



Агент Solar webProxy

Версия 4.1

Руководство по установке, обновлению и удалению

Москва, 2024

Содержание

Перечень терминов и сокращений	4
1. Введение	5
1.1. Область применения	5
1.2. Краткое описание возможностей	5
1.3. Уровень подготовки пользователя	5
2. Требования к аппаратному и программному обеспечению	6
2.1. Требования к аппаратному обеспечению	6
2.2. Требования к программному обеспечению	6
3. Взаимодействие Агента с прокси-сервером	7
3.1. Схема работы Агента	7
4. Установка, обновление и удаление	8
4.1. Установка через командную строку	8
4.2. Установка через GPO	10
4.3. Удаление и обновление	11
5. Журналирование работы Агента	13
6. Действия в аварийных ситуациях	14
6.1. Действия в случае обнаружения аварийной ситуации	14
6.1.1. Не работает Агент	14
6.1.2. Нет связи с Агентом и прокси-сервером	14
6.1.3. Не устанавливается Агент	14
6.2. Получение технической поддержки	14
Лист контроля версий	15

Список иллюстраций

3.1. Схема работы Агента	7
--------------------------------	---

Перечень терминов и сокращений

APM	Автоматизированное рабочее место
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
SSL	Secure Sockets Layer – цифровой сертификат, удостоверяющий подлинность веб-сайта и позволяющий использовать зашифрованное соединение.

1. Введение

1.1. Область применения

Агент Solar webProxy (далее – Агент) представляет собой программный компонент для установки на рабочие станции пользователей в информационной системе. Агент предназначен для принудительного перенаправления веб-трафика браузеров и приложений с рабочих станций пользователей на прокси-серверы Solar webProxy с целью обеспечения доступа к внешним ресурсам.

1.2. Краткое описание возможностей

Агент обеспечивает удаленный контроль перенаправления веб-трафика пользователя на рабочей станции под управлением ОС Windows и связь с прокси-сервером Solar webProxy.

Агент обеспечивает следующие функциональные возможности:

- Перенаправление через прокси-сервер веб-трафика браузеров и приложений с целью выполнения проверки фильтрации приложений клиента, не поддерживающих настройки прокси.
- Перехват веб-трафика на конечной станции и обработка соединений (без SSL) с заданными настройками прокси-сервера.
- Передача с рабочей станции на прокси-сервер данных для аутентификации пользователя с поддержкой NTLM и Kerberos-аутентификации.
- Журналирование важных и критических событий.
- Взаимодействие с несколькими прокси-серверами.
- Активация режима **BYPASS** при недоступности основного или резервного прокси-сервера. Режим обеспечивает трансляцию веб-трафика без блокировки доступа к внешним ресурсам пользователя.

1.3. Уровень подготовки пользователя

Для установки, настройки и применения Агента требуются знания и навыки администрирования ОС Windows, навыки администрирования Solar webProxy и умение реализовывать с его помощью корпоративную политику безопасности в части, относящейся к информационному обмену.

2. Требования к аппаратному и программному обеспечению

2.1. Требования к аппаратному обеспечению

Для установки и эффективной работы Агента рекомендуется следующая конфигурация рабочей станции:

- CPU – не менее двух ядер,
- ОЗУ – 2 ГБ,
- свободное место на системном разделе жесткого диска – 100 МБ.

2.2. Требования к программному обеспечению

Агент Solar webProху функционирует под управлением ОС:

- Windows 7,
- Windows 8,
- Windows 8.1,
- Windows 10,
- Windows 11,
- Windows Server 2008 R2,
- Windows Server 2012,
- Windows Server 2016.

3. Взаимодействие Агента с прокси-сервером

3.1. Схема работы Агента

Агент, установленный на рабочую станцию пользователя, соединяется с прокси-сервером (по адресу, указанному при установке, формата **<hostname:port>**). От прокси-сервера Агент получает свои параметры настроек (конфигурацию) и политику, в соответствии с которой во время работы он будет перенаправлять веб-трафик на прокси-сервер. Схема работы Агента с прокси-сервером показана на [Рис.3.1](#).

