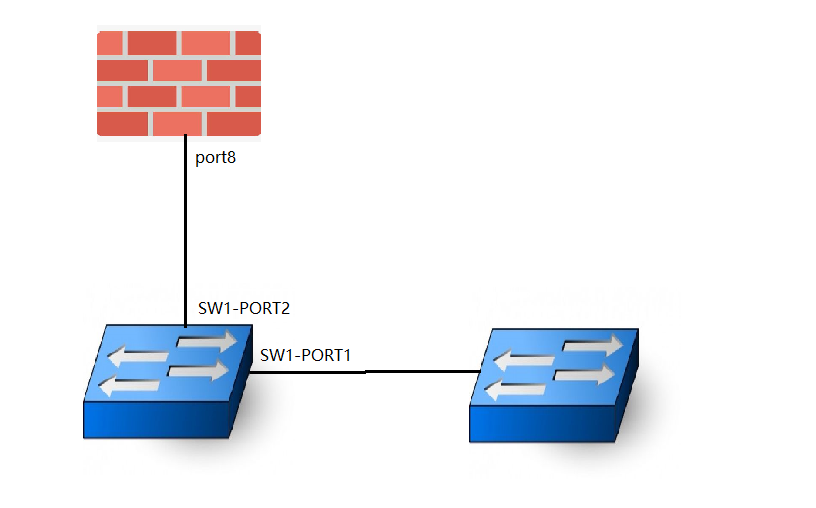
## 旁路（探测）模式

  NGFW可以以旁路方式部署于网络中，连接至交换机的镜像接口，对过往的流量进行嗅探，发现并记录其中的安全威胁或可疑行为（如病毒、入侵、网络滥用等），无需改变网络结构，也不会影响网络流量并形成新的故障点。

拓扑图如下图所示：



### 旁路模式配置要点

1. 交换机配置（根据实际情况进行配置，建议由客户方维护人员进行配置）：

配置sw port1为镜像口，将sw1-port1口上下行流量镜像到sw1-port2口

1. 防火墙配置
2. 配置接口，开启port8的探测模式，让port8口可以对收到的数据包进行分析
3. IPS、DDOS、应用控制规则列表的参数模板（本文中均以default规则为例）
4. 配置防火墙探测策略，将IPS、DDOS、应用程序控制等规则应用于port8口 开启IPS、和流量日志 （可结合现象需要，分别只开启IPS,DDOS,应用控制探测）

