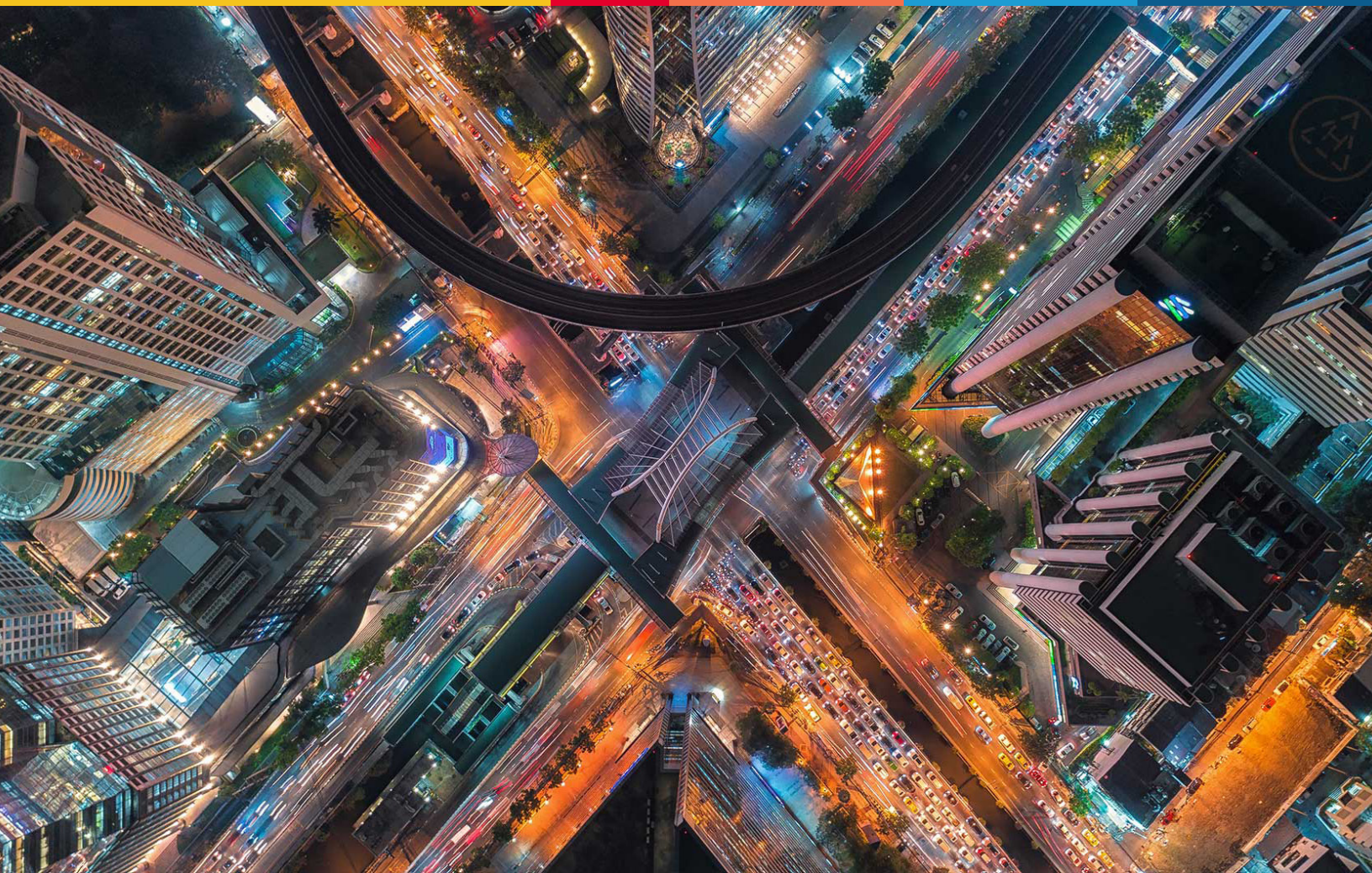
F5® Distributed Cloud DDoS Mitigation

Managed Service

F5 Distributed Cloud DDoS Mitigation is a managed, SaaS-delivered service that will detect and mitigate large-scale, volumetric network and application-targeted attacks in real-time to defend your businesses and your customers against multi-vector, denial of service activity that may potentially exceed hundreds of gigabits per second in attack traffic.



