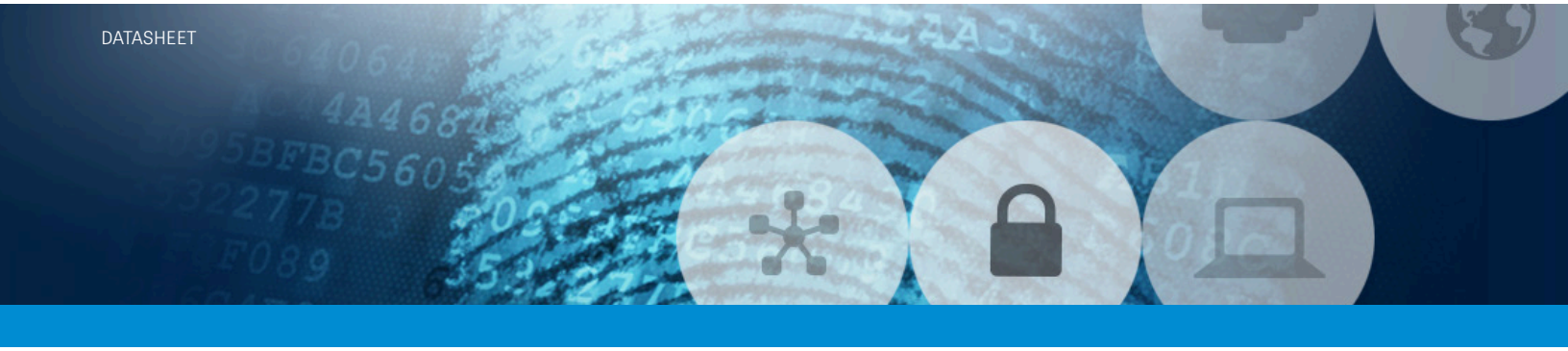
F5® Silverline®
DDoS Protection

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 with stealthy, low-and-slow, application-targeted techniques. To stop DDoS attacks from reaching the enterprise network, organizations need a hybrid solution for cloud-based mitigation in addition to on-premises protection.

F5® Silverline® DDoS Protection is a service delivered via the F5 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 24x7x365 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, 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 attack mitigation insights
The F5 customer portal provides transparent 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—with industry-leading DDoS attack mitigation that features multi-terabit capacity.

Get expert service
F5 Security Operations Center (SOC) experts are available 24x7x365 with optimum service SLAs for uptime and response to DDoS attacks in minutes.

Drive efficiencies with a hybrid DDoS solution
F5 offers comprehensive DDoS protection both on-premises and with the Silverline cloud-based application services platform.

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.

Throughout the F5 infrastructure and process, Silverline DDoS Protection maintains PCI DSS compliance by protecting and controlling data access, encrypting and retaining data, and archiving or deleting data.

