



# F5 Distributed Cloud Services Base Package

## What's Inside

- 2 Web Application Firewall
- 3 Web App Scanning
- 3 DDoS Mitigation
- 3 API Security
- 3 Bot Defense
- 3 Client-Side Defense
- 3 App Connect
- 4 Network Connect
- 4 DNS
- 4 DNS Load Balancer
- 5 Observability
- 5 Support
- 6 Other

## Essential application security for your website or publicly accessible applications

The F5® Distributed Cloud Services Base Package is a set of features offered on the F5 Distributed Cloud platform. This package includes a basic deployment architecture and equips customers with the essential tools required to secure applications with F5 Distributed Cloud Web App and API Protection (WAAP). It follows a traditional SaaS model, leveraging a proxy to manage the flow of application and API traffic between clients on the internet and the F5 Global Network Regional Edges (RE). By enforcing security services and policies at these locations, attacks can be intercepted before they threaten your broader network. This proactive approach minimizes the impact of malicious application and API traffic before it reaches the customer's infrastructure, resulting in a more secure environment, improved overall performance, and cost savings on infrastructure and bandwidth.

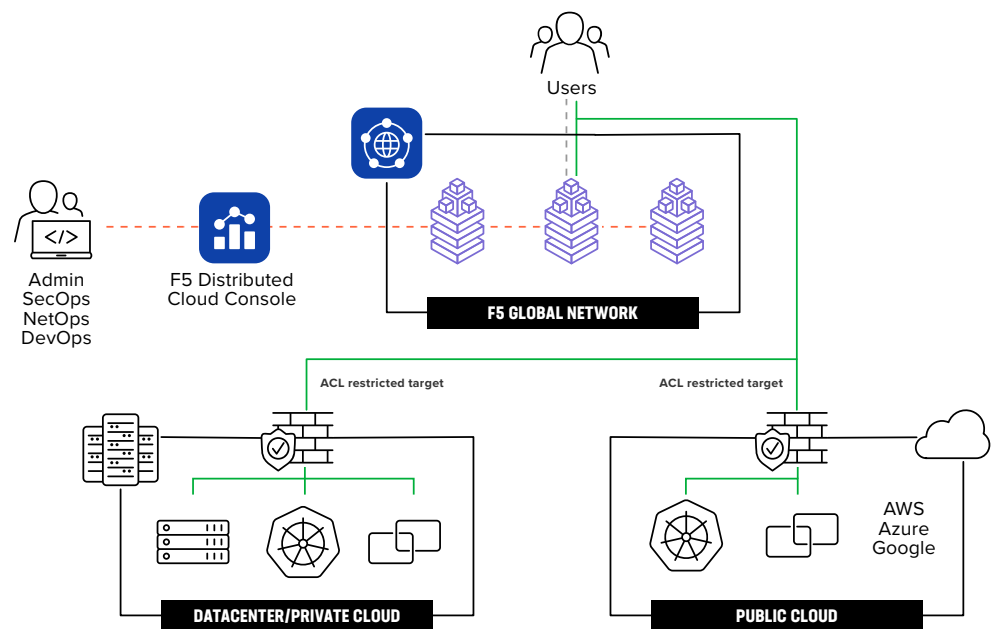


Figure 1: Clients connect to the nearest F5 Global Network RE; traffic is targeted to be a determined load balancer configuration, and security services are applied.



