INFOWATCH

IW Gateway Adapter. Руководство по установке и конфигурированию

14/09/2026

© АО “ИнфоВотч”

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

1 Введение 4

2 Аудитория 5

3 Общая информация об InfoWatch Gateway Adapter 6

3.1 Состав InfoWatch Gateway Adapter 6

3.2 Схема работы InfoWatch Gateway Adapter 6

3.3 Функции InfoWatch Gateway Adapter 8

3.3.1 События Gateway Adapter в Traffic Monitor 8

Фильтрация событий для отправки в Traffic Monitor 10

4 Аппаратное и программное обеспечение для InfoWatch Gateway Adapter 11

4.1 Требования к аппаратному обеспечению 11

4.2 Требования к программному обеспечению 11

4.3 Почтовые приложения 11

4.4 Почтовый сервер 12

5 Установка InfoWatch Gateway Adapter 13

5.1 Установка на сервер под управлением ОС Red Hat Enterprise Linux или Oracle Linux 13

5.1.1 Обновление в рамках одной версии ОС 14

5.2 Установка на сервер под управлением ОС Astra Linux 14

5.2.1 Обновление в рамках одной версии ОС 15

6 Установка плагина Gateway для InfoWatch Traffic Monitor 16

6.1 Поддержка OWA, IMAP и SMTP 16

7 Настройка InfoWatch Gateway Adapter 18

7.1 Настройка после установки и запуск Gateway Adapter 18

7.1.1 Настройки в конфигурационном файле 18

Добавление сертификата и ключа 18

Настройки портов прокси 19

Подключение к Traffic Monitor 19

Очередь отправки событий 21

Поддержка Outlook Web App, IMAP и SMTP 22

Черные и белые списки сотрудников 23

7.1.2 Управление модулем Gateway Adapter 24
7.2 Настройка для работы с несколькими почтовыми серверами 24
7.2.1 Настройка Gateway Adapter для работы с несколькими почтовыми серверами 25
8 Диагностика InfoWatch Gateway Adapter 26
8.1 Лог-файлы 26
8.2 Дампы трафика 26
9 Удаление InfoWatch Gateway Adapter 28

1 Введение

В настоящем руководстве представлены сведения по установке, настройке и администрированию InfoWatch Gateway Adapter (далее также Gateway Adapter, Gateway). В настоящем руководстве не рассматриваются вопросы установки и настройки почтовых серверов (Microsoft Exchange и других). За получением необходимых сведений вы можете обратиться к официальной документации Microsoft Exchange, документации Postfix, Exim и т.д.

2 Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов InfoWatch Traffic Monitor, которым требуется перехватывать события Exchange Gateway на почтовых серверах.

Руководство рассчитано на пользователей, имеющих навыки администрирования в среде операционных систем Microsoft Windows и Linux.

3 Общая информация об InfoWatch Gateway Adapter

InfoWatch Gateway Adapter – программный модуль, который обеспечивает взаимодействие между InfoWatch Traffic Monitor и почтовым сервером и предназначен для:

- Контроля активности использования почты на мобильных устройствах;
- Контроля облачных почтовых сред без возможности прямого администрирования и установки агента;
- Защиты опубликованных корпоративных ресурсов без агента и за периметром.

InfoWatch Gateway Adapter позволяет контролировать канал корпоративной почты. Перехват осуществляется по протоколам:

- ActiveSync и OWA (Outlook Web App), базирующихся на протоколе HTTP;
- IMAP (включая IMAP через TLS);
- SMTP (включая SMTP через TLS, SMTP через opportunistic TLS (STARTTLS)).

Если устройство сотрудника обменивается данными с сервером по протоколу Exchange Gateway, то Traffic Monitor создает событие типа *Gateway – Почта* и анализирует полученную информацию. Аналогично для протоколов OWA, IMAP и SMTP создаются события с типами *OWA – Почта* и *IMAP – Почта*, *SMTP – Почта*.

В этом разделе:

- Состав InfoWatch Gateway Adapter
- Схема работы InfoWatch Gateway Adapter
- Функции InfoWatch Gateway Adapter

