Profense™ Features

Protecting and securing websites and web applications can be a complicated business. Profense web application firewall simplifies protection with an affordable and easy to use, feature rich, solution that gives you full PCI DSS 1.1 and 1.2 section 6.6 compliance. To make it easy, we put this all together in an easily configurable software solution with its own hardened OS (the ultra secure OpenBSD) to allow easy install and the ability to use it in your production, development and staging environments with only one license saving you tens of thousands of dollars.

Filtering

Positive and negative URL filtering

Profense™ validates all parts of a HTTP request (including the path, query and segment) according to the defined access policy. Requests not-matching the access-policy, are per default flagged as illegitimate, rejected and logged for further analysis. This allows system administrators to have a strict white-list of legitimate URLs for a given web application.

Negative URL matching allows for a less fine grained global policy. Policy rules can be specified using a combination of positive matching for specific URL and negative for all other.

Positive and negative query filtering

Profense™ validates all parts of a query in a URL request according the defined white-list access policy.

Negative matching of parameters allows for less fine grained general policies in combination with positive policy rules for specific parameters.

Positive and negative web services requests filtering

XML (including XML-RPC and SOAP) and JSON services are supported.

Profense validates all parts of a web services request according the defined access policy.

Web services requests are mapped as queries and as with normal queries combinations of negative and positive policy rules can be enforced.

HTTP headers compliance checking

Profense™ can enforce pragmatic and strict standard HTTP headers compliance (RFC2068/RFC2616).

Output filtering and rewriting

Profense™ allows for parsing and rewriting the body of server responses. This is useful for screening (and replacing) output for confidential data like credit card numbers in order to provide a last resort for preventing information leakage.

Session validation and CSRF protection

Profense™ protects against session hijacking and CSRF (Cross Site Request Forgery) by injecting cryptographic validation cookies and parameters to responses from the web system.

Session and CSRF protection policies are built automatically by the Learner.

DoS mitigation

Profense™ mitigates the effect of DoS and DDoS attacks by limiting the number of concurrent TCP connections and the rate at which connections can be established on a source IP basis. The limits are configurable.

Network level blocking

Instead of denying the request at the application level Profense can be configured to automatically create network firewall policy rules that blocks IP addresses at the network level if attacks exceeding a certain risk level are denied.

Web server cloaking and isolation

Profense™ completely isolates the web server from direct Internet requests and information and web system technology information is removed from web server responses.

Load balancing

HTTP and HTTPS request switching

Load balancing is performed on layer 7 based on the http request.

Round robin load balancing

Requests are distributed equally in a round robin fashion to all active servers.

Session persistence

When a server is selected according to the methods above all subsequent requests for the same client can be sent to the same physical server in order keep state information for that client on that server. This method is also referred to as client stickyness.

Health checking

Profense proactively checks backend web server availability and allows programmed event based disabling of failed or overburdened web servers with immediate alerting of the event via email or Syslog. HTTP response code and response body checksum methods are supported.

Policy management

Adaptive learning with instant protection
Profense™ offers Auto mode using a combination of positive and negative policy rules with adaptive learning of changes in the web applications. The Auto mode provides instant protection which improves as Profense learns the web applications and consequently can create positive policy rules for critical application components.

Automated Policy Generation
Profense™ automatically generates access policies for even complex web applications and web systems.

Regular expressions support
Profense™ has full support for standard PCRE (Perl Compatible Regular Expressions).

Global URL wild-cards
In order to simplify the ACL Profense™ supports the definition of URL wild cards based on regular expressions which matches URLs without parameters on a proxy global basis.

URL wild-cards are built automatically by the web site analyzer engine.

Global parameter wild-cards
Rules which match parameters on a global basis can be specified using regular expressions.
Parameter wild cards are built automatically by the web site analyzer engine.

Class based input validation
Filtering rules can be specified using classes for easy administration. Classes are defined globally and can be applied both when manually editing the access policy, when the access policy is built automatically and when rules are added or modified from log.