KEY BENEFITS

Keep Your Business Online During a DDoS attack
Stop DDoS attacks before they reach your enterprise network and affect your business, using real-time, DDoS attack detection and mitigation in the cloud.

Rapidly Protect Against All DDoS Attack Vectors
Engineered to rapidly respond and mitigate DDoS attack threats with multi-layered L3-L7 DDoS attack protection against all attack vectors.

Gain Attack Mitigation Insights
The F5 Distributed Cloud Services customer console provides transparent attack mitigation visibility and reporting before, during and after an attack.

Defend Against Volumetric Attacks
Protect your business from the largest DDoS attacks with industry leading DDoS attack mitigation that features multi-terabit migitation capacity.

SaaS Delivered, Globally Available, Minimal Business Impact
Deploy cloud DDoS protection rapidly with no impact on business operations, no additional investments in hardware or software to manage, using the F5 global network.

Obtain Expert Service
The F5 SOC (Security Operations Center) security engineers support you every step of the way and are available 24x7 to provide optimum service SLAs for uptime and response to DDoS attacks.

F5 Distributed Cloud DDoS Mitigation offers a SaaS-based, managed service option that detects and mitigates DDoS attacks in real-time. The F5 Security Operations Center (SOC) provides 24x7 global support. Our F5 SOC security engineers support the on-going availability of your applications.

F5 Distributed Cloud DDoS Mitigation leverages a globally secured network with Regional Edges (RE), hosted in scrubbing data centers, interconnected across a dedicated, multi-terabit, redundant, private backbone, operated by Tier 1 Carriers. Our highly available, global scrubbing centers and network reduce the risk of a single scrubbing center from being overwhelmed by intercepting traffic closer to the source of the origin of the DDoS attacks. The current list of scrubbing centers and operational status is available at F5 Distributed Cloud Status.

Distributed Cloud DDoS Mitigation

Effective security to protect your network and applications from targeted denial of service attacks aimed at disrupting your business

F5 Distributed Cloud DDoS Mitigation offers protection against a wide variety of DDoS attacks, targeted at Layer 3, 4, 7 internet protocols. Examples of common DDoS attacks mitigated by the service are:

Reflection and Amplification Floods	DNS Cache Poisoning
Datagram Fragmentation Attacks	Vulnerability Attacks
TCP Stack Attacks	Resource ExhaustionAttacks
Application Attacks	Flash Crowd Protection
SSL/TLS Attacks	NXDOMAIN Attacks

F5 Distributed Cloud mitigation inspects and subsequently scrubs customer traffic for large volumetric DDoS attacks, and is designed to permit only clean traffic to pass through and be returned securely back to the customers' origin network.

The DDoS mitigation service includes automatically applied edge mitigation that detects and proactively blocks traffic for known attack vectors for all customers across our entire network. F5 SOC DDoS engineers will by performing additional in-depth analysis of the traffic and apply countermeasures to mitigate attack vectors not addressed by the automatic edge mitigation. F5 Distributed Cloud DDoS Mitigation delivers full DDoS threat visibilty, reporting and Threat Intelligence services to block known malicious threats.

Customers may work with SOC engineers to establish values for rate-limiting return traffic to avoid overwhelming the customer edge network devices or application infrastructure. Granular detection and mitigation mechanisms provide customers flexibility in mitigating L7 DDoS attacks, without impacting the user experience.

F5 Distributed Cloud DDoS Mitigation Managed Service Components

Customers working with F5 will obtain maximum protection against DDoS activity to automatically mitigate the most egregious attacks

OPERATIONAL MODEL

F5 Distributed Cloud DDoS Mitigation managed service is delivered in two deployment modes; **Always On** (customer traffic is continuously routed through the F5 network) or **Always Available** (The F5 SOC or customers activate route changes to the F5 network prior to or while under a DDoS attack).

Customers may obtain F5 Distributed Cloud DDoS Mitigation services with a one, two or three year subscription. There are several values utilized to calculate the cost of the service. These include; number of FQDN's (Fully Qualified Domains) to be protected and/or number of data centers and routers to be protected, 95th percentile measured - peak amount of clean bandwidth consumed in bps, edge routers to be monitored for netflow/sflow data, and mode of operation (always on or always available).

STATISTICS INDICATE THAT BUSINESSES RISK BEING TARGETED WITH DDOS ATTACKS. THE GOAL OF THESE ATTACKS IS TO DISRUPT APPLICATION PERFORMANCE OR AVAILABILITY, BUT THE ATTACK VECTORS CAN VARY—TARGETING AVAILABLE BANDWIDTH, APPLICATION RESOURCES LIKE CPU AND MEMORY, OR CRITICAL INFRASTRUCTURE PROTOCOLS LIKE DNS AND TLS.

DEPLOYMENT MODES

F5 Distributed Cloud DDoS Mitigation service is available in two distinct modes: **Routed Mode** and **Proxy Mode**.

Routed Mode

Distributed Cloud DDoS Mitigation offers Routed Mode for customers who have at least one publicly advertised routing subnet [Class C - CIDR /24 prefix]. The service leverages the Border Gateway Protocol (BGP) to advertise the routing prefix through F5 carriers. Once the routing prefix is announced through the F5 platform and global network, all customer traffic inbound to the customer's prefix will be routed through F5 global scrubbing facilities for inspection and mitigation. Customers will control the route advertisement with the assistance of the SOC engineers.

Customers can select several configuration options to return clean traffic back to their network that include one or multiple GRE (Generic Tunnel Encapsulation) tunnels, an L2 connection and/or by privately peering with F5 global network through the Equinix Fabric and other connectivity providers. The SOC will work with customers to build complete redundancy into their network by providing a primary and backup return path(s) from selected scrubbing centers.

F5 OFFERS DENIAL-OF-SERVICE PROTECTION IN THE ARCHITECTURAL AND OPERATIONAL MODEL THAT WORKS BEST FOR YOUR BUSINESS, BASED ON WHERE YOUR APPLICATIONS ARE HOSTED—IN THE CLOUD, ON-PREMISES, OR A MIX OF BOTH—AND WITH THE LEVEL OF HANDS-ON MANAGEMENT YOU PREFER.

Load Balancer Mode

Distributed Cloud DDoS Mitigation services provide Load Balancer (LB) Mode for customers who do not have a publicly advertisable routing subnet [Class C - CIDR /24 or more specific prefix]. Customers must deploy F5 Distributed Cloud application Load Balancers to take advantage of this mode of deployment. Load Balancer Mode customers can utilize Authoritative DNS resolution to route traffic to the scrubbing centers for inspection and mitigation. Routed mode includes ten Load Balancers, however, customers may purchase LBs in a standalone configuration, independently of Routed Mode deployments.

PLATFORM

F5 Distributed Cloud DDoS Mitigation managed service employs a global Software Defined Network (SDN) that is architected for maximum resiliency, high configurability and rapid scalability. The network includes 24 Regional Edges (REs) in 22 Metro Regions and has 13Tbps capacity available for attack mitigation. Regional Edge locations can be found here.

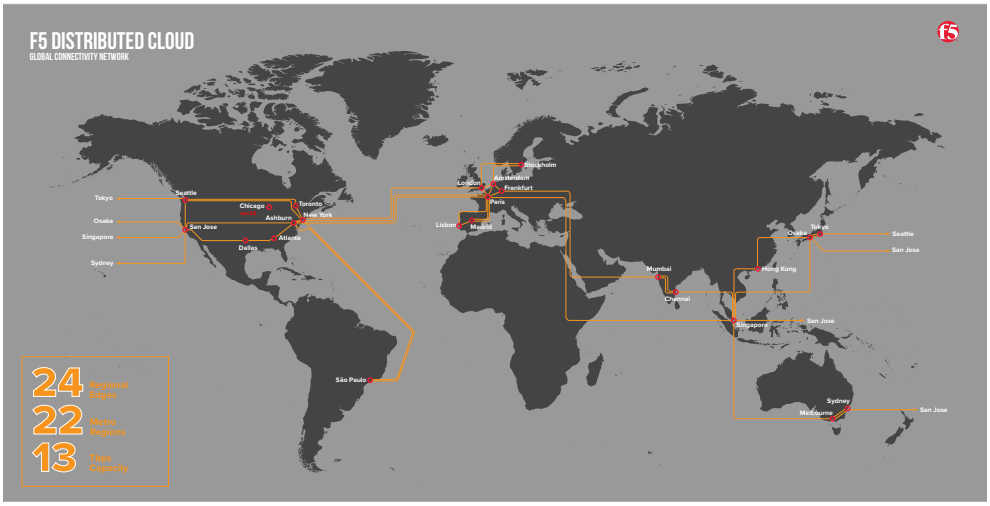
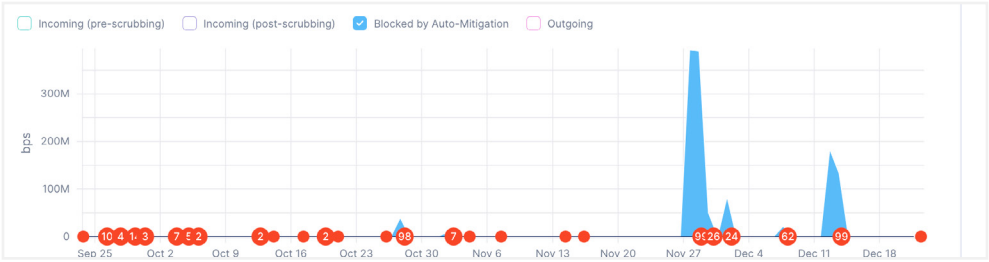


Figure 1: F5 Distributed Cloud Network

AUTO MITIGATION AT EDGE

The platform offers immediate mitigation through our auto-mitigation edge protection. This architectural enhancement sits at the edge of our network and the underlying strength of this solution stems from its incredibly fast Time To Mitigate (TTM) the most common attack vectors. DDoS attacks can be particularly damaging due to extremely high Bandwidth/Packets Per Second attack volume that can last only a few minutes. These attacks can be potentially devastating to an unprotected entity. The AI/ML telemetry associated with this enhancement has the ability to block malicious attack traffic at an incredibly fast and effective rate.

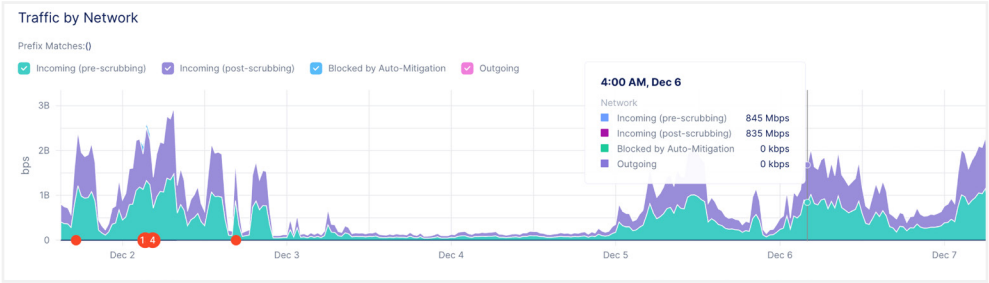
Figure 2: Automatic Edge Mitigation

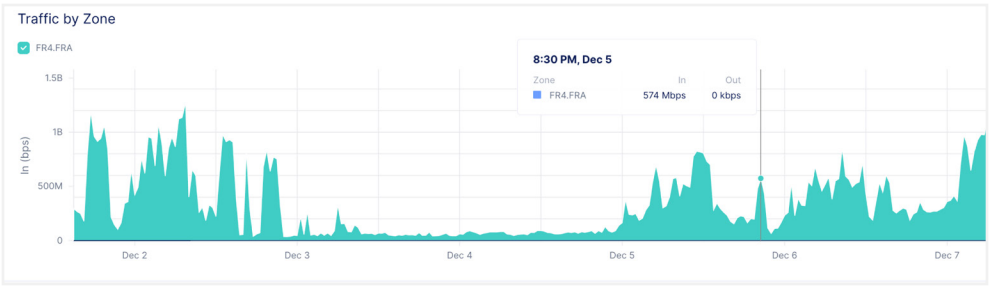


VISIBILITY

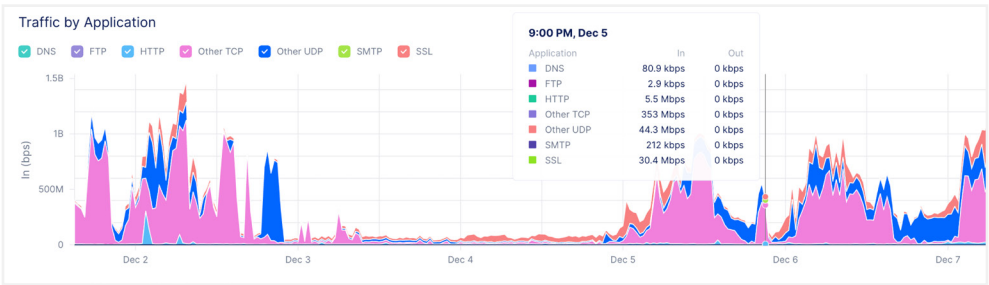
F5 Distributed Cloud DDoS Mitigation includes access to the management console for configuration and visibility. The console provides detailed real-time information on DDoS attack activity.

Figure 3: System Management Console Traffic and Mitigation





F5 APPLICATION SERVICES ARE AVAILABLE IN UTILITY, PERPETUAL, SUBSCRIPTION, AND ENTERPRISE LICENSE AGREEMENTS.



- Type and size of the attack
- Attack origin
- Mitigation techniques
- Countermeasures applied to suppress the attack

KEY FEATURES

Multi-layered global DDoS protection
DDoS mitigation tools and technology are distributed across the F5 Distributed Cloud global network edges to provide protection against large volumetric attacks. Mitigation countermeasures at edge prevent L3/L4 protocol threats and advanced L7 application DoS attacks.

High-capacity defense
The F5 Distributed Cloud secure global network and scrubbing infrastructure spans 23 network edges globally, designed to handle the largest, most complex DDoS attacks with more than 13 Tbps of capacity.

Flexible, scalable service options
F5 has the capacity to mitigate attacks of varying sizes and has service selections to deliver solutions that are custom-built specifically for the protection of a customer network and application configuration. The service provides BGP or Load Balancer routing with on-demand or always-on service options.

Centralized observability and management
The F5 Distributed Cloud console provides actionable information on DDoS attack activity within a single-pane-of-glass management interface.

Expert management and mitigation
Enjoy continuous attack monitoring/mitigation and leverage our team of industry leading SOC engineers to obtain the highest level of protection and uptime for all your applications.

- Protocols being used to attack
- IP address range and ports being attacked
- Inbound attack traffic and Outbound clean traffic to customer network
- Daily DDoS attack reports

The console also provides information on DDoS attack patterns for a specific time period and customizable DDoS dashboards that showcase relevant information based on user persona. Periodic reporting is also available on-demand.

NETOPS/DEVOPS/SOCOPS INTEGRATION API

F5 Distributed Cloud platform is an API-first SaaS offering all system functionality is exposed via REST APIs and documented in the API Dev portal. Extensibility of system functionality via the API is currently in development. The API calls will be able to enable/disable route announcements, define new prefixes, build tunnels, obtain additional reporting metrics and other functions.

SYSTEM STATUS

Real-time system status of F5 Distributed Cloud services is available on an externally hosted portal. F5 Distributed Cloud provides at least fifteen calendar days' notice to customers for routine maintenance work. However, F5 reserves the right to perform emergency maintenance at any time. Emergency maintenance notices are made available to customers prior to any maintenance work performed. Current and historical maintenance notices are available for viewing on the customer portal and at F5 Distributed Cloud Status. Customers can subscribe to status updates to receive real-time notifications in their communication method of choice.

MITIGATION WORKFLOW

DDoS analysts will continually monitor customer prefixes through a variety of toolsets. Upon detection of malicious activity:

1. SOC engineers will be notified of an impending condition that may be classifed as an attack (alerts/events/baselines/thresholds from toolsets) by our mitigation gear.
2. Several SOC analysts will initate steps to take the appropriate mitigative action.
3. The primary SOC engineer will begin constructing the mitigation parameters based on the observed vectors, being as granular and specific as possible with the countermeasures while ensuring the route through our scrubbing centers is following best path with no route leaks.

4. The secondary SOC team, will reference and follow the Real Time Incident Procedures (RTIP) outlined in the console tenant by the customer. These procedures may include, initiating calls to customer SOC/NOC/DevOps/NetOps managers and generating an escalation incident to send to the customer team for on-going resolution tracking purposes.
5. Once the attack activity has been mitigated, customers may request a Post Incident Report from the SOC team.

CUSTOMER SUCCESS

F5 Distributed Cloud DDoS Mitigation service includes a named Customer Success Manager (CSM) assigned to the customer account for the duration of the subscription period. The CSM will work with our customer during the onboarding process to ensure all tasks are completed successfully. After onboarding is completed, the CSM will continue to engage to establish a preferred schedule of recurring checkpoints (usually quarterly or bi-annually) to review customer configurations, system utilization, industry trends, new features and enhancements to the service and provide assistance to plan for future growth and acquisition of additional services.

