CARRIER-GRADE DDoS MITIGATION WITH F5 AND GENIE NETWORKS

KEY FEATURES

Network-wide detection—Carrier-grade DDoS detection in traffic data and for anomalies with unknown content signatures

Comprehensive DDoS mitigation—On-premises, out-of-path (OOP), and cloud-based traffic scrubbing of volumetric attacks to secure the network backbone and data center

Real-time traffic visibility—Carrier-grade network coverage and on-the-fly traffic matrix reports to enable 24x7x365 network monitoring and analysis

Managed security service provisioning—Highly scalable, multi-tenant portal design with intuitive GUI for managed security service providers

Network troubleshooting and forensics—An instant view of suspicious traffic and drill-down analysis for root cause investigation and retrospective analysis of anomalies

Industry-leading performance—Monitor traffic from up to 12,000 routers and detect terabyte-per-second attack scales per deployment

THE CHALLENGES OF CARRIER-GRADE DDoS MITIGATION

Distributed denial-of-service (DDoS) attacks continue to be a major threat to service providers. These volumetric attacks have increased year over year and often originate from a large number of geographically distributed bots. The high bandwidth of volumetric DDoS attacks not only saturates the target victim's resources but also exhausts network processing capacity and interrupts network connectivity. Consequently, a volumetric DDoS attack harms not only the target, but also the service provider's network infrastructure as well as customer networks sharing the same backbone resources. While today's DDoS attacks may use techniques such as reflection, NTP amplification, SSL, low-and-slow application levels, and advanced persistent threats, many are volumetric.

There are two primary challenges that service providers must overcome to prevent DDoS attacks:

- **Deploying detection everywhere is cost prohibitive**—The sooner an attack can be detected as it enters the network infrastructure, the easier it is to minimize harm. However, the distributed nature of DDoS attacks makes them difficult to detect because an attack can come from anywhere in the network. Deploying detection systems on every edge-link connecting the backbone network to customer or peering networks is cost prohibitive.
- **Early mitigation requires comprehensive DDoS mitigation**—Even when distributed traffic is gathered from all bots at certain points in the network, traffic behavior from each individual bot may appear normal, yet the network can still be harmed. To effectively detect DDoS attacks early, network-wide pervasive data collection is required, along with centralized detection intelligence, to provide a network-wide view of the traffic visibility.

KEY BENEFITS

Cost-effective performance—Enable small deployments with flow technologies and an out-of-path shared scrubbing center architecture.

Layered protection—Gain first-line L3–4 detection and scrubbing with L7 and cloud-based services.

No in-line risks—Eliminate latency and single-point-of-failure risks for normal traffic.

Managed security service provider (MSSP) enabling—Easily use GenieATM as a cost-effective, multi-tenant MSSP platform.

Comprehensive analysis—Provide network insights for real-time and retrospective traffic analysis.

THE CARRIER-GRADE DDoS ATTACK MITIGATION SOLUTION

F5 and Genie Networks have collaborated to deliver carrier-grade, out-of-path DDoS detection and mitigation with GenieATM and the F5® DDoS Protection reference architecture. This integrated solution offers service providers cost-effective DDoS mitigation capabilities that take advantage of IP flow records, centralized detection, and high-performance traffic scrubbing without the need for a DDoS mitigation device at every link.

F5 DDoS PROTECTION

The F5 DDoS Protection solution supports high-scale, high-performance architectures with full-proxy and SSL interception. The following products and services comprise the solution to meet the specific needs of service providers' networks:

- F5® BIG-IP® Advanced Firewall Manager™ (AFM) performs intrinsic L3–7 security that inspects every single user connection instead of sampling or watching traffic off a mirrored port.
- F5® DDoS Hybrid Defender® provides multi-layered security at the application layer with flexibility and scale for inline, out-of-band, and hybrid deployments.
- The F5® Silverline® DDoS Protection cloud-based service detects and mitigates even the largest of volumetric DDoS attacks at L3–7 before they reach the network.
- F5® Advanced Web Application Firewall™ (Advanced WAF), which can work in combination with the DDoS Protection solution for traffic scrubbing.

