Ростелеком
Солар

Программный комплекс Solar webProxy

Руководство по установке и настройке

Москва, 2019

Содержание

Список иллюстраций

Список таблиц

Перечень сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
ИБ	Информационная безопасность
КА	Контентный анализ
Кластер	Совокупность серверов Solar webProxy, соединённых между собой управляющими связями.
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface – интерфейс командной строки
CRL	Certificate Revocation List – список отозванных сертификатов
GUI	Graphical User Interface – графический интерфейс пользователя
FQDN	Fully Qualified Domain Name – полное имя домена (имя домена, не имеющее неоднозначностей в определении)
MIME	Multipurpose Internet Mail Extension – многоцелевое расширение интернет-почты
MITM	Man-In-The-Middle – атака «человек посередине», при которой злоумышленник тайно ретранслирует и при необходимости модифицирует данные между двумя сторонами
RFC	Request for Comments – спецификации и стандарты, применяемые в интернете
SMTP	Simple Mail Transfer Protocol – простой протокол передачи почты

1. Введение

1.1. Область применения

Программный комплекс Solar webProxy (далее – Solar webProxy) представляет собой систему анализа веб-трафика, передаваемого по протоколам HTTP, HTTPS и FTP over HTTP, с целью идентификации событий, которые могут свидетельствовать о нарушении правил информационного обмена. Для этого весь веб-трафик должен проходить через Solar webProxy.

1.2. Краткое описание возможностей

Solar webProxy осуществляет контроль проходящего веб-трафика с целью предотвращения доступа к запрещённым ресурсам и утечки важной информации. Solar webProxy обеспечивает следующие функциональные возможности:

- Анализ веб-трафика по различным критериям. Объектом анализа является информация, передаваемая в запросах и ответах протоколов HTTP, HTTPS и FTP over HTTP.
- Выполнение заранее определенных действий над передаваемой информацией, соответствующей заданным критериям. Примерами действий могут быть блокировка доступа, явное разрешение доступа и разрешение доступа после подтверждения пользователем.
- Автоматизированное помещение в архив данных о передаваемой информации, отвечающей заданным критериям.
- Формирование отчетов о действиях пользователей в сети Интернет по различным критериям, таким как адрес сайта, время доставки информации, объем доставляемой информации.
- Предоставление администраторам безопасности, прошедшим процедуру аутентификации, возможности просмотра информации, собранной в процессе мониторинга.
- Предоставление администраторам безопасности, прошедшим процедуру аутентификации, возможности настройки функций безопасности.

1.3. Уровень подготовки системного администратора

Квалификация системного администратора Solar webProxy должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех ее компонентов.

К задачам системного администратора Solar webProxy относятся:

- установка и настройка компонентов Solar webProxy;
- мониторинг функционирования процессов системы;
- реагирование на служебные уведомления системы.

Системный администратор Solar webProxy должен:

- ориентироваться в особенностях работы Solar webProxy;

- понимать работу сетевых протоколов;
- обладать знаниями в области безопасности ОС класса UNIX.

В своей работе системные администраторы Solar webProxy должны использовать документацию по обслуживанию Solar webProxy и документацию по ОС Linux.

1.4. Перечень эксплуатационной документации для ознакомления

Системный администратор Solar webProxy должен ознакомиться со следующими эксплуатационными документами:

- *Руководство по установке и настройке* (настоящий документ).
- *Руководство системного администратора*.
- *Руководство администратора безопасности*.

2. Назначение и возможности Solar webProxy

Solar webProxy предназначен для защиты корпоративных локальных вычислительных сетей от рисков, связанных с использованием веб-ресурсов. Защита обеспечивается комплексом мер, включая фильтрацию содержимого информационного обмена, осуществляемого по протоколам HTTP HTTPS и FTP over HTTP (через HTTP-прокси для HTTP- и FTP-трафика), авторизацию пользователей и протоколирование их действий.

3. Требования к программному и аппаратному обеспечению

3.1. Требования к АРМ системного администратора

3.1.1. Требования к аппаратному обеспечению

АРМ системного администратора Solar webProxy должно быть оборудовано персональным компьютером. Особых требований к аппаратному обеспечению нет. Рекомендуются следующие характеристики персонального компьютера:

- процессор P-IV с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жёсткого диска не менее 20 ГБ.

3.1.2. Требования к программному обеспечению

В состав программного обеспечения АРМ системного администратора Solar webProxy должен входить браузер. Рекомендуемые браузеры:

- Mozilla Firefox
- Google Chrome

Работа с управляющим интерфейсом Solar webProxy возможна в других браузерах, но в таком случае полноценная работоспособность Solar webProxy не гарантируется.

Для корректной работы Solar webProxy настоятельно рекомендуется разрешить выполнение javascript и сохранение cookies (настройка по умолчанию).

Внимание!

Если вручную увеличить размер шрифта в браузере, дизайн интерфейса Solar webProxy будет нарушен, и интерфейс станет непригодным к использованию.

3.2. Требования к серверу

3.2.1. Требования к аппаратному обеспечению

Рекомендуемые характеристики аппаратного обеспечения сервера для установки Solar webProxy, рассчитанного на 100 пользователей:

- 4 процессора (vCPU) P-IV с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 16 ГБ;
- жесткий диск не менее 60 ГБ (зависит от интенсивности использования и времени хранения журналов фильтра);
- сетевой интерфейс со скоростью передачи данных не ниже 1 Гбит/с.

Установка Solar webProxy требует наличия как минимум 2 ГБ свободного пространства на диске в каталоге **/opt**. Помимо этого, в процессе работы Solar webProxy потребуется свободное дисковое пространство под журнальные файлы в каталоге **/data** (использование дискового пространства можно оценить, исходя из того, что 1 ГБ журнальных файлов содержит примерно 1,5 млн. записей). Кроме того, в каталог **/data/spool/skvt/cache/** записывается спул-файл сервиса **skvt-cache**. Также необходимо выделить достаточное количество места под временные файлы в каталоге **/var/tmp**, учитывая то, что в зависимости от политики сервис **skvt-wizor** по умолчанию записывает в этот каталог файлы, которые пользователи загружают из интернета.

3.2.2. Требования к программному обеспечению

Solar webProxy функционирует под управлением ОС Linux CentOS/RHEL версии 7.6.

3.2.3. Требования к конфигурации ОС

Solar webProxy поддерживает работу только по протоколу IPv4. Использование ПО, работающего по протоколу IPv6, может приводить к ошибкам в работе Solar webProxy. Рекомендуется отключить использование IPv6 средствами операционной системы.

Кроме того, в процессе работы Solar webProxy необходим файл с региональными установками **ru_RU.UTF8** для корректного отображения пользовательского веб-интерфейса Solar webProxy.

В настройках ОС должны быть открыты сетевые порты, которые используются в работе Solar webProxy (см. **Табл.3.1**).

Табл. 3.1. Номера портов по умолчанию, которые используются в работе Solar webProxy

Номер порта	Сервис	Назначение
Взаимодействие сервисов внутри фильтра		
2230	skvt-auth-server	skvt-auth-server ожидает запросы на аутентификацию от skvt-wizor
2260	skvt-url-checker	Ожидает URL и в ответ выдает определенную категорию для этого URL
2261	skvt-url-checker	Проверяет принадлежность ресурсов (URL) к категориям, диагностический порт
2264	filestorage-ng	HTTP-порт файлового хранилища
2266	filestorage-ng	HTTPS-порт файлового хранилища
2269	abook-daemon	Выполняет синхронизацию с подчинёнными экземплярами Досье
7199, 7000, 9042	skvt-cassandra	Skvt-trafdaemon подключается к Cassandra для получения счетчиков трафика. Skvt-wizor подключается к Cassandra за подтверждениями доступа. При наличии нескольких экземпляров БД Cassandra они могут обмениваться данными также по любому порту
2228	skvt-cache	Принимает и обрабатывает HTTP/FTP/HTTPS-запросы от локального skvt-wizor
2225	skvt-ntlm-server	Принимает запросы от skvt-wizor для проведения NTLM-аутентификации через skvt-winbind
2226	skvt-kerberos-server	Выполняет аутентификацию пользователей через механизм Kerberos
2271	skvt-detector	Принимает запросы с фрагментами сообщений от skvt-wizor для определения их типов данных

Номер порта	Сервис	Назначение
2555	policy-daemon	Принимает запросы от skvt-play-server, выполняет генерациию политик
9998	smap-tikaserver	Принимает запросы от skvt-wizor
Взаимодействие между фильтром и мастер-хостом		
2299	Интерфейс между skvt-trafdaemon и skvt-cassandra	Организует обмен данными между skvt-trafdaemon и skvt-wizor
Взаимодействие с сервером отчетов (reporter)		
2244	skvt-reporter	Принимает запросы на вставку новых данных в хранилище от skvt-wizor, а также обрабатывает поисковые запросы от skvt-httpd-admin
Взаимодействие фильтра с внешними сервисами (номера внешних портов)		
25, 1025	Solar Dozor	Отправляет POST-запросы от skvt-wizor на запись данных в архив
1344	Антивирус	Принимает запросы на поиск вирусов по протоколу ICAP от skvt-wizor
2272	ICAP-сервер	ICAP-сервер принимает запросы от ICAP-прокси
25	SMTP-server	Принимает запросы на отправку почтовых сообщений от различных сервисов и утилит
445, 88, 389	Сервер Active Directory	Принимает запросы от утилиты net на добавление машины в домен, а также выполняет аутентификацию пользователей
993, 995, 110, 143	skvt-auth-server	Выполняет аутентификацию пользователей на IMAP/POP3-серверах
8080	skvt-url-checker	Принимает запросы от внешней базы категоризации Blue Coat
Веб-интерфейсы		
2280	skvt-httpd-admin	Принимает запросы от skvt-play-server
443	skvt-play-server	Принимает запросы от браузеров системных администраторов, обеспечивает управление Solar webProxy через веб-интерфейс. Порт сервера управления
2277	skvt-wizor	Вспомогательный сервисный порт
2270	skvt-wizor	Принимает HTTP/HTTPS-запросы от браузеров пользователей и обрабатывает их
2281	skvt-wizor	Порт вспомогательного веб-сервера, встроенного в skvt-wizor для реализации действия confirm в политике фильтрации
2443	skvt-wizor	SSL-порт
2444	skvt-wizor	Порт для прозрачного режима

3.2.4. Рекомендации по разбиению дисков в ОС при установке Solar webProxy

По умолчанию Solar webProxy для ОС Linux настроен на использование следующих логических разделов диска:

- **`/opt`** – раздел, в который производится установка компонентов Solar webProxy.
- **`/data`** – раздел для размещения репозитория Solar webProxy.

3.2.5. Рекомендации по размещению в сетевой инфраструктуре

Аппаратное и программное обеспечение сервера должно располагаться внутри защищённого периметра безопасности с целью исключения несанкционированного доступа.

3.2.6. Требования к паролю

Solar webProxy обеспечивает функцию стойкости паролей для доступа в систему. При создании пользователей система проверяет качество паролей, которое определяется следующими параметрами:

1. Минимально разрешённая длина пароля.
2. Известная и документированная максимальная длина пароля.
3. Количество различных символов в пароле.
4. Количество символов в пароле из следующих наборов:
   - заглавные буквы латиницы;
   - прописные буквы латиницы;
   - цифры;
   - служебные символы: ~ ! @ # $ % ^ & * ( ) + - = ` ' _ / \ | "

   Также служебным символом является пробел.