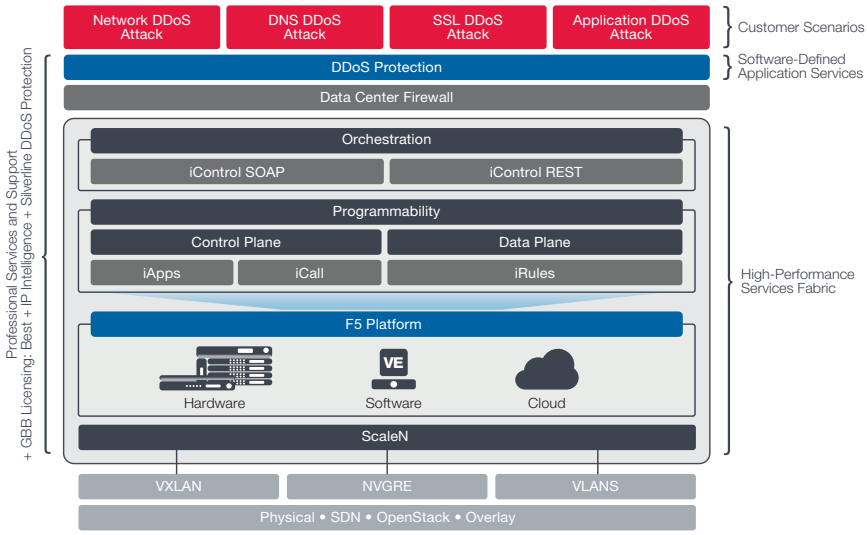


Figure 1: F5 provides a comprehensive DDoS solution with both on-premises protection and cloud-based Silverline DDoS Protection.

Hybrid Signaling

During a DDoS attack, F5 on-premises solutions use Hybrid Signaling, a feature of Silverline DDoS Protection, to alert F5 security experts and to reroute traffic for Silverline cloud scrubbing. Hybrid Signaling enables true hybrid DDoS protection by integrating on-premises equipment with Silverline cloud-based scrubbing technology.

Hybrid Signaling provides real-time communication to Silverline DDoS Protection when volumetric attacks are detected on-premises—alerting the F5 Security Operations Center and enabling rapid mitigation. Hybrid Signaling can also be leveraged, for instance, with F5 BIG-IP® Application Security Manager™ (ASM) on premises to determine bad actors. When BIG-IP ASM determines that a source IP address is a bad actor, it uses Hybrid Signaling to block the IP address in the cloud with Silverline DDoS Protection.

Real-Time 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.

Silverline cloud-scrubbing centers are designed with industry-leading security and open source technologies to detect, identify, and mitigate threats in real time and return clean traffic back to your site. By utilizing the breadth of the most advanced security hardware, software, rules engines, and customized tools, Silverline DDoS Protection provides comprehensive, multi-layered attack analysis and mitigation that cannot be achieved with other scrubbing services that use a single-vendor technology architecture. Silverline DDoS Protection 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.

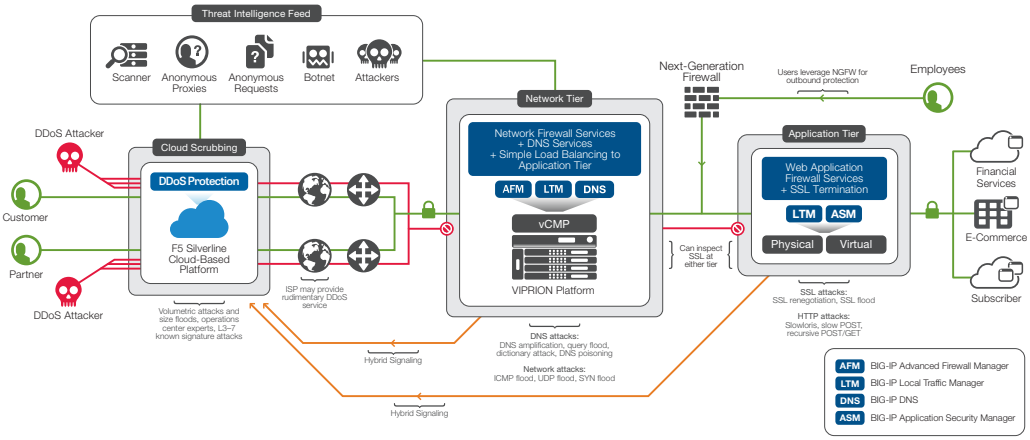


Figure 2: Divert traffic with Hybrid Signaling to Silverline DDoS Protection for cloud-scrubbing when your network is under attack, or use it to continuously scrub all traffic to prevent a DDoS attack from ever reaching your network.

As traffic enters the F5 scrubbing center, it is steered and broken down into a “spectrum of suspicion.” F5 then determines the best scrubbing techniques 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 to your website with little to no impact to the end user.

