

Information Technology Policy

Enterprise Web Application Firewall

<i>ITP Number</i> ITP-SEC004	<i>Effective Date</i> January 15, 2010
<i>Category</i> Recommended Policy	<i>Supersedes</i>
<i>Contact</i> RA-ITCentral@pa.gov	<i>Scheduled Review</i> Annual

This Information Technology Policy (ITP) establishes policy and enterprise-wide standards for Web Application Firewalls.

1. Purpose

Web application firewalls address the needs of limiting Internet attacks and monitoring of Web applications located in the commonwealth. This Information Technology Policy (ITP) establishes the policy and enterprise-wide standards for web application firewalls. A web application firewall provides a number of key benefits to the commonwealth's Enterprise Server Farm (ESF) and the agencies that house web applications there. These benefits include:

- Protecting against web attacks.
- Minimizing the threat window for each exposure by blocking access to vulnerability until the vulnerability can be fixed in the source code.
- Meeting PCI compliance requirements.
- Monitoring end-user's transactions with a web application.
- Providing an additional layer of web application hardening.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction are strongly encouraged to follow this ITP.

3. Objective

To establish policy and enterprise-wide standards for use of the web application firewalls.

4. Policy

In order to ensure the highest levels of security and overall effectiveness of protecting Internet-facing web applications, compliance rule sets will be invoked by Office of Information Security to automatically block attacks coming from the Internet. Internet-facing web application located in commonwealth datacenters are encouraged to use the web application firewall standard for protecting sensitive information or information classified by the data owner that meets the criteria for an Internet attack.

- A business-determined mission critical Internet-facing web application infrastructure can be secured by either a hardware or software form factor.
- The web application firewall may not disallow an authorized request from an Internet user and may not affect legitimate business traffic in the IT infrastructure while protecting web applications.
- The web application firewall default configuration must be able to monitor and prevent specific web application attacks until emergency patches and or source-code changes can be made to the vulnerable web application.
- The default web application rule configuration must be able to monitor and immediately block types of Web attacks targeting the web application.
- A SSL certificate is required by the web application firewall to inspect data passed between the Web servers.
- The web application firewall must be able to track, log, and inspect the following information relating to the web applications access by the end-user:
 - Application layer network traffic;
 - External and internal user sessions;
 - External and internal user-encrypted sessions;
 - Simulated attacks;
 - Blocked attacks; and
 - HTTP, HTTPS, Proxy error logging.
- Real-time automated failover architecture is required when web application firewall is integrated inline and could impact the flow of business-critical network traffic.

Monitoring

In accordance with the Commonwealth of Pennsylvania Information Technology Acceptable Use Policy, Management Directive 205.34, *CoPA Information Technology Acceptable Use Policy*, communication with a commonwealth authorized user may be audited by the Office for Information Security on a random basis to ensure compliance with set Web application firewall protection rules.

5. Product Standards for Web Application Firewalls

CURRENT STANDARDS

(These technologies or products meet the requirements of the current architecture and are recommended for use.)

Technology or Product	Product or Platforms	Technology Classification
iMPERVA (SecureSpere)	Hardware based (Appliance)	Current
Fortify (360 Application Defense Module)	Software based (Agent)	Current

CONTAIN

(These technologies or products no longer meet the requirements of the current architecture and are not recommended for use. They are to be phased out over time. No date has been set for their discontinuance.)

Technology or Product	Product or	Technology Classification
------------------------------	-------------------	----------------------------------

	Platforms	
--	--	Contain

RETIRE

(These technologies or products are being phased out. Plans are to be developed for their replacement, especially if there is risk involved, such as lack of vendor support. A date for retirement has been set.)

Technology or Product	Product or Platforms	Technology Classification
--	--	Retire mm/dd/yy

EMERGING / RESEARCH

(Emerging technologies have the potential to become current standards. At the present time, they are to be used only in pilot or test environments where they can be evaluated. Use of these technologies is restricted to a limited production mode, and requires approval of a waiver request. Research technologies are less widely accepted and time will determine if they will become a standard.)

Technology or Product	Product or Platforms	Technology Classification
--	--	Emerging / Research

6. Web Application Firewall Compliance Standards

This minimum compliance standard is intended to provide a default set of Web application firewall protection rules to protect commonwealth confidential data from Internet web attacks. The minimum Web application compliance standard consists of protection categories with the following settings:

Web Application Firewall Standard Protection (A shaded category indicates blocking is enabled for the protection rule)	
Category type for a protection rule	Counter measures
Application Buffer Overflow	Sending too much data in a request to the application.
Cross-site scripting (XSS)	Inserting scripting language into text fields to be displayed to other users.

Cookie Poisoning	Modifying the cookie file causing the return of unauthorized information or enabling performance of activity on behalf of another user.
Forceful Browsing	Gaining access to the constrained areas in a Web server directory.
Hidden Field Manipulation	Modifying form fields allowing damaging data to pass to the Web application.
Parameter Tampering	Modify the parameters being passed as part of the URL.
Stealth Commanding (e.g., SQL/OS Injections)	A code injection technique that exploits a security vulnerability occurring in the database layer of an application.
URL & Unicode encoding	Encoding certain characters in the URL to bypass application filters, thus accessing restricted resources on the Web server.

No “protection rules” may appear before this enterprise “protection rules” without approval from Office for Information Security.

Agencies may request additional “protection rules” for their agencies’ business requirements by contacting the Office for Information Security.

7. Responsibilities

The commonwealth's Chief Information Security Officer (CISO) will regularly audit for compliance with this policy and its associated standards.

Agency Information Security Officers (ISO's) or designates are to ensure agency internet traffic is in accordance with this policy.

8. Related ITPs/Other References

- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- MD 205.34 - *CoPA Information Technology Acceptable Use Policy*

9. Authority

- Executive Order 2011-05, Enterprise Information Technology Governance

10. Publication Version Control

It is the user’s responsibility to ensure they have the latest version of this publication. Questions regarding this publication are to be directed to RA-itcentral@pa.gov.

This chart contains a history of this publication’s revisions:

Version	Date	Purpose of Revision
Original	1/15/2010	Base Document
	4/2/2014	ITP Reformat; Merged OPD-SEC004B, STD-SEC004A into ITP