FortiWeb 离线（offline）模式上线指南

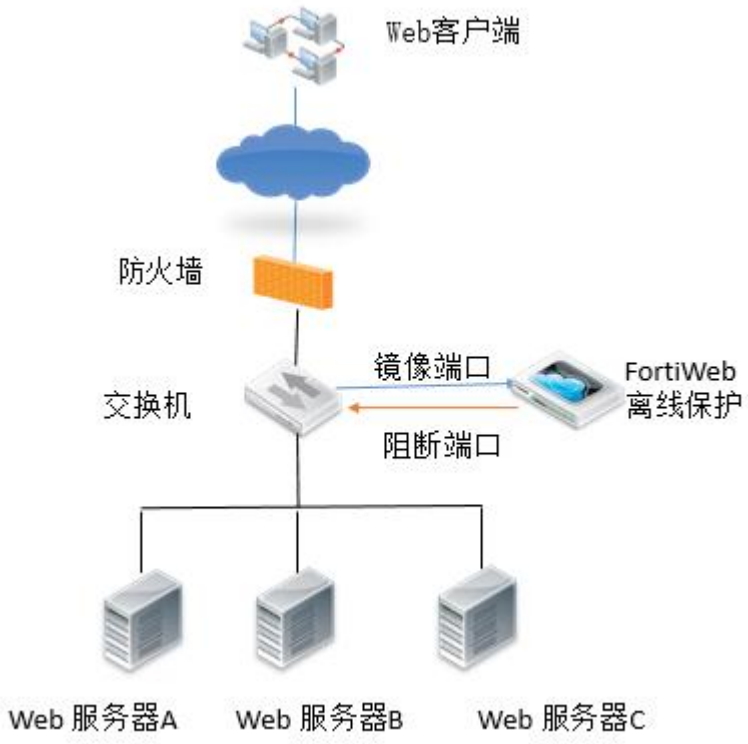
版本	1.1
时间	2016 年 12 月
支持的版本	FortiWeb -v5.0.x 以上
作者	李威峰
状态	草稿
反馈	support_cn@fortinet.com

目录

离线保护（offiline）模式介绍

离线模式（离线检测）即物理旁挂部署在网络上，即 Sniffer 模式，采用听的“抓包”方式对通过的流量进行分析，对检测到的攻击通过阻断端口发送 TCP-Reset 报文阻断，有很多功能上的限制。比如，对于 HTTPS 协商安全套件算法（Diffie-Hellman key exchanges），不能解密，这不是 FortiWeb 的本身的问题。

离线保护模式拓扑：



配置思路

1. 交换机镜像需要需要分析的流量给 FortiWeb。（如果有 vlan tag，不需要在 FortiWeb 上创建，FortiWeb 能够处理）。
2. 对需要保护的 HTTPS 业务，需要获取到服务器证书和服务器对应关系。

