Carrier-Grade DDoS Protection with NBIP NaWas and GenieATM

Challenge

Distributed Denial of Service (DDoS) attacks have emerged as one of the most prevalent and disruptive cyber threats targeting communications service providers (CSPs) in recent years. The scale and frequency of these attacks continue to escalate, with attack sizes growing year over year. Volumetric DDoS attacks not only impact the target victim but also exhaust the processing capacity of network resources, leading to interruptions in network connectivity and affecting the CSP's network infrastructure and other customer networks sharing the same resources.

For CSPs, it is crucial to detect DDoS attacks as early as possible within the network infrastructure to minimize their impact. However, the distributed nature of these attacks makes detection challenging, as they can originate from anywhere within the network. The high cost and hassle of deployment makes inplementing detection systems on every edge link connecting the backbone to customer networks impractical. Moreover, despite the distributed traffic from bots collectively can harm the network, the traffic behavior of each individual bot may appear normal, making it even more difficult to identify attacks. Therefore, effective DDoS attack detection requires a network-wide approach that includes pervasive flow data collection and centralized detection intelligence. This approach provides a comprehensive view of traffic visibility across the network while enabling proactive detection and mitigation measures.

Key Features

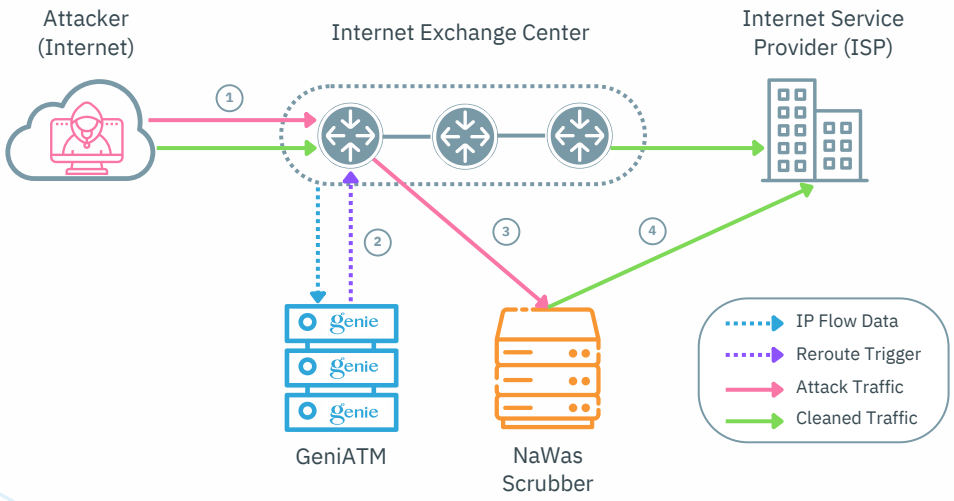
- Cost-efficiency with simple flow-based deployment and on-demand cloud mitigation
- Unparalleled DDoS threat detection with centralized control and machine-learned intelligence
- Cloud mitigation to ensure traffic cleaning as close to the source of the attack as possible
- Real-time and retrospective monitoring and in-depth analysis for network-wide traffic
- Multi-tenant, user-friendly web portal interface for easy MSSP Enabling
- No in-line latency and single-point-of-failure risks for normal traffic

GenieATM+NaWas Solution

Genie Networks and NBIP have partnered to deliver a comprehensive and cost-effective anti-DDoS solution with NaWas and GenieATM, which leverages IP Flow records, centralized detection, and out-of-path (OOP) traffic scrubbing. The joint solution offers a de facto standard for carrier-grade DDoS protection, including pervasive network visibility, real-time traffic analysis, and instant attack detection from GenieATM; and cloud-based high-performance scrubbing from NaWas , which offers direct connectivity to commonly used autonomous systems to ensure efficient mitigation as close to the attack source as possible.

Deployment

IP flow data from routers and switches across the network are constantly collected by GenieATM, which compares real-time traffic against established anomaly patterns and normal traffic baselines. When the real-time traffic matches an anomaly pattern or the traffic rate deviates from the baseline threshold, GenieATM generates an alert and initiates on-demand traffic scrubbing by redirecting suspicious traffic to the OOP NaWas scrubbing center through BGP route injection. After scrubbing, the clean traffic is returned to the border of the protected ISP via the Clean Path in the form of a port, dedicated or virtual, provided by the Internet Exchange. Only the traffic identified as suspicious by GenieATM is affected, ensuring precise and targeted mitigation. When the attack ends, traffic diversion is stopped, and all traffic goes back to its normal data path.



Out-of-Path Mitigation with NBIP NaWas and GenieATM

Benefits

With the joint solution of GenieATM and NBIP NaWas, CSPs are ensured with extensive coverage in protection against DDoS attacks. The network traffic intelligence provided by GenieATM enables early identification of sophisticated attack behaviors, while automatic mitigation orchestration and the NAWas scrubbing center ensure swift response to any suspicious traffic and eliminate it at early stage to minimize impacts. Network administrators can access detailed traffic information and scrubbing results through GenieATM's Web GUI, enabling manual mitigation, troubleshooting, and incident forensics in real-time.Through utilizing flow-based detectors and out-of-path cleaners, CSPs can benefit significantly from higher traffic rates and reduced deployment costs compared to inline devices. Providing DDoS detection and mitigation capabilities as managed security services presents an opportunity for CSPs to generate additional revenue for their end-user customers.

About NBIP

The Dutch National Internet Providers Management Organization (Nationale Beheersorganisatie Internet Providers, NBIP) provides supporting services to Internet providers. Among other things, it operates NaWas, the National Anti-DDoS Scrubbing Center, specialized in mitigating large volume DDoS attacks launched at ISPs and hosting providers. NaWas is an independent, non-profit and cooperative initiative that was launched in less than three months. It brought together rivalling companies to solve a problem that all faced: large scale botnet attacks resulting in serious downtime, angry customers and high mitigation costs. NaWas offers an on-demand DDoS protection to its participants. For more information, visit www.nbip.nl/en/nawas

About Genie Networks

Genie Networks is a leading provider of network traffic intelligence and security solutions that ensure complete visibility into data traffic trends and instant protection against cyber threats. Genie's head office resides in Taipei, Taiwan, with regional branches in Beijing, Shanghai, Tokyo, Mumbai, Singapore, and Moscow. Genie's products are deployed in more than 40 countries serving more than 650 customers worldwide. Learn more at www.genie-networks.com