Barrier Networks F5 Silverline
DDoS / WAF Protection

G Cloud 11 Service Definition Document
Copyright

The copyright in this work is vested in Barrier Networks Limited and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under direct agreement or with the consent in writing of Barrier Networks Limited.

No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing to any third party, being an individual firm or company, or any employee thereof without the prior consent in writing of Barrier Networks Limited.

© Barrier Networks Limited 2019

Barrier Networks Limited
272 Bath Street, Glasgow, G2 4JR
Tel: 0141 356 0101
1 Introduction

Barrier Networks Ltd is a privately-owned cybersecurity company who specialises in the integration of cybersecurity solutions. Established in 2006, the company work with all vertical markets that require specialist security advice. We are a partner with leading technology vendors including Fortinet, F5 Networks, Cisco, WhiteHat Security, Microsoft, AlienVault and Thales eSecurity.

Barrier Networks is committed to ensuring that our customers benefit from our years of experience within cybersecurity. Our consultants hold various levels of industry certifications right up to Cisco’s prestigious expert-level CCIE Security. We are accredited to assess and certify against the National Cyber Security Centre Cyber Essentials scheme and work as an authorised “Trusted Partner” of the Scottish Business Resilience Centre.

1.1 Barrier Networks Pedigree

At Barrier we believe that our skills, experience and technology are among the best in the industry and certainly the best in the region, some of our unique advantages include:

- Best of breed technology that is highly rated by Gartner Research.
- UK Based
- Detect advanced threats, malicious insiders and third-party supplier risk.
- Significant experience in full spectrum cybersecurity operations.
- Certified consultants and engineers who hold active security clearances.
- Flexible commercial models with options for Opex based solutions.
2 Solution Description / Silverline DDoS

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.

F5 Silverline is your first line of defence against today’s massive DDoS attacks and has 10 times the bandwidth per customer of the largest existing DDoS mitigation providers. F5 Silverline has very large, very new data centers with the latest equipment built specifically to deal with the attacks seen in the last year. F5 Silverline is a service and so is underpinned by an experienced team of highly skilled and certified SOC analysts in our state-of-the-art Security Operations Center.

F5 Silverline protects against the entire spectrum of DDoS attacks, from Layer 7 attacks to the increasingly frequent large-scale attacks, many of which have overwhelmed traditional DDoS mitigation services and exceeded the size of the Internet pipe before any traffic can even reach an organization on premises mitigation equipment. The benefits over legacy DDoS mitigation services include:

2.1 Fastest Time to Mitigation

F5 Silverline’s proprietary Traffic Actioner technology intercepts each packet of traffic, determines its legitimacy, and automatically routes it to the most appropriate of F5. Silverline’s several hundred different mitigation solutions for the industry’s fastest time-to-mitigation. It breaks down multi-layer attacks into their components for more thorough mitigation via the only systems specifically designed to mitigate each attack vector, versus legacy DDoS solutions that have a “one box does all” approach. Additionally, legacy DDoS mitigation services are based on having a human in the process. The new technologies created by Barrett Lyon and the F5 team have automated the process where mitigation decisions and actions can be taken at the millisecond level, far faster than a human can respond. When needed, a human can be inserted into the mitigation process.

2.2 All Internet Services Protected

While DDoS attacks have traditionally been aimed at the Web operations of their targets, hackers are increasingly attacking non-Web based protocols which are the foundation of many of the mission critical applications housed within the data center (NTP, TELNET, FTP, SNMP, SMTP, POP-3, CHARGEN, MIME and DNS).

2.3 Eliminates Mitigation Side Effects

F5 Silverline technologies eliminate the damaging side effects created by legacy DDoS mitigation solutions such as false positives, blocked users, fraud alerts, fragmentation, slow page loads, broken links, and stalled or timed out video streams. As a service, all mitigations are backed up by our team of SOC experts and thoroughly tested to ensure that legitimate users gain the application access they need.
2.4 Highest Levels of Visibility Before, During and After an Attack

F5 Silverline includes AttackView, the only interactive customer portal to instantly provide the detailed information on an attack in real-time, as well as post-attack analysis. AttackView breaks down each attack into a unique timeline “story” and contains information on attack type, source and size and also the mitigation techniques utilized. It includes data not typically provided by leading DDoS mitigation services, including attack origin, diagnostics of the attack traffic, specific mitigations performed, the result of each mitigation vector on attack traffic, and how each attack responds and morphs based on the specific mitigations performed.

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.

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 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

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 Tier 1 carriers for guaranteed bandwidth that is not shared or based on peering arrangements like other cloud-based services.
2.5 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.

There are a number of options for the delivery of clean traffic. The AttackView™ portal gives you the customer full control over the configuration if desired. Of course should you prefer to work with our SOC team, they are available 24x7x365 to assist.

![Figure 4: Silverline DDoS Protection Routed Configuration](image)

2.6 Simple Application Protection

For enterprises that require minimum network changes and do not control a full Class C network, prefer to protect only a few applications or need to protect additional external 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.

There is no difference in the pricing between Routed and Proxy mode and the two modes can be utilized concurrently. Because of the requirement to protect a number of externally hosted applications, both routed and proxy modes are recommended to meet requirements.
2.7 F5 Silverline AttackView

F5 Silverline AttackView is a proprietary customer portal engineered to instantly provide the detailed information customers really want (and seldom get) both during and after a DDoS attack. A major complaint with traditional DDoS vendors is the lack of transparency. Customers want to know a lot more information than the size of the attack. They want to understand where the attack appeared to be coming from, what types of traffic were used in the attack, what mitigations we performed, and what the impact of each mitigation on the attack. They also want to know how the attack changed to respond to our defences and what adaptive mitigations we employed as the attack evolved. We often hear that vendors provide no attack information at all, taking a secretive Black Box approach.

