F5® Silverline® Web Application Firewall Onboarding: Technical Note

F5® Silverline® Web Application Firewall Onboarding

With organizations transitioning application workloads to the cloud, traditional centralized application security architectures fail to deliver consistent policies, user experiences, and regulatory compliance across environments. The result is significant security vulnerabilities, higher expenses, and increased time to remove bad actors and maintain compliance.

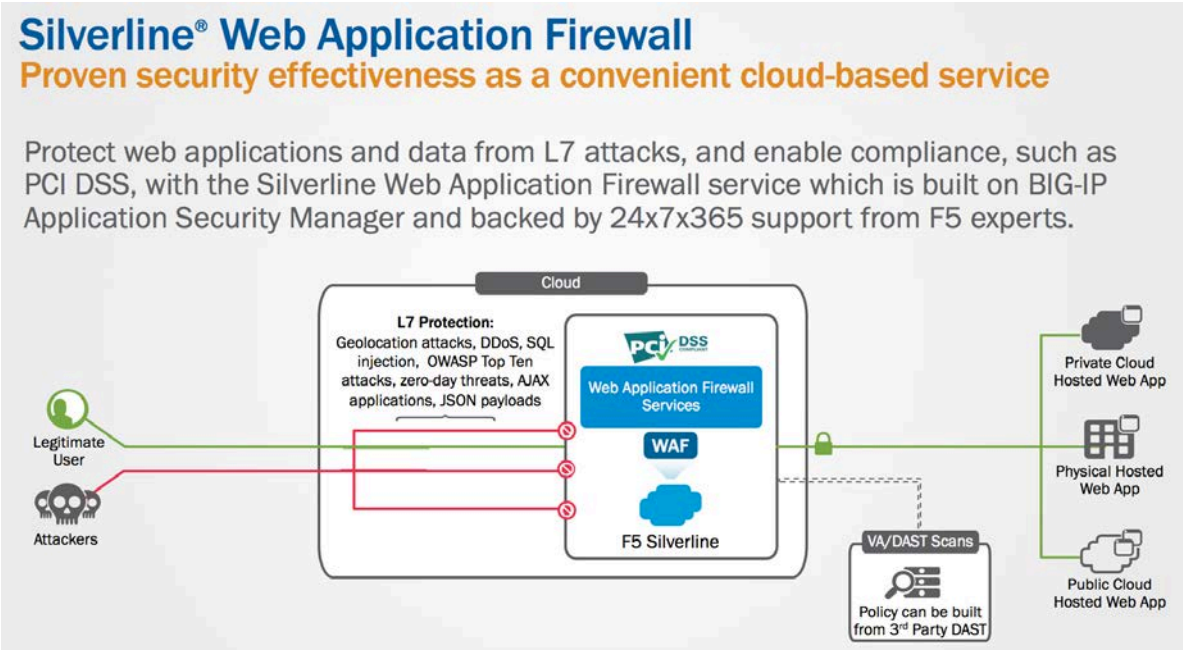
F5® Silverline® Web Application Firewall is a service built on BIG-IP® Application Security Manager™ (ASM™) with support from highly specialized security experts who build and maintain web application firewall policies to defend organizations against web attacks and achieve regulatory compliance across traditional and cloud environments.

Challenges in Protecting Web Applications

Organizations are finding difficulties operationally keeping up with the increasingly sophisticated security attacks and risks threatening enterprise data in the growth of cloud-hosted web applications. Keeping up-to-date on the large volume of security attacks and protection measures while simultaneously meeting the stringent compliance requirements for online commerce and data sharing across traditional and cloud environments presents an enormous challenge to security teams and system owners.

Organizations must choose between employing highly specialized IT security teams in-house – which results in higher expenses and increased time to deploy policies against vulnerabilities – or offloading the complex WAF policy management and compliance to a service to drive operational and cost efficiencies.

The Silverline® Web Application Firewall service delivers comprehensive and operationally efficient layer 7 attack protection and compliance for enterprise data and web applications across traditional and cloud environments. Support from highly specialized security experts helps to 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 Architecture

Silverline® Web Application Firewall is a security service built on F5's purpose-built BIG-IP Application Security Manager web application firewall to protect applications from OWASP top 10 threats and other zero-day threats.