### 防火墙配置步骤

1. 配置接口，开启接口PORT8的探测模式



1. IPS、DDOS、应用控制规则列表的参数模板（如下举例供参考）

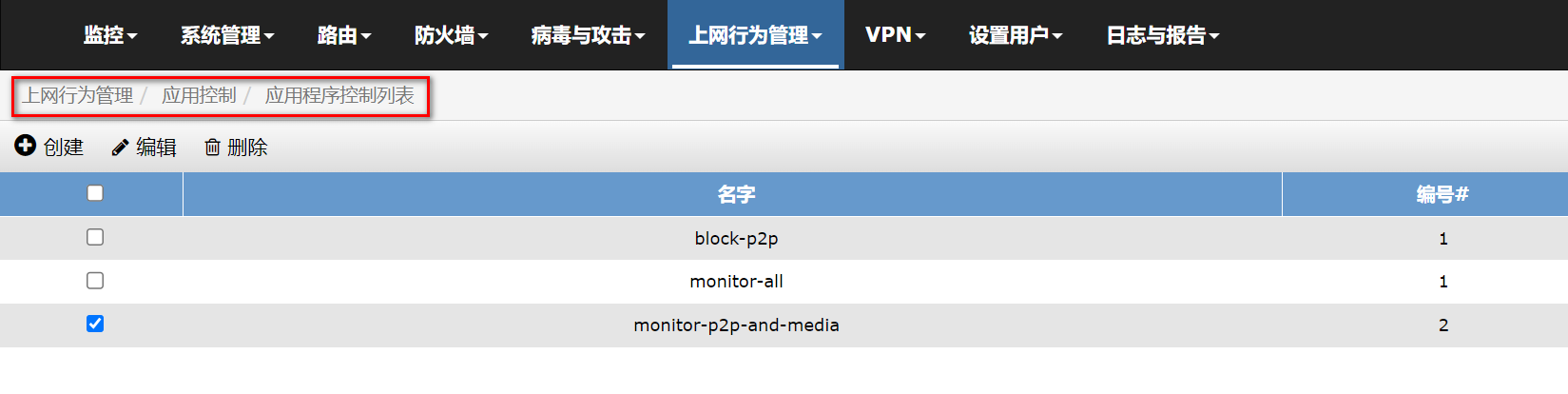
1）IPS配置模板



2）DDOS 配置模板



3）应用控制程序列表



1. 配置探测策略，并开启探测功能中的各项功能



**探测策略各项功能：**

【源接口/区】：必选项 使能探测模式的接口，选择需要配置探测策略的接口

【源地址】：可选项，默认all ;可以按照源地址选择需要进行探测的流量

【目的地址】：可选项 默认all ; 可以按照目的地址选择需要进行探测的流量

【服务】：可选项，默认any ; 可以按照服务类型选择需要进行探测的流量

【记录流量】： 是否记录流量日志，默认不勾选；（如期望产生流量日志，勾选此项，Ips配置模板项也需要同时勾选）

【ddos配置模板】：可选项，默认不启用；启用后可探测流量中的ddos攻击；探测到的ddos攻击日志记录在：日志与报告-日志访问-IPS和DDOS，如下图所示

【IPS配置模板】可选项，默认不开启；启用后可以探测流量中的IPS识别的攻击和漏洞；探测到的IPS日志记录在：日志与报告-日志访问-IPS和DDOS，如下图所示

【应用控制列表】可选项：默认不开启；启用后可以探测流量中的应用程序类型和漏洞；探测到的应用控制类型日志记录在: 日志与报告-日志访问-应用程序控制，如下图所示

如下：图1 流量日志 图2 IPS和DDOS日志 图3 应用控制程序日志

图1 流量日志：



图2 IPS和DDOS日志：



