?????????? ?? ICAP-?????????? KATA

????????

Данное руководство содержит информацию об интеграции платформы KATA со сторонними решениями по протоколу ICAP, такими как Proxy server или NGFW. Также поддерживается возможность интеграции с другими решениями, поддерживающими передачу данных по ICAP. Описывает процесс настройки и проверки интеграции, встречающиеся проблемы в PoC, эксплуатации и шаги по их устранению.

??????? ???????? ???????

Kaspersky Anti Targeted Attack Platform — решение для защиты IT-инфраструктуры организации и своевременного обнаружения атак «нулевого дня», целевых атак и APT. Решение разработано для корпоративных пользователей.

Решение может получать и обрабатывать данные через подключение к прокси-серверу по ICAP, включая HTTP-, FTP- и HTTPS-трафик (с SSL-подменой на прокси).

- Подключаться к прокси-серверу по протоколу ICAP, получать и обрабатывать данные HTTP- и FTP-трафика, а также HTTPS-трафика, если администратор настроил подмену SSL-сертификата на прокси-сервере.



В роли ICAP-сервера может выступать **Central Node** с функцией Sensor или отдельный компонент **Sensor**.

> **Важно:** KATA не обеспечивает шифрование ICAP-трафика и аутентификацию клиентов по умолчанию. Необходимо самостоятельно настроить защищенное соединение между прокси-сервером и KATA.

ICAP-клиентом обычно является прокси, который отправляет данные на ICAP-сервер. Решение о пересылке данных и режим работы принимается на клиенте.

Добавлена ICAP-интеграция с обратной связью в двух режимах:

- **Стандартная проверка** — объект доступен Sandbox, при обнаружении угрозы блокируется.
- **Усиленная проверка** — объект недоступен Sandbox, при угрозе блокируется.

> **Примечание:** При включении приема ICAP-трафика в режиме «Отключено» работает режим **respmod**: вердикт не возвращается, но результат доступен **в интерфейсе KATA** для роли **«Офицер безопасности»**.

> Для оптимизации нагрузки приложение может временно переключиться из режима усиленной проверки ICAP-трафика в режим стандартной проверки. В этом случае файлы, полученные из ICAP-трафика и отправленные на проверку в Sandbox, остаются доступными для скачивания. При обнаружении угрозы в проверенных файлах приложение создает алерт. Проверка файлов модулями Anti-Malware Engine и YARA продолжает работать в штатном режиме.

Если вы используете режим распределенного решения и мультитенантности, выполняйте действия включения приема ICAP трафика в веб-интерфейсе того сервера PCN или SCN, параметры которого вы хотите настроить.

На многих прокси серверах или системах поддерживающих передачу данных по ICAP, достаточно будет активировать функциональность ICAP-клиент и указать адрес ICAP-сервер.

Детальнее по настройке и работе решения можно ознакомится в онлайн документации.

?????????? ???????????

????????? ?????? ICAP ?? Central Node

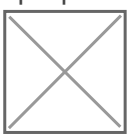
1. Перейдите в веб-интерфейс CN по адресу:

   ```
   https://<IP_CN>:8443
   ```

2. Введите учетные данные учетной записи с ролью Администратор (по умолчанию это учетная запись **admin** автоматически созданная при установки системы).

LogIn

3. Далее переходим в раздел **“Серверы Sensor”**. В данном разделе **встроенный Sensor в компонент Central Node** называется **«Embedded Sensor»**. Нажимаем **«Изменить»**.

4. В открывшемся меню перейдите в раздел **“ICAP-интеграция”**. В данном разделе переведите в состояние **“включено”** для включения функционала обработки “ICAP-трафика”.

5. Далее в зависимости от типа проверки и принципа работы данной интеграции, выставьте режим **“проверки в реальном времени”(описан выше)** в зависимости от требований и типов проверки, которыми, хотели бы проверять передаваемые данные от **“ICAP-клиента” (PROXY/NGFW)**.