AttackView lets you see the summary data our SOC sees about your attack as the attack occurs. AttackView breaks each attack into a unique timeline ‘Story’ and contains information on attack type, source and size and also the mitigation techniques utilized. Each Story can be expanded and you can dig as deep as you want to get to the low level attack data. Designed with a secure multi-tenant architecture, each customer is given secure remote access to only their network and attack data.
2.8 F5 Silverline Security Operations Center (SOC)

F5’s Security Operations Center isn’t support that’s outsourced to a third-party. It’s our own high standard of service that’s on the line. The F5 Silverline SOC includes the best and brightest DDoS mitigation experts and network operators in the world, including veterans of Prolexic, Verisign, BitGravity, Juniper, Box.net and Apple’s security team. Our 24x7x365 SOC is staffed by only tier II and above dedicated DDoS analysts as the first line of support and is the only DDoS Mitigation provider to offer an SLA of Tier 3 senior analyst escalation within 15 minutes. You can count on the deep product knowledge of the F5 engineers that develop and support the products you’re using.

2.9 Technical Details

2.9.1 Silverline Cloud Content Scrubbing

F5 Silverline is not a Tier 1 ISP but instead partners with 3 Tier 1 providers for bandwidth capacity and upstream mitigation:

- TeliaSonera International Carrier (TSIC)
- TATA Communication
- NTT

F5 operates 5 scrubbing centers globally:

- Germany
- US West Coast
- US East Coast
- Singapore
- London

These scrubbing centers cover all countries with very low latency (typical 15-40 ms). Our network is designed as an IP Anycast network and each IP is multi-homed. Traffic will be scrubbed at the closest location to the origin.

2.9.2 False Positives

Customer reported false positives are documented with a reported rate of less than .000001%. Any incorrectly implemented signatures are documented and shared throughout the SOC via our standardized training program to ensure knowledge transfer amongst SOC staff. Since false positives are considered far more detrimental than false negatives, traffic filtering will often allow a certain number of false negatives to ensure uptime of customer, as long as the false negatives do not impact said service.

2.9.3 Escalation Procedures

During On boarding procedures, F5 Silverline Security Operations Analysts consult with the customer on which scenarios F5 can take autonomous actions to mitigate and which actions may require pre-authorization. This notation will include an escalation procedure of all contacts within the organization having authorization to provide mitigation. For any events in which fall outside the pre-agreed DDoS parameters, F5 Silverline will by default seek authorization to mitigate.
2.9.4 SLA

The key service deliverables are in coordination with the F5 Silverline SLAs which are as follows:

- Availability of Service - 99.999%
- Time to Detect/Notify of an attack - 15 minute SLA
- Time to Mitigate an attack - 15 minute SLA
- Time to escalate support - 15 minute SLA

2.9.5 Mitigation technics

F5 Silverline has 4 points of mitigation in the data plane of the service. We use a combination of router ACL and FPGA accelerated mitigation rules for routed-customers. For proxy-customers we apply additional mitigation methods in our proxy environment. This spans from rate limiting (with source IP awareness) in hardware to FPGA accelerated mitigation rules.

Mitigation in F5 Silverline usually takes place within a few seconds depending on the nature of the attack. The SLA states 15 minutes for time to mitigation.

Statistical Analysis / Deep Learning have the advantage of being able to look at a trend change and apply rules for acceptable deviation from the baseline. We have decided not to rely exclusively on this due to risk of False Positives when tuned. Combining statistical analysis/deep learning together with Source IP aware rate limiting allows us to tune the mitigation to a more precise level and achieve a better instant protection as well as a solution that can follow trends and compensate for them.

2.9.6 Attack size Support

Each of F5's 5 scrubbing centers is equipped with 360 Gbps Internet bandwidth from Tier 1 carriers.

- TeliaSonera International Carrier (TSIC)
- TATA Communication.
- NTT

As we operate a global IP Anycast network we can block/soak up to 1 Tbps across our scrubbing centers. In addition to this we have a contract with our providers to be able to push ACL’s into their carrier routers to block identified attackers upstream. This gives us the possibility to mitigate attack bandwidth of up to 2 Tbps with no impact on other customers being protected by our scrubbing center.

2.9.7 Protocol Support

All protocols are supported for both Routed and Proxy configurations, the ones highlighted below are the commonly targeted services and protocols:

- HTTP/HTTPS
- DNS/NTP/SSDP/CHARGEN/UPnP
- FTP
- SMTP
- Other TCP
- Other UDP
- Other SSL

There are no additional charges
2.9.8 Availability

F5 Silverline guarantees 99.999% availability of its infrastructure Service Level Agreements are in place for downtime that exceeds 1 minute over the course of a calendar month.

2.10 Types of attack mitigated by F5 Hybrid architecture

2.10.1 Detecting good and bad traffic

The first stages for detection that F5 Silverline will use are pattern recognition, statistical analytics / deep learning and rate-limiting. (Applies to all customers). F5 Silverline and the on-site Viprions includes transaction-based anomaly detection (monitors the client side), latency-based anomaly detection (monitor the server side) as well as monitoring heavy URL’s (monitor specific heavy resources on the server side). These prevention techniques include injecting JavaScript challenge with the responses (thereby eliminating most of the BOTs that are often uses in this type of attack as they cannot respond to the JavaScript challenge). Other prevention techniques include presenting a Captcha Challenge (served from F5) to rate limiting just the traffic causing the increased server latency. In addition to ASM detecting and applying mitigation techniques, it can signal upstream to the Silverline DDoS cloud service, so the offending source IP’s can be blocked in the cloud. These measures ensure that only bad traffic is blocked.