F5 Silverline protects against various application attacks, including:	**Security Operations Center services include:**
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 RFC compliance Bot protection VA Scan importation with 3rd party DAST Vendors PCI compliance reports Web scraping prevention Geolocation-based blocking	Expert policy setup Policy fine-tuning Policy staging Proactive alert monitoring False positives tuning Detection tuning Whitelist / Blacklist configuration **Security services include:** RFC compliance Web services security Data Guard and cloaking Bot protection DAST integration with Whitehat Sentinel, HP WebInspect, IBM Rational AppScan, Cenzic Hailstorm and QualysGuard Web Application Scanning Application dashboard, with report visibility, metrics, and analytics Web scraping prevention Response capturing for valid or attack requests Geolocation-based blocking Web services encryption/decryption and digital signature verification Better threat protection with external IP Intelligence ICAP support

Activating the Service

Most configuration tasks can be completed using the Silverline® Customer Portal at https://portal.f5silverline.com. The assigned customer contact will receive an activation email from the F5 Security Operations Center (SOC). The email will contain an activation link, which will enable the customer to setup authentication credentials and enter configuration information for the service to be deployed.

Proxy Configuration

Customers leverage a full HTTP/HTTPS proxy to protect their application. The proxy can be set up very quickly, with minimum impact to the customer's existing network setup.

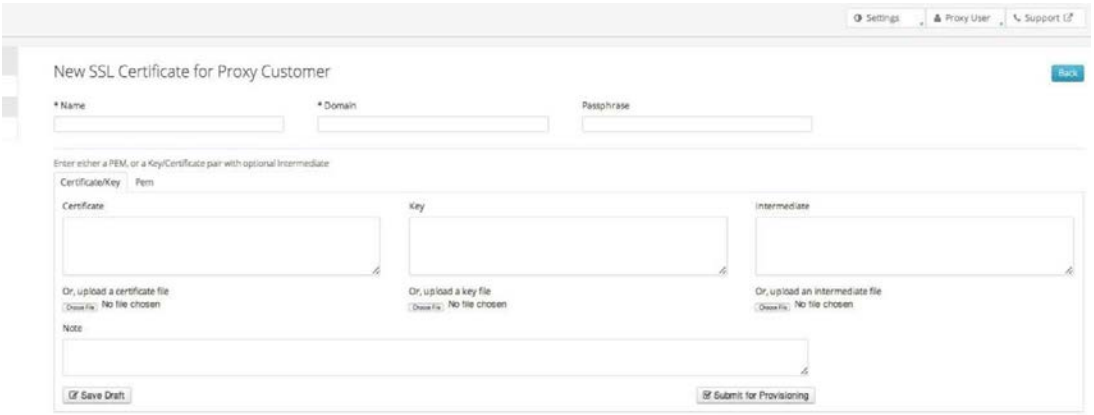
Requirements

The requirements for setting up proxy mode are minimal. It requires the ability to update Domain Name Service (DNS) settings for the Fully Qualified Domain Names (FQDNs) to be protected. Additionally, customers may wish to block general Internet traffic to the application's origin IP address after the Silverline® Web Application Firewall service is configured for additional protection.

