INFOWATCH

InfoWatch ActiveSync Adapter. Руководство по установке и конфигурированию

19/01/2024

© 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 ActiveSync Adapter 6

3.1 Состав InfoWatch Active Sync Adapter 6

3.2 Схема работы InfoWatch ActiveSync Adapter 6

3.3 Функции InfoWatch ActiveSync Adapter 7

3.3.1 События ActiveSync Adapter в Traffic Monitor 7

4 Аппаратное и программное обеспечение для InfoWatch ActiveSync Adapter 9

4.1 Требования к аппаратному обеспечению 9

4.2 Требования к программному обеспечению 9

4.3 Почтовые приложения 9

4.4 MS Exchange Server 9

5 Установка Webfilter 10

5.1 Установка с использованием внешних репозиториев 10

5.2 Установка без доступа к внешним репозиториям 11

6 Установка плагина ActiveSync для InfoWatch Traffic Monitor 13

7 Настройка InfoWatch ActiveSync Adapter 14

7.1 Настройка после установки и запуск Webfilter 14

7.1.1 Добавление сертификата и ключа 14

7.1.2 Настройка для non-TLS / HTTP соединений 14

7.1.3 Подключение к Traffic Monitor 15

7.1.4 Очередь отправки событий 16

7.1.5 Направления перехвата 17

7.1.6 Черные и белые списки сотрудников 18

7.1.7 Управление модулем Webfilter 18

7.2 Настройка маршрутизации 19

7.2.1 Автоматическое восстановление настроек 19

7.2.2 Настройка Webfilter для работы с несколькими почтовыми серверами 21

8 Диагностика InfoWatch ActiveSync Adapter 22

8.1 Лог-файлы 22
8.2 Дампы трафика 22
9 Удаление InfoWatch ActiveSync Adapter 24

1 Введение

В настоящем руководстве представлены сведения по установке, настройке и администрированию InfoWatch ActiveSync Adapter. В настоящем руководстве не рассматриваются вопросы установки и настройки сервера Exchange. За получением необходимых сведений вы можете обратиться к официальной документации Microsoft Exchange.

2 Аудитория

Информация, содержащаяся в руководстве, предназначена для администраторов InfoWatch Traffic Monitor, которым требуется перехватывать события Exchange ActiveSync в Exchange Server.

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

3 Общая информация об InfoWatch ActiveSync Adapter

Infowatch ActiveSync Adapter – программный модуль, предназначенный для обеспечения взаимодействия между InfoWatch Traffic Monitor и почтовым сервером Exchange.

Infowatch ActiveSync Adapter позволяет контролировать канал корпоративной почты. Если устройство сотрудника обменивается данными с сервером Exchange по протоколу Exchange ActiveSync, то Traffic Monitor создает событие типа **ActiveSync – Почта** и анализирует полученную информацию.

В этом разделе:

- Состав InfoWatch Active Sync Adapter
- Схема работы InfoWatch ActiveSync Adapter
- Функции InfoWatch ActiveSync Adapter