2.10.2 Signalling

By configuring a simple 'signalling template' called an 'iApp' on the on-site devices this allows the on-site devices to signal upstream to the Silverline scrubbing service in the event that an attack is under way. This signalling informs the Silverline SOC to make the necessary changes (BGP or DNS) so that traffic is changed from being routed to CUSTOMER DC’s to being directed to the Silverline scrubbing DC’s. The on premise signalling also updates the scrubbing DC’s with source IPs involved in attacks, so that Silverline can add the IP’s to its blacklist and block them in the cloud.

2.10.3 'low and slow’ attack

This type of attack is detected by the on-site F5 devices. F5 ASM (Application Security Manager), 'Application DOS' configurations can detect if backend servers are slowing down (a typical symptom of a low and slow attack) and then ASM can employ a number of mitigation techniques to determine if it really is a low and slow attack. These prevention techniques include injecting JavaScript challenge with the responses (thereby eliminating most of the BOTs that are often uses in this type of attack as they cannot respond to the JavaScript challenge). Other prevention techniques include presenting a Captcha Challenge (served from F5) to rate limiting just the traffic causing the increased server latency. In addition to ASM detecting and applying mitigation techniques, it can signal upstream to the Silverline DDoS cloud service, so the offending source IP’s can be blocked in the cloud.

2.10.4 Signature based protection

For certain types of attacks that have a defined signature, such as cross site scripting, or SQL injection, F5 on premise devices will utilize its signature database but for the most part, the overall solution does not rely on signatures.
2.10.5 Attack Mitigation in the cloud

Attack Mitigations supported: TCP/IP - IPv4 based (RFC 6274, RFC 6814), ICMP - (RFC 5927), ICMP - (draft-ietf-opsec-icmp-filtering-04), ICMP RFC4907 - more ICMP, TCP based - (draft-ietf-tcpm-tcp-security-03), UDP based DNS – Spoofing, Malformed HTTP, Malformed HTTPS, Malformed SSL/TLS, Network - ping sweep (including slow stealth modes), Network - port sweep (including slow stealth modes), Zero Day Attack detection/mitigation, ICMP UDP based, NAT - resource exhaustion, SYN (brute force and slow attacks), ACK, Connection based (brute force and slow attacks), SSL/TLS, HTTP, E-Mail Flood, Workload attacks - resource intensive, Idle Timeouts, Brute Force, Reflection, Amplification, Known Botnets

Given the variance of types of DDoS attacks, F5 does not distinguish SLA’s based on the type of attack. Because attacks are variable in scope and severity, it is not possible to provide a guaranteed time to provide mitigation. F5 however does provide a 15 minute SLA to begin mitigation and scrubbing activities. Average time to mitigate is 1.8 minutes from detection, authorization and re-direction of traffic.

2.10.6 L7 DDOS

The solution detects abnormal behaviours that are symptomatic of DDoS attacks, such as spikes in connections/sec, floods or increased server latency and then applies a variety of prevention techniques to thwart the attack.

Specificities are:

- TPS based anomaly: ASM module monitor request per second and reacts when traffic change from known pattern. This is setup and monitored per protected application.
- Latency based anomaly: ASM module tracks website latency and activate mitigation when servers start responding slower than usual. This is setup and monitored per protected application.
- Heavy URL Protection: ASM detect specific application’s urls slower than other because of heavy resources consumed by application to handle them. It can them react appropriately to these specific urls.
- Proactive Bot Defence: On mitigation technic propose by ASM when suspecting bot activity is injecting JavaScript code in server's responses which will detect non-human activity.
2.11 Solution Deployment

2.11.1 Silverline Cloud Content Scrubbing Deployment

F5 Silverline is a fully managed cloud based service, thus implementation can be performed remotely by our Security Operations Center. F5 Silverline supports and works with the customer to test the redirection and mitigation before deploying. Below are steps of implementation

- Portal Account Created and sent to assigned technical contacts.
- Customer On boarding call is suggested in order cover on boarding process, information needed, testing schedule, mitigation templates, and mitigation authorization.
- Customer Inputs configuration into User Portal: Proxy Settings, GRE settings, SSL Certificates, White/Black lists.
- Configuration made to network by F5 Security Operations Center Analyst (SOC). Configurations for Proxy can be completed in 15 minutes. Completions for Routed can be completed in 24-48 hours.
- Tests conduction to GRE or proxy connections with non-production applications
- Service is deployed
- If using in Always on mode, Customer redirects traffic via BGP (for routed) or DNS (for proxy).

Total timeline for implementation is 2-5 days (The above depends on the options taken and is subject to change)

2.11.2 Silverline Support

The current support team for F5 Silverline is the F5 Security Operations Center (SOC). This team, which is the first point of contact for any service related enquires or escalations, is comprised of a 24x7 rotation of Tier II and above DDoS analysts. F5 SOC employee hold more than eighteen security certifications, including CISSP, CEH, CSFA, CDRE, Security+, CCNA Security, F5 Certified, GIAC. In addition to training on DDoS inspection and mitigation toolsets, the F5 SOC staff are specifically trained in customer support and are constantly evaluated by Customer Satisfaction Surveys (CSATs) with of average of score of 9.5 out 10. The CSAT scores measure overall satisfaction ratings with ticket response times. As a service option, F5 Silverline provides a Service Delivery Manager.
A member of F5 Silverline Sales Specialist team, will be assigned to each account to act as your point of contact for any account related questions, issues, upgrades, renewals and escalations required for F5 Silverline DDoS. This person will act as a member of the F5 Sales Account team, which will be assigned to manage the account relationship for all F5 products. At this time, F5 Silverline does not make available individual dedicated resources for one account, but will consider on an as needed basis.

