

## 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

在系统一状态中可以看到工作模式

操作模式      离线检测 **[更改]**

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

在服务器策略一服务器中设置

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

名称	v-server
IP地址	1.1.1.1/255.255.255.0
接口	port1

物理服务器：指向真实的 Web 服务器地址

名称	p-server
IP地址	172.22.8.102

服务器 Farm：指定 Web 服务器的端口号，其他选项不用配置

ID	auto
物理服务器	p-server
端口	8000

**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

规范名称:	offline - 20100127155945
操作模式:	离线检测

**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。

策略名称	policy1
策略类型	Web保护
虚拟服务器	v-server
模式	Offline Detection
服务器Farm	farm
保护的服务器	[选择...]
Web保护规范	offline20100127160003
WAF自学习规范	offline20100127160003
URL大小写敏感	<input type="checkbox"/>

**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。

The screenshot shows the Fortinet web interface for the URL `/login.aspx` on IP `172.22.8.102:8000`. The interface includes a left sidebar with a file tree and a main content area with tabs for Overview, Attacks, Visits, and Parameters. The Overview tab is active, displaying an "Overview Table" with the following data:

Item	Value	More
Web Domain	172.22.8.102:8000	
URL	/login.aspx	
<a href="#">Hits Count</a>	2	13.3 % of total accesses
<a href="#">Attack Count</a>	0	0 % of total attacks

点击一个页面在参数中可以参看该页面参数规则。

The screenshot shows the Fortinet web interface for the URL `/login.aspx` on IP `172.22.8.102:8000`. The interface includes a left sidebar and a main content area with tabs for Overview, Attacks, Visits, and Parameters. The Parameters tab is active, displaying a "Parameter Table" with the following data:

Name	Type	TypeMatch	MinLen	MaxLen	AverageLen	Required	Set
stamp	Number	100%	17	17	17	50%	
infloat	Number	100%	1	1	1	100%	
handlekey	String	100%	5	5	5	50%	
inajax	Number	100%	1	1	1	100%	
ajaxtarget	Unknown	100%	14	14	14	50%	
&inajax	Unknown	100%	0	0	0	50%	
username	String	100%	4	4	4	50%	
password	China Post Code	100%	6	6	6	50%	
question	Number	100%	1	1	1	50%	
answer	Unknown	100%	0	0	0	50%	
templateid	Number	100%	1	1	1	50%	

<< first < prev 1 next > last >>

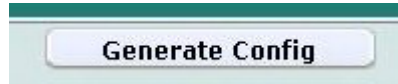
### 步骤七：察看日志

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

Profile Name:  - 20100128165702

Profile Type:  ▼

在 Web 保护—Web 保护规范—inline 保护规范中察看生成的配置

**Inline Protection Profile**

#	Name	Se Mana
1	inlineweb20100128165714	Di