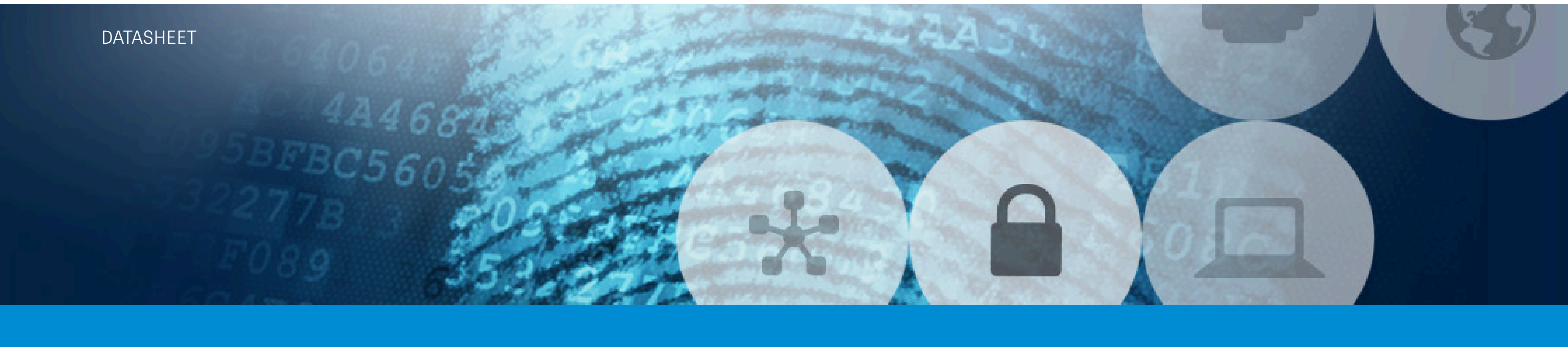
F5® Silverline™
DDoS Protection

DATASHEET



Protect Your Business and Stay Online During a DDoS Attack

What's Inside

DDoS attacks are increasing in scale and complexity, threatening to overwhelm the internal resources of businesses globally. These attacks combine high-volume traffic clogging with stealthy, low-and-slow, application-targeted techniques. To stop DDoS attacks from reaching the enterprise network, organizations need a solution for cloud-based mitigation in addition to on-premises protection.

F5® Silverline™ DDoS Protection is a service delivered via the Silverline cloud-based platform. It detects and mitigates DDoS attacks in real time, with industry-leading DDoS attack mitigation bandwidth to stop even the largest of volumetric DDoS attacks from ever reaching your network. F5 security experts are available 24/7 to keep your business online during a DDoS attack with comprehensive, multi-layered L3–L7 DDoS attack protection.

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, fully automated DDoS attack detection and mitigation in the cloud.

Protect against all DDoS attack vectors
Engineered to respond to the increasing threats, escalating scale, and complexity of DDoS attacks, F5 offers multi-layered L3–L7 DDoS attack protection against all attack vectors.

Gain real-time attack mitigation insights
The AttackView customer portal provides transparent, real-time attack mitigation visibility and reporting before, during, and after an attack.

Defend against volumetric attacks
Protect your business from even the largest of DDoS attacks—over hundreds of gigabits per second.

Get 24/7 access to DDoS experts
The F5 Security Operations Center (SOC) is available 24/7 with security experts ready to respond to DDoS attacks within minutes.

Drive efficiencies with a hybrid DDoS solution
F5 offers comprehensive DDoS protection both on-premises and as a service.

Comprehensive DDoS Protection

The Silverline DDoS Protection service complements F5's on-premises DDoS solution to protect organizations against the full spectrum of modern DDoS attacks. This hybrid DDoS protection solution from F5 combines industry-leading DDoS protection solutions on premises for detecting and mitigating mid-volume, SSL, or application-targeted attacks—with the high-capacity Silverline DDoS Protection service to stop the volumetric attacks before they ever reach your network.