The F5 SOC is available to help/support any type of attack and initial setup for delivery method of clean traffic (NAT/GRE/IP REFLECTION/L2VPN).

F5 do not enforce additional SOC fee for assistance during the contract period. The SOC is available 24/7/365 to help you understand, mitigate and tune the protection profiles for your environment.

F5 Silverline provides the option for a Service Delivery Manager. The Service Delivery Manager (SDM) is available for proactive and reactive services to ensure security solutions maintain high availability and provide ongoing business continuity.

The designated F5 Security SDM works closely with you the customer to review security issues and goals, then matches your objectives with F5 Services recommended practices to provide exceptional service and a stronger security posture.
The Security SDM consolidates communication and all required activities under a single Global Services contract to improve the agility, efficiency, and effectiveness of the customer’s security strategy – Further information on SDM function is provided below:

- Provide continuity across the F5 Services portfolio, including Support, Professional Services, and Knowledge Services
- Main point of communication on active issues across F5
- Prepare Security Service Delivery Plan
- Regular open case status reviews
- Quarterly Security Business Reviews
- Security product optimization & utilization
- Industry intelligence & event management

2.11.3 Silverline Change Management / DDOS Testing

- These change procedures usually only impact proxied applications.
- For customers with Routed mode deployments, additional applications can be detected and baselines created transparently.
- For customers with proxy-mode deployments we manage changes for the proxy environment either through the customer portal where you can make necessary changes and add additional services/applications, or by speaking to the SoC directly over phone/email.
- All changes made through the portal are committed by the SOC after being added by the customer. A new service/application can be up within a few minutes.
- In proxy mode the service covers a number of IP addresses, if customer has used all of the available IP addresses, individual or additional blocks of IPs can be purchased.
- F5 will provide an external vendor contact specialized in DDOS testing. It is recommended that DDOS mitigation is tested once a quarter on each change network facing components

2.11.4 Silverline Data Availability

F5 Silverline mitigates Layer 7/ SSL attacks though its Proxy redirection method, securely provide their SSL certificates/keys. When SSL certificates/key for an application are provided, the F5 Silverline DDoS Protection service has full payload visibility. SSL termination can be selected on a per IP basis. If the traffic is not SSL encrypted, then Proxy mode can provide full payload visibility and analysis. Installing a physical appliance designed to identify and mitigate Layer 7 attacks on a client’s premises reduces the need to mitigate Layer 7 attacks in a cloud based solution. F5 Silverline integrates with F5 BIG IP Application Security Manager (ASM) - the market leading on premise Web Application Firewall. This integration between on premise equipment and cloud based infrastructure facilitates the automatic signalling of bad actor information from one to the other. The result being immediate detection and logging of attacks on premise and automatic blocking of those detected bad actors in the cloud.

In this hybrid configuration, the Silverline cloud service mitigates non encrypted volumetric attacks and potentially clear text L7 attack traffic, whilst the on premise devices which terminate SSL can provide signalling to indicate malicious IP’s for blocking in the cloud.
2.12 Silverline Data Security

All F5 Silverline Network and personnel is PCI DSS 3.2 Certified and audited an annual basis. F5 Silverline is a service provider, thus no customer data passing through is being stored, outside of what is necessary for DDoS mitigation. Customer data is isolated to defined customer accounts and stored with appropriate audit logging and access controls to meet PCI Requirements. Only registered users for a given customer have access to the configuration portions of the service.

Sensitive data is encrypted both in transit as well as at rest. All access to sensitive information is stored in the Silverline Portal.

SSL Certificate and Key combination is securely uploaded either via direct entry of the certificate and key contents or via file upload. Upon upload, the portal systems create an MD5 hash of the Certificate and Key and then encrypt them prior to storage into the portal database. After upload, the only allowable action is to delete the Certificate and Key configuration; there is no option available for download or modification. When a customer provisions a proxy configuration, an SSL Certificate is assigned to the proxy configuration. The SSL traffic is only decrypted within the BIG-IP proxy itself, at no time is the decrypted traffic copied or spanned off box. When the proxy is configured, a secure API extracts the certificate out of the Silverline database and installs it on the BIG-IP proxy.

2.13 Silverline Log Management

For F5 Silverline DDoS Protection Routed customers, we do not retain a log of communication to or from a customer’s web-site. We do retain meta-data as defined by Netflow statistics on this traffic which would include source and destination IP addresses, source and destination ports and overall volume of traffic (payload size).

For Proxy customers, by default we store request and response traffic for troubleshooting purposes; this can be disabled as required by the customer via the portal.

The Netflow metadata is stored indefinitely. The request/response logging information, if stored at all, is stored for 1 year.

All customer data is stored via a unique instance ID within the logging infrastructure. Only logs generated by a specific customer’s configuration are defined within the customer instance. Customers do not have access to these logs in any form; they are for internal usage only. All F5 Silverline infrastructure components are PCI DSS compliant and while this may not be directly relevant to all customers, defines a standard for access control and logging that is adhered to for all processes and data within F5 Silverline.

