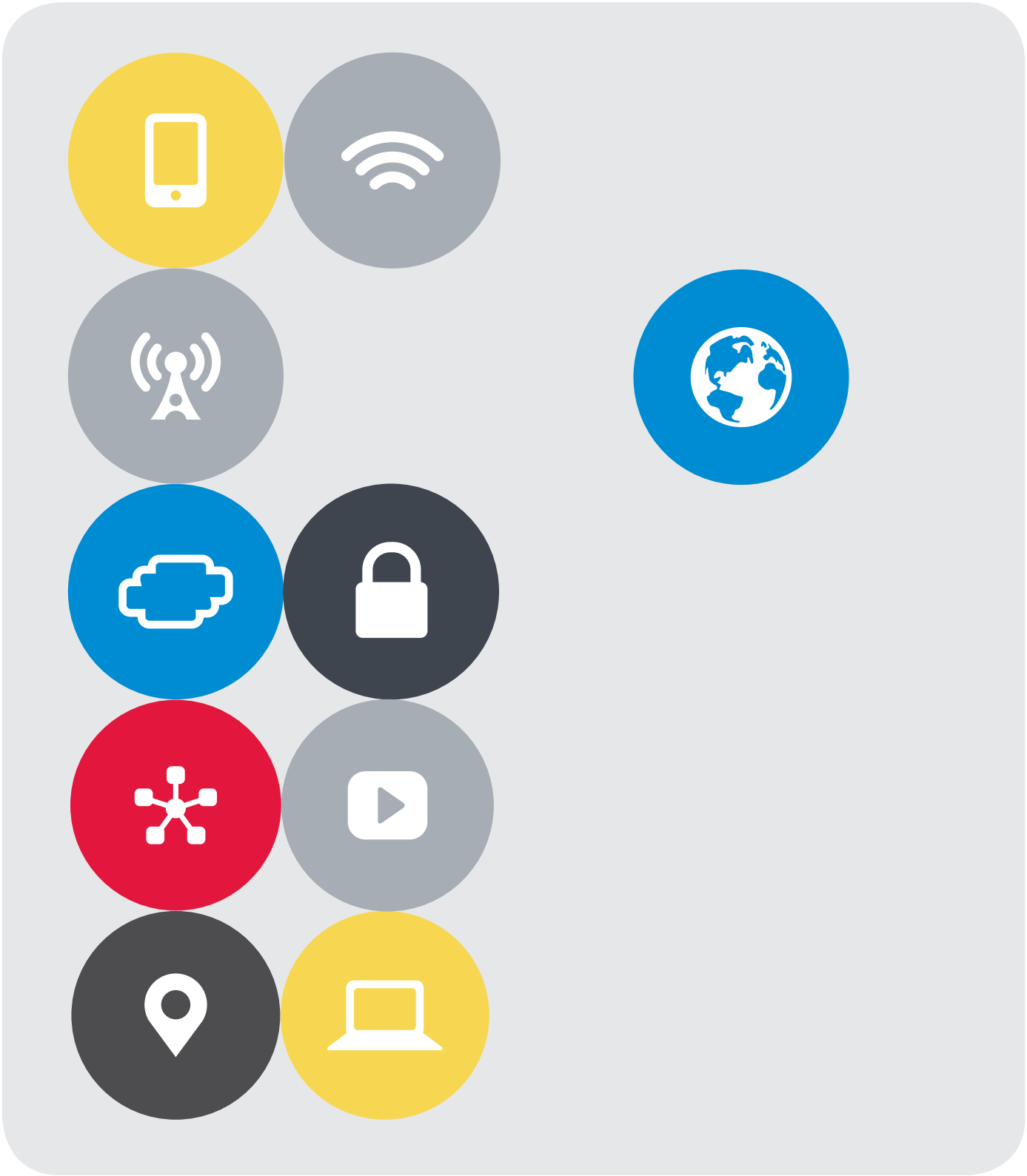
OVERVIEW

Carrier-Grade DDoS Mitigation with F5 and Genie Networks



Carrier-Grade DDoS Mitigation

Key features

- Network-wide detection—carrier-grade network coverage leveraging IP flow records from routers/switches.
- Analysis-based network behavior—traffic data analysis to detect anomalies with unknown content signature.
- In-line cleaning on demand—in-line cleaning for suspicious traffic only.
- Real-time traffic visibility—on-the-fly reports of normal traffic, anomaly traffic, scrubbed traffic, traffic snapshots, and forensic reports.
- Industry-leading performance—monitors traffic from up to 3,000 routers and scrubs the suspicious traffic up to 155 Gbps per deployment.