F5 is the first leading application services company to offer a hybrid solution for DDoS protection. By implementing Silverline DDoS Protection in addition to the on-premises solution, customers can keep their businesses online when under DDoS attack with a reduced risk of downtime, real-time DDoS mitigation response times, unparalleled visibility and reporting, and cost efficiencies. The on-premises DDoS Protection solution and Silverline DDoS Protection can be implemented independently of each other, or together as a hybrid solution for the most comprehensive L3–L7 DDoS protection.

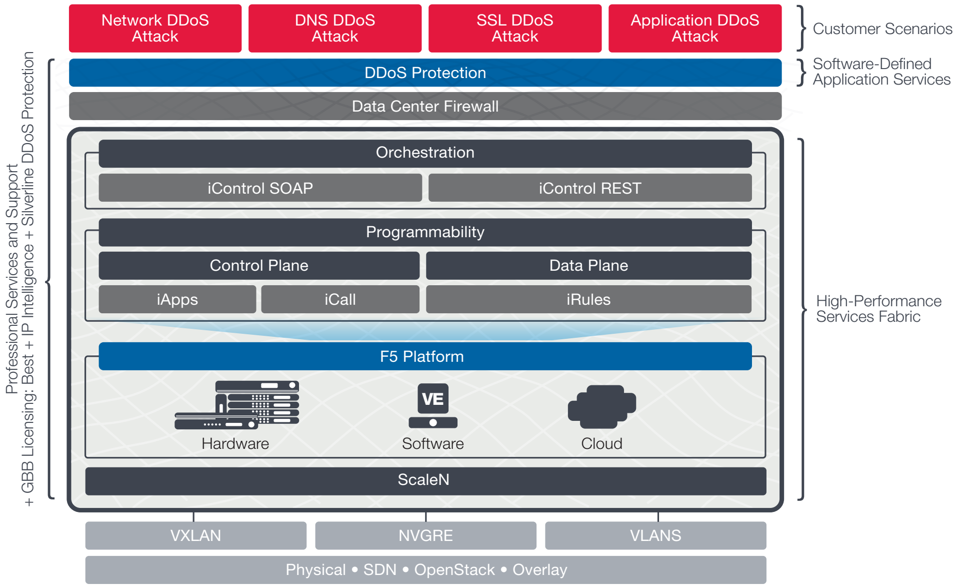


Figure 1: F5 provides a comprehensive DDoS solution with both on-premises protection and cloud-based Silverline DDoS Protection.

Real-Time, Fully Automated Cloud-Scrubbing Technologies

Any organization that delivers content or applications over the Internet can use cloud-based DDoS protection to keep their business online during an attack with minimal impact to users. Engineered to respond to the increasing threats, escalating scale, and complexity of DDoS attacks, Silverline DDoS Protection offers multi-layered L3–L7 protection against all attack vectors. This cloud-based security service utilizes fully automated cloud-scrubbing technologies to detect, identify, and mitigate threats in real time—returning clean traffic back to your site. It can run continuously to monitor all traffic and stop attacks from ever reaching your network, or it can be initiated on demand when your site is under DDoS attack.

