redirect the traffic and instruct an out-of-path mitigation device to scrub the attack, with no need of manual intervention.

On top of DDoS protection, AFR-IX Telecom required NPMD analysis tools that would provide them with detailed reporting and alerting, allowing for deep post-attack analysis and efficient solving of daily operational issues.

CUSTOMER TESTIMONIAL

Armen Durgaryan, Network Engineer at AFR-IX Telecom

"The joint solution of Flowmon and F5 helps us keep our lines clear from malicious traffic even in the middle of an attack, preventing degradation of service on the side of our customers who are mostly ISPs and enterprises in western and central Africa. Moreover, the in-built NPMD tools decrease MTTR for troubleshooting operational problems and help optimize overall network performance."

THE DEPLOYED SOLUTION

The first part of the deployment was a **Flowmon Collector VA**. Its purpose is to collect, receive, and store sampled flow data from tens of flow sources. The collector capacity was optimized for storing months of unaggregated flow data history.

Once the collector was deployed, AFR-IX Telecom gained detailed visibility into their network traffic and a perfect overview of what was happening in the system at any given time.

Armen Durgaryan, Network Engineer at AFR-IX Telecom, sums up the NPMD features after six months of hands-on experience: "*Compared to the previously used SNMP and basic flow-based monitoring solutions, it is now much easier for us to visualize the traffic and get instant insight whenever we receive complaints or system alerts on service degradations. What is more, we always have hard evidence of the traffic legitimacy and it's also easier to find the root cause of the degradation.*"

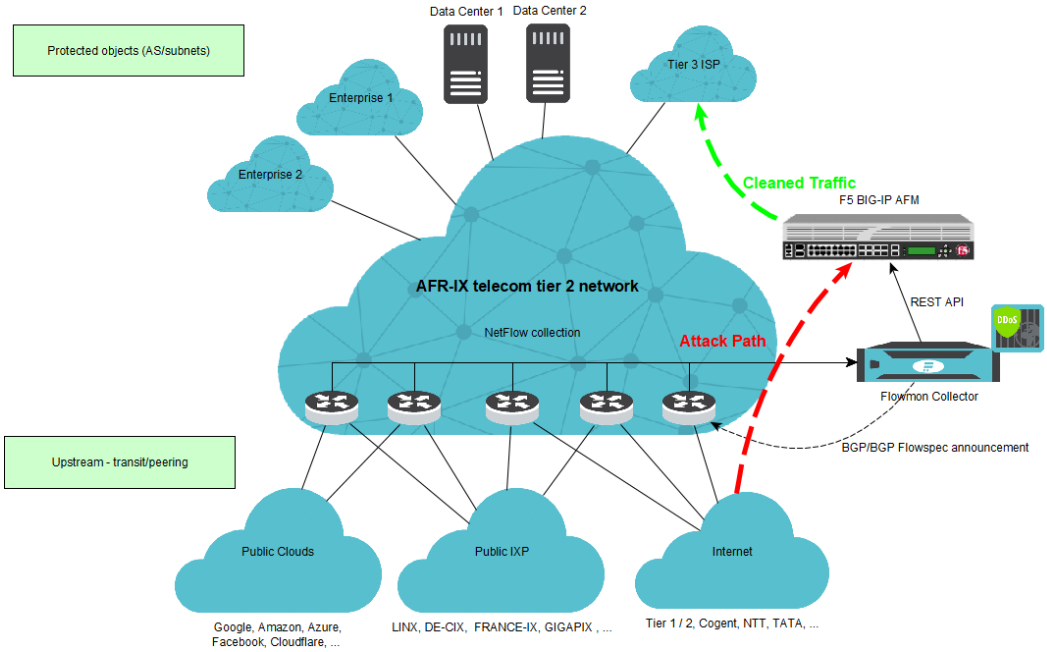
The next vital part of the deployment is the **Flowmon DDoS Defender** module, installed on the collector. Its task is to monitor the traffic and raise alerts according to baselines that are dynamically adjusted for each protected segment individually. AFR-IX Telecom chose to define the protected segments by the number of AS (Autonomous Systems) as their customers are local ISPs with their own AS. This approach is flexible and makes the system resistant to changes in the ISPs' subnets.

In case of an unexpected traffic increase in any network segment, DDoS Defender immediately reports an ongoing DDoS attack. AFR-IX Telecom opted to configure the solution to automatically redirect an attack lasting more than two minutes to a mitigation device, which is **F5 BIG-IP AFM**, deployed out-of-path. Thanks to the seamless integration of Flowmon and F5, DDoS Defender can configure the BIG-IP AFM device automatically, which makes it possible to redirect the harmful traffic instantly and without human intervention.

Finally, the **BGP Flowspec** feature can send commands to routers according to a dynamic signature of an attack, for example, it can instruct routers to redirect or drop the traffic that corresponds to the signature.

The described solution architecture means that AFR-IX Telecom can react flexibly to network threats and offer effective, tailored mitigation strategies to their customers.

[Learn more about Flowmon & F5 integration.]



ABOUT THE COMPANY

AFR-IX Telecom operates a Telecommunications network in West and Central Africa, offering the largest MetroEthernet fiber network coverage in the region. Thanks to the extensive core network, its protected backbone in Europe (London, Paris, Lisbon, Frankfurt…), and partnership with the best local telecommunications operators and ISPs, AFR-IX also provides the fastest connection to the rest of the world.

AFR-IX prides itself on being able to cater for connectivity needs of companies of any size, in both private and public sector. The service includes setting up a complete IT infrastructure and providing high-quality IPLC, MPLS L2 and L3 services.