Блокировка адресов при помощи Cisco ASA Firewall на основе сработок алертов

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **НЕ** ???????? ??????????? ????????????? ???????.

?????? ?????? ???????? ????????????? KUMA Community ? ?????????????? AS IS ??? ?????-???? ???????? ? ??????????????.

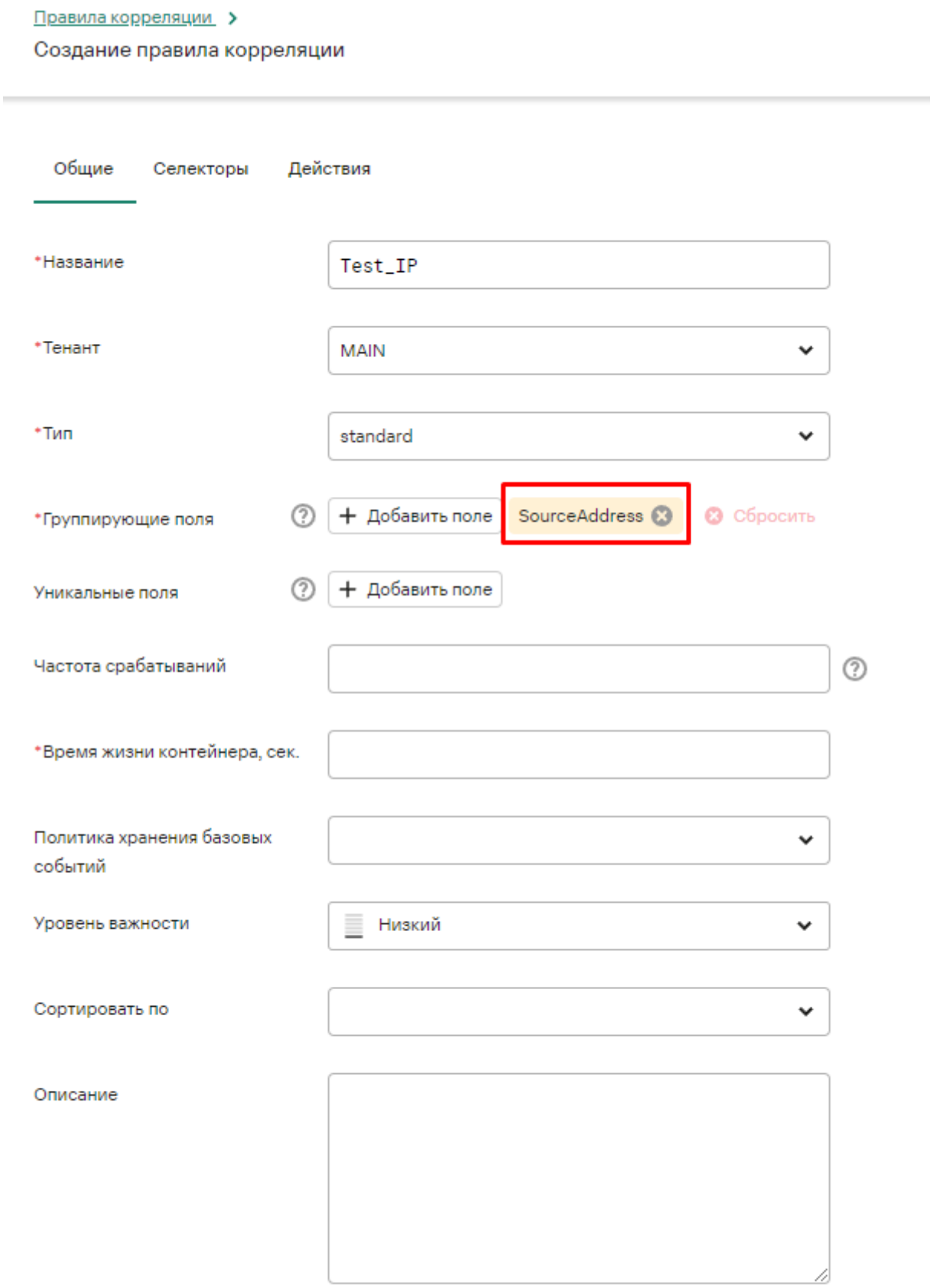
? ????? ?????? ?? ??? ?????? ??????? ??????????, ?? ?????? ????? ???-??????? Apache, ????????? ???????? ?????? ?? ??????? ???????.

