设置 FortiWeb Inline 自学习

说明：

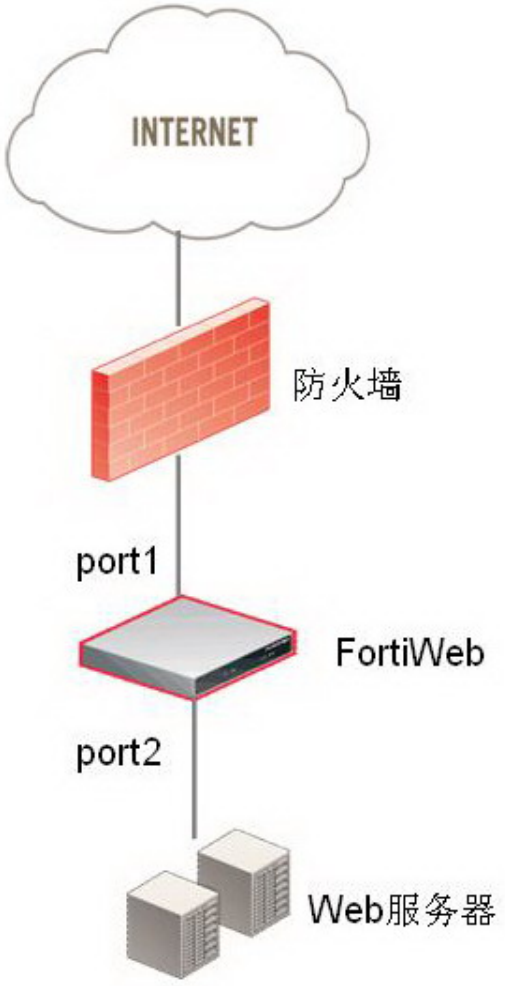
本文档针对 FortiWeb Inline 自学习配置进行说明。Inline 自学习指 FortiWeb 显式部署在服务器和防火墙之间，通过代理 HTTP 流量，自动学习 Web 服务器的 url 访问记录，http 访问方法，攻击记录和页面参数输入规则等信息，并生成流量日志和攻击日志的过程。自学习一段时间后 FortiWeb 可以根据自学习结果生成推荐配置，将配置加载到服务器策略就可以保护 Web 服务器安全。

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

如下图所示，FortiWeb 的 port1（管理）接口与上游交换机连接，port2 接口与下游服务器连接。防火墙将公网地址映射给虚拟服务器（V-server）, FortiWeb 将虚拟服务器和物理服务器（P-server）关联，显式代理 HTTP 流量。



步骤二：配置模式

在系统—状态中可以看到工作模式

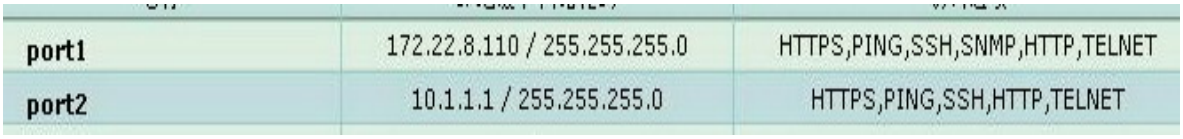
如果不是透明模式，点击更改，将模式改为透明模式

步骤三：配置接口 IP

在系统—网络—接口中点击配置。

Port1：与上游交换机连接

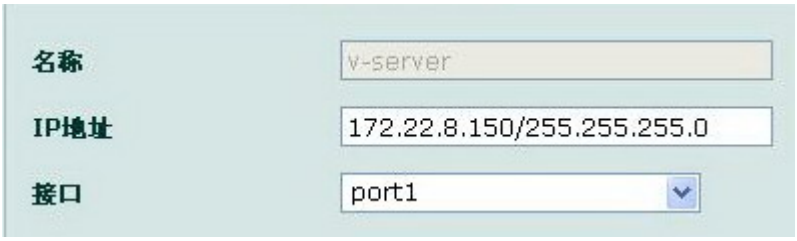
Port2：与下游服务器连接。服务器的网关要配成 port2 接口 IP 地址。



步骤四：配置服务器

在服务器策略—服务器中设置

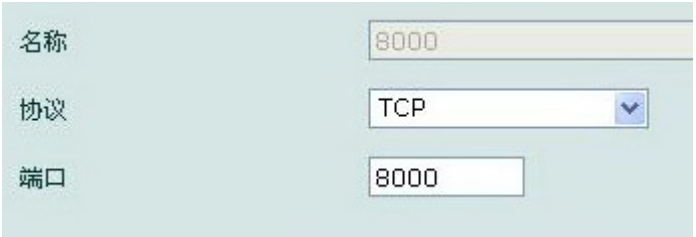
虚拟服务器：防火墙将公网地址映射给的私网 IP 地址，并选择上游接口



物理服务器：指向真实的 Web 服务器地址

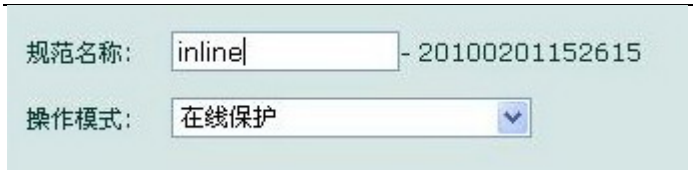
服务：使用的 tcp 端口，预定义为 80 和 443，本例使用 8000 端口