Пароль должен иметь длину не менее шести символов. Система не позволит создать пароль, если он не соответствует заданному в настройках уровню сложности – например, если он содержит более двух символов подряд из одного набора.

При создании пароля система рассчитывает уровень его сложности (от 0 до 10). По умолчанию уровень сложности пароля равен 0. Расчёт уровня сложности пароля выполняется на основании следующих условий:

1. Если длина пароля равна или больше минимальной, прибавляется 1.
2. Если длина пароля максимальная, прибавляется 2.
3. Если пароль содержит символы из двух наборов, прибавляется 1.
4. Если пароль содержит символы из трёх наборов, прибавляется 1.
5. Если пароль содержит символы из четырёх наборов, прибавляется 1.
6. Если пароль не содержит более двух символов из одного набора подряд, прибавляется 1.
7. Если пароль не содержит более одного символа из одного набора подряд, прибавляется 2.
8. Если количество разных символов больше минимальной длины пароля, прибавляется 1.
9. Если пароль выполняет условия пунктов 1, 5, 7, 8, прибавляется 1.

Если сумма условий больше 10, уровень сложности пароля считается равным 10.

В настройках по умолчанию минимальная длина пароля равна 6, максимальная длина пароля – 12, минимально допустимый уровень сложности пароля – 6. Таким образом, если уровень сложности меньше 6, система не позволит создать пароль.

Настройки по умолчанию можно изменить, отредактировав с помощью GUI следующие параметры конфигурационного файла **skvt-play-server.conf** (секция **skvt-play-server**):

- **password-minlen** – минимальная длина пароля.
- **password-maxlen** – максимальная длина пароля.
- **password-level** – минимально допустимый уровень сложности пароля.

4. Подготовка к установке Solar webProxy

Приведённые в этом разделе процедуры предварительной настройки должны быть выполнены на всех серверах Solar webProxy.

Внимание!

До завершения установки Solar webProxy следует строго придерживаться описанных ниже процедур и не устанавливать какие-либо пакеты или обновления системы. Дистрибутив Solar webProxy содержит все необходимые для работы пакеты, и в случае его установки на ОС с дополнительно установленными пакетами и/или обновлениями не гарантируется корректная работа Solar webProxy.

4.1. Настройка DNS

Необходимо проверить содержимое следующих файлов настройки DNS на всех узлах Solar webProxy:

- **/etc/hosts**
- **/etc/sysconfig/network**
- **/etc/nsswitch.conf**

Файл **/etc/hosts** должен содержать строки, состоящие из IP-адреса узла кластера, его полного (FQDN) и краткого (домен нижнего уровня) доменного имени, например, так:

```
10.199.21.148 proxymaster.company.local proxymaster
10.199.21.149 filter1.company.local filter1
10.199.21.147 filter2.company.local filter2
```

IP-адрес и записи доменного имени должны быть разделены символом табуляции. Строки, содержащие информацию о узлах кластера, должны совпадать на всех узлах кластера (можно заполнить файл **hosts** на одном узле и затем скопировать его на все остальные).

Внимание!

При указании доменного имени узла нельзя использовать символ подчёркивания.

Файл **/etc/sysconfig/network** должен содержать записи следующего вида:

```
NETWORKING=yes
NETWORKING_IPV6=no
HOSTNAME=proxymaster
```

Корректность задания доменных имен можно проверить с помощью следующих команд:

```
# hostname -f
```

```
# hostname -s
```

Вывод первой команды должен являться полным доменным именем узла, вывод второй команды – кратким.

Строка **HOSTNAME** должна содержать краткое доменное имя узла, совпадающее с аналогичной записью в файле **/etc/hosts** на этом узле.

Файл **/etc/nsswitch.conf** должен содержать следующую строку:

```
hosts:      files dns
```

Внимание!

Если этот пункт не выполнен, Solar webProxy не сможет нормально установиться и работать в распределенном режиме.

4.2. Настройка синхронизации времени

В отсутствие домен-контроллера или другого источника точного времени, рекомендуется синхронизировать узлы Solar Dozor между собой. Если этого не сделать, возникнут проблемы из-за разного времени в журналах и метках времени на данных; также возможны проблемы с функциями учёта трафика и с работой протоколов HTTPS, Kerberos.

Синхронизация времени в CentOS версии 7.6 настраивается с помощью утилиты **timedatectl**. Для настройки синхронизации времени необходимо на всех узлах Solar webProxy выполнить следующие действия:

1. Найти нужную временную зону, выполнив следующую команду:

   # timedatectl list-timezones

   Для удобства поиска можно воспользоваться сортировкой, например:

   # timedatectl list-timezones | grep Europe

2. Установить нужную временную зону, выполнив команду следующего вида:

   # timedatectl set-timezone <timezone>

   где **<timezone>** – значение, найденное в предыдущем шаге.

3. Удостовериться в правильности настройки временной зоны, выполнив следующую команду:

   # timedatectl

5. Установка Solar webProxy

Solar webProxy использует БД Clickhouse. Для корректного функционирования этой БД необходимо, чтобы процессор поддерживал набор инструкций **sse4_2**. Проверить наличие этой поддержки можно с помощью следующей команды:

```
# grep sse4_2 /proc/cpuinfo
```

Вывод команды должен быть непустым.

Для установки пакетных файлов Solar webProxy необходимо на каждом узле кластера выполнить следующие действия:

1. Скопировать файлы дистрибутива и скрипта-инсталлятора в локальный каталог (например, **/var/tmp/**).

2. Проверить корректность FQDN всех серверов, на которые планируется установить Solar webProxy (см. раздел 4.1).

3. Проверить наличие доступа к стандартным репозиториям CentOS, выполнив команду:

   ```
   # yum makecache
   ```

   Если доступ отсутствует, следует удалить эти репозитории, выполнив следующие команды:

   ```
   # mkdir /etc/yum.repos.d/old
   ```

   ```
   # mv /etc/yum.repos.d/*.repo /etc/yum.repos.d/old/
   ```

4. Отключить сервис **firewalld**, выполнив команды:

   ```
   # systemctl stop firewalld
   ```

   ```
   # systemctl disable firewalld
   ```

5. Установить пакеты **iptables-services**, выполнив команду:

   ```
   # yum -y install iptables-services
   ```

6. Запустить сервис **iptables**, выполнив команду:

   ```
   # systemctl enable iptables
   ```

7. Настроить сервис **iptables**, выполнив команды:

   ```
   iptables -F
   ```

   ```
   iptables -X
   ```

   ```
   iptables -t nat -F
   ```

   ```
   iptables -t nat -X
   ```

   ```
   iptables -t mangle -F
   ```

```
iptables -t mangle -X

iptables -P INPUT ACCEPT

iptables -P FORWARD ACCEPT

iptables -P OUTPUT ACCEPT

/sbin/service iptables save
```

8. Назначить скрипту-инсталлятору права на исполнение, выполнив команду:

   ```
   # chmod +x /var/tmp/wp-install.sh
   ```

9. Установить пакеты Solar webProxy, выполнив команды:

   ```
   # cd /var/tmp/

   # wp-install.sh wp-3.1.1-<build>.centos7.tar.gz
   ```

   где **<build>** – номер актуальной сборки дистрибутива.

10. После установки удалить все пакеты, связанные с пакетом **abrt**, выполнив следующую команду:

    ```
    # rpm -qa | grep abrt | xargs rpm -e
    ```

6. Первоначальная настройка Solar webProxy

6.1. Настройка кластера

После установки пакетов Solar webProxy на все узлы кластера необходимо выполнить следующие действия:

1. Выбрать среди узлов кластера сервер, который планируется использовать как master-узел, подключиться к нему по SSH и назначить ему управляющую роль, выполнив следующие команды:

   ```
   # /opt/dozor/bin/shell

   # set-role master main

   # dsctl boot
   ```

2. Зарегистрировать slave-узлы в кластере, выполнив на всех slave-узлах следующие команды:

   ```
   /opt/dozor/bin/shell

   reg-slave <master-host> [name]
   ```

   где **<master-host>** – FQDN master-узла (например, **proxymaster.company.local**), а **<name>** – имя регистрируемого узла. Если оно не указано, то по умолчанию будет использоваться сетевое имя узла, на котором запускается утилита **reg-slave**.

6.2. Первый вход в систему и загрузка лицензии

После настройки кластера необходимо сменить пароль по умолчанию для доступа к GUI. Для этого необходимо открыть браузер и перейти по адресу **https://<master-host>** либо **https://<master-ip>**, где **<master-host>** – полное доменное имя master-узла, например, **proxymaster.company.local**, а **<master-ip>** – IP-адрес master-узла, например, 10.199.21.148. В открывшемся окне авторизации ввести имя пользователя и пароль по умолчанию: **admin/admin**. После этого система потребует изменить пароль. Следует установить новый пароль требуемого уровня надёжности (см. раздел **3.2.6**), и авторизоваться с новым паролем.

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии (см. рисунок **Рис.6.1**). Для загрузки лицензии следует нажать кнопку **Смотреть лицензию**, и в появившемся окне **Лицензия** нажать кнопку **Загрузить лицензию**.

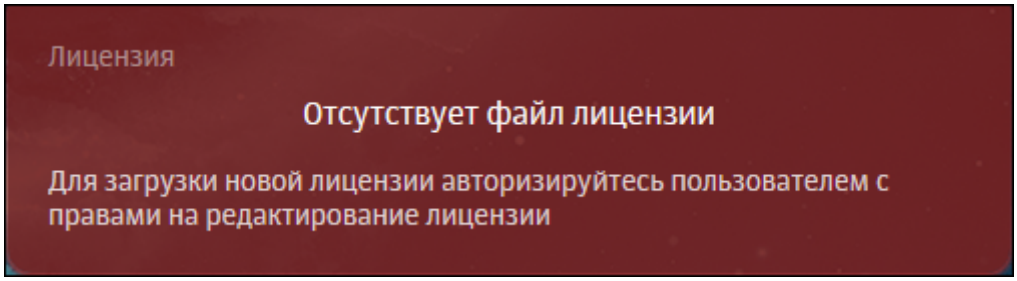

Рис. 6.1. Уведомление об отсутствии лицензии

В открывшемся окне проводника указать путь к файлу с лицензией, после чего нажать кнопку **Открыть** (**Open**) и дождаться загрузки лицензии. При этом она автоматически сохранится в файле с именем **license.xml**.

Для просмотра сведений о лицензии Solar webProxy следует выбрать пункт главного меню **Лицензия**.

