Руководство по эксплуатации

1. ArtX TLSproxy

Руководство по эксплуатации

В документе описано назначение и применение ArtX TLSproxy, сформулированы его общие характеристики как объекта администрирования, определены основные технические операции и мероприятия по подготовке объектов администрирования к вводу в действие, определен порядок обновления ПО, определен регламент работы объекта администрирования в аварийных ситуациях. Сведения, приведенные в этом документе, могут быть изменены в любой момент без предварительного уведомления.

1.1. **Проблемы, решаемые ArtX TLSproxy**

По различным оценкам, до 90% сетевого трафика составляет SSL/TLS-трафик, для контроля которого создан класс решений SSL Visibility. TLS proxy является решением класса SSL Visibility и выполняет разворачивание SSL/TLS сессий и предоставление обработанного трафика во внешние системы для его аудита или модификации.

1.2. Цели и задачи внедрения ArtX TLSproxy

ArtX TLSproxy решает следующие задачи:

★ Раскрытие для последующего анализа SSL/TLS-трафика рабочих станций, ноутбуков, мобильных и любых других устройств.

★ Отправка копии обработанного сетевого трафика в сторонние системы для дальнейшего анализа

★ Пропуск без модификации определенных сетевых соединений по различным критериям, таким как VLAN ID, MAC-адрес, IP-адрес или подсети, веб-домен (SNI).

2. Описание продукта

ArtX TLSproxy - программный продукт, функционирующий в среде Linux. ArtX TLSproxy устанавливается "в разрыв" на периметре сети организации, проксируя весь сетевой трафик, или же трафик определенных сегментов сети.

ArtX TLSproxy находит в сетевых соединениях начало SSL/TLS-сессии, затем для всех таких соединений выполняет подмену сертификатов (Man-in-the-Middle), представляясь клиенту соединения сервером, а серверу клиентом. Таким образом, ArtX TLSproxy представляет все данные SSL/TLS-соединений в раскрытом виде.

Для нахождения начала SSL-соединения внутри сессии используется сигнатурный метод, что позволяет разворачивать SSL-трафик вне зависимости от сетевого порта сервера соединения. Все не SSL/TLS-соединения пропускаются без изменений.

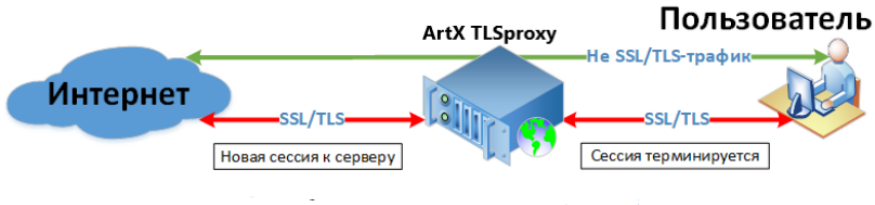


Рисунок 1. Принцип работы ArtX TLSproxy

Результатом работы ArtX TLSproxy является одна или более копий развернутого сетевого трафика (RX- и TX-пакеты), направленные в Mirror-интерфейсы, к которым подключаются внешние системы для анализа сетевых соединений.

Принцип обработки SSL/TLS-соединений в ArtX TLSproxy:

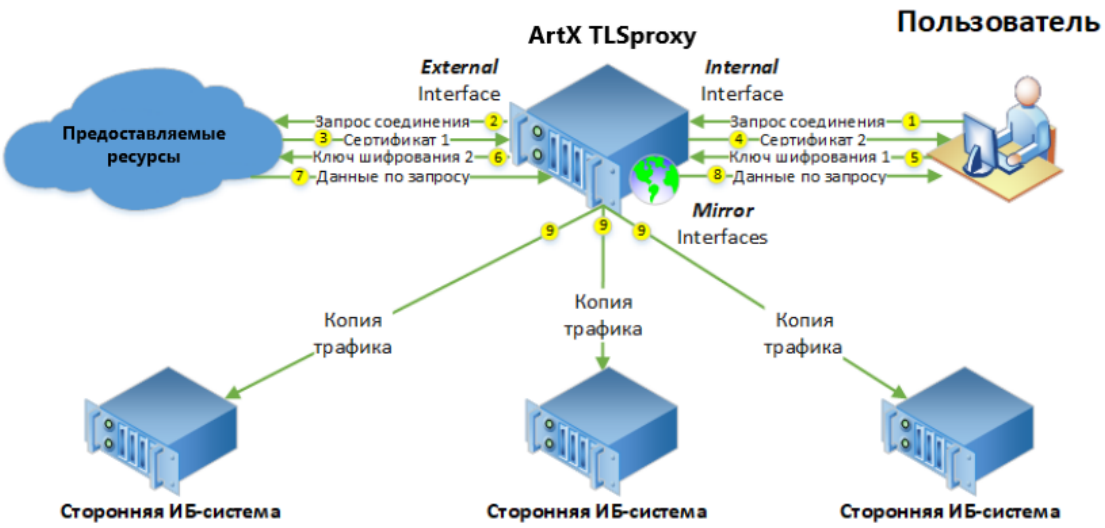


Рисунок 2. Принцип обработки SSL/TLS-соединений

ArtX TLSproxy может работать в двух режимах:

1. Прозрачный режим L2 (Bridge) - в этом режиме ArtX TLSproxy функционирует на уровне L2 сетевой модели OSI, являясь невидимым для пользовательской сети.
2. Режим шлюза L3 (Router) - в этом режиме ArtX TLSproxy функционирует на уровне L3 сетевой модели OSI, являясь шлюзом для пользовательской сети, то есть явно указывается в сетевых настройках рабочих станций в качестве сетевого шлюза по умолчанию.

★ В ArtX TLSproxy разработан механизм исключений, позволяющий пропускать без изменений соединения к интернет-сервисам, которые не требуется контролировать.

Исключения устанавливаются как по IP-адресам источника и назначения, так и по интернет доменам. Также для упрощения работы с исключениями поддерживаются wildcard-синтаксис, например, *.domain.com. В ArtX TLSproxy также имеется настройка автоисключений Auto-bypass — возможность автоматически заносить в список временных исключений соединения, завершившиеся с обрывом связи на стороне клиента определенное количество раз за заданный промежуток времени. ArtX TLSproxy хранит автоисключения в течение заданного в его настройках времени. За это время администратор может

либо назначить им статус постоянных исключений, либо сообщить разработчикам о проблеме и потребовать её решения. Эта функциональность значительно упрощает процесс интеграции ArtX TLSproxy за счет минимизации риска выхода из строя бизнес-приложений.

2.1. Сферы применения

Задача разворачивания SSL/TLS-соединений естественным образом возникает во многих ИТ-сферах, где требуется аудит трафика или его изменение в режиме реального времени.

ArtX TLSproxy не имеет жёсткой зависимости от экосистемы какого-либо производителя программного обеспечения или аппаратной платформы (отсутствует т.н. vendor-lock).

Поэтому ArtX TLSproxy может использоваться с любыми смежными системами, которым требуется решение задачи разворачивания SSL/TLS-соединений.

2.2. Типовые схемы включения

ArtX TLSproxy может быть развернут в сетевой инфраструктуре организации в режиме L2 (Bridge) и в режиме L3 (Router). Также ArtX TLSproxy может работать как в классическом режиме раскрытия SSL/TLS-трафика пользовательских рабочих станций, так и в режиме Reverse-Proxy.

2.2.1. Схема включения в режиме L2 (Bridge)

ArtX TLSproxy в режиме работы L2 (Bridge) выступает в роли сетевого моста, прозрачно проксируя все сетевые соединения между логическими сетевыми интерфейсами Internal и External. В этом случае ArtX TLSproxy не подменяет MAC-адреса и IP-адреса, и не выполняет функции маршрутизации или NAT-сервера. Когда ArtX TLSproxy выключен, ОС выполняет функции прозрачного сетевого моста, не модифицируя сетевой трафик. Когда ArtX TLSproxy работает в режиме L2 (Bridge), он использует следующие логические сетевые интерфейсы:

Internal Получение/отправка пакетов с пользовательских устройств.

External Отправка/получение пакетов с пользовательских устройств в сеть Интернет.

Management Управление ОС и ArtX TLSproxy. Для доступа по протоколам SSH и HTTPS необходим IP-адрес. Для обновления пакетов окружения

ArtX TLSproxy требуется доступ в Интернет.

Mirror Один или более сетевых интерфейсов для отправки копии развернутогого сетевого трафика системам-потребителям. Интерфейсы Internal и External в этом режиме работы полностью идентичны, их можно логически менять местами в веб-интерфейсе. Логическая схема включения ArtX TLSproxy в режиме L2 (Bridge) в сетевую инфраструктуру организации показана ниже.

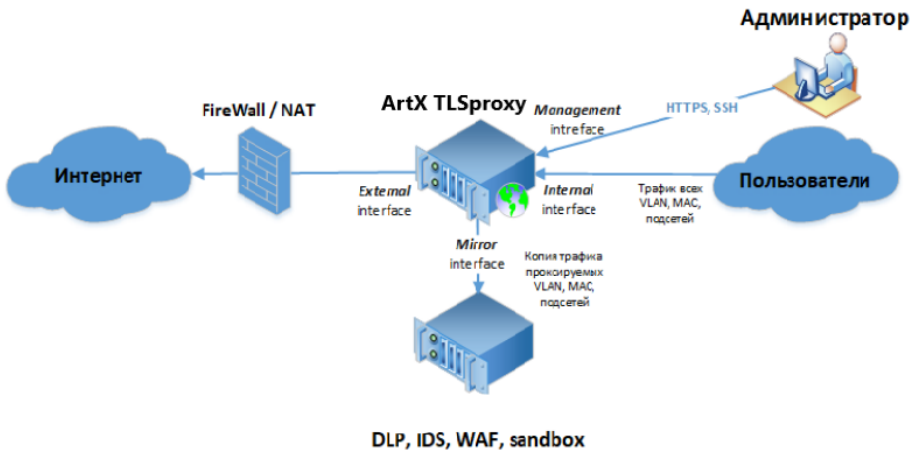


Рисунок 3. Логическая схема включения ArtX TLSproxy в режиме L2 (Bridge) в сетевую инфраструктуру организации.

ArtX TLSproxy обрабатывает все TCP-соединения вне зависимости с какого сетевого интерфейса они были инициированы: с Internal или External интерфейса.

Важно:

В виртуальной среде, вне зависимости от типа гипервизора (VmWare, Azure/Hyper-V, KVM), рекомендуется установка ArtX TLSproxy в режиме L3 (Router). При работе в среде виртуализации в режиме L2 (Bridge) развёртывание ArtX TLSproxy значительно усложняется за счет следующего:

1. Необходимости изолирования Internal, External и Mirror подсетей в разных VirtualSwitch во избежание возникновения сетевой петли.
2. В случае использования среды виртуализации VmWare возникает необходимость включения в VirtualSwitch опций Promiscuous Mode и Forget Transmit для сохранения MAC-адресов на сетевых интерфейсах Internal and External.

2.2.2. Схема включения в режиме L3 (Router)

ArtX TLSproxy в режиме работы L3 (Router) выступает в роли шлюза по умолчанию для проксируемых устройств (default gateway). Для работы в режиме L3 в ArtX TLSproxy следует настроить минимально необходимые правила маршрутизации. При этом следует иметь в виду, что ArtX TLSproxy не выполняет функции NAT-сервера или полнофункционального маршрутизатора, так как это не является его задачей и не предусмотрено в его архитектуре.

Когда ArtX TLSproxy работает в режиме L3 (Router), используются следующие логические сетевые интерфейсы:

Internal

Получение пакетов с пользовательских устройств. Требуется IP-адрес, на который будут направляться пакеты с пользовательских устройств в Интернет. Этот IP-адрес также следует указать как шлюз по умолчанию на проксируемых устройствах.

External

Отправка пакетов с пользовательских устройств в сеть Интернет. Для интерфейса External необходим IP-адрес с доступом в Интернет.

Management

Управление ОС и ArtX TLSproxy. Для доступа по протоколам SSH и HTTPS необходим IP-адрес. Для обновления пакетов окружения ArtX TLSproxy требуется доступ в Интернет.

Mirror

Один или более сетевых интерфейсов для отправки копии развернутого сетевого трафика системам-потребителям. IP-адреса на интерфейсах Internal и External должны находиться в разных подсетях. Логическая схема включения ArtX TLSproxy в режиме L3 (Router) в сетевую инфраструктуру организации показана ниже.

Такая схема включения идеально подходит для работы ArtX TLSproxy в виртуальных средах VmWare, Azure/Hyper-V, Linux KVM.

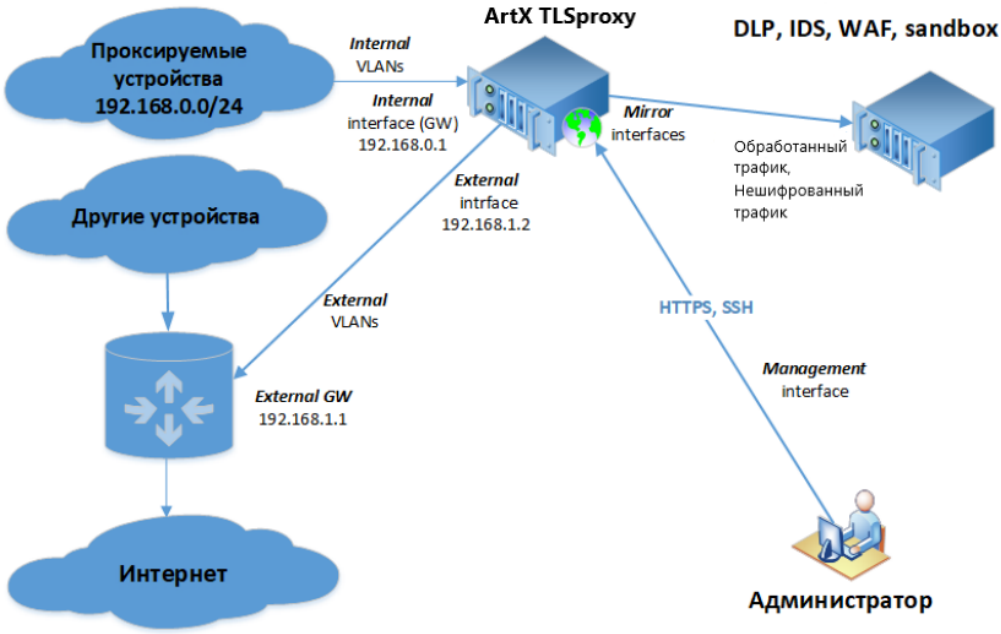


Рисунок 4. Логическая схема включения ArtX TLSproxy в режиме L3 (Router) в сетевую инфраструктуру организации.

2.2.3. Место ArtX TLSproxy в сети

ArtX TLSproxy спроектирован таким образом, чтобы имелась возможность установить его в любую точку сети, которую необходимо контролировать. Например, для мониторинга развернутого трафика какого-либо департамента организации самым простым решением будет установить ArtX TLSproxy "в разрыв" между коммутатором данного департамента и вышестоящим коммутатором. Богатые возможности по работе с исключениями также позволяет установить ArtX TLSproxy непосредственно перед UPLINK (точкой выхода в Интернет), предварительно указав список VLAN, MAC, IP, для которых необходимо выполнять проксирование. Для всех остальных устройств следует выполнять bypass.

Важно:
Рекомендуется устанавливать ArtX TLSproxy до NAT, чтобы в результате работы ArtX TLSproxy системы-потребители раскрытого трафика видели внутренние IP-адреса пользовательских устройств.

Если же необходимо направлять через ArtX TLSproxy не весь Интернет-трафик, а только определенные сегменты, необходимо изучить возможности имеющегося сетевого оборудования по поддержке PBR (Policy Based Routing) или другой аналогичной функциональности, позволяющей задавать правила для направления сетевого трафика в определенные сетевые интерфейсы по VLAN, MAC, IP или другим критериям.

Пример логической схемы ответвления Интернет-трафика через ArtX TLSproxy при помощи PBR:

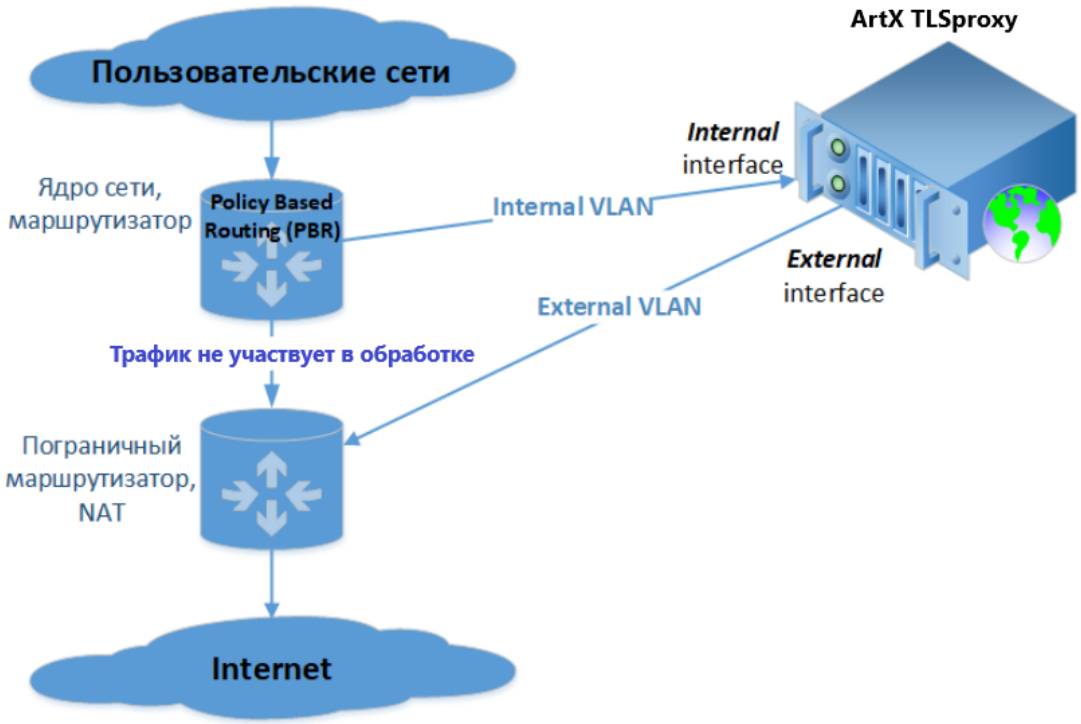


Рисунок 5. Пример логической схемы ответвления Интернет-трафика через ArtX TLSproxy при помощи PBR

2.3. Отказоустойчивость

ArtX TLSproxy поддерживает работу в отказоустойчивом режиме. Для различных схем включения отказоустойчивость реализуется разными методами.

В режиме L2 (Bridge) вы можете сконфигурировать отказоустойчивый кластер ArtX TLSproxy с помощью настроек сетевого оборудования, к которому подключены его серверы.

Для этого на коммутаторах (test-switch-1 и test-switch-2 на схеме ниже) настройте агрегацию сетевых интерфейсов (802.3ad, LACP). Для балансировки нагрузки на сетевом оборудовании используйте хеш srcip для test-switch-1 и хеш dstip для test-switch-2.

На рисунке ниже показан пример подключения двух серверов ArtX TLSproxy в отказоустойчивом режиме.

На первом этапе настройте PortChannel Active/Active между коммутаторами test-switch-1 и testswitch-2. На коммутаторе test-switch-1 укажите хеширование srcip, а на коммутаторе testswitch-2 укажите хеширование dstip.

Таким образом вы добьетесь равномерного распределения сетевых пакетов между серверами ArtX TLSproxy, а также целостного распределения сессий: RX- и TX-пакеты одной сессии всегда попадут на один и тот же сервер ArtX TLSproxy.

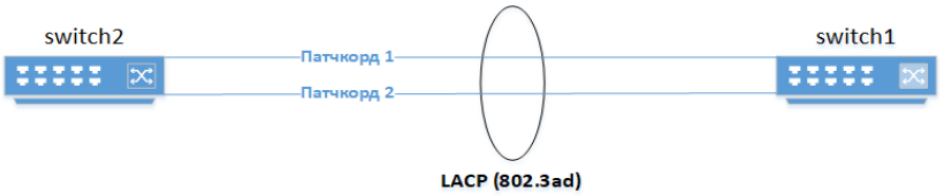


Рисунок 6. Пример подключения ArtX TLSproxy в отказоустойчивом режиме (L2), этап 1

На втором этапе установите сервер ArtX TLSproxy-1 в разрыв патчкорда 1. Подключите его физический интерфейс External к test-switch-2, затем подключите его физический интерфейс Internal к test-switch-1. Установите сервер ArtX TLSproxy-2 в разрыв патчкорда 2. Подключите его физический интерфейс External к test-switch-2, затем подключите его физический интерфейс Internal к test-switch-1.

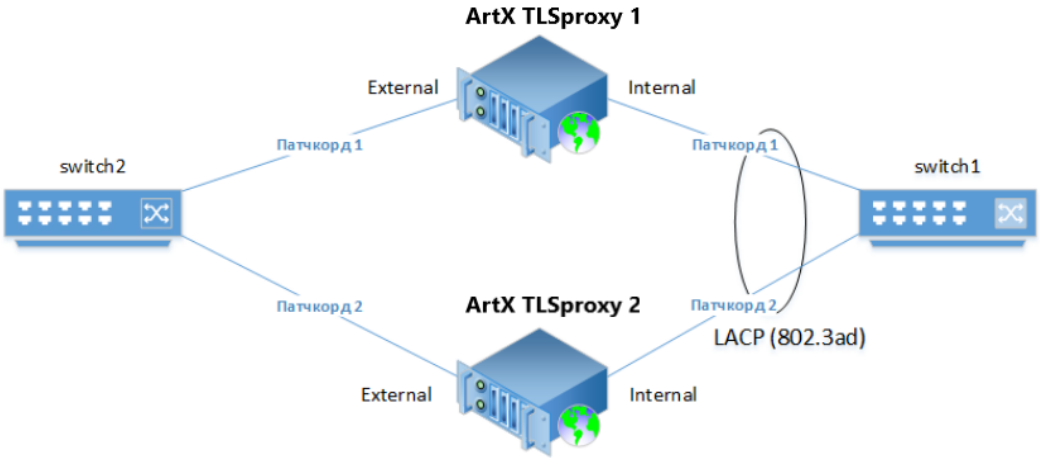


Рисунок 7. Пример подключения ArtX TLSproxy в отказоустойчивом режиме режиме (L2)

Для равномерного распределения нагрузки между серверами ArtX TLSproxy установите одинаковый алгоритм хеширования сетевых соединений на коммутаторах (srcmac/dstmac, srcip/dstip).