??? ????????? ???????????? ?????????? Cisco ASA (?????????? IP ???????) (??????, ??? ??????????? ?? SSH) ??????????:

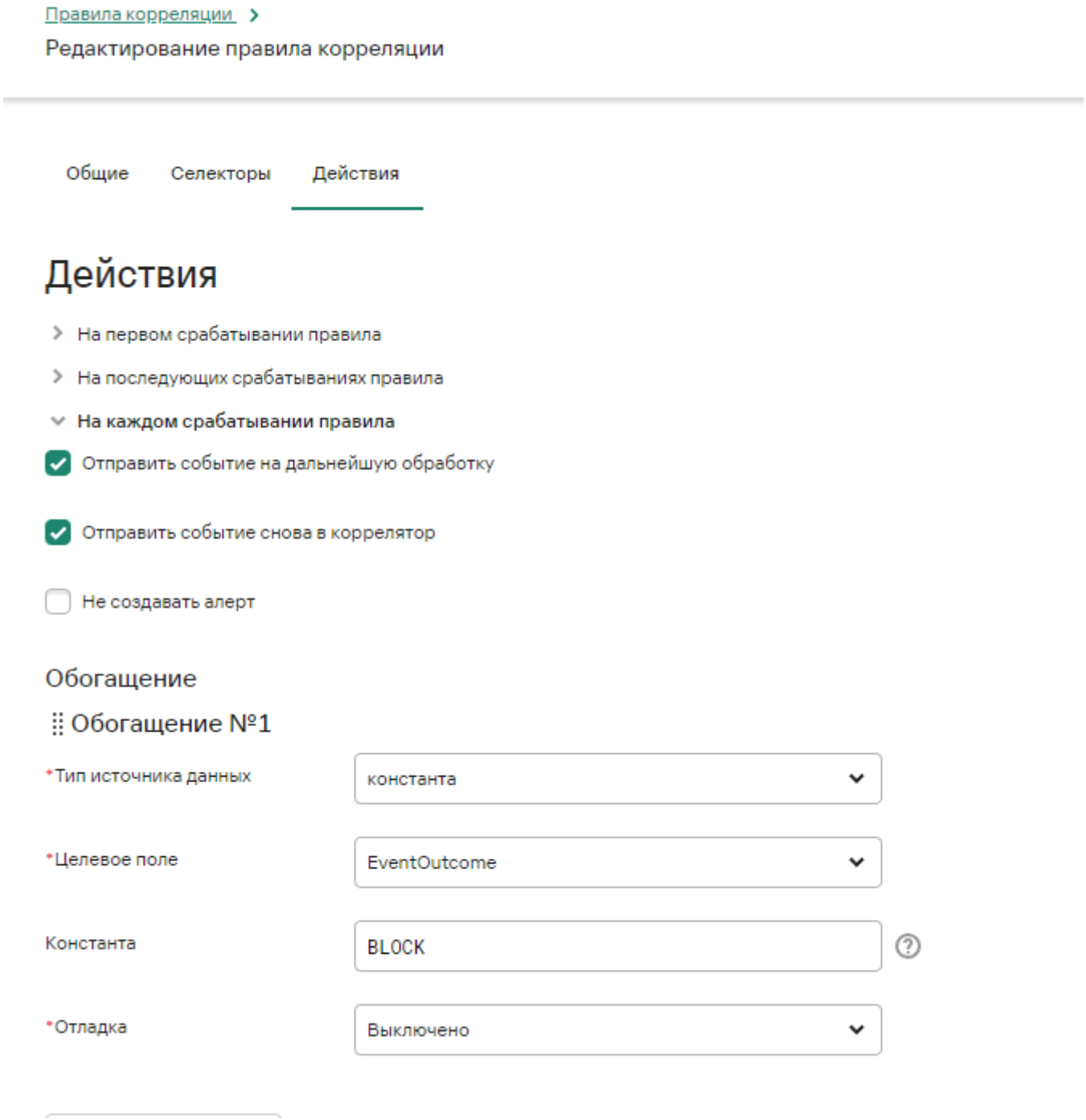
1. ?????????????? ?? ASA ? ????????????, ???????????? ?????????? ? ????? ???????????????, ????????? ???????
   `conf t`
2. ??????? ??????, ? ??????? ??? ?????? ????? ????????? ?????? (?????? ??????), ??????? ??? BLACKLIST. ??????? ????????
   `object network BLACKLIST`
3. ?? ASA ??????? access-list, ??????? ????? ??????????? ???????? ??????? ?????????? ?? ????????? ?? IP ??????????? ? ????? ???????. ??????:
   `access-list INTERNET extended deny ip object-group BLACKLIST any`