配置总步骤

1. 调整模式 FortiWeb 工作模式。
2. 配置物理服务器池。
3. 配置保护规范。
4. 配置策略。

HTTP 场景

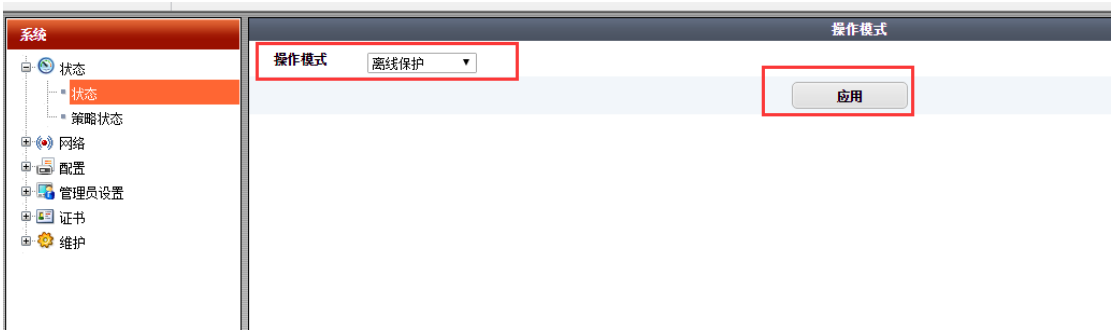
需求描述

FortiWeb 串接在防火墙和交换机中间，串接位置没有 vlan tag。

物理服务器服务			
客户端 IP	物理服务器 IP	物理服务器应用类型	物理服务器端口号
	192.168.10.13	HTTP	808

配置步骤

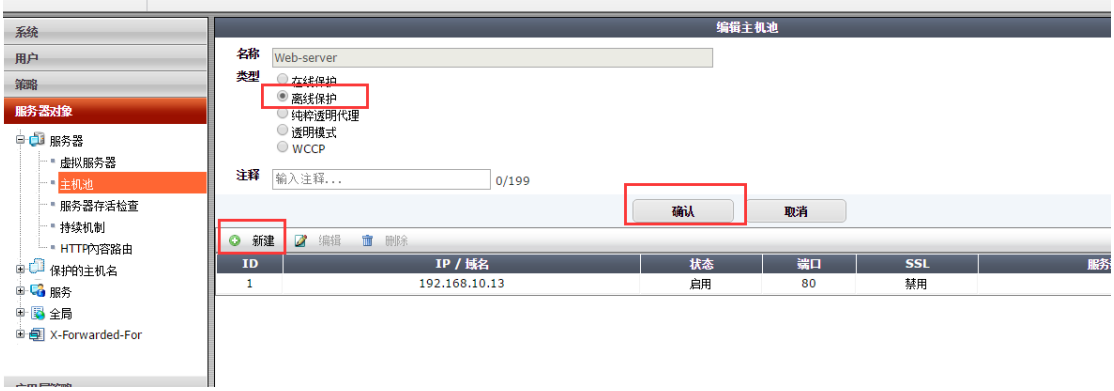
修改模式



修改模式为 离线保护（检测）模式。

配置主机池，即真实的物理服务器。

类型选择 离线保护，然后确认。

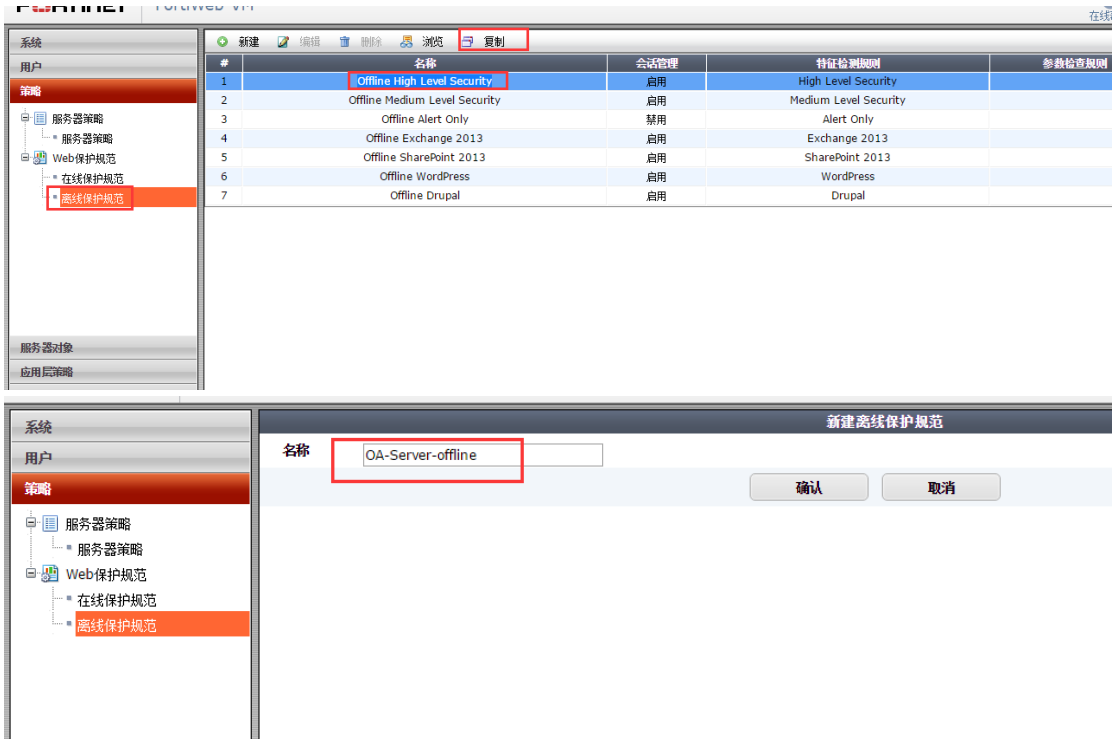


添加主机

建议把类型相同的服务器添加到一个主机池中，以减少策略条目。

配置 保护规范

因为离线保护不代理 HTTP 流量，是离线的，所以在离线保护规范 中 Copy 一个保护规范模板，copy Offline High Level Security 离线规范，