Используйте коммутаторы одной серии для гарантии одинаковой реализации механизма агрегации физических каналов. Также отказоустойчивость и балансировку нагрузки между серверами ArtX TLSproxy можно обеспечить при помощи внешнего балансировщика.

2.4. Конкурентные преимущества

Ниже представлены основные конкурентные преимущества ArtX TLSproxy.

★ **Разворачивание любых протоколов внутри SSL/TLS**

Альтернативные решения класса Proxy-All-in-One обеспечивают только развертку протоколов HTTPS и FTPS. При этом метод доставки развернутогого трафика по протоколу ICAP накладывает существенные ограничения на обработку трафика.

ArtX TLSproxy обеспечивает разворачивание непосредственно транспортного протокола SSL/TLS, предоставляя системе-потребителю передаваемый внутри SSL/TLS-тоннеля контент вне зависимости от протокола.

Это свойство делает ArtX TLSproxy применимым вместе с системами АСУ ТП, SIEM, UEBA, DLP, DPI и другими.

★ **Детектирование SSL/TLS сигнатурным методом**

ArtX TLSproxy определяет начало SSL/TLS-соединения сигнатурным методом, а не, например, по номеру порта. Это позволяет эффективно извлекать данные, передаваемые в тоннелях с любым уровнем вложенности. Например, в случае использования схемы Client -> HTTP-Proxy -> SOCKS-Proxy -> HTTPS-Proxy -> -> Server, система-потребитель развернутого трафика получит от ArtX TLSproxy данные, передаваемые по протоколу.

★ **Нет навязанной избыточной функциональности**

ArtX TLSproxy предназначен только для качественного решения задачи развертывания SSL/TLS - соединений. Нет необходимости покупки дорогостоящей системы класса Proxy-All-in-One, FireWall-All-in-One или UTM только лишь для контроля SSL/TLS - соединений.

★ **Мощный механизм исключений и автоисключений**

Большой набор критериев для формирования политики проксирования или исключения из проксирования позволяет:

1) Минимизировать риски прерывания критичных бизнес-процессов
2) Значительно упростить процесс внедрения за счет возможности создания политик исключений непосредственно на ArtX TLSproxy, а не на сетевом оборудовании
3) Значительно упростить поддержку за счет добавления исключений в автоматическом режиме.

★ **Поддержка виртуализации**

ArtX TLSproxy успешно функционирует как на физическом оборудовании, так и в самых распространенных средах виртуализации: VmWare, Linux KVM, Hyper-V.

★ **Масштабируемость и отказоустойчивость**

ArtX TLSproxy поддерживает установку в отказоустойчивом режиме с неограниченным количеством одновременно работающих серверов. Это позволяет использовать его в самых сложных и важных проектах.

★ **Несколько режимов работы**

ArtX TLSproxy может работать как в режиме L2 Bridge (Transparent), так и в режиме L3 Router (Explicit). Это делает возможным его использование в любой сетевой архитектуре.

★ **Поддержка** ООО “АртЭКС” осуществляет прямую техническую поддержку заказчиков и партнёров.

2.5. Системные требования

Минимальные системные требования физического сервера для устойчивой работы ArtX TLSproxy представлены в таблице ниже.

Канал	50 Mbps	150 Mbps	250 Mbps	500 Mbps	750 Mbps	1.5 Gbps	2.5 Gbps	5 Gbps
Пользователей	100	300	500	1000	1500	3000	5000	10000
CPU	1CPU*2 Cores	1CPU*4Cores	1CPU*4Cores	1CPU*4Cores	1CPU*4Cores	1CPU*6Cores	1CPU*8Cores	1CPU*10Cores
RAM	1 GB	4 GB	4 GB	8 GB	16 GB	32 GB	64 GB	128 GB
HDD	73 GB SAS 10K	2x73 GB SAS 10K RAID1	2x73 GB SAS 10K RAID1	2x146 GB SAS 10K RAID1	2x146 GB SAS 10K RAID1	2x300 GB SSD RAID1	2x300 GB SSD RAID1	4x500 GB SSD RAID10
NIC	4 x 100Mbps	4 x 1Gbps	4 x 1Gbps	4 x 1Gbps	4 x 1Gbps	4 x 10Gbps	4 x 10Gbps	4 x 10Gbps

Минимальные системные требования приведены исходя из следующих критериев (все критерии учитывают рабочее время):

★ Один пользователь в среднем потребляет 0.5Mbps от Интернет-канала.

★ Один пользователь в среднем держит 15 одновременных сетевых сессий.

★ Средним количеством пакетов в одной сессии считается 80 пакетов.

Настоятельно рекомендуется использовать сервер с 4 или более сетевыми адаптерами - это значительно упрощает схему включения, в том числе при работе со множеством VLAN.

Данные требования приведены без учета резервирования серверных компонентов.

Рекомендуется использовать ОЗУ DDR4 или новее.

Процессор должен поддерживать инструкции AES-NI. Количество ядер процессора напрямую влияет на производительность ArtX TLSproxy. В высоконагруженных инсталляциях (более 5Gbps) рекомендуется использовать процессоры линейки AMD Ryzen/Napple 16/32 Cores.

Для отказоустойчивой конфигурации рекомендуется использование двух и более серверов в одинаковой аппаратной конфигурации. Только в такой конфигурации в отказоустойчивой схеме с "холодным резервом" в случае отказа одного сервера второй сервер может полноценно обрабатывать пользовательский трафик.

В случае использования отказоустойчивой схемы с двумя и более активными серверами и равномерной балансировкой нагрузки, требования равномерно распределяются между всеми серверами.

При функционировании в виртуальной среде необходимо использовать сетевые адаптеры Intel E1000. Также рекомендуется использовать сетевые адаптеры Intel E1000 для обеспечения гарантированной бесперебойной работы ArtX TLSproxy.

3. Работа с ArtX TLSproxy

В данном разделе описаны основные аспекты работы с ArtX TLSproxy:
Выпуск сертификата
Установка
Управление работой ArtX TLSproxy
Работа с исключениями
Диагностика
Логирование

3.1. Выпуск сертификата

Для подмены сертификатов ArtX TLSproxy может использовать как самоподписанный сертификат, так и выпущенный в удостоверяющем центре.

В любом случае, на устройствах пользователей, трафик которых проходит через ArtX TLSproxy, в доверенных корневых центрах сертификации должен быть установлен либо сам сертификат ArtX TLSproxy, либо сертификат удостоверяющего центра, который использовался для выпуска сертификата ArtX TLSproxy.

Файлы сертификата, закрытого ключа и цепочки сертификатов хранятся в каталоге /etc/tlsproxy.

3.1.1. Самоподписанный сертификат

В случае установки с использованием веб-конфигуратора, самоподписанный сертификат создаётся на шаге 7. Сертификат. Сгенерированный в результате корректного заполнения полей формы сертификат и закрытый ключ автоматически создаются в каталоге /etc/tlsproxy.

Файл сертификата доступен в веб-интерфейсе в разделе Настройки — Сертификаты для загрузки и распространения по контролируемым устройствам. Подробнее работа веб-конфигуратора описывается в разделе Установка ArtX TLSproxy в автоматическом режиме.

В случае ручной установки для выпуска самоподписанного сертификата необходимо выполнить следующие команды.

1. Перейти в каталог хранения конфигурации и сертификатов:

```
cd /etc/tlsproxy
```

2. Сгенерировать ключ:

```
openssl genrsa -out ca.key 4096
```

3. Сгенерировать сертификат на основании созданного ранее ключа, 1826 - количество дней действия сертификата:

```
openssl req -new -x509 -sha512 -days 1826 -key ca.key -out ca.crt
```

Программа openssl во время выполнения этой команды запросит данные для полей сертификата, чтобы выполнить генерацию ключа для цепочки сертификатов:

★ Country Name (2 letter code) - код страны, например, RU

★ State or Province Name (full name) - республика, край, область. например, Altay

★ Locality Name (e.g., city) - город, поселок, деревня, например, Gorno-Altaysk

★ Organization Name (e.g., company) - название организации, например, Advanced Influence LTD

★ Organizational Unit Name (e.g., section) - название подразделения, например, Security Dept

★ Common Name (e.g., server FQDN or YOUR name) - FQDN-имя сервера ArtX TLSproxy, например, tlsproxy.ai.local

★ Email Address - Email-адрес, например, support@ai.com

4. Сгенерировать закрытый ключ для создаваемых "на лету" подменных сертификатов:

```
openssl genrsa -out chain.key 2048
```

Файл сертификата ca.crt необходимо установить на каждое устройство, SSL/TLS-трафик которого необходимо разворачивать при помощи ArtX TLSproxy, в том числе и на мобильные устройства, если такие имеются.

Устанавливать сертификат необходимо в раздел Доверенные корневые центры сертификации (Root CA).

Важно: Не всё программное обеспечение использует хранилище сертификатов операционной системы. Например, ПО Mozilla, такое как Thunderbird или Firefox, использует собственное хранилище. Для корректной работы такого ПО необходимо устанавливать самоподписанный сертификат во все используемые хранилища сертификатов на устройстве.

3.1.2. Выпуск сертификата ArtX TLSproxy в УЦ организации

Если в организации используется домен, то по умолчанию на всех устройствах при включении в состав домена в раздел Доверенные корневые центры сертификации (Root CA) устанавливается корневой сертификат данного домена.

В таком случае имеется возможность выпустить сертификат по запросу, сгенерированному в удостоверяющем центре организации.

Сертификат ArtX TLSproxy, выпущенный на основании корневого доменного сертификата, автоматически считается доверенным для всех хранилищ сертификатов на устройствах пользователей, где установлен корневой доменный сертификат.

Важно: В целях повышения безопасности следует формировать CSR-запрос и выпускаемый сертификат с поддержкой алгоритма подписи SHA256 или SHA512, так как SHA1 считается устаревшим для всех современных веб-браузеров и других клиентов SSL/TLS.

Проверить текущую версию алгоритма подписи центра сертификации для Windows Server можно с помощью оснастки certsrv.msc:

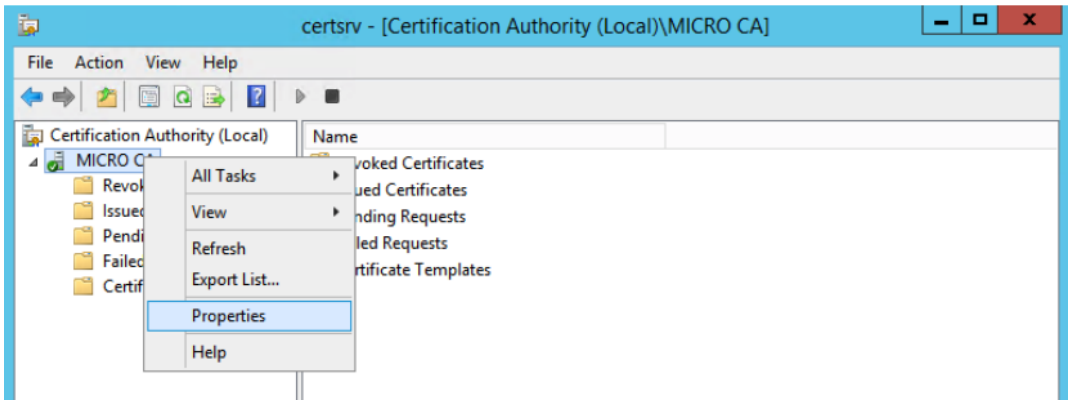


Рисунок 8. Окно настройки certsrv.msc

Затем следует нажать правой кнопкой мыши на пункте меню Properties:

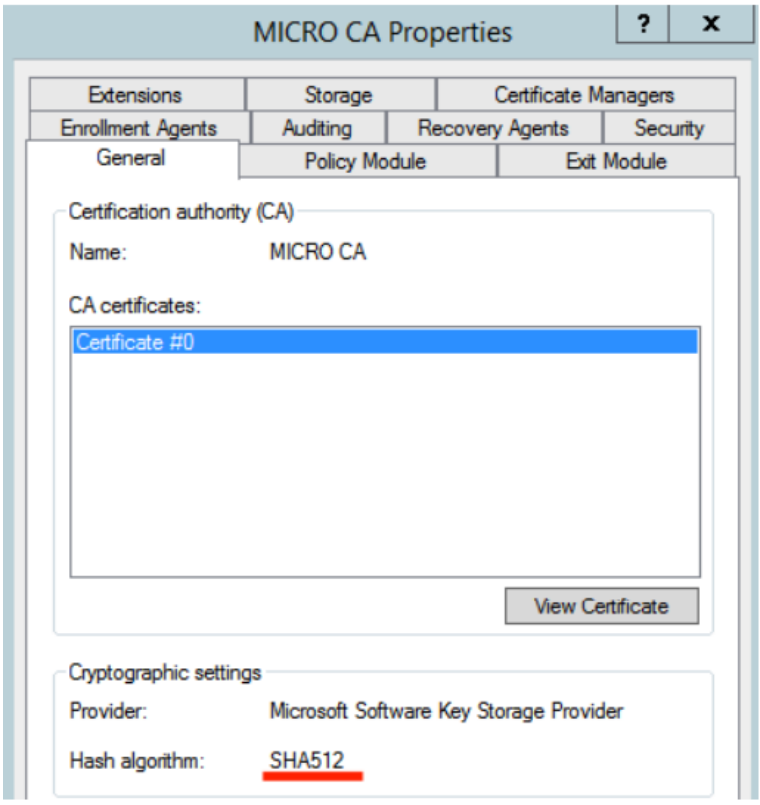


Рисунок 9. Окно настройки алгоритма подписи центра сертификации

Для изменения алгоритма подписи SHA256 необходимо на сервере с ролью удостоверяющего центра выполнить в PowerShell следующую команду (данная команда приведет к перевыпуску доменного корневого сертификата):

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

Чтобы сделать CSR-запрос на выпуск сертификата, необходимо выполнить следующие действия.

1. Создать CSR-запрос сертификата:

1.1. Войти на Windows-машину, включенную в состав домена, машины которого должны проксироваться ArtX TLSproxy. Входить необходимо под доменным пользователем, обладающим правами локального администратора на данной машине, а также входящего в доменную группу Cert Publishers

1.2. Запустить утилиту управления сертификатами локального компьютера certlm.msc

1.3. В разделе Certificates - Local Computer -> Personal кликнуть в меню Actions -> All Tasks -> Advanced Operations -> Create Custom Request....

1.4. В окне Before You Begin нажать Next

1.5. В окне Select Certificate Enrollment Policy выбрать Confirured by your administrator -> Active Directory Enrollment Policy и кликнуть Next.

1.6. В окне Custom request выбрать Template: Subordinate Certification Authority, Request format: PKCS #10, кликнуть Next

1.7. В окне Certificate Information в выбранном по умолчанию элементе списка Subordinate Certification Authority кликнуть Details и затем Property

1.8. В открывшемся окне во вкладке Subject выставить Type: Common Name, вписать желаемое значение в поле Value (например, tlsproxy.ai.com для домена ai.com), нажать на кнопку Add для добавления атрибута в CSR-запрос. Аналогично выставить другие необходимые атрибуты будущего сертификата. Убедиться, что во вкладке Extensions для параметра Key usage выставлены опции CRL signing, Digital signature и Key certificate signing. Во вкладке Private key в параметре Key options указать Key size равным 2048 или 4096. Кликнуть Apply и OK.

1.9. В окне Where do you want to save the offline request? указать путь для сохранения файла CSR-запроса. Формат (File format) при этом выбрать Base 64. Далее необходимо передать специалистам Удостоверяющего Центра сохраненный файл CSR-запроса.

2. Сформировать файл сертификата для ArtX TLSproxy по CSR-запросу (выполняется специалистами Удостоверяющего Центра).

2.1. На доменной машине с ролью удостоверяющего центра из-под пользователя, имеющего права на формирование сертификатов, открыть оснастку Certification Authority (certsrv.msc)

2.2. Выбрав в меню соответствующий домену удостоверяющий центр, кликнуть меню Action -> All Tasks -> Submit new request....

2.3. В открывшемся окне указать путь к полученному файлу CSR-запроса, кликнуть Next
2.4. Указать путь для сохранения сгенерированного файла сертификата, кликнуть Next
2.5. Передать сгенерированный файл сертификата в подразделение информационной безопасности.
В результате перечисленных действий вы получите файл сертификата, который следует переименовать в ca.crt и перенести его в каталог /etc/tlsproxy сервера ArtX TLSproxy.

3. Экспортировать закрытый ключ

3.1. В открытом в пункте 1 окне утилиты управления сертификатами локального компьютера certlm.msc в разделе Certificates - Local Computer -> Certificate Enrollment Requests -> Certificates найти созданный ранее CSR-запрос, выделить его и кликнуть в меню Actions -> All Tasks -> Export
3.2. В открывшемся окне кликнуть Next, выбрать Yes, export the private key, Next, Next, установить флаг Group or user names (recommended). Убедиться, что в списке пользователей указан текущий пользователь, Next Выбрать путь и имя файла, в котором сохранить закрытый ключ, Next, Finish.
3.3. Открыть текстовым редактором (например, notepad.exe) экспортированный файл закрытого ключа, скопировать блок текста закрытого ключа -----BEGIN PRIVATE KEY-----— ... —-- END PRIVATE KEY---- в новый текстовый файл и сохранить его с именем ca.key. Полученный файл ca.key скопировать в каталог /etc/tlsproxy сервера ArtX TLSproxy. Если при установке ArtX TLSproxy используется веб-конфигуратор, то полученную пару ключ/сертификат необходимо загрузить на шаге 7. Сертификат. Подробнее работа с веб-конфигуратором описана в разделе Установка ArtX TLSproxy в автоматическом режиме.

3.1.3. Распространение сертификата на устройства

Общая концепция

Для корректной работы ArtX TLSproxy требуется наличие доверия к сертификату ArtX TLSproxy. А для этого требуется наличие доступа к контролируемым устройствам. В случае доменной инфраструктуры удаленный доступ к устройствам предполагается сам собой.

В случае с устройствами в рабочей группе, либо функционирующих на базе ОС Linux, Mac OS, Android или iOS, существует несколько способов установки сертификата в список доверенных:

Удаленный доступ к управлению устройствами

Ниже в данном разделе описываются методы удаленного добавления сертификата ArtX TLSproxy в список надежных для различных ОС.

***hotSpot*-страница**

Web-ресурс, доступный всем контролируемым устройствам, содержащий ссылку для загрузки сертификата ArtX TLSproxy и инструкции по его самостоятельной установке для различных ОС. Этот Web-ресурс также может содержать описание политик информационной безопасности в организации, предусматривающих добавление данного сертификата в список доверенных сертификатов на всех устройствах.

Доменные устройства

В случае с доменными устройствами сертификат, выпущенный в удостоверяющем центре Active Directory, распространять не обязательно. Групповыми политиками при включении устройства в состав домена автоматически добавляется корневой доменный сертификат, на основании которого выпускается промежуточный сертификат ArtX TLSproxy.

Таким образом, клиентское программное обеспечение, использующее SSL/TLS, при проверке сертификата сервера (в роли которого выступает ArtX TLSproxy), убеждается в том, что в цепочке сертификатов ArtX TLSproxy присутствует уже установленный доверенный корневой сертификат домена.

В случае отсутствия удостоверяющего центра в домене, распространение сертификата выполняется на доменные устройства при помощи Group Policy Object.

3.2. Установка ArtX TLSproxy

В данном разделе описаны действия по установке ArtX TLSproxy шаг за шагом.

★ Требования к ОС и среде выполнения

★ Установка ArtX TLSproxy в автоматическом режиме

3.2.1. Требования к среде выполнения

ArtX TLSproxy может быть установлено на любую ОС, функционирующую на ядре Linux версии не ниже 4.4.0-124. Рекомендуется использовать ОС Ubuntu Server 16.04 LTS x64 с ядром версии 4.4.0-165 (пакеты linux-image-4.4.0-165-generic linux-headers-4.4.0-165-generic).

ArtX TLSproxy тесно взаимодействует с ядром файловой системы и сетевой подсистемой, поэтому рекомендуется отключить автоматическую установку обновлений для ОС и программного обеспечения. Также рекомендуется отключить NetworkManager, если он установлен.

После установки ОС необходимо настроить Management-интерфейс, выделив для него IP-адрес, доступный с рабочего места администратора ArtX TLSproxy. Также включите автоматический запуск данного интерфейса при старте ОС. Рекомендуется выделять статический IP-адрес, либо, в случае выделения адреса по DHCP, выполнять резервирование данного адреса для ArtX TLSproxy с фиксированным DNS-именем.

Важно: При планировании схемы включения ArtX TLSproxy рекомендуется резервировать для Management-интерфейса IP-адрес из той точки сети, доступ к которой с рабочего места администратора будет осуществляться в обход работающего ArtX TLSproxy.

3.2.2. Установка ArtX TLSproxy в автоматическом режиме

Для установки в автоматическом режиме от пользователя требуется минимальное количество действий.

Для начала установки ArtX TLSproxy в автоматическом режиме установите DEB-пакет, предоставленный поставщиком. Выполните команду:

```
cd <path-to-installer>
apt-get install ./<package name>.deb
```

В процессе установки DEB-пакета будет задан вопрос о создании необходимых зависимостей. Введите Y и нажмите Enter.

В результате установки DEB-пакета будут созданы все необходимые зависимости, а также актуальная поддерживаемая версия ядра Linux. Также будет создан стартовый скрипт и запущен веб-сервер.

В случае самого первого запуска ArtX TLSproxy будет запущен веб-конфигуратор, доступный по интерфейсу Management. Иначе будет запущен прикладной веб-интерфейс.

Если в консоли после установки появилась надпись:

```
Please restart server via 'shutdown -r now'
```

перезагрузите сервер, выполнив команду:

```
shutdown -r now
```

Далее перейдите в браузере по адресу: http://<ip-address-management>, где <ip-address-management> – это IP-адрес интерфейса Management. Затем выполните настройку ArtX TLSproxy в веб-конфигураторе.