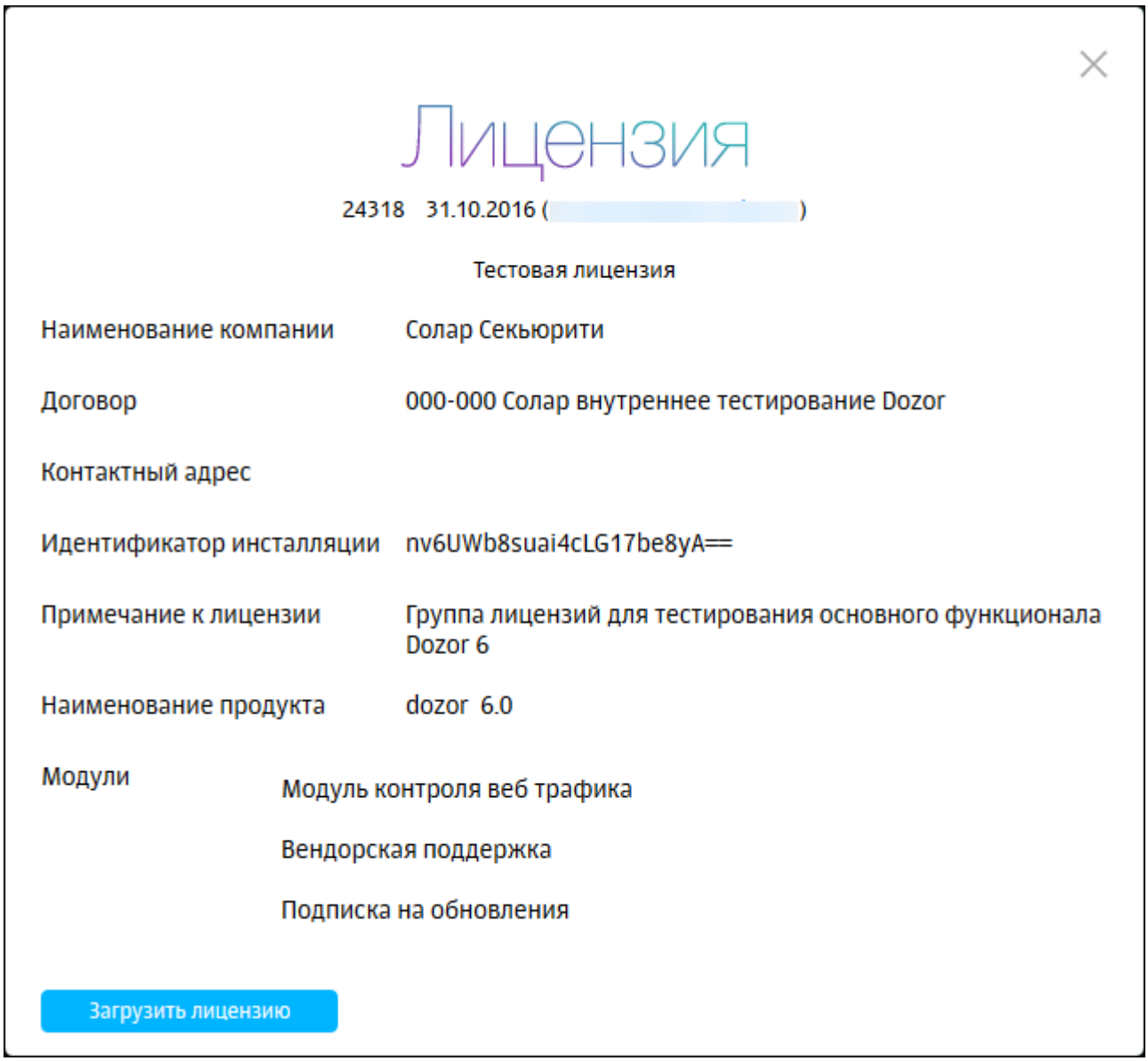

Рис. 6.2. Окно лицензии

Постоянная лицензия Solar webProxy всегда жёстко привязана к конкретной аппаратной платформе (виртуальной или физической) master-узла кластера Solar webProxy. Для однозначной привязки используется идентификатор инсталляции, представляющий собой особым образом формируемый хэш, зависящий от некоторых уникальных характеристик аппаратного обеспечения master-узла. Идентификатор инсталляции формируется при первом запуске GUI Solar webProxy и передаётся инженерами внедрения в вендорскую службу поддержки, которая на его основе выпускает активированную лицензию для постоянного использования. Изменение хотя бы одной из характеристик master-узла, от которых зависит идентификатор инсталляции, приводит к недействительности выпущенной

лицензии и неработоспособности Solar webProxy. При функционировании master-узла в виртуальной среде миграция виртуальной машины приводит к тем же последствиям. В этих случаях необходимо обратиться в вендорскую службу поддержки для повторного выпуска лицензии.

Примечание

Идентификатор инсталляции не зависит от характеристик оперативной памяти и жёстких дисков, то есть их замена не приводит к недействительности лицензии.

6.3. Назначение ролей

После загрузки лицензии и входа в систему можно назначать роли узлам с помощью GUI. Для этого необходимо перейти в раздел **Конфигурации** на вкладку **Роли и сведения**, выбрать строку с нужным узлом и в раскрывшемся списке (см. Рис.6.3) выбрать все необходимые роли.

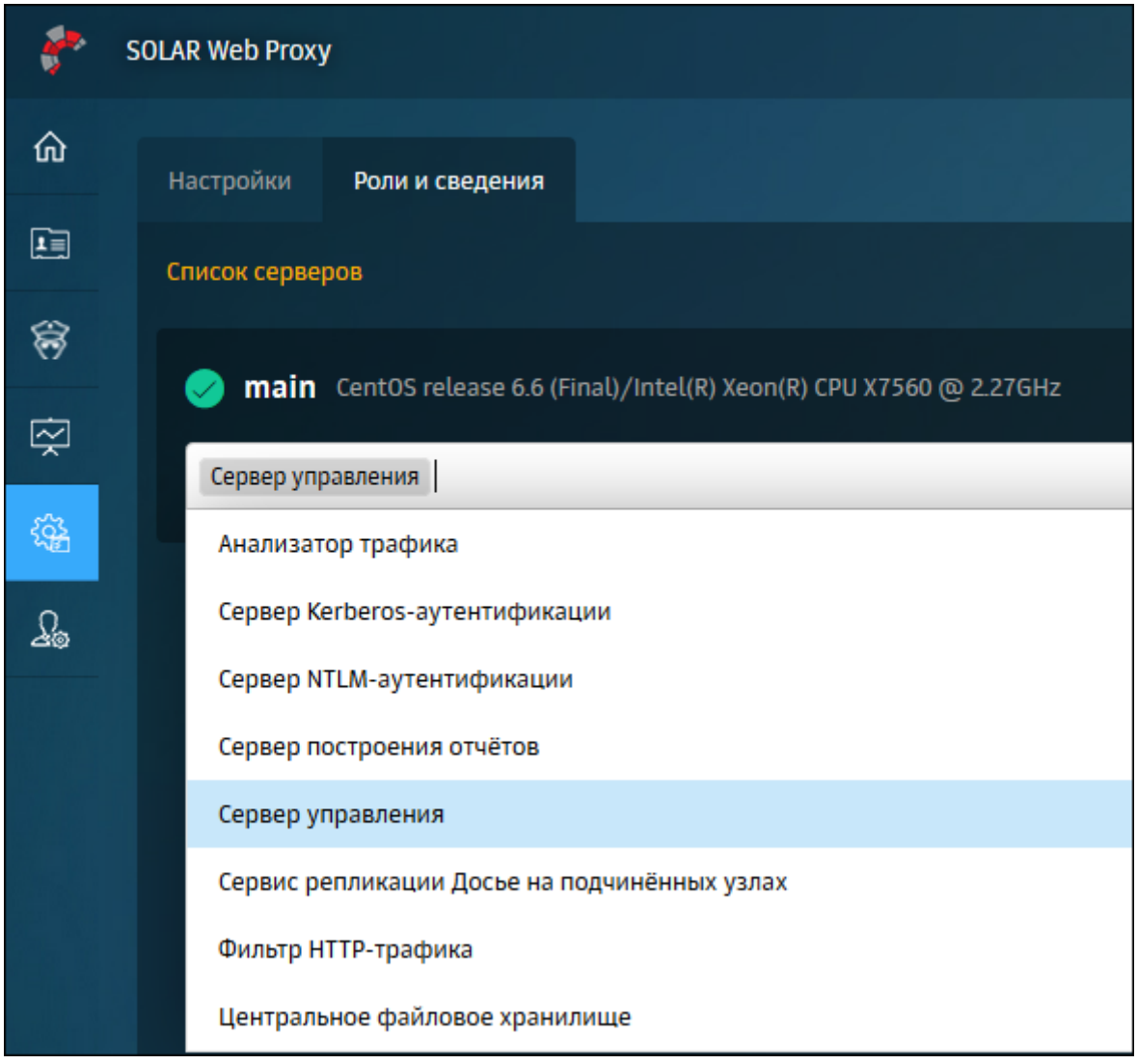

Рис. 6.3. Добавление роли для узла

После установки ролей для всех узлов следует нажать **Сохранить и применить**.

Рекомендации по назначению ролей приведены в разделе (6.17).

6.4. Настройка ротации журналов доступа

Для настройка ротации журналов доступа необходимо внести в расписание планировщика **cron** следующую запись:

```
0 0 1 * * /opt/dozor/clickhouse/bin/cleanup-db.sh -d <days>
```

где **<days>** – значение времени в днях. Данные журналов доступа старше этого значения будут удаляться. В данном примере вызов скрипта **`cleanup-db.sh`** будет происходить первого числа каждого месяца.

6.5. Настройка аутентификации

Механизм аутентификации Solar webProxy поддерживает следующие виды источников учётных записей:

- Локальный список IP-адресов и диапазонов
- Локальный список учётных записей
- LDAP
- IMAP
- POP3

При создании схемы аутентификации необходимо учитывать следующие особенности:

1. Проверка по IP-адресам имеет наивысший приоритет.
2. При доменной аутентификации используется только один источник в связи с уникальностью настроек **samba**, **krb5**, **winbind**.
3. Следует снять флажок **abort-by-error** (**Конфигурации > Сервер аутентификации > Схема аутентификации > Прерывать процесс аутентификации при возникновении ошибок**) в тех схемах, где это нужно. Параметр **abort-by-error** регулирует возможность прерывания процесса аутентификации при возникновении ошибок. Параметр предназначен для настройки разного поведения сервера аутентификации в случае возникновения ошибок с конкретным источником аутентификации. Например, если источник недоступен из-за сетевых проблем, то:
   - если флаг **abort-by-error** снят, поиск пользователей в БД данного источника не будет выполняться, и сервер аутентификации продолжит поиск подходящего пользователя в БД других заданных источников;
   - если флаг **abort-by-error** установлен, при появлении ошибок в процессе взаимодействия с данным источником сервер аутентификации будет выдавать ошибку и дальнейший поиск выполняться не будет.

В Solar webProxy используются следующие методы аутентификации:

- По IP-адресам (раздел **6.5.2**).
- basic (раздел **6.5.1**).
- NTLM (раздел **6.5.3**).
- Kerberos (раздел **6.5.3**).
- Прозрачная (раздел **6.5.4**).

Эти типы аутентификации используются в следующих режимах:

- Permissive – разрешительный режим. Аутентификация не разрешается только если запись пользователя заблокирована. Используется IP-аутентификация.
- Prohibitary – запретительный режим. Аутентификация разрешается только если запись пользователя существует и не заблокирована. Используется IP-аутентификация.
- basic – HTTP-аутентификация методом basic.
- ntlm – доменная аутентификация методом NTLM.
- Negotiate – доменная аутентификация методом Negotiate. По выбору клиента выполняется методом Kerberos или NTLM.
- ntlm+Negotiate – доменная аутентификация методом Negotiate либо NTLM. Метод выбирается клиентом. Этот режим используется если заранее неизвестно, поддерживает ли клиент метод Negotiate.

6.5.1. Настройка basic-аутентификации

Для basic-аутентификации могут использоваться следующие типы хранилищ:

- Локальный список (раздел **6.5.1.1**).
- LDAP (раздел **6.5.1.2**).
- Active Directory (раздел **6.5.1.3**).
- IMAP (раздел **6.5.1.4**).
- POP3 (раздел **6.5.1.5**).