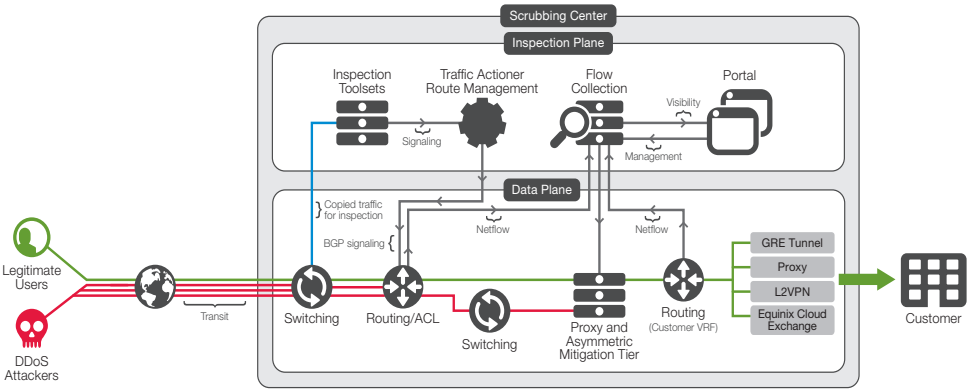


Figure 3: Silverline DDoS Protection multi-layered cloud-scrubbing technologies.

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 with multi-terabit capacity to protect your business from even the largest DDoS attacks. F5 partners directly with three Tier 1 carriers 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 has several asymmetric traffic return mechanisms. These include Layer 2 VPN (L2VPN) technology, allowing high-traffic sites to take advantage of protection without affecting the user experience. Only a fraction of the bandwidth is required to process inbound traffic, ensuring normal delivery of traffic back to your users with the lowest rate of false positives and with maximum performance. Based on your needs, clean traffic can be delivered back to your site through GRE tunnels, proxy, L2VPN, or connection via Equinix Cloud Exchange (in select locations).

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 critical customer 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.

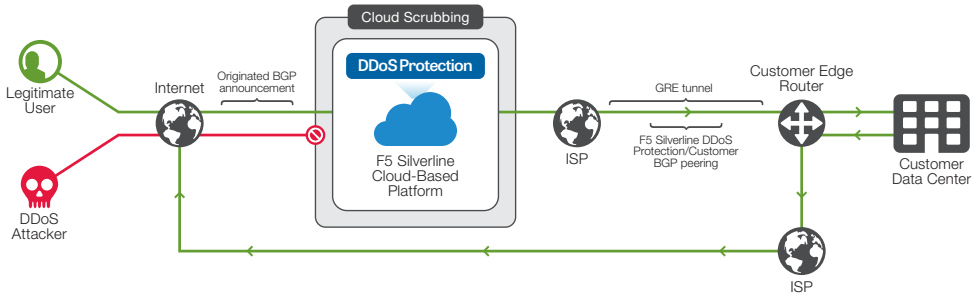


Figure 4: F5 routed mode leverages BGP and GRE tunnels to offer DDoS protection to your network.

L2VPN is an alternative asymmetric technique that provides network infrastructure protection without the need for GRE tunnels. Organizations with on-premises BIG-IP® Local Traffic Manager (LTM) can leverage L2VPN for clean traffic return. With L2VPN there is no need to modify any IP addresses, and return traffic is not encapsulated.

Application protection

For enterprises that require minimum network changes and do not control a full public Class C subnet or prefer to protect only a few applications, Silverline DDoS Protection can be used in proxy mode. Proxy mode supports any application running TCP or UDP such as HTTP, HTTPS, SFTP, DNS, and more on either IPv4 or IPv6. Proxy mode can be set up quickly with simple DNS changes and with little impact to your existing network configuration.

