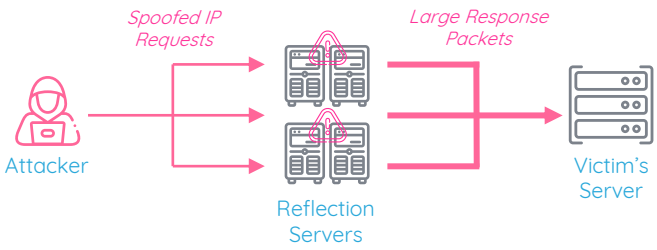
Solution Brief

Overcoming the Challenges of Modern DDoS Attacks for CSPs

The Evolving DDoS Threat Landscape

Over the past decade, Distributed Denial of Service (DDoS) attacks have been one of the major threats for Communications Service Providers (CSPs). Typically, DDoS attacks are launched with thousands of compromised devices flooding a targeted server with network packets or overwhelming a victim's internet connectivity to prevent legitimate use of a service. As technology advances, today's DDoS attacks are constantly evolving with the following characteristics:

- **Higher volume** – New volumetric attacks can be generated by leveraging IoT bots or new techniques such as a reflection-amplification. A reflection attacker spoofs a source IP address and sends a query via User Datagram Protocol (UDP) or Transmission Control Protocol (TCP). The server, unable to distinguish the spoofed IP from the actual victim's, responds to the query by sending answers to the victim's IP. An amplification attack involves the attacker using a relatively low level of bandwidth to cause a significant higher level of traffic to degrade the target victim's resources. Combining both a reflection and an amplification attack would allow the attacker to magnify and conceal the actual source of a DDoS threat.



A Reflection-Amplification Attack

- **More complexity** – The attacker can combine various techniques in a single attack to launch multi-vector attacks and dodge defense. An example is a carpet-bombing attack that sends attack traffic to multiple IP addresses and subnets within a CSP's network. The attack traffic alone may not be enough to devastate each individual target's connection and resources but can cumulatively bring down the CSP's network resources while evading mitigation systems.
- **Greater attack force** – Involves the attacker forming massive collection of enslaved botnets (especially IoT-based) by compromising more devices.

In addition to the growing sophistication, DDoS attacks continue to increase in magnitude and frequency. A tera-bit level attack is no longer an uncommon case, while events exceeding hundreds of Gbps are observed on a regular basis.

The Shortfall of Traditional Defense

Legacy inline solutions may be effective against state-exhaustion and application-layer attacks. But they alone lack the ability to provide comprehensive DDoS protection coverage, especially for CSPs.

A distributed DoS attack can easily have thousands, or even hundreds of thousands of attacking sources, coming from any links connecting to a network backbone. The more distributed the sources are, the more serious an attack's impact gets. Unlike the early days, many of today's attack traffic originate from compromised hosts within a CSP's network, rather than from the Internet. Furthermore, it is difficult to identify an attack traffic when observing from an individual source, as it usually appears normal. Only when the traffic gathers at a certain point in the attacking path, it brings harm to the targeted victim as well as to the network infrastructure it is passing through. An inline DDoS solution can only identify the portion of the attack traffic passing through the link it sits on and has no network-wide view to timely detect network-wide distributed attacks.

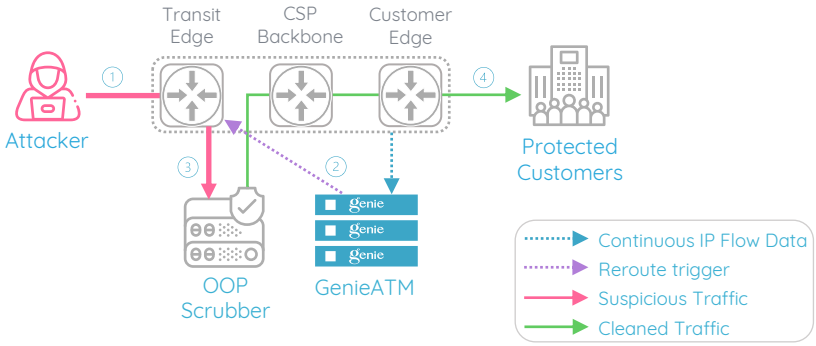
Another weakness of inline defense is that the device is often implemented near the protected servers to secure against the incoming attacks only, instead of the target victim's upstream network. If the upstream network is paralyzed, the Internet connectivity is lost, causing the targeted victim to be out of service. Volumetric malicious traffic not only jeopardizes the targeted victim but can also cause massive collateral damages to all the other hosts, servers, resources, and customer networks connecting to the same network infrastructure, resulting in severe service disruptions for CSPs.

To get a macroscopic view and perform timely detection over the entire network, it would only make sense to deploy an inline device on every link across the network perimeter, which means more deployment hassle and extremely higher cost for CSPs.

The GenieATM Carrier-grade DDoS Solution

GenieATM is purpose-built for comprehensive DDoS defense across the entire network infrastructure at carrier-grade scalability and performance. Based on a distributed architecture, GenieATM collects flow telemetry from routers and switches across the network. The system's centralized machine-learning detection engine then aggregates and correlates the collected data in real-time and performs cross-link analysis. GenieATM monitors not only the traffic bit rates and packet rates, but also the entropy of traffic source and destination IP addresses. The detection engine builds traffic baselines driven by machine learning mechanisms such as an ARIMA model for forecasting traffic time-series data. The machine-learning mechanisms ensure speedy, precise detection that spots attack within seconds with significantly reduced false negatives and false positives.

Upon detection, GenieATM integrates and automates attack mitigation countermeasures to minimize the impacts of widespread network disruption. These include blocking or shaping the anomaly traffic through BGP black-holing or FlowSpec, or simply diverting anomaly traffic to a scrubbing device deployed out-of-path (OOP). The scrubbing device then scrubs the diverted traffic and re-injects the cleaned traffic back to its original destination using a dedicated tunnel. When the attack ends, the black-holing, traffic shaping or traffic redirection will be stopped, and all traffic goes back to its normal data path. GenieATM continuously retrieves the cleaning stats of the diverted attacks from the scrubbing device and displays them as real-time attack mitigation reports via GenieATM's GUI.



Out-of-Path Mitigation with GenieATM

Comprehensive Protection at Better Cost

With GenieATM, CSPs achieve:

- Pervasive detection coverage by adopting a distributed architecture.
- Early detection of sophisticated attack behaviors through comprehensive network traffic intelligence.
- Immediate response to minimize the impacts with automatic mitigation orchestration.
- Lower CAPEX:

  - On the detection side, a flow-based detector can support much higher traffic rate and more network devices than an inline DDoS device.

  - On the mitigation side, the performance and capacity demand of an OOP cleaner is considerably lower than deploying an inline cleaner on an extremely high-capacity link or deploying multiple inline cleaners on multiple links. This is because an OOP cleaner doesn't need to inspect all the network traffic, but only the ingress and suspicious traffic diverted to it. The automatic traffic diversion mechanism also contributes to lower deployment cost as OOP cleaning resources can be shared dynamically among several DDoS service subscribers.

- Additional revenue generation by providing DDoS defense as value-added managed security service to their end customers like enterprises and government organizations.

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.

+886 2 2657 1088
sales@genie-networks.com
www.genie-networks.com