The F5 DDoS Protection solution offers high-performance protection from network layer attacks by using hardware (FPGA) accelerations, application-layer anomaly detections, web application firewalling, and SSL attack mitigation.

GenieATM MONITORING

GenieATM monitors the network by collecting IP flow records from various router/switch locations and comparing real-time traffic information against anomaly patterns and normal traffic baselines. Once the real-time traffic matches an anomaly pattern and the traffic rate deviates from the baseline threshold, GenieATM generates an alert. This alert triggers on-demand traffic scrubbing by diverting the suspicious traffic to the DDoS Protection solution. In combination with Advanced WAF, the DDoS Protection solution uses L3–7 security capabilities to remove threats from the off-ramped traffic. The cleaned traffic is forwarded back to the original customer destinations via tunneling mechanisms. In this way, the attacks are mitigated only when the traffic detected as suspicious by GenieATM is affected.

SERVICE PROVIDER HOSTED PROTECTION, ON DEMAND

GenieATM detects DDoS attacks from any part of the network without requiring detection systems on every link. GenieATM detects attacks by receiving IP flow records exported from the routers in the network and uses its analytics engine to determine if anomaly traffic is occurring. If so, it instructs the BGP routers to redirect the anomaly traffic to tunnel through BIG-IP AFM or DDoS Hybrid Defender deployed out-of-path (OOP) for scrubbing. After the anomaly traffic has been scrubbed, the cleaned traffic is sent back to the origin network via a generic routing encapsulation (GRE) tunnel. When GenieATM does not detect any more anomaly traffic, it instructs the BGP routers to restore traffic along its original path.

In a deployment like Figure 1 below, with the aid of GenieATM traffic detection and diversion, the DDoS Protection solution can also scrub traffic from other parts of the network that are not along its path or line of defense. Optionally, F5 Advanced WAF can sit in front of the service provider's servers, enabling the F5 DDoS scrubbing device to detect and mitigate layer 7 or application-level attacks that may not be volumetric but are nonetheless malicious. Service providers can cost effectively mitigate DDoS traffic by using GenieATM and F5 DDoS Protection to detect and scrub DDoS traffic from any incoming link in the networks without purchasing multiple in-line devices.

The traffic details of detected anomalies and the traffic scrubbing results are presented to network operators and service providers through the GenieATM GUI. A range of actions can be taken to initiate and stop a mitigation action automatically or manually and to perform real-time troubleshooting and incident forensics.

GenieATM and F5 DDoS Protection comprise an integrated solution that enables service providers to monitor, detect, mitigate, and trace back DDoS attacks. The solution helps ensure network backbone security and also serves as the basis for a managed DDoS mitigation service. Service providers can generate revenues by offering DDoS detection and mitigation capabilities for their managed security service (MSS) customers.

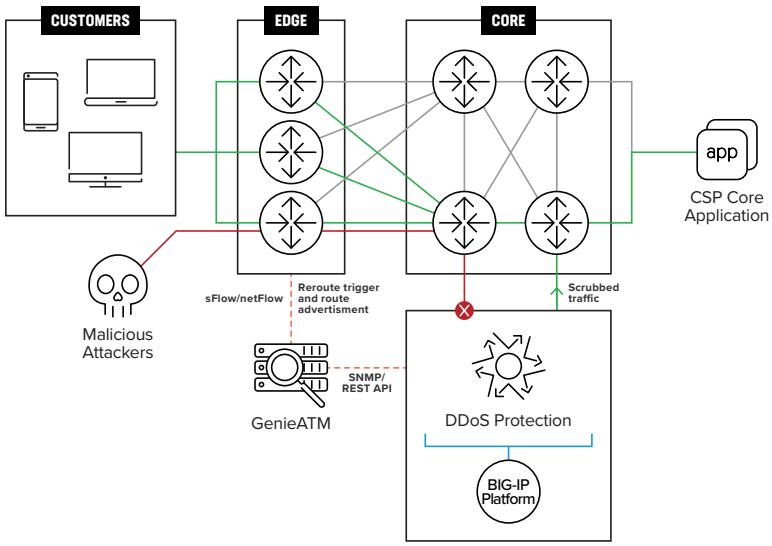

Figure 1: DDoS attack detection and mitigation with GenieATM and F5 DDoS Protection

