设置 FortiWeb Offline 自学习

说明：

本文档针对 FortiWeb Offline 自学习配置进行说明。Offline 自学习指 FortiWeb 通过交换机的端口镜像功能分析 Web 服务器的双向流量，自动学习 Web 服务器的 url 访问记录，http 访问方法，攻击记录和页面参数输入规则等 http 信息，并生成流量日志和攻击日志的过程。自学习一段时间后 FortiWeb 可以根据自学习结果生成推荐配置，再切换到 Inline 或透明模式，就可以保护 Web 服务器安全。

环境介绍：

本文使用 FortiWeb1000B 做演示。本文使用的系统版本为 4.0.。

步骤一：部署方式

Offline 即旁路方式指将 FortiWeb 与交换机相连，在交换机上使用端口镜像功能，让到达和流出 Web 服务器的双向流量都复制一份给 FortiWeb。

步骤二：配置模式

在系统—状态中可以看到工作模式

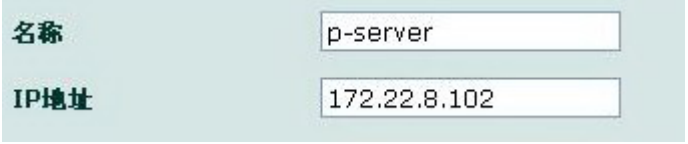
如果不是离线模式，点击更改，将模式改为离线

步骤三：配置服务器

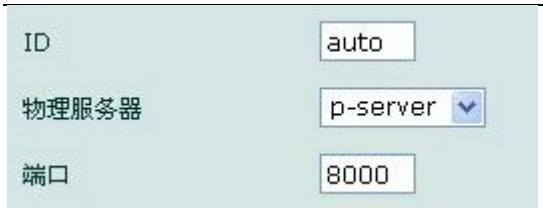
在服务器策略—服务器中设置

虚拟服务器：在 Offline 状态下只要确定连接交换机的接口即可，IP 任意填写

物理服务器：指向真实的 Web 服务器地址



服务器 Farm：指定 Web 服务器的端口号，其他选项不用配置



步骤四：配置自学习内容表

在自动学习—默认自动学习规范中输入名称，选择离线检测模式

步骤五：配置策略

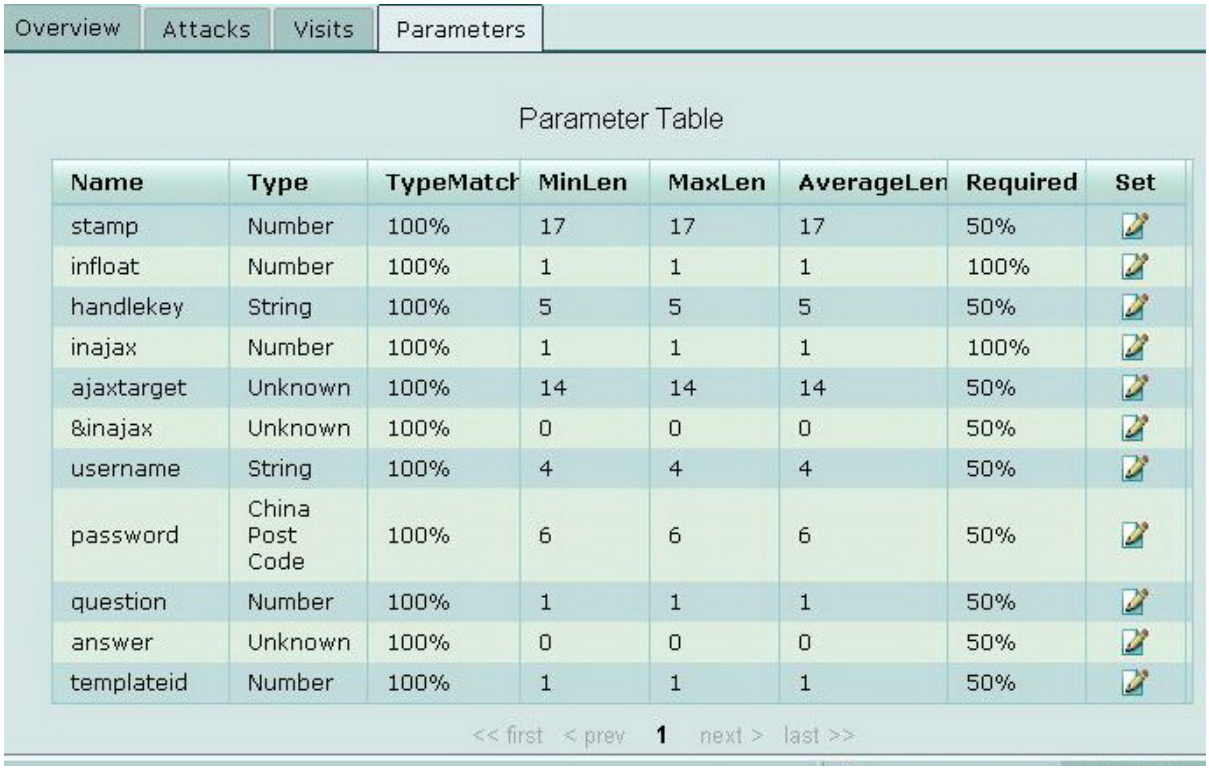
在服务器策略—策略中点击新建，选择步骤三中定义好的虚拟服务器和服务器 Farm，选择步骤四中定义好的 Web 保护规范和 WAF 自学习规范。

步骤六：察看自学习内容

在自动学习—自动学习报告中点击 

察看报告。报告中记录了用户访问过的所有 URL、产生的攻击和页面的参数记录。

点击一个页面在参数中可以参看该页面参数规则。



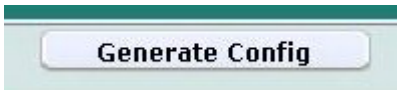
步骤七：察看日志

在日志—攻击中可以察看攻击日志

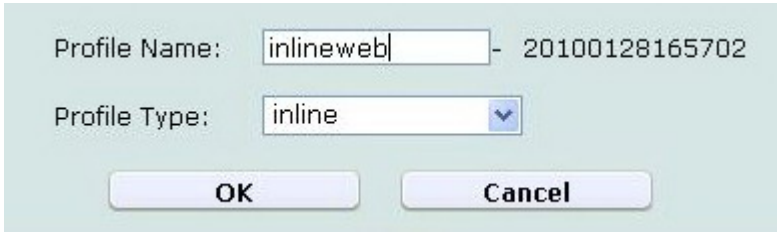
Source	Destination	Policy	Message	Packet Log
172.22.8.1	172.22.8.102	policy1	SQL Injection: Blind SQL Injection	
172.22.8.1	172.22.8.102	policy1	SQL Injection: Blind SQL Injection	
172.22.8.1	172.22.8.102	policy1	XSS: Common XSS	
172.22.8.1	172.22.8.102	policy1	DETECT_RESPONSE_INFORMATION_disclosure	
172.22.8.1	172.22.8.102	policy1	DETECT_RESPONSE_INFORMATION_disclosure	
172.22.8.1	172.22.8.102	policy1	DETECT_RESPONSE_INFORMATION_disclosure	
172.22.8.1	172.22.8.102	policy1	DETECT_RESPONSE_INFORMATION_disclosure	

步骤八：生成自学习配置

在自学习报告中点击生成配置



输入配置名称，配置类型选择 inline，因为 offline 自学习是为 inline 模式作准备



在 Web 保护—Web 保护规范—inline 保护规范中察看生成的配置