配置服务器策略

阻止端口和数据截获端口可以不是同一个接口。

服务器策略中的监视模式 ，监视模式含义是无论保护规范的命中特征的动作如何配置，都不阻断。建议不熟悉 FortiWeb 的同学一定要启用，以防止特征误报影响业务。

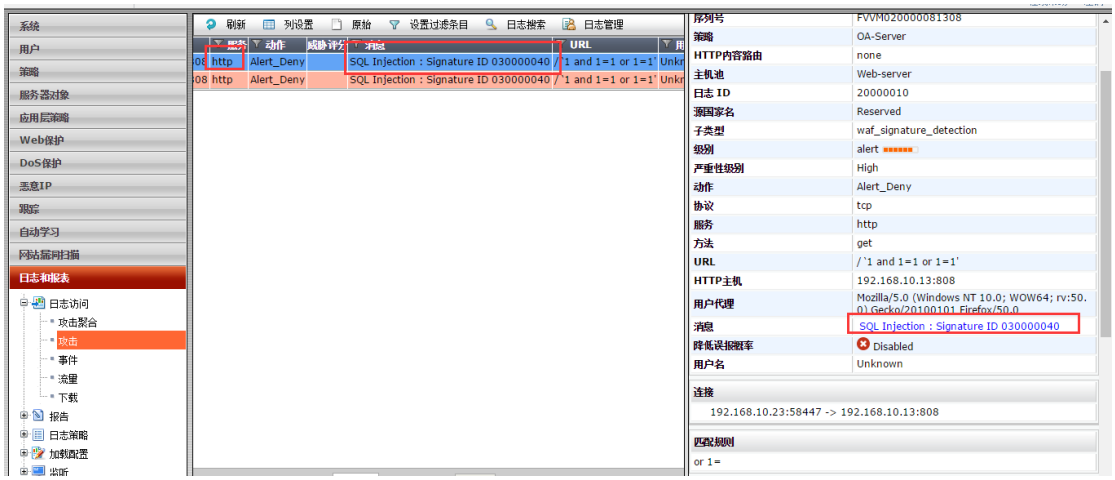
到此为止，配置基本结束。

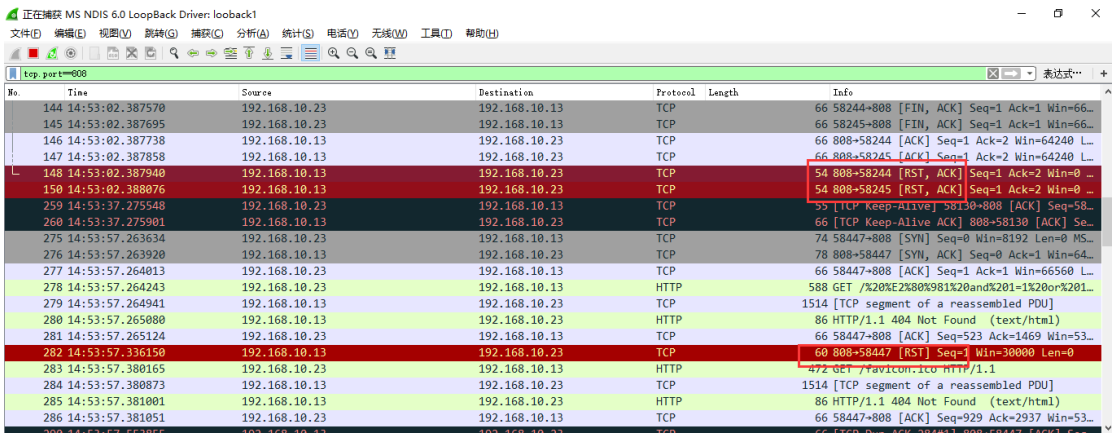
测试

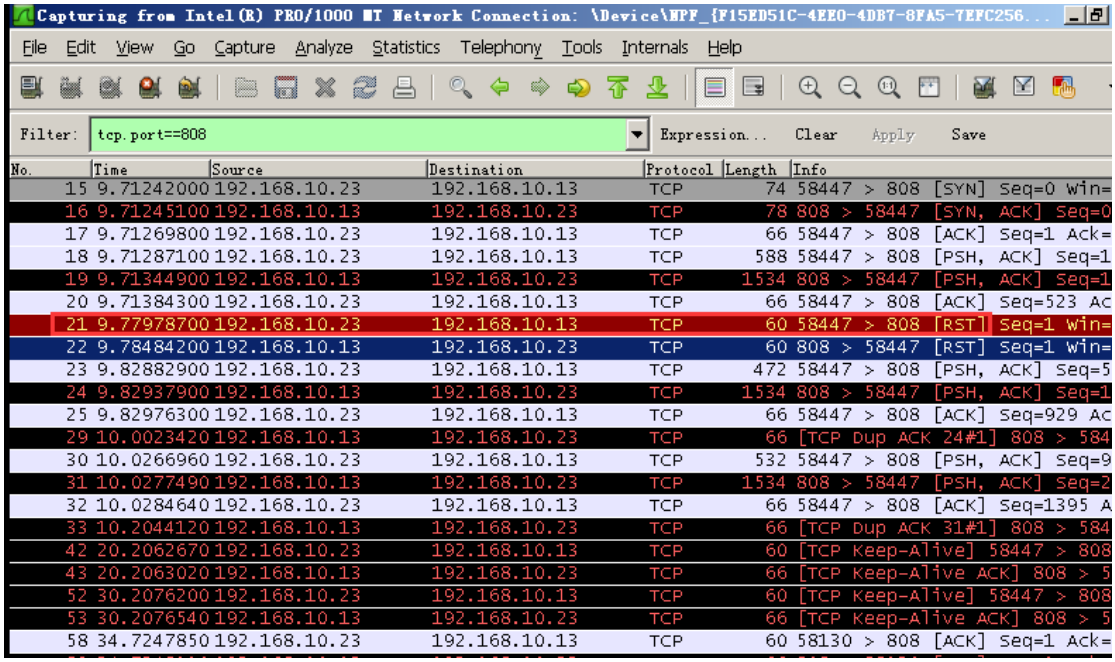
测试几种常见的攻击。

测试 SQL 注入

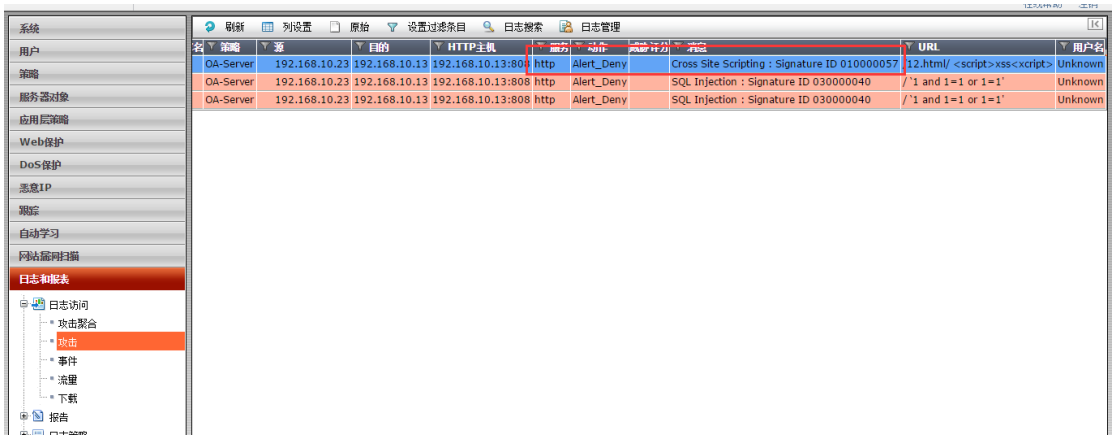
离线保护部署重写阻断页面，而是发 TCP-Reset 报文。




正在捕获 MS NDIS 6.0 LoopBack Driver: loopback1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp.port==808
No. Time Source Destination Protocol Length Info
144 14:53:02.387570 192.168.10.23 192.168.10.13 TCP 66 58244→808 [FIN, ACK] Seq=1 Ack=1 Win=66…
145 14:53:02.387695 192.168.10.23 192.168.10.13 TCP 66 58245→808 [FIN, ACK] Seq=1 Ack=1 Win=66…
146 14:53:02.387738 192.168.10.13 192.168.10.23 TCP 66 808→58244 [ACK] Seq=1 Ack=2 Win=64240 L…