## BASE PACKAGE

Web Application Firewall	
Globally-distributed load balancer with WAF	Unlimited number of endpoints (i.e., origin servers). Unlimited number of endpoint locations for health checks. The granularity of health checks for endpoints is one second. This includes one load balancer.
Signature-based protection	Mitigate application and API vulnerabilities with F5's core WAF technology, backed by our advanced signature engine containing over 8,000 signatures for CVEs, plus other known vulnerabilities and techniques including bot signatures.
Threat campaigns	Delivers protection against sophisticated, multi-vector attack campaigns via fully vetted attack campaign signatures developed by F5 threat researchers.
Compliance enforcement	Combination of violations, evasions, and HTTP protocol compliance checks.
Automatic attack signature tuning	Self-learning probabilistic model that suppresses false-positive triggers.
Mask sensitive parameters or data in logs	Users can mask sensitive data in request logs by specifying HTTP header names, cookie names, or query parameter names. Only values are masked. By default, values of query parameters card, pass, .pwd files, and password are masked.
Custom blocking pages and response codes	When a request or response is blocked by the WAF, users can customize the blocking response page served to the client.
Allowed responses codes from origin	User can specify which HTTP response status codes are allowed.
IP reputation	Analyzes IP threats and publishes a dynamic dataset of millions of high-risk IP addresses maintained by F5 to protect app endpoints from inbound traffic from malicious IPs. IP threat categories include Spam Sources, Windows Exploits, Web Attacks, Botnets, Scanners Denial of Services, Phishing, and more.
Sensitive data protection for apps	Data Guard prevents HTTP and HTTPS responses from exposing sensitive information, like credit card numbers and social security numbers, by masking the data.
Exclusion rules	Rules that define the signature IDs and violations or attack types that should be excluded from WAF processing based on specific match criteria. The specific match criteria include domain, path, and method. If the client request matches all these criteria, then the WAF will exclude processing for the items configured in the detection control.
CSRF protection	Allows users to easily configure or specify the appropriate, allowed source domains.
Cookie protection	Cookie protection provides the ability to modify response cookies by adding SameSite, Secure, and HTTP Only attributes.
GraphQL protection	The WAF engine inspects GraphQL requests for vulnerabilities and will block traffic based on the F5 signature database.

<b>Web App Scanning</b>	
Web App Scanning (WAS)	Dynamically and continuously scan your external attack surface to un-cover exposed web apps and APIs. Find and report vulnerabilities with automated penetration testing. (3 web apps included)
<b>DDoS Mitigation</b>	
Fast ACLs	Network firewall controls allow users to block ingress traffic from specific sources or apply rate limits to network traffic from a specific source. Enhanced protections allow for filtering traffic based on source address, source port, destination address, destination port, and protocol. This includes 100 IP prefixes included and policing capabilities.
Layer 3–4 DDoS mitigation	Multi-layered, volumetric attack mitigation. This includes a combination of pre-set mitigation rules with auto-mitigation and advanced distributed denial-of-service (DDoS) mitigation scrubbing for customers consuming F5 Distributed Cloud Services only. The platform protects customer-provisioned services on the F5 network from DDoS attacks.
Layer 7 DoS detection and mitigation	Anomaly detection and alerting on abnormal traffic patterns and trends across apps and API endpoints. F5 leverages advanced machine learning to detect spikes, drops, and other changes in app and API behavior over time by analyzing request rates, error rates, latency, and throughput with the ability to deny or rate limit endpoints including auto-mitigation.
Layer 7 DoS policy-based challenges	Custom policy-based challenges can be set up to execute JavaScript or Captcha challenges. Define match criteria and rules for triggering challenges based on source IP and reputation, ASNs, or labels (e.g., cities, countries). This helps filter out attackers trying to execute an attack from legitimate clients. Includes 200 service policy rules.
Slow DDoS mitigation	"Slow and low" attacks tie up server resources, leaving none available for servicing requests from actual users. This feature allows for the configuration and enforcement of request timeout and request header timeout values.
<b>API Security</b>	
Discovery	API endpoint discovery, PII detection, Authenticated API detection. Supported for 1 application.
Protection	Schema upload, API Protection Rules, Rate limiting. Up to 500k requests per month.
Signature based protection	Supports inspection of the popular API protocols like JSON.
<b>Bot Defense</b>	
Signature-based protection	The WAF signature engine includes unique signatures for automated threats and bot techniques, including crawlers, DDoS attacks, DoS attacks, and more.
<b>Client-Side Defense</b>	
Client-Side Defense	Provides multi-phase protection for web applications against Formjacking, Magecart, digital skimming, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation, with 1 million transactions included.
<b>App Connect</b>	
End-to-end-encryption	Native TLS encryption for all data transit across networks.

<b>Network Connect</b>	
Multicloud transit	Layer 3 network transit between public clouds, on-premises datacenters, and distributed edge sites.
Security service insertion	Integrate external network firewall services, such as F5 BIG-IP and Palo Alto Networks, across multiple cloud networks.
Network segmentation	Granular network isolation and micro segmentation to secure network segments on premises and across public cloud networks.
End-to-end-encryption	Native Transport Layer Security (TLS) encryption for all data transit across networks.
Automated provisioning	Automated provisioning and orchestration of public cloud network constructs.
Traffic	To the Internet or customer network.