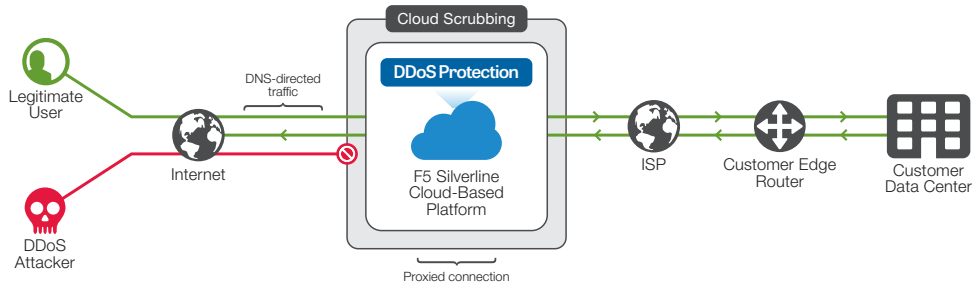


Figure 5: Protect your applications by making a DNS change to direct traffic through Silverline DDoS Protection.

In addition, F5 offers Silverline® Threat Intelligence for additional detection and blocking of IPs known to support malicious traffic. This service reduces unwanted attack communications on your network and helps you avoid further mitigation requirements. Emerging threats are continuously captured and published, while IP addresses that are no longer malicious are removed from the threat data. Silverline Threat Intelligence enhances Silverline DDoS Protection (in proxy mode) or Silverline® Web Application Firewall (WAF) services without compromising access to legitimate IP addresses.

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

The Silverline DDoS Protection includes access to the F5 customer 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. With transparent attack mitigation visibility and reporting, the F5 customer portal provides details about an attack as it occurs, including the type and size of the attack, IP origin, attack vectors, mitigation process, all actions taken by the Security Operations Center during mitigation, and a transcript of all communications (when leveraging secure instant messaging).

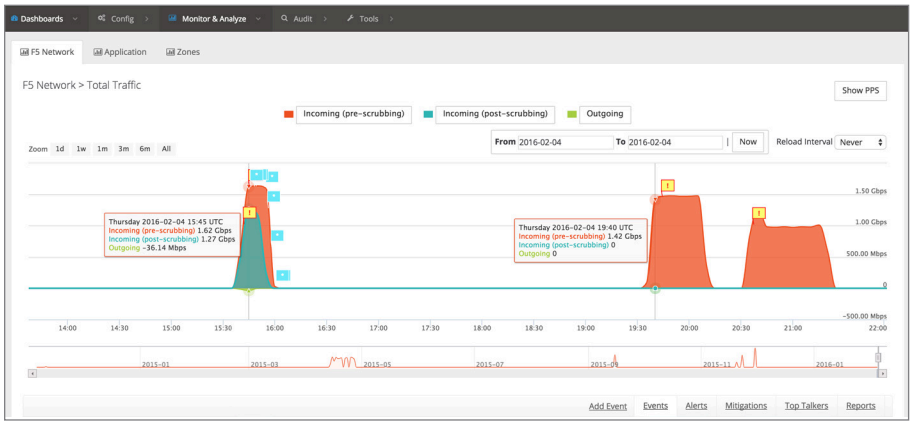


Figure 6: Use the F5 customer portal to inspect attack mitigation design, configure and provision deployment preferences, and view attack events and communications.

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 longer-term views of attack traffic—the F5 customer portal allows you to see the pattern of attacks over time to help you plan for the future. In addition to logging DDoS events to be explored and analyzed, you have the option of exporting logs via Syslog to various SEIM vendor solutions, such as Splunk, ArcSight, and QRadar.

Complete Attack Protection

Silverline DDoS Protection safeguards against a wide variety of attacks, including those 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	All, including: HTTP/HTTPS/SFTP/SNMP/SMTP/ POP-3/CHARGEN/MIME/DNS/IMAP

Flexible Subscriptions

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

Always On	Always Available
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.

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/support.

DevCentral

The F5 DevCentral™ user community of more than 250,000 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 Reference Architecture

F5 Silverline DDoS Protection

If you're under DDoS attack,
F5 offers 24-hour support:

866-329-4253

+1 (206) 272-7969

f5.com/attack

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com