Настройка на стороне KUMA

1. ? ???????????? ???? **правила корреляции** ?????? ?????????? ??????? ????, ??????? ???????????? ? ???????? ????????????, ? ????? ??????? ??? **sourceAddress**



2. ? "?????????" ? "????????" ?????? ??????????? ? ?????? ????? ?????????. ??????????? ???????? ?????????? ??????? EventOutcome (??? ??????? ?? ?????????), ??? ???? (???????) ??? ?????????? ????? ?? ??????? ??????? ????????????.



3. ????????? ?????? (????????? ? ????? ???????-????) ?????????????? ??????? ???????? ?????? ? ???????, ? ??????:ip asa, login, password ? ???????, ???????????? ??? ?????????? ? ?????? BLACK (??. ????, ???? ????????? ASA)
4. ?????? ???????? ?? ???????(-??) ?? ???? `/opt/kaspersky/kuma/correlator/<id>/scripts/` ? ????????????? ????? ???????????? kuma, ????? ?????? ????? ??????????? ????? ??? ??????? ???????, ?????????:
   `chown kuma:kuma /opt/kaspersky/kuma/correlator/<id>/scripts/asa.py`
   `chmod +x /opt/kaspersky/kuma/correlator/<id>/scripts/asa.py`
5. **Данный этап индивидуален и зависит конкретно от Вашего экземпляра ОС, возможно будут дополнительные ошибки при**

запуске скрипта, для проверки скрипт можно запускать вручную с сервера и проверять работоспособность

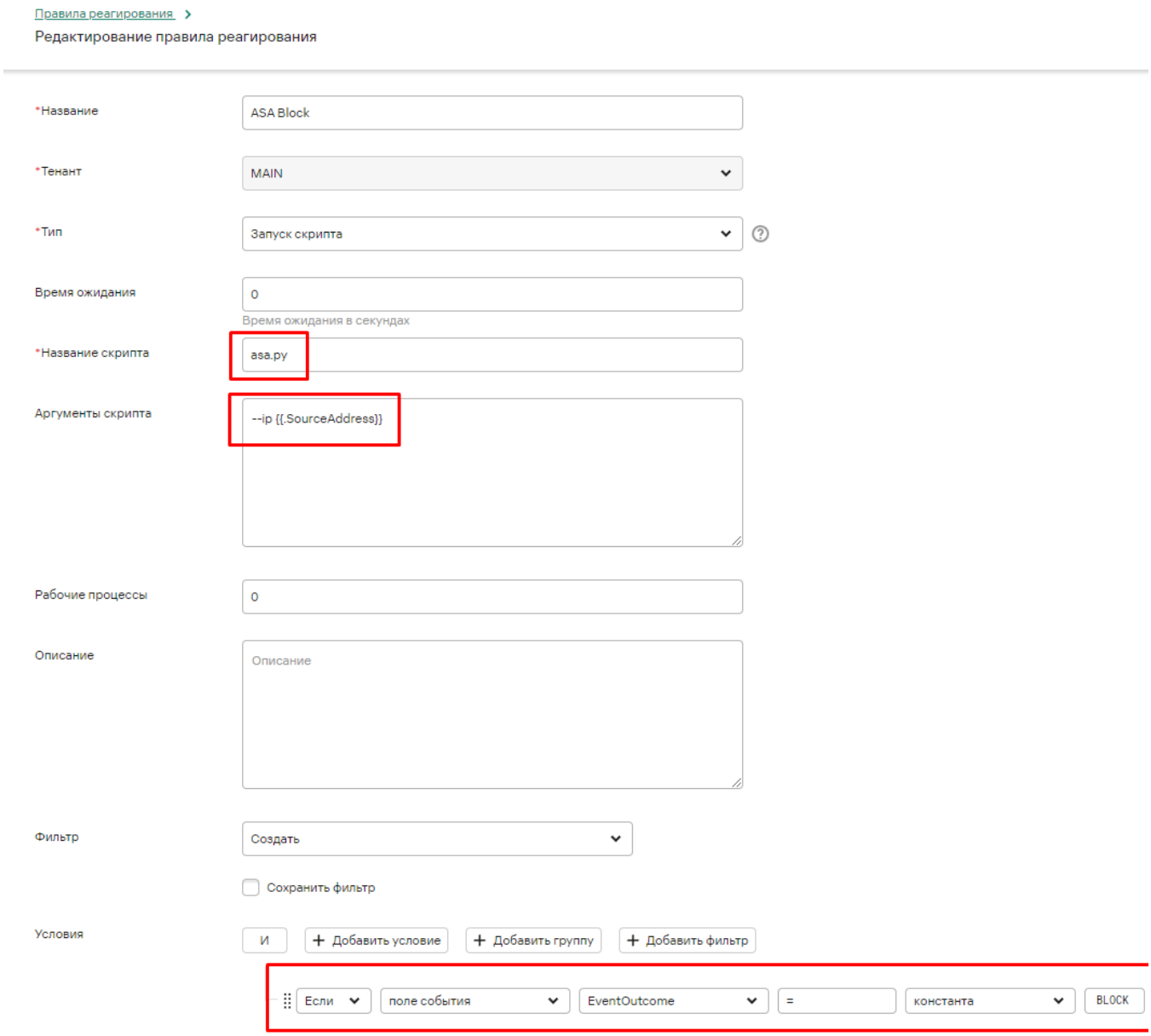
????? ?? ?????? ??????????? ? pip3 ?????????? ?? ?????????? ????????? ??????????, ??? ??????????? ??????? python3.*

