Hybrid DDoS Defense for the Data Center

F5® DDoS Hybrid Defender™ provides next-generation cloud and on-premises distributed denial-of-service (DDoS) defenses to ensure real-time protections against volumetric DDoS threats; dynamic network and applications attacks; and threats hiding within encrypted traffic.

DDoS attacks remain a significant concern, and are a leading cause of business service outages facing organizations today. Such attacks threaten businesses of all sizes, and are often used as a smoke screen for more sophisticated and dangerous hacks or theft. DDoS attacks have evolved to be multi-layered and complex—it's no longer about just attacking the network: the application layer is directly in the crosshairs. How quickly you discover and stop attacks is critical to keeping your business applications operational.

Key Solution Benefits

Stateful Security, Stateless Scale

F5 DDoS Hybrid Defender delivers the best of both stateful and stateless security. The stateful capabilities help to detect and defend against the broadest range of layer 4-7 attacks including SYN Flood, SSL/TLS protocol attacks, and application low-and-slow attacks. These stateful capabilities are executed with the performance and resiliency of a stateless solution, providing the best of both worlds: intelligent, stateful protection with the dependability and scale of a stateless solution.

Ultra-Resilient Hybrid Design

F5 DDoS Hybrid Defender integrates with the F5 Silverline® DDoS Protection, a high performance cloud-scrubbing service. The hybrid combination delivers unmatched performance and resiliency to defend against the most intensive of attacks. The on-premises appliance serves as the primary defense under normal conditions. When needed, F5 DDoS Hybrid Defender redirects volumetric attack traffic to the Silverline cloud scrubbing centers. Expert F5 Security Operations Center (SOC) engineers analyze the attack and signaling detail, and implement mitigations to scrub network traffic, which prevents saturation of inbound pipes on-premises. Once attack traffic has subsided to normal levels, DDoS Hybrid Defender and Silverline DDoS Protection smoothly transition back to on-premises protection.

WHY F5 DDOS HYBRID DEFENDER?

- Complete coverage in a single offering with combined network and application DDoS defense, SSL/TLS decryption, behavioral analysis, and cloud scrubbing.
- Sub-second attack detection with geo-tracking, intelligent signaling, and hardware assist—inline or in out-of-band mode.
- In-depth and real-time attack visibility for more effective decisions with 3000+ L3–L4 metrics, detailed logging, actionable reports, and intelligence sharing.
- Proactive bot defense that discovers malicious bot activity in advance of attacks.

Operations Speed

F5 DDoS Hybrid Defender helps your SOC staff run with efficiency and intelligence: you won't need a large staff to make a big impact. Self-tuning and automated, the solution deploys easily without the need for managed services. F5 DDoS Hybrid Defender learns optimal performance levels and automatically determines appropriate thresholds. You won't waste staff time on continuous tuning and complicated traffic analysis, providing faster value than other solutions.

The dashboard provides your team with what they need to see, so they won't waste time chasing down false positives. When action is required, your staff can take immediate mitigation actions with just a few clicks. Rapid, real-time updates show the mitigation results so that SOC staff can be assured the threat has been mitigated.

Self-Tuning and Automated Behavioral Defense

In addition to the standard security signatures, the solution creates dynamic signatures automatically—enabling faster and more accurate threat identification and blocking of evasive threats. These include low-and-slow and short, sporadic bursts of traffic that may go undetected. Security policy implementation is not a one-time procedure. F5 DDoS Hybrid Defender discovers and fingerprints new and unusual traffic patterns without human intervention, distinguishing and isolating potential malicious traffic from legitimate traffic almost instantaneously. Mitigation aggressiveness is based on sophisticated analysis of network and application stress. The aggressiveness of automated mitigations is determined using the current health of applications and networks. Real-time status is fed back to the mitigation engine, where mitigation signatures are automatically built, deployed, and analyzed for effectiveness. This reduces false positives and enables a "hands-off" automated protection cycle that continuously tunes and refines the precision of the mitigations as the attack continues or evolves—scaling mitigations up and down as needed.

F5 Security Intelligence

Information from all DDoS attacks discovered and mitigated by on-premises devices and F5 Silverline DDoS Protection can be automatically communicated to F5 SOCs for expert research and global threat analysis. This information, combined with F5's global threat feeds, drives standard signature updates and security enhancements. Collectively, the trend analysis intelligence helps F5 safeguard against future threats.

Deploy Where You Need It Most

F5 DDoS Hybrid Defender eliminates common concerns with deployment, especially where network architectures are more complex. It offers an interface designed for the security professional, and a simplified "out-of-the-box" experience—with automatic sizing and configuration of DDoS protection features. Its flexible deployment options enable DDoS protection services to be easily deployed within the data center as a physical or virtual appliance, directly in the path of traffic or out of band for analysis of traffic behavior.

