DSL Service Provider
Africa
DSL

Case Study

Africa national carrier secures DSL infrastructure against cyber attacks without installing new equipment

About the Carrier

Our DSL service provider is the national telecommunications carrier of the country, established in the 1990s, and today serving close to 146,000 customers. As the leading provider of high-speed broadband service, the operator offers unlimited downloads, Internet on the go, and much more. Broadband and mobile broadband service plans are available throughout the country, including underserved areas, making the Internet accessible, affordable and safe for everyone.

Challenge

For a number of years, the national carrier had been successfully managing traffic and controlling congestion on their 5 POPS which provide both local peering and international Internet exchange links for the operator. Allot Service Gateways are deployed at 4 of the 5 POPS where they provide complete visibility of all network traffic as well as central management and reporting. Over time, the carrier noticed that despite their traffic management policy and enforcement measures, the network was experiencing more frequent and extended episodes of congestion which threatened the quality of experience they were able to deliver. The carrier turned to Allot channel partner, Business Connexion (BCX), a leader in advanced ICT products, services and solutions throughout Africa, to help them find the cause of the congestion and to control it.

Solution

The experts at Business Connexion suspected volumetric cyber attacks were causing the congestion and threatening infrastructure assets and service availability. Since Allot Service Gateways were already deployed at critical points in the network, the integrator knew there was a fast and effective way to verify our hunch, without disrupting broadband service or installing new equipment. BCX recommended a proof-of-concept trial in which Allot ServiceProtector sensors would be activated in one of the Allot Service Gateways deployed at a local POP. Allot ServiceProtector provides real-time DDoS Protection and Bot Containment services that are fully integrated and embedded in every Allot service delivery platform.

After simple remote activation, Allot's Network Behavior Anomaly Detection (NBAD) sensor began to identify volumetric attacks coming into the POP. Likewise, Allot's Host Behavior Anomaly Detection (HBAD) sensor identified outbound traffic anomalies that were most likely generated by spammers and other bot infections within the carrier network. Real-time notifications and detailed attack reports provided by Allot revealed that the network was being threatened from without and from within. In fact, 99% of these disruptive events were outgoing spam in the form of massive DNS and SMTP attacks.

Business Connexion
Connective Intelligence

Allot ServiceProtector shows who is attacking and abusing the network and automatically stops the attack in its tracks - before it can damage service availability and business continuity."

Challenge

Discover the cause of frequent and unpredictable episodes of network congestion and the best way to control it.

Solution

Activate Allot ServiceProtector DDoS Protection and Bot Containment services embedded in the Allot Service Gateway platforms deployed at peering points and manage it all centrally.

Benefits

Assure service availability

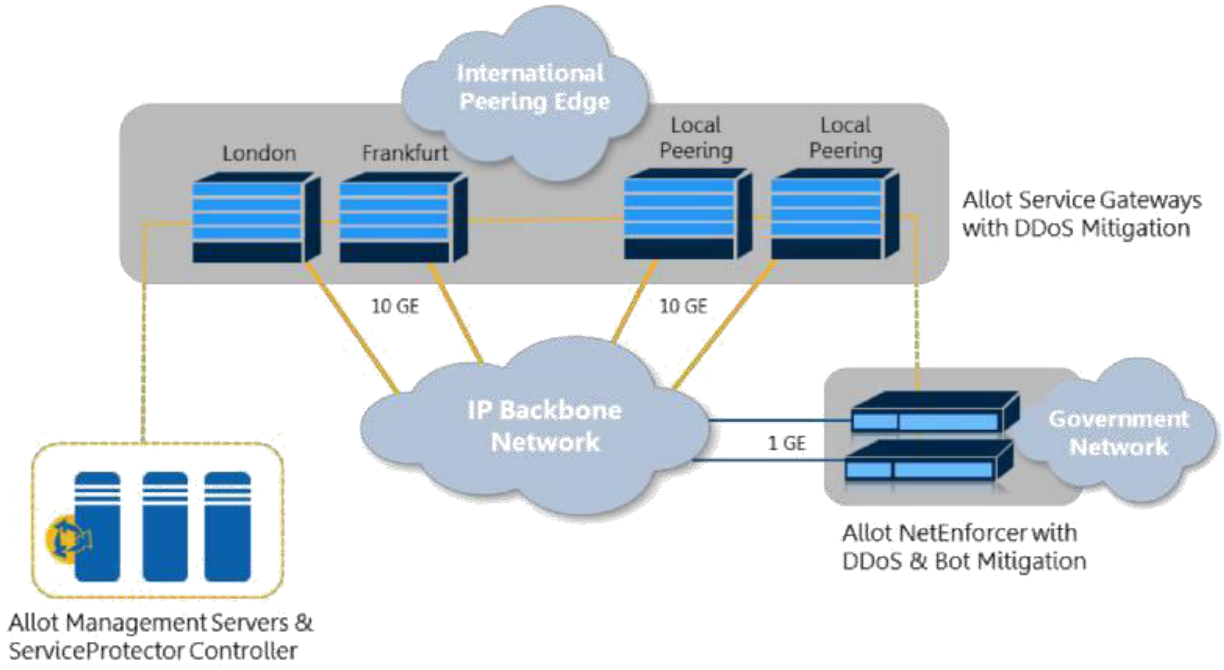
- Protect national infrastructure and ISP domain from blacklisting
- Eliminate traffic spikes and congestion from attack traffic

Maintain consistent

Allot communications

Deployment

Carrier operations personnel and Business Connexion agreed that the next step was to deploy Allot ServiceProtector at each of their international POPs so they could neutralize DDoS attacks at the network edge, far from their subscribers and before network performance was affected. Fast implementation was aided by Business Connexion engineers who asked the right questions, explored deployment scenarios and verified requirements up front, so once the decision was made, both DDoS Protection and Bot Containment services were up and running within one week. ROI began just a few days after installation, when Allot ServiceProtector detected and surgically blocked a large outbound spamming attack before the spam traffic could go out over the international links and result in blacklisting of the national broadband carrier's IP domain. And the protection has continued ever since.



The National Broadband Carrier deploys Allot DDoS Protection and Bot Containment services at critical peering and service nodes to neutralize inbound and outbound threats before they affect service availability and customer quality of experience

Benefits

By deploying Allot's DDoS Protection and Bot Containment services at international and local peering POPs, the National Broadband Carrier is able to:

- Increase available bandwidth by halting volumetric DDoS attacks at the network edge
- Protect national infrastructure from debilitating attacks and their IP domain from blacklisting
- Maintain consistently good quality of experience across the entire network
- Reduce the complexity and time spent on congestion management
- Gain accurate visibility into cyber attacks and their targets in the network

Conclusion

Allot's ability to integrate multiple solutions in a single platform allowed the carrier to trial and implement the network security services we needed in very little time and without introducing new inline systems. The carrier now has more accurate visibility and knows what is happening at all times on the network. They are so satisfied with the results of their deployment of Allot ServiceProtector, they are planning to extend the solution to the customer access edge, and in doing so, protect their network from DDoS attacks that originate in the access network.

© 2016 Allot Communications Ltd. All rights reserved. Specifications are subject to change without notice. Allot Communications, Sigma and NetEnforcer and the Allot logo are trademarks of Allot Communications. All other brand or product names are the trademarks of their respective holders.