

第一阶段-WAF 评分标准

24、公司内部有一台网站服务器直连到 WAF，地址是 RS 上 VLAN10 网段内的第五个可用地址，端口是 8080，开启记录访问日志和记录防护日志；配置将服务访问日志、WEB 防护日志、服务监控日志信息发送 syslog 日志服务器，IP 地址是 VLAN10 内第六个可用地址，UDP 的 514 端口；

共 8 分，共 2 处。

1.4 分

编辑服务

* 服务名称：	web
服务类型：	HTTP
* 主机地址：	10.80.0.5 <small>点分十进制整数，形如：192.168.23.4</small>
* 主机端口：	8080 (1~65535)
域名：	
策略集：	P-xxx
字符集：	utf-8
MAC绑定：	<input type="checkbox"/> 启用服务与MAC地址绑定
* 记录访问日志：	<input checked="" type="radio"/> 是 <input type="radio"/> 否
* 记录防护日志：	<input checked="" type="radio"/> 是 <input type="radio"/> 否
链路绑定：	br_default

2.4 分

基本配置 日志导出 日志清空 日志服务器							
日志服务器							
添加...							
序号	名称	服务器IP	端口	状态	协议类型	日志类型	操作
1	syslog	10.80.0.6	514	✓	udp	服务访问，WEB防护，服务监控	 

25、在公司总部的 WAF 上配置，阻止常见的 WEB 攻击数据包访问到公司内网服务器；

共 8 分，共 3 处。

第 1 处 2 分，第 2 处 3 分，第 3 处 3 分。

基本攻击防护

策略名称：

P-xxx

基本攻击防护

状态：

☒ 开启

☐ 关闭

选择是否开启基本攻击防护。推荐：是。

应答体检测

状态：

☐ 启用

是否启用应答体检测。此选项对性能有一定影响，建议在对应答时间没有特殊要求的情况下使用。

防护动作

动作：

阻止

防护动作可以选择允许（允许继续请求服务器资源），阻止（阻止请求，返回403页面，或，相应的错误过滤页面），重定向（重定向请求到配置的重定向URL），阻断（在设置的阻断时间内，阻止同源IP的请求）。

默认攻击防护类型

☒ SQL注入攻击防护

☒ 跨站脚本攻击防护

☒ 操作系统注入命令

☒ 远程文件包含攻击防护

☒ 目录遍历攻击防护

☒ 其他

创建自定义规则

规则名称：

规则名称用于识别自定义规则,最大长度为32

URI匹配：

/

对URI进行字符串匹配，大小写不敏感。如配置'/*',表示不对URI进行检测，最大长度为512。

高级匹配：

/

用于配置HTTP请求头域的检测规则，大小写不敏感

添加

自定义规则列表

规则名称	启用	URL匹配	高级匹配	操作
------	----	-------	------	----

确定

重置

26、配置暴力浏览攻击防护，单 IP 最大请求数 3000 次，防护动作为阻止；编辑防护策略，定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击，防护动作为阻止；