F5 Silverline is PCI DSS 3.0 compliant and audited an annual basis. PCI DSS 3.0 attestation is available upon request.
2.14 IP Reputation Database

F5 IP Intelligence incorporates external, intelligent services to enhance automated application delivery with better IP intelligence and stronger, context-based security. By identifying IP addresses and security categories associated with malicious activity, the IP Intelligence service can incorporate dynamic lists of threatening IP addresses into the F5 BIG-IP platform, adding context to policy decisions. IP Intelligence service reduces risk and increases data center efficiency by eliminating the effort to process bad traffic. Categories available thru the IP Intelligence database are described here:

<table>
<thead>
<tr>
<th>Category Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnets</td>
<td>IP addresses of computers that are infected with malicious software (Botnet Command and Control channels, and infected zombie machines) and are controlled as a group by a Bot master, and are now part of a botnet. Hackers can exploit botnets to send spam messages, launch various attacks, or cause target systems to behave in other unpredictable ways.</td>
</tr>
<tr>
<td>Cloud Provider Networks</td>
<td>IP addresses and networks that are used by cloud providers.</td>
</tr>
<tr>
<td>Denial-of-Service</td>
<td>IP addresses that have launched denial-of-service (DoS) attacks, distributed denial-of-service (DDoS) attacks, anomalous SYN flood attacks, or anomalous traffic detection. These attacks are usually requests for legitimate services, but occur at such a fast rate that targeted systems cannot respond quickly enough and become bogged down or unable to service legitimate clients.</td>
</tr>
<tr>
<td>Illegal Web sites</td>
<td>IP addresses that contain criminally obscene or potentially criminal internet copyright and intellectual property violations.</td>
</tr>
<tr>
<td>Infected Sources</td>
<td>Active IP addresses that issue HTTP requests with a low reputation index score, or that are known malicious web sites offering or distributing malware, shell code, rootkits, worms, or viruses.</td>
</tr>
<tr>
<td>Phishing</td>
<td>IP addresses that host phishing sites, and other kinds of fraud activities, such as ad click fraud or gaming fraud.</td>
</tr>
<tr>
<td>Proxy/Anonymous Proxies</td>
<td>IP addresses that are associated with web proxies that shield the originator's IP address (such as proxy and anonymization services). This category also includes TOR anonymizer addresses.</td>
</tr>
<tr>
<td>Scanners</td>
<td>IP addresses that are involved in reconnaissance, such as probes, host scan domain scan, and password brute force, typically to identify vulnerabilities for later exploits.</td>
</tr>
<tr>
<td>Spam Sources</td>
<td>IP addresses that are known to distribute large amounts of spam email by tunneling spam messages through proxy, anomalous SMTP activities, and forum spam activities.</td>
</tr>
<tr>
<td>Web Attacks</td>
<td>IP addresses involved in cross site scripting, iFrame injection, SQL injection, cross domain injection, or domain password brute force.</td>
</tr>
<tr>
<td>Windows Exploits</td>
<td>Active IP addresses that have exercised various exploits against Windows resources by offering or distributing malware, shell code, rootkits, worms, or viruses using browsers, programs, downloaded files, scripts, or operating system vulnerabilities.</td>
</tr>
</tbody>
</table>
3 Solution Description / Silverline WaF

Organisations that move application workloads to the cloud face challenges protecting enterprise data. As security attacks across traditional and cloud environments become more sophisticated, in-house security teams often struggle to stay up to date on the latest attacks and protection measures, and deliver consistent policies and compliance across environments. A lack of consistency can result in security vulnerabilities, higher expenses, and a slower response to threats and compliance issues.

F5 Silverline Web Application Firewall is a cloud-based service built on BIG-IP Application Security Manager (ASM)—with 24x7x365 support from highly specialized security experts to help organizations protect web applications and data, and enable compliance with industry security standards, such as PCI DSS.

Silverline Web Application Firewall Offers:

- Ensure application security and compliance
- Get comprehensive protection from advanced layer 7 attacks, OWASP Top Ten application security risks, and zero-day attacks—and enable compliance with key regulatory mandates.
- Get 24x7x365 expert service
- Receive 24x7x365 access to web application firewall (WAF) experts who build, proactively monitor, and fine-tune WAF policies against known and emerging threats.
- Deploy flexibly across hybrid environments
- Ensure consistent web application security, availability, and user experiences across traditional and cloud data centers.
- Defend with proven security effectiveness
- Leverage security efficacy with technology built on the NSS Labs–recommended BIG-IP ASM, based on tests that demonstrate 99.89 percent overall security effectiveness.
- Drive operational and cost efficiencies
- Remove the complexity of WAF management, increase the speed to deploy new policies, and decrease operational expenses.
- Gain attack insights and intelligence
- Access reports through the cloud-based customer portal and incorporate external intelligence for securing apps against identified threats.
- Get Expert Service to Protect Web Applications and Achieve Compliance

The growth of cloud-hosted web applications has been accompanied by increasingly sophisticated security attacks and risks that threaten enterprise data. As a result, administrators and security teams face challenges keeping up to date on the latest attacks and protection measures. At the same time, they must meet the stringent compliance requirements for online commerce and data sharing across traditional and cloud environments.

Organisations must choose between employing specialized IT security teams in-house—resulting in higher expenses and increased time to deploy policies—or offloading the complex WAF policy management and compliance to a service to drive efficiencies.
The Silverline Web Application Firewall service delivers comprehensive, efficient layer 7 protection and compliance for enterprise data and web applications across all environments. The service also includes expert support from highly specialized security experts who remove the complexity of WAF policy management, increase the speed to deploy new policies, and free up internal IT resources and budget for other projects.