CLOUD-BASED PROTECTION, ON DEMAND

GenieATM can divert DDoS traffic to Silverline DDoS Protection, a cloud-scrubbing service delivered via the Silverline cloud-based platform. Anomaly traffic detected by GenieATM can be diverted to Silverline DDoS Protection under the following conditions:

- GenieATM detects that the DDoS attack volume could potentially overwhelm the service provider's network infrastructure.
- In a DDoS volumetric attack of unprecedented size, the service provider's on-premises device (OOP or inline) isn't large enough to handle the DDoS volume.

Under these conditions, GenieATM will perform a BGP route injection to re-direct the anomaly traffic through the Silverline DDoS Protection scrubbing infrastructure. The diverted DDoS traffic passing through the Silverline cloud-based infrastructure will scrub traffic from layer 3 all the way to layer 7. The scrubbed traffic is then tunneled back to the original service provider's network through a virtual private network (VPN) or GRE connection.

This is how GenieATM and Silverline DDoS Protection can provide an integrated hub for on-premises and cloud-based scrubbing that delivers full DDoS, high-capacity mitigation for service providers and their customers.

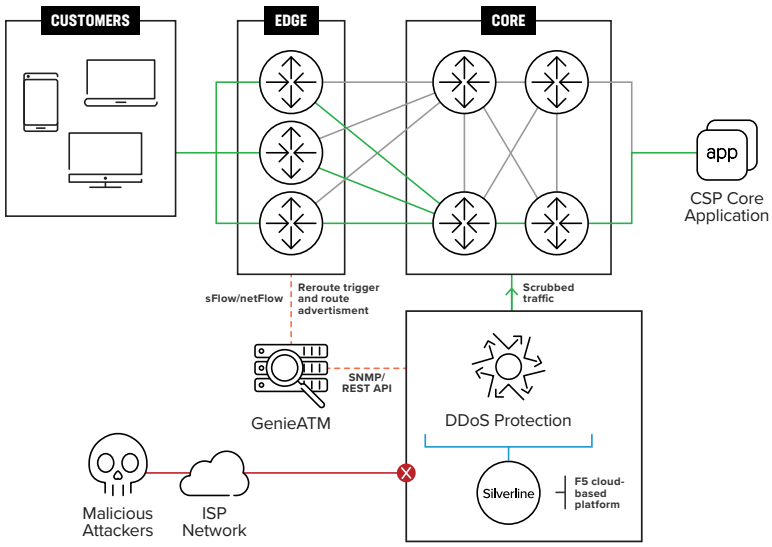

Figure 2: DDoS attack detection and mitigation with GenieATM and Silverline DDoS Protection

F5 DDoS PROTECTION SOLUTION AND GenieATM PROVIDE:

DDoS security—In-cloud detection and OOP mitigation for network backbone, Internet data center (IDC), and Internet-exchange DDoS protection

On-premises and cloud-based DDoS protection—Comprehensive defense with a cloud-based option for massive volumetric attacks that might overwhelm infrastructure

Managed security service provisioning—A scalable, multi-tenancy design that offers a cost-effective platform for MSSPs

Network-wide visibility—Network topology-based traffic matrix reports for 24x7x365 network monitoring and analysis

Network troubleshooting—An instant view of suspicious traffic and drill-down analysis for root cause investigation

Network forensics—Retrospective analysis for anomaly investigations

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, and Singapore. Genie's products are deployed in more than 40 countries, serving more than 500 customers worldwide.

LEARN MORE

For more information about GenieATM and the F5 DDoS Protection solution, visit:

Genie Solutions
F5 Genie DDoS Solution