Скопируйте ICAP-адреса:

```
icap://<IP-Сенсора>:1344/av/respmod
icap://<IP-Сенсора>:1344/av/reqmod
```



> **Важно** - Для настройки на ICAP-клиенте используйте указанные адреса из поля Host.

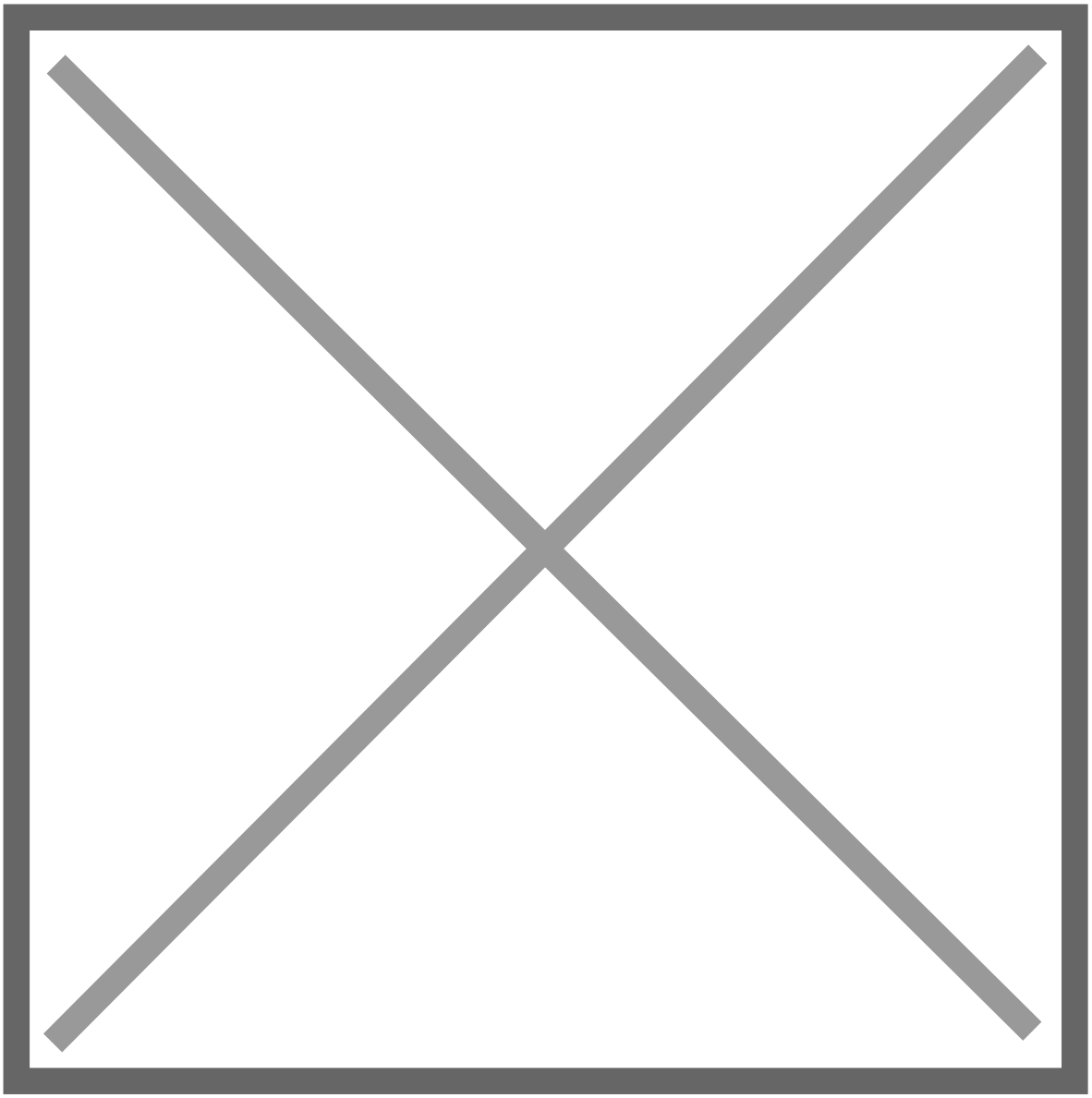
????????? ?????????? ICAP

В разделе **Параметры → Проверка трафика ICAP** можно:

- В разделе **“Уведомления”** настроить собственные шаблоны страниц блокировки при разных типах срабатывания;
- В пункте **“Порог блокировки”** выставить при каком уровне угрозы блокировать проверяемый файл;

- В пункте **“Время ожидания проверки”** выставить время ожидания ответа по проверке.

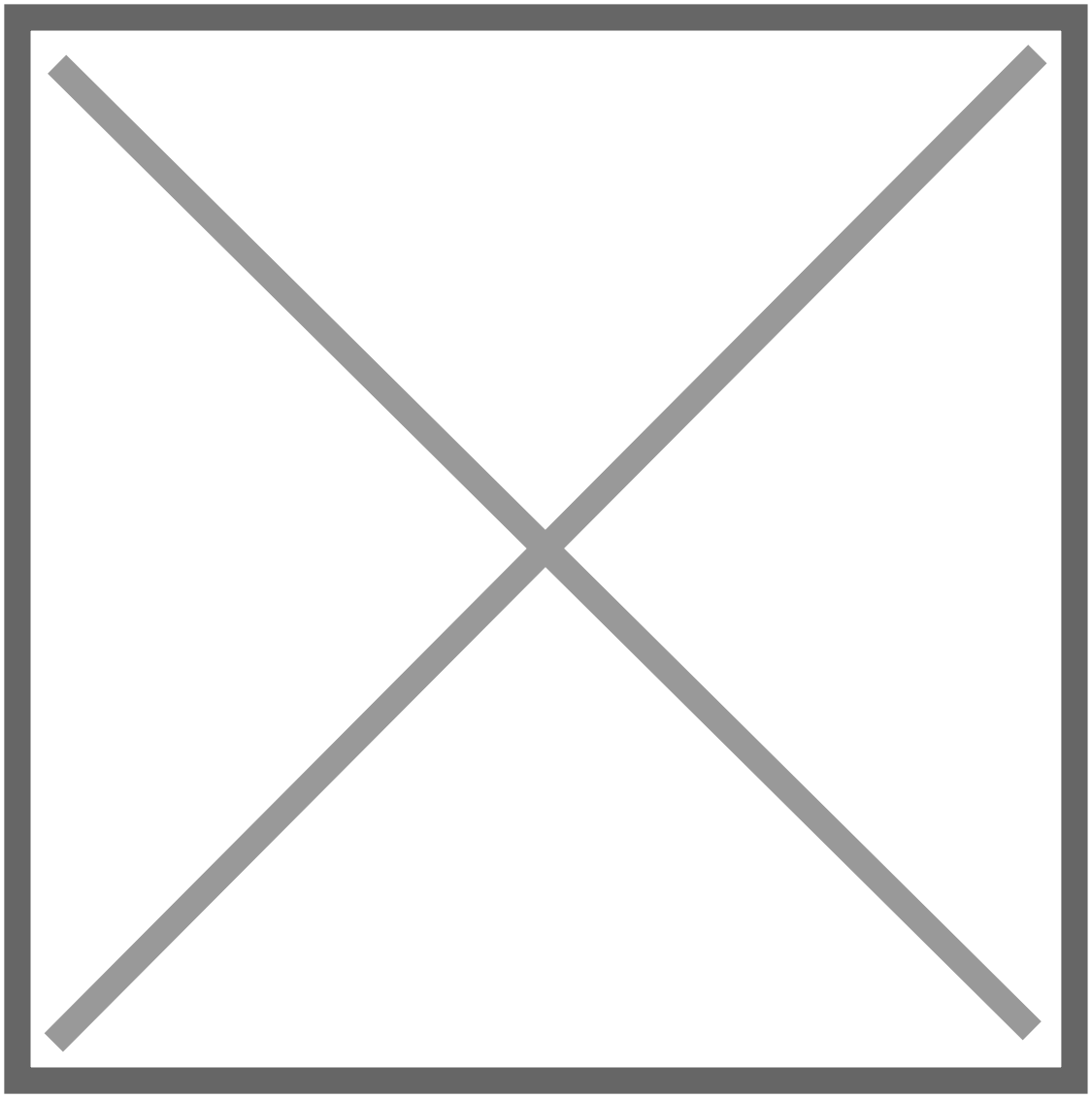
Детальнее по настройке и работе решения можно ознакомится в онлайн документации.