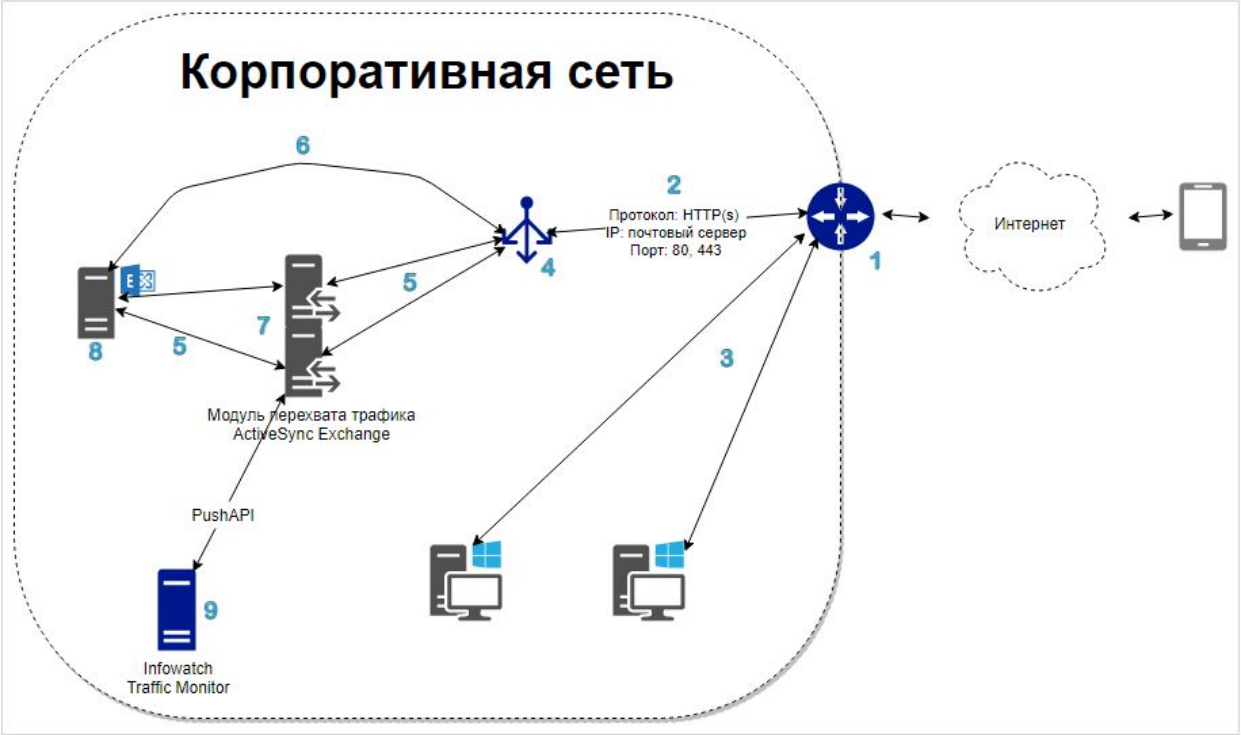
3.1 Состав InfoWatch Active Sync Adapter

Модуль InfoWatch Active Sync Adapter – это Webfilter-сервер, который состоит из следующих компонентов:

- Apache Traffic Server 6.0.0;
- Плагин Webfilter к HTTP-прокси Traffic Server. Traffic Server предоставляет специализированный API, позволяющий плагину перехватывать события в рамках HTTP-транзакции и получать доступ к её атрибутам, таким как: заголовки HTTP, URL, IP запроса, содержимое ответа и т. п.

3.2 Схема работы InfoWatch ActiveSync Adapter

На рисунке показан принцип работы InfoWatch ActiveSync Adapter.



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).
3. Прочий трафик между шлюзом (1) и узлами корпоративной сети.
4. Балансирующий узел LVS кластера.
5. HTTP(S) *(*TCP port 80, 443*)* трафик между балансирующим узлом и почтовым сервером, распределенный между узлами перехвата.
6. Резервный низко-приоритетный канал трафика, используемый в случае отказа в обслуживании со стороны узлов перехвата.
7. Кластер узлов перехвата трафика.
8. Почтовый сервер, поддерживающий протокол синхронизации Exchange ActiveSync.
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 MS Exchange сервером (8). Для мониторинга и перехвата трафика предполагается использовать следующие компоненты:

- балансирующий узел LVS кластера (5);
- один или несколько узлов перехвата трафика ActiveSync 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. 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 ActiveSync Adapter

InfoWatch ActiveSync Adapter создает события в следующих случаях:

- Устройство отправляет данные на сервер Exchange.
  Примеры:
  - сотрудник отправляет письмо с мобильного устройства;
  - сотрудник сохраняет черновик письма на мобильном устройстве.
- Сервер Exchange 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 ActiveSync Adapter в Traffic Monitor

События модуля в Traffic Monitor имеют тип **ActiveSync – Почта**.

Типы событий модуля (атрибут **Тип события active sync**):

- **sendmail** – сотрудник отправил письмо;
- **fetchmail** – сотрудник прочитал письмо / письмо было загружено на устройство сотрудника с сервера Exchange в результате синхронизации;
- **load_attachment** – сотрудник скачал вложение;
- **senddraft** – сотрудник сохранил черновик письма на личном устройстве, данные о черновике были отправлены с устройства сотрудника на сервер Exchange;

- **fetchdraft** – черновик письма был загружен на устройство сотрудника с сервера Exchange в результате синхронизации.

<table>
<tr><td rowspan="2"></td><td colspan="5">Тип события active sync</td></tr>
<tr><td>send mail</td><td>fetch mail</td><td>senddr aft</td><td>fetchdraft</td><td>load_attachment</td></tr>
<tr><td>Тема письма</td><td colspan="4">Тема письма</td><td>Тема письма не определяется. Всегда указывается значение: load attachment</td></tr>
<tr><td>Отправители</td><td colspan="5">Аккаунт на устройстве, которое обменивалось данными с сервером Exchange</td></tr>
<tr><td>Получатели</td><td colspan="3">Аккаунты получателей письма</td><td>Аккаунты получателей письма и аккаунт на устройстве, которое обменивалось данными с сервером Exchange</td><td rowspan="2">Аккаунт сотрудника, который скачал файл</td></tr>
<tr><td>Отправитель письма active sync</td><td colspan="4">Аккаунт отправителя письма</td></tr>
<tr><td>Содержимое события</td><td colspan="4">Текст письма и вложения</td><td>Файл</td></tr>
</table>

Пример:

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

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

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

4 Аппаратное и программное обеспечение для InfoWatch ActiveSync Adapter

4.1 Требования к аппаратному обеспечению

Количество пользователей	Процессор	Оперативная память	Жесткий диск	Сетевой интерфейс
100	Количество ядер – 1	2 GB	100 GB 7200rpm	100 Mbps Ethernet
10 000	Количество ядер – 16	6 GB		1 Gbps Ethernet

4.2 Требования к программному обеспечению

- CentOS, начиная с версии 7.x;
- Red Hat Enterprise Linux, начиная с версии 7.x;
- Oracle Linux, начиная с версии 7.x.

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**.

- Почта (приложение Windows 10).

> **Примечание:**
>
> Поддерживаются только события с типом **sendmail**, **fetchmail**, **load_attachment**.

4.4 MS Exchange Server

Почтовый сервер MS Exchange Server должен поддерживать протокол Exchange ActiveSync и иметь открытые порты 80 и 443.

5 Установка Webfilter

Дистрибутив Webfilter представляет собой RPM-пакет:

- Для RHEL 7, Oracle Linux 7, CentOS 7: `webfilter-server-x.x-x.el7.x86_64.rpm`, где `x.x-x` – номер версии;
- Для RHEL 8, Oracle Linux 8: `webfilter-server-x.x-x.el8.x86_64.rpm`, где `x.x-x` – номер версии.

5.1 Установка с использованием внешних репозиториев

Чтобы установить Webfilter:

1. Установите репозиторий EPEL с помощью менеджера пакетов YUM или DNF:
   - Для RHEL 7, RHEL 8, CentOS 7:
     - YUM: `yum install epel-release`
     - DNF: `dnf install epel-release`
   - Для Oracle Linux 7:
     - YUM: `yum install oracle-epel-release-el7`
     - DNF: `dnf install oracle-epel-release-el7`
   - Для Oracle Linux 8:
     - YUM: `yum install oracle-epel-release-el8`
     - DNF: `dnf install oracle-epel-release-el8`
2. Если установка производится в Oracle Linux 7, включите репозиторий `ol7_optional_archive`. Репозиторий содержит пакет `libcap-ng-utils`, который требуется для установки Webfilter.
   a. Откройте для редактирования файл `/etc/yum.repos.d/oracle-linux-ol7.repo`
   b. Укажите в файле:

```
[ol7_optional_archive]
name=Oracle Linux $releasever Optional ($basearch) - Archive
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL7/optional/archive/
$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1
```

   c. Сохраните внесенные изменения.
3. Установите пакет Webfilter с помощью менеджера пакетов YUM или DNF:

> **Примечание:**

Пакеты, которые требуются для Webfilter, будут автоматически установлены из подключенных репозиториев.

- Для RHEL 7, Oracle Linux 7, CentOS 7:
  - YUM:
    `yum install webfilter-server-x.x-x.el7.x86_64.rpm`
  - DNF:
    `dnf install webfilter-server-x.x-x.el7.x86_64.rpm`
- Для RHEL 8, Oracle Linux 8:
  - YUM:
    `yum install webfilter-server-x.x-x.el8.x86_64.rpm`
  - DNF:
    `dnf install webfilter-server-x.x-x.el8.x86_64.rpm`

После установки Webfilter:

1. Установите плагин (см. "Установка плагина ActiveSync для InfoWatch Traffic Monitor").
2. Настройте Webfilter (см. "Настройка InfoWatch ActiveSync Adapter").

5.2 Установка без доступа к внешним репозиториям

1. Вручную загрузите и установите пакеты:
   - Для RHEL 7, Oracle Linux 7, CentOs 7:

```
hwloc-1.11.8-4.el7.x86_64.rpm
libcap-ng-utils-0.7.5-4.el7.x86_64.rpm
hwloc-libs-1.11.8-4.el7.x86_64.rpm
tcl-8.5.13-8.el7.x86_64.rpm
unzip-6.0-24.el7_9.x86_64.rpm
boost-filesystem-1.53.0-28.el7.x86_64.rpm
boost-system-1.53.0-28.el7.x86_64.rpm
boost-thread-1.53.0-28.el7.x86_64.rpm
thrift-0.9.1-15.el7.x86_64.rpm
libicu-50.2-4.el7_7.x86_64.rpm
```

   - Для RHEL 8, Oracle Linux 8:

```
hwloc-2.2.0-3.el8.x86_64.rpm
libcap-ng-utils-0.7.11-1.el8.x86_64.rpm
hwloc-libs-2.2.0-3.el8.x86_64.rpm
tcl-8.6.8-2.el8.x86_64.rpm
unzip-6.0-45.el8_4.x86_64.rpm
boost-filesystem-1.66.0-10.el8.x86_64.rpm
boost-system-1.66.0-10.el8.x86_64.rpm
boost-thread-1.66.0-10.el8.x86_64.rpm
thrift-0.13.0-2.el8.x86_64.rpm
libicu-60.3-2.el8_1.x86_64.rpm
```

2. Установите пакет Webfilter с помощью менеджера пакетов YUM или DNF:
   - Для RHEL 7, Oracle Linux 7, CentOS 7:

        - YUM:
          `yum install webfilter-server-x.x-x.el7.x86_64.rpm`
        - DNF:
          `dnf install webfilter-server-x.x-x.el7.x86_64.rpm`
    - Для RHEL 8, Oracle Linux 8:
        - YUM:
          `yum install webfilter-server-x.x-x.el8.x86_64.rpm`
        - DNF:
          `dnf install webfilter-server-x.x-x.el8.x86_64.rpm`

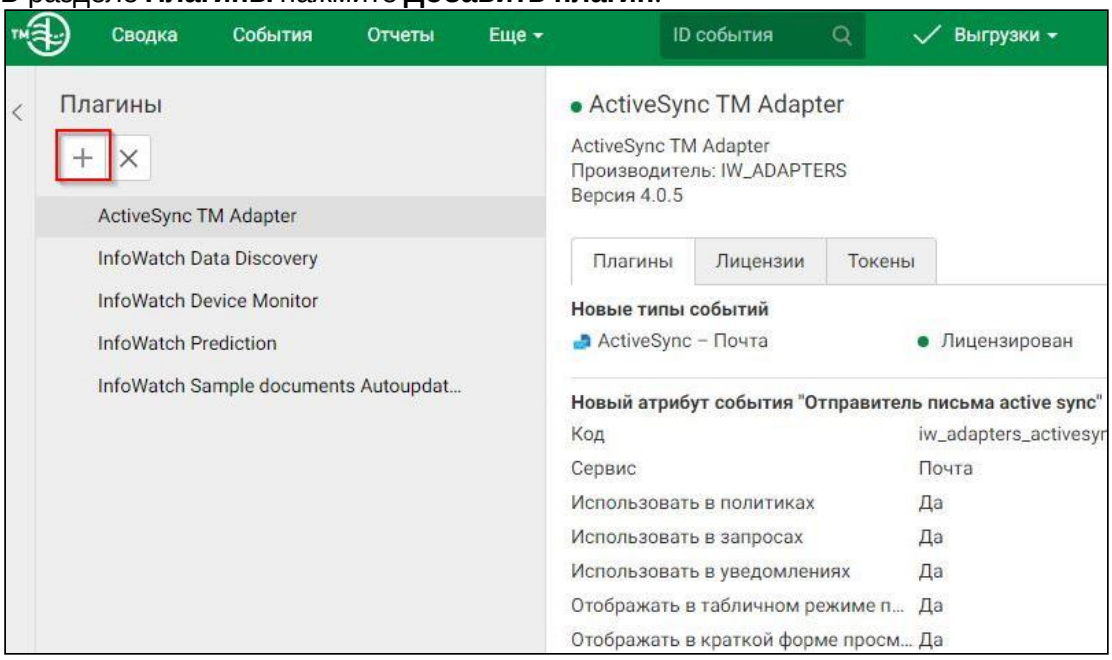
После установки Webfilter:

1. Установите плагин (см. "Установка плагина ActiveSync для InfoWatch Traffic Monitor").
2. Настройте Webfilter (см. "Настройка InfoWatch ActiveSync Adapter").

6 Установка плагина ActiveSync 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.

7 Настройка InfoWatch ActiveSync Adapter

Для корректной работы произведите первичную настройку Webfilter (см. "Настройка после установки и запуск Webfilter") и настройте маршрутизацию (см. "Настройка маршрутизации").

Настройка модуля Webfilter производится на сервере, на котором он установлен.

7.1 Настройка после установки и запуск Webfilter

Важно!

Если модуль Webfilter уже запущен, то для применения новых настроек требуется перезапустить модуль.

7.1.1 Добавление сертификата и ключа

Чтобы Webfilter мог работать с TLS-соединениями, требуются файлы сертификата и закрытого ключа сервера Exchange.

Чтобы добавить сертификат и ключ в Webfilter:

1. Экспортируйте файл сертификата и файл закрытого ключа из сервера Exchange.
2. Поместите файл сертификата в формате PEM и файл закрытого ключа в формате PEM в директорию: `/opt/webfilter/server/etc/trafficserver`
3. В файле `/opt/webfilter/server/etc/trafficserver/records.config` укажите следующие настройки, где:
   - `cert.pem` – имя файла с сертификатом Exchange;
   - `key.pem` – имя файла с закрытым ключом Exchange.

```
CONFIG proxy.config.ssl.webfilter.server.certificate.enabled INT 1
CONFIG proxy.config.ssl.webfilter.Cert.filename STRING cert.pem
CONFIG proxy.config.ssl.webfilter.Cert.privkey STRING key.pem
```

Примечание:

В случае если передается HTTP-трафик Exchange, который зашифровывается в рамках инфраструктуры:

- `cert.pem` – имя файла с сертификатом, который позволяет установить TLS-соединение с другими хостами в инфраструктуре;
- `key.pem` – имя файла с закрытым ключом сервера Webfilter.

7.1.2 Настройка для non-TLS / HTTP соединений

Если не требуется работа с TLS-соединениями, в файле `/opt/webfilter/server/etc/trafficserver/records.config` замените строку

```
CONFIG proxy.config.http.server_ports STRING 8080:tr-in:ssl
```

на строку:

```
CONFIG proxy.config.http.server_ports STRING 8080:tr-in
```

7.1.3 Подключение к Traffic Monitor

Укажите в файле `/opt/webfilter/server/webfilter/config/webfilter.conf` настройки для подключения к Traffic Monitor:

```
content_dispatch.tma.destination = 10.70.229.153:9101
content_dispatch.tma.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w
#content_dispatch.tma.server_fqdn = localhost
```

Параметры:

- **`content_dispatch.tma.destination`** – адрес сервера Traffic Monitor. Формат: **`IP:PORT`**
  - **`IP`** – IP-адрес;
  - **`PORT`** – порт сервиса xapi для получения событий, по умолчанию: **`9101`**.
- **`content_dispatch.tma.credentials`** – данные для авторизации. Формат: **`COMPANY:TOKEN`**
  - **`COMPANY`** – значение ключа **`common_name`** из файла лицензии для модуля InfoWatch ActiveSync Adapter. По умолчанию в лицензии указано: **`IW_ADAPTERS`**;
  - **`TOKEN`** – токен плагина ActiveSync Adapter. Вы можете получить токен в Консоли управления Traffic Monitor: *Управление → Плагины → ActiveSync TM Adapter → Токены*.
- **`content_dispatch.tma.server_fqdn`** – полное доменное имя сервера, на котором установлен Webfilter. Параметр не является обязательным. По умолчанию параметр не используется и оформлен как комментарий.

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.

Если инстансов Traffic Monitor несколько, укажите настройки для подключения в следующем формате:

```
content_dispatch.tma.<TYPE>.<NAME>.destination = IP:PORT
content_dispatch.tma.<TYPE>.<NAME>.credentials = COMPANY:TOKEN
#content_dispatch.tma.<TYPE>.<NAME>.server_fqdn = localhost
```

- **`<TYPE>`** – тип инстанса. Может иметь значение `master` или `slave`;

- **<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.

> **Примечание:**
>
> Если в настройках подключения к инстансу Traffic Monitor отсутствуют составляющие `<TYPE>` и `<NAME>`, то их значения равны `<TYPE> == master` и `<NAME> == default`.
> В файле конфигурации можно указать настройки, не содержащие составляющие `<TYPE>` и `<NAME>`, только для одного инстанса Traffic Monitor.

Пример:

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

Для этого в файле `/opt/webfilter/server/webfilter/config/webfilter.conf` укажите следующие настройки:

```
content_dispatch.tma.master.tm1.destination = 10.70.229.153:9101
content_dispatch.tma.master.tm1.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w1
content_dispatch.tma.master.tm1.server_fqdn = localhost

content_dispatch.tma.master.tm2.destination = 10.70.229.154:9101
content_dispatch.tma.master.tm2.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w2
content_dispatch.tma.master.tm2.server_fqdn = localhost

content_dispatch.tma.master.tm3.destination = 10.70.229.155:9101
content_dispatch.tma.master.tm3.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w3
content_dispatch.tma.master.tm3.server_fqdn = localhost

content_dispatch.tma.slave.tm4.destination = 10.70.229.156:9101
content_dispatch.tma.slave.tm4.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w4
content_dispatch.tma.slave.tm4.server_fqdn = localhost

content_dispatch.tma.slave.tm5.destination = 10.70.229.157:9101
content_dispatch.tma.slave.tm5.credentials = IW_ADAPTERS:i2swkk1q5wq01k5ruf4w5
content_dispatch.tma.slave.tm5.server_fqdn = localhost
```

7.1.4 Очередь отправки событий

Если все инстансы Traffic Monitor, и с типом `master`, и с типом `slave`, не доступны, 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/webfilter/server/webfilter/config/webfilter.conf` укажите следующие параметры:

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

```
content_dispatch.tma.storage_path=/opt/webfilter/server/webfilter/custom_queue_dir
```

Директория по умолчанию: `/opt/webfilter/server/webfilter/transport/queue`.

- Количество потоков, обслуживающих очередь отправки событий:

```
content_dispatch.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:

```
content_dispatch.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.

7.1.5 Направления перехвата

Файл `/opt/webfilter/server/webfilter/config/webfilter.scl` по умолчанию содержит следующие настройки:

```
// Comment line

Pass(): RequestContentDispatch() ;

Pass(): ResponseContentDispatch() ;
```

- `Pass(): RequestContentDispatch() ;` – перехват данных, которые передаются с устройства сотрудника на почтовый сервер (например, отправка писем);
- `Pass(): ResponseContentDispatch() ;` – перехват данных, которые передаются с почтового сервера на устройство сотрудника (например: чтение писем, скачивание файлов и синхронизация).

Чтобы отключить перехват, оформите строку как комментарий или удалите строку.

Например, чтобы перехватывать только данные, которые передаются с почтового сервера на устройство сотрудника:

```
// Comment line

// Pass(): RequestContentDispatch() ;

Pass(): ResponseContentDispatch() ;
```

7.1.6 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/webfilter/server/webfilter/config` 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/webfilter/server/webfilter/config/webfilter.conf`:
   - Черный список:

     ```
     content_dispatch_accounts.blacklist=list.txt
     ```

   - Белый список:

     ```
     content_dispatch_accounts.whitelist=list.txt
     ```

7.1.7 Управление модулем Webfilter

- Чтобы запустить Webfilter, выполните команду: `systemctl start webfilter-server`

- Чтобы получить информацию о состоянии Webfilter, выполните команду: `systemctl status webfilter-server`
- Чтобы остановить Webfilter, выполните команду: `systemctl stop webfilter-server`

7.2 Настройка маршрутизации

Webfilter работает в качестве прозрачного прокси-сервера.

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

На хосте Webfilter необходимо настроить маршрутизацию для обеспечения передачи трафика. В случае, если имеется один интерфейс:

1. Настройте `iptables`:

   ```
   iptables -t mangle -A PREROUTING -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x1/0x1
   iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j TPROXY --on-port 8080 --on-ip
   0.0.0.0 --tproxy-mark 0x1/0x1
   ```

   Если через порт 80 может проходить non-TLS / HTTP трафик:

   ```
   iptables -t mangle -A PREROUTING -p tcp -m tcp --sport 80 -j MARK --set-xmark 0x1/0x1
   iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 80 -j TPROXY --on-port 8080 --on-ip
   0.0.0.0 --tproxy-mark 0x1/0x1
   ```

2. Настройте правила маршрутизации:

   ```
   ip rule add fwmark 1/1 table 1
   ip route add local 0.0.0.0/0 dev lo table 1
   ```

3. Остановите сервисы `firewalld` и `NetworkManager`:

   ```
   systemctl stop firewalld
   systemctl disable firewalld
   systemctl stop NetworkManager
   systemctl disable NetworkManager
   ```

7.2.1 Автоматическое восстановление настроек

Настройки маршрутизации на сервере будут сброшены, если произошла перезагрузка сервера.

Чтобы настройки восстанавливались при каждом запуске сервера:

1. Создайте скрипт для командной строки, например, `/root/example.sh`:

   ```
   touch /root/example.sh
   ```

2. Укажите команды для настройки маршрутизации в файле `/root/example.sh`. Пример содержания файла:

```
#!/bin/bash
iptables -t mangle -A PREROUTING -p tcp -m tcp --sport 443 -j MARK --set-xmark 0x1/0x1
iptables -t mangle -A PREROUTING -p tcp -m tcp --dport 443 -j TPROXY --on-port 8080 --on-ip
0.0.0.0 --tproxy-mark 0x1/0x1

ip rule add fwmark 1/1 table 1
ip route add local 0.0.0.0/0 dev lo table 1
```

3. Убедитесь, что root является владельцем файла и что файл является исполняемым:

   a. `chown root:root /root/example.sh`

   b. `chmod 750 /root/example.sh`

4. Создайте файл сервиса `example-service`:

```
touch /etc/systemd/system/example-service.service
```

5. Укажите настройки сервиса в файле `/etc/systemd/system/example-service.service`. Пример содержания файла:

```
[Unit]
Description=Example Service
After=network.target
[Service]
Type=oneshot
User=root
ExecStart=/root/example.sh
[Install]
WantedBy=multi-user.target
```

6. Обновите конфигурации `systemd`:

```
systemctl daemon-reload
```

7. Запустите сервис `example-service` и проверьте его статус:

   a. `systemctl start example-service`

   b. `systemctl status example-service`

8. Включите автоматический запуск сервиса `example-service`:

```
systemctl enable example-service
```

В результате скрипт `/root/example.sh` будет выполняться при каждом запуске сервера.

7.2.2 Настройка Webfilter для работы с несколькими почтовыми серверами

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

Чтобы настроить работу Webfilter с несколькими почтовыми серверами:

1. В файле `/opt/webfilter/server/etc/trafficserver/records.config` укажите настройку (по умолчанию строка оформлена как комментарий):

   ```
   CONFIG proxy.config.hostdb.origin_servers_enabled INT 1
   ```

2. В файле `/opt/webfilter/server/etc/trafficserver/origins.config` укажите адреса почтовых серверов. Каждый адрес должен быть указан на отдельной строке. Формат: IP-адрес или FQDN. Пример:

   ```
   10.60.70.26
   10.60.71.32
   host.example.com
   ```

3. Перезапустите модуль `webfilter-server`.

8 Диагностика InfoWatch ActiveSync Adapter

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

8.1 Лог-файлы

Лог-файлы расположены в директории `/opt/webfilter/server/var/log/trafficserver`.

Чтобы получать подробную отладочную информацию:

1. Откройте на редактирование файл `/opt/webfilter/server/etc/trafficserver/records.config`.
2. В секции `Debugging` укажите:

```
CONFIG proxy.config.diags.debug.enabled INT 1
```

3. Настройте ротацию лог-файлов в секции `Logging Config`:
   a. Укажите настройку:

   ```
   CONFIG proxy.config.log.rolling_enabled INT 3
   ```

   Ротация файлов будет проводиться, если истек временной интервал `proxy.config.log.rolling_interval_sec` или если размер файла превышает `proxy.config.log.rolling_size_mb`.
   b. Укажите временной интервал для ротации в секундах. Например, чтобы ротация проводилась раз в день:

   ```
   CONFIG proxy.config.log.rolling_interval_sec INT 86400
   ```

   c. Укажите размер файла в МБ, который необходим для ротации:

   ```
   CONFIG proxy.config.log.rolling_size_mb INT 10
   ```

4. Сохраните изменения.
5. Перезапустите модуль `webfilter-server`.

8.2 Дампы трафика

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

Чтобы настроить создание дампов трафика:

1. Откройте на редактирование файл `/opt/webfilter/server/webfilter/config/webfilter.conf`.
2. Укажите настройку, чтобы включить создание дампов:

```
content_dispatch.tma.content_logging_enabled=1
```

3. Если требуется создавать дампы только для определенного пользователя Exchange, добавьте настройку:

   ```
   content_dispatch.tma.logging_contact=user@example.com
   ```

   Здесь `user@example.com` – логин пользователя Exchange.

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

4. Сохраните изменения.
5. Перезапустите модуль `webfilter-server`.

Файлы сохраняются в директории `/opt/webfilter/server/var/log/trafficserver/contents`. Каждый файл содержит информацию об одной транзакции. Имя файла содержит дату, время перехвата и логин пользователя.

9 Удаление InfoWatch ActiveSync Adapter

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

Удалите Webfilter с помощью менеджера пакетов YUM или DNF:

- YUM:
  `yum erase webiflter-server`
- DNF:
  `dnf erase webfilter-server`