共 8 分，共 3 处。

1-2 处，每处 3 分。

暴力浏览攻击防护

请将配置项填写完整，否则防护不生效。

策略名称：P-xxx

暴力浏览防护

状态：

开启

关闭

选择是否开启暴力浏览防护。

单IP允许的最大请求数：

3000

请求计数的最大值，计数满足最大值时，将执行已配置的防护动作，数值范围：1-32767

防护动作

动作：

阻止

防护动作可以选择阻止（阻止请求，返回403页面，或，相应的错误过滤页面）。

确定

重置

3. 2 分

协议规范检测

策略名称：P-xxx

协议规范检测

状态：

开启

关闭

开启对HTTP协议各组成元素的长度限制功能。这些检查能够有效阻断缓冲溢出等攻击。推荐：是

请求头域值的最大长度：

8192

定义请求报头值的最大长度。推荐8192

请求头名称的最大长度：

64

定义报头名称的最大长度。推荐:64

请求头域的最大个数：

20

定义了一个请求能够包含的最多报头个数。推荐：20

请求体的最大长度：

256

请求body的最大长度。POST请求有一个包含表单参数和值的请求body。推荐：32768

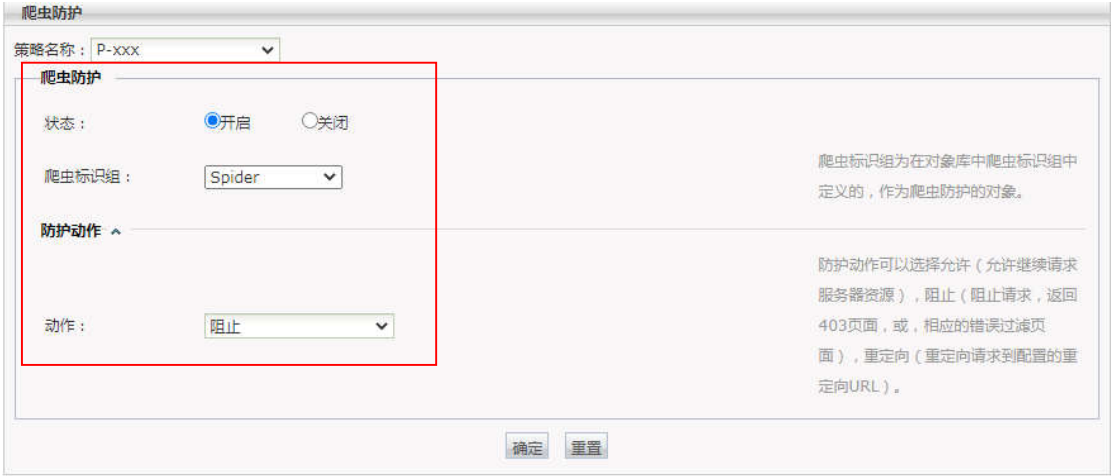
27、WAF 上配置开启爬虫防护功能，当爬虫标识为 Spider，自动阻止该行为；WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件；WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问*.bat 的文件；

共 8 分，共 4 处。

1.2 分



2.2 分



3.2 分

输入参数验证

策略名称：

P-xxx

参数验证

状态：

开启

关闭

防护动作

动作：

阻止

上传文件格式特征检测

DOC

DOCX

GIF

JPG

JPEG

PDF

PNG

RAR

XLS

XLSX

ZIP

未检测文件动作：

阻止

创建参数

类型	匹配方式	匹配表达式	操作
<div>查询参数名称</div>	<div>正则匹配</div>	<div></div>	<div>添加</div>
表单参数名称	字符串匹配	userName	<div></div>
表单参数值	字符串匹配	admin	<div></div>
表单参数值	正则匹配	admin	<div></div>

选择是否开启输入参数验证。推荐：是。

防护动作可以选择允许（允许继续请求服务器资源），阻止（阻止请求，返回403页面，或，相应的错误过读页面），重定向（重定向请求到配置的重定向URL）。

检测上传文件的格式特征，文件格式不正确，不允许其上传。

若上传文件格式特征检测都不勾选，则默认检测动作为允许。

用于检测请求的查询参数和表单参数，可选择正则匹配或字符串匹配。匹配表达式支持中英文字符，最长32字符。

确定

重置

4.2 分

黑白名单

策略名称：

P-block

黑白名单

状态：

开启

关闭

类型	黑白名单种类	匹配模式	值	操作
<div>黑名单</div>	<div>URI</div>	<div>正则匹配</div>	<div>*.bat</div>	<div>添加</div>
黑名单	URI	正则匹配	*.bat	<div></div>
黑名单	URI	字符串匹配	dvwa	<div></div>

确定

重置

28、WAF 上配置，使用 WAF 的漏洞立即扫描功能检测服务器（10.52.0.100）的安全漏洞情况，要求包括信息泄露、SQL 注入、跨站脚本编制；

共 8 分，共 2 处，每处 4 分。

编辑“漏洞扫描”任务

基本配置

任务名称：

scan

扫描目标：

10.50.0.100:80

执行方式：

☒ 立即执行

☐ 将来执行

☐ 周期执行

扫描内容：

☒ 信息泄露

☒ SQL注入

☐ 操作系统命令

☒ 跨站脚本编制

☐ 认证不充分

☐ 拒绝服务

高级配置

SSL链接：

☐ 启用

☒ 不启用

用于支持扫描以HTTPS协议访问的网站

登陆方式：

无认证

指定URI：

☐ 是

☒ 否

是否扫描指定的URI

忽略URI：

☐ 是

☒ 否

是否添加忽略的URI

是否发送扫描报告：

☐ 发送

☒ 不发送

是否发送扫描报告

确定

取消

29、在公司总部的 WAF 上配置，将设备占用空间和内存占用空间超过 50%时通过邮件（发送到 bn2021@digitalchina.com）及短信方式（发送到 13812345678）发送告警信息给管理员；
共 8 分，共 4 处，每处 2 分。

WEB攻击告警

网页篡改告警

设备状态告警

告警管理-设备状态告警

日志空间检测：

☒ 是

☐ 否

设备占用空间：

50

%

请在日志配置模块中编辑，超过此值

内存检测：

☒ 是

☐ 否

内存占用空间：

88

%

大小请输入 1 到 95(%)，超过此值

告警开关：

☒ 开启

☐ 关闭

发送间隔：

5

分钟

告警方式：

☒ 邮件

☒ 短信

接收邮箱：

bn2021@digitalchina.com

↑

↓

邮件之间用半角
仅允许输入10

接收手机号码：

13812345678

↑

↓

手机号码之间
仅允许输入10

保存

重置