????????? ICAP ?? Sensor

Настрйока ICAP на Sensor выполняется точно также как и для встроенного **Embedded Sensor/Central Node**.

Детальнее по настройке и работе решения можно ознакомится в онлайн документации.



???????? ????????????????? ??????????

После завершения настроек на стороне KATA и ICAP-клиента (прокси) проверьте корректность работы следующим образом:

1. Убедитесь, что тестовый ПК настроен на использование вашего прокси.
2. Выполните запрос на загрузку тестового файла EICAR через HTTPS.
3. В интерфейсе Central Node:
   - Перейдите в раздел **Dashboards**.
   - В панели **Processed** выберите источник (ICAP) — IP-адрес вашего прокси и период (например, Last hour).

- Убедитесь, что на графике есть активность (число обработанных URLs и Files больше нуля).

4. Авторизуйтесь в CN под учетной записью с ролью **Офицера безопасности**, чтобы проверить срабатывание по загруженному файлу:
   - Откройте раздел **Alerts**.
   - Отфильтруйте события по полю **File name**, указав `EICAR`.
   - Проверьте список событий — убедитесь, что отображается нужный файл.
   - Откройте событие и проверьте карточку с подробностями:
     - **Data Source** должно содержать `ICAP Sensor <IP>` — значит, трафик шел через настроенный ICAP.
     - В разделе **Object information** отобразится информация о проверенном файле (например, `eicar.zip`).
     - Проверьте источник запроса, адреса Proxy и Web-сервера, убедитесь, что обращение было по HTTPS.

?????? ? ICAP-???????????

Пользователи с ролью **Старший сотрудник службы безопасности** могут создавать список ICAP-исключений — перечень данных, которые **Kaspersky Anti Targeted Attack Platform** не будет проверять.

Можно создать правила ICAP-исключений для следующих данных:

- Формат
- Агент пользователя
- MD5
- Маска URL
- IP или подсеть источника

Пользователи с ролями **Аудитор** и **Сотрудник службы безопасности** могут просматривать список правил ICAP-исключений.

??????????? ? ????????????? ???????

- В режиме распределенного решения:
  - ICAP-исключения, созданные на **SCN**, распространяются на все компоненты Sensor, подключенные к этой SCN.
  - ICAP-исключения, созданные на **PCN**, распространяются на SCN, установленную на одном устройстве с PCN, и все подключенные к этой SCN компоненты Sensor.

Детальнее по настройке и работе решения можно ознакомится в онлайн документации.



?????????? ?? ?????????? ? ?????????

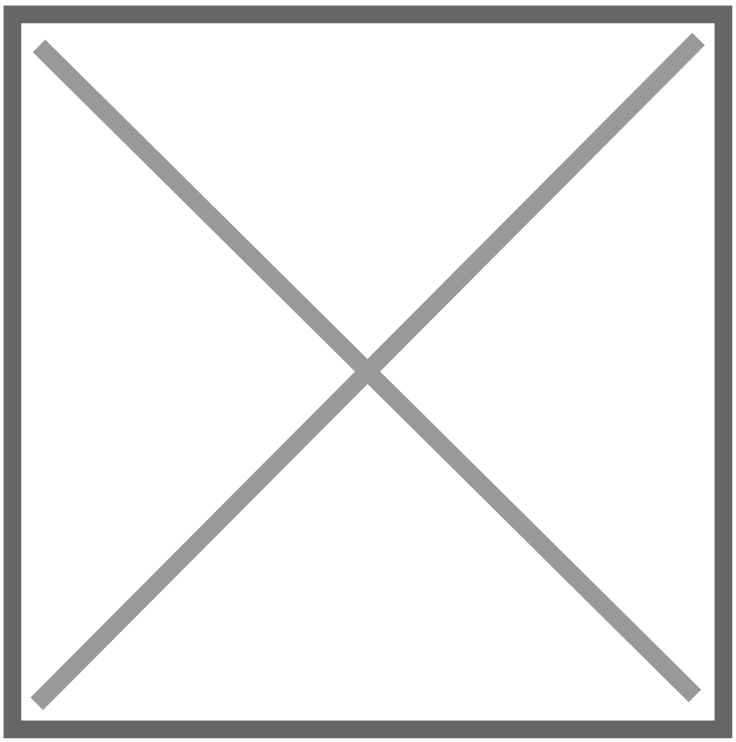
SQUID

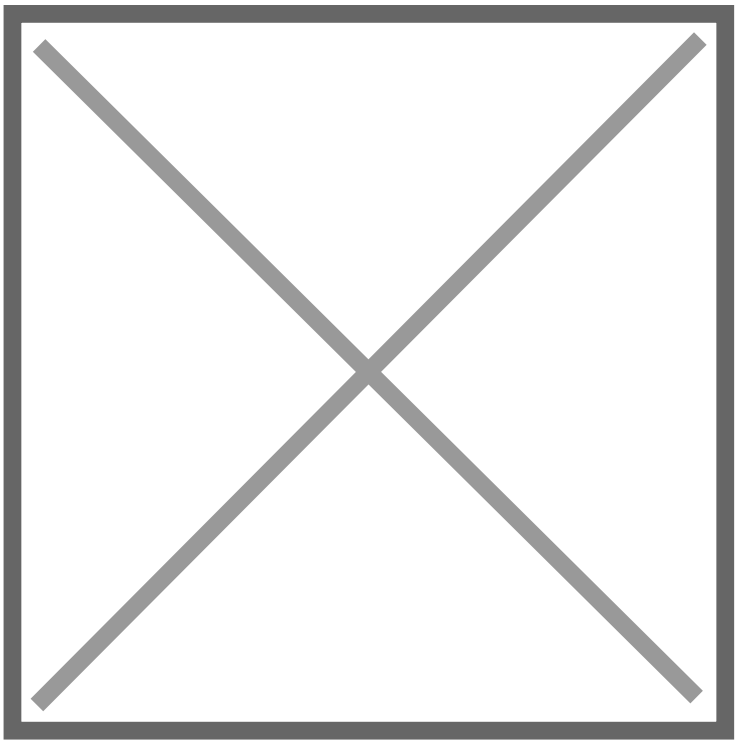
Конфигурация SQUID для настройки интеграции прописываемая в **squid.conf**:

```
icap_enable on
adaptation_send_username on
icap_client_username_header X-Client-Username
adaptation_send_client_ip on
adaptation_meta X-Client-Port "%>p"
icap_service_failure_limit -1
icap_service_revival_delay 30
icap_preview_enable off
icap_206_enable off
icap_service is_kata_req reqmod_precache 0 icap://[ICAP_SERVER_IP]:1344/av/reqmod
icap_service is_kata_resp respmod_precache 0 icap://[ICAP_SERVER_IP]:1344/av/respmod
adaptation_access is_kata_req allow all
adaptation_access is_kata_resp allow all
icap_io_timeout 60 seconds
```

UserGate

- В UserGate необходимо создать ICAP-сервер и указать адреса, полученные на CN:

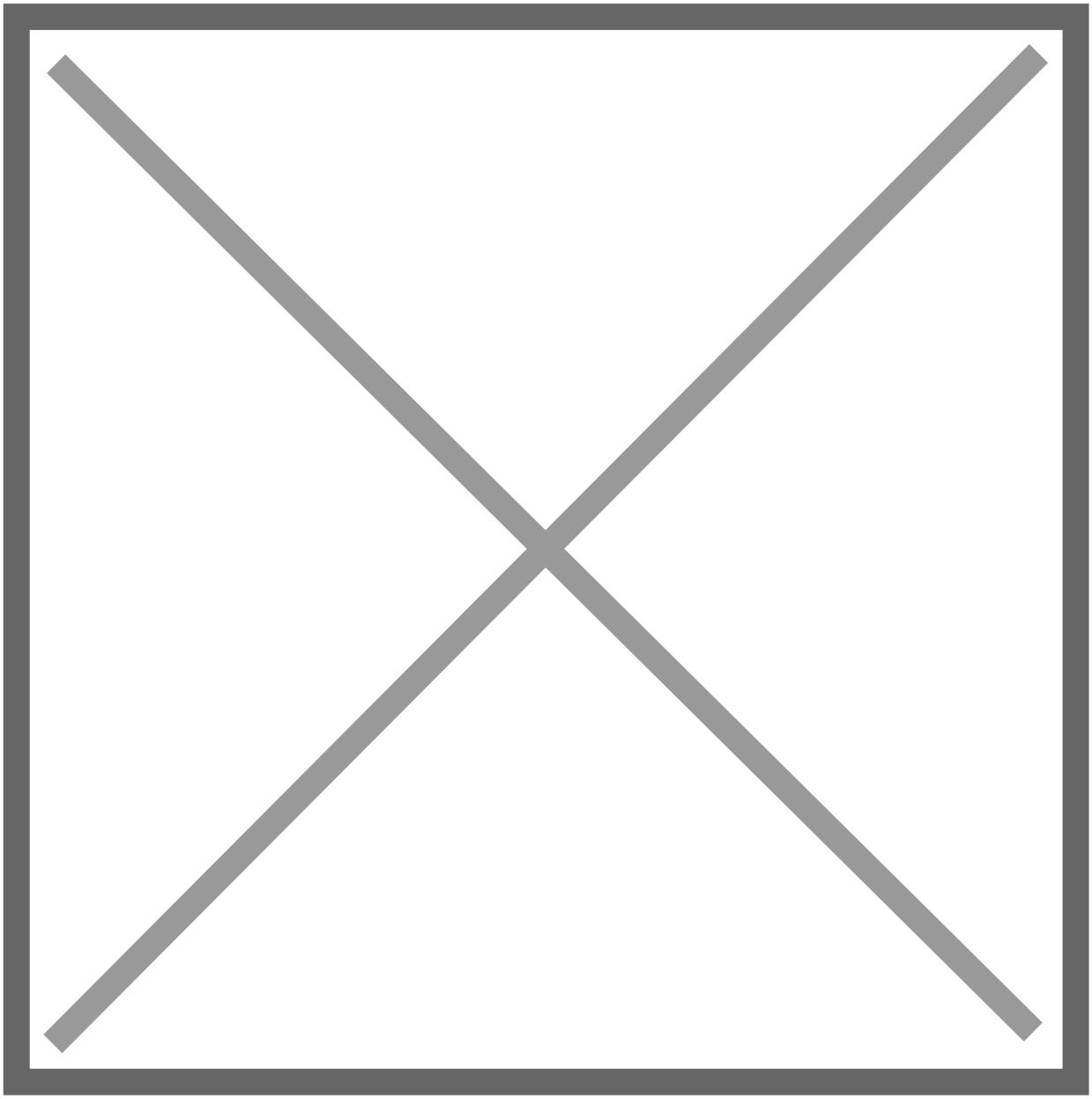



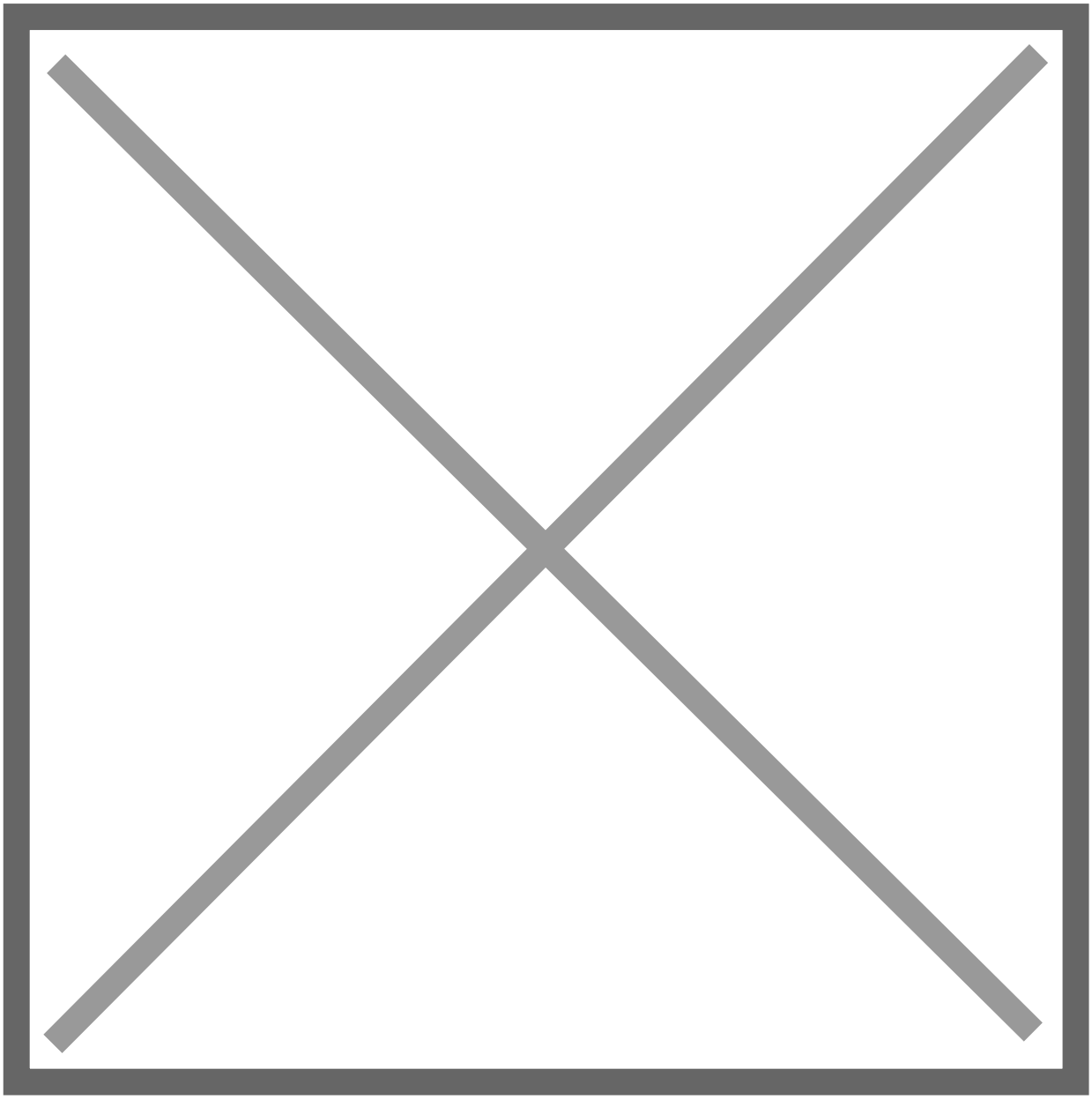


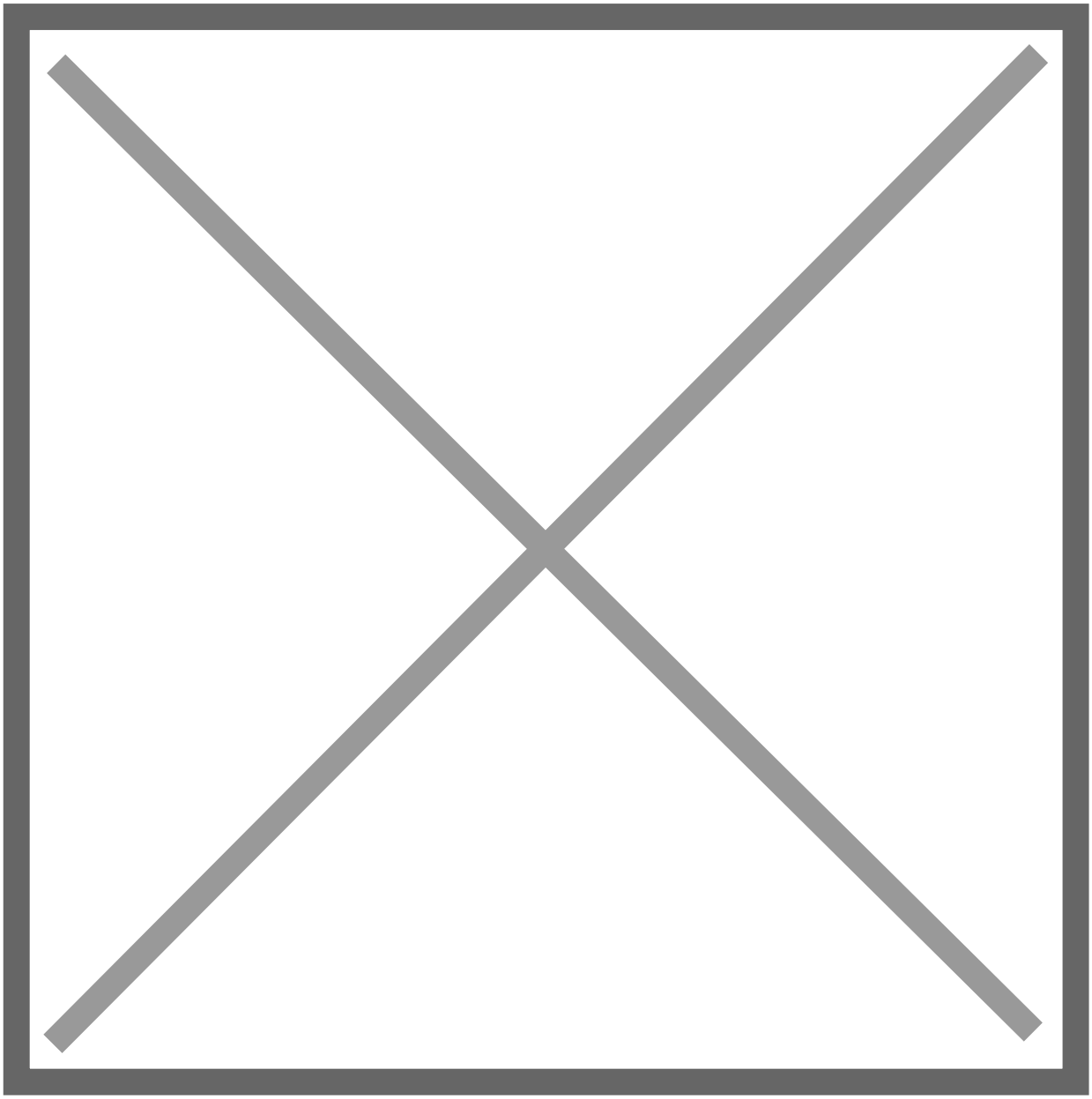
- При необходимости активируйте опции:
- «Посылать имя пользователя»
- «Посылать IP-адрес»

- Потом создаете ICAP правило, где выбираете ранее созданный ICAP server.









Проверяем связь между системами

Revision #28
Created 30 June 2025 10:56:55 by Николай
Updated 6 February 2026 11:07:28 by Кирилл