The Silverline Web Application Firewall service protects web applications no matter where the app is hosted—in the private cloud, the public cloud, or a physical data center.

3.1 Defend with Proven Security Effectiveness

Silverline Web Application Firewall is built on BIG-IP ASM, which is recognized as the most scalable WAF on the market and is deployed in more data centers worldwide than any other WAF. NSS Labs recommends BIG-IP ASM based on tests that demonstrate 99.89 percent overall security effectiveness with minimal false positives (0.124 percent) as compared with competitors.

3.2 Comprehensive Attack Protection

Silverline Web Application Firewall provides comprehensive geolocation attack protection from layer 7 distributed denial-of-service (DDoS), SQL injection, OWASP Top Ten application security risks, cross-site scripting (XSS), and zero-day web application attacks. It prevents execution of fraudulent transactions, stops in-browser session hijacking, and secures AJAX applications and JSON payloads. The service also delivers proactive bot defence capabilities that provide always-on protection—preventing automated layer 7 DoS attacks, web scraping, and brute force attacks. Silverline Web Application Firewall provides live updates for attack signatures to ensure up-to-date protection, geolocation-based blocking, and an integrated XML firewall. For more details on these attack protections, please see the BIG-IP ASM datasheet.

3.3 Built-in Compliance and Reporting Capabilities

Advanced, built-in security protection and remote auditing help organizations comply with industry security standards, including the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Basel II, and SOX—cost effectively and without multiple appliances, application changes, or rewrites. Silverline Web Application Firewall reports previously unknown threats, such as layer 7 DoS and SQL injection attacks, and mitigates web application threats to shield the organization from data breaches.

3.4 Receive Expert Policy Building and Monitoring

Websites are diverse, complex, and constantly changing—requiring policies with hundreds if not thousands of clear and precise rules. The Silverline Web Application Firewall service includes the highest level of service in the industry with F5 Security Operations Center (SOC) experts who manage policy changes while balancing the strictest security controls with legitimate user access. Unlike other WAF service vendors that provide self-service capabilities and expect the customers to handle most of the configurations and policy management, the F5 SOC experts are available 24 hours a day, 7 days a week, 365 days a year. These experts build, monitor, and fine-tune policies to protect web applications and data from new and emerging threats.
3.5 Expert policy creation

F5 SOC experts are available to work with customers to rapidly deploy policies and create more advanced policies based on heuristic learning and specific application-security needs. Policies can be created to work in conjunction with existing BIG-IP ASM configurations.

3.6 Expert policy staging

F5 SOC experts work to reduce false positives by staging and testing policies in a live environment using attack signatures, file types, URLs, and other parameters. These tests determine if changes are needed before a policy is enforced, without reducing current protection levels. Policies are redesigned and retested until they are ready for live implementation.

3.7 Gain Attack Insights and Intelligence

The Silverline Web Application Firewall service includes access to the Silverline customer web portal—enabling administrators to securely communicate with F5 SOC experts and view centralized threat-monitoring reports. The customer portal provides immediate attack details and enhanced visibility into the mitigation techniques used to detect and prevent the application attack. Details include source geo-IP mapping, blocked vs. alerted attacks, blocked traffic, blocked attack types, alerted attack types, threats, bandwidth used, hits/sec, and the type of traffic and visits (bots v. humans).

3.8 Integration for agility and adaptability

The ability to respond to frequent changes in attack methods is a key component of web application security. By integrating with third-party products, Silverline Web Application Firewall provides a dynamic and adaptable security solution. Data can be uploaded from WhiteHat Sentinel, IBM Rational AppScan, HP WebInspect, Cenzic Hailstorm, and QualysGuard Web Application Scanning products. These products offer vulnerability assessment, auditing, and real-time database reporting to provide security breach reviews, attack prevention, and compliance.
3.9 The Silverline Web Application Firewall Architecture

Silverline Web Application Firewall is a security service built on F5’s unique BIG-IP ASM web application firewall to protect applications from OWASP Top 10 threats and other zero-day threats.

Silverline Web Application Firewall protects against application attacks including:

- OWASP Top Ten attacks
- Layer 7 DoS and DDoS
- Brute force
- Parameter and HPP tampering
- Sensitive information leakage
- Buffer overflows
- Cookie manipulation
- Various encoding attacks
- Forceful browsing
- Hidden fields manipulation
- Request smuggling
- XML bombs/DoS
- Web scraping
- Reverse engineering
- Application tampering
- Zero-day web application attacks
- AJAX/JSON web threats
- Security Operations Center

services include:
- Expert policy setup
- Policy fine-tuning
- Policy staging
- Proactive alert monitoring
- False positives tuning
- Detection tuning
- Whitelist/Blacklist configuration
- Additional security features:
- RFC compliance
- Bot protection
- VA Scan importation with third-party
- DAST Vendors
- PCI compliance reports
- Web scraping prevention
- Geolocation-based blocking
3.10 F5 Hybrid DDOS Architecture

While the DDoS threat landscape is constantly evolving, F5 has found that attacks continue to fall within four attack types: volumetric, asymmetric, computational, and vulnerability-based. These attack categories have the following characteristics:

- **Volumetric**—Flood-based attacks that can be at layer 3, 4, or 7.
- **Asymmetric**—Attacks designed to invoke timeouts or session-state changes.
- **Computational**—Attacks designed to consume CPU and memory.
- **Vulnerability-based**—Attacks that exploit software vulnerabilities.

Defensive mechanisms have evolved to deal with these different categories, and today’s high-profile organizations have learned to deploy them in specific arrangements to maximize their security posture. By working with these companies and fine-tuning their components, F5 has developed a recommended DDoS mitigation architecture that can accommodate specific data center size and industry requirements.