图3 应用控制程序日志：



### 工控类防火墙

工控类除了上述NGFW旁路部署外，增加了工控协议相关的工控流量审计、工控自学习和工控规则策略3项探测功能。【详见工控协议的配置参考】

**配置步骤：**

1. 配置接口，开启接口PORT8的探测模式



1. 配置工控流量审计、工控自学习模板、工控规则策略的参数模板（如下举例供参考）

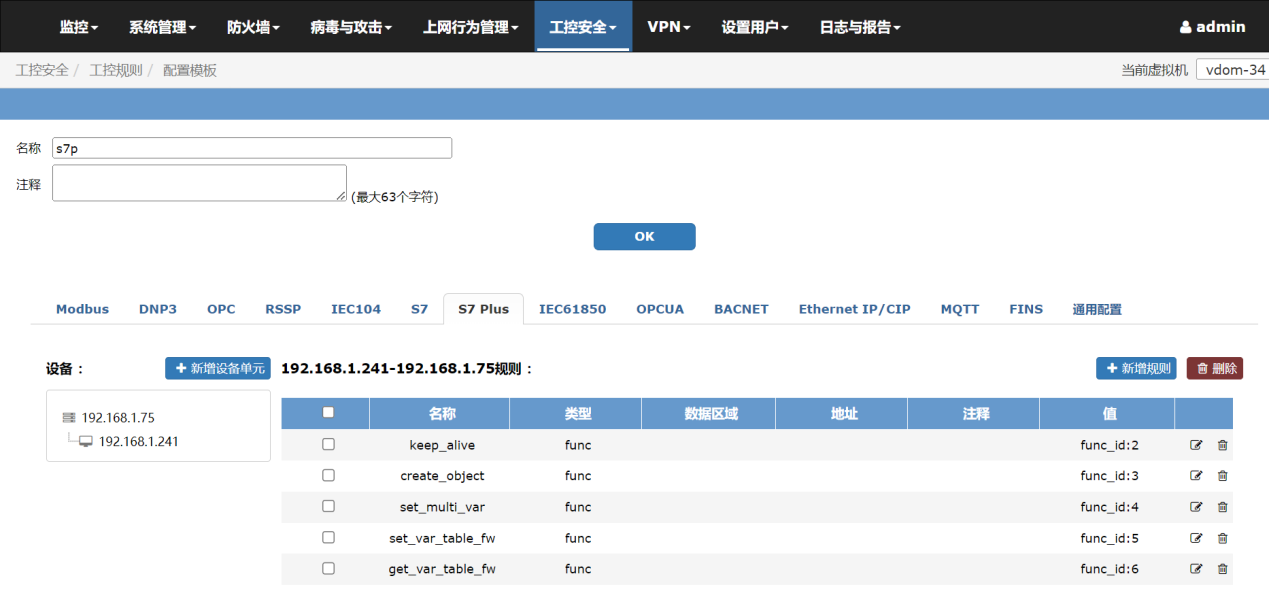
1）配置工控流量审计模板



2）配置工控自学习模板



3）配置工控规则模板



1. 配置探测策略，并启用工控规则相关探测



**探测策略各项功能**：

【源接口/区】：必选项 使能探测模式的接口，选择需要配置探测策略的接口

【源地址】：可选项，默认all ;可以按照源地址选择需要进行探测的流量

【目的地址】：可选项，默认all ; 可以按照目的地址选择需要进行探测的流量

【服务】：可选项，默认any ; 可以按照服务类型选择需要进行探测的流量

【记录流量】：是否记录流量日志，默认不勾选（如期望产生流量日志，勾选此项，Ips配置模板项也需要同时勾选）

【应用工控规则策略】 可选项，默认不启用；启用后可探测流量中的工控规则；探测到的工控规则日志记录在 ：日志与报告-日志访问-工控安全事件，如下图所示

【应用工控自学习】可选项，默认不开启；启用后可以对工控流量自学习生成规则文件，用于生成工控规则策略（没有工控规则策略时，必须开启一段时间的工控自学习，并且有相应的工控流量，才能完成自学习，并生成自学习规则文件）；工控自学习到的规则文件记录在：日志与报告-文档文件读取-工控自学习内容