147 14:53:02.387858 192.168.10.13 192.168.10.23 TCP 66 808→58245 [ACK] Seq=1 Ack=2 Win=64240 L…
148 14:53:02.387940 192.168.10.13 192.168.10.23 TCP 54 808→58244 [RST, ACK] Seq=1 Ack=2 Win=0 …
150 14:53:02.388076 192.168.10.13 192.168.10.23 TCP 54 808→58245 [RST, ACK] Seq=1 Ack=2 Win=0 …
259 14:53:37.275548 192.168.10.23 192.168.10.13 TCP 55 [TCP Keep-Alive] 58130→808 [ACK] Seq=58…
260 14:53:37.275901 192.168.10.13 192.168.10.23 TCP 66 [TCP Keep-Alive ACK] 808→58130 [ACK] Se…
275 14:53:57.263634 192.168.10.23 192.168.10.13 TCP 74 58447→808 [SYN] Seq=0 Win=8192 Len=0 MS…
276 14:53:57.263920 192.168.10.13 192.168.10.23 TCP 78 808→58447 [SYN, ACK] Seq=0 Ack=1 Win=64…
277 14:53:57.264013 192.168.10.23 192.168.10.13 TCP 66 58447→808 [ACK] Seq=1 Ack=1 Win=66560 L…
278 14:53:57.264243 192.168.10.23 192.168.10.13 HTTP 588 GET /%20%E2%80%981%20and%201=1%20or%201…
279 14:53:57.264941 192.168.10.13 192.168.10.23 TCP 1514 [TCP segment of a reassembled PDU]
280 14:53:57.265080 192.168.10.13 192.168.10.23 HTTP 86 HTTP/1.1 404 Not Found (text/html)
281 14:53:57.265124 192.168.10.23 192.168.10.13 TCP 66 58447→808 [ACK] Seq=523 Ack=1469 Win=53…
282 14:53:57.336150 192.168.10.13 192.168.10.23 TCP 60 808→58447 [RST] Seq=1 Win=30000 Len=0
283 14:53:57.380165 192.168.10.23 192.168.10.13 HTTP 472 GET /favicon.ico HTTP/1.1
284 14:53:57.380873 192.168.10.13 192.168.10.23 TCP 1514 [TCP segment of a reassembled PDU]
285 14:53:57.381001 192.168.10.13 192.168.10.23 HTTP 86 HTTP/1.1 404 Not Found (text/html)
286 14:53:57.381051 192.168.10.23 192.168.10.13 TCP 66 58447→808 [ACK] Seq=929 Ack=2937 Win=53…