The following table shows the mapping of DDoS architecture components to the four DDoS attack categories they mitigate.

<table>
<thead>
<tr>
<th>Attack Category</th>
<th>Mitigation Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volumetric</td>
<td>Cloud based scrubbing service</td>
</tr>
<tr>
<td>Web Application Firewall</td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td>Web application Firewall</td>
</tr>
<tr>
<td>Computational</td>
<td>Application Delivery Controller</td>
</tr>
<tr>
<td>Network firewall</td>
<td></td>
</tr>
<tr>
<td>Vulnerability-based</td>
<td>IP reputation Database</td>
</tr>
<tr>
<td>Intrusion Prevention/detection Systems (IDS/IPS)</td>
<td>Application Delivery Controller</td>
</tr>
</tbody>
</table>

F5 recommends a hybrid cloud/on-premises DDoS solution. Volumetric attacks will be mitigated by F5 Silverline DDoS Protection—a service delivered via the F5 Silverline cloud-based platform.

Silverline DDoS Protection will analyse and remove the bulk of the attack traffic. Sometimes, a DDoS campaign may include application layer attacks that must be addressed on premises. These asymmetric and computational attacks can be mitigated using the network defence and application defence tiers. The network defence tier is composed of layer 3 and 4 network firewall services and simple load balancing to the application defence tier. The application defence tier consists of more sophisticated (and also more CPU-intensive) services including SSL termination and a web application firewall stack.
There are compelling benefits to separating network defence and application defence for the on-premises portion of the DDoS Protection architecture.

- The network and application defence tiers can be scaled independently of one another. For example, when web application firewall usage grows, another appliance (or blade) can be added to the application tier without affecting the network tier.
- The network and application defence tiers can use different hardware platforms and even different software versions.
- When new policies are applied at the application defence tier, the network defence tier can direct just a portion of traffic to the new policies until they are fully validated.

### 3.11 F5 BIG-IP on premise

This is outlined as an optional avenue for CUSTOMER to compliment the Silverline cloud offering. DOS and application protection on premise is provided by F5 ADC award winning technology BIG-IP appliances. Among all security features available two main modules allows covering DOS security protection:

- Application Security Manager: ASM for application DDOS and security protection.

Both modules can be consolidated into a single appliance to create perfect Data Center first line of defence.

**F5 BIG-IP Advanced Firewall Manager (AFM)** is a high-performance, stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols. Built on F5’s industry-leading Application Delivery Controller (ADC), BIG-IP AFM gives enterprises and service providers the scalability, flexibility, performance, and control needed to mitigate the most aggressive, volumetric distributed denial-of-service (DDoS) attacks before they reach the data center.

BIG-IP AFM’s unique application-centric design enables greater effectiveness in guarding against targeted network-level attacks. It tracks the state of network sessions, maintains deep application
awareness, and uniquely mitigates attacks based on more granular details than traditional firewalls. With BIG-IP AFM, organizations receive protection from over 100 attack signatures—more hardware-based signatures than any other vendor—and unsurpassed programmability, interoperability, and visibility into threat conditions.

**Scale to meet network demand**

Meet demands for higher bandwidth usage and concurrency rates with F5’s proven TMOS® architecture, hardware systems, and virtual editions to ensure performance while under attack.

**Ensure application availability**

Secure networks from DDoS threats across a variety of protocols, with in-depth rules customization and increased performance and scalability.

**Protect with an app-centric full-proxy Firewall**

Inspect all incoming client connections and server-to-client responses, and mitigate threats based on security and application parameters before forwarding them on to the server.

**Inspect SSL sessions**

Fully terminate and decrypt SSL traffic to identify potentially hidden attacks—at high rates and with high throughput.

**Streamline firewall deployment**

Simplify security configuration with firewall policies oriented around applications and an efficient rules and policy GUI.

**Customize reporting for visibility**

Easily understand your security status with rich customizable reports, logging, and charts that provide insight to all event types and enable effective forensic analysis.

**BIG-IP Application Security Manager (ASM)** is an on-premises web application firewall (WAF), deployed in more data centers than any enterprise WAF on the market. With advanced firewall capabilities, it secures applications against layer 7 distributed-denial-of-service (DDoS) attacks and application vulnerabilities where other WAFs fail. Built on F5’s industry-leading Application Delivery Controller with the F5 TMOS® operating system, BIG-IP ASM delivers flexible and comprehensive protections wherever apps reside and without compromising performance—all on a platform that consolidates application protection and access management.

BIG-IP ASM is uniquely offered as an appliance, virtual edition, and as a managed service, providing automated WAF services that meet complex deployment and management requirements while protecting your apps with great precision. It is the most effective solution for guarding web applications and data from existing and emerging threats, and maintaining compliance with key regulatory mandates.

**Ensure application security and compliance**

Gain comprehensive security against sophisticated layer 7 attacks and enable compliance with key regulatory mandates.
Turn on protection immediately

Simplify security with pre-built policies, out-of-the-box signatures, and a streamlined approach to policy management that decreases operational expenses.

Patch vulnerabilities fast

Identify and resolve app vulnerabilities in minutes with leading DAST integration and automatic virtual patching.

Deploy flexibly

Deploy as an appliance, in virtual or cloud environments, and support multi-tenant services while incorporating external intelligence that secures against known IP threats.

Defend with proven advanced protections

Identify and block attacks with advanced, highly programmable technology demonstrating 99.89% overall security effectiveness.