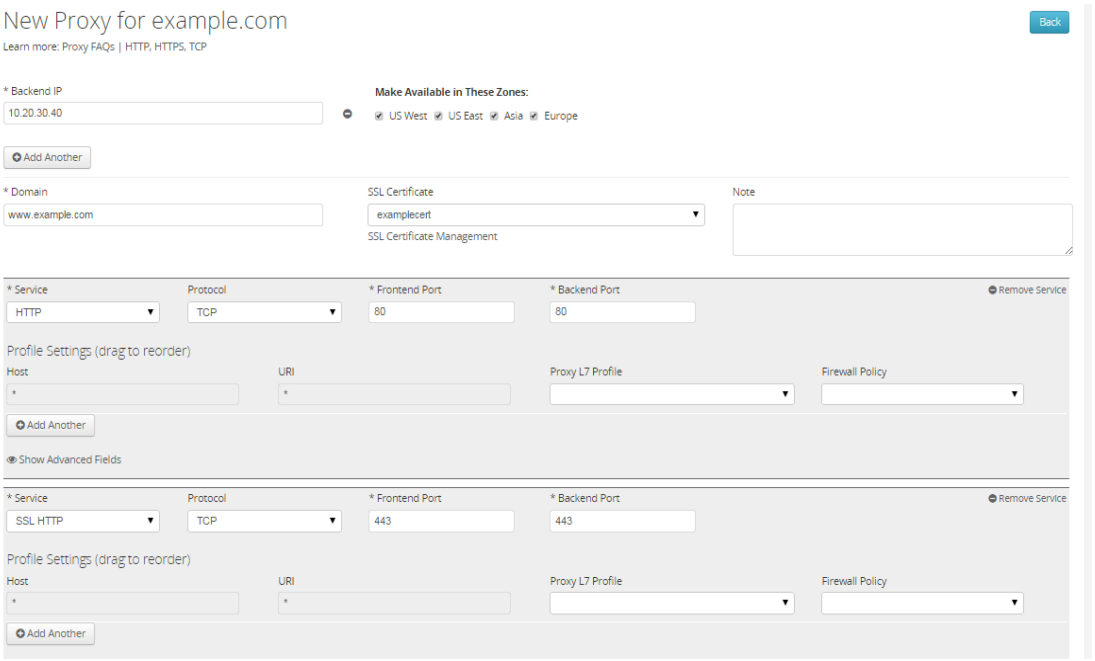
Configuration

In order to set up the proxy, log in to the customer portal and navigate to the configuration section. Make the following changes:

1. Import SSL keys to the proxy for SSL traffic.

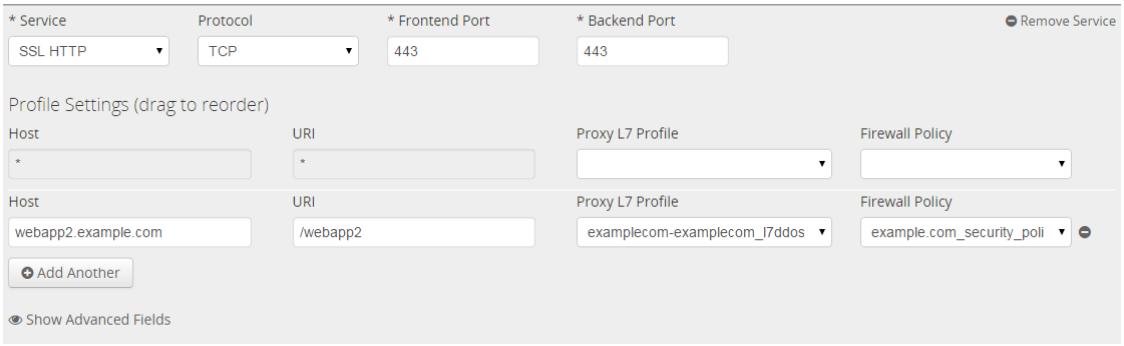


2. Complete proxy configuration on the user portal. The server IP address (also known as backend IP address), service and ports, are required to configure the proxy set-up. Multiple ports can be configured on the same frontend/backend IP address pair.