Distributed denial-of-service (DDoS) attacks continue to be a major threat to service providers. These volumetric attacks have increased year over year and usually originate from a large number of geographically distributed bots. The high bandwidth of volumetric DDoS attacks saturates not only the target victim's resources, but also exhausts network processing capacity and interrupts network connectivity. Consequently, a volumetric DDoS attack impacts not only the target victim, but also the service provider's network infrastructure—as well as customer networks sharing the same network backbone resources. While many attacks are still volumetric, attackers leverage many other techniques including NTP amplifications, SSL, and low-and-slow attacks at the application level.

Challenges of Providing DDoS Security

Securing a network poses two main challenges:

- Cost prohibition of securing every peering link to prevent DDoS attacks
- Comprehensive DDoS detection and mitigation

Cost prohibition

The sooner an attack can be detected as it enters the network infrastructure, the easier it is to minimize its impact. 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 backbone networks to customer or peering networks is cost prohibitive.

Comprehensive DDoS mitigation

Even when distributed traffic is collected 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, which possesses a network-wide view of the traffic visibility.

The Solution

Key benefits

- Cost performance—small deployment due to flow technologies and shared scrubbing center architecture.
- Layered protection—first-line L4 detection for volumetric attacks with L7 attack scrubbing capability.
- No in-line risks—no in-line latency or single-point-of-failure risks for normal traffic.
- Managed security service provider (MSSP) enabling—web GUI portal with multi-tenant design for enabling MSSPs easily.
- Comprehensive analysis—traffic insights for security incidents and reports for peacetime traffic.

F5 and Genie Networks have collaborated to bring carrier-grade, out-of-path DDoS mitigation with F5® DDoS Protection and GenieATM solutions. These integrated solutions enable cost-effective DDoS mitigation capabilities for service providers by leveraging IP flow records, centralized detection, and high-performance traffic scrubbing—without the need for a DDoS mitigation device at every peering link.

F5 DDoS Protection

The F5 DDoS Protection solution supports high-scale, high-performance architectures, with full-proxy and SSL interception. It provides an intrinsic L3–7 security that inspects every single user connection instead of sampling or watching traffic off a mirrored port. The F5 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 triggers on-demand traffic scrubbing by diverting the suspicious traffic to the F5 DDoS Protection solution. F5 DDoS Protection uses L3–L7 security capabilities to remove threats from the off-ramped traffic. The cleaned traffic is then forwarded back to the original customer destinations via tunneling mechanisms. In this way, the attacks are mitigated when only the traffic detected as suspicious by GenieATM is affected.

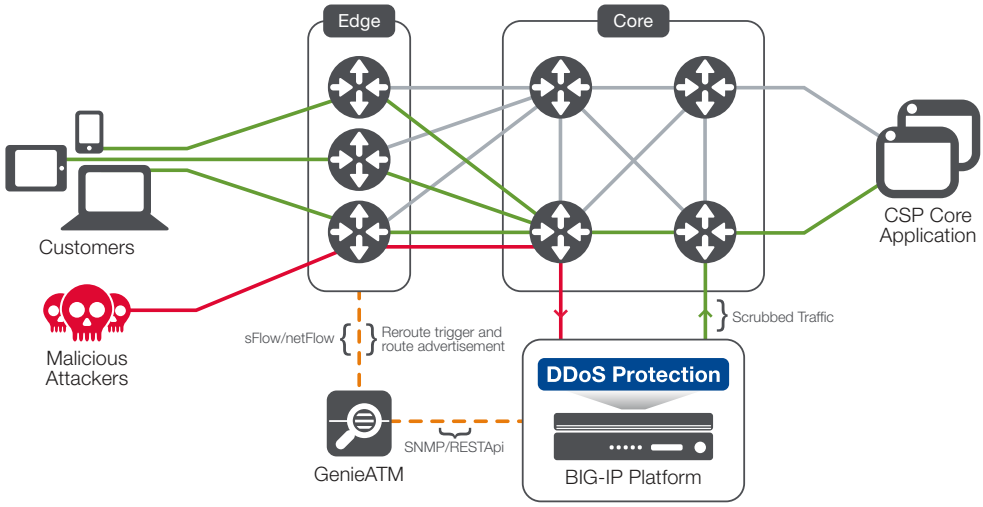
On-premises F5 DDoS Protection and GenieATM integration

With GenieATM, DDoS attacks from any part of the network can be detected without having to deploy detection systems on every link. This is done through integration with Border Gateway (BGP) routers, which send IP flow records to GenieATM. GenieATM uses its analytics engine to determine if an attack is occurring. If so, it directs the BGP routers to re-direct the affected traffic to F5 DDoS Protection for scrubbing. After the traffic has been cleaned and GenieATM has not detected further DDoS traffic, it directs the BGP routers to restore traffic along its original path.