3.1 Состав InfoWatch Gateway Adapter

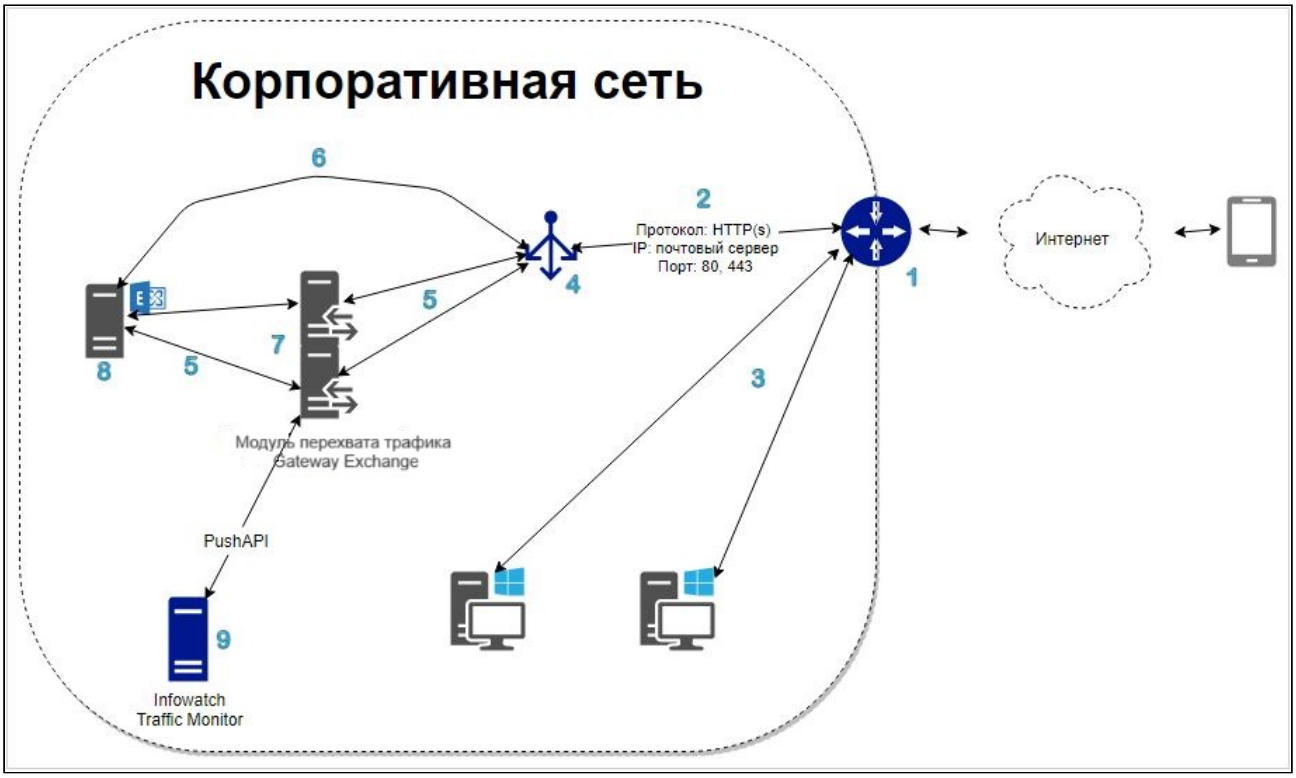
Модуль InfoWatch Gateway Adapter – это прокси-сервер, который позволяет перехватывать события в рамках HTTP-, IMAP- или SMTP- транзакции и получать доступ к ее атрибутам.

Модуль состоит из следующих компонентов:

- Сетевой прокси-сервер;
- Парсеры протоколов HTTP, ActiveSync, OWA, IMAP, SMTP;
- Загрузчик событий в Traffic Monitor;
- База данных дедупликации и контекста транзакций.

3.2 Схема работы InfoWatch Gateway Adapter

На рисунке показан принцип работы InfoWatch Gateway Adapter на примере протокола **ActiveSync**. Для протоколов **OWA**, **IMAP** и **SMTP** схема работы адаптера аналогична.



Элементы схемы, отмеченные цифрами на рисунке:

1. Основной шлюз между корпоративной сетью и интернетом.
2. HTTP(S) *(*TCP port 80, 443*)* трафик, проходящий между балансирующим узлом и шлюзом, предназначенный для почтового сервера (8).

   > **Примечание:**
   >
   > В случае протокола IMAP используется TCP порт 143, IMAPS (IMAP через SSL/TLS) порт 993. Для протокола SMTP используется TCP порт 25, для протокола SMTPS используется порт 587.

3. Прочий трафик между шлюзом (1) и узлами корпоративной сети.
4. Балансирующий узел.
5. Трафик между IW Gateway и прокси-сервером.
6. Резервный низко-приоритетный канал трафика, используемый в случае отказа в обслуживании со стороны узлов перехвата.
7. Кластер узлов перехвата трафика.
8. Почтовый сервер.
9. DLP-система InfoWatch Traffic Monitor.

Схема подключения подразумевает установку в корпоративной сети клиента "прослушивающего" кластера для HTTP(S)-трафика, проходящего между шлюзом выхода в сеть (1) и почтовым сервером (8). Для мониторинга и перехвата трафика предполагается использовать следующие компоненты:

- балансирующий узел (4);
- один или несколько узлов перехвата трафика Gateway Exchange (7).

Потоки трафика настраиваются таким образом, что на балансирующий узел (4) приходит только HTTP(S)-трафик, предназначенный для почтового сервера (8). Далее балансирующий узел производит

равномерное распределение данного трафика по узлам перехвата (5). В целях отказоустойчивости производится настройка дополнительного канала обвода трафика с низким приоритетом (6). Данный канал имеет более низкий приоритет и не будет использоваться до момента, пока успешно работает хотя бы один узел перехвата (7).

3.3 Функции InfoWatch Gateway Adapter

InfoWatch Gateway Adapter создает события в следующих случаях:

- Устройство отправляет данные на почтовый сервер.
  Примеры:
  - сотрудник отправляет письмо с мобильного устройства;
  - сотрудник сохраняет черновик письма на мобильном устройстве.
- Почтовый сервер отправляет данные на устройство.
  Примеры:
  - сотрудник читает письмо на мобильном устройстве;
  - сотрудник скачивает вложение на мобильное устройство;
  - мобильное устройство синхронизируется с сервером, например, загружает письма с сервера.

События отображаются в Traffic Monitor.

3.3.1 События Gateway Adapter в Traffic Monitor

События модуля в Traffic Monitor имеют тип *ActiveSync – Почта*, *OWA – Почта*, *IMAP – Почта* или *SMTP – Почта* в зависимости от перехватываемого протокола.

Типы событий модуля (атрибут *Тип события ActiveSync*, *Тип события OWA* или *Тип события IMAP*, *Тип события SMTP*):

Тип события	Описание	Атрибуты события
`sendmail`	Сотрудник отправил письмо	• *Тема письма* • *Отправители* – аккаунт на устройстве, которое обменивалось данными с почтовым сервером • *Получатели* – аккаунты получателей письма • *Отправитель письма gateway* – аккаунт отправителя письма • *Содержимое события* – текст письма и вложения
`fetchmail`	Сотрудник прочитал письмо / письмо было загружено на устройство сотрудника с почтового сервера в результате синхронизации	
`senddraft`	Сотрудник сохранил черновик письма на личном устройстве, данные о черновике были отправлены с устройства сотрудника на почтовый сервер	
`fetchdraft`	Черновик письма был загружен на устройство сотрудника с почтового сервера в результате синхронизации	• *Тема письма* • *Отправители* – аккаунт на устройстве, которое обменивалось данными с почтовым сервером

Тип события	Описание	Атрибуты события
		• *Получатели* – аккаунты получателей письма и аккаунт на устройстве, которое обменивалось данными с почтовым сервером • *Отправитель письма gateway* – аккаунт отправителя письма • *Содержимое события* – текст письма и вложения
`load_attachment`	Сотрудник скачал вложение	• *Тема письма* не определяется. Всегда указывается значение: `load_attachment` • *Отправители* – аккаунт на устройстве, которое обменивалось данными с почтовым сервером • *Получатели* – аккаунт сотрудника, который скачал файл • *Отправитель письма gateway* – аккаунт сотрудника, который скачал файл • *Содержимое события* – Файл **Примечание:** Для событий протокола *ActiveSync* также перехватываются вложения календарей и встреч.

Пример:

Пользователь **User1** отправляет письмо с рабочей станции пользователям **User2** и **User3**.

User2 синхронизирует почту с помощью Exchange Gateway на мобильном устройстве. Данные о письме загружаются на мобильное устройство. В результате синхронизации будет создано событие с атрибутами:

- *Тип события gateway* – `fetchmail` (письмо получено в результате синхронизации);
- *Отправители* – **User2** (устройство этого пользователя получило данные с сервера в результате синхронизации);
- *Отправитель письма gateway* – **User1** (пользователь является фактическим отправителем письма);
- *Получатели* – **User2**, **User3**.

> **Примечание:**
>
> События перехвата в Traffic Monitor определяются взаимодействием клиента и почтового сервера. Состав событий перехвата зависит от особенностей реализации протокола ActiveSync на клиенте и сервере, а также их настроек. Поэтому события в Traffic Monitor могут формироваться не полностью.

Фильтрация событий для отправки в Traffic Monitor

По умолчанию в Traffic Monitor отправляются все типы событий, а также события любого размера. Вы можете задать список типов событий и минимальный и/или максимальный размер событий, подлежащих отправке в Traffic Monitor.

> **Примечание:**
>
> Под размером события понимается размер тела письма.

Определение типов событий

Если эта опция включена, отправляться будут только указанные типы событий.

Чтобы включить опцию, необходимо указать в файле `/opt/iw/gateway/etc/gateway.conf` следующую настройку:

```
<PROTO>.tma.event_filter=<типы событий через запятую>
```

где `<PROTO>` – один из протоколов: `activesync`, `imap`, `owa`, `smtp`.

Пример:

Включена отправка по протоколу `activesync` типов событий `sendmail` и `load_attachment` в Traffic Monitor:

```
activesync.tma.event_filter=sendmail,load_attachment
```

Определение размеров событий

Если эта опция включена, отправляться будут только те события, которые подпадают под указанные ограничения размера.

Чтобы включить опцию, необходимо указать в файле `/opt/iw/gateway/etc/gateway.conf` следующие настройки:

```
<PROTO>.tma.min_event_size=<минимальный размер события>
<PROTO>.tma.min_event_size=<максимальный размер события>
```

где `<PROTO>` – один из протоколов: `activesync`, `imap`, `owa`, `smtp`.

Допускается указание как обеих, так и одной из этих настроек. Значения минимального и максимального размера события указываются в байтах.

Пример:

Указано минимальное значение для протокола `activesync` равное 1024 Б и максимальное значение для протокола `smtp` равное 1000000 Б:

```
activesync.tma.min_event_size=1024
smtp.tma.min_event_size=1000000
```

4 Аппаратное и программное обеспечение для InfoWatch Gateway Adapter

4.1 Требования к аппаратному обеспечению

Требования к аппаратному обеспечению в зависимости от предполагаемой нагрузки:

Аппаратное обеспечение	Количество пользователей	
	100	10 000
Процессор (количество ядер)	1	16
Оперативная память	2 ГБ	6 ГБ
Жесткий диск	100 ГБ 7200 об/мин	
Сетевой интерфейс	100 Мб/с Ethernet	1 Гб/с Ethernet

4.2 Требования к программному обеспечению

Поддерживается установка адаптера на сервер под управлением операционной системы:

- Red Hat Enterprise Linux, начиная с версии 8.x;
- Oracle Linux, начиная с версии 8.x;
- Astra Linux 1.8.

4.3 Почтовые приложения

Поддерживается перехват следующих приложений:

- Boxer - Workspace ONE (приложение Android);
- Почта (встроенное приложение IOS);
- Blue Mail (приложение Android/IOS).

> **Примечание:**
>
> Поддерживаются только события с типом **sendmail**, **fetchmail**, **load_attachment**. Подробнее о типах событий см. *Функции InfoWatch Gateway Adapter*.

- Почта (приложение Windows 10);

> **Примечание:**

Поддерживаются только события с типом **sendmail**, **fetchmail**, **load_attachment**.

- Microsoft Outlook Web App (далее также OWA; веб-клиент).

  Примечание:

  Поддерживаются только события с типом **sendmail**, **fetchmail**, **fetchdraft**.

4.4 Почтовый сервер

Почтовый сервер должен поддерживать протоколы, которые необходимо перехватывать.

На сервере должны быть открыты порты:

- в случае протоколов Exchange Gateway и OWA: 80 и 443;
- в случае протокола IMAP: 993 и 143;
- в случае протокола SMTP: 25 и 587.

5 Установка InfoWatch Gateway Adapter

Для установки адаптера используйте инструкции:

- Установка на сервер под управлением ОС Red Hat Enterprise Linux или Oracle Linux
- Установка на сервер под управлением ОС Astra Linux

5.1 Установка на сервер под управлением ОС Red Hat Enterprise Linux или Oracle Linux

Дистрибутив Gateway Adapter представляет собой RPM-пакет:

```
iw_gateway-1.3-0.el8.x86_64.rpm
```

Выполните шаги:

1. Установите репозитории:
   В случае установки с использованием внешних репозиториев:

   Установите репозиторий EPEL с помощью менеджера пакетов YUM или DNF:

   - Для RHEL 8:

     ```
     yum install epel-release
     ```

     или

     ```
     dnf install epel-release
     ```

   - Для Oracle Linux 8:

     ```
     yum install oracle-epel-release-el8
     ```

     или

     ```
     dnf install oracle-epel-release-el8
     ```

   > **Примечание:**
   >
   > Пакеты, которые требуются для Gateway Adapter, будут автоматически установлены из подключенных репозиториев при установке адаптера.

   В случае установки без доступа к внешним репозиториям:

   Вручную загрузите и установите пакеты, если они ранее не были установлены в ОС:

```
zlib
thrift
libcap-ng-utils
```

2. Установите Gateway с помощью менеджера пакетов YUM или DNF:

```
yum install iw_gateway-1.3-0.el8.x86_64.rpm
```

или

```
dnf install iw_gateway-1.3-0.el8.x86_64.rpm
```

После установки Gateway Adapter:

1. Установите плагин (см. *Установка плагина Gateway для InfoWatch Traffic Monitor*).
2. Настройте Gateway (см. *Настройка InfoWatch Gateway Adapter*).

5.1.1 Обновление в рамках одной версии ОС

Для обновления адаптера в рамках той версии ОС, где он был установлен, используйте команду:

```
rpm -Uvh iw_gateway-1.3-0.el8.x86_64.rpm
```

5.2 Установка на сервер под управлением ОС Astra Linux

Дистрибутив Gateway Adapter представляет собой DEB-пакет:

```
iw_gateway-1.3-1.deb
```

Выполните шаги:

1. **В случае установки без доступа к внешним репозиториям:**

   Вручную загрузите и установите пакеты, если они ранее не были установлены в ОС:

```
libthrift-0.17.0
libcap-ng-utils
```

2. Установите Gateway с помощью менеджера пакетов APT:

```
sudo apt install ./iw_gateway-1.3-1.deb
```

После установки Gateway Adapter:

1. Установите плагин (см. *Установка плагина Gateway для InfoWatch Traffic Monitor*).
2. Настройте Gateway Adapter (см. *Настройка InfoWatch Gateway Adapter*).

5.2.1 Обновление в рамках одной версии ОС

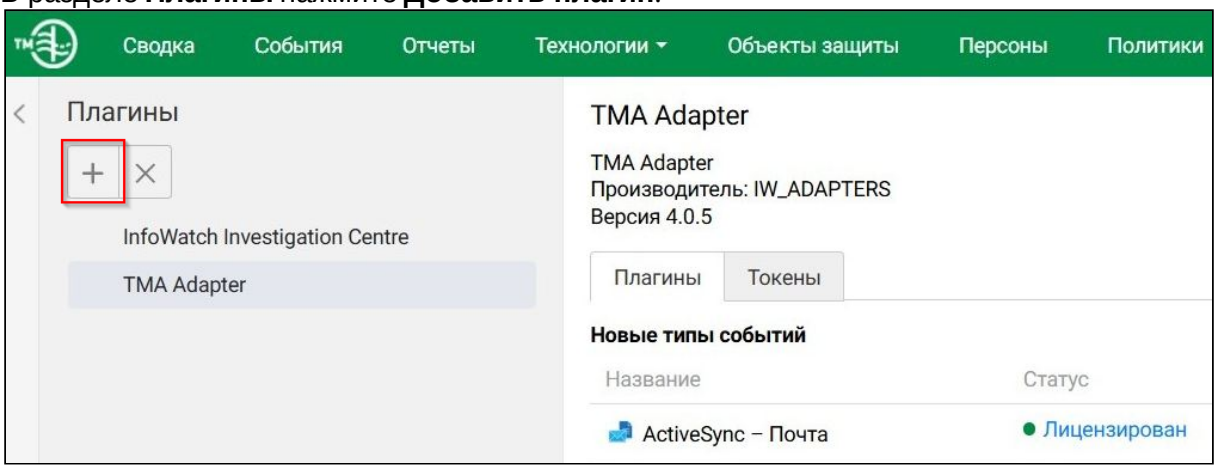
Для обновления адаптера в рамках той версии ОС, где он был установлен, используйте команду:

```
sudo apt install ./iw_gateway-1.3-1.deb
```

6 Установка плагина Gateway для InfoWatch Traffic Monitor

Чтобы установить плагин для InfoWatch Traffic Monitor:

1. В разделе **Плагины** нажмите **Добавить плагин**.



2. В появившемся окне нажмите **Загрузить**.
3. Выберите файл плагина (`.zip`).
4. Убедитесь, что напротив плагина установлен статус *Лицензирован*. Если напротив плагина установлен статус *Не лицензирован*, то:
   a. Убедитесь, что в файле плагина (`.zip`) присутствуют `manifest.json` и файл лицензии (`.license`).
   b. Откройте `manifest.json` на редактирование и пропишите в параметре `LICENSE` путь до нужного файла лицензии. Путь укажите относительно файла `manifest.json` . Например, если файл лицензии `tm_license.license` и `manifest.json` находятся в одной директории, то укажите:

```
"LICENSE": [
      { "PATH" : "tm_license.license" }
   ]
```

   c. Сохраните изменения и повторите шаги 1-4.

6.1 Поддержка OWA, IMAP и SMTP

Для корректной работы перехватчика трафика с OWA, IMAP и SMTP загрузка содержимого должна производиться с идентификаторами сервисов `owa` , `imap` и `smtp` соответственно. Для этого требуется регистрация в манифесте плагина и лицензии.

Пример фрагмента манифеста плагина с регистрацией перехватчиков ActiveSync, OWA и SMTP:

```
"ADDS_SERVICES": {
    "SERVICE_TYPE": [
        {
            "SERVICE_MNEMO": "activesync",
            "DATA_CLASS": ["kEmail"],
            "ICON": "icon/WP_icon.png",
            "LOCALE":
            {
                "rus": "ActiveSync – Почта",
```

```
                "eng": "ActiveSync – Mail"
            }
        },
        {
            "SERVICE_MNEMO": "owa",
            "DATA_CLASS": ["kEmail"],
            "ICON": "icon/WP_icon.png",
            "LOCALE":
            {
                "rus": "OWA – Почта",
                "eng": "OWA – Mail"
            }
        }
    ]
},
{
            "SERVICE_MNEMO": "smtp",
            "DATA_CLASS": ["kEmail"],
            "ICON": "icon/WP_icon.png",
            "LOCALE":
            {
                "rus": "SMTP – Почта",
                "eng": "SMTP – Mail"
            }
        }
    ]
},
```

7 Настройка InfoWatch Gateway Adapter

Для корректной работы произведите первичную настройку Gateway Adapter (см. *Настройка после установки и запуск Gateway Adapter*) и настройте маршрутизацию (см. *Настройка для работы с несколькими почтовыми серверами*).

Настройка Gateway Adapter производится на сервере, на котором он установлен.

7.1 Настройка после установки и запуск Gateway Adapter

После установки выполните настройки в конфигурационном файле `/opt/iw/gateway/etc/gateway.conf`:

- Добавление сертификата и ключа
- Настройки портов прокси
- Подключение к Traffic Monitor
- Очередь отправки событий
- Поддержка Outlook Web App, IMAP и SMTP
- Черные и белые списки сотрудников

> **Важно!**
>
> Если Gateway Adapter уже запущен, то для применения новых настроек требуется его перезапустить. О перезапуске и проверке статуса см. Управление модулем Gateway Adapter.

7.1.1 Настройки в конфигурационном файле

Добавление сертификата и ключа

Чтобы Gateway Adapter мог работать с TLS-соединениями, требуются файлы сертификата и закрытого ключа почтового сервера.

Чтобы добавить сертификат и ключ в Gateway Adapter:

1. Экспортируйте файл сертификата и файл закрытого ключа из почтового сервера.
2. Поместите PEM-файлы сертификата и закрытого ключа в директорию `/opt/iw/gateway/etc`.
3. В файле `/opt/iw/gateway/etc/gateway.conf` укажите настройки вида:

   ```
   proxy.<PROTO>.certificate
   proxy.<PROTO>.private_key
   ```

   где `<PROTO>` – наименование протокола (см. ниже).

Пример:

```
proxy.https.certificate=exchange.pem
proxy.https.private_key=privkey.pem
proxy.imaps.certificate=exchange.pem
```

```
proxy.imaps.private_key=privkey.pem
proxy.smtpstls.certificate=exchange.pem
proxy.smtpstls.private_key=privkey.pem
```

где

- `exchange.pem` – имя файла с сертификатом;
- `privkey.pem` – имя файла с закрытым ключом.

Настройки портов прокси

В конфигурационном файле `/opt/iw/gateway/etc/gateway.conf` укажите настройки:

```
proxy.<PROTO>.port
```

где `<PROTO>` – это наименование одного из протоколов:

- `http` – протоколы на основе HTTP (ActiveSync, OWA);
- `https` – протоколы на основе HTTPS (ActiveSync, OWA);
- `imap` – IMAP;
- `imaps` – IMAP через TLS;
- `smtp` – SMTP;
- `smtps` – SMTP через TLS;
- `smtpstls` – SMTP через opportunistic TLS (STARTTLS).

Пример:

```
proxy.http.port=80
proxy.https.port=443
proxy.imap.port=143
proxy.imaps.port=993
proxy.smtpstls.port=587
```

Настройка для HTTPS и non-TLS / HTTP соединений

Если требуется использовать HTTP-соединения, в файле `/opt/iw/gateway/etc/gateway.conf` укажите:

```
proxy.http.port=80
```

В случае использования HTTPS:

```
proxy.https.port=443
```

Подключение к Traffic Monitor

Укажите в файле `/opt/iw/gateway/etc/gateway.conf` настройки для подключения к Traffic Monitor:

```
#Адрес сервера Traffic Monitor
<INTERCEPTOR>.tma.<TYPE>.<IFACE>.<NAME>.destination = IP:PORT
#Данные для авторизации
<INTERCEPTOR>.tma.<TYPE>.<IFACE>.<NAME>.credentials = COMPANY:TOKEN
# Полное доменное имя сервера, на котором установлен Gateway Adapter; необязательный параметр
<INTERCEPTOR>.tma.<TYPE>.<IFACE>.<NAME>.server_fqdn = localhost
```

Где:

- `<INTERCEPTOR>` – тип перехватчика протокола. Может иметь значения:
  - `activesync` – протокол ActiveSync;
  - `owa` – протокол OWA;
  - `imap` – протокол IMAP;
  - `smtp` – протокол SMTP.
- Необязательные составляющие:
  - `<TYPE>` – тип инстанса. Может иметь значение `master` (по умолчанию) или `slave`. Подробнее об инстансах см. ниже;
  - `<IFACE>` – тип API-интерфейса Traffic Monitor. Подробнее см. документ *InfoWatch Traffic Monitor. Введение в API*;
    - `thrift` (по умолчанию);
    - `rest`.
  - `<NAME>` – имя инстанса Traffic Monitor, являющееся его уникальным идентификатором в модуле перехвата трафика. Может принимать любое строковое значение, состоящее из символов ASCII. Данное имя будет указываться в лог-файлах. Значение по умолчанию: `default`.

> **Примечание:**
>
> В файле конфигурации можно указать настройки, не содержащие составляющие `<TYPE>` и `<NAME>`, только для одного инстанса Traffic Monitor.

Формат указания значений:

- `IP:PORT` – формат указания адреса сервера Traffic Monitor: IP-адрес и порт сервиса xapi для получения событий, по умолчанию – `9101`.
- `COMPANY:TOKEN` – формат данных для авторизации:
  - `COMPANY` – значение ключа `common_name` из файла лицензии для модуля InfoWatch Gateway Adapter. По умолчанию в лицензии указано: `IW_ADAPTERS`;
  - `TOKEN` – токен плагина Gateway Adapter. Вы можете получить токен в Консоли управления Traffic Monitor: *Управление → Плагины → Gateway TM Adapter → Токены*.

Пример:

```
activesync.tma.destination = 10.70.229.153:9101
activesync.tma.credentials = TSW:i2swkk1q5wq01k5ruf4w1
activesync.tma.server_fqdn = localhost
```

Инстансы Traffic Monitor

Для распределения нагрузки вы можете указать несколько инстансов Traffic Monitor. Инстанс – это отдельно установленная система Traffic Monitor, имеющая уникальные IP-адрес, параметры авторизации и пр. Для каждого из инстансов укажите тип:

- `master`, т.е. основной
  или
- `slave`, т.е. резервный

События распределяются равномерно между всеми доступными инстансами, заданными как `master`, по принципу round-robin. Если ни один из инстансов Traffic Monitor с типом `master` не доступен, события отправляются на инстансы Traffic Monitor с типом `slave` и распределяются между ними также по принципу round-robin.

Пример:

Требуется задать параметры подключения к двум инстансам Traffic Monitor с типом `master` и `slave`.

Для этого в файле `/opt/iw/gateway/etc/gateway.conf` укажите следующие настройки:

```
activesync.tma.master.master1.destination = 10.70.228.31:9101
activesync.tma.master.master1.credentials = IW_ADAPTERS:master1token
activesync.tma.slave.slave1.destination = 10.70.228.33:9101
activesync.tma.slave.slave1.credentials = IW_ADAPTERS3:slave1token
```

Очередь отправки событий

Если все инстансы Traffic Monitor, и с типом `master`, и с типом `slave`, недоступны, то события записываются в очередь, которая сохраняется на локальный диск. Как только хотя бы один инстанс Traffic Monitor становится доступен, сохраненные события отправляются в Traffic Monitor. После отправки всех сохраненных событий, файлы очереди очищаются.

Вы можете настроить очередь отправки событий. Для этого в файле `/opt/iw/gateway/etc/gateway.conf` укажите следующие параметры:

- Директорию на локальном диске, в которой хранятся файлы очереди:

  ```
  activesync.tma.storage_path=/opt/gateway/custom_queue_dir
  ```

  Директория по умолчанию: `/opt/iw/gateway/transport/queue`.
- Количество потоков, обслуживающих очередь отправки событий:

  ```
  activesync.tma.threads=<количество потоков>
  ```

  По умолчанию количество потоков равно количеству ядер центрального процессора. Каждый поток создает отдельный файл в директории.
- Предельный размер файла одного потока в ГБ:

  ```
  activesync.tma.storage_limit=<размер файла в ГБ>
  ```

  Значение по умолчанию: 32.

Примечание:

Максимальный размер дискового хранилища для очереди отправки событий равен произведению количества потоков на предельный размер файла одного потока.
Если файл потока достигнет своего предельного размера, то события не будут сохраняться.

Поддержка Outlook Web App, IMAP и SMTP

Важно!

Убедитесь, что перехватчики OWA, IMAP и SMTP зарегистрированы в манифесте плагина и лицензии (см. *Установка плагина Gateway для InfoWatch Traffic Monitor*).

Поддержка Outlook Web App

Для включения перехвата трафика OWA все настройки в конфигурационном файле `gateway.conf` должны содержать идентификатор `owa` в начале строки.

Пример:

Указаны адрес сервера Traffic Monitor, данные для авторизации и полное доменное имя сервера, на котором установлен Gateway Adapter, содержащие в начале строки идентификатор `owa` :

```
owa.tma.master.tm1.destination = 10.70.229.153:9101
owa.tma.master.tm1.credentials = TSW:i2swkk1q5wq01k5ruf4w1
owa.tma.master.tm1.server_fqdn = localhost
```

Для перехвата трафика OWA настройки Gateway Adapter менять не требуется, однако загрузка содержимого должна производиться с идентификатором сервиса `owa` .

Поддержка протокола IMAP

Важно!

Под IMAP в этом руководстве подразумевается IMAPS, т. к. современный почтовый сервер поддерживает только шифрованное IMAP-подключение по протоколу TLS.

При включении перехвата трафика убедитесь, что в настройках указан протокол безопасности TLS (993 порт).

Для включения перехвата трафика по протоколу IMAP все настройки в конфигурационном файле `gateway.conf` должны содержать идентификатор `imap` в начале строки.

Пример:

Указаны адрес сервера Traffic Monitor, данные для авторизации и полное доменное имя сервера, на котором установлен Gateway Adapter, содержащие в начале строки идентификатор `imap`:

```
imap.tma.master.tm1.destination = 10.70.229.153:9101
imap.tma.master.tm1.credentials = TSW:i2swkk1q5wq01k5ruf4w1
imap.tma.master.tm1.server_fqdn = localhost
```

Загрузка содержимого должна производиться с идентификатором сервиса `imap`.

Поддержка SMTP

Для включения перехвата трафика SMTP все настройки в конфигурационном файле `gateway.conf` должны содержать идентификатор `smtp` в начале строки.

Пример:

Указаны адрес сервера Traffic Monitor, данные для авторизации и полное доменное имя сервера, на котором установлен Gateway Adapter, содержащие в начале строки идентификатор smtp:

```
smtp.tma.master.tm1.destination = 10.70.229.153:9101
smtp.tma.master.tm1.credentials = TSW:i2swkk1q5wq01k5ruf4w1
smtp.tma.master.tm1.server_fqdn = localhost
```

Для перехвата трафика SMTP настройки Gateway Adapter менять не требуется, однако загрузка содержимого должна производиться с идентификатором сервиса smtp.

Важно!

Gateway Adapter может работать либо в режиме перехвата протоколов, базирующихся на HTTP (ActiveSync, OWA), либо в режиме перехвата протоколов, базирующихся на IMAP. Одновременный перехват IMAP и OWA/ActiveSync на данный момент не поддерживается.

Черные и белые списки сотрудников

Вы можете настроить перехват с помощью черных и белых списков:

- **Черный список**: модуль перехватывает только те события, в которых участвует хотя бы один сотрудник из списка. Например:
  - сотрудник является получателем/отправителем;
  - устройство сотрудника синхронизировалось с почтовым сервером.
- **Белый список**: модуль не перехватывает событие, если в нем участвует хотя бы один сотрудник из списка. Например:
  - сотрудник является получателем/отправителем;
  - устройство сотрудника синхронизировалось с почтовым сервером.

Примечание:

Если вы указали черный и белый списки одновременно, то будет использоваться только черный список.

Чтобы указать черный/белый список:

1. В директории `/opt/iw/gateway/etc.conf` создайте текстовый файл, например: `list.txt`.
2. Укажите аккаунты сотрудников в файле. Каждая строка должна содержать запись вида `<формат>:<аккаунт>`. Доступные форматы:
   - `auth` – логин авторизации сотрудника, например: `user@example`
   - `email` – адрес почты сотрудника, например: `user@example.com`

   Пример содержимого файла:

   ```
   auth:user1@example
   email:user2@example.com
   auth:user3@example
   ```

3. Укажите настройку в файле `/opt/iw/gateway/etc.conf`:
   - Черный список:

     ```
     <PROTO>.accounts.blacklist=list.txt
     ```

     где `<PROTO>` – протокол.

     Пример: `activesync.accounts.blacklist`
   - Белый список:

     ```
     <PROTO>.accounts.whitelist=list.txt
     ```

   Пример: `imap.accounts.whitelist`

7.1.2 Управление модулем Gateway Adapter

- Чтобы запустить Gateway Adapter, выполните команду:

  ```
  systemctl start iw_gateway
  ```

- Чтобы получить информацию о состоянии Gateway Adapter, выполните команду:

  ```
  systemctl status iw_gateway
  ```

- Чтобы остановить Gateway Adapter, выполните команду:

  ```
  systemctl stop iw_gateway
  ```

7.2 Настройка для работы с несколькими почтовыми серверами

Gateway Adapter работает в качестве прозрачного прокси-сервера.

На внешних маршрутизаторах должны быть настроены правила маршрутизации. Правила должны перенаправлять трафик, предназначенный для почтового сервера, на хост Gateway Adapter.

7.2.1 Настройка Gateway Adapter для работы с несколькими почтовыми серверами

Gateway Adapter может перенаправлять трафик на несколько почтовых серверов. В этом случае Gateway Adapter равномерно распределяет трафик между серверами.

Чтобы настроить работу Gateway Adapter с несколькими почтовыми серверами:

1. В файле `/opt/iw/gateway/etc/gateway.conf` укажите настройку (по умолчанию строка оформлена как комментарий):

   ```
   proxy.origin.<NAME>.address
   ```

   `<NAME>` – это строковое наименование.
2. В файле `/opt/iw/gateway/etc/gateway.conf` укажите адреса почтовых серверов. Каждый адрес должен быть указан на отдельной строке. Формат: IP-адрес.
   Пример:

   ```
   proxy.origin.SRV1.address=10.60.44.50
   proxy.origin.SRV2.address=10.60.44.51
   ```
3. Перезапустите модуль `iw_gateway`.

8 Диагностика InfoWatch Gateway Adapter

Вы можете настроить сбор отладочной информации на сервере, где установлен Gateway Adapter.

8.1 Лог-файлы

Лог-файлы расположены в директории `/opt/iw/gateway/log`.

Чтобы получать подробную отладочную информацию:

1. Откройте на редактирование файл `/opt/iw/gateway/etc/gateway.conf`.
2. Настройте ротацию лог-файлов:
   a. Укажите настройку уровня логирования:

      ```
      # log.level
      ```

      возможные значения: `info, debug`. Пример: `log.level=info`
   b. Укажите максимальный суммарный размер файла логов (в GB/MB/KB):

      ```
      # log.max_file_size
      ```

      Пример: `log.max_file_size=50MB`
   c. Укажите максимальный суммарный размер файла логов (в GB/MB/KB):

      ```
      # log.max_size
      ```

      Пример: `log.max_size=1GB`
3. Сохраните изменения.
4. Перезапустите Gateway Adapter.

8.2 Дампы трафика

Gateway Adapter позволяет создавать дампы трафика. Дампы трафика – файлы, которые содержат контент транзакций.

Вы можете сохранить как все транзакции, так и те из них, которые относятся к определенной персоне.

Чтобы настроить создание дампов трафика:

1. Откройте на редактирование файл `/opt/iw/gateway/log /gateway .conf`.
2. Добавьте настройку, чтобы включить создание дампов:

   ```
   <PROTO>.content_logging_enabled=1
   ```

   где `<PROTO>` – один из ID перехватчиков: activesync, owa, imap, smtp.
3. Если требуется создавать дампы только для определенного пользователя почтового сервера, помимо настройки включения дампов, добавьте также настройку:

```
<PROTO>.logging_contact=user@domain
```

Здесь `<PROTO>` – один из ID перехватчиков: activesync, owa, imap, smtp, а `user@domain` – логин пользователя почтового сервера.

> **Примечание:**
>
> Если не добавить настройку, дампы будут создаваться для всех транзакций.

> **Пример:**
>
> Включение дампа трафика протокола activesync для персоны ivanov@example.ru, и протокола smtp для всех персон:
> `activesync.content_logging_enabled=1`
> `activesync.logging_contact=ivanov@company.ru`
> `smtp.content_logging_enabled=1`

4. Сохраните изменения.
5. Перезапустите модуль iw gateway.

Файлы сохраняются в директории `/opt/iw/gateway/log/contents`. Каждый файл содержит информацию об одной транзакции. Имя файла содержит дату и логин пользователя.

9 Удаление InfoWatch Gateway Adapter

Удаление InfoWatch Gateway Adapter производится на сервере, где он установлен.

Удалите Gateway Adapter с помощью менеджера пакетов YUM или DNF:

```
yum erase iw_gateway
```

или

```
dnf erase iw_gateway
```