（注：用户无需关注此归档文件；当用户生成工控规则时会自动调用）

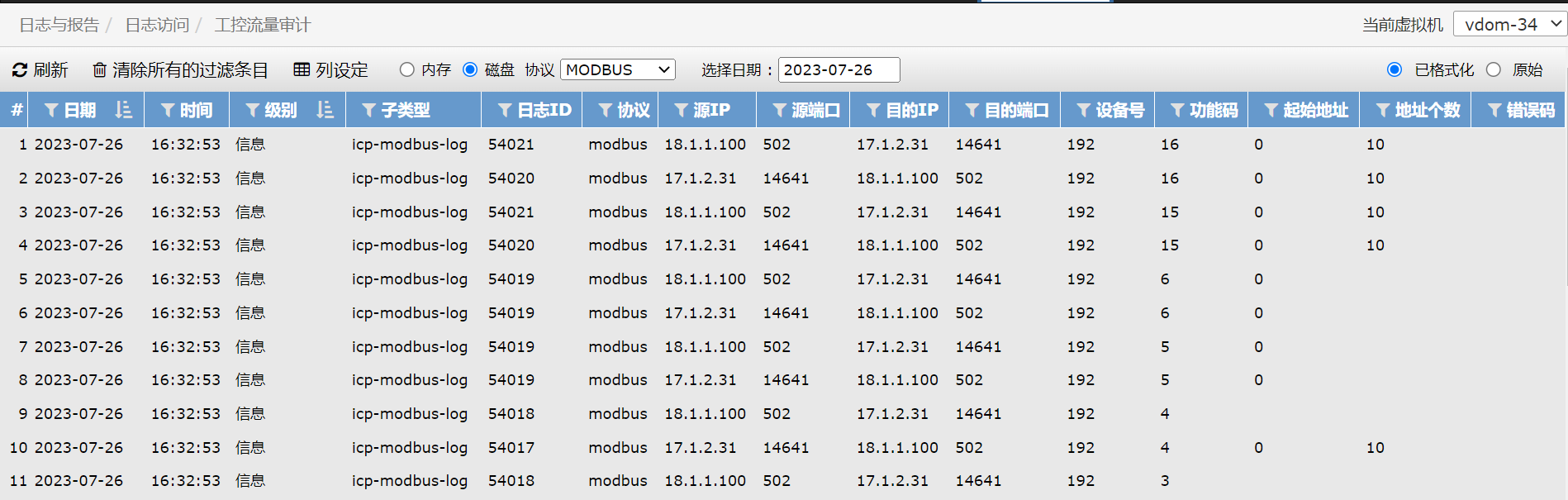
【启用工控流量审计】可选项：默认不开启；启用后可以探测流量中的工控流量并进行记录；启用工控流量审计的日志记录在: 日志与报告-日志访问-工控流量审计，如下图所示

如下：图1 工控安全事件截图 图2 工控流量审计截图

图1 工控安全事件截图：



图2 工控流量审计截图



### 探测策略常见问题

1. **镜像过来的流量为单向流量**

防火墙需要分析双向流量，才能进行更详细的解析；所以如果从现场交换机或路由器镜像过来的一个方向的流量，可能会有探测解析不全问题

1. **设备开启所有的探测项，有的探测项不出来日志的问题**

低端防火墙CPU 内存低的情况下，全部开启各种探测，会导致IPS引擎利用率99.9%。 造成部分探测的日志无法打印。建议采用较高性能的设备，或探测策略中开启部分

(部分低端设备，内存4G 默认只开启一个IPS引擎；如手工配置引擎数量，需要同步增大8G以上内存，否则不建议增加Ips引擎开启数量)

1. **常用定位命令：**

**1） dump test application ipsmonitor**

11 是把session写入共享内存：dump test application ipsmonitor 11

12 是把内存中的内容都出来：dump test application ipsmonitor 12

例：

APW1KMB001001902 # dump test application ipsmonitor

<Integer> test level

APW1KMB001001902 # dump test application ipsmonitor 11

APW1KMB001001902 # dump test application ipsmonitor 12

Total entries : 81

192.168.12.66 51902 111.161.124.96 443 6

192.168.12.34 51044 23.46.26.136 80 6

192.168.12.66 53820 142.251.8.188 5228 6

192.168.12.66 49060 101.198.2.136 443 6

192.168.12.81 48766 4.2.2.1 53 17

192.168.22.6 53886 192.168.12.232 10003 6

192.168.12.65 43708 140.207.176.101 80 6

192.168.12.34 51042 157.255.209.248 80 6

192.168.22.6 53230 192.168.12.232 10003 6

192.168.12.34 62655 157.148.61.140 443 6

192.168.12.50 58828 157.148.59.240 80 6

192.168.12.50 58808 211.93.242.60 443 6

192.168.12.50 61314 111.161.124.96 443 6

192.168.12.65 59638 60.28.172.100 80 6

192.168.12.254 53639 192.168.12.83 443 6

192.168.12.50 62452 192.168.1.231 23 6

192.168.12.254 40966 192.168.12.83 443 6

192.168.12.69 59115 8.8.8.8 53 17

192.168.12.65 54961 116.130.229.204 443 6