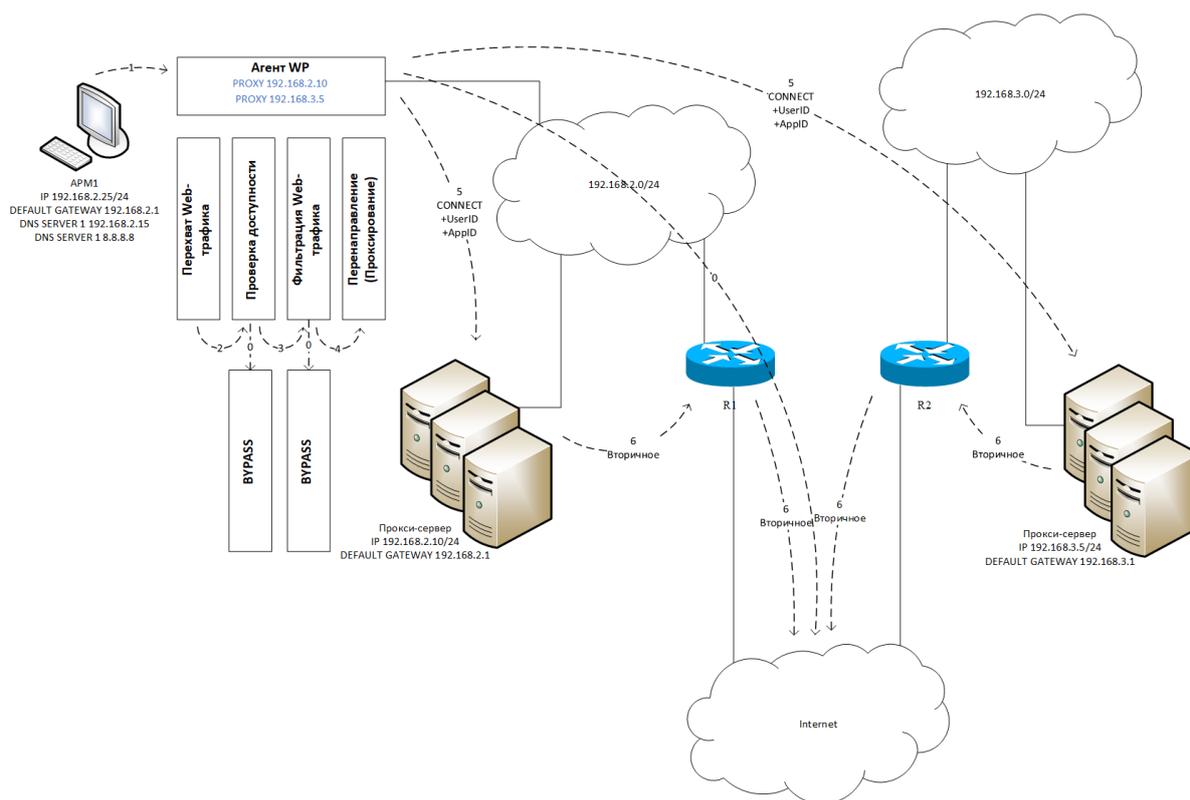


Рис. 3.1. Схема работы Агента

Агент работает в следующих режимах:

- Перенаправление веб-трафика через основной прокси-сервер.
- Перенаправление веб-трафика через резервный прокси-сервер, если основной прокси-сервер недоступен.

Примечание

Если основной и резервный прокси-серверы находятся на разных доменах, необходимо установить доверительные отношения между ними.

- Режим **bypass**. Агент перенаправляет веб-трафик через стандартный шлюз в обход основного и резервного серверов, если они недоступны.

4. Установка, обновление и удаление

Перед установкой, обновлением и удалением Агента необходимо авторизоваться под учетной записью с ролью администратора.

4.1. Установка через командную строку

Для установки Агента выполните следующие действия:

1. Создайте файл **proxy-config.json** со следующими полями:

- **ProxyList** – полное имя прокси-сервера в формате **<hostname:port>**.

Примечание

*В поле **ProxyList** можно указать несколько прокси-серверов.*

- **CertUrl** – URL-адрес для получения сертификата от сервера Solar webProxy.
- **LogLevel** – способ фильтрации событий в журнале. Значение атрибута:
 - **TRACE** – отслеживание активности Агента;
 - **DEBUG** – отслеживание состояния системных переменных и регистров, которые относятся к драйверу перехвата трафика;
 - **INFO** – журналирование основных событий;
 - **CRITICAL** – отображение критических ошибок (например, недоступность одного из прокси-серверов).
- **RuleResolveSecTimeout** – интервал проверки доступных правил. Допустимые значения от 30 с до 600 с;
- **ProxyResolveSecTimeout** – интервал проверки доступности прокси-сервера. Допустимые значения от 30 с до 600 с.
- **Rules** – тип правила. Допустимые значения атрибута:
 - **Redirect** – список правил, по которым соединение будет перенаправляться на прокси-сервер. Если соединение не подходит ни под одно правило, перенаправление веб-трафика не происходит;
 - **Ignore** – список правил, по которым соединение не будет перенаправляться на прокси-сервер (более приоритетно, чем **Redirect**).