6.5.1.1. Настройка параметров для basic-аутентификации по списку пользователей

Для настройки basic-аутентификации по списку пользователей необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).
2. Открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:
   - **Режим аутентификации** – **Proxy-Auth**

- **Метод аутентификации** – **Basic**

3. Нажать **Сохранить**, **Применить**.

6.5.1.2. Настройка параметров для basic-аутентификации с LDAP-сервером

Для настройки basic-аутентификации с источником аутентификации LDAP необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Схема аутентификации** (раздел **Конфигурации > Сервер аутентификации**).

2. Открыть группы параметров, как показано на Рис.6.4, установить флажок **Включить источник аутентификации** и для параметра **Источник** установить значение **ldap**.

3. Заполнить появившиеся поля, описание которых приведено в документе *Руководство администратора безопасности*.

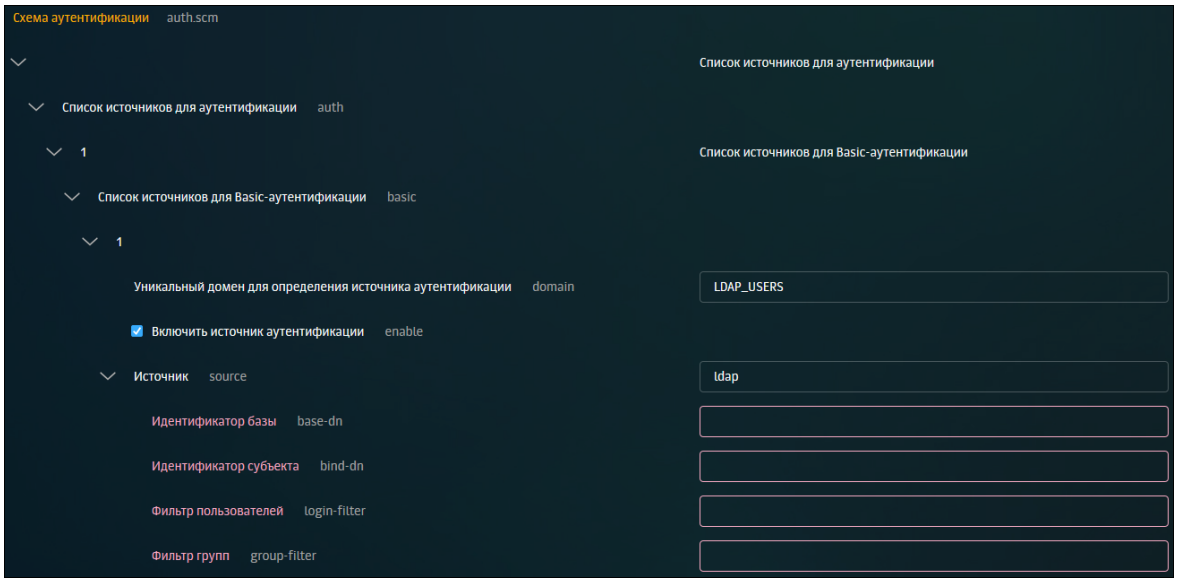

Рис. 6.4. Настройка basic + ldap аутентификации

4. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).

5. Открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**
   - **Метод аутентификации** – **Basic**

6. Нажать **Сохранить**, **Применить**.

Примечание

Рекомендуется использовать в качестве LDAP-сервера только Active Directory.

Можно задать более одного домена при выполнении аутентификации. Для этого необходимо в секции **Схема аутентификации** нажать на кнопку  в строке **Список источников для Basic-аутентификации**, в результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, а при ошибке или таймауте новый запрос делается к следующему серверу из списка. В случае ошибки на последнем сервере, из списка опять выбирается первый сервер. При превышении заданного времени выполнения запроса (параметр **timeout**, секция **Настройки сервера аутентификации**) он прерывается, даже если ещё не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

Механизм failover поддерживается только для двух равноправных контроллеров домена.

6.5.1.3. Добавление настроек для basic-аутентификации со службой Active Directory

Для настройки basic-аутентификации со службой Active Directory необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Схема аутентификации** (раздел **Конфигурации > Сервер аутентификации**).
2. Открыть группы параметров, как показано на **Рис.6.4**, установить флажок **Включить источник аутентификации** и для параметра **Источник** установить значение **ad**.
3. Заполнить появившиеся поля аналогично тому, как показано на **Рис.6.5**:

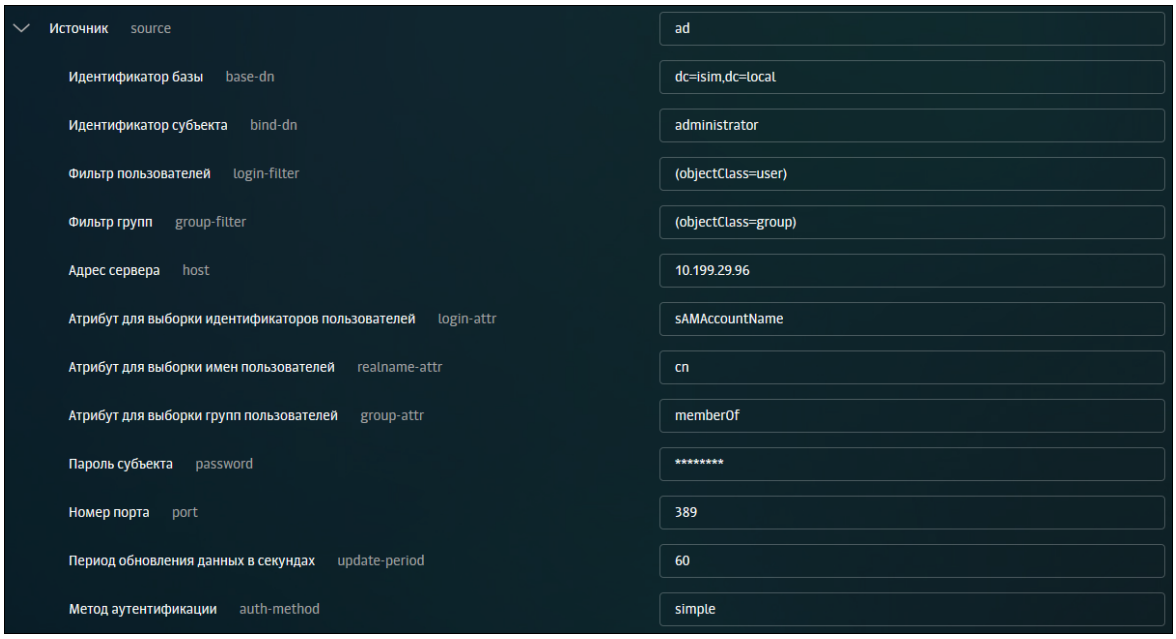

Рис. 6.5. Настройки сервера Active Directory

4. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).

5. Открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**
   - **Метод аутентификации** – **Basic**

6. Нажать **Сохранить**, **Применить**.

Можно задать более одного домена. Для этого необходимо в секции **Схема аутентификации** нажать на кнопку  в строке **Список источников для Basic-аутентификации**, в результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, а при ошибке или таймауте новый запрос делается к следующему серверу из списка. В случае ошибки на последнем сервере, из списка опять выбирается первый сервер. При превышении заданного времени выполнения запроса (параметр **timeout**, секция **Настройки сервера аутентификации**) он прерывается, даже если ещё не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

Механизм failover поддерживается только для двух равноправных контроллеров домена.

6.5.1.4. Добавление настроек для basic-аутентификации с IMAP-сервером

Для настройки basic-аутентификации с источником аутентификации IMAP необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Схема аутентификации** (раздел **Конфигурации > Сервер аутентификации**).

2. Открыть группы параметров, как показано на **Рис.6.4**, установить флажок **Включить источник аутентификации** и для параметра **Источник** установить значение **imap**.

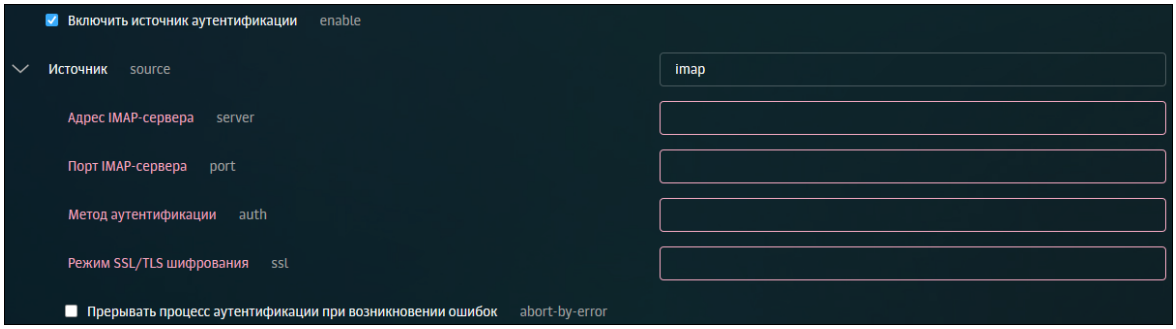

Рис. 6.6. Настройка аутентификации basic + imap

3. Задать следующие параметры (**Рис.6.6**):

   - **Адрес IMAP-сервера** – IP-адрес IMAP-сервера;
   - **Порт IMAP-сервера** – порт IMAP-сервера;

   Выбрать метод аутентификации и режим SSL/TLS-шифрования из предлагаемых вариантов.

4. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).

5. Открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**
   - **Метод аутентификации** – **Basic**

6. Нажать **Сохранить**, **Применить**.

6.5.1.5. Добавление настроек для basic-аутентификации с POP3-сервером

Для настройки basic-аутентификации с источником аутентификации POP3 необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Схема аутентификации** (раздел **Конфигурации > Сервер аутентификации**).

2. Открыть группы параметров, как показано на **Рис.6.4**, установить флажок **Включить источник аутентификации** и для параметра **Источник** установить значение **pop3**.

Рис. 6.7. Настройка аутентификации basic + pop3

3. Задать следующие параметры (**Рис.6.7**):

   - **Адрес POP3-сервера** – IP-адрес POP3-сервера;
   - **Порт POP3-сервера** – порт POP3-сервера;

   Выбрать режим SSL/TLS-шифрования из предлагаемых вариантов.

4. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).

5. Открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**
   - **Метод аутентификации** – **Basic**

6. Нажать **Сохранить**, **Применить**.

6.5.2. Настройка аутентификации по IP-адресам

Аутентификация по IP-адресам может работать в одном из двух режимов:

- Разрешительный – доступ разрешён с любых IP-адресов без исключений.
- Запретительный – доступ разрешён только в соответствии с настроенным слоем политики **Доступ без аутентификации**. Подробная информация о настройке этого слоя приведена в документе *Руководство администратора безопасности*.

Для настройки режима аутентификации необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**), открыть группу **Аутентификация и авторизация** и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**

- **Метод аутентификации**:
  - **Permissive** – для разрешительного режима.
  - **Prohibitary** – для запретительного режима.

2. Нажать **Сохранить**, **Применить**.

6.5.3. Настройка NTLM и Kerberos-аутентификации

Для настройки NTLM-аутентификации необходимо выполнить следующие действия:

1. Назначить одному из узлов Solar webProxy роль **Сервер NTLM-аутентификации**. Это будет сервер аутентификации Solar webProxy.