Capturing from Intel(R) PRO/1000 MT Network Connection: \Device\NPF_{F15ED51C-4EE0-4DB7-8FA5-7EFC256...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.port==808
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
15 9.71242000 192.168.10.23 192.168.10.13 TCP 74 58447 > 808 [SYN] Seq=0 Win=
16 9.71245100 192.168.10.13 192.168.10.23 TCP 78 808 > 58447 [SYN, ACK] Seq=0
17 9.71269800 192.168.10.23 192.168.10.13 TCP 66 58447 > 808 [ACK] Seq=1 Ack=
18 9.71287100 192.168.10.23 192.168.10.13 TCP 588 58447 > 808 [PSH, ACK] Seq=1
19 9.71344900 192.168.10.13 192.168.10.23 TCP 1534 808 > 58447 [PSH, ACK] Seq=1
20 9.71384300 192.168.10.23 192.168.10.13 TCP 66 58447 > 808 [ACK] Seq=523 Ac
21 9.77978700 192.168.10.23 192.168.10.13 TCP 60 58447 > 808 [RST] Seq=1 Win=
22 9.78484200 192.168.10.13 192.168.10.23 TCP 60 808 > 58447 [RST] Seq=1 Win=
23 9.82882900 192.168.10.23 192.168.10.13 TCP 472 58447 > 808 [PSH, ACK] Seq=5
24 9.82937900 192.168.10.13 192.168.10.23 TCP 1534 808 > 58447 [PSH, ACK] Seq=1
25 9.82976300 192.168.10.23 192.168.10.13 TCP 66 58447 > 808 [ACK] Seq=929 Ac
29 10.0023420 192.168.10.13 192.168.10.23 TCP 66 [TCP Dup ACK 24#1] 808 > 584
30 10.0266960 192.168.10.23 192.168.10.13 TCP 532 58447 > 808 [PSH, ACK] Seq=9
31 10.0277490 192.168.10.13 192.168.10.23 TCP 1534 808 > 58447 [PSH, ACK] Seq=2
32 10.0284640 192.168.10.23 192.168.10.13 TCP 66 58447 > 808 [ACK] Seq=1395 A
33 10.2044120 192.168.10.13 192.168.10.23 TCP 66 [TCP Dup ACK 31#1] 808 > 584
42 20.2062670 192.168.10.23 192.168.10.13 TCP 60 [TCP Keep-Alive] 58447 > 808
43 20.2063020 192.168.10.13 192.168.10.23 TCP 66 [TCP Keep-Alive ACK] 808 > 5
52 30.2076200 192.168.10.23 192.168.10.13 TCP 60 [TCP Keep-Alive] 58447 > 808
53 30.2076540 192.168.10.13 192.168.10.23 TCP 66 [TCP Keep-Alive ACK] 808 > 5
58 34.7247850 192.168.10.23 192.168.10.13 TCP 60 58130 > 808 [ACK] Seq=1 Ack=