## **DNS**

### **250 primary and/or secondary zones included**

Automatic failover	Ensure high availability of DNS environments with seamless failover to F5 Distributed Cloud DNS service.
Auto-scaling	Automatically scale to keep up with demand as the number of applications increases, traffic patterns change, and request volumes grow.
DDoS Protection	Prevent DDoS attacks or manipulation of domain responses with built-in protection.
DNSSEC	DNS extension that guarantees authenticity of DNS responses, including zone transfers. It also returns Denial of Existence responses that protect your network against DNS protocol and DNS server attacks.
TSIG authentication	Automate services with declarative APIs and an intuitive GUI.
API support	Transaction signature (TSIG) keys that authenticate communications about zone transfers between client and server.

## **DNS Load Balancer**

### **50 included**

Global location-based routing	Direct clients to the nearest application instance with geolocation-based load balancing for the best user experience.
Intelligent load balancing	Directs application traffic across environments, performs health checks, and automates responses. Includes fully automated disaster recovery.
API support	Automate services with declarative APIs and an intuitive GUI.
ADC telemetry	Track performance, app health, and usage with basic visualization.
Multi-faceted security	Dynamic security includes automatic failover, built-in DDoS protection, DNSSEC, and TSIG authentication.
Health checks	Health checks to origin servers provides responses based on application availability. Includes 200 health checks.

<b>Observability</b>	
Reporting, rich analytics, and telemetry	Unified visibility from application to infrastructure provided across heterogeneous edge and cloud deployments, including granular status of application deployments, infrastructure health, security, availability, and performance.
Security incidents	Events view that groups thousands of individual events into related security incidents based on context and common characteristics. Aimed at making investigation of app security events easier.
Security events	Single dashboard view that consolidates all security events across the full breadth of web application and API security functionality with customization and drill-down into all WAF, bot, API, and other layer 7 security events.
Global Log Receiver: Log export integration	Log distribution to external log collection systems including Amazon S3, Datadog, Splunk, SumoLogic, and more. This feature includes two configurations.
Synthetic monitoring	Easily monitor your critical applications and systems from regions around the world. Quickly correlate performance and availability issues to a specific region or location. Leverage built-in TLS reports to quantify risk of certificate expiry, assess the use of vulnerable protocols and ciphers, and determine overall TLS score for your monitored endpoints. Receive relevant alerts before your customers start calling in and clearly identify if they were impacted during the last change window or outage. Includes 500 thousand executions.
Metrics	30 days
Request logs	Seven days
Audit logs	30 days
Alerts and notifications	Policy rules
<b>Support</b>	
24/7/365 support	Support is provided in various methods including console ticketing, email, and phone support.
Uptime SLAs	99.99%
Security logs	30 days
Response SLA	One hour
Onboarding	Customer Success Team and access to training.

Other	
Service policies	Enables micro-segmentation and supports advanced security at the application layer with development of allow/deny lists, Geo IP filtering, and custom rule creation to act on incoming requests, including match and request constraint criteria based on a variety of attributes and parameters such as TLS fingerprint, geo/country, IP prefix, HTTP method, path, headers, and more.
CORS policy	Cross-Origin Resource Sharing (CORS) is useful in any situation where the browser, by default, disallows cross-origin requests, but you have a specific need to enable them. CORS policy is a mechanism that uses additional HTTP headers to inform a browser to allow a web application running at one origin (domain) to have permission to access selected resources from a server at a different origin.
Trusted client IP headers	Identification of real client IP addresses for monitoring, logging, and defining allow/deny policies. When this feature is enabled, security events and request logs will show this real client IP address as the source IP.
Mutual TLS	Support for both TLS and Mutual Transport Layer Security (mTLS) for authentication with policy-based authorization on the load balancer. Proxy provides the capability to enforce end-to-end security of application traffic. Mutual TLS supports the ability to send client certificate details to origin servers in x-forwarded-client-cert request headers.
Administration	Unlimited number of users Single Sign On Role Based Access Control
Global Anycast	One VIP included

**Contact F5** to learn how Distributed Cloud Services can help.