2. Открыть секцию **Настройка конфигурации Kerberos-аутентификации** раздела настроек **Конфигурации > Регистрация сервера в домене** и задать значения следующих параметров:

   - **Название домена** – имя домена.
   - **Адрес KDC-сервера** – IP-адрес сервера центра выдачи ключей (KDC) в сети. Можно добавлять и удалять записи о серверах, используя кнопки  и  .
   - **Адрес административного сервера** – IP-адрес контроллера домена в сети. Можно добавлять и удалять записи о серверах, используя кнопки  и  .

3. Открыть секцию **Настройки подключения к контроллеру домена** и задать значения следующих параметров:

   - **Название домена** – имя домена AD.
   - **NETBIOS-имя для сервера Web Proxy** – краткое доменное имя Solar webProxy.
   - **Сетевой адрес контроллера домена** – FQDN контроллера домена в сети.
   - **Рабочая группа** – NetBIOS-имя домена.
   - **Идентификатор пользователя с правами администратора контроллера домена** – имя учетной записи администратора контроллера домена.
   - **Пароль пользователя с правами администратора контроллера домена** – пароль этой учетной записи.

4. На сервере аутентификации Solar webProxy открыть для редактирования файл **`/etc/resolv.conf`** и добавить в него строки следующего вида:

   ```
   nameserver <namesrvIP>
   ```

   где **<namesrvIP>** – IP-адрес контроллера домена. Если таких адресов несколько, следует добавить несколько таких строк, в порядке уменьшения надёжности контроллеров домена. В каждой строке может быть только один IP-адрес.

5. Добавить сервер аутентификации в домен, выполнив на нём с помощью CLI следующую команду:

   ```
   # net ads join -U administrator
   ```

6. Перейти в GUI, открыть секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**) и задать значения следующих параметров:

   - **Режим аутентификации** – **Proxy-Auth**
   - **Метод аутентификации**:
     - **NTLM** – если планируется безальтернативное использование метода аутентификации NTLM.
     - **Negotiate** – если предполагается, что клиент будет выбирать между методами аутентификации NTLM и Kerberos (см. ниже).
     - **NTLM+Negotiate** – если предполагается использование предыдущей схемы, но заранее неизвестно, поддерживает ли клиентское ПО метод Negotiate.

7. Нажать **Сохранить** и **Применить**.

Для настройки Kerberos-аутентификации необходимо выполнить все предыдущие шаги, учитывая следующее:

- В шаге 1 необходимо назначить роль **Сервер Kerberos-аутентификации** вместо **Сервер NTLM-аутентификации**.
- В шаге 6 для параметра **Метод аутентификации** следует выбрать значение **Negotiate** или **NTLM+Negotiate**.

После этого следует с помощью CLI на контроллере домена создать ключ, выполнив следующую команду:

```
C:\Users\Administrator>ktpass.exe -out C:\krb5.keytab -princ HTTP/auth-skvt.solar.local@WINDOWS.DOMAIN -mapuser skvt2 -pass password -cryptoAll -ptype KRB5_NT_PRINCIPAL
```

подменяя следующие значения:

- **auth-skvt.solar.local** – FQDN сервера аутентификации Solar webProxy.
- **WINDOWS.DOMAIN** – имя домена.
- **skvt2** – пользователь Solar webProxy – владелец ключа.
- **password** – пароль этого пользователя.

В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после ключа **-out**, в данном примере – **`C:\krb5.keytab`**. Следует скопировать этот ключ и поместить его в каталог **`/etc`** на сервере аутентификации Solar webProxy.

Если серверов фильтрации несколько, то ключ генерируется на общее доменное имя для всех этих серверов. Например, если имеется два сервера фильтрации с сетевыми именами **filter1.org.local** и **filter2.org.local**, и IP-адресами 10.10.10.1 и 10.10.10.2 соответственно, то следует выбрать общее имя для них, например **proxy.org.local**. Ключ должен быть сгенерирован для имени **proxy.org.local**, а на каждом сервере фильтрации в файл **/etc/hosts** необходимо добавить запись вида:

```
10.10.10.1 proxy.org.local
```

```
10.10.10.2 proxy.org.local
```

На каждом сервере фильтрации должна быть только одна из этих записей, соответствующая его IP-адресу.

6.5.4. Настройка прозрачной аутентификации

Прозрачная аутентификация применяется в случаях, когда настройка браузеров рабочих станций пользователей невозможна, затруднена или неприемлема. При этом имеются следующие ограничения на архитектуру корпоративной сети:

- Каждому IP-адресу должен соответствовать только один пользователь.
- Между рабочими станциями пользователей и Solar webProxy не должно быть других прокси-серверов и оборудования, осуществляющего трансляцию адресов.
- Работа терминальных серверов не поддерживается.
- Поддерживается только доменная аутентификация.

Для корректного использования режима прозрачной аутентификации необходимо добавить сертификат Solar webProxy в список доверенных на всех рабочих станциях пользователей.

Кроме того, необходимо добавить сервер с ролью **Фильтр HTTP-трафика** (skvt-wizor) в прямую и обратную зоны DNS согласно настройке параметра **web-host** в группе **Веб-сервер** (секция **Конфигурации > Фильтрация и кэширование трафика > Настройки фильтрации и анализа трафика пользователей**). В противном случае браузер не сможет корректно аутентифицировать пользователей и будет выполнять перенаправление на страницу авторизации.

Режим прозрачной аутентификации заменяет обычную аутентификацию на прокси-сервере (HTTP 407: Proxy Authorization Required). При обращении к Solar webProxy рабочей станции пользователя, IP-адрес которой не содержится в хранилище Solar webProxy, её запрос перенаправляется на служебную страницу. На этой странице пользователю предлагается ввести учётные данные (HTTP 401: Unauthorized), и в случае успешной авторизации IP-адрес добавляется в хранилище, и продолжается обработка первоначального запроса. Запросы с рабочих станций, IP-адреса которых содержатся в хранилище, обрабатываются без перенаправлений.

В первую очередь следует настроить пакетные фильтры на всех узлах фильтрации, для чего необходимо выполнить следующие действия:

1. Открыть конфигурационный файл **/etc/sysctl.conf** и для параметра **net.ipv4.ip_forward** заменить значение **0** на **1**. Сохранить и закрыть файл.

2. Применить настройки пакетного фильтра, выполнив команду:

```
/sbin/sysctl -p
```

3. Включить поддержку TPROXY в подсистеме маршрутизации, выполнив следующие команды:

```
ip -f inet rule add fwmark 1 lookup 100
```

```
ip -f inet route add local default dev eth0 table 100
```

4. Подготовить Solar webProxy к перенаправлению запросов, выполнив следующие команды:

```
iptables -t mangle -N DIVERT
```

```
iptables -t mangle -A DIVERT -j MARK --set-mark 1
```

```
iptables -t mangle -A DIVERT -j ACCEPT
```

```
iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
```

5. Настроить перенаправление запросов в Solar webProxy, выполнив следующие команды:

```
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j TPROXY --
tproxy-mark 0x1/0x1 --on-port 2444
```

```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY --
tproxy-mark 0x1/0x1 --on-port 2270
```

Внимание!

Если для фильтрации используется master-узел, вместо приведённых команд следует выполнить следующие:

```
iptables -t mangle -A PREROUTING ! -d <master-IP> -p tcp --
dport 443 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 2444
```

```
iptables -t mangle -A PREROUTING ! -d <master-IP> -p tcp --
dport 80 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 2270
```

где <master-IP> – IP-адрес master-узла.

6. Создать конфигурационные файлы настроек маршрутизации и правил, выполнив следующие команды:

```
touch /etc/sysconfig/network-scripts/rule-eth0
```

```
touch /etc/sysconfig/network-scripts/route-eth0
```

7. Открыть файл **/etc/sysconfig/network-scripts/rule-eth0** и записать в него следующую строку:

```
fwmark 1 lookup 100
```

Сохранить и закрыть файл.

8. Открыть файл **/etc/sysconfig/network-scripts/route-eth0** и записать в него следующую строку:

```
local default dev eth0 table 100
```

Сохранить и закрыть файл.

9. Перезапустить сетевую службу, выполнив следующую команду:

```
service network restart
```

Для включения режима прозрачной аутентификации необходимо перейти в GUI Solar webProxy и выполнить следующие действия:

1. Перейти в секцию параметров **Настройки фильтрации и анализа трафика пользователей** (раздел **Конфигурации > Фильтрация и кэширование трафика**).

2. В группе параметров **Аутентификация и авторизация** для параметра **Режим аутентификации** установить значение **Transparent**.

3. В группе параметров **Фильтрация** установить флажок для параметра **Прозрачный режим работы шлюза** .

4. Убедиться, что в группе параметров **HTTPS** значения параметров **Интерфейс для перехваченных HTTPS соединений** и **Порт для перехваченных HTTPS соединений** установлены по умолчанию (**0.0.0.0** и **2444** соответственно).

5. Перейти в секцию **Настройка доступа администратора** и установить флажок для параметра **Запускать от имени пользователя root**. Нажать **Сохранить**, затем **Применить**.

6. Перезапустить сервис **skvt-wizor**.

6.6. Настройка WCCP

Перед настройкой WCCP необходимо настроить прозрачный режим работы Solar webProxy (см. раздел 6.5.4).

6.6.1. Настройка оборудования Cisco

Для настройки маршрутизатора Cisco необходимо выполнить следующие действия:

1. Настроить сетевые интерфейсы маршрутизатора так, чтобы один интерфейс находился в локальной подсети организации, в которой размещен кластер Solar webProxy, а другой – в подсети провайдера сети Интернет.

2. Авторизоваться в CLI маршрутизатора и создать обратную петлю, отвечающую за GRE-туннель, выполнив следующие команды:

```
cisco> enable

cisco# configure terminal

cisco(config)# interface loopback 1
```

```
cisco(config)# ip address <loopback-IP> 255.255.255.255
```

где **<loopback-IP>** – IP-адрес обратной петли. Этот адрес выбирается сетевым администратором организации на его усмотрение.

3. Создать список управления доступом со списком адресов WCCP-клиентов, выполнив следующие команды:

```
cisco(config)# access-list 10 permit <WP-IP>

cisco(config)# ip wccp web-cache group-list 10
```

где **<WP-IP>** – IP-адрес узла фильтрации Solar webProxy.

4. Создать список управления доступом с правилами маршрутизации трафика на Solar webProxy, выполнив следующие команды:

```
cisco(config)# ip access-list extended WCCP_ACCESS

cisco(config-ext-nacl)# remark ACL for HTTP/HTTPS

cisco(config-ext-nacl)# remark WebProxy bypass WCCP

cisco(config-ext-nacl)# deny ip host <WP-IP> any

cisco(config-ext-nacl)# remark LAN clients proxy port 80/443

cisco(config-ext-nacl)# permit tcp <LAN-IP> <INV-LAN-MASK> any eq
www 443

cisco(config-ext-nacl)# remark all others bypass WCCP

cisco(config-ext-nacl)# deny ip any any
```

где **<WP-IP>** – IP-адрес узла фильтрации Solar webProxy, **<LAN-IP>** – пространство IP-адресов локальной сети, в которой находятся АРМ сотрудников организации (например, **192.168.100.0**), **<INV-LAN-MASK>** – инверсная маска этой сети (в данном примере – **0.0.0.255**).