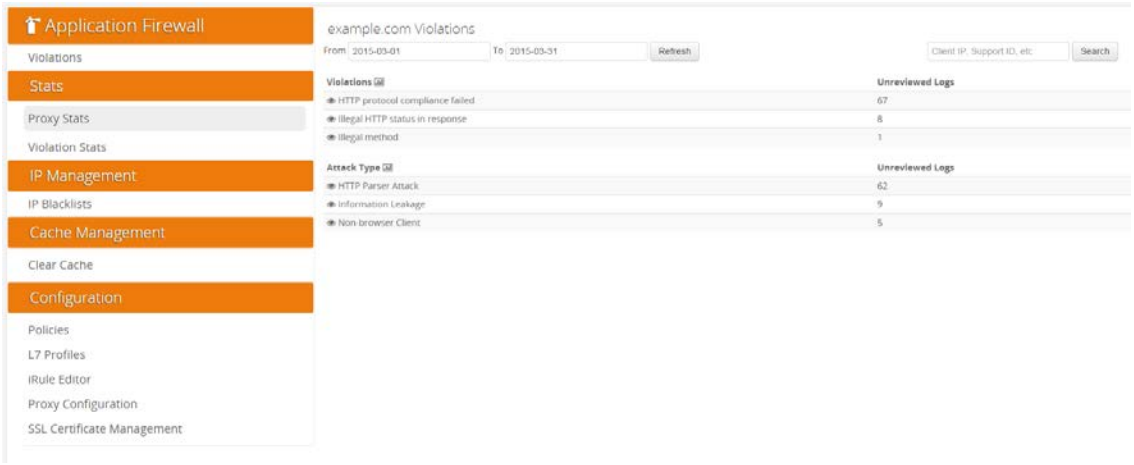


3. Change, or request that your DNS provider to change, the DNS for the domain and point to the IP address(es) provided by F5.
4. Optionally, the customer can request their carrier to implement an Access Control List (ACL), which whitelists F5 IP addresses, blacklists all others from the general Internet, and protects the application's origin IP address.
5. The customer or F5 SOC analyst then creates a security policy to be used to protect the web application. A baseline is chosen to apply typical settings, based upon the technologies used by the application, for example, IIS/Apache, PHP, CGI, MySQL, MS-SQL, ASP, JSP…

6. The F5 SOC will then assists in deploying the policy to the system and applies it to the proxy. It is possible to specify different policies per-URL and per-Host, in case a number of web applications with differing protection requirements are hosted under a single FQDN.

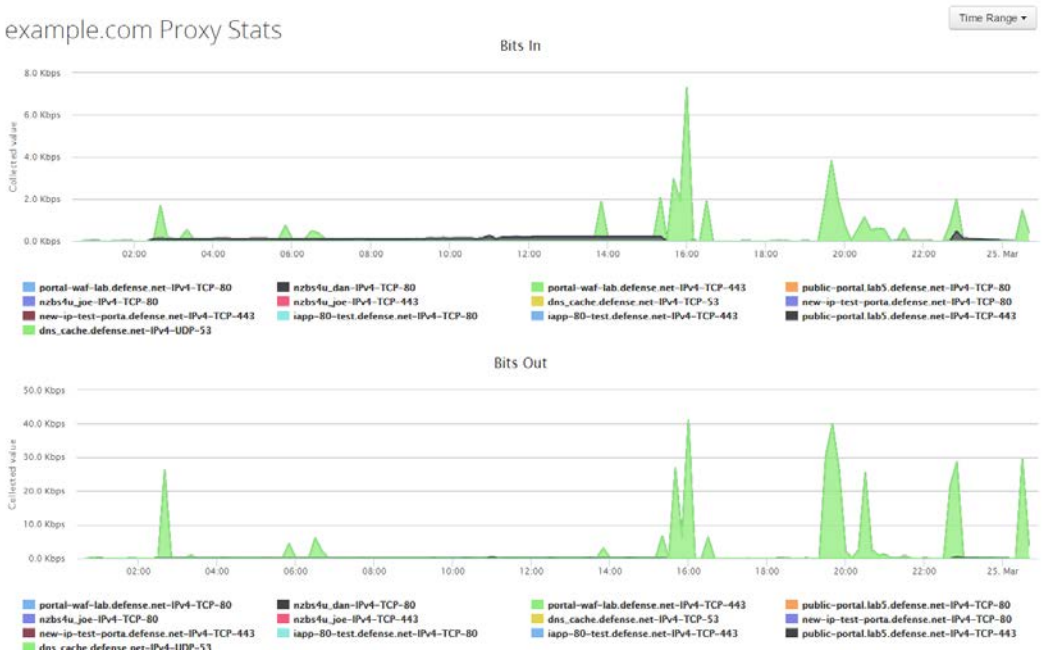


7. In a typical deployment scenario, a WAF policy is initially be deployed in Learning Mode, meaning that it does not block traffic, but will generates log alerts when a request causes a violation that *would* have been blocked. The customer needs to generate realistic web application traffic through the protected proxy while it is in Learning mode. As such, the F5 SOC works with the customer to determine whether particular requests are valid for the web application. Either the SOC analyst or the customer can mark individual violations as **Block** or **Allow**, which updates the policy iteratively.



8. This process repeats until the F5 SOC and customer are satisfied that the policy is ready to move to Blocking mode. After this stage, requests that violate the policy are blocked as well as logged.

9. Detailed statistics are available in the Silverline® Customer Portal



Legal Notices

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at http://www.f5.com/about/guidelines-policies/patent