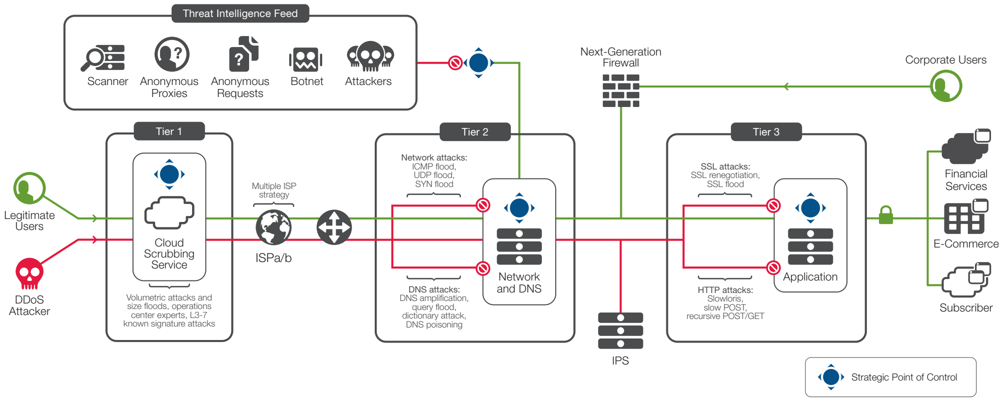

Threat Intelligence Feed
Scanner
Anonymous Proxies
Anonymous Requests
Botnet
Attackers
Next-Generation Firewall
Corporate Users
Tier 1
Cloud Scrubbing Service
Volumetric attacks and size floods, operations center experts, L3-7 known signature attacks
Legitimate Users
DDoS Attacker
Multiple ISP strategy
ISPa/b
Tier 2
Network attacks: ICMP flood, UDP flood, SYN flood
DNS attacks: DNS amplification, query flood, dictionary attack, DNS poisoning
Network and DNS
IPS
Tier 3
SSL attacks: SSL renegotiation, SSL flood
HTTP attacks: Slowloris, slow POST, recursive POST/GET
Application
Financial Services
E-Commerce
Subscriber
Strategic Point of Control

Figure 2: Divert traffic to Silverline DDoS Protection for cloud-scrubbing when your network is under attack, or use it to continuously scrub all traffic to prevent a DDoS attack from ever reaching your network.

As traffic enters the F5 scrubbing center, it is steered and broken down into a “spectrum of suspicion.” F5 then determines the best scrubbing routes for each segment of traffic and automatically directs traffic through the cloud scrubbing centers for real-time mitigation. Traffic continues to be tapped as it traverses the scrubbing center to confirm the malicious traffic has been fully removed. Clean traffic is then returned through your website with little to no impact to the end user.

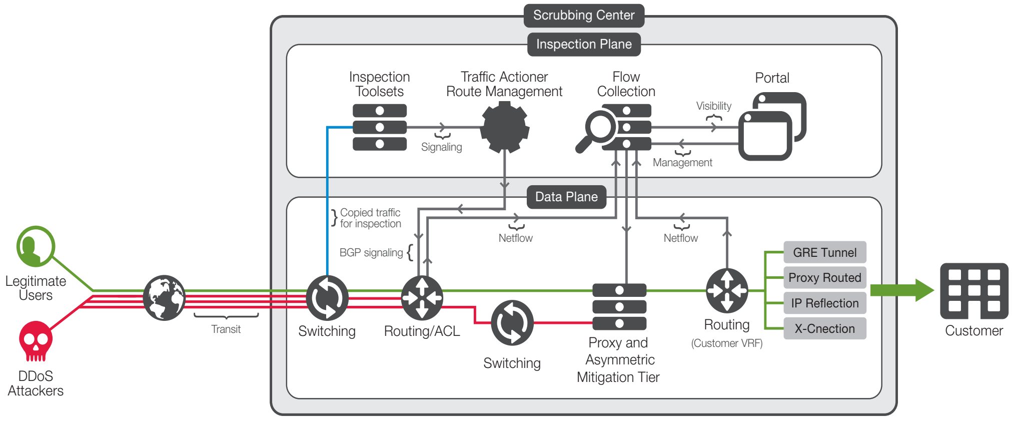


Figure 3: Silverline DDoS Protection multi-layered cloud-scrubbing technologies.

Resilient Attack Mitigation

F5’s fully redundant and globally distributed data centers and scrubbing centers are built with advanced systems and tools engineered to deal with the increasing threats, escalating scale, and complexity of DDoS attacks. Silverline DDoS Protection provides attack mitigation bandwidth capacity of over 2.0 Tbps and scrubbing capacity of over 1.0 Tbps to protect your business from even the largest DDoS attacks. F5 partners directly with a Tier 1 carrier for guaranteed bandwidth that is not shared or based on peering arrangements like other cloud-based services.

Ensure the Best User Experience

The DDoS attack mitigation is invisible to your users, ensuring their experience is uninterrupted during a DDoS attack by always allowing legitimate customer traffic through to your site and eliminating false positive alerts. Unlike other DDoS cloud-scrubbing services that process traffic symmetrically, degrading the user experience with slow page load times or broken links, Silverline DDoS protection may use IP Reflection™ technology (similar to routed mode) for asymmetric processing of only inbound traffic, allowing high-traffic sites to take advantage of protection without affecting the user experience. Only a fraction of the bandwidth is required to process only inbound traffic, ensuring normal delivery of traffic back to your users with the lowest rate of false positives. Based on your needs, clean traffic can also be delivered back to your site through Amazon Web Services Direct Connect, GRE tunnels, proxy, or physical fiber connection.