5. Установить правила перенаправления для WCCP, выполнив следующие команды:

```
cisco(config)# ip wccp web-cache redirect-list WCCP_ACCESS

cisco(config)# ip wccp 70 redirect-list WCCP_ACCESS
```

6. Настроить перенаправление на внутреннем интерфейсе, выполнив следующие команды:

```
cisco(config)# interface <ifname>

cisco(config-if)# ip wccp web-cache redirect in

cisco(config-if)# ip wccp 70 redirect in
```

где **<ifname>** – имя интерфейса маршрутизатора Cisco, находящегося в локальной сети.

7. Завершить конфигурирование маршрутизатора и сохранить конфигурацию, выполнив следующие команды:

   ```
   cisco(config)# end

   cisco# copy running-config startup-config
   ```

6.6.2. Настройка оборудования Solar webProxy

Для настройки Solar webProxy необходимо выполнить следующие действия:

1. Настроить GRE-туннель, выполнив следующие команды:

   ```
   iptunnel add wccp0 mode gre remote <CISCO-IP> local <WP-IP> dev eth0

   ip link set wccp0 up
   ```

   где **<CISCO-IP>** – IP-адрес маршрутизатора Cisco, а **<WP-IP>** – IP-адрес узла фильтрации Solar webProxy

2. Перейти в GUI Solar webProxy, открыть секцию настроек **Конфигурации > Фильтрация и кэширования трафика > Настройки кэширования данных от внешних веб-серверов**, установить флажок **Использовать протокол WCCP** и указать IP-адрес маршрутизатора Cisco в качестве значения параметра **IP-адрес роутера**. Нажать **Сохранить**, **Применить**.

6.6.3. Проверка работоспособности

Для проверки работоспособности настроенной схемы необходимо авторизоваться в CLI маршрутизатора и выполнить следующую команду:

```
show ip wccp
```

На экране будет отображён вывод следующего вида:

```
Global WCCP information:
    Router information:
        Router Identifier:                   192.168.30.138
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             1
        Number of routers:                   1
        Total Packets Redirected:            0
        Redirect access-list:                WCCP_ACCESS
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
    Service Identifier: 70
        Number of Cache Engines:             1
        Number of routers:                   1
        Total Packets Redirected:            0
        Redirect access-list:                WCCP_ACCESS
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
```

Если схема настроена правильно, параметр **Number of Cache Engines** для обоих потоков WCCP будет отличен от нуля.

6.7. Настройка синхронизации Досье

6.7.1. Синхронизация с внешним источником

Для настройки синхронизации данных Досье с внешним источником необходимо выполнить следующие действия:

1. Перейти в GUI, выбрать раздел **Конфигурации > Досье**, и в секции **Настройки сервиса обновления Досье** установить параметр **Режим работы** в положение **Главный**.

2. В секции **Настройки доступа к источникам данных** раскрыть группы параметров как показано на Рис.6.8 и установить параметр **Параметры доступа к источнику данных** в положение **ldap**.

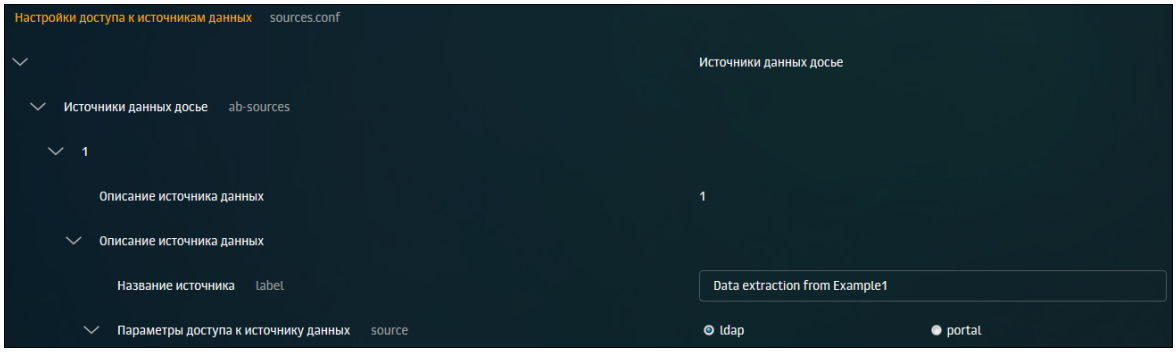

Рис. 6.8. Настройка синхронизации Досье

3. Задать значения следующих параметров:

   - **Название источника** – указать произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.

   - **DN пользователя** – имя учётной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например – **admin@organization.local**).

   - **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре.

   - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).

   - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.

4. Раскрыть группу параметров **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами AD и атрибутами досье.

Примечание

Например, адреса электронной почты пользователей могут содержаться в атрибуте proxyAddresses, а не email.

5. Нажать **Сохранить** и **Применить**.

6. Перейти в CLI и выполнить следующие команды:

```
# /opt/dozor/abook-daemon/bin/abook-sync

# /opt/dozor/bin/shell

# dsctl restart clickhouse
```

7. Вернуться в GUI и проверить наличие оргструктуры в разделе **Досье > Организационная структура**.

8. При необходимости задать интервал синхронизации. Открыть секцию **Настройки сервиса обновления Досье** и в группе **Режим работы > Автоматическая синхронизация с источниками** задать значение параметра **Периодичность запуска** (значение в часах). Нажать **Сохранить** и **Применить**.

6.7.2. Синхронизация со сторонним Досье

Досье Solar webProxy может работать в подчинённом режиме, то есть использовать Досье другого кластера Solar webProxy или Solar Dozor. Для этого сторонний кластер должен иметь собственное хранилище Досье. В этом режиме локальный кластер Solar webProxy подключается к Досье стороннего кластера и загружает в оперативную память локальную копию Досье. Все изменения, вносимые в Досье со стороны любого из кластеров, становятся доступными со стороны другого кластера. В подчинённом режиме нельзя подключиться к Досье кластера, также использующего подчинённый режим.

Для настройки синхронизации данных Досье Solar webProxy с Досье Solar Dozor или Solar webProxy необходимо выполнить следующие действия:

1. На master-узле перейти в CLI и выполнить команду:

```
# /opt/dozor/abook-daemon/bin/reg-abook-slave <host>
```

   где **<host>** – FQDN master-узла кластера Solar Dozor или Solar webProxy, с Досье которого будет выполняться синхронизация. При выполнении команды система запросит пароль пользователя **root** на удалённом master-узле.

2. Перейти в GUI, выбрать раздел **Конфигурации > Досье**, и в секции **Настройки сервиса обновления Досье** задать значения следующих параметров:

   - **Режим работы** – **Подчиненный**
   - **Сетевой адрес** – FQDN master-узла кластера Solar Dozor или Solar webProxy, с Досье которого будет выполняться синхронизация.

- **Номер порта** – порт, на котором сервис **abook-daemon** ожидает соединения по HTTPS (по умолчанию – 2269).

3. Нажать **Сохранить**, **Применить**.

4. Перезапустить сервис **abook-daemon** на локальном и удалённом master-узлах.

5. Перейти в CLI и выполнить следующие команды:

```
# /opt/dozor/bin/shell

# dsctl restart clickhouse
```

6.8. Настройка стороннего ICAP-прокси

В Solar webProxy предусмотрена возможность интеграции со сторонними прокси-серверами по протоколу ICAP.

Для настройки интеграции необходимо в настройках стороннего прокси-сервера в качестве ICAP-URI указать значение вида **icap://<WP_IP>:2272/KuroiNeko**, где **<WP_IP>** – IP-адрес сервера фильтрации Solar webProxy.

Описание настроек политики фильтрации приведено в документе *Руководство администратора безопасности*, раздел *Управление политиками*.

6.9. Настройка категоризаторов и стоп-листов

В Solar webProxy для фильтрации веб-трафика используются внешние категоризаторы **IAdmin** и **Blue Coat**, внутренние стоп-листы **Blacklists**, основанные на ПО SquidGuard, и стоп-листы **DNSBL**, **cDNS** и **Kaspersky**.

Порядок опроса категоризаторов можно посмотреть, выполнив в CLI следующие команды:

```
# source $PREFIX/etc/env.dsctl/base

# url-checker -C -D $CONFIG_FINAL_REPOS/`node_name`/skvt-url-checker
-h | grep prio
```

При необходимости порядок опроса категоризаторов можно изменить. Для этого необходимо перейти в раздел **Конфигурации > Категоризатор веб-ресурсов** открыть секцию **Настройки категоризатора веб-ресурсов** и выполнить настройку параметров.

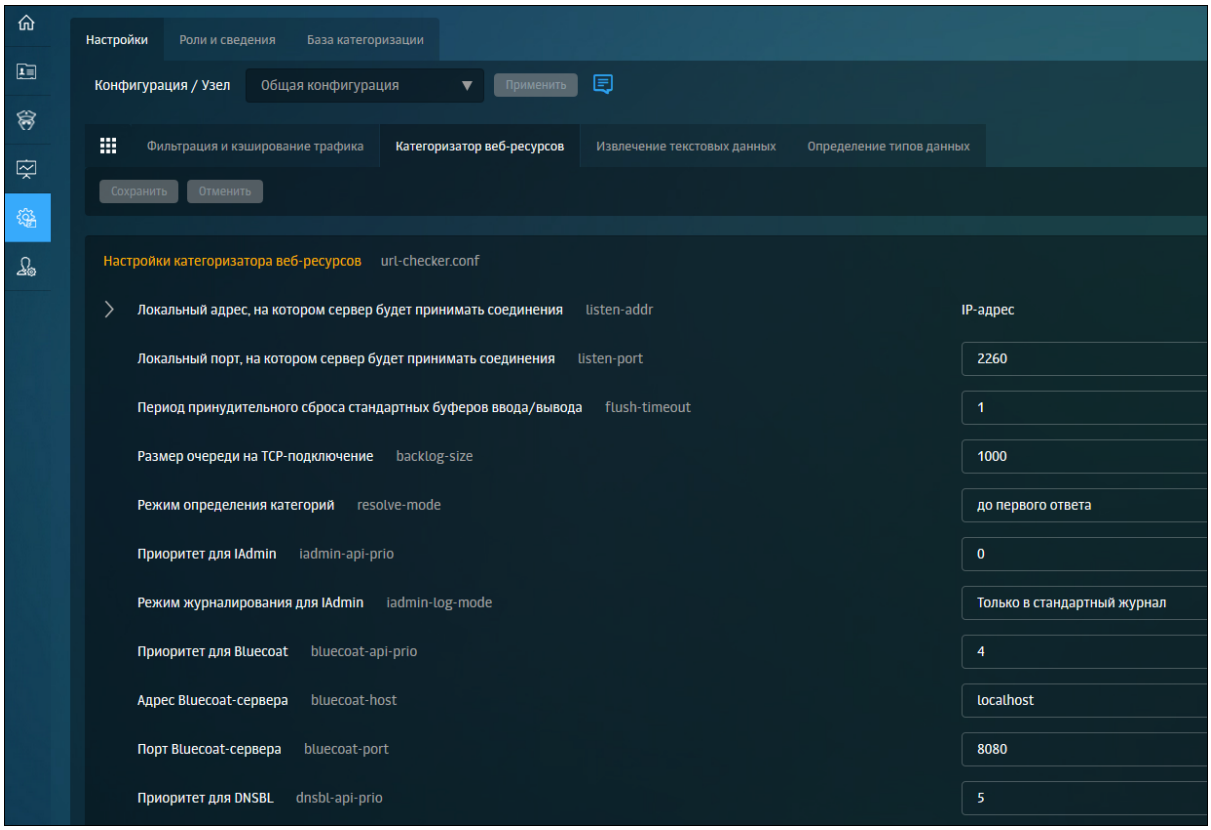

Рис. 6.9. Настройки категоризатора веб-ресурсов

Для использования того или иного категоризатора или стоп-листа необходимо установить для него величину приоритета в соответствующем поле. Чем меньше значение – тем выше приоритет. Категоризаторы и стоп-листы опрашиваются в порядке их приоритета. Для отключения того или иного категоризатора или стоп-листа необходимо в качестве его приоритета установить значение 0.