The service provider can cost effectively mitigate DDoS traffic using GenieATM and F5 DDoS Protection to detect and scrub DDoS traffic from any incoming link in the network—without purchasing multiple devices. The F5 solution can also scrub traffic from other parts of the network that are not in its path or line of defense. Optionally, F5's web application firewall 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, which may not be volumetric but malicious nonetheless.

The traffic details of the detected anomalies and the traffic scrubbing results are presented to network operators and managed service providers through GenieATM's web GUI. This allows a range of actions to be taken, including initiating/stopping a mitigation action manually or performing real-time troubleshooting and incident forensics.

F5 DDoS Protection and GenieATM solutions enable service providers to monitor, detect, mitigate, and trace back DDoS attacks. These solutions help ensure network backbone security and also serve 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.



GenieATM monitors the traffic while the F5 BIG-IP® platform (a component of F5 DDoS Protection) remains idle on an OOP link. Upon attack discovery, the traffic to the network under attack is diverted to the F5 solution for scrubbing. The BIG-IP device mitigates the attack and forwards the clean traffic to its original destination. When the attack ends, GenieATM removes the route injection for traffic diversion through the BIG-IP device.

Cloud-based F5 Silverline DDoS Protection and GenieATM integration

The GenieATM is also able to divert DDoS traffic to F5 Silverline® DDoS Protection, a cloud-scrubbing service delivered via the F5 Silverline cloud-based platform. DDoS traffic 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 attack of unprecedented size, the on-premises device isn't large enough to handle the DDoS volume.

Under these conditions, GenieATM will perform a BGP route injection to advertise the route to the destination or target server through the Silverline DDoS Protection scrubbing infrastructure. DDoS traffic passing through this cloud-based infrastructure will scrub traffic from layer 3 all the way to layer 7. The scrubbed or cleaned traffic is then directed back to the service provider's network through a virtual private network (VPN) connection.

Learn more

For more information about F5 DDoS Protection and GenieATM solutions, please see the following resources or use the search function on f5.com and genie-networks.com.

Web pages

F5 DDoS Protection solution

BIG-IP Advanced Firewall Manager

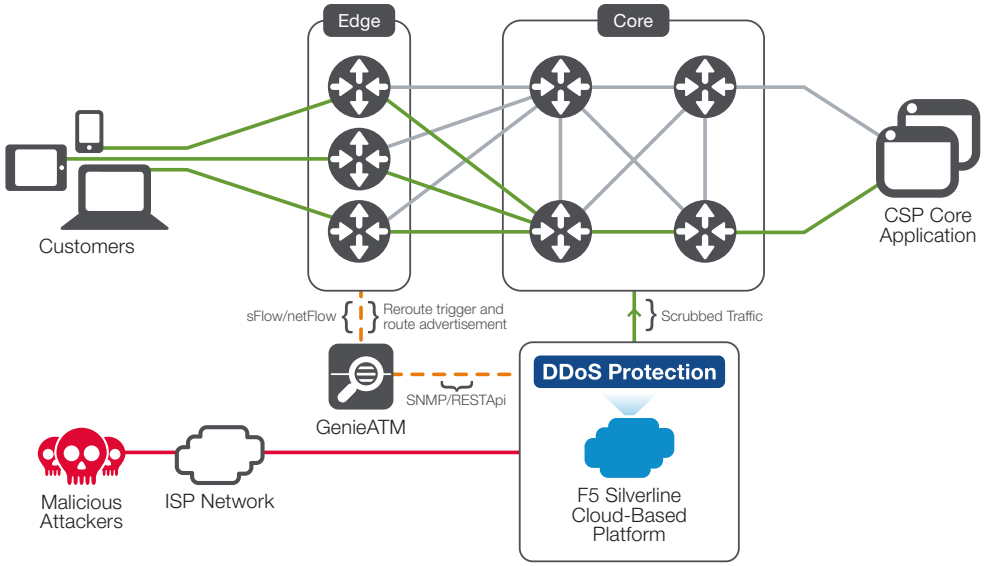
BIG-IP Application Security Manager

F5 Silverline DDoS Protection

GenieATM 6000 Series

White papers

The F5 DDoS Protection Reference Architecture



GenieATM diverts DDoS attacks to F5 Silverline DDoS Protection.

F5 DDoS Protection and GenieATM solutions provide:

- DDoS security—in-cloud detection and out-of-Path (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—the scalable, multi-tenancy design 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.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan K.K. f5j-info@f5.com

Solutions for an application world.