Deployment Modes

Complete network protection

For enterprises that need to protect their entire network infrastructure, Silverline DDoS Protection leverages Border Gateway Protocol (BGP) to route all the traffic to its scrubbing and protection center, and utilizes a Generic Routing Encapsulation (GRE) tunnel to send the clean traffic back to your network. Routed mode configuration is a scalable design for enterprises with large network deployments. Routed mode configuration does not require any application-specific configuration and provides an easy option to turn the service on or off.

IP Reflection is an alternative asymmetric technique that provides network infrastructure protection without the need for GRE tunnels. Organizations with devices that support destination NAT can leverage IP Reflection. With IP Reflection there is no need to change any IP address, and the IP address space is not affected as it is with GRE.

Simple application protection

For enterprises that require minimum network changes and do not control a full Class C network or prefer to protect only a few applications, Silverline DDoS Protection can be used in proxy mode. Proxy mode supports a wide variety of applications including IPv4, IPv6, SIP, FTP, and many more TCP-, UDP-, and IPsec-based applications. Proxy mode can be set up quickly with simple DNS changes and with little impact to your existing network setup.

Unparalleled Visibility and Reporting Before, During, and After a DDoS Attack

Silverline DDoS Protection includes access to the AttackView portal, which provides everything you need to securely set up and manage SOC services, configure proxy and routing, and receive unparalleled visibility and reporting of attack mitigation in real time. With transparent attack mitigation visibility and reporting, AttackView provides instant details about an attack as it occurs, including the type and size of the attack, IP origin, attack vectors, mitigation process, and yellow-flagged annotations of the Security Operations Center communications.

Attacks can be explored and analyzed, and packet capture reports (PCAPs) are also available for download. With detailed after-action reports available by attack and with longerterm views of attack traffic, AttackView allows you to see the pattern of attacks over time to help you plan for the future.

Complete Attack Protection

Silverline DDoS Protection safeguards against a wide variety of attacks, shown below.

DDoS attack protection	
Protocol anomaly detection	TCP/HTTP/UDP/ICMP/SYN/NTP/GET flood
L3–L4 DDoS protection	SYN flood, TCP flood, ICMP flood, UDP flood, known signature attacks, Teardrop, Smurf, Ping of Death, Mixed Flood, Reflected ICMP
L7 DDoS protection	NTP, HTTP Flood, Slowloris
DNS traffic protection	DNS flood, DNS reflection attacks, DNS amplification attacks

Protected Internet services	
Internet services	HTTP/HTTPS/FTP/SNMP/SMTP/POP-3/CHARGEN/MIME/DNS/IMAP

Flexible Licensing

Silverline DDoS Protection is available as a one- or three-year subscription with flexible options for protected bandwidth and payment terms: Always On,™ Always Available,™ and Ready Defense.™

Always On	Always Available	Ready Defense
Primary protection as the first line of defense The Always On subscription stops bad traffic from ever reaching your network by continuously processing all traffic through the cloud-scrubbing service and returning only legitimate traffic to your site.	**Primary protection available on demand** The Always Available subscription runs on standby and can be initiated when under attack.	**Secondary protection for additional capacity** The Ready Defense subscription runs on standby and can be initiated as a secondary line of defense when you're under attack, in addition to a primary DDoS mitigation solution.

F5 Global Services

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and reliable. For more information about F5 Global Services, contact consulting@f5.com or visit f5.com/services.

DevCentral

The F5 DevCentral™ user community of more than 170,000 members is your source for the best technical documentation, discussion forums, blogs, media, and more related to Application Delivery Networking.

More Information

To learn more about Silverline DDoS Protection, visit f5.com to find these and other resources:

Web pages

DDoS Protection

F5 Silverline DDoS Protection

Under Attack? We can Help.