Web acceleration

HTTP Compression
Dynamic compression of transmission data reduces bandwidth consumption by 30 to 60% and increases transfer rate by 50 - 100%.

Caching of static and dynamic content
Configurable caching of static and dynamic documents off-loads web servers and improve the ability to handle peak situations.

SSL termination
SSL termination off-loads web servers from the burden of encrypting and decrypting. Re-encryption is optional.

TCP connection off-loading
When forwarding legitimate requests from clients to back-end web servers, Profense will reuse socket connections already established with the back-end web server.

Log function

Profense Management Dashboard
The Profense Management Dashboard presents system and website statistics and events in an aggregated view allowing for rapidly identifying and focusing on the most important events. The website deny log Dashboard give greater visibility to threatening activity and allow for aggregate and individual website deny log viewing, highly specific policy building and highly configurable event reporting. The Profense Dashboard allows for individual and cross website analysis.

Attack classification
All rejected requests are classified in major attack groups (i.e. SQL-injection, buffer overflow, etc.) using a combination of cross validation, heuristic patterns and statistics.

External notification
Alerts can be sent to external syslog server or email. Alert levels are completely configurable and are mapped to standard syslog priorities (information levels).

Deny log
The management interface includes a comprehensive security log displaying all the necessary details about blocked requests, including the time stamp, IP address, HTTP methods, path and query segments, HTTP headers violations, attack classification and raw request data.

Access log
The access log includes information about all requests including request, ip-address, timestamp, response size, response time, server response error code and caching status.

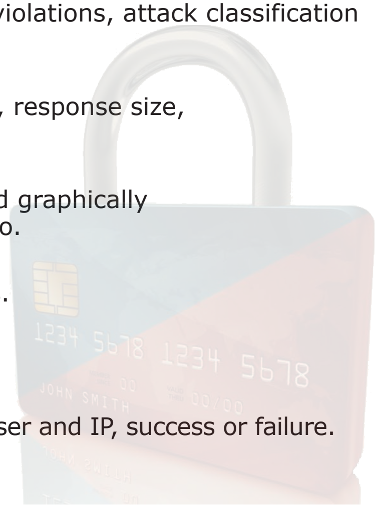
Traffic statistics
Traffic statistics are generated for 8 hour, 24 hour, week and month intervals. Data are displayed graphically and includes served requests, caching and compression ratio and web server response code ratio.

Customizable search criteria
Multiple search criteria can be specified using wildcards allowing for detailed drill down searches.

Customizable reporting
All log views (search filter sets) can be exported to printable reports or XML

Audit logging
All administrative actions are logged to a system log with requested action, payload (what to do), user and IP, success or failure.

The audit log and other system logs can be sent to an external Syslog server.



Operation

Automated remote backup

The complete running Profense™ installation including all settings, proxies and access policies can be automatically backed up by Profense™ to a remote FTP server.

Manual full and partial backup

A complete Profense™ installation or the entire configuration of a single proxy can also be backed up manually with a few clicks in the management interface.

Easy restore

A complete Profense™ configuration including access policy for all defined proxies can be restored from an FTP-server or the file system with a few clicks in the management interface.

Scalability and availability

Policy synchronization

All policy changes are automatically synchronized across the nodes in a Profense™ cluster.

High availability

Profense™ can be run in active/passive configurations where two or more physical Profense™ nodes together comprise a logical Profense™ unit with automatic fail-over.

Clustering

Active/active clustering with automatic policy synchronization allows for virtually unlimited scalability. No additional load balancer is required as Profense™ is "self load balancing".

Requirements compliance

OWASP Top Ten

Defenses against all OWASP Top Ten vulnerabilities.

PCI DSS 1.1 and 1.2 section 6.6 requirements

Profense™ provides full PCI DSS 1.1 and 1.2 section 6.6 requirements compliance.

For more information, contact us
by e-mail at sales@symtrex.com
or call us toll-free at 1.866.431.8972

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
sales@symtrex.com
www.symtrex.com

symtrex inc.
Network Security Specialists

Who's Watching Your Network?