Внимание!

Перед использованием Solar webProxy необходимо убедиться, что хотя бы для одного категоризатора или стоп-листа установлен приоритет, отличный от 0.

Если результаты работы внешних категоризаторов по их базам неточны или по каким-то причинам неудобны, то необходимо прописывать исключения в текущий blacklist и устанавливать соответствие между требуемыми категориями.

Предусмотрена возможность добавления в систему дополнительных категоризаторов, выгрузки категорий, а также добавления URL в выбранную категорию (подробно описано в разделе **Управление базами категоризации** документа *Руководство администратора безопасности*).

Если не используются коммерческие категоризаторы, то будут применяться общедоступные стоп-листы **blacklists**, основанные на ПО SquidGuard, и стоп-листы **dnsbl**.

Для того чтобы отключить неиспользуемый категоризатор, необходимо перейти в секцию **Настройки категоризатора веб-ресурсов** в разделе **Конфигурации > Категоризатор веб-ресурсов** и в поле ***-api-prio**, где * – имя категоризатора, указать значение 0.

Определение категорий производится в соответствии с одним из следующих режимов работы категоризатора:

1. **URL** – определяется категория только того ресурса, на который был сделан запрос. Этот режим работы выбран по умолчанию, предназначен для совместимости с более старыми версиями Solar webProxy.

2. **Заголовки** – определяется категория того ресурса, на который был сделан запрос, и осуществляется поиск URL в заголовках запроса и ответа. Кроме того, из запроса извлекается и декодируется url-encode.

3. **Тело ответа в пределах preview** – URL извлекаются из тела ответа (только текстовые типы данных) в пределах размера preview.

4. **Заголовки и тело ответа в пределах preview** – установка режима 2 или режима 3 (определение категорий производится в соответствии с тем режимом, который сработал раньше).

5. **Тело ответа** – URL извлекаются из тела ответа (только текстовые типы данных) и передаются в категоризатор (без ограничений на размер).

6. **Заголовки и тело ответа** – установка режима 2 или режима 5 (определение категорий производится в соответствии с тем режимом, который сработал раньше).

Конкретный режим работы категоризатора задается при формировании политики фильтрации веб-трафика в разделе **Политики** > **Слои правил политики > Фильтрация запросов > Категории**.

Для определения названия категории и результата обработки всех включенных категоризаторов по URL ресурса необходимо выполнить команду:

```
# telnet localhost 2261
```

В результате выполнения команды на экран будет выведена информация следующего вида:

```
# telnet localhost 2261
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
mail.ru
customlists:
iadmin:
guest(15) -> host(1600) -> label(ИТ)
guest(18) -> host(712) -> label(Поисковые системы/порталы)
blacklists:
guest(mail) -> host(701) -> label(web-почта)
guest(webmail) -> host(701) -> label(web-почта)
dnsbl:
1600
ИТ
caml.ru
```

```
customlists:
iadmin:
guest(15) -> host(1600) -> label(ИТ)
blacklists:
dnsbl:
```

Система сохраняет информацию об ответах баз категоризаций на запросы о принадлежности URL. В журнале событий файла **`url-checker`** выводятся ответы всех баз категоризаций, которые содержат следующие атрибуты информации: время; URL, по которому запрашивалась категория; имя базы категоризации; категория, к которой относится URL согласно ответу базы категоризации. Журнал событий выглядит следующим образом:

```
2011-07-29 12:26:10.346497500 process requests (cur 0/max 8/clients 1)
2011-07-29 12:26:10.346499500 while process requests (cur 0/max 8/clients 1)
2011-07-29 12:26:10.346499500  - local queue length: 1
2011-07-29 12:26:10.346500500 run engine (iadmin-api)
2011-07-29 12:26:10.346501500 engines is done (engine: iadmin-api, request:

mail.ru/, categories: ИТ,Поисковые системы/порталы)
2011-07-29 12:26:10.346502500 run engine (blacklists)
2011-07-29 12:26:10.346503500 engines is done (engine: blacklists, request:

mail.ru/, categories: web-почта,web-почта)
2011-07-29 12:26:10.346515500 run engine (customlists)
2011-07-29 12:26:10.346516500 engines is done (engine: customlists, request:

mail.ru/, categories: )
2011-07-29 12:26:10.346517500 run engine (dnsbl)
2011-07-29 12:26:10.619051500 dnsbl ip-based left-hand
(94.100.191.201.pbl.spamhouse.org) -> (pbl.spamhouse.org,127.0.0.2)
2011-07-29 12:26:10.777581500 dnsbl host-based right-hand
(ru.mail.zen.spamhaus.org) -> (,)
2011-07-29 12:26:10.777583500 engines is done (engine: dnsbl, request:
mail.ru/, categories: Музыка,Неопределенная категория)
2011-07-29 12:26:10.777584500 no more resolve engines for current request
2011-07-29 12:26:10.777585500 url(mail.ru/), module(dnsbl), categories((Музыка

as 202)(web-почта as 701)(Поисковые системы/порталы as 712)(ИТ as 1600))
```

Примечание

Для вывода журнала событий необходимо включить параметры verbose и debug (секция Настройки категоризатора веб-ресурсов раздела Конфигурации > Категоризатор веб-ресурсов).

6.9.1. Настройка категоризатора Интернет Администратор

Solar webProxy использует категоризатор **Интернет Администратор**, поставляемый внешним производителем (**iadmin.ru**).

Дистрибутив **Интернет Администратор** представляет собой файловый архив, который распаковывается в рабочий каталог (по умолчанию **`/opt/dozor/iadmin/`**).

Если в сетевой архитектуре между кластером Solar webProxy и сетью Интернет расположен вышестоящий прокси-сервер, необходимо создать переменную окружения **http_proxy**, выполнив следующую команду:

```
export http_proxy=http://<parent-proxy-fqdn>:3128
```

где **<parent-proxy-fqdn>** – FQDN вышестоящего прокси-сервера. Эту команду следует выполнить на всех узлах, где будет использоваться **Интернет Администратор**.

Для работы программы необходима отдельная лицензия. Для регистрации ключа необходимо выполнить следующие действия:

1. Перейти в GUI в раздел **Конфигурации > Категоризатор веб-ресурсов** и в секции **Настройки модуля категоризации iAdmin** задать значение ключа в параметре **Ключ для работы модуля iAdmin**. Нажать **Сохранить**. Введённый ключ будет находиться в файле **/opt/dozor/iadmin/etc/key**.

   Примечание

   Если ранее на данной инсталляции Solar webProxy использовался другой ключ, следует удалить файлы с расширением ****.supd*** *из каталога* ***/opt/dozor/iadmin/share/bases*** *и записать значение 472 в файл* ***/opt/iadmin/etc/ver*** *в качестве версии базы.*

2. Перейти в CLI и выполнить команду:

   ```
   # /opt/dozor/iadmin/bin/iadminupdate -regkey
   ```

   После выполнения команды на экран выводится информация следующего вида:

   ```
   18.07.2008 19:33:16 IAdmin Update service is started
   18.07.2008 19:33:16 Entering configuration mode.
   18.07.2008 19:33:16 Attempting to register license key...
   18.07.2008 19:33:16 Attempting direct connection...
   18.07.2008 19:33:16 Direct connection established.
   18.07.2008 19:33:16 213 bytes was downloaded.
   18.07.2008 19:33:16 Server answer: Operation complete successfully. Error
    code: 0
   18.07.2008 19:33:16 IAdmin Update service is stopped
   ```

3. Проверить регистрацию ключа, выполнив команду:

   ```
   # cat /opt/iadmin/etc/userinfo
   ```

   Если регистрация ключа прошла успешно, то на экран выводится информация следующего вида:

   ```
   Licensed end user: Jet Infosystems for Testing ONLY
   End user IP address: 194.87.88.134
   ```

Примечание

Регистрация ключа автоматически проверяется и производится при изменениях настроек конфигурационного файла ***url-checker.conf*** *(например, при смене прокси-сервера) и при генерации ключа (в результате его изменения).*

Текущее значение ключа содержится в параметре **key-value** конфигурационного файла **iadmin.conf**.

Для получения рабочей конфигурации категоризатора необходимо выполнить команду:

```
# /opt/dozor/iadmin/bin/iadminupdate –checkcfg
```

Для получения обновления базы категоризатора необходимо выполнить команду:

```
# /opt/dozor/iadmin/bin/iadminupdate
```

Примечание

После выполнения этой команды необходимо перезапустить url-checker:

```
# dsctl restart skvt-url-checker
```

В дальнейшем обновление базы категоризатора будет выполняться автоматически (в соответствии с настройками конфигурационного файла).

На экран будет выведена информация следующего вида:

```
18.07.2008 19:10:01 IAdmin Update service is started
18.07.2008 19:10:01 ################ Connecting to iadmin update server...
18.07.2008 19:10:01 Attempting direct connection...
18.07.2008 19:10:02 Direct connection established.
18.07.2008 19:10:02 153 bytes was downloaded.
18.07.2008 19:10:02 Processing update 1 of 0
18.07.2008 19:10:02 No new updates was found. You have the last full category
 +database.
18.07.2008 19:10:02 ################ Disconnected from server
18.07.2008 19:10:02 IAdmin Update service is stopped
```

Сервис проверки URL по категориям **skvt-url-checker** вызывает функцию **IAdminLoadUpdate** для загрузки обновлений, по умолчанию - раз в 60 секунд. При наличии обновлений загружаются последние обновления. При необходимости для загрузки обновлений требуется в конфигурационном файле категоризатора прописать настройки **parent-proxy.**

Примечание

Поскольку информация о попытках регистрации ключа не записывается в журнал сервиса skvt-url-checker, то при настройке IAdmin рекомендуется организовать журналирование не только в стандартный журнал, но и в файл ***/opt/iadmin/etc/update.log****.*

Подробная информация о настройке IAdmin содержится в документации на категоризатор.

6.9.2. Настройка стоп-листов

Solar webProxy использует стоп-листы **blacklists**, основанные на ПО SquidGuard, и стоп-листы **dnsbl**.

Рабочий каталог для модуля **blacklists** находится в каталоге **`/opt/dozor/blacklists`**. В каталоге находятся подкаталоги с файлами по категориям. Файлы могут представлять собой как список доменных имён, так и список URL. Категории в этом каталоге обновляются централизованно из пакета. Основу пакета составляют категории с сайта http://urlblacklist.com.

Стоп-листы **dnsbl** – это списки серверов, основанные на DNS. Для модуля **dnsbl** в сервисе **skvt-url-checker** предусмотрен параметр **dnsbl-servers**, ограничивающий список используемых **dnsbl**-серверов:

```
# url-checker -h | grep dnsbl-servers
--, --dnsbl-servers ..... (dnsbl.cyberlogic.net zen.spamhaus.org) list over
 space of DNSBL servers
```

6.9.3. Настройка категоризатора Blue Coat

После настройки категоризатора **Blue Coat** необходимо настроить параметры **bluecoat-api-prio**, **bluecoat-host** и **bluecoat-port** в секции настроек **Настройки категоризатора веб-ресурсов** раздела **Конфигурации** > **Категоризатор веб-ресурсов**.