threading
paramiko
sys
argparse
subprocess

???????:

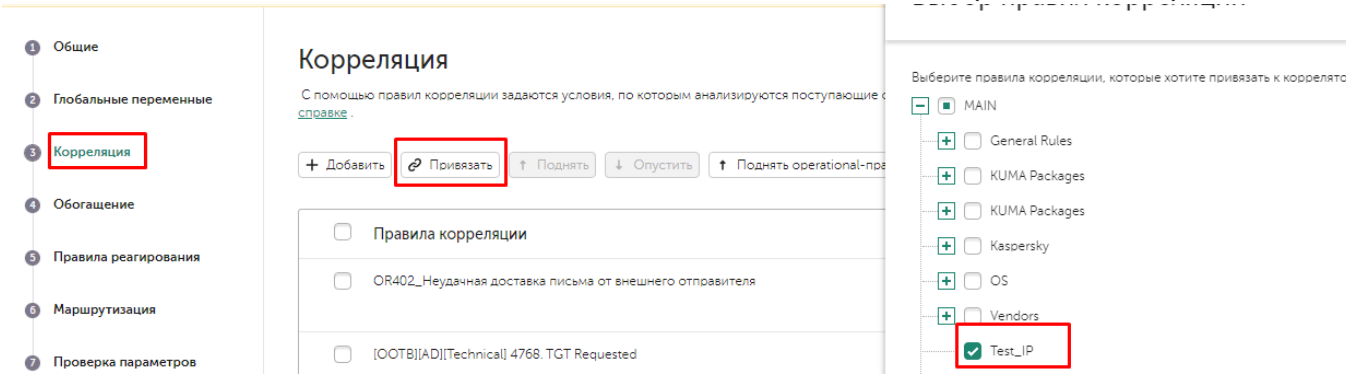
```
pip3 install threading paramiko sys argparse subprocess
```

6. ??????? ??????? ????????????, ??????? ????? ??????????????? ????????? ?????? ?? ?????????? (??? 4)