Веб-конфигуратор содержит шаги, необходимые для успешной настройки ArtX TLSproxy. В результате успешного выполнения каждого шага в правом нижнем углу становится активной кнопка: Дальше. Эта кнопка ведёт к следующему шагу конфигуратора.

Шаг 1: Лицензия

На данном шаге кликните на кнопку Файл лицензии. В открывшемся окне укажите путь к файлу лицензии.

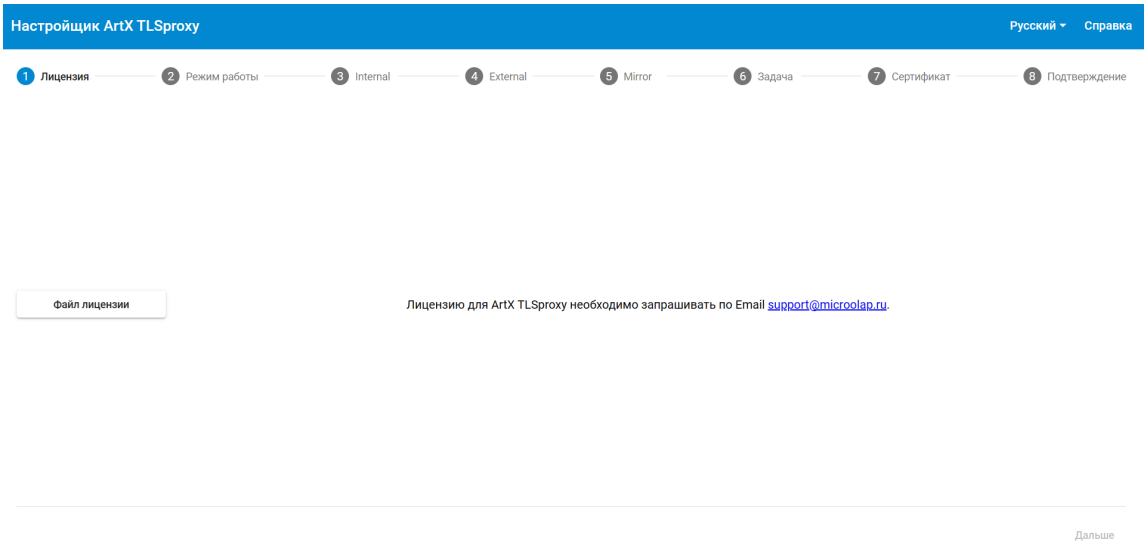


Рисунок 10. Установка ArtX TLSproxy в автоматическом режиме. Лицензия

Шаг 2. Режим работы

На данном шаге выберите режим работы ArtX TLSproxy. Для промышленной эксплуатации рекомендуется установить ArtX TLSproxy в режим L2 (Bridge).

Для проведения пилотного проекта, либо в случае использования виртуального сервера рекомендуется установить ArtX TLSproxy в режим L3 (Router).

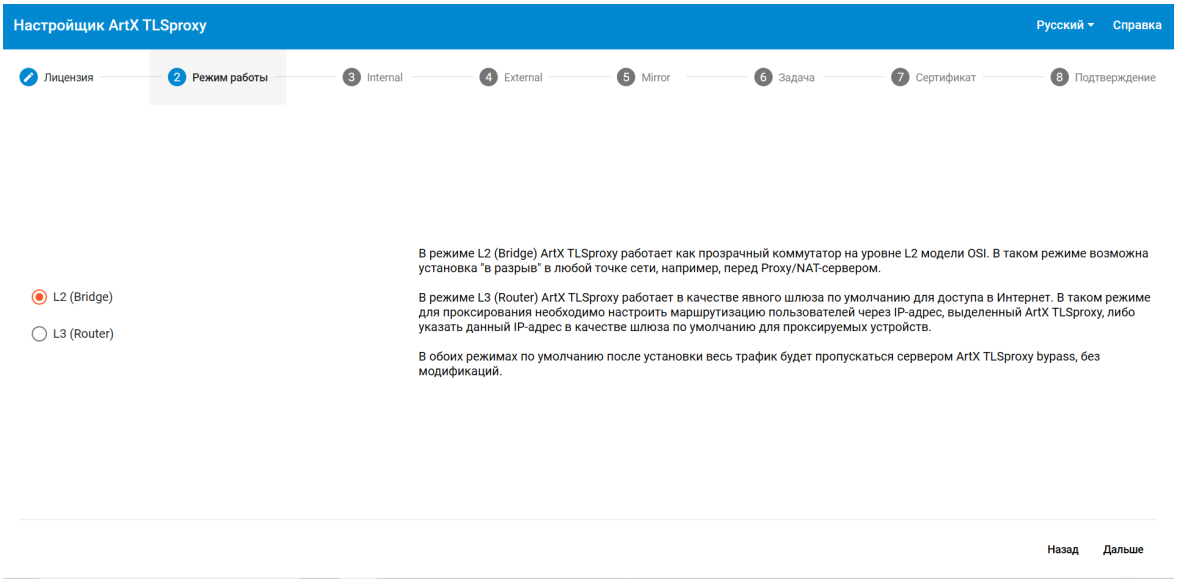


Рисунок 11. Установка ArtX TLSproxy в автоматическом режиме. Режим работы

Шаг 3: Internal

На данном шаге укажите сетевой интерфейс, выполняющий роль Internal. Интерфейс с этой ролью получает сетевые пакеты от клиентов сетевых соединений. В случае использования режима L2 (Bridge) интерфейсы Internal и External выполняют одинаковую роль и их можно менять местами.

Однако, в случае использования режима L3 (Router) для интерфейса Internal необходимо также указать настройки IP, на который явно или при помощи маршрутизатора будет направляться сетевой трафик пользователей. Например, этот IP-адрес можно указывать в качестве шлюза по умолчанию для подсети группы пользователей пилотного проекта.

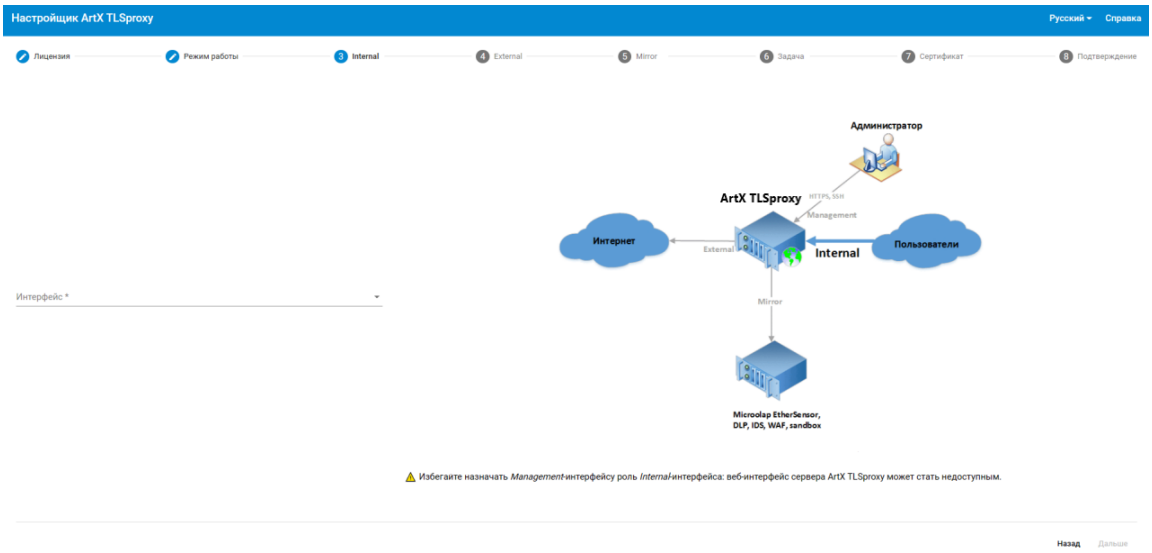


Рисунок 12. Установка ArtX TLSproxy в автоматическом режиме. Internal

Шаг 4: External

На данном шаге укажите сетевой интерфейс, выполняющий роль External. Интерфейс с этой ролью отправляет сетевые пакеты в сеть Интернет к серверам сетевых соединений. В случае использования в режиме L2 (Bridge) интерфейс External имеет аналогичную интерфейсу Internal роль и не имеет настроек IP.

В режиме L3 (Router) требуется указать IP-адрес и адрес шлюза по умолчанию, через который входящие Интернет-запросы будут направляться в Интернет.

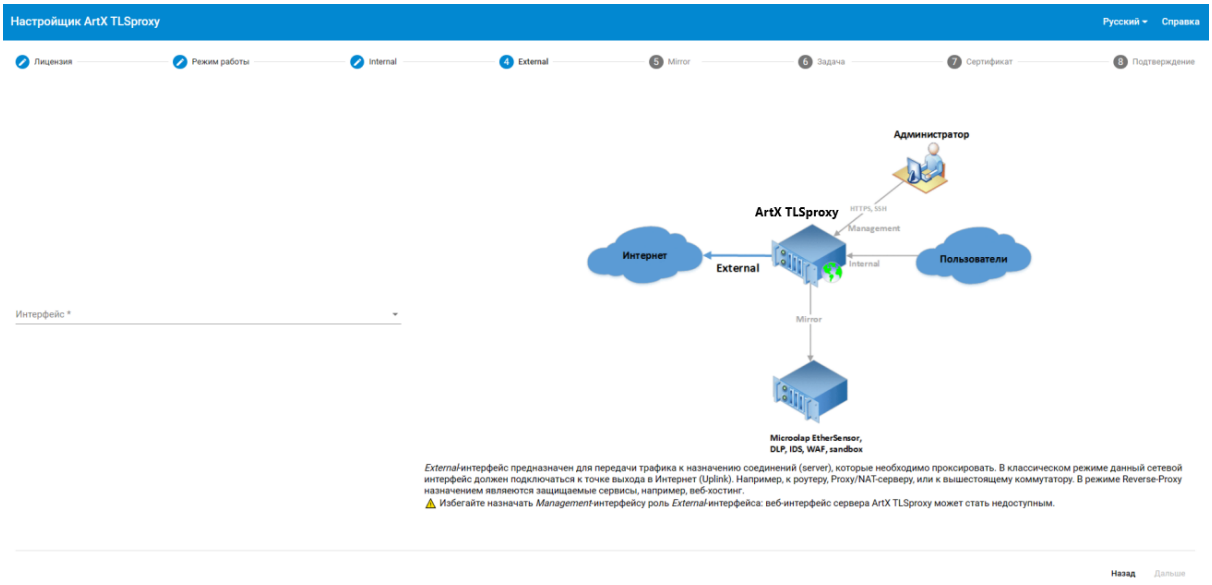


Рисунок 13. Установка ArtX TLSproxy в автоматическом режиме. External

Шаг 5: Mirror

На данном шаге укажите один или более сетевых интерфейсов Mirror, в которые ArtX TLSproxy будет отправлять копию развернутого трафика. Для добавления Mirror-интерфейсов нажмите на значок +.

Для каждого Mirror-интерфейса необходимо также указать MAC-адрес системы-потребителя, на который будет отправляться копия трафика. Также рекомендуется указать комментарий, благодаря которому можно будет позднее отличать данный сетевой интерфейс от других интерфейсов.

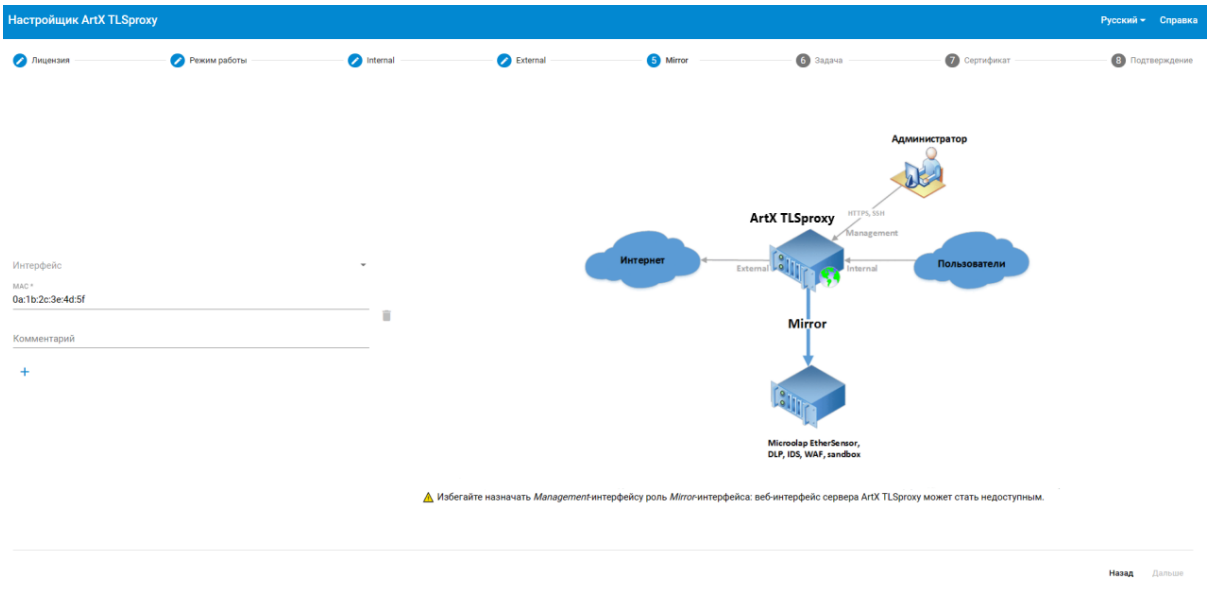


Рисунок 14. Установка ArtX TLSproxy в автоматическом режиме. Mirror

Шаг 6: Задача

На данном шаге укажите одну из следующих задач:

Контроль трафика организации

Классический режим мониторинга трафика пользователей организации при их доступе к Интернет-ресурсам.

Контроль защищаемых сервисов (Reverse-Proxy)

Режим контроля входящего трафика внешних Интернет-пользователей к корпоративным ресурсам в сегменте DMZ.

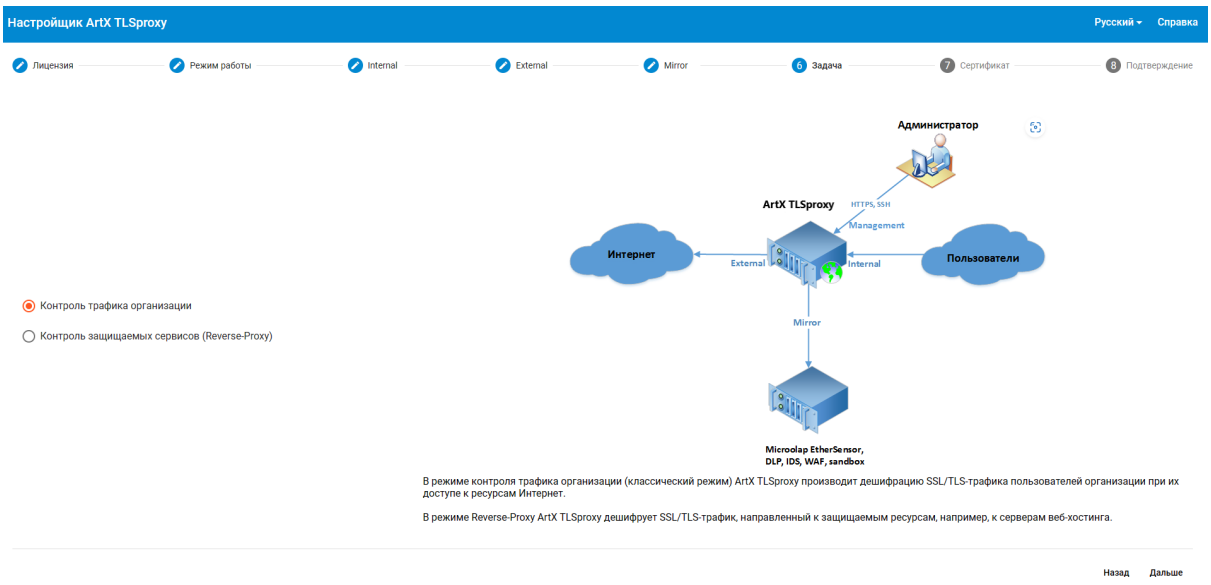


Рисунок 15. Установка ArtX TLSproxy в автоматическом режиме. Задача

Шаг 7: Сертификат

На данном шаге решите, какой сертификат будет использоваться в ArtX TLSproxy: самоподписанный сертификат или сгенерированный в доменном удостоверяющем центре.

Чтобы использовать самоподписанный сертификат, создайте его, нажав кнопку Генерировать.

Затем заполните все поля в открывшемся окне:

Bits (обязательное поле)

Стойкость ключа. Рекомендуемое значение: 4096.

Common name (обязательное поле)

Общее имя сертификата ArtX TLSproxy, из-под которого будут генерироваться "на лету" подменные сертификаты запрашиваемых веб-ресурсов. Обычно используется название tlsproxy, где соответствует интернет-домену организации, например, tlsproxy.ai.local.

Название страны

Название страны текущего местоположения сервера ArtX TLSproxy. Например, RU.

Регион

Название региона текущего местоположения сервера ArtX TLSproxy. Например, Altay.

Город

Название города текущего местоположения сервера ArtX TLSproxy. Например, Gorno-Altaysk.

Наименование организации

Наименование текущей организации. Например, Advanced Influence LTD.

Наименование подразделения

Наименование подразделения, в чьих целях эксплуатируется ArtX TLSproxy. Например, Security Dept.

Содержимое данных полей будет отображаться в сертификате. Сертификат можно будет просмотреть в веб-браузере или другом клиенте, трафик которого проксируется через ArtX TLSproxy.

Иногда содержимое данных полей помогает пользователю понять, куда следует обращаться в случае возникновения нештатных ситуаций в работе клиентского программного обеспечения при работе с Интернет-сервисами через ArtX TLSproxy.

Генерация сертификата и закрытого ключа может занять некоторое время, но не более пяти минут.

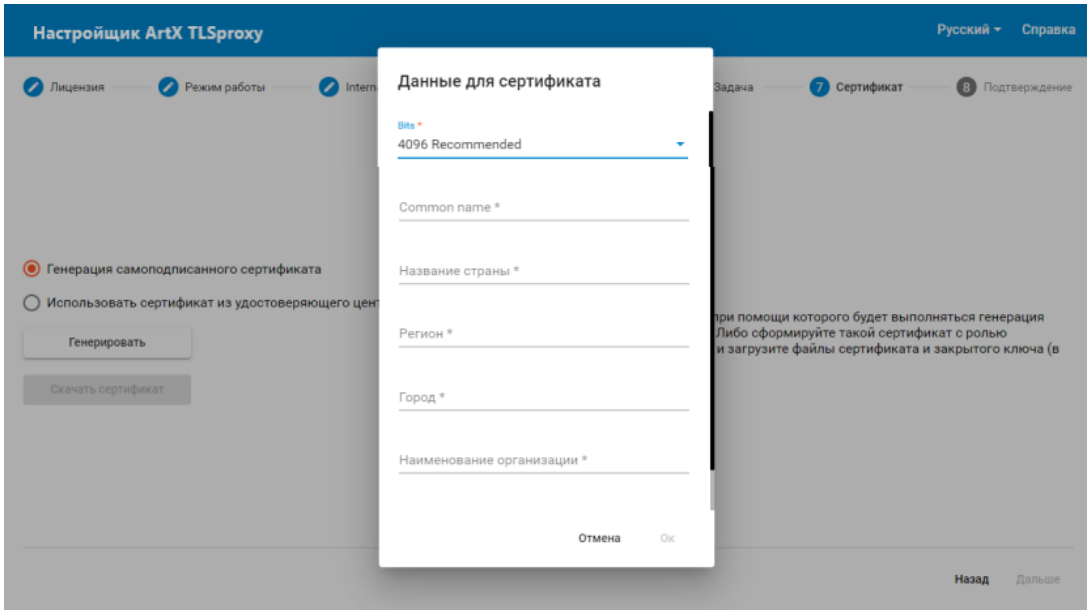


Рисунок 16. Установка ArtX TLSproxy в автоматическом режиме. Сертификат

В случае использования доменного сертификата создайте его согласно указаниям раздела Распространение сертификата и загрузите файлы сертификата и закрытого ключа, нажав кнопки Загрузить серт (.pem) и Загрузить ключ (.key). Ожидаемый формат файлов сертификата и закрытого ключа – PEM.

Шаг 8: Подтверждение

На данном шаге тщательно проверьте все введенные настройки, особенно роли сетевых интерфейсов. Затем кликните по кнопке Завершить.

После завершения настройки в веб-конфигураторе перезагрузите страницу, в результате будет автоматически запущен прикладной веб-интерфейс. Также будет запущено приложение ArtX TLSproxy с включенной опцией Черный список.

В этом режиме ArtX TLSproxy будет проксировать только трафик всех VLAN, MAC и IP-адресов, включенных в Черный список. Поскольку Черный список ещё пуст, на этот момент ArtX TLSproxy будет настроен на работу в режиме bypass.

3.2.3. Установка ArtX TLSproxy в ручном режиме

Данный раздел предназначен для сетевых специалистов и системных администраторов, обладающих достаточной экспертизой по части работы ОС Linux, сети, и приложения ArtX TLSproxy.

3.2.3.1. Установка окружения

Перед установкой ArtX TLSproxy настройте среду. Для этого выполните следующие действия в консоли Linux с правами пользователя root: 1. Обновите ядро Linux до версии 4.4.0-130-generic:

1. Обновите ядро Linux до версии 4.4.0-130-generic:

```
apt-get update apt-get install linux-image-4.4.0-130-generic linux-headers-4.4.0-130-generic linuximage-extra-4.4.0-130-generic
```

2. Отредактируйте GRUB, определив позицию необходимой версии ядра Linux в системе. Для этого выполните следующее:

```
ai@tlsproxy:~$ grep submenu /boot/grub/grub.cfg submenu 'Advanced options for Ubuntu' $menuentry_id_option 'gnulinux-advanced-dbcf053b6a2f-4128-b71b-c2486f896e91' {
```

В данном примере значением submenu будет gnulinux-advanced-dbcf053b-6a2f-4128-b71bc2486f896e91

2.1. Получите значение submenu, указанное в кавычках после переменной $menuentry_id_option

```
ai@tlsproxy:~$ grep gnulinux /boot/grub/grub.cfg | grep menuentry | grep 4.4.0-130 menuentry 'Ubuntu, with Linux 4.4.0-130-generic' --class ubuntu --class gnu-linux -- class gnu --class os $menuentry_id_option 'gnulinux-4.4.0-130-generic-advanceddbcf053b-6a2f-4128-b71b-c2486f896e91' { menuentry 'Ubuntu, with Linux 4.4.0-130-generic (recovery mode)' --class ubuntu --class gnu-linux --class gnu --class os $menuentry_id_option 'gnulinux-4.4.0-130- generic-recovery-dbcf053b-6a2f-4128-b71b-c2486f896e91' {
```

Здесь 4.4.0-130 - необходимая версия ядра.

2.2. Получите значение menuentry, указанное в кавычках после переменной $menuentry_id_option нужной строки (обычно первой). В данном примере значением menuentry будет gnulinux-4.4.0-130-generic-advanced-dbcf053b-6a2f-4128-b71b-c2486f896e91

ВНИМАНИЕ: Значения submenu и menuentry уникальны для каждой инсталляции, поэтому их необходимо определять для каждой новой инсталляции заново.

2.3. Отредактируйте конфигурационный файл GRUB:

```
vi /etc/default/grub
```

А именно:

★ Закомментируйте GRUB_HIDDEN_TIMEOUT=0

★ Закомментируйте GRUB_HIDDEN_TIMEOUT_QUIET=true

★ Установите GRUB_TIMEOUT=10,

★ Установите GRUB_DEFAULT="submenu>menuentry" где submenu и menuentry - значения, вычисленные выше,

★ Сохраните изменения и закройте файл. В данном примере параметр GRUB_DEFAULT должен выглядеть следующим образом:

```
GRUB_DEFAULT="gnulinux-advanced-dbcf053b-6a2f-4128-b71b-c2486f896e91>gnulinux-4.4.0-130-generic-advanced-dbcf053b-6a2f-4128-b71b-c2486f896e91"
```

3. Отключите Active-State Power Management, для этого в файле /etc/default/grub добавьте к параметру GRUB_CMDLINE_LINUX_DEFAULT значение pcie_aspm=off.
Например:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet splash pcie_aspm=off"
```

4. Примените изменения для GRUB:

```
update-grub
```

5. Перезагрузите систему:

```
reboot
```

6. После перезагрузки системы убедитесь, что загрузилась нужная версия ядра Linux:

```
# uname -r 4.4.0-130-generic
```

7. Обновите все пакеты:

```
apt-get update
apt-get upgrade
```

8. Установите необходимый набор утилит:

```
apt-get install telnet bridge-utils vlan zip ifstat iproute2 xtables-addons-common ipset build-essential
```

9. Убедитесь в том, что на всех сетевых интерфейсах отключены следующие функции: GSO, GRO, TSO. Для отключения этих функций выполните следующую команду:

```
ethtool -K eth0 gso off gro off tso off
```

Здесь eth0 - имя сетевого интерфейса. При необходимости добавьте выполнение данной команды в конфигурационный файл start_env.sh.

3.2.3.2. Каталоги ArtX TLSproxy

После настройки среды выполнения ArtX TLSproxy необходимо создать каталоги в файловой системе:
1. Каталог установки ArtX TLSproxy:

```
mkdir /opt/tlsproxy
```

2. Каталог для монтирования виртуального диска ArtX TLSproxy:

```
mkdir /opt/tlsproxy/disk
```

3.2.3.3. Установка ArtX TLSproxy

Для установки исполняемых модулей ArtX TLSproxy необходимо скопировать виртуальный диск с ArtX TLSproxy на сервер в каталог /opt/tlsproxy.
1. Смонтируйте виртуальный диск с программным обеспечением ArtX TLSproxy:

```
mount -o loop /opt/tlsproxy/disk /opt/tlsproxy/disk
```

2. Скопируйте конфигурационный файл (по умолчанию это файл с именем config.json):

```
cp /opt/tlsproxy/disk/contrib/config.json /etc/tlsproxy
```

Или запустите Веб-конфигуратор:

```
cd /opt/tlsproxy/disk sh _install.sh
```

3. В случае, если необходимо использовать собственный файл окружения, необходимо скопировать файл настроек сетевого окружения start_env.sh:

```
cp /opt/tlsproxy/disk/contrib/start_env.sh /opt/tlsproxy
```

В данном случае необходимо также выставить параметр "createEnv": false в конфигурационном файле config.json.
Далее необходимо отредактировать конфигурационный файл config.json и, в случае необходимости, файл сетевого окружения ArtX TLSproxy.
Если вы настроили сетевое окружение приложения ArtX TLSproxy правильно, то сетевой трафик должен проходить через сервер ArtX TLSproxy без модификаций (bypass).

3.2.3.4. Конфигурационный файл сетевого окружения

ВНИМАНИЕ: Конфигурационный файл сетевого окружения ArtX TLSproxy не является обязательным. Все описанные в этом файле действия система производит автоматически при запуске. Если вам необходимо настроить собственное сетевое окружение для ArtX TLSproxy, вы можете воспользоваться этим файлом, определив в конфигурационном файле config.json параметр "createEnv": false. Используйте файл с настройками сетевого окружения ArtX TLSproxy только на свой страх и риск.

Настройки сетевого окружения ArtX TLSproxy определены в файле /opt/tlsproxy/start_env.sh. Описание параметров приведено ниже.

Директива	Описание	Пример
IFACE-UP	Имя сетевого интерфейса External	IFACE_UP=eth1
IFACE_DOWN	Имя сетевого интерфейса Internal	IFACE_DOWN=eth2
IFACE_MIRROR	Имя сетевого интерфейса Mirror	IFACE_MIRROR=eth3
PROXY_IP	IP-адрес и маска подсети	PROXY_IP=192.168.100.5/29

	логического сетевого интерфейса Bridge	
PROXY_GW	IP-адрес шлюза по умолчанию для сетевого интерфейса External (шлюз по умолчанию для доступа в Интернет)	PROXY_GW=192.168.100.1/29

После корректной настройки сетевого окружения сетевой трафик должен проходить через сервер ArtX TLSproxy bypass, без модификаций.
Ниже представлен пример файла настройки сетевого окружения start_env для работы в режиме L2 (Bridge):

```
#!/bin/sh
# Load modules

modprobe xt_TPROXY
modprobe 8021q
modprobe bridge
modprobe ebtables
modprobe ebtable_filter
modprobe ip_set

# If Net Namespace already exists - exit
ip netns list | grep -q proxy && exit 0

# Define Network Interfaces' names
IFACE_UP=ens33
IFACE_DOWN=ens34
IFACE_MIRROR=ens36

# Define IP address for Bridge Interface (for Gateway availability checks only) PROXY_IP=10.10.10.2/24

# Gateway for Bridge interface (Uplink gateway) PROXY_GW=10.10.10.1

# Name for Bridge interface IFACE_BR=br0

# Insert TLSproxy kernel modules
insmod ./disk/tlsproxy/kernel/`uname -r`/fw.ko
insmod ./disk/tlsproxy/kernel/`uname -r`/sock0.ko

echo 1 > /proc/sys/kernel/hung_task_panic
echo 1 > /proc/sys/kernel/hardlockup_all_cpu_backtrace
echo 1 > /proc/sys/kernel/hardlockup_panic
echo 1 > /proc/sys/kernel/softlockup_all_cpu_backtrace
echo 1 > /proc/sys/kernel/softlockup_panic

# Add Net Namespace
```

```
ip netns add proxy

# Inherit sysctl params
ip netns exec proxy sysctl -f /etc/sysctl.conf

# Move network interfaces (Internal, External and Mirror) into the namespace
ip link set $IFACE_DOWN netns proxy
ip link set $IFACE_UP netns proxy
ip link set $IFACE_MIRROR netns proxy

# Preparing interfaces
ip netns exec proxy ifconfig lo 127.0.0.1/8
ip netns exec proxy ifconfig $IFACE_DOWN up
ip netns exec proxy ifconfig $IFACE_UP up
ip netns exec proxy ifconfig $IFACE_MIRROR up

# Enable promisc Mode on Mirror interface
ip netns exec proxy ifconfig $IFACE_MIRROR promisc

# Add Bridge interface and linking Internal and External interfaces to Bridge
ip netns exec proxy brctl addbr $IFACE_BR
ip netns exec proxy brctl addif $IFACE_BR $IFACE_DOWN
ip netns exec proxy brctl addif $IFACE_BR $IFACE_UP

# Add IP address for Bridge interface (for check Gateway availability only) ip netns exec proxy ifconfig $IFACE_BR $PROXY_IP

# Define rp_filter = 0 for all interfaces (needed for normal bridge operation)
ip netns exec proxy sysctl -w net.ipv4.conf.${IFACE_UP}.rp_filter=0
ip netns exec proxy sysctl -w net.ipv4.conf.${IFACE_DOWN}.rp_filter=0
ip netns exec proxy sysctl -w net.ipv4.conf.${IFACE_BR}.rp_filter=0

# Add ipset lists (FireWall bypass, WhiteList)
ip netns exec proxy ipset create whitelist hash:net
ip netns exec proxy ipset create fw_bypass hash:net

# iptables configuring
ip netns exec proxy iptables -t mangle -N DIVERT
ip netns exec proxy iptables -t mangle -A DIVERT -j MARK --set-mark 1
ip netns exec proxy iptables -t mangle -A DIVERT -j ACCEPT
ip netns exec proxy iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
ip netns exec proxy iptables -t mangle -A PREROUTING -p tcp -j TPROXY \ --tproxy-mark 0x1/0x1 --
on-port 8843 --on-ip 127.0.0.1

# Add mark rule
ip netns exec proxy
ip -f inet rule add fwmark 1 lookup 100 ip netns exec proxy ip -f inet route add local default dev
$IFACE_BR table 100
# Add default gw for Bridge interface ip netns exec proxy route add default gw $PROXY_GW
```

3.2.3.5. Автозапуск ArtX TLSproxy

Для настройки автоматического запуска ArtX TLSproxy выполните следующие действия:

1. Создайте стартовый скрипт /opt/tlsproxy/systemctl.sh:

```
#!/bin/sh

if [ ! -f /opt/tlsproxy/disk/_start_tlsproxy.sh ]; then
|       /bin/mount -o loop /opt/tlsproxy/tlsproxy.sqf /opt/tlsproxy/disk
fi

if [ ! -f /var/run/netns/proxy ]; then
|       /sbin/ip netns add proxy
fi

cd /opt/tlsproxy/disk
case "$1" in
 start)
        echo -n "Starting TLSproxy..."
        modprobe ip_tables
        modprobe iptable_filter
        modprobe xt_TPROXY
        modprobe 8021q
        modprobe bridge
        modprobe ip_set
sh _start_tlsproxy.sh
echo -n "TLSproxy has been started."
;;
stop)
echo -n "Stopping TLSproxy..."
sh _stop_tlsproxy.sh
cd /opt/tlsproxy/
/bin/umount /opt/tlsproxy/disk
echo -n "TLSproxy has been stopped."
;;
esac
```

2. Установите права на выполнение скрипта:

```
chmod +x /opt/tlsproxy/systemctl.sh
```

3. Добавьте службу в systemctl, создав файл /lib/systemd/system/tlsproxy.service:

```
[Unit]
Description=TLSproxy
Documentation=
After=network-online.target
```

```
[Service]
User=root
Group=root
LimitNOFILE=65536
RemainAfterExit=yes
ExecStart=/opt/tlsproxy/systemctl.sh start
ExecStop=/opt/tlsproxy/systemctl.sh stop
Type=oneshot
KillMode=control-group

[Install]
WantedBy=multi-user.target
Alias=tlsproxy.service
```

4. Установите права доступа к скрипту и включите его автозапуск при загрузке сервера:

```
chmod 664 /etc/systemd/system/tlsproxy.service
systemctl daemon-reload
systemctl enable tlsproxy.service
```

5. Для просмотра лога запуска службы ArtX TLSproxy используйте команду journalctl:

```
journalctl -u tlsproxy.service
```

3.2.3.6. Управление работой ArtX TLSproxy

Для управления ArtX TLSproxy вам понадобятся права root на серверах. Также все команды по управлению ArtX TLSproxy необходимо выполнять в контексте сетевого окружения по умолчанию. См. раздел Диагностика.
Для запуска ArtX TLSproxy выполните команду:

```
systemctl start tlsproxy.service
```

Для остановки ArtX TLSproxy выполните команду:

```
systemctl stop tlsproxy.service
```

После остановки ArtX TLSproxy весь сетевой трафик, направленный через него, будет пропускаться без изменений, не терминируя сетевые соединения (bypass).
Для перезапуска ArtX TLSproxy выполните команду:

```
systemctl restart tlsproxy.service
```

Для проверки состояния ArtX TLSproxy выполните команду:

```
systemctl monitor tlsproxy.service
```

Для проверки наличия работающих процессов приложения ArtX TLSproxy выполните команду:

```
ps aux | grep [t]cpproxy
```

При нормальной работе результат должен отобразить хотя бы один работающий процесс ArtX TLSproxy.

3.3. Управление ArtX TLSproxy

В данном разделе описаны действия по управлению ArtX TLSproxy как через прикладной веб-интерфейс, так и при помощи команд и утилит в консоли Linux.

3.3.1. Веб-интерфейс

Основная работа с ArtX TLSproxy происходит с использованием прикладного веб-интерфейса.

Для доступа к веб-интерфейсу ArtX TLSproxy следует использовать веб-браузер Google Chrome версии 69 или выше, либо Mozilla Firefox 61 или выше.

Чтобы открыть прикладной веб-интерфейс ArtX TLSproxy, введите в адресной строке браузера http://<IP-адрес или FQDN сервера ArtX TLSproxy>.

ВАЖНО: В случае необходимости доступа к веб-интерфейсу по протоколу HTTPS добавьте в каталог /etc/tlsproxy/ файлы сертификата и закрытого ключа с именами httpscert.pem и https-key.pem соответственно. Также необходимо указать параметр "https": {"enable": true} в конфигурационном файле config.json.

Для доступа к веб-интерфейсу на странице аутентификации используйте следующие учётные данные:
Логин: admin
Пароль: chgstr4

На рисунке ниже представлен прикладной веб-интерфейс ArtX TLSproxy и его ключевые элементы.

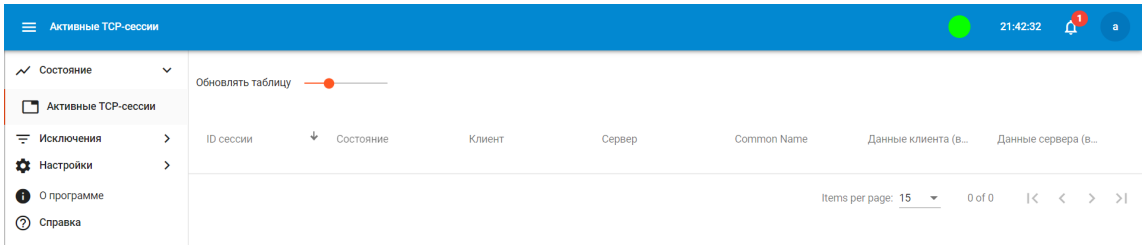


Рисунок 17. На рисунке ниже представлен прикладной веб-интерфейс ArtX TLSproxy.

В правом верхнем углу расположены следующие иконки, описанные ниже справа налево:
1. Текущий пользователь. При нажатии на иконку пользователя появляется меню Профиль с персонифицированными настройками пользователя ArtX TLSproxy, а также кнопка Выход, завершающая сессию работы с веб-интерфейсом.
2. Область уведомлений. Здесь появляются уведомления о событиях изменения настроек, синхронизации между серверами ArtX TLSproxy, или другие события, требующие действий от администратора системы.
3. Индикатор состояния ArtX TLSproxy: зеленый кружок означает, что ArtX TLSproxy запущен и выполняет проксирование, желтый кружок означает, что ArtX TLSproxy выключен и все соединения проходят через сервер ArtX TLSproxy прозрачно (без терминирования сессий, как через обычный коммутатор), красный кружок означает, что веб-сервер ArtX TLSproxy не запущен или недоступен.

3.3.1.1. Раздел "Состояние"

Раздел Состояние отображает текущее состояние работы ArtX TLSproxy. Включает подраздел Активные сессии.

3.3.1.1.1. Активные сессии

Подраздел Активные сессии предназначен для просмотра и мониторинга всех TCP-сессий, полученных приложением ArtX TLSproxy.

Отображаемые в данном разделе сессии не обязательно проксируются сервером ArtX TLSproxy, но они им терминируются. Их появление в данном разделе означает, что сессия от клиента (источника) была установлена с сервером ArtX TLSproxy, и от ArtX TLSproxy была установлена аналогичная сессия с сервером назначения сессии.

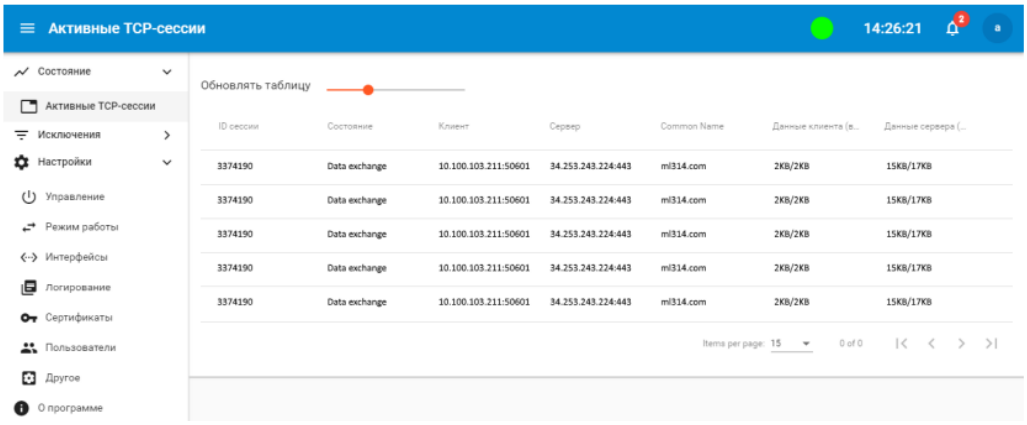


Рисунок 18. Раздел активные сессии

Данная страница содержит таблицу текущих сессий со следующими столбцами:

ID сессии

Уникальный идентификатор сессии. Используется для анализа проблемных соединений в логах ArtX TLSproxy, а также для возможности отслеживания новых соединений вверху списка при сортировке по данному полю.

Состояние

Текущее состояние сессии:

Инициализация

Инициализация нового соединения

Подключение клиента

SSL Handshake с клиентом соединения

Подключение сервера

SSL Handshake с сервером соединения

Ожидание сервера

Истекло время ожидания ответа от сервера

Обмен данными

Активная установленная сессия, идет обмен данными или ожидание данных

Bypass

Данное соединение проходит bypass

Закрытие

Соединение закрывается

Разрыв

Принудительный разрыв соединения

Остановка

Остановка соединения по инициативе клиента или сервера

Ошибка

Ошибка.

Клиент

Источник соединения, устройство, инициировавшее соединение к серверу, а также порт на стороне клиента, с которого было открыто данное соединение

Сервер

Назначение соединения, сервер в сети Интернет или локальной сети, к которому обращено данное соединение, а также порт сервера

Common Name

Имя сервера из сертификата (SNI), возвращенного сервером по запросу клиента (обычно это домен URL в HTTPS-соединениях)

Данные клиента (вх/исх)

Объем данных, полученных ArtX TLSproxy от клиента и отправленных ArtX TLSproxy в ответ клиенту

Данные сервера (вх/исх)

Объем данных, отправленных ArtX TLSproxy серверу назначения соединения и полученных от него в ответ.

Над каждым столбцом имеется поле для поиска необходимых значений, привязанное к соответствующему столбцу.

Данная таблица обновляет данные автоматически, частота обновления регулируется слайдером. При необходимости есть возможность остановить обновление таблицы путем смещения слайдера в крайнее левое положение.

В этом случае останавливается автообновление таблицы и вы можете скопировать, отфильтровать или проанализировать необходимые соединения, пока они не закрылись.

3.3.1.2. Раздел "Исключения"

Раздел Исключения предназначен для работы в прикладном веб-интерфейсе ArtX TLSproxy с исключениями из проксирования и содержит следующие подразделы:

- ★ Группы
- ★ Исключения
- ★ Неисключаемые ресурсы
- ★ Автоисключения
- ★ Белый/Чёрный список

Следует помнить, что обработка исключений из проксирования может происходить на разных уровнях:

На уровне ядра ОС

За исключения на уровне ядра ОС отвечает модуль fw программного обеспечения ArtX TLSproxy. Модуль fw проверяет низкоуровневые данные, такие как VLAN, MAC, IP и порты соединения. Правила модуля fw позволяют исключать из проксирования без терминирования сессии, направляя пакеты в служебный Bridge-интерфейс.

На уровне приложения ArtX TLSproxy

На этом уровне, помимо описанных выше критериев, добавляется возможность проверять Common Name (SNI) по точному совпадению, wildcard-маске или регулярному выражению.

3.3.1.2.1. Группы

Данный раздел предоставляет возможность объединять различные сущности (IP-адреса, MAC-адреса и Common Name) в группы для удобства работы с исключениями. Это упрощает работу с исключениями за счет уменьшения количества операций по добавлению в списки исключений.

Например, для решения задачи "Исключить из проксирования трафик сотрудников бухгалтерии", создается группа "Бухгалтерия", в которую заносятся IP-адреса или подсети рабочих станций бухгалтерии, затем в разделе Исключения — Исключения вы можете указать только одну запись для всей группы "Бухгалтерия".

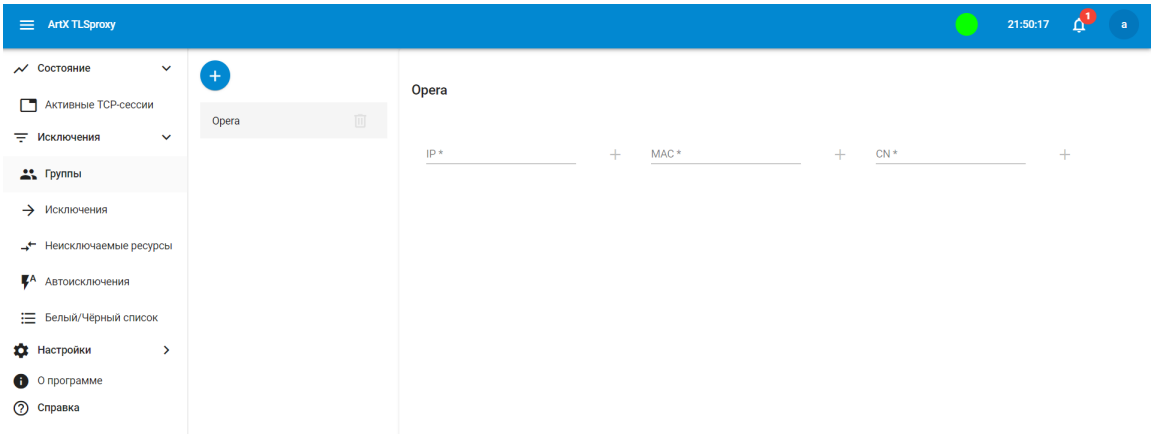


Рисунок 19. Раздел группы.

3.3.1.2.2. Исключения

Подраздел Исключения веб-интерфейса ArtX TLSproxy предназначен для работы с постоянными исключениями — правилами для исключения из проксирования по определенным критериям.

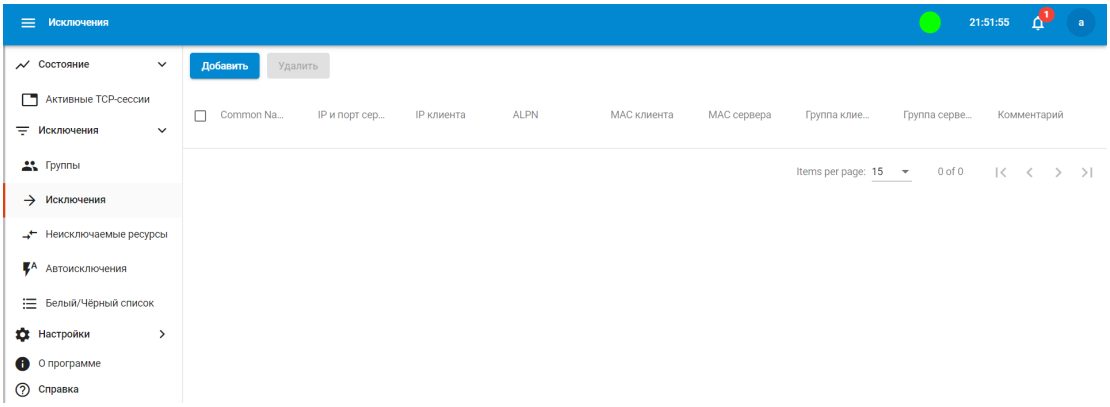


Рисунок 20. Раздел исключения

Описание столбцов таблицы исключений:

Common Name

Имя службы на стороне сервера, возвращаемое сервером в сертификате (возможно указание в виде регулярного выражения PCRE или wildcard)

IP и порт сервера

IP-адрес и порт сервера соединения

IP клиента

IP-адрес клиента соединения

ALPN

Набор параметров соединения, включающий в себя требования по версии протокола передачи данных и т.д.

MAC клиента

MAC-адрес клиента соединения

MAC сервера
MAC-адрес сервера соединения с точки зрения сервера ArtX TLSproxy
Группа клиентов
Набор IP-адресов и/или MAC-адресов клиентов соединения
Группа серверов
Набор IP-адресов, MAC-адресов и/или Common Name серверов соединения
Комментарий
Комментарий правила исключения из проксирования.

Для удаления одного или нескольких правил исключений необходимо установить напротив их строчек флаг в левом столбце таблицы и нажать на кнопку Удалить. Возможна фильтрация по полям столбцов или по общему полю поиска по таблице.

Также в левом столбце таблицы есть возможность установки флажка — при его установке будут выделены все неотфильтрованные строки на всех страницах. Например, для удаления правил домена whatsapp.net из постоянных исключений выполните следующие действия:
1. Указать в фильтре столбца Common Name whatsapp.net
2. Выделить все показанные строки, выставив флаг в заголовке левого столбца
3. Нажать на кнопку Удалить.

Для добавления нового правила исключения из проксирования необходимо нажать на кнопку Добавить. Откроется окно добавления нового правила:

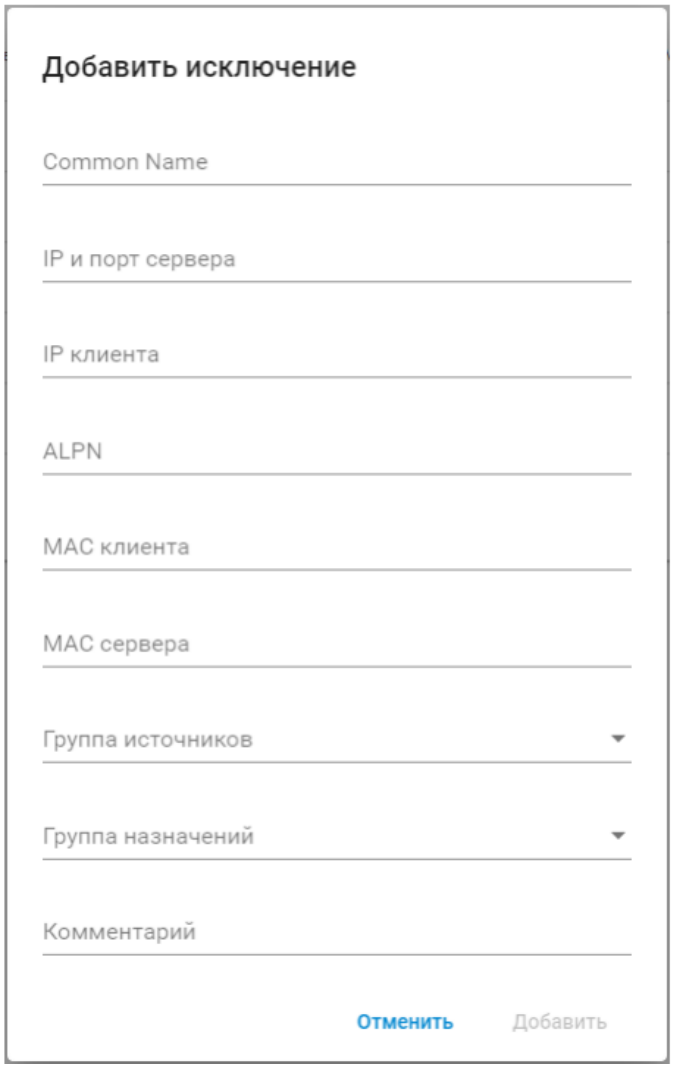


Рисунок 21. Таблица добавления исключения

ВНИМАНИЕ: Поле Комментарий является обязательным при добавлении нового правила исключения из проксирования.

ВНИМАНИЕ: Следует учитывать, что только в случае добавления исключения по IP-адресу для такого правила будет работать bypass на уровне ядра ОС, то есть все сессии данного IP-адреса не будут терминироваться сервером ArtX TLSproxy. Во всех остальных случаях для всех указанных в данном разделе правил TCP-соединения будут терминироваться (разрываться на 2 части, клиент-ArtX TLSproxy и ArtX TLSproxy-сервер), но не будут модифицироваться.

Фактически, данный раздел позволяет работать с базой данных noproxy утилиты dbctl. См. раздел Постоянные исключения.

3.3.1.2.3. Неисключаемые ресурсы

Подраздел Неисключаемые ресурсы веб-интерфейса ArtX TLSproxy предназначен для работы со списком неисключаемых ресурсов.

Список неисключаемых ресурсов — перечень Common Name, доступ к которым обязательно должен проксировать сервер ArtX TLSproxy.

Ниже представлена страница с разделом неисключаемых ресурсов в веб-интерфейсе ArtX TLSproxy.

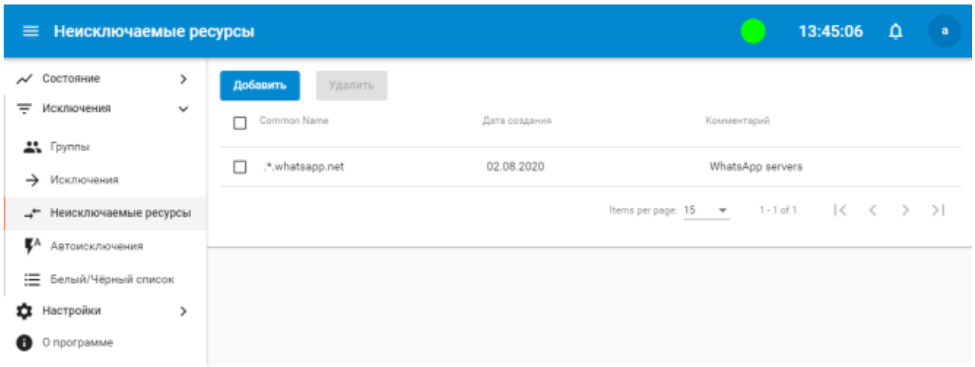


Рисунок 22. Раздел неисключаемые ресурсы.

Фактически, данный раздел является веб-интерфейсом для работы с базой данных teb утилиты dbctl. См. раздел Список неисключаемых ресурсов (принудительное проксирование).

3.3.1.2.4. Автоисключения

Подраздел Автоисключения веб-интерфейса ArtX TLSproxy предназначен для работы со списком автоисключений.

Функциональность автоисключений позволяет ArtX TLSproxy идентифицировать и учитывать в работе различные ошибки на стороне клиента соединения, приводящие к отказу установки соединения с сервером с участием ArtX TLSproxy.

Основной причиной таких ошибок является Certificate Pinning — проверка приложением на клиентском устройстве, инициировавшем соединение, сертификата, подменяемого сервером ArtX TLSproxy**.**

Механизм автоисключений позволяет ArtX TLSproxy после определенного количества неудачных попыток соединения со стороны клиента автоматически добавлять правило исключения для аналогичных соединений от данного клиента к данному серверу. Учитывая особенность современных приложений производить постоянные переподключения, данная функциональность исключает следующие проблемы на этапе внедрения:

★ Сертификат, возвращаемый сервером ArtX TLSproxy, не является доверенным на клиентской машине (например, в случае с самоподписанным сертификатом сервера ArtX TLSproxy, сертификат не добавлен в Доверенные корневые центры сертификации).

★ Приложение выполняет проверку возвращаемого сервером ArtX TLSproxy сертификата, отвергая его (Certificate Pinning).

★ Другие возможные причины, в том числе сетевые проблемы.

Ниже представлена страница с разделом автоисключений в веб-интерфейсе ArtX TLSproxy.

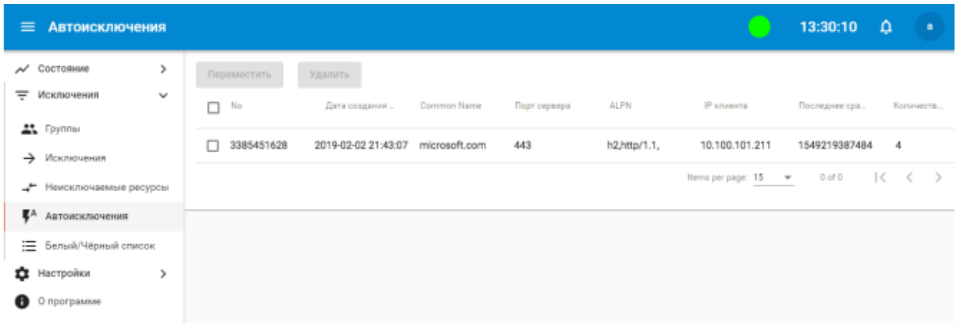


Рисунок 23. Раздел Автоисключения

Выделив одно или несколько правил автоисключений можно выполнить одно из следующих действий над ними:

- Удалить, нажав кнопку Удалить.
- Перенести в раздел Исключения или Неисключаемые ресурсы, нажав кнопку Переместить.

Ниже представлена страница с окном переноса автоисключения:

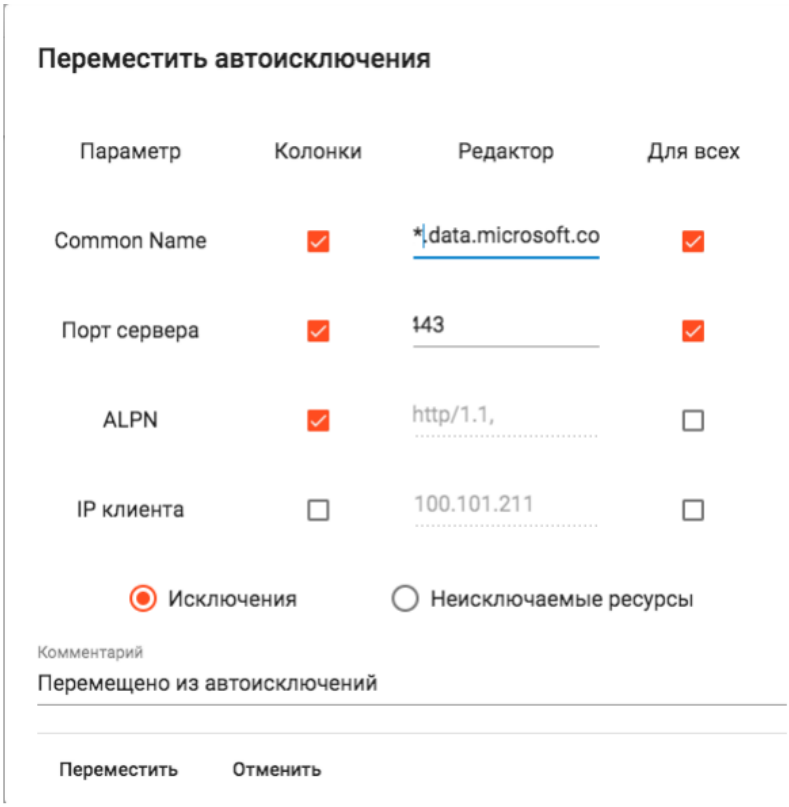


Рисунок 24. Окно переноса автоисключения.

Установите флаг Колонки напротив соответствующей колонки, чтобы значение данной колонки было учтено при создании нового правила исключений или неисключаемых ресурсов.

Установите флаг Для всех напротив соответствующей колонки, чтобы появилась возможность отредактировать значение для создания нового правила исключений или неисключаемых ресурсов.

В данном примере был установлен флаг Для всех для колонки Common Name и отредактировано значение Common Name для создаваемого правила ".*icq\.com". Если создать такое правило в разделе Неисключаемые ресурсы, то приложению ArtX TLSproxy будет запрещено создавать автоисключения для запросов ко всем доменам, заканчивающимся на icq.com.

ВНИМАНИЕ: ArtX TLSproxy допускает использование как точного указания Common Name, так и использование регулярных выражений (диалект PCRE). За работу функциональности автоисключений отвечает параметр Автоисключения.

Фактически, данный раздел является веб-интерфейсом для работы с базой данных tmpexcl утилиты dbctl. См. раздел Автоисключения.

3.3.1.2.5. Белый/Чёрный список

Подраздел Белый/Чёрный список предназначен для работы в прикладном веб-интерфейсе ArtX TLSproxy с Белым или Черным списками проксируемых или непроксируемых ресурсов соответственно.

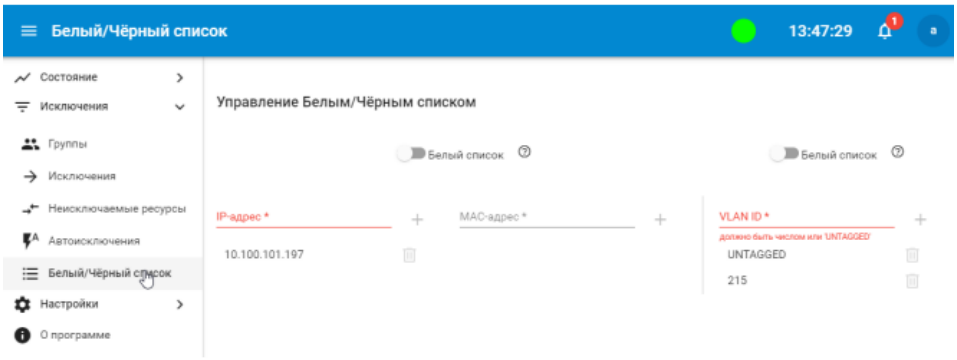


Рисунок 25. Черный/Белый список

Белый список

Список ресурсов, который ArtX TLSproxy не должен проксировать, все остальные адреса должны проксироваться

Чёрный список

Тот же самый список, но с обратной логикой (только все указанные в нём должны проксироваться).

Для управления списками VLAN имеется отдельный переключатель с аналогичной логикой поведения.

3.3.1.3. Раздел "Настройки"

Раздел Настройки предназначен для системных администраторов, отвечающих за сетевую техническую поддержку серверов ArtX TLSproxy и содержит следующие подразделы:

★ Управление
★ Режим работы
★ Интерфейсы
★ Логирование
★ Сертификаты
★ Другое

В случае изменения любых настроек появляется уведомление в области уведомлений. При подтверждении изменений необходимо выполнить перезапуск процессов приложения ArtX TLSproxy в подразделе Управление.

3.3.1.3.1. Управление

Подраздел Управление предназначен для управления состоянием сервера ArtX TLSproxy

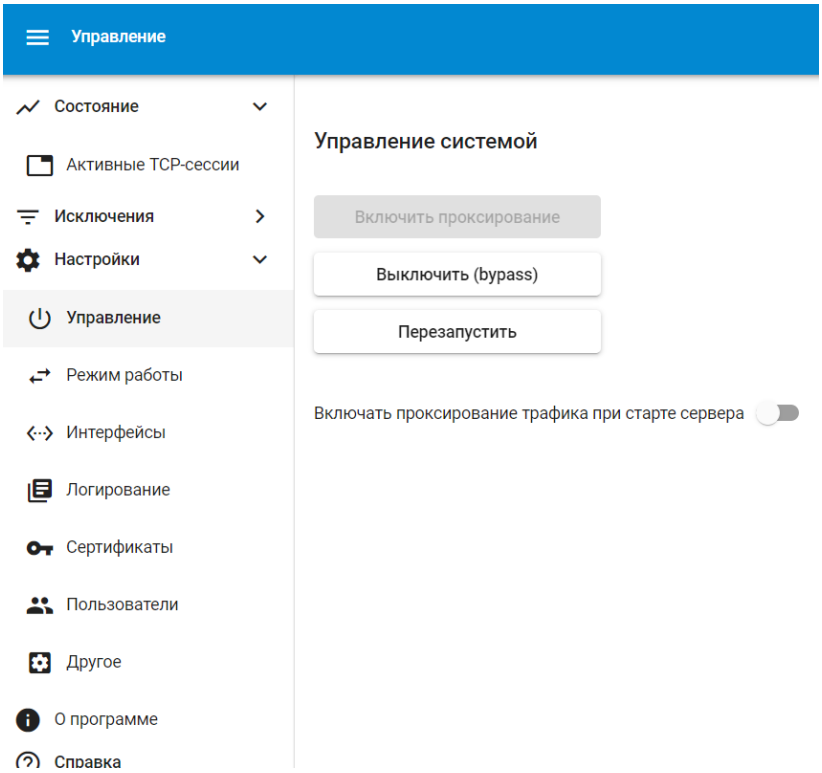


Рисунок 26. Управление состоянием сервера ArtX TLSproxy

Кнопка Включить проксирование активна тогда, когда сервер ArtX TLSproxy вообще не выполняет проксирование. В таком случае индикатор состояния на верхней панели жёлтый, что означает состояние bypass, то есть отсутствие работающих процессов приложения ArtX TLSproxy. Трафик при этом проходит прозрачно на уровне ядра ОС без терминирования сессий, любых возможных модификаций, а также какого бы то ни было влияния на него со стороны ArtX TLSproxy. В этом состоянии в разделе Активные сессии не отображается ни одно соединение.

При нажатии на активную кнопку Включить проксирование происходит запуск процессов приложения ArtX TLSproxy и начинается проксирование согласно установленной логике белых/черных списков и других исключений. После запуска проксирования индикатор состояния на верхней панели зелёный, кнопка Включить проксирование становится неактивной, и в разделе Активные сессии начинают отображаться проксируемые соединения.

Кнопка Выключить (bypass) имеет действие, обратное кнопке Включить проксирование: при включенном режиме проксирования она активна, и при нажатии на нее завершается работа всех текущих процессов приложения ArtX TLSproxy. Приложение ArtX TLSproxy переходит в режим bypass. В случае нажатия на данную кнопку в режиме L2 (Bridge) появится окно с уведомлением о "Плавном выключении": в случае риска нарушения критичных бизнеспроцессов имеется возможность "плавного выключения" с указанием таймаута для самостоятельного завершения всех текущих проксируемых TCP-сессий.

Кнопка Перезапустить выполняет перезапуск всех текущих процессов приложения ArtX TLSproxy и веб-сервера и переводит систему в рабочее состояние проксирования согласно установленной логике белых/черных списков и других исключений. Аналогично кнопке Выключить (bypass), в случае использования режима L2 (Bridge) нажатие на кнопку Перезапустить вызовет открытие окна с настройками "Плавного выключения".

В случае изменения настроек в веб-интерфейсе ArtX TLSproxy появится требование подтверждения изменений с кнопкой Перезапустить для их применения.

ВНИМАНИЕ: Нажатие на кнопки Включить проксирование, Выключить (bypass) и Перезапустить, как и ручное управление процессами приложения, приводит к разрыву всех текущих открытых сетевых соединений, обрабатываемых ArtX TLSproxy, которые отображаются в разделе Активные сессии.

Флаг Запускать ArtX TLSproxy при старте сервера позволяет запомнить текущее состояние. Если этот флаг установлен, приложение ArtX TLSproxy при перезагрузке будет запущено в режиме проксирования, иначе будет запущен только веб-интерфейс и все соединения будут проходить в режиме bypass на уровне ядра ОС, без терминирования.

3.3.1.3.2. Режим работы

Подраздел Режим работы предназначен для управления основными опциями функционирования ArtX TLSproxy, которые определяются целью его применения и Схемой включения.

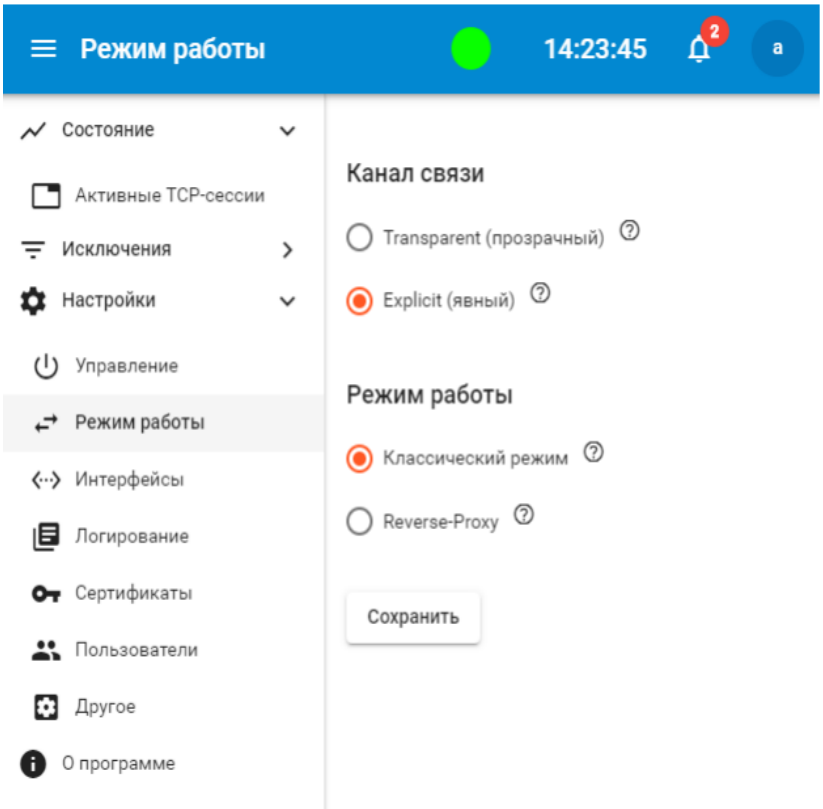


Рисунок 27. Подраздел режим работы

Параметр Канал связи позволяет указать режим работы ArtX TLSproxy:

- В режиме L2 (Bridge) (Transparent, прозрачный режим) сервер ArtX TLSproxy выполняет роль "медного провода" или простого коммутатора. Он в этом случае не имеет рабочего IP-адреса и невидим в сети.
- В режиме L3 (Router) (Explicit, явный режим) ArtX TLSproxy имеет IP-адреса на сетевых интерфейсах Internal и External из разных подсетей. В таком режиме IP-адрес Internal интерфейса указывается в качестве шлюза по умолчанию для проксируемых устройств, а с IP-адреса External-интерфейса имеется доступ в сеть Интернет.

Параметр Режим работы указывает на то, какую именно задачу в настоящий момент решает сервер ArtX TLSproxy:

- В классическом режиме ArtX TLSproxy проксирует соединения пользователей при доступе в Интернет, используя подменный сертификат (классический MiTM). При этом, если в разделе Сертификаты указаны регулярные выражения и пары закрытый ключ/сертификат, то для них ArtX TLSproxy выполняет проксирование соответствующих соединений с указанными ключом/сертификатом.
- В режиме Reverse-Proxy ArtX TLSproxy выполняет проксирование только в случае совпадения запрашиваемого клиентом ресурса указанным регулярным выражениям, как классический Reverse-Proxy. Имейте в виду, что External-интерфейс должен смотреть в сторону защищаемых веб-ресурсов (назначений соединения).

Подробнее о режимах работы см. раздел Типовые схемы включения.

3.3.1.3.3. Интерфейсы

Подраздел Интерфейсы предназначен для назначения ролей логическим сетевым интерфейсам сервера ArtX TLSproxy.

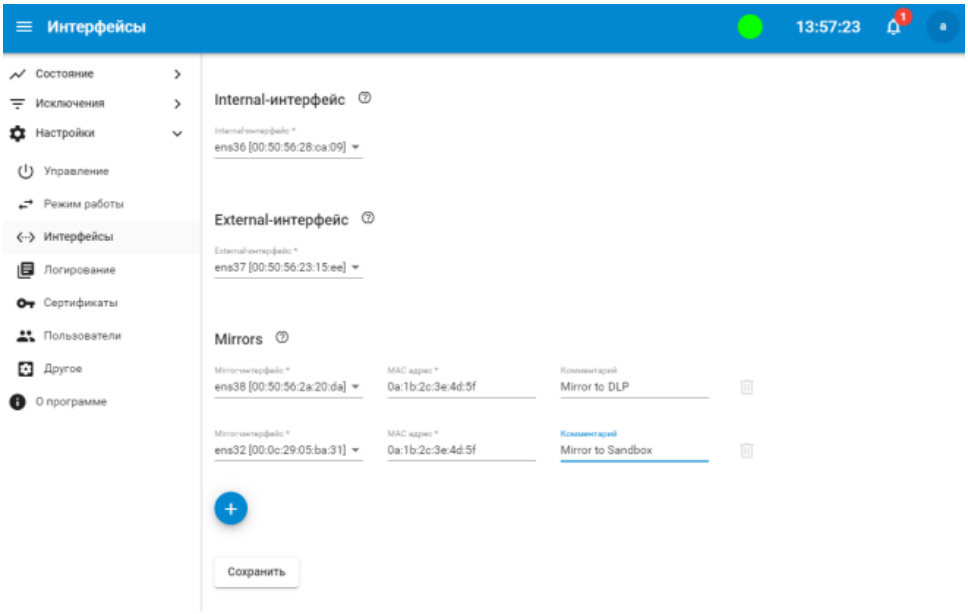


Рисунок 28. Подраздел интерфейсы

В параметрах Internal-интерфейс и External-интерфейс назначаются роли для Internal и External интерфейсов соответственно.

В случае использования режима L3 (Router) в данном разделе также будут доступны настройки IP-адресов сетевых интерфейсов Internal и External.

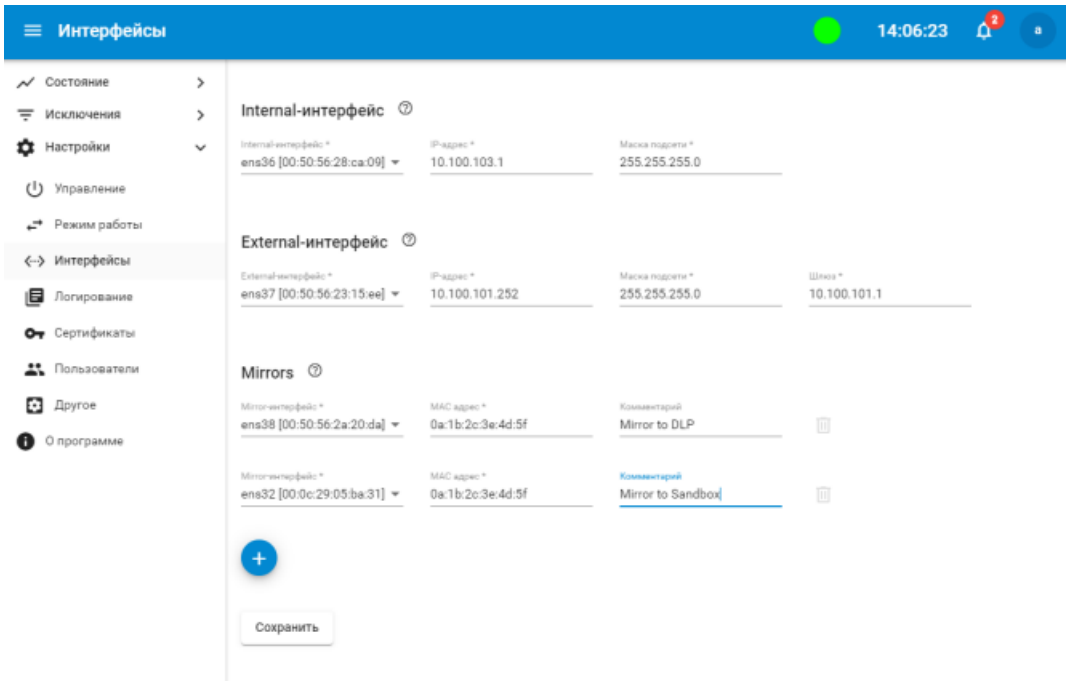


Рисунок 29. Подраздел интерфейсы. Режим L3 (Router)

Для интерфейса External необходимо указать настройки доступа в Интернет, включая шлюз по умолчанию, через который будет осуществляться доступ проксируемых устройств в Интернет. Для интерфейса Internal требуется указать IP-адрес и маску подсети. Данный адрес обычно указывается в роли шлюза по умолчанию для проксируемых устройств.

ВНИМАНИЕ: В архитектуре сервера ArtX TLSproxy заложена необходимость разнесения Internal и External сетей в разные непересекающиеся подсети для режима L3 (Router). Также стоит учитывать, что по умолчанию в режиме L3 (Router) ArtX TLSproxy не выполняет сетевую трансляцию адресов (NAT). Включение NAT производится в разделе Другое (параметр Сохранять IP-адреса клиентов (только L3)). Также стоит учитывать, что данная настройка включает трансляцию сетевых адресов только для проксируемых TCPсоединений.

В параметре Mirrors указываются один или более сетевых интерфейсов, в которые сервер ArtX TLSproxy будет отправлять копию развернутого трафика в зависимости от значения параметра Зеркалирование трафика в разделе Другое.

ВНИМАНИЕ:
В случае, если указываемые сетевые интерфейсы Mirror и системы-потребители развернутого трафика скоммутированы напрямую или через network TAP (либо коммутатор с включенным режимом promisc), MAC-адрес системы-потребителя можно указать любой, например, 0a:1b:2c:3d:4e:5f.
В ином случае необходимо указать MAC-адрес прослушивающего сетевого интерфейса системы-потребителя.

В случае двух и более систем-потребителей рекомендуется добавить исчерпывающий комментарий, идентифицирующий систему, которая получает копию трафика через данный сетевой интерфейс.

Для добавления ещё одного Mirror-интерфейса необходимо нажать на кнопку +.

ВНИМАНИЕ: При изменении настроек сетевых интерфейсов обратите внимание на имена управляемых интерфейсов, чтобы по ошибке не использовать Management-интерфейс — в таком случае может прекратиться доступ к прикладному веб-интерфейсу. Также при работе к Linux-консоли стоит учитывать, что сетевые интерфейсы, участвующие в обработке трафика, расположены в net namespace proxy.

3.3.1.3.4. Логирование

Подраздел Логирование предназначен для настройки режимов логирования ArtX TLSproxy.

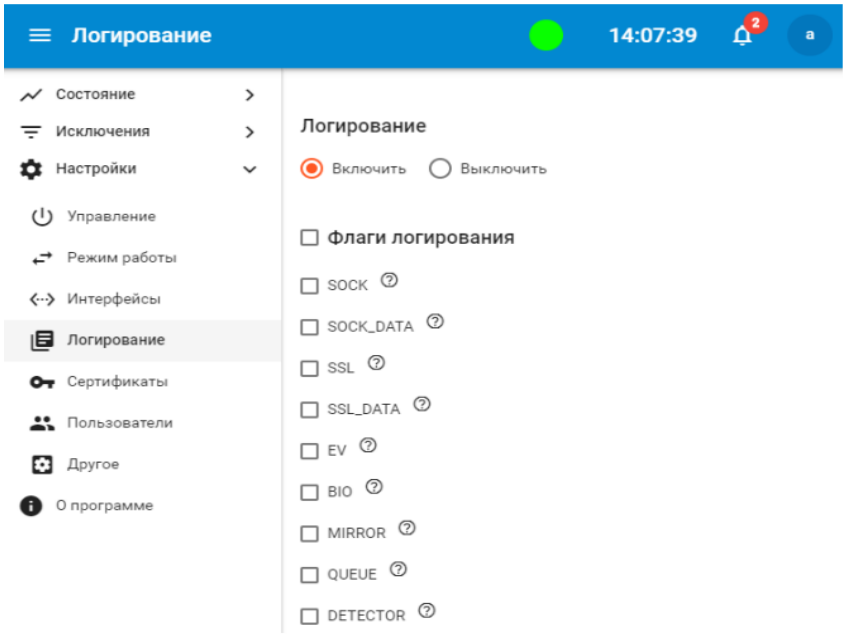


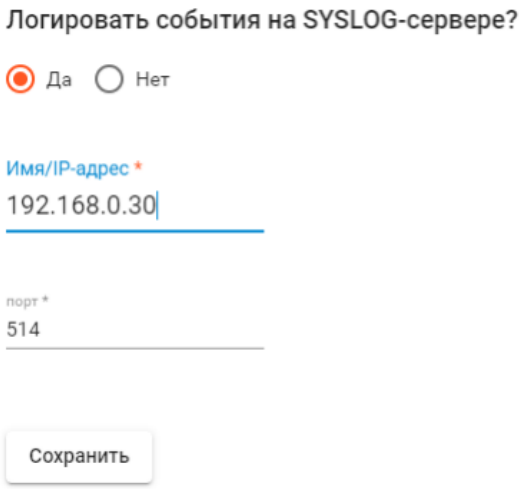
Рисунок 30. Подраздел логирование

Логирование

Позволяет включить или отключить запись лога на файловую систему в каталог /var/tlsproxy/ . При включенном логировании предполагается установка флагов логирования, определяющих категории логируемых событий по умолчанию.

Логировать события на SYSLOG-сервере?

При включении данного параметра становится доступным указание хоста и порта, на который будут отправляться события, подлежащие логированию по протоколу Syslog.



ВНИМАНИЕ:

Логирование при существенных объемах обрабатываемого ArtX TLSproxy сетевого трафика может создавать большую нагрузку на файловую систему сервера. Это может приводить к деградации производительности.

При рабочей эксплуатации рекомендуется использовать выборочное логирование, описанное в разделе Логирование.

3.3.1.3.5. Сертификаты

Подраздел Сертификаты предназначен для управления SSL/TLS сертификатами, используемыми сервером ArtX TLSproxy.

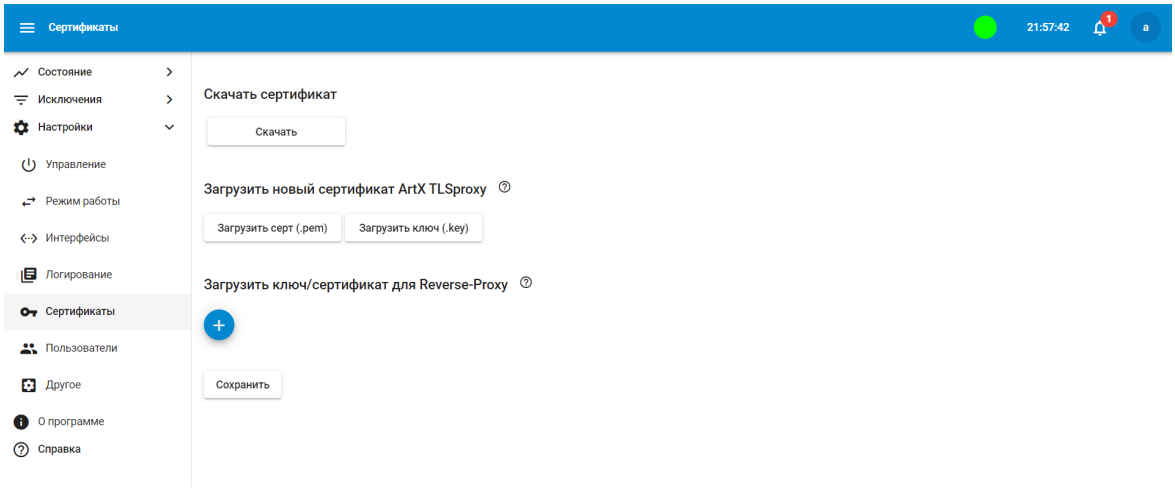


Рисунок 31. Подраздел сертификаты

Скачать сертификат

Позволяет скачать используемый сервером ArtX TLSproxy сертификат для генерации сертификатов, запрашиваемых веб-ресурсов "на лету". Этот сертификат (или сертификат, изпод которого его выпустили, в случае его создания УЦ организации) должен быть установлен на всех проксируемых устройствах в доверенных корневых центрах сертификации. Подробно процедура добавления сертификата на проксируемые устройства описана в разделе Распространение сертификата.

Загрузить новый сертификат ArtX TLSproxy

Позволяет загрузить новую пару закрытый ключ/сертификат, которая будет использоваться для генерации сертификатов запрашиваемых веб-ресурсов "на лету". Это может быть, например, сертификат, сгенерированный в УЦ организации из-под доменного корневого сертификата с ролью Subordinate CA.

Загрузить ключ/сертификат для Reverse-Proxy

Позволяет добавлять правила для работы в режиме Reverse-Proxy. Например, в случае, если необходимо осуществлять SSL- соединения к ресурсам *.ai.ru, укажите регулярное выражение \.ai\.ru$ (PCRE) и добавить пары ключ/сертификат с веб-сервера, на котором работает ресурс https://ai.ru.

В случае, если выбран классический режим работы, то помимо общей логики проксирования при доступе проксируемых устройств на веб-сайт https://www.ai.ru данное соединение между клиентом и сервером будет свертываться в SSL при помощи указанной пары ключ/сертификат. Если же сервер ArtX TLSproxy работает в режиме Reverse-Proxy, то только соединения с ресурсами, попадающими под указанное регулярное выражение, будут проксироваться с использованием данной пары ключ/сертификат. Все остальные соединения будут проходить bypass согласно указанной логике исключений. Для добавления таких правил нажмите кнопку +.

3.3.1.3.6. Пользователи

В разделе Пользователи представлена информация о пользователях веб-интерфейса приложения ArtX TLSproxy.

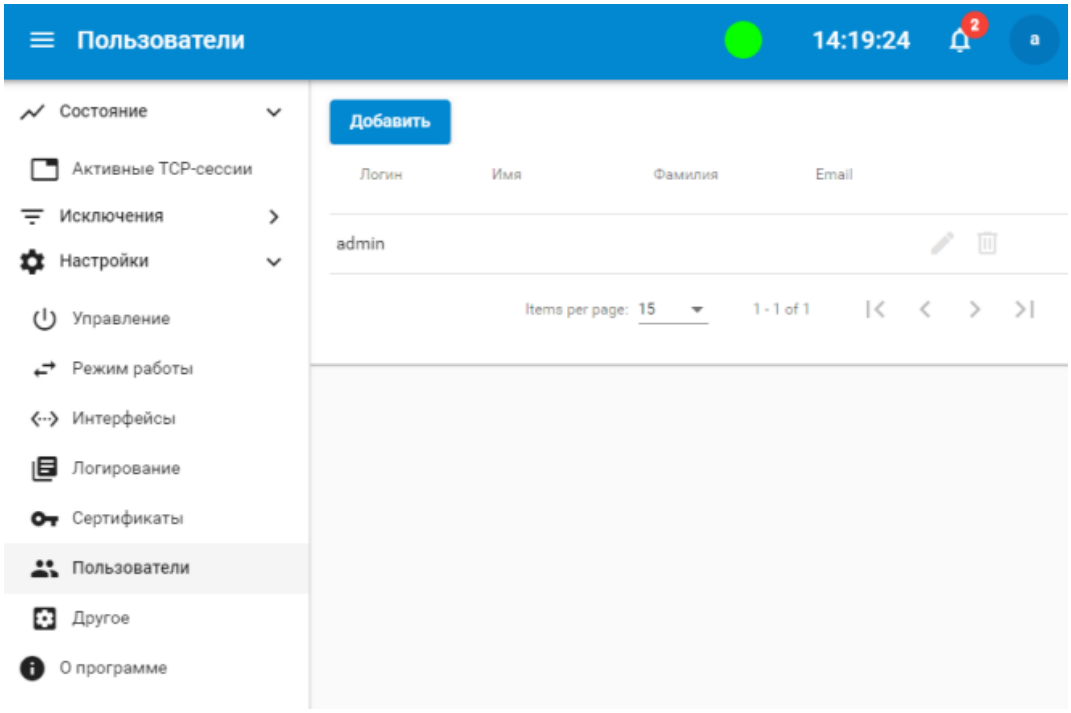


Рисунок 32. Раздел Пользователи

В ArtX TLSproxy реализована ролевая модель доступа к веб-интерфейсу со следующими ролями:

Администратор

Администратор имеет полный доступ ко всем настройкам.

Оператор

Оператор имеет полный доступ к разделам Состояние и Исключения. Таким образом, Оператор может управлять правилами проксирования и исключениями, а также просматривать список текущих сессий. Также Оператор имеет доступ к просмотру настроек ArtX TLSproxyArtX TLSproxy.

Аудитор

Аудитор имеет доступ только к просмотру разделов Состояние и Исключения. Таким образом, Аудитор может просматривать правила проксирования и исключений, а также список текущих сессий. Также Аудитор имеет доступ к просмотру настроек ArtX TLSproxy.

Для создания нового пользователя используйте кнопку Добавить вверху раздела Пользователи, при нажатии на которую откроется окно с соответствующими полями.

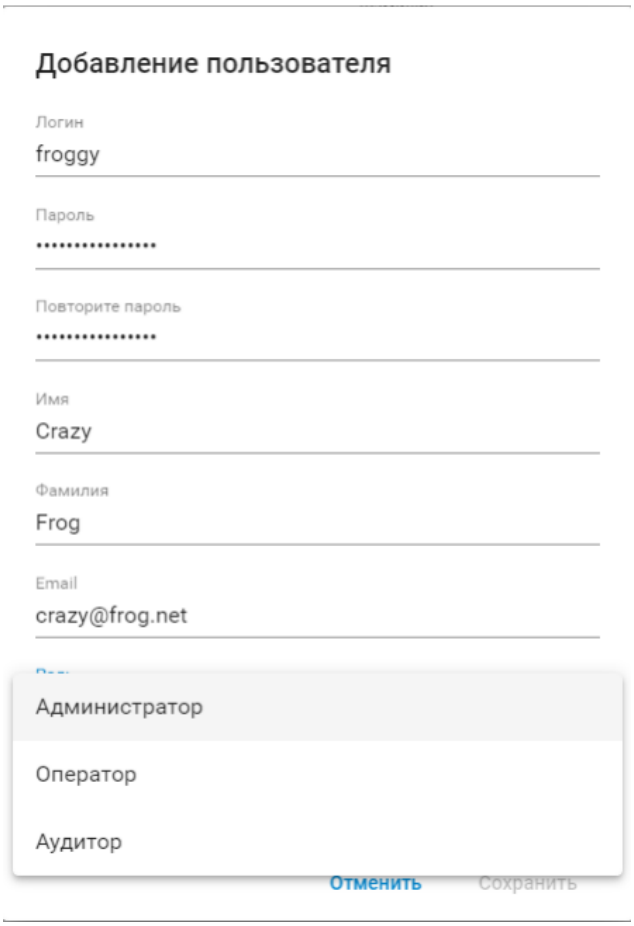


Рисунок 33. Добавление пользователя

Для редактирования или удаления пользователей в правой части таблицы напротив строки пользователя расположены кнопки редактирования (иконка "карандаш") и удаления (иконка "корзина").

По умолчанию после установки и настройки в веб-конфигураторе в ArtX TLSproxy существует только пользователь admin с ролью Администратор.

3.3.1.3.7. Другое

Подраздел Другое предназначен для изменения других настроек работы ArtX TLSproxy, а именно:

Количество процессов ArtX TLSproxy

Количество одновременно работающих процессов приложения ArtX TLSproxy, обрабатывающих сетевой трафик. Трафик между процессами балансируется равномерно автоматически.

Рекомендуется указывать количество процессов, не превышающее количество физических ядер процессоров сервера.

Зеркалирование трафика

Установить, какой трафик отправлять в Mirror-интерфейсы: только обработанный или еще и изначально необработанный.

Автоисключения

Данный параметр управляет логикой работы автоисключений. В случае, если включено, должны быть указаны следующие параметры:

★ Количество попыток неудачных соединений за период времени: в случае их превышения за указанный период создается автоисключения и все последующие соединения от данного клиента к запрашиваемому веб-ресурсу устанавливаются без проксирования (bypass). Допустимые значения от 1 до 100. Чем ближе данное значение к 1, тем более "мягкий" режим используется: при каждой ошибке добавляется правило автоисключения.

★ Период времени, в течение которого подсчитываются неудачные соединения для создания автоисключений, указывается в секундах. Допустимые значения от 1 до 900. Чем меньше это значение, тем более "мягкий" режим используется.

Сохранять IP-адреса клиентов (только L3)?

Данный параметр применим только для режима L3 (Router). Если включен, то трафик, отправляемый системе-потребителю, будет содержать оригинальные IP-адреса клиентов запросов.

Ограничить потребление CPU (%)

Данный параметр позволяет задать ограничение по утилизации процессорного времени для каждого процесса приложения ArtX TLSproxy, указывается в процентах от 0 до 100, 0 — без ограничений.

Объем кеша сертификатов (КБ)

Данный параметр позволяет ограничить максимальный объем базы кешированных пар ключ/сертификат, генерируемых сервером ArtX TLSproxy "на лету" для проксируемых соединений. Указывается в килобайтах, рекомендуемый объем — 16384КБ.

Включить SNMP/MACLookup?

Данный параметр позволяет вести в автоматизированном режиме таблицу пар MAC-адрес — IP-адрес для использования в белых и чёрных списках (раздел Белый/Чёрный список). В случае, если сервер ArtX TLSproxy установлен в такую точку сети, где не видно клиентских MAC-адресов, а работа DHCP не позволяет указывать исключения по IP-адресам, этот механизм позволяет периодически опрашивать по протоколу SNMP сетевое оборудование для актуализации данной таблицы.

Проверять статус клиента для автоисключений?

Данный параметр устанавливает проверку приложением ArtX TLSproxy статуса клиента (помимо общих свойств). Если включено, повышает точность создания автоисключений.

Проверять на Certificate Pinning для автоисключений?

Данный параметр устанавливает проверку приложением ArtX TLSproxy помимо общих свойств и статуса клиента, специальные коды ошибок клиента в случае разрыва соединения. При включенном состоянии существенно повышает точность создания автоисключений.

Включить ArtX TLSproxy**?**

Данный параметр устанавливает использование механизма кеширования генерируемых "на лету" пар ключ/сертификат для проксируемых соединений. Во включенном состоянии существенно повышает производительность сервера ArtX TLSproxy. Кэш этих данных хранится в базе данных, объем которой указывается в параметре Объем кеша сертификатов (КБ) (certDbSize).

Включить TLS Ticketing?

Данный параметр отвечает за поддержку механизма TLS-Ticketing, необходимого в работе некоторых приложений и протоколов поверх SSL, например, в работе FTPS.

Отправлять статистику в InfluxDB?

Данный параметр позволяет отправлять статистику работы приложения ArtX TLSproxy в базу данных InfluxDB для последующего анализа и построения аналитических отчетов по работе приложения.

3.3.1.4. Раздел "О программе"

В разделе О программе представлена информация об установленном файле лицензии и версии приложения.

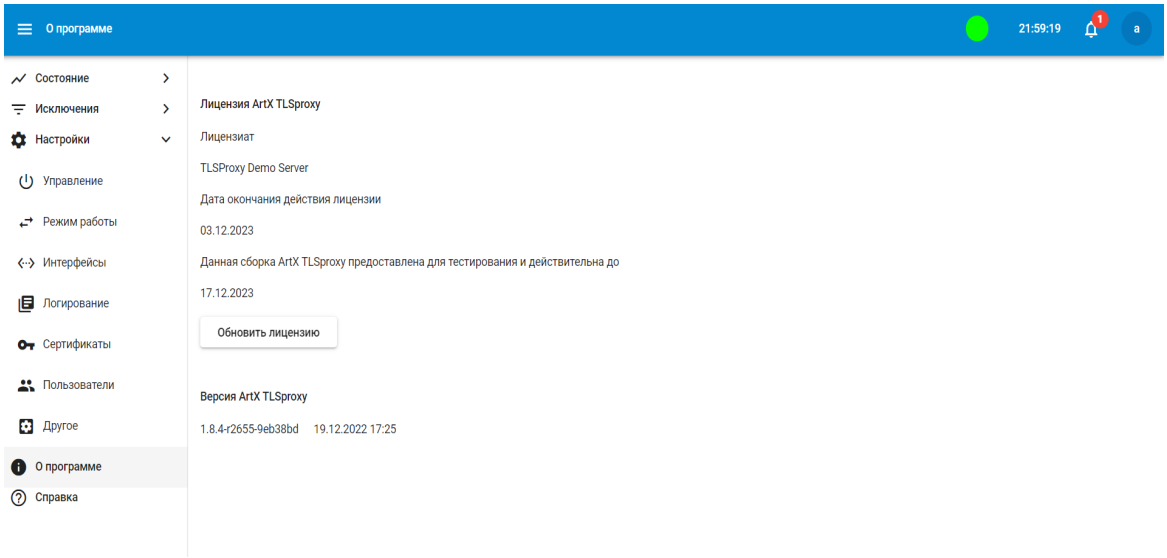


Рисунок 34. Раздел "О программе"

3.3.2. Консоль

Консольный интерфейс предназначен для управления ArtX TLSproxy через Linux-консоль сервера.
Работа в данном режиме рекомендуется только в том случае, если для решения задач управления приложением не хватает возможностей веб-интерфейса.

3.3.2.1. Управление приложением

Для управления сервером ArtX TLSproxy необходимо обладать привилегиями root. Также все команды по управлению ArtX TLSproxy необходимо выполнять в контексте сетевого окружения по умолчанию. См. раздел Диагностика.
Для запуска ArtX TLSproxy выполните команду:

```
systemctl start tlsproxy.service
```

Для остановки ArtX TLSproxy выполните команду:

```
systemctl stop tlsproxy.service
```

После остановки ArtX TLSproxy весь сетевой трафик, направленный через ArtX TLSproxy, будет пропускаться без изменений, не терминируя сетевые соединения (bypass).
Для перезапуска ArtX TLSproxy выполните команду:

```
systemctl restart tlsproxy.service
```

Для включения автозапуска ArtX TLSproxy при старте сервера выполните команду:

```
systemctl enable tlsproxy.service
```

Для отключения автозапуска ArtX TLSproxy при старте сервера выполните команду:

```
systemctl disable tlsproxy.service
```

Для проверки наличия работающих процессов приложения ArtX TLSproxy выполните команду:

```
ps aux | grep [t]cpproxy
```

При нормальной работе (проксировании) в результат команды должен показывать хотя бы один процесс ArtX TLSproxy.

ВНИМАНИЕ:
Управление приложением через утилиту systemctl включает в себя запуск / остановку / перезапуск прикладного веб-интерфейса ArtX TLSproxy. Для более безопасной работы с приложением рекомендуется управлять им через прикладной веб-интерфейс в разделе Управление.

3.3.2.2. Работа с исключениями

В ArtX TLSproxy реализован гибкий механизм исключений, упрощающий развёртывание и использование его в сети организации.

Исключение в системе понятий ArtX TLSproxy означает пропуск без изменения определенных сетевых соединений по различным критериям, таким как:

- MAC-адрес источника или назначения соединения
- IP-адрес и порт источника или назначения соединения
- Подсеть источника или назначения соединения
- Fingerprint сертификата сервера
- CN (Common Name) соединения с сервером
- URL запроса.

Работа с исключениями ведется при помощи следующих средств:

Регулярные выражения в config.json

Параметр noproxyRE в конфигурационном файле config.json позволяет задать список регулярных выражений для URL-адресов, которые необходимо исключить из проксирования ArtX TLSproxy.

Утилита dbctl

Встроенная в ArtX TLSproxy утилита, позволяющая работать со списками внутри окружения ArtX TLSproxy. Все правила, сформированные с помощью dbctl, действуют при включенном сервисе ArtX TLSproxy.

3.3.2.2.1. Утилита dbctl

Утилита dbctl расположена в каталоге приложения ArtX TLSproxy. Запуск без параметров выводит информацию об использовании утилиты:

```
./dbctl Usage: dbctl [--daemon] [--db noproxy|cert|cipers|debug|tmpexcl|teb|wl] [-v] [-l] -a|-d
```

Параметр --db (алиас -D) позволяет указать, для какой базы данных нужно выполнить команду:

noproxy

База данных для работы с постоянными исключениями. Используется по умолчанию, если не указан параметр -D

cert

База данных для кешируемых сертификатов сервера

ciphers

База данных для задания списка поддерживаемых сервером алгоритмов SSL обработки

debug
База данных для хранения настроек выборочного логирования
tmpexcl
База данных для хранения автоисключений
teb
База данных для хранения параметров соединений, принудительно проксируемых ArtX TLSproxy
wl
"Белый список", база данных для хранения списка исключаемых/проксируемых MAC-адресов источника и назначения соединения
ml
База данных для хранения списка соответствия IP-адресов MAC-адресам клиентов соединений, MacLookup.

Для просмотра содержимого любой базы данных используйте параметр -l. Для добавления в одну из баз данных используйте параметр -a. Для удаления используйте параметр -d.

3.3.2.2.1.1. Постоянные исключения

Постоянные исключения — это список CN (Common Name) серверов, соединения с которыми должны пропускаться сервером ArtX TLSproxy без проксирования (bypass). Данный список хранится в базе данных noproxy, используемой утилитой dbctl по умолчанию (без параметра - D). В автоисключения обычно добавляются Интернет-сервисы, использующие личную информацию пользователей, трафик которой не несет полезной информации для службы информационной безопасности, такие как Интернет-банки, бухгалтерские сервисы, корпоративные порталы и так далее.

Важно:
В постоянных исключениях используется не URL-адрес Интернет-ресурса, а CN (Common Name). Пример CN показан ниже.

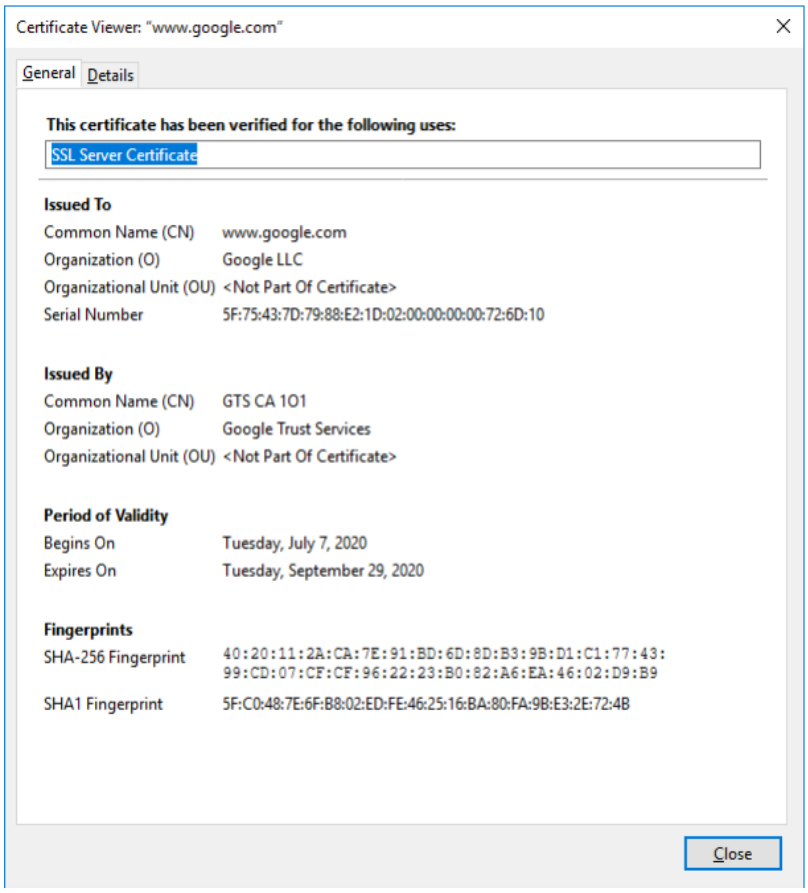


Рисунок 35. Пример CN (Common Name) Интернет-ресурса

Просмотр списка постоянных исключений:

```
./dbctl -l
CN: *.sec-p.ru
CN: 85.249.229.245:443
CN: *.adriver.ru
CN: *.kaspersky.com
CN: focus.kontur.ru
CN: counter.yadro.ru
CN: *.doubleclick.net
CN: *.wns.windows.com
CN: *.google-analytics.com
CN: sls.update.microsoft.com
CN: online.sberbank.ru
CN: online.vtb24.ru
CN: .*whatsapp\.(?:com|net)$
…
```

Добавление постоянного исключения для сервиса *.web-service.com:

```
./dbctl -a *.web-service.com
```

Удаление CN (Common Name) по маске *.web-service.com из перечня постоянных исключений:

```
./dbctl -d *.web-service.com
```

Например, чтобы исключить из проксирования сайт ai.ru, необходимо узнать CN и выполнить команду:

```
./dbctl -a ai.ru
```

ВНИМАНИЕ:
ArtX TLSproxy допускает использование как точного указания Common Name, так и регулярных выражений (диалект PCRE).

3.3.2.2.1.2. Автоисключения

Функциональность автоисключений ArtX TLSproxy разработана для автоматизации процесса работы с исключениями и упрощения интеграции в сетевую инфраструктуру.

Автоисключения включаются параметром AE:disable в конфигурационном файле config.json. Параметр AE:retry устанавливает максимальное количество обрывов соединения на стороне источника, после которых соединения с такими же параметрами необходимо пропускать без проксирования.

Критериями неудачного соединения служат обрыв соединения на стороне источника со статусом REJECT либо установка SSL/TLS-соединения без последующей передачи данных. Обычно такое поведение вызывает Certificate Pinning (сравнение сертификата сервера с сертификатом, хранящемся в приложении).

Параметр AE:timeout конфигурационного файла config.json устанавливает период времени в секундах, за которое должно произойти количество неудачных попыток установки соединения, указанное в параметре AE:retry.

Например:

В конфигурационном файле config.json установлены параметры AE:retry:1 и AE:timeout:180.

Пользователь запускает на проксируемом мобильном устройстве приложение, использующее Certificate Pinning (например, Facebook Messenger). Приложение один раз пытается соединиться с сервером (ArtX TLSproxy в этот момент выступает в роли сервера), затем приложение сравнивает эталонный сертификат с сертификатом, полученным от ArtX TLSproxy, и закрывает SSL/TLS-соединение со статусом REJECT.

В этом случае ArtX TLSproxy получает статус закрытия соединения REJECT и автоматически добавляет автоисключение со следующими критериями выполнения:

Для <IP-адрес пользователя> с ALPN <ALPN h2,http/1.1> все соединения на <порт сервера> с отпечатком сертификата сервера <server fingerprint>, CN сервера <messenger.facebook.com> пропускать без изменений.

После этого все последующие соединения данного приложения на данном устройстве, попадая под эти критерии, будут пропускаться без изменений.

Аналогичное действие происходит и в том случае, если приложение установило соединение с ArtX TLSproxy, но не передает никаких данных, сбрасывая соединения по таймауту: это - известная особенность поведения некоторых клиентских приложений. В этом случае ArtX TLSproxy добавит автоисключение после трех попыток установки соединения. При этом к другим приложениям, которые будут обращаться к этому серверу, данное правило автоисключения не будет применяться, если у них будет отличные от указанного в настройках значение ALPN.

Таким образом, механизм автоисключений ArtX TLSproxy гарантирует нормальную работу приложений даже в случае использования Certificate Pinning или отсутствия сертификата ArtX TLSproxy в списке доверенных на устройстве.

Просмотр списка автоисключений:

```
./dbctl -D tmpexcl -l hash: 0x502f54bc CN: scontent-arn2-1.xx.fbcdn.net ALPN h2,http/1.1, SRCIP: 10.10.180.159 PORT: 443 HASH: 15: 21: 51: b3: 87: 41: 2a: 95: ab: 90: fd: 46: 64: f2: d9: 88: 80: 40: 8e: 9e: 43: 91: 31: 24: e4: c9: 12: 26: a4: 83: 38: 6b: ! @734 1505724547503 STR 'autoexclude' SUBJ: /C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com ISSR: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA CIDS [52662,52663,52340,52321,] AT: 1506072186165 CNTR: 26
```

Параметры данной записи:
hash: 0x502f54bc
Идентификатор записи, по которому ее позже можно будет удалить
CN: scontent-arn2-1.xx.fbcdn.net
Common Name (CN) сервера
ALPN h2,http/1.1
ALPN источника
SRCIP: 10.10.180.159
IP-адрес источника
PORT: 443
Порт сервера
HASH:
15:21:51:b3:87:41:2a:95:ab:90:fd:46:64:f2:d9:88:80:40:8e:9e:43:91:31:24:e4:c9:12:26:a4:83:38:6b:
Отпечаток сертификата сервера (fingerprint)
@734
Process ID процесса ArtX TLSproxy, добавившего автоисключение (может понадобиться при анализе логов автоисключений для выяснения причин создания автоисключения)
1505724547503
Время создания автоисключения (в формате UNIX Timestamp)
SUBJ: /C=US/ST=California/L=Menlo Park/O=Facebook, Inc./CN=*.facebook.com
Параметры сертификата сервера

ISSR: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert SHA2 High Assurance Server CA
Параметры сертификата удостоверяющего центра, выпустившего сертификат сервера
CIDS [52662,52663,52340,52321,]
Идентификаторы соединений, по причине которых было создано автоисключение (может понадобиться при анализе логов автоисключений для выяснения причин создания автоисключения)

AT: 1506072186165
Время добавления автоисключения в формате UNIX Timestamp
CNTR: 26

Количество непроксируемых по причине данного автоисключения соединений.
Удаление автоисключения:

```
./dbctl -D tmpexcl -d 0x502f54bc
```

Удаление производится по hash-идентификатору автоисключения.

Внимание:
Обслуживание ArtX TLSproxy предполагает периодический анализ базы данных
автоисключений для переноса определенных событий в список постоянных исключений,
либо в список неисключаемых ресурсов.

3.3.2.2.1.3. Список неисключаемых ресурсов (принудительное проксирование)

Список неисключаемых ресурсов создан для тех случаев, когда нужно не допускать создание автоисключений при обращении к определенным веб-ресурсам.
В данный список добавляются:

★ Ресурсы, данные которых являются критичными для систем-потребителей трафика, развернутого ArtX TLSproxy

★ Ресурсы, доступ к которым необходимо блокировать в случае, если нет возможности контролировать информационный обмен с ними

★ Ресурсы, во время доступа к которым случаются сбои приложения, в результате чего создаются автоисключения (например, при сбоях внутри приложения, приводящих к его перезапуску).

В список неисключаемых ресурсов следует добавлять Common Name (CN) хостов соответствующих сервисов.
Просмотр списка неисключаемых ресурсов:

```
./dbctl -D teb -l
```

```
CN: hh.ru
CN: vk.com
CN: *.facebook.com
CN: mail.ru
CN: *.mail.ru
CN: google.ru
CN: yandex.ru
CN: rambler.ru
```

Добавление неисключаемого ресурса

```
./dbctl -D teb -a imap.google.com
```

Удаление неисключаемого ресурса

```
./dbctl -D teb -d imap.google.com
```

3.3.2.2.1.4. Черные и белые списки

Черные и белые списки предназначены для упрощения процедуры ответвления сетевого трафика на ArtX TLSproxy.

Белый список

MAC-адреса добавленных в этот список устройств проксируются, все остальные не проксируются

Черный список

MAC-адреса добавленных в этот список устройств не проксируются, все остальные проксируются.

Использование чёрных и белых списков рекомендуется в случаях, когда:

★ Необходимо проксировать только небольшой список устройств, Интернет-трафик которых нет возможности ответвить на ArtX TLSproxy**.** В таком случае на ArtX TLSproxy ответвляется Интернет-трафик всех пользователей, а список проксируемых устройств определяется белым списком

★ В ответвленном на ArtX TLSproxy Интернет-трафике имеются критичные устройства, приложения которых не имеет смысла или невозможно проксировать (корпоративный портал, открытая изолированная гостевая Wi-Fi сеть, защищенный сегмент сети и т.д.).

По умолчанию ArtX TLSproxy работает в режиме черного списка, проксируя все устройства, MAC-адреса которых не добавлены в базу данных wl утилиты dbctl.
Просмотр всего списка:

./dbctl -D wl -l
SRCNET: 10.100.102.0/255.255.255.0 VAL: 1
SRCNET: 10.100.101.0/255.255.255.0 VAL: 0
SRCNET: 10.100.100.0/255.255.255.0 VAL: 1

Добавление устройства в список:

```
./dbctl -D wl -a SRCNET:10.100.102.0/24 1
```

Здесь 1 в конце означает, что запись активна. Отключение записи без удаления:

```
./dbctl -D wl -a SRCNET:10.100.102.0/24 0
```

Здесь 0 в конце означает, что запись не активна. Удаление записи из списка:

```
./dbctl -D wl -d SRCNET:10.100.102.0/24
```

3.3.2.2.1.5. База MacLookup

В базе данных MacLookup (ml) утилиты dbctl ArtX TLSproxy хранит список соответствия IP-MAC на тот случай, если в обрабатываемом трафике не видно реальных MAC-адресов источника и назначения соединения. Это может быть необходимо для управления исключениями по MAC-адресам.

Раздел Другое позволяет настроить актуализацию macLookup с сетевым оборудованием организации по протоколу SNMP.
Также допускается добавление и удаление записей в базе данных ml в ручном режиме.
Добавление пары IP-MAC:

```
./dbctl -D ml --a 192.168.5.5 08:cc:a7:19:b4:79
```

Удаление пары IP-MAC:

```
./dbctl -D ml -a 192.168.5.5 08:cc:a7:19:b4:79
```

3.3.2.2.2. Регулярные выражения

Параметр noproxyRE в конфигурационном файле config.json позволяет задать список регулярных выражений для URL-адресов, которые необходимо исключить из проксирования ArtX TLSproxy.
Изменение данного списка требует перезапуска ArtX TLSproxy.

3.3.2.2.3. Алгоритм работы с исключениями

Логика работы ArtX TLSproxy с исключениями различных типов описана в схеме ниже.

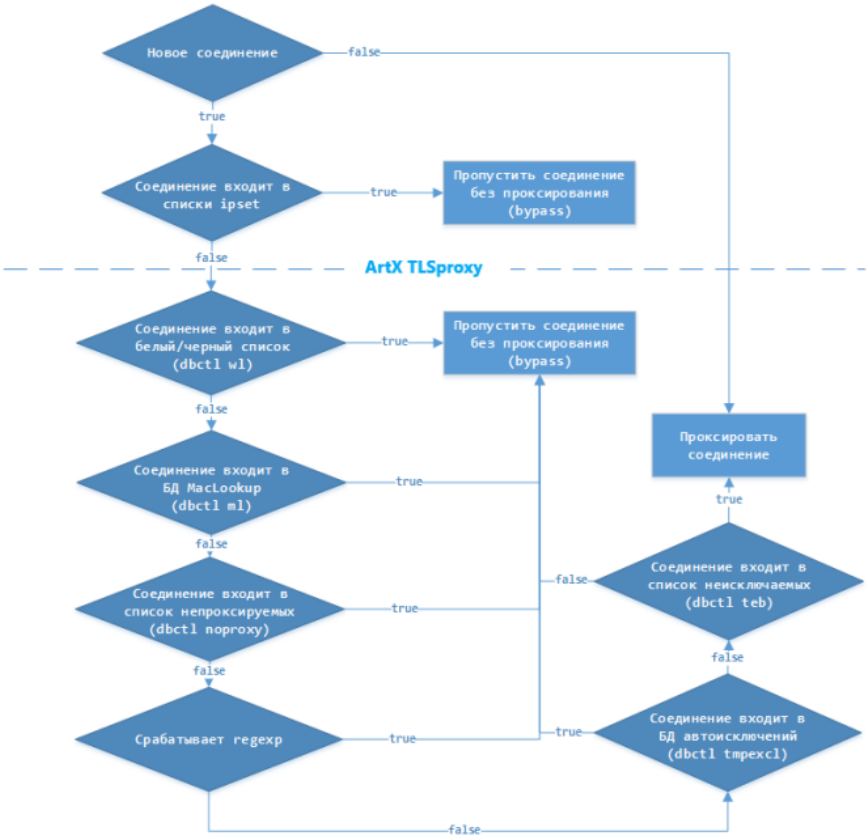


Рисунок 36. Алгоритм работы с исключениями

3.3.2.3. Конфигурационный файл config.json

Конфигурационный файл /etc/tlsproxy/config.json является главным конфигурационным файлом ArtX TLSproxy и включает в себя параметры, указанные в таблице ниже.
Таблица 3. Описание конфигурационного файла config.json

Директива	Значение по умолчанию	Описание
licenseFile	/etc/tlsproxy/config.json	Полный путь к файлу лицензии ArtX TLSproxy
extraArgsFirst	null	Дополнительные аргументы при запуске процессов ArtX TLSproxy
chrootEnv	true	Запускать приложение с использованием chroot
createEnv	true	Создавать и настраивать окружение (net namespace, сетевые интерфейсы, модули ядра, маршрутизация и другие пункты подготовки) автоматически
certDbSize	16384	Максимальный объем БД кэша отпечатков сертификатов
certdb	"/var/tlsproxy/certdb"	Путь к кэшу отпечатков сертификатов
certdir	"/etc/tlsproxy"	Каталог хранения сертификата Intermediate CA и файла закрытого ключа. С учетом mount, по умолчанию каталог /etc/tlsproxy/
bindir	"."	Путь к каталогу, в котором находятся исполняемые файлы

		ArtX TLSproxy
proxyns	"proxy"	Имя Linux Network Namespace, в котором работает сетевое окружение ArtX TLSproxy
binlog	false	Включение/отключение полного логирования всех соединений (false/true)
binlog_flush	true	Минимизировать обращения к HDD за счет сбрасывания в лог соединений агрегированных данных
iface_up	"eth1"	Имя логического интерфейса External (в сетевом контейнере ArtX TLSproxy
iface_up_addr	null	IP-адрес интерфейса External в CIDR-нотации (применимо только для режима L3 (Router), иначе игнорируется). Адрес находится в сетевом контейнере ArtX TLSproxy. Например, "192.168.1.2/24"
iface_down	"eth2"	Имя логического интерфейса Internal (в сетевом контейнере ArtX TLSproxy)
iface_down_addr	null	IP-адрес интерфейса

		Internal в CIDR-нотации (применимо только для режима L3 (Router), иначе игнорируется). Адрес находится в сетевом контейнере ArtX TLSproxy. Например, "192.168.1.1/24"
iface_span	[]	Интерфейсы Mirror (в сетевом контейнере ArtX TLSproxy). Содержит в себе набор объектов, соответствующих описаниям логических сетевых интерфейсов Mirror.
iface	eth3	Сетевой интерфейс Mirror, в который направляется копия обработанного трафика. "iface" - имя логического сетевого интерфейса; "dstmac" - MAC-адрес системы-потребителя, на который будет отправляться копия трафика с данного интерфейса; "comment" - комментарий, позволяющий пометить данный сетевой интерфейс.
dstmac	"00:0c:29:0a:b5:f6"	
comment	""	

bypassOnStart	true	Автозапуск приложения ArtX TLSproxy при загрузке ОС. true - запускается прикладной веб-интерфейс и само приложение ArtX TLSproxy в режиме проксирования. false - запускается только прикладной веб-интерфейс и режим bypass.
restartProxy	true	Перезапускать ArtX TLSproxy в случае ошибки ПО
fullLog	"/var/tlsproxy/full.log"	Путь к логу работы ArtX TLSproxy
fullLogManual	false	Включение или отключение полного логирования (/var/tlsproxy/_full.*.log). true - полное логирование в FULL-лог отключено; false - включено полное логирование в FULL-лог.
debugState	0	Уровень логирования (в лог, путь к которому указан в директиве "fullLog") (null - отключено, "DEF": логирование по умолчанию)
debugOptDefault	null	Уровень отладочного логирования. (0 - отключено, 1 -

		логирование ошибок, 2 - полное логирование binlog)
connectionLogDir	"/var/log/tlsproxy/connlog"	Каталог для хранения логов сетевых соединений в случае включенной опции binlog
l3mode	false	Управление режимами работы: false - включен режим L2 (Bridge); true - включен режим L3 (Router). При переключении режима требуется перезагрузка сервера.
keepOriginalIps	true	Сохранять оригинальный IP-адрес при передаче пакетов из интерфейса Internal в External и наоборот (true/false). По сути реализация SNAT для проксируемых TCP сессий.
certDbSize	8192	Максимальный объем кэша отпечатков сертификатов
proxyTaskCount	1	Количество процессов ArtX TLSproxy (рекомендуется устанавливать не больше количества физических ядер в сервере)

startEnv	["./start_env.sh"]	Путь к скриптам инициализации сети внутри сетевого окружения ArtX TLSproxy
noMirrorPassThru	true	Передавать в Mirror-интерфейсы: только обработанный трафик (true); Необработанный + обработанный (false)
AE		Раздел автоисключений
disable	false	Включены ли Автоисключения (true/false)
retry	3	Количество попыток установки SSL/TLS-соединения с одинаковыми параметрами, после которого добавляется автоисключение
timeout	90000	Период времени, за который проводится подсчет неудачных попыток соединения (в секундах)
debugSpool	"/var/tlsproxy/connlog/ae"	Каталог хранения логов автоисключений
Influx		Раздел подключения к внешней БД Influx для хранения и визуализации статистики
enable	true	Включено ли

		хранение статистики (true/false)
host	"localhost"	Имя/IP-адрес сервера хранения статистики
database	"tlsproxy"	Имя БД для хранения статистики
remoteSyslog	"1.2.3.4:514"	Имя/IP-адрес удаленного Syslog-сервера для приема и хранения статистики и логов (для отключения закомментировать
macLookup		Раздел синхронизации ARP-таблицы
enable	false	Включение синхронизации ARP-таблицы
snmp		Раздел настройки подключения к SNMP-серверу
oid	".1.3.6.1.2.1.3.1.1.2"	OID для получения таблицы соответствия MAC-IP
host	"1.2.3.4"	Имя/IP-адрес сервера для актуализации таблицы соответствия MAC-IP
community	"CommunityPassPhrase"	Имя Community для актуализации таблицы MAC-IP
period	300000	Частота SNMP-опроса сервера (в миллисекундах)

bypassUnkn own	true	Управление режимом "Черный"/"Белый" список (если true - используется режим "Белого" списка, false - режим "Черного" списка)
vlanList	[0]	Список VLAN ID, которые необходимо проксировать (если vlanInvert=false), или пропускать без изменений (если vlanInvert=true). VLAN ID указываются через запятую с пробелом. 0 - untagged-трафик, проксируется по умолчанию.
vlanInvert	false	Инвертирование списка vlanList. Если true - список vlanList пропускается без изменений, а все остальные VLAN ID проксируются. Если false - список vlanList проксируется, остальные VLAN ID пропускаются без изменений.
http_port	80	Порт веб-сервера прикладного веб-интерфейса
https		Настройка работы прикладного веб-интерфейса по протоколу HTTPS

enable	false	Включение работы прикладного веб-интерфейса по протоколу HTTPS
key	"/etc/tlsproxy/https-key.pem"	Полный путь к файлу закрытого ключа для HTTPS-соединения при доступе к прикладному веб-интерфейсу
cert	"/etc/tlsproxy/https-cert.pem"	Полный путь к файлу публичного ключа (сертификата) для HTTPS-соединения при доступе к прикладному веб-интерфейсу
useSessionCache	true	Использование механизма TLS Sessions - кеширование ключей TLS-сессий.
useSessionTickets	true	Использование механизма TLS Ticketing - кеширование TLS-тикетов (необходимо, например, для развертывания протокола FTPS).
checkClientState	true	Проверка статуса отброшенного клиентом соединения для механизма автоисключений. Во включенном режиме повышает требования для создания автоисключений.

forceRejectCheck	true	Проверка статуса отброшенного клиентом соединения на предмет Certificate Pinning для механизма автоисключений. Во включенном режиме повышает требования для создания автоисключений.
useFWWhitelist	false	Использование WhiteList - возможность указать выборочный список IP-адресов для проксирования. Необходимо учитывать, что данная логика начинает срабатывать после проверки на проксируемый или непроксируемый VLAN (если указанные адреса будут в непроксируемом VLAN согласно настройке параметра vlanList , то изменений в работе не будет). Проверить состояние списка можно утилитой ipset внутри контейнера proxy - список whitelist.
invertFWWhitelist		Инвертирование логики списка WhiteList. Если true,

		указанные адреса не проксируются, а остальные проксируются. Если же указан false, указанные адреса проксируются, а все остальные пропускаются без проксирования.
useFWBypass	false	Использование модуля Bypass на уровне ядра. Для IP-адресов из этого списка не выполняется терминирование TCP-сессий на сервере ArtX TLSproxy. Их пакеты маршрутизируются ядром ОС как обычным коммутатором.
enableFW	true	Использование модуля fw (FireWall), отвечающего за исключения на уровне ядра Linux. Отвечает за синхронизацию списков whitelist и bypassfw между утилитой ipset и ArtX TLSproxy.
domainCerts	[]	Раздел для функциональности Reverse-Proxy. Содержит правила следующего вида: {

		"re": ".*\\.ai\\.ru$", "cert": "ai.ru.crt", "key": "ai.ru.key" }, в которых: re - регулярное выражение для Common Name (SNI).
domainCertBypass	false	Указание для ArtX TLSproxy работать только в режиме Reverse-Proxy. Если включено, выполняется проксирование только сервисов, попадающих под один из regex из списка domainCerts. Все остальные соединения проходят bypass. Если выключено, то ArtX TLSproxy работает в классическом режиме, но в случае попадания SNI по regex из списка domainCerts, производится шифрование указанными для них ключами.

3.3.2.4. Диагностика

Запуск shell в контексте сетевого окружения ArtX TLSproxy:

```
ip netns exec proxy bash
```

Проверка наличия активных процессов ArtX TLSproxy:

```
ps -aux | grep "[t]cpproxy
```

Анализ нагрузки на сетевые интерфейсы:

```
sudo ip netns exec proxy ifstat -b
```

Анализ нагрузки процессов ArtX TLSproxy:

```
top -p `pgrep tlsproxy | tr "\\n" "," | sed 's/,$//'`
```

Или, если установлена утилита htop:

```
htop -p `pgrep tlsproxy | tr "\\n" "," | sed 's/,$//'`
```

Анализ нагрузки на дисковую подсистему:

```
iostat -x -t 1
```

Анализ сетевого трафика:

```
tcpdump -nli tcp and host [-As0] [-X] [-E] [-w dump.pcap]
```

Параметры:
tcp
Показать только TCP-трафик
host
Показать только трафик заданного хоста
-As0
Отобразить передаваемые данные
-X
Отобразить данные в виде HEX-dump
-E

Отобразить MAC-адреса
-w dump.pcap
Перенаправить вывод в файл dump.pcap.

Анализ сетевого трафика утилитой tcpdump позволяет определить возможные проблемы с доступом пользователей в сеть Интернет через ArtX TLSproxy. Необходимо помнить, что когда ArtX TLSproxy работает в нормальном режиме, то:
1. Сетевой трафик на логических сетевых интерфейсах Internal и External содержит пакеты клиентов и серверов соединений. В ином случае необходимо обратиться к сетевому администратору для проверки настроек сетевого оборудования в соответствии с согласованной схемой включения ArtX TLSproxy (скорее всего, пакеты сервера направляются по другому маршруту).
2. Сетевой трафик логических интерфейсов Internal и External должен быть идентичным. В ином случае необходимо проверить настройки ArtX TLSproxy или обратиться в техническую поддержку.
3. ArtX TLSproxy может влиять только на TCP-трафик. На UDP, ICMP и т.д. ArtX TLSproxy никак не влияет. Поэтому, если в ходе настройки сервер ArtX TLSproxy не пропускает ICMP-пакеты в одну или другую сторону, необходимо проверить прохождение ICMP-пакетов команды ping, запущеной на проксируемом устройстве, а также на интерфейсах Internal и External утилитой tcpdump, включая запросы клиента и ответы сервера.

Если прикладной веб-интерфейс ArtX TLSproxy **недоступен по протоколу HTTP:**
Необходимо проверить наличие запущенных процессов nodejs:

```
root@tlsproxy:~# ps aux | grep "[n]odejs"
```

Если процесс nodejs существует, необходимо убедиться, что он запущен не в контексте сетевого окружения ArtX TLSproxy (не в namespace proxy):

```
ip netns identify `pidof nodejs`
```

Если результат выполнения команды не пустой, ArtX TLSproxy запущен из контекста сетевого окружения ArtX TLSproxy (namespace

proxy). В таком случае необходимо остановить ArtX TLSproxy, выйти из контекста сетевого окружения ArtX TLSproxy, затем запустить ArtX TLSproxy из namespace default.

Если "исчезли" один или более сетевых интерфейсов Необходимо убедиться, что текущая shell-сессия запущена в контексте сетевого окружения ArtX TLSproxy (namespace proxy). Сетевые интерфейсы, выполняющие роль Internal, External и Mirror должны быть доступны в namespace proxy.

Для определения текущего контекста сетевого окружения (namespace) необходимо выполнить команду:

```
ip netns identify `echo $$`
```

Пустой результат выполнения данной команды означает, что текущая сессия shell выполняется в namespace default.

Анализ VLAN, используемых в точке подключения ArtX TLSproxy:

```
ip netns exec proxy tcpdump -c 10000 -nlei enp3s0 vlan | grep vlan | awk '{print $11}' | sed 's/.$//' | sort | uniq -c
```

где:

-c 10000

Количество пакетов, собираемых для анализа

enp3s0

Имя сетевого интерфейса для анализа

vlan

Фильтровать весь нетегированный трафик.

Пример вывода (в левом столбце количество пакетов из выборки (из 10000 пакетов)):

```
ip netns exec proxy tcpdump -c 10000 -nlei enp3s0 vlan | grep vlan | awk '{print $11}'
| sed 's/.$//' | sort | uniq -c
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
10000 packets captured 10118 packets received by filter
0 packets dropped by kernel
3 packets dropped by interface
37 1020
39 105
40 111
```

```
8806 112
113 20
417 3
2 61
226 71
58 72
96 91
166 93
```

3.3.2.5. Логирование

В ArtX TLSproxy реализовано многоуровневое логирование различных событий: как прикладных, так и сетевого трафика.
Для включения полного логирования всех данных проксируемых соединений необходимо включить в конфигурационном файле config.json параметр debugState.

После этого все данные проксируемых соединений будут записываться в файл лога full.log, расположенный в каталоге, указанном в параметре fullLog конфигурационного файла config.json, а также в файл /var/log/syslog. При включенном параметре remoteSyslog конфигурационного файла config.json подлежащие логированию события также будут отправляться на указанный в значении этого параметра SYSLOG-сервер.

Также в каталог connlog, указанный в параметре connectionLogDir конфигурационного файла config.json, в случае выставления параметра binlog в true, записываются логи сетевых соединений с разбивкой по IP-адресам источников и назначений соединений.
В каталог connlog/ae, указанный в параметре debugSpool конфигурационного файла config.json, записываются логи автоисключений.

Важно:
Полное логирование создает большую нагрузку на сервер, в особенности на дисковую подсистему и CPU, что может оказать сильное влияние на производительность. В штатном режиме функционирования рекомендуется отключать полное логирование, в том числе binlog. Для диагностических целей рекомендуется использовать выборочное логирование.

Выборочное логирование позволяет анализировать различные каналы для определенных проксируемых устройств, не перегружая при этом систему не представляющими интереса событиями.
Для включения возможности выборочного логирования необходимо установить параметр fullLogManual конфигурационного файла config.json в true.

Для работы с выборочным логированием используется база данных debug утилиты dbctl.

Примеры:

Включение выборочного логирования для устройства с IP-адресом 192.168.1.5:

```
./dbctl -D debug -a 192.168.1.5 1
SOCK,SSL,EV,BIO,MIRROR,QUEUE,DETECTOR,MEM,CONN,XMPP,MRA,BRIDGE,STATS,UTIL,
CTL,PROFILER, NODEJS,DB
```

Здесь параметр 1 означает включение выборочного логирования. Временное отключение выборочного логирования для устройства с IP-адресом 192.168.1.5:

```
./dbctl -D debug -a 192.168.1.5 0
```

Здесь параметр 0 означает временное отключение выборочного логирования.
Полное отключение выборочного логирования для устройства с IP-адресом 192.168.1.5:

```
./dbctl -D debug -d 192.168.1.5
```

4. Рекомендации по внедрению ArtX TLSproxy

В данном разделе описаны основные рекомендации по внедрению ArtX TLSproxy в тестовую или рабочую среду.

4.1. Внедрение

Основные требования к серверу для ArtX TLSproxy описаны в разделе Системные требования. В данном разделе указываются дополнительные рекомендации по внедрению.

Количество сетевых интерфейсов сервера

В требованиях к оборудованию указано не менее 4 сетевых интерфейсов для сервера ArtX TLSproxy, и это требование настоятельно рекомендуется выполнять. Наличие четырёх сетевых интерфейсов значительно упрощает процедуру внедрения, так как ArtX TLSproxy можно при любой архитектуре сети представить заказчику "медным кабелем", который просто устанавливается "в разрыв", по умолчанию пропуская весь сетевой трафик без изменений.

После проверки работоспособности всех сегментов сети, настроенных на работу через ArtX TLSproxy, следует поэтапно настроить проксирование.

Рекомендованный порядок действий при внедрении

- Выполнить установку и настройку ArtX TLSproxy согласно разделу Установка ArtX TLSproxy. Проанализировать корректность работы оборудования (анализ логов /var/log/messages, dmesg).
- Направить через ArtX TLSproxy трафик тестовой рабочей станции. Убедиться, что сетевой трафик проходит через сервер ArtX TLSproxy прозрачно (bypass). Убедиться, что ArtX TLSproxy успешно проксирует сетевой трафик тестовой рабочей станции. Проверить доставку копии развернутого ArtX TLSproxy трафика системам-потребителям.
- Выполнить настройку автозапуска сетевого окружения, позволяющего серверу ArtX TLSproxy пропускать сетевой трафик bypass или же проксировать его сразу после перезагрузки. Протестировать работу автозапуска путём перезагрузки.
- Добавить в настройки ArtX TLSproxy согласованный заранее список исключений.

- Выпустить сертификат и распространить его среди проксируемых ArtX TLSproxy устройств, обратить внимание на алгоритм хеширования (должен быть SHA256/SHA512). См. раздел Выпуск сертификата
- Поэтапно пропускать через ArtX TLSproxy сетевой трафик пользователей, следить за потреблением сервером ресурсов, а также за работоспособностью доступа в Интернет и к локальным сетевым ресурсам.
- Проанализировать список автоисключений, размещая их в Исключения или Неисключаемые ресурсы.