

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

KICS for Networks ? ?

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

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

?????? ? ? ? ? ?

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

????

Для формирования набора правил используется предварительно обученная система KICS for Networks. Качество обучения системы не имеет особого значения: важным условием является наличие в системе достаточного количества записей о сетевых сессиях. Идеальный вариант — наличие в системе данных о максимальном количестве сетевых сессий узлов защищаемого сегмента сети.

1. ????????????? ? ? ? ? ? ? ? ? ? ?

На первом этапе необходимо сформировать перечень всех сетевых сессий (активных и завершённых) для конкретного защищаемого узла. Для этого в карточке актива следует перейти к выборке необходимых сетевых сессий, используя кнопку «Показать связи» → «Сетевые сессии».

[image.png](#)

2. ??????? ? ? ? ? ?

На следующем этапе необходимо выполнить экспорт всех сетевых сессий в CSV-файл. В разделе «Сетевые сессии» выберите все записи и нажмите кнопку «Экспортировать в CSV-файл».

[image.png](#)

3. ????????? ? ? ? ? ? ? ? ?

Откройте сформированный файл.

image.png

Для удобства дальнейшей работы создайте копию единственной вкладки.

image.png

Присвойте вкладкам названия, соответствующие целевым наборам разрешённых входящих и исходящих соединений (например, «Исходящие», «Входящие»).

image.png

4. ????????????? ???????? ????????????? ?????????????

На вкладке «Исходящие» создайте фильтр данных, в котором для столбца «Сторона 1» выберите защищаемый узел.

image.png

Аналогично создайте фильтр данных, в котором для столбца «Сторона 2» выберите узлы, взаимодействие с которыми разрешено или предусмотрено для защищаемого узла проектной документацией. В случае отсутствия проектной документации перечень узлов, с которыми разрешено взаимодействие, определяется экспертно.

image.png

Полученная выборка представляет собой перечень фактических взаимодействий из числа разрешённых.

image.png

5. ??????? ???????? ? ????????????????? ????????

Выборка должна быть проанализирована на предмет использования в соединениях динамических портов:

- для ОС Windows — 49152–65535;
- для ОС Linux — 32768–60999;
- для проприетарных протоколов и стороннего ПО — используемые диапазоны.

Для таких случаев при формировании набора правил в соответствующих правилах необходимо указывать действующие диапазоны портов. Если определить диапазон портов невозможно, допускается фильтрация только по IP-адресу (наименее безопасный вариант).

Для взаимодействий, в которых порт определяется однозначно, правило формируется по соответствующему порту. Для служебных взаимодействий (например, по портам 137, 138) правила могут не формироваться, если соответствующий функционал (например, NetBIOS для портов 137, 138) не используется в защищаемой системе.

При работе с выборкой сессий дубликаты записей удаляются или скрываются инструментами Excel.

6. ????????????? ?????? ??? ?????????? ??????????????????

Правила для входящих взаимодействий формируются аналогичным образом.

[image.png](#)

На этапе фильтрации данных защищаемый узел выступает в качестве стороны 2.

[image.png](#)

7. ????

По результатам анализа и оценки сформированных выборок взаимодействий составляется набор правил для средств периметральной защиты (программно-аппаратных или программных межсетевых экранов), позволяющий реализовывать функционал защищаемой системы при минимальном количестве разрешённых взаимодействий. Стоит отметить, что для настройки современных межсетевых экранов, работающих по принципу Stateful (в том числе функционал "Сетевой экран" KICS for Nodes), создания правил для обратного трафика не требуется, достаточно создания разрешающего правила от стороны, инициировавшей сессию, до узла назначения, обратные пакеты будут пропущены через МЭ автоматически.

[image.png](#)

ВАЖНО! Включение средств периметральной защиты систем промышленной автоматизации в режиме блокирования отдельных сетевых взаимодействий должно осуществляться только после проведения соответствующих приемочных испытаний и проверки отсутствия деструктивного воздействия на работоспособность защищаемых систем.