测试 XSS



测试 command 命令注入

略

HTTPS 场景

需求描述

FortiWeb 串接在防火墙和交换机中间，串接位置没有 vlan tag。

物理服务器服务			
客户端 IP	物理服务器 IP	物理服务器应用类型	物理服务器端口号
	192.168.10.13	HTTPS	443

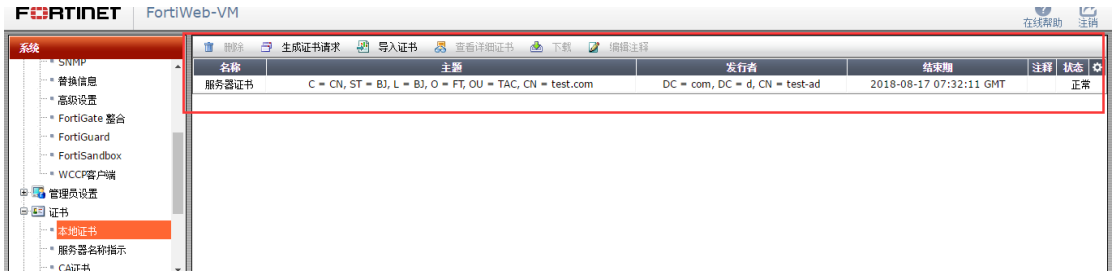
配置步骤

修改模式（略）

导入服务器相关证书

■ HTTPS 服务器证书（证书和 KEY）

FortiWeb 支持证书格式，PEM+KEY 或 PFX（证书和私钥放到一起）格式。



配置主机池，即真实的物理服务器。

配置主机池，因为业务为 HTTPS，所以要 enable SSL。

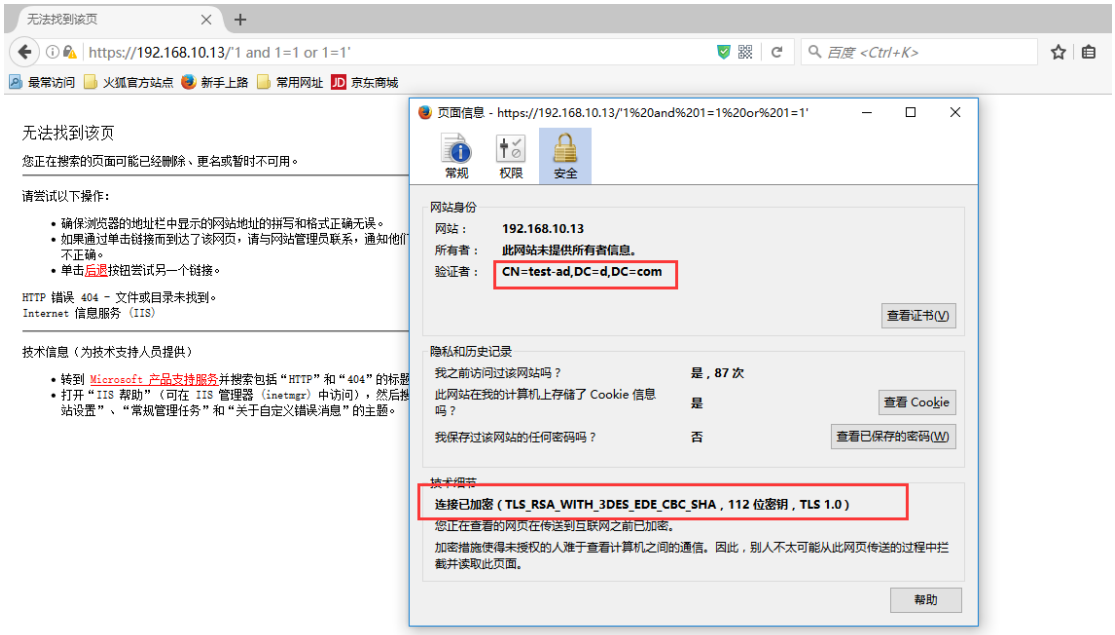
同时把服务器证书和该服务器对应，因为这个证书仅仅用于解密，不会发给客户端，所以没有必要配置中间证书链。

配置服务器策略（略）

测试

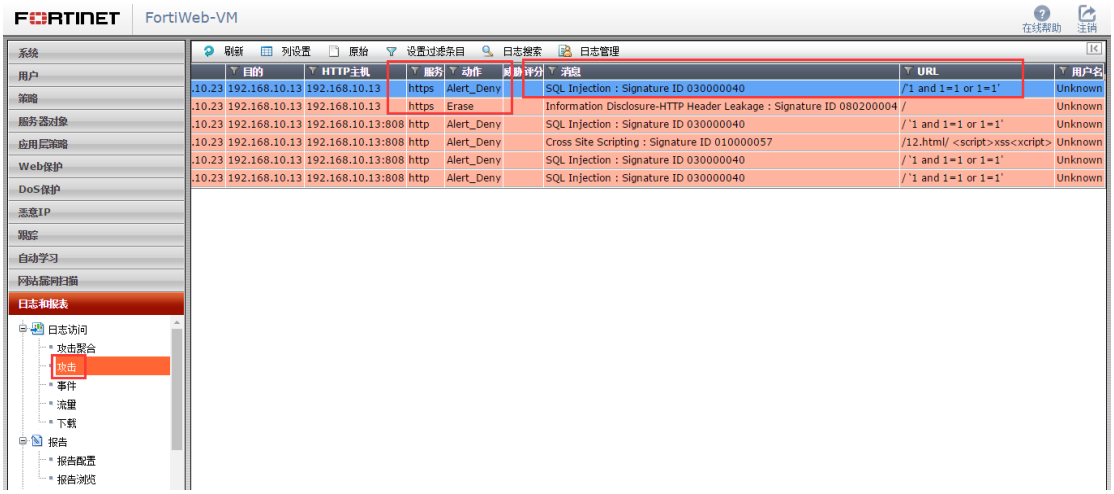
测试 SQL 注入

先观察协商的 HTTPS 协商的加密套件。



注意：对于 FortiWeb 工作在透明检测模式（Sniffer 监听模式），并非所有的加密套件都能解密，对于加密套件中有 DH 或 DHE 的不能加密，这不是 FortiWeb

的问题，而是由于这种算法决定的。



测试 XSS（略）

测试命令注入（略）