6.9.4. Настройка категоризатора Kaspersky

Для настройки категоризатора Kaspersky необходимо выполнить следующие действия:

1. Загрузить ключ категоризатора с сайта производителя (**Kaspersky Labs**). Скопировать ключ на master-узел в каталог по усмотрению (например, **`/var/tmp/`**).

2. Подключиться к master-узлу по протоколу SSH.

3. Загрузить командную оболочку, выполнив команду:

   `# /opt/dozor/bin/shell`

4. Зарегистрировать ключ категоризатора, выполнив команду:

   `# kasper-reg-certificate <path-to-kasper-key>`

   где **<path-to-kasper-key>** – путь к ключу, включая имя файла ключа.

5. Подождать две минуты либо выполнить на каждом узле команду:

   `# accept-settings`

6. На всех slave-узлах выполнить команду:

   `# kasper-base-update`

Примечание

Для корректного выполнения этой команды требуется соединение с сервером https://wlinfo.kaspersky.com:443.

7. Перейти в раздел GUI **Конфигурации > Категоризатор веб-ресурсов** и открыть секцию **Настройки категоризатора веб-ресурсов**.

8. Для параметра **kasper-api-prio** установить значение приоритета по отношению к другим категоризаторам: **iadmin-api-prio** (Интернет Администратор), **bluecoat-api-prio** (Blue Coat), **dnsbl-api-prio** (внешние стоп-листы), **cdns-api-prio** (категоризатор cair.ru), **blacklists-api-prio** (внутренние стоп-листы, основанные на SquidGuard), **customlists-api-prio** (Локальная БД категорий). Чем меньше значение параметра, тем выше приоритет.

9. Для параметра **Период запуска функций обновления баз категоризаторов** установить значение периода обновления баз категоризации в секундах. Значение по умолчанию – 43200 (12 часов).

10. Если используется вышестоящий прокси-сервер, то переключатель **Настройка прокси-сервера для получения обновлений** установить в значение **Настройка прокси-сервера** и задать следующие подчинённые параметры:

    - **Адрес прокси-сервера** – FQDN или IP-адрес вышестоящего прокси-сервера.
    - **Порт прокси-сервера** – порт, на котором вышестоящий прокси-сервер ожидает соединения.
    - **Логин для Basic-аутентификации на прокси-сервере** – имя пользователя для авторизации на вышестоящем прокси-сервере.
    - **Пароль для Basic-аутентификации на прокси-сервере** – пароль этого пользователя.

11. Нажать **Сохранить**, **Применить**.

6.10. Настройка балансировщика

Кластер Solar webProxy может использовать несколько серверов фильтрации. В этом случае для распределения трафика по серверам используют балансировщик.

Балансировщик управляет потоками данных (прозрачно и незаметно для клиентов) и позволяет увеличить производительность Solar webProxy за счет параллельной обработки запросов на нескольких узлах кластера. Балансировщик контролирует работоспособность серверов фильтрации и автоматически отключает узлы от процесса обработки запросов в случае их недоступности.

6.10.1. Настройка Squid

Ниже приведён пример реализации механизма балансировки потоков данных в Solar webProxy с использованием ПО Squid 3.1. Параметры Squid (балансировщика) хранятся в конфигурационном файле `/etc/squid/squid.conf`. Содержимое этого файла имеет следующий вид:

```
cache_mem 8 MB
cache_dir ufs /var/spool/squid 10 16 128
acl all src all
cache_peer SKVT_WIZOR_1 parent 2270 0 proxy-only round-robin no-netdb-exchange
no-query no-digest login=PASS connection-auth=on
cache_peer SKVT_WIZOR_2 parent 2270 0 proxy-only round-robin no-netdb-exchange
no-query no-digest login=PASS connection-auth=on
http_port 3128
http_access allow all
icp_access allow all
htcp_access allow all
persistent_connection_after_error on
access_log /var/log/squid/access.log squid
never_direct allow all
```

где **SKVT_WIZOR_1** и **SKVT_WIZOR_2** – FQDN или IP-адреса серверов фильтрации Solar webProxy.

Для настройки Squid необходимо выполнить следующие действия:

1. Отредактировать конфигурационный файл **`/etc/squid/squid.conf`**, указав необходимые доменные имена или IP-адреса серверов фильтрации Solar webProxy.

2. Перезапустить сервис **squid**, выполнив следующую команду:

   `/etc/init.d/squid reload`

3. В настройках браузеров пользователей Solar webProxy в качестве прокси-сервера указать адрес и порт балансировщика.

Примечание

Для корректной работы действия confirm требуется включение параметра Использовать заголовок X-Forwarded-For (секция Конфигурации > Фильтрация и кэширование трафика > Настройки фильтрации и анализа трафика пользователей, группа параметров Аутентификация и авторизация).

6.10.2. Настройка HAProxy

Для настройки балансировщика HAProxy необходимо выполнить на master-узле следующие действия:

1. Перейти в CLI и установить пакет **haproxy**, выполнив команду:

   `yum install haproxy`

2. Открыть для редактирования файл **`/etc/haproxy/haproxy.cfg`** и записать в строке **bind** актуальный порт, который будет доступен пользователям APM.

3. В строках **server** записать IP-адреса и порты серверов фильтрации Solar webProxy. Значение порта, на котором Solar webProxy ожидает соединения с HAProxy: 2278. Сохранить и закрыть файл.

Примечание

При необходимости, номер порта можно изменить на любое другое незанятое значение, но в этом случае следует записать такое же значение в конфигурации Solar webProxy (раздел Конфигурации > Фильтрация и кэширование трафика > Фильтрация, параметр Порт для подключения HAProxy).

4. Перезапустить сервис **haproxy**, выполнив команду:

   `/etc/init.d/haproxy restart`

5. Применить конфигурацию сервиса **haproxy**, выполнив команду:

   `chkconfig haproxy on`

6. Проверить, что сервис **haproxy** ожидает соединения на порту, указанном в конфигурации, выполнив команду:

   `netstat -nlp | grep haproxy`

Пример содержимого файла **`/etc/haproxy/haproxy.cfg`** для HTTP-режима:

```
global
        log 127.0.0.1 local2 notice
        chroot /var/lib/haproxy
        user haproxy
        group haproxy
        daemon
        maxconn 10000

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        retries 3
        option redispatch
        maxconn 10000
        option httpclose
  option http-server-close
        option forwardfor
        timeout connect 5000
        timeout client  50000
        timeout server  50000
        stats enable
        stats uri /haproxy
        stats realm Haproxy\ Statistics
        stats auth admin:123456
        stats refresh 30s

frontend Haproxy
       mode http
       bind *:3128
       option http-keep-alive
       timeout client 30s
```

```
       option forwardfor except 127.0.0.1
       default_backend back

backend back
        mode http
        balance roundrobin
        option httpclose
        option forwardfor
        option http-keep-alive
        option prefer-last-server
        timeout server 30s
        timeout connect 4s
        server pr-1 10.10.0.1:2278 check
        server pr-2 10.10.0.2:2278 check

http-request add-header X-Forwarded-Proto https if { ssl_fc }
```

Пример содержимого файла **`/etc/haproxy/haproxy.cfg`** для TCP-режима:

```
global
        log 127.0.0.1 local2 notice
        chroot /var/lib/haproxy
        user haproxy
        group haproxy
        daemon
        maxconn 10000

defaults
        log     global
        mode    tcp
        option  dontlognull
        retries 3
        option redispatch
        maxconn 10000
        option httpclose
  option http-server-close
        timeout connect 5000
        timeout client  50000
        timeout server  50000

frontend Haproxy
       mode tcp
       bind *:3128
       option http-keep-alive
       timeout client 30s
       default_backend back

backend back
        mode tcp
        balance roundrobin
        option httpclose
        option http-keep-alive
        timeout server 30s
        timeout connect 4s
        server pr-1 10.10.0.1:2278 check
        server pr-2 10.10.0.2:2278 check

http-request add-header X-Forwarded-Proto https if { ssl_fc }
```

6.11. Настройка авторизации в web-интерфейсе с учётной записью в домене

Для настройки аутентификации с доменной учётной записью необходимо выполнить следующие действия:

1. Перейти в секцию параметров **Схема аутентификации** (раздел **Конфигурации > Сервер аутентификации**).

2. Открыть группы параметров, как показано на Рис.6.4, установить флажок **Включить источник аутентификации** и для параметра **Источник** установить значение **ad**.

3. Заполнить появившиеся поля аналогично тому, как показано на Рис.6.5:

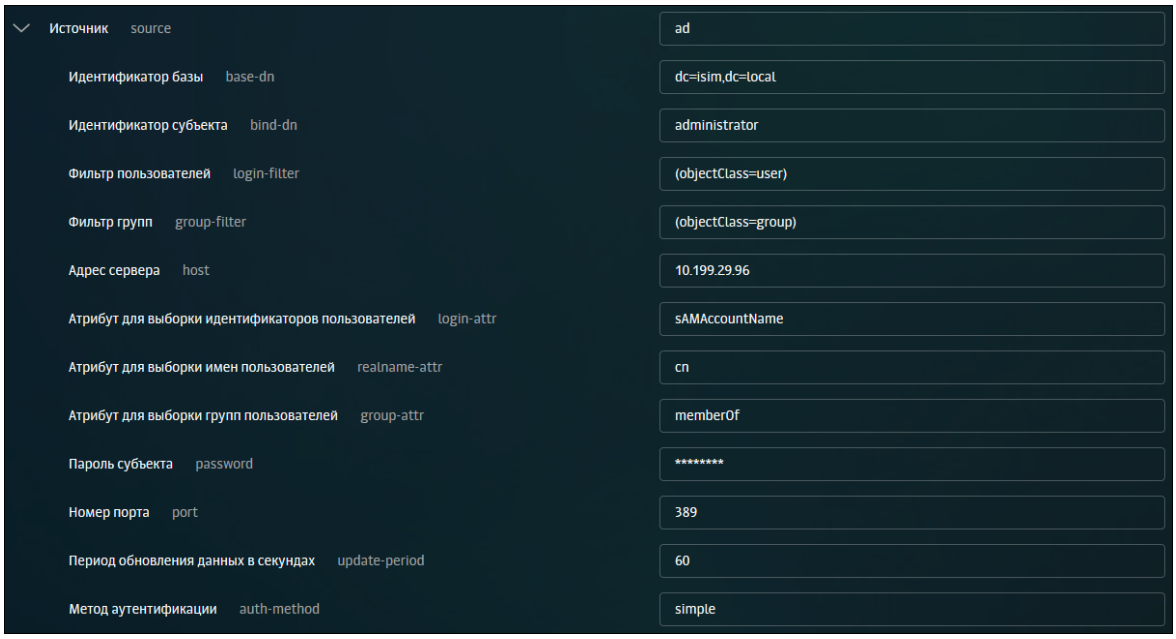

Рис. 6.10. Настройки сервера Active Directory

4. Задать значения параметров секции **Настройки сервера веб-интерфейса** (раздел **Конфигурации > Интерфейс**) аналогично тому, как показано на Рис.6.11:

