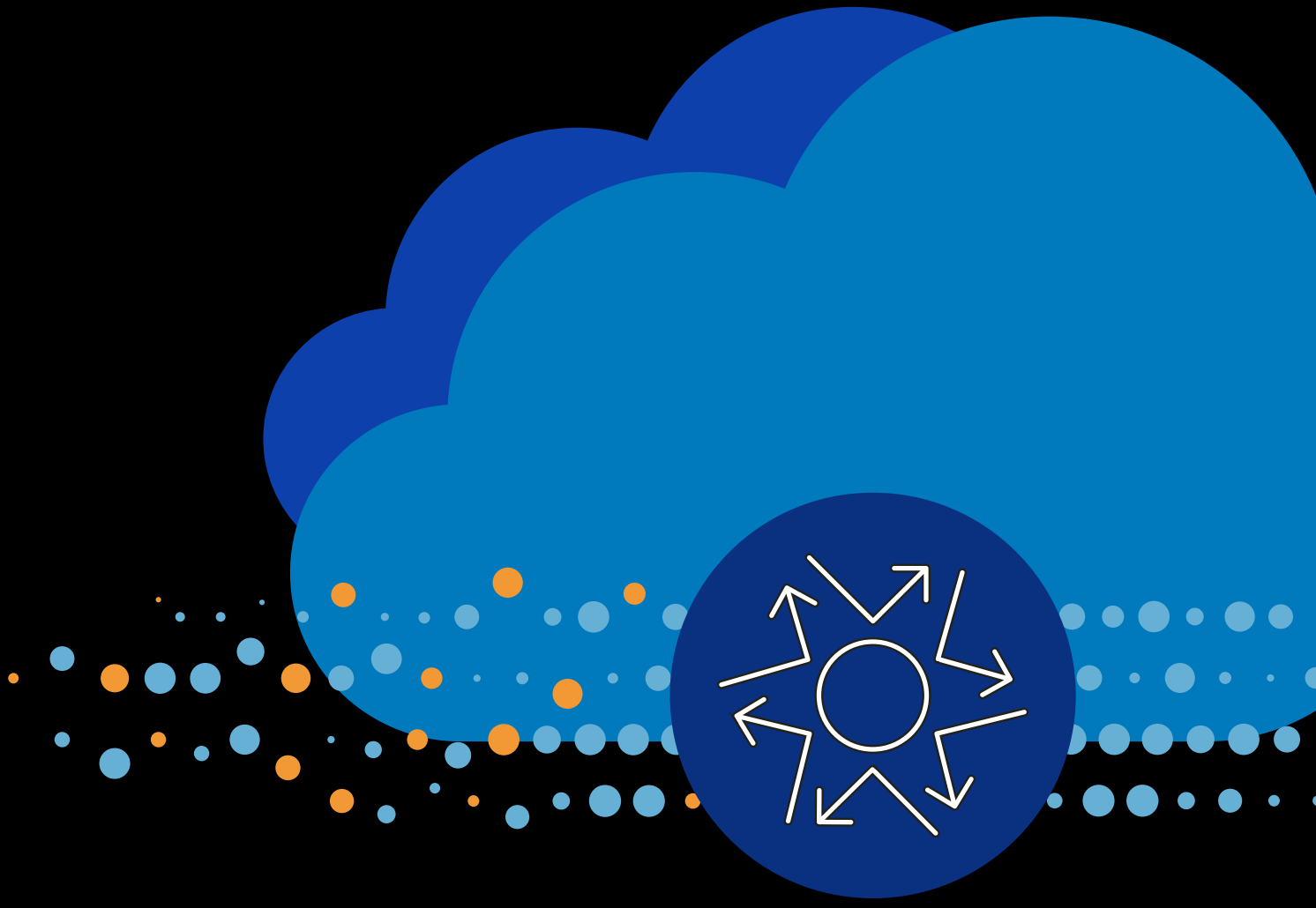
SOLUTION OVERVIEW

F5 Distributed Cloud DDoS Mitigation

F5 Distributed Cloud DDoS Mitigation is a managed, SaaS-delivered service that detects and mitigates large-scale, volumetric network and application-targeted attacks in real-time.



Key benefits

Prevent business disruptions
Stop DDoS attacks before they reach the enterprise network using real-time DDoS attack detection and mitigation in the cloud.

Secure all DDoS attack vectors
Rapidly respond to and mitigate DDoS attacks with multi-layered L3, L4, and L7 protection for all vectors.

Gain attack mitigation insights
Use the F5 Distributed Cloud Services Console for transparent attack mitigation visibility and reporting before, during, and after an attack.

Scale protection
Protect your business from the largest DDoS attacks with industry-leading capabilities featuring multi-terabit mitigation capacity.

Simplify operations
Work with F5 SOC engineers that support you every step of the way and are available 24x7 to respond to attacks and maintain uptime.

Managed defense against large-scale 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 infrastructure and applications.

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

Stay ahead of today's volumetric threats

F5 Distributed Cloud DDoS Mitigation offers protection against a wide variety of DDoS attacks, targeted at Layers 3, 4, and 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
- Resource exhaustion attacks
- Application attacks
- Flash crowd attacks
- SSL/TLS attacks
- NXDOMAIN attacks

F5 Distributed Cloud DDoS 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 a customer's 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. For F5 Distributed Cloud Mitigation customers, F5 SOC DDoS engineers will perform additional in-depth analysis of the traffic and apply countermeasures to mitigate attack vectors not addressed by the automatic edge mitigation. The service delivers full visibility, reporting, and intelligence services to block known malicious threats.

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

Key features

Multi-layered global DDoS protection
DDoS mitigation tools and technology are distributed across the F5 global network to provide protection against large volumetric, application, and multi-vector attacks.

High-capacity defense
The F5 Global Network and scrubbing infrastructure spans 39 network points of presence globally, and is designed to handle the largest, most complex DDoS attacks.

Flexible, scalable service options
F5 has the capacity to mitigate attacks from hundreds of gigabits to multi-terabits per second, with BGP or proxy-based routing and on-demand or always-on service options.

Centralized observability and management
The F5 Distributed Cloud console provides actionable information on DDoS attack activity across all vectors, including active countermeasures with timestamps, plus detection and mitigation timelines.

Expert management and mitigation
Continuous attack monitoring/ mitigation, backed by F5's team of industry leading SOC engineers, delivers the highest level of protection and uptime for critical infrastructure and applications.

Distributed Cloud DDoS mitigation components

Service models

Distributed Cloud DDoS Mitigation service is delivered in two distinct service models; Always On where customer traffic is continuously routed through the F5 network or Always Available where the F5 SOC or customers activate route changes to the F5 network prior to or while under a DDoS attack.

Customers may obtain 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 FQDNs (Fully Qualified Domain Names) to be protected and/ or number of data centers and routers to be protected, peak amount of clean bandwidth consumed in bytes per second measured to the 95th percentile, edge routers to be monitored for netflow/sflow data, and mode of operation (Always On or Always Available).

Deployment modes

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 F5 SOC engineers.

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

Proxy Mode

Distributed Cloud DDoS Mitigation provides a proxy mode option for customers who do not have a publicly advertisable routing subnet (Class C - CIDR /24 or more specific prefix). Customers would deploy Distributed Cloud Services application load balancers to take advantage of this deployment option. Proxy mode customers would utilize authoritative DNS resolution to route traffic to the F5 global network and its scrubbing centers for inspection and mitigation.

Platform

Distributed Cloud DDoS Mitigation employs a global software-defined network (SDN) that is architected for maximum resiliency, high configurability, and rapid scalability. The network includes 39 REs across 30 metro regions and has 17Tbps capacity available for attack mitigation. RE locations can be found in the F5 global network map below.

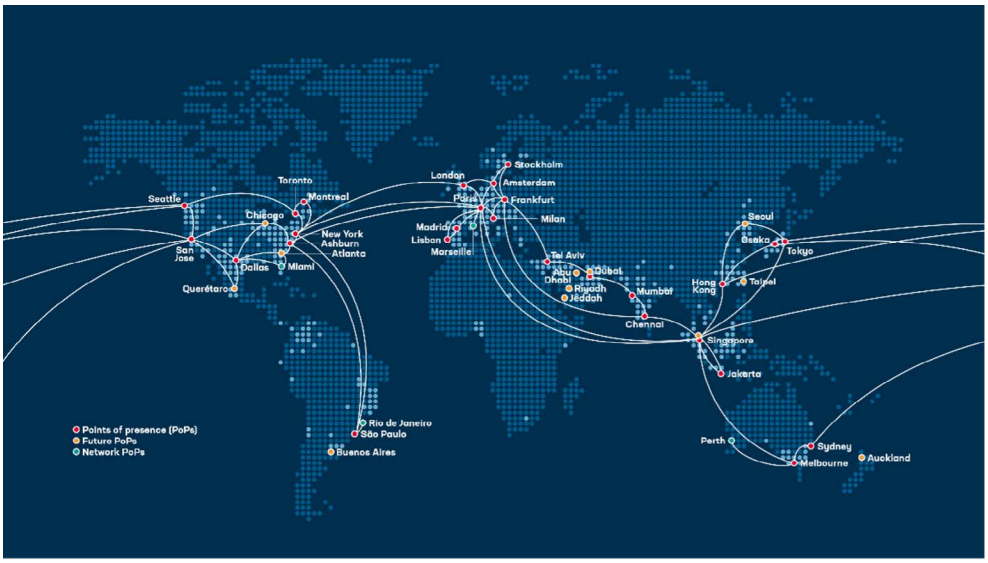


Figure 1: The F5 global network, which serves as the backbone for DDoS protection and mitigation.

Automatic mitigation at the edge

The platform offers immediate mitigation through F5 auto-mitigation edge protection. This function sits at the edge of the F5 network and delivers a rapid time to mitigate (TTM) across the most common attack vectors. DDoS attacks can be particularly damaging due to extremely high bandwidth/packets per second attack volume. These attacks can be potentially devastating to an unprotected entity. F5 AI/ML telemetry can block malicious attack traffic quickly and effectively.

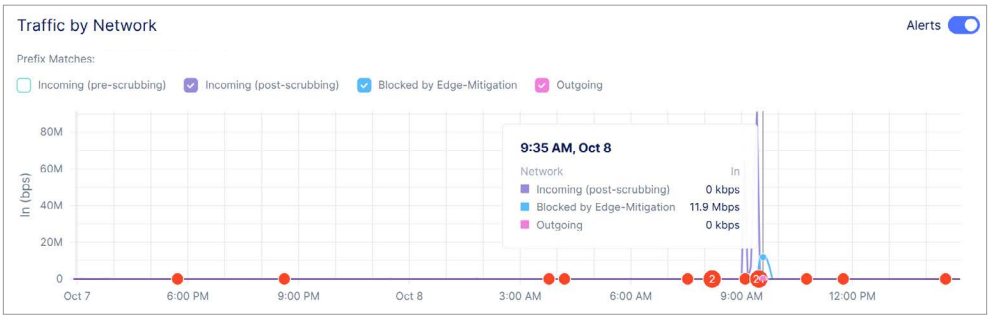


Figure 2: Automatic edge mitigation insights.

Visibility

Distributed Cloud DDoS Mitigation includes access to the management console for initial set up, ongoing management of service components, and continued visibility into attacks and countermeasures. The console provides organizations with detailed real-time information on DDoS attack activity including a timeline of activity and mitigation steps (e.g. countermeasures implemented) for each attack campaign. Other available insights include:

- Type and size of attack
- Attack origin details
- Protocols being used to attack
- IP address range(s) and ports being attacked
- Mitigation techniques and countermeasures applied
- Inbound attack traffic and outbound clean traffic returned to customer network(s)
- Daily DDoS attack report(s)

The console also provides information on DDoS attack patterns across any specific time period and customizable DDoS dashboards that showcase relevant information based on user persona. Periodic reporting is also available on demand via requests to the F5 SOC.

Figure 3: System management console and mitigation insights.

NetOps, DevOps and SecOps integration via API

F5 Distributed Cloud platform is an API-first SaaS offering that exposes all system functionality via REST APIs, with documentation offered in the API Dev Portal. Extensibility of system functionality via the API is available, allowing customers to leverage API calls and automation to enable/disable route announcements, define new prefixes, build tunnels, obtain additional reporting metrics, and carry out other functions.

System status

F5 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 Cloud Status. Customers can subscribe to status updates to receive real-time notifications in their communication method of choice.

Mitigation workflow

F5 SOC engineers will continually monitor customer prefixes through a variety of tool sets. Upon detection of malicious activity:

1. SOC engineers will be notified of an impending condition that may be classified as an attack (alerts/events/baselines/thresholds from toolsets) by F5 mitigation capabilities.
2. Several SOC analysts will initiate steps to take the appropriate mitigation action(s).
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 F5 scrubbing centers is following an optimal path with no route leaks.
4. The 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 contacts as well as generating an escalation incident to send to the customers team(s) 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

Distributed Cloud DDoS Mitigation includes a named Customer Success Manager (CSM) assigned to the customer account for the duration of the subscription period. The CSMs work with customers during the onboarding process to ensure all tasks are completed successfully. After onboarding is completed, CSMs will 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. They will also assist in planning for future growth and acquisition of additional services.

Additional services

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

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.

Threat intelligence

Threat intelligence is an add-on service for proxy mode customers only. Threat intelligence leverages IP reputation to block traffic and uses a continuously updated list of known bad IP addresses, maintained by F5. Customers may select sub-categories of identified malicious actors and block their activity so that it never reaches their origin network and applications.

Service delivery responsibilities

Task	Customer	F5 SOC
Traffic routing to the F5 Global Network for mitigation	Customers route traffic through the F5 network via BGP for Routed Mode or DNS resolution for Proxy Mode.	SOC assistance provided as needed.
Clean traffic delivery configuration	Customers work with the SOC on GRE tunnels/F5 Distributed Cloud Private Links.	SOC engineer(s) provision GRE tunnels/ Distributed Cloud Private Links
Load balancer (proxy) configuration	Customers may deploy or work with the SOC engineers to provision load balancers (proxies) using the customer console.	SOC engineer(s) will assist customers to provision load balancers (proxies) upon request.
Router monitoring configuration	Customers provide their edge routers' Flow or Netflow (v5, v9) plus SNMP configuration information.	SOC engineer(s) configure 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(s) construct and configure rules.
Threat intelligence configuration	Customer works with the SOC to configure threat intelligence rules.	SOC engineer(s) construct threat intelligence profile.
DDoS attack detection	Automatically deployed and implemented by the SOC engineering team. See mitigation workflow for steps related to SOC mitigation execution.	SOC engineer(s) review traffic/application anomalies, confirm attacks and apply countermeasures to mitigate attacks not identified by edge mitigation.
Mitigation of volumetric DDoS attacks at L3, L4, and L7	No action required from customer. Customers may collaborate with the SOC during attacks for concurrent countermeasures or traffic shaping.	SOC engineer(s) 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(s) provide recommendations for threshold and mitigation configurations upon request.

Service delivery responsibilities

Service level agreement (SLA)	Service level description	Remedy
99.99% uptime	99.99% availability of DDoS protection service to mitigate attacks.	Based on duration of service outage, customer is entitled to service credits: • **> 60 consecutive seconds:** 2 day service credit • **> 60 consecutive minutes:** 5 day service credit • **> 24 consecutive hours:** 10 day service credit
15-minute time to notify (TTN)	Maximum time allowed for F5 to notify customer they are experiencing an attack incident.	Customer is entitled to a 1-day service credit per violation.
15-minutes time to mitigate (TTM)	Maximum time allowed for F5 to begin DDoS attack mitigation. Edge mitigation is automatic and occurs in seconds.	Customer is entitled to a 1-day service credit per violation.
Support escalation	Attack incidents will be escalated to Tier 2 and Tier 3 support within 15 minutes.	Customer is entitled to a 1-day service credit per violation.

Next steps

Explore more technical details and documentation about the service.

View Distributed Cloud DDoS Mitigation documentation.