allot
See. Control. Secure.

Success Story

African National Broadband Carrier

National Carrier Secures DSL Infrastructure Against Cyber Attacks Without Installing New Equipment

About African National Broadband Carrier

This 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 several 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.

Vertical | Service Provider

Industry | Fixed

Region | EMEA

Solution | DDoS Protection

Challenge

- Random extended episodes of congestion
- Existing traffic management policy and enforcement measures were not enough

Solution

The carrier had 4 existing Allot Service Gateways at critical network points. Business Connexion (BCX, Allot channel partner) was able to diagnose and test a suspicion about the source or the congestion by remotely activating the embedded DDoS Secure technology. Proof of concept was demonstrated and DDoS Secure was activated on all four Service Gateways to solve the challenges without incurring significant infrastructure investment costs. Within days, the ROI began when our solution mitigated a large outbound spamming attack that could have resulted in IP blacklisting.

Benefits

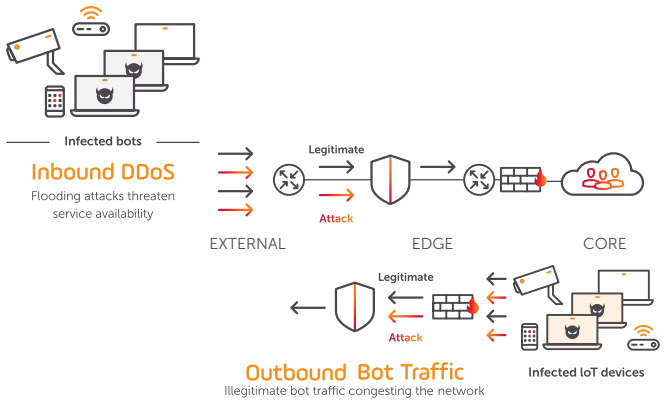
- Assure service availability and maintain high QoE
- Protect national infrastructure and ISP domain from blacklisting
- Eliminate traffic spikes and congestion from attack traffic
- Maintain consistent “SpeedTest” performance

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, it was easy to verify the hunch without disrupting broadband service or installing new equipment. BCX recommended a proof-of-concept trial in which Allot DDoS Secure sensors would be activated in one of the Allot Service Gateways deployed at a local POP.

Allot DDoS Secure provides real-time DDoS Protection and Bot containment services that are fully integrated and embedded in every Allot service delivery platform. After a 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 external sources and from within the network. In fact, 99% of these disruptive events were outgoing spam in the form of massive DNS and SMTP attacks.



After the successful proof of concept, carrier operations personnel and Business Connexion agreed that the next step was to deploy Allot DDoS Secure at each of their international POPs to mitigate the attacks. 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 DDoS Secure 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. The protection has continued ever since.

> With Allot DDoS Secure, the carrier can see who is attacking and abusing the network and automatically stop the attack in in real-time - before it damages DSL service availability and business continuity."
>
> IT Network Manager, Africa National Broadband Carrier

Deploying Allot DDoS Protection and Bot Containment services at critical peering and service nodes enables the carrier 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

Resources

About DDoS Secure

About Service Aware DDoS Mitigation

Frost & Sullivan DDoS Mitigation Whitepaper

Learn more about Allot's Solutions »

Aug 2019