Price-Performance

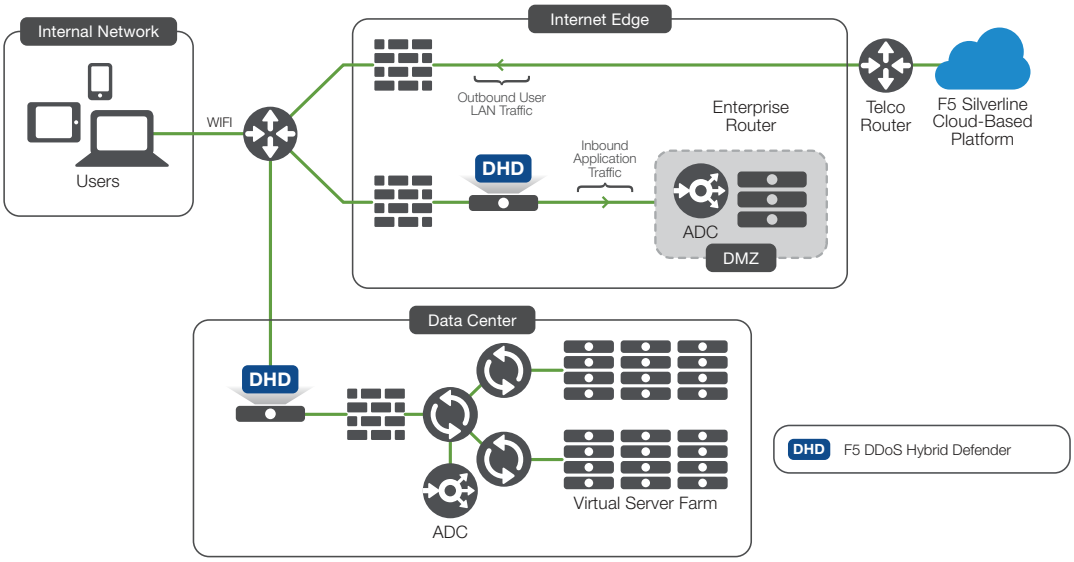
F5 DDoS Hybrid Defender delivers cost-effective security at scale. With a design purpose-built for DoS mitigation and SSL/TLS decryption, the solution provides integrated L3-7 protection. Multiple appliance form factors, a virtual offering, and chassis solution with on-demand scale provides right-sized options for all environments, from mid-sized enterprise applications to service providers. As a hybrid solution, DDoS Hybrid Defender can perform hardware-accelerated mitigation of network and application attacks, while using advanced behavioral analysis and machine learning to identify and fingerprint sophisticated network and application layer attacks. When attacks could overwhelm the data center's bandwidth, DDoS Hybrid Defender automatically redirects traffic to F5 Silverline cloud-scrubbing services where the malicious traffic is blocked and the good traffic is re-routed appropriately.

Specifications

F5 DDoS Hybrid Defender protects the most complex infrastructures, enabling organizations to improve data center and application level security, protect customer data and access, and enhance overall security postures.

DDoS Mitigation:	All layer 3, 4, and 7 DoS/DDoS threats including flood/sweep with Src/Dst IP address awareness, UDP/DNS/HTTP/TCP/SIP/SYN/ ACK/RST/FIN using sub-second detection, network behavior analysis, 120+ DDoS vectors, application anomaly detection, dynamic filtering, protocol analysis, source tracking, control policies, and more.
DDoS Auto-Thresholding:	Automatically generated and adjusted for all DDoS network and application threshold values for TPS, PPS, and requests per second.
Comprehensive Bot Defense:	Proactive bot defense, captcha challenges, headless browser detection, bot categorizations identifying severity and good/bad bots, device fingerprinting.
IP Intelligence:	Bad actor information can be communicated across other DHD devices; F5 IP Intelligence licensed services provide global DDoS threat intelligence feeds.
DDoS Detection:	Out-of-band SPAN port, NetFlow monitoring.
SSL Inspection (Decryption):	Advanced, purpose-built TLS stack. Hardware accelerated: Key exchange and bulk inspection; RC4, DES, 3DES, AES-CBC, AES-GCM, AES-GMAC, RSA, DSA, DH, ECDSA, ECDH, MD5, SHA, SHA2 ciphers. Keys protected by F5 BIG-IP® Secure Vault. FIPS 140-2 Levels 1, 2 and 3 available.
Reporting and Forensics:	Dashboard summary, current attack and drill-down reporting, standard and customizable charts and graphs; blocked/passed traffic; app health, bot signatures; Top 10 threats/destination IPs/source IPs; sys mon; max # of attacks; IPs participating in attack.
Mitigation Techniques:	Rate limiting/blocking, connection limiting, source limiting, shunning/ blacklisting/whitelisting, BGP route injection and RTBH (source and destination), dynamic signature filtering. Volumetric/cloud scrubbing redirection: manual or automated.

Management:	REST; CLI, Web UI; RBAC management
Deployment Modes:	Asymmetric and symmetric flow support. Inline and Out-of-Path: L2 Bridged, L2 Virtual Wire, and L3. Out-of-Band: SPAN/Tap and Netflow. Form Factors: BIG-IP Appliance, Virtual Edition, network functions virtualization, VIPRION chassis.
Event Notifications:	SNMP, Syslog, email
Cloud Signaling:	BGP/BGP Flowspec route injection for manual or automated redirection to licensed F5 Silverline or third-party volumetric scrubbing solutions. REST API route activation with licensed F5 Silverline DDoS Protection cloud-based scrubbing.
High Performance (HA):	Support HA active/passive



DC0318 | OV-SEC 217605008 | 0318