F5 PROVIDES DDOS MITIGATION SERVICES THAT PROTECT AGAINST LARGE-SCALE VOLUMETRIC DDOS AND TARGETED APPLICATION DOS IN REAL TIME—DEFENDING YOUR BUSINESS FROM BLENDED, SOPHISTICATED, MULTI-VECTOR ATTACKS.

ADDITIONAL SERVICES

F5 Distributed Cloud DDoS Mitigation provides additional, complementary services customers can leverage to increase protection and threat mitigation.

Threat Intelligence

Threat Intelligence is an add-on service for Always On and Always Available customers. Customers must deploy application proxies to take advantage of this service. Threat Intelligence leverages IP reputation to block traffic and uses a continously updated, list of known bad IP addresses. Customers may select sub-categories of identified malicious actors and block their activity so that it never reaches their origin network and applications.

Router Monitoring

Router Netflow or Sflow Monitoring is an add-on service for Always Available customers. The Router Monitoring service utilizes traffic samples from a customers' edge routers to detect potential activity associated with volumetric L3/L4/L7 DDoS attacks. The F5 SOC will continuously analyze the data and will alert customers when a DDoS attack is detected. The SOC will work with customers to define the internal policy for responding to an attack and either automatically or at a customer's request, redirect customer traffic to scrubbing centers for mitigation.

Service Delivery Responsibilities

Task	Customer	F5 Distributed Cloud SOC
Clean Traffic Delivery Configuration	Customers work with the SOC on GRE tunnels/Private Links.	SOC engineer provisions GRE tunnels/Private Links.
Load Balancer Configuration	Customers may deploy or work with the SOC engineers to provision Load Balancers using the Customer Console.	SOC engineer will assist customer to provision Load Balancers upon request.
Router Monitoring Configuration	Customers provide their edge routers' flow configuration information.	SOC engineer configures the service to receive Flow information from customer routers.
Edge Mitigation Rule Configuration	Customer works with the SOC to define edge mitigation rules.	SOC engineer constructs and configures rules.
Threat Intelligence Configuration	Customer works with the SOC to configure Threat Intel rules.	SOC engineer constructs Threat Intel profile.
DDoS Attack Detection	Automatically deployed and implementd by SOC engineering team. View "Migration Workflow" for steps related to SOC mitigation execution.	SOC engineers review the traffic anomalies, confirm attacks and apply countermeasures to mitigate attacks not identified by edge mitigation.
Traffic Route in the F5 Distributed Cloud	Customers route traffic through F5 Distributed Cloud platform via BGP for Routed Mode or DNS resolution for Proxy Mode.	SOC assistance provided as needed.
Mitigation of volumetric DDoS attacks at L3-L4-L7 protocols	No action required from Customer. Customers may collaborate with the SOC during attacks for concurrent countermeasures or traffic shaping.	The SOC engineers deploy appropriate mitigations based on the attack type.
DDoS Protection for L7 Protocols	Customers will work with the SOC to define threshold values for L7 attack vectors.	SOC engineer provides recommendations for threshold and mitigation configurations upon request.

Service Level Agreement	Service Level Description	Remedy
99.99% Uptime	99.99% Availability of Distributed Cloud DDoS Protection Service to mitigate attacks.	Based on duration of Service Outage, Customer is entitled to the Service Credits defined in the table below: Service Outage Duration — Service Credit > 60 consecutive seconds — 2 Days > 60 consecutive minutes — 5 Days > 24 consecutive hours — 10 Days
Time to Notify (TTN) – 15 minutes	Maximum time allowed for F5 to notify Customer they are experiencing an attack incident.	Customer is entitled to 1 day service credit per violation.
Time to Mitigate (TTM) – 15 minutes	Maximum time allowed for F5 to begin DDoS attack mitigation. (Edge mitigation is automatic in it occurs in seconds).	Customer is entitled to 1 day service credit per violation.
Support Escalation	Attack incidents will be escalated to Tier-2 and to Tier-3 Support within 15 minutes.	Customer is entitled to 1 day service credit per violation.

DC 0323 | GUIDE-CLOUD-1076137789