在服务器策略—服务—自定义中设置



步骤五：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，选择在线保护



步骤六：配置策略

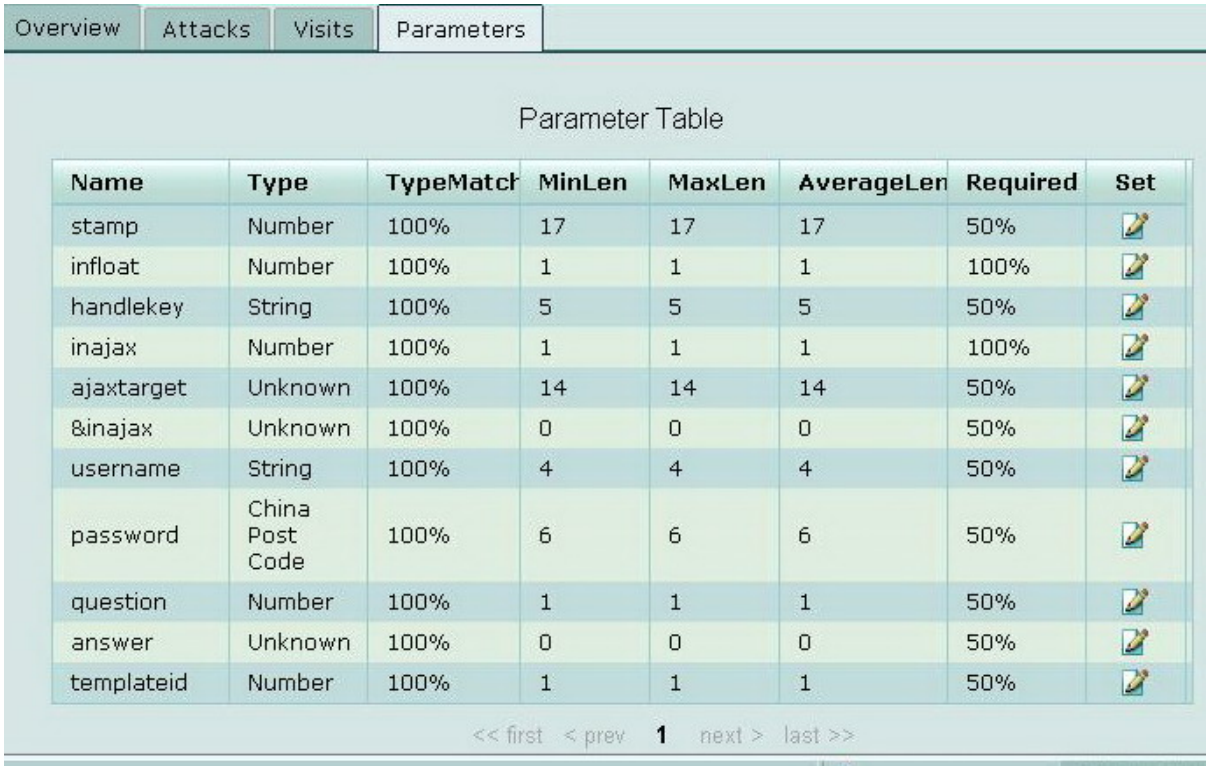
在服务器策略—策略中点击新建。选择步骤四中定义好的虚拟服务器、物理服务器和服务；设置服务器端口，本例为 8000；选择步骤五中定义好的 Web 保护规范和 WAF 自学习规范。

步骤七：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。



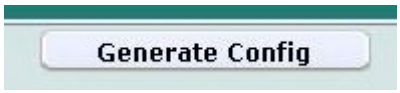
步骤八：察看日志

在日志—攻击中可以察看攻击日志

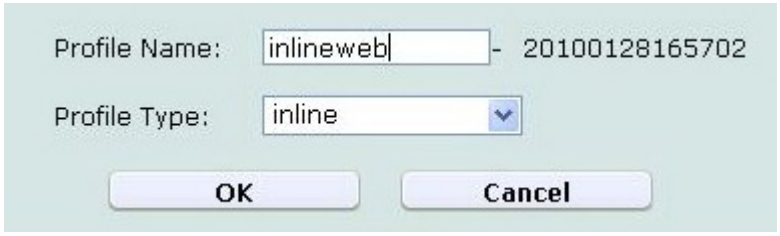
Source	Destination	Policy	Message	Packet Log
172.22.8.1	172.22.8.102	policy1	SQL Injection: Blind SQL Injection	
172.22.8.1	172.22.8.102	policy1	SQL Injection: Blind SQL Injection	
172.22.8.1	172.22.8.102	policy1	XSS: Common XSS	
172.22.8.1	172.22.8.102	policy1	DETECT_RESPONSE_INFORMATION_disclosure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

步骤九：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