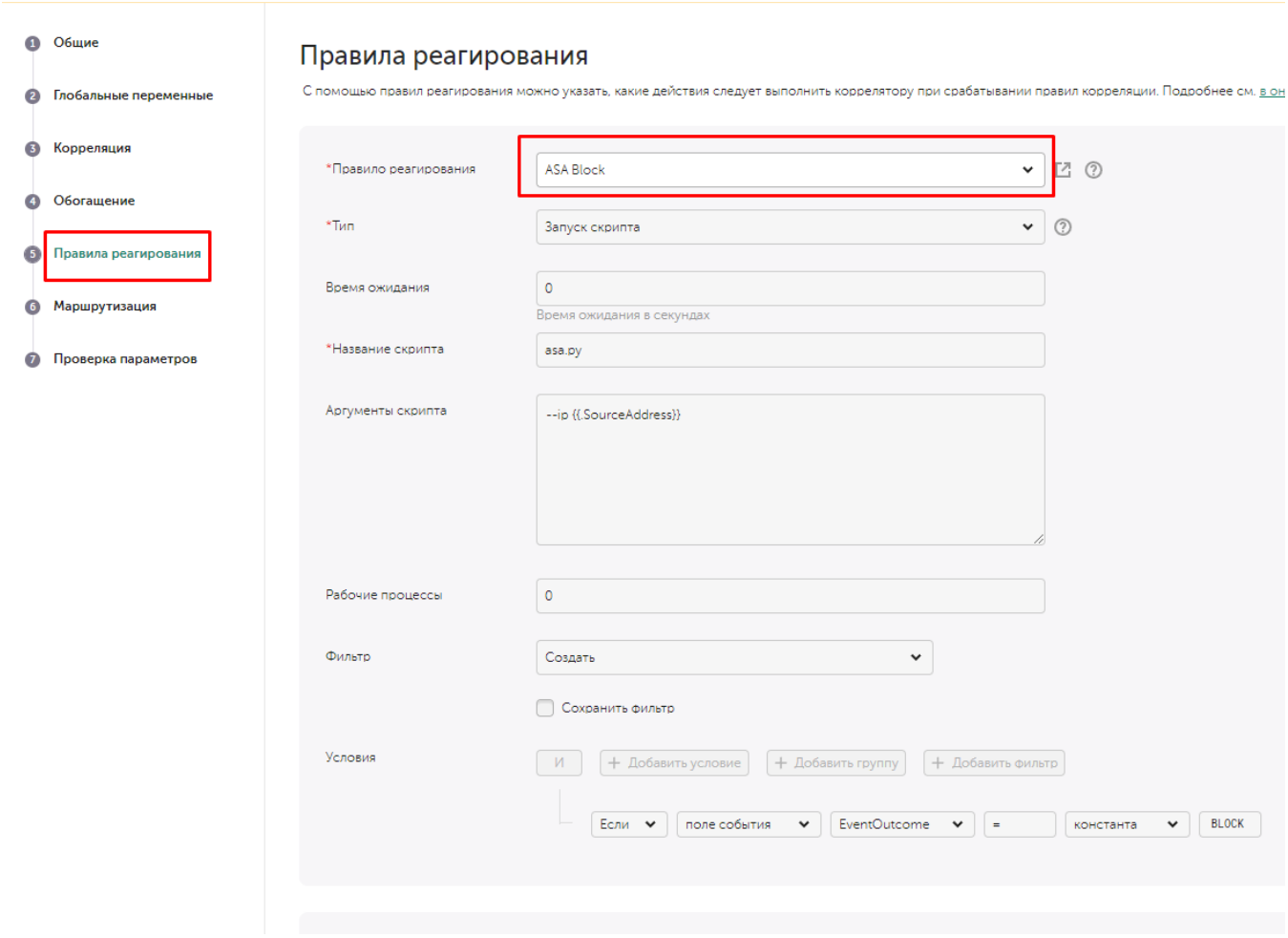


????????, ?????? ???????? ???????, ??????? ?? ????????? ?? ?????? ??????????? (??? 4), ????? ????????? ???????, ??? ?? ????????? ? ???????? ???? EventOutcome = BLOCK (??????????? ??? ???????????? ??????, ??? ?????? ??????????) (??????? ??? ??????, ????? ?????? ??????? ? ??????? ??????).

7. ???????? ????????? ????? ??????? ??????????. ??????????? ? ???????????. ??????? -> ??????????? -> ???????? ??? -> ??????????, ????????? (?? ?????????)



8. ????? ?????????? ????? ?? ???????? ??????? ???????????



9. ??????, ????????? ? ?????????? ?????????? (?)

Revision #9
Created 2023-12-08 17:34:20 UTC
Updated 2024-11-11 10:32:38 UTC by Koala