Magnify threat knowledge

Easily understand your security status with detailed forensic analysis and rich insight into all events and user types.
4 Proposed Architecture

4.1 CUSTOMER Hybrid Architecture

Current CUSTOMER architecture deploys F5 in DMZ and other strategic internal networks within the Data Center for mainly Load balancing but in some cases have far more modules (including in some locations WAF).

Based on this topology we will initially propose the following architecture for both DDoS and WaF services, this can be expanded to include On-premise mitigation but is optional for this bid.

![Proposed Architecture Diagram]

*Figure 8: proposed architecture option 1*
CUSTOMER will be using BGP routing to route traffic through Silverline for DDoS mitigation. They have 16 external subnets whereby all or a subset can be routed through the service either on an Always On or Always Available preference.

For redundancy there will be a GRE tunnel from each of our Edge routers in the Frankfurt data center to each Edge router in the 3 CUSTOMER data centers, so a total of 12 GRE tunnels.

Additionally, we will be monitoring the CUSTOMER routers using Netflow to detect any on premise anomalies.

For WaF services CUSTOMER have highlighted the below URL’s for WaF protection. We will issue public Silverline IP’s which CUSTOMER will use to make DNS changes for Silverline to protect these resources.

CUSTOMER will then specify a backend destination for that service and the traffic will be proxied back through the Silverline service.

4.2 F5 vs Competitor Solutions

F5 offers the complete L2-L7 mitigation and scrubbing services versus the competitors who only offer L3-L4 mitigation and have to partner with other vendors for offering an on premise + cloud design. On the other hand, F5 uses purpose built patented hardware FGPAs to perform complex L7 multi-threaded mitigation without increasing any application latency or effecting overall performance utilization on the f5 device. F5’s TCL scripting language, iRules, allows the f5 device to write filters for complex or zero day attacks on the fly. While other vendors will take days or weeks to mitigate against a zero-day attack, f5 engineers will write a simple iRule in a matter of a few minutes to mitigate an attack that can possibly cost organization millions of dollars in revenue. So, for threats like Heartbleed, Poodle, LogJam, and etc., customers with f5 can mitigate those attacks very simply via our GUI and due to the f5 device being a fully L2-L7 proxy that terminates the SSL sessions.

F5 has extensive experience in providing the critical service of handling traffic for large enterprises for over two decades. With the purchase of Defense.Net two years ago, f5 has seamlessly integrated it's on- premise solution with Defense.net cloud based solution and marketed the service as Silverline. Before the acquisition, Defense.net was very particular on which type of customers to protect due to avoiding the risk of high risk vertical companies that deal with online gaming and other industries that have a high risk of being attacked. Dealing with high risk companies increases the ‘concentration risk’, meaning the service may not always be available when the customer needs it as other customers are consuming their scrubbing capacity. This can also lead to side-effects (collateral damage) for always-on customers who are permanently routed through their infrastructure. In contrast, F5 Silverline offers the highest capacity per customer in the industry and plans to scale with our customer base to ensure this is always the case.

Most cloud DDoS providers offer a single threaded DDoS solution which has many limitations in regards to Layer 7 and results in a high number of false positives. In contrast, F5 has a whole host of the best of breed commercially available and our own proprietary technology replicated across all of our dedicated mitigation facilities, meaning we’re able to deliver multi-threaded mitigation, better layer 7 mitigation and lower false positives.

Most cloud DDoS providers scrubbing centers in EMEA and APAC have very limited scrubbing capacity, which means there’s likely to be a considerable performance hit (latency) when mitigating larger attacks as data must be sent to another scrubbing facility once bandwidth at the primary
mitigation facility is consumed. By comparison, F5 has over 240Gbp/s of scrubbing capacity at each site.

Some Cloud DDoS providers also sell other services such as DNS solutions. These providers have been taken down multiple times due to DDoS attacks, that have ranged from simple L3-L4 attacks to outright DNS attacks. This is publicly available information and can be found with a simple Google search. F5 utilizes its own solution (called “Dogfood” internally) and we have never succumbed to a DDoS attack due to having a full suite of L2-L7 on-premise and cloud-base protection.

F5 is fully confident in our mitigation service that if DDoS attacks exceed over 72 hours, f5 offers a free coverage contact. We believe we are the only vendor today that offers this.

The competitors SoC has no support specialization in tier I-II (i.e. support is trained in Managed DNS, web monitoring, and anti-DDOS). In contrast all the analysts in the f5 SOC are qualified DDoS engineers and are able to authorize and begin mitigations without having to escalate the call. This means a faster time to enact the service and mitigate an attack.

F5’s solution is fully PCI compliant and we can provide certification on request. Competitors solution are not PCI certified. PCI compliance is very important for any security vendor, even if the customer is not doing any financial transactions. In the security vendor industry, it’s considered a basic compliance to have on any device or service.

F5’s cloud based and on premise solution is the only complete solution which doesn’t involve working with multiple vendors to provide different pieces of a DDoS solution. Having a single vendor that provides a full suite of L2-L7 security solution allows f5 to be fully accountable for protecting our customer’s networks. Other competitors are lacking a full solution, so having a solution that involves different partners split the risk showcases that these vendors do not want to take full accountability in protecting their customer’s network.

Competitors on-prem solutions are utilizing a pure software solution on generic off the shelf hardware. F5 has made the investment in writing our own software and designing our own hardware to be fully independent of other vendors and that allows f5 to be the leader in innovation and act as the strategic point of control for our customers.

F5 being a single hardware vendor offering a complete on-prem and cloud solution reduces the OPEX cost for customers as they have to deal with only one vendor.