Содержание атрибута поля **Rules**:

- **ProcessName** – имя процесса, соединение которого подлежит перенаправлению. Полный путь не требуется. Примеры: "chrome.exe", "firefox.exe".

- **Ip** (IP-адрес ресурса или диапазон внутренних IP-адресов назначения (10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, 192.168.0.0 - 192.168.255.255)) или **Host** (URL-адрес ресурса) – можно добавить только один из параметров.
- **Port** – порт или диапазон портов.

Пример заполнения файла **proxy-config.json**:

Примечание

При обновлении Агента Solar webProxy обратите внимание, что значение в поле **Ip** указывается в кавычках, а не квадратных скобках. При заполнении файла **proxy-config.json** убедитесь, что его содержание соответствует примеру.

```
{
  "ProxyList": [ "wp1.solar.local:2270" "wp2.solar.local:2270"],
  "CertUrl": "http://mitm.it:2281/cert/download/crt",
  "LogLevel": "TRACE",
  "RuleResolveSecTimeout": 300,
  "ProxyResolveSecTimeout": 60,
  "Rules": {
    "Ignore": [
      {
        "ProcessName": "",
        "Ip": "",
        "Host": "",
        "Port": "80"
      }
    ],
    "Redirect": [
      {
        "ProcessName": "chrome.exe",
        "Ip": "",
        "Host": "yandex.ru",
        "Port": "443"
      },
      {
        "ProcessName": "Firefox.exe",
        "Ip": "192.168.0.10",
        "Host": "ya.ru",
        "Port": "443-444"
      },
      {
        "ProcessName": "",
        "Ip": "192.168.0.10-192.168.0.20",
        "Host": "",
        "Port": "80"
      }
    ]
  }
}
```

2. В CLI выполните команду:

```
msiexec /i "C:\Users\%USERPROFILE%\Desktop\swp-proxy.msi" /L*V  
"C:\Users\%USERPROFILE%\Desktop\install.log"  
PROXYCONFIGPATH="C:\Users\%USERPROFILE%\Desktop\proxy-config.json"
```

где PROXYCONFIGPATH – путь до файла **proxy-config.json**, а %USERPROFILE% – имя учетной записи, например, administrator.

После выполнения команды файл **install.log** будет находиться в каталоге **C:\Users\%USERPROFILE%\Desktop\install.log**.

- Успешность установки отображается в файле **install.log** и на Рабочем столе пользователя, от имени которого был установлен Агент. Также в Диспетчере задач отображается фоновый процесс *swp-proxy*.

4.2. Установка через GPO

Групповая политика создается средством **Group Policy Management**.

Запуск **Group Policy Management** выполняется командой **gpmc.msc** из командной строки, которая открывается с помощью клавиш **Win+R**.

Окно **Group Policy Management** разделено на две части, в левой отображен список доменов.

Для создания и применения групповой политики:

- Выберите домен в списке и в контекстном меню домена пункт **Create a GPO in this domain, and Link it here**.
- В открывшемся окне **New GPO** задайте имя объекта групповой политики и нажмите **OK**.
- В контекстном меню созданной группы выберите пункт **Edit**.
- В левой части открывшегося окна **Group Policy Management Editor** выберите раздел **Software installation (Computer Configuration > Policies > Software Settings)**.
- В контекстном меню раздела **Software installation** выберите пункт **New > Package**.
- В открывшемся окне **Open** выберите дистрибутив Агента и нажмите **Open**.

Внимание!

Каталог, в котором расположен дистрибутив, должен быть доступен по сети.

- В окне **Deploy Software** установите переключатель метода установки в состояние **Advanced**. Этот метод обеспечивает возможность применения пакета трансформации. Нажмите кнопку **OK**.
- В контекстном меню добавленного дистрибутива выберите пункт **Properties**, перейдите на вкладку **Modifications** и нажмите кнопку **Add**. Это позволит применить файл трансформации, подготовленный ранее.

-
9. В окне **Open** выберите нужный пакет трансформации (файл с расширением **.mst**) и нажмите кнопку **Open**.
 10. В поле **Modifications** появится выбранный пакет трансформации. Нажмите кнопку **OK**.
 11. Закройте окно **Group Policy Management Editor**.
 12. В правой части окна **Group Policy Management** очистите поле **Security Filtering**, а затем нажмите кнопку **Add** и добавьте группу безопасности, созданную ранее.

В результате выполненных действий Агент будет установлен на рабочих станциях при следующей загрузке ОС Windows.

После установки Агента на рабочие станции следует удалить созданную ранее политику GPO (чтобы в дальнейшем со стороны GPO не было попыток установить/удалить Агент на рабочих станциях).

4.3. Удаление и обновление

Удалить Агент можно через Мастер установок.

Примечание

В разных ОС удаление программ может выполняться по-разному.

Чтобы удалить Агент в ОС Windows 10:

1. Откройте окно **Параметры > Приложения**.
2. В окне выделите **Solar Web Proxy Agent** и выберите действие **Удалить**.
3. Подтвердите удаление.

Также Агент можно удалить через групповые политики. Для этого:

1. Откройте **Пуск > Администрирование > Active Directory Users and Computers**.
2. В дереве консоли нажмите правой кнопкой мыши на домен и выберите **Properties**.
3. Перейдите на вкладку **Group Policy**, выберите установочный файл Агента, затем нажмите **Edit**.
4. Разверните контейнер **Software Settings**, в котором находится установочный файл Агента.
5. Выберите контейнер Агента.
6. В правой области окна **Group Policy** правой кнопкой мыши нажмите на Агента и выберите **All Tasks > Remove**.

В процессе удаления Агента система очищается от всех файлов, каталогов и настроек, которые были созданы в процессе его установки.

Для обновления Агента удалите предыдущую версию программы. После перезагрузки станции установите новую версию Агента.

5. Журналирование работы Агента

Журналирование работы Агента необходимо для своевременного реагирования на ошибки и нарушения функционирования, а также для эффективного принятия решения по исправлению ошибок техническими службами поддержки.

В папку **Program Files (x86) > Solar > Web Proxy Agent > Logs** записываются журнальные файлы сессий соединений Агента на рабочих станциях.

Для настройки журнала используется переменная уровня журналирования **LogLevel**, значение которой необходимо задавать в файле **proxy-config.json**.

6. Действия в аварийных ситуациях

6.1. Действия в случае обнаружения аварийной ситуации

6.1.1. Не работает Агент

В некоторых ситуациях Агент может не запускаться на рабочей станции пользователя. При возникновении ошибки:

1. Проверьте состояние Агента в **Журнале событий**. Для этого откройте меню **Пуск**, в командной строке введите **eventvwr** и нажмите клавишу ВВОД, чтобы открыть **Просмотр событий**.
2. Если Агент не работает, необходимо через инструмент **SysInternals** и утилиты **ProcDump** собрать пакет данных. От имени администратора в CLI выполните команды:

```
# \\live.sysinternals.com\tools\coreinfo
```

```
# \\live.sysinternals.com\tools\procdump.exe
```

```
# \\live.sysinternals.com\tools\procdump -ma -mk -h web-proxy.exe
```

Полученные данные вместе с файлом **proxy-config.json** необходимо передать специалистам компании [«Ростелеком-Солар»](#).

6.1.2. Нет связи с Агентом и прокси-сервером

После успешной настройки Агента не происходит соединение с прокси-сервером (основным или резервным), или ресурсы открываются с ошибками. Необходимо собрать данные о событиях Агента с помощью программного обеспечения **Wireshark** и утилиты **tcpdump**. Собранные данные вместе с файлом **proxy-config.json** необходимо передать в компанию [«Ростелеком-Солар»](#).

6.1.3. Не устанавливается Агент

При установке могут возникнуть ошибки. В этом случае передайте файл **install.log** в компанию [«Ростелеком-Солар»](#).

6.2. Получение технической поддержки

Для получения консультации по техническим вопросам можно обратиться по адресу support@rt-solar.ru.

С условиями поддержки можно ознакомиться на сайте компании [«Ростелеком-Солар»](#) (по адресу: <http://solar-rt.ru/support/>). При оформлении запроса укажите номер контракта на техническую поддержку, опишите проблему, укажите свое полное имя, адрес электронной почты и номер телефона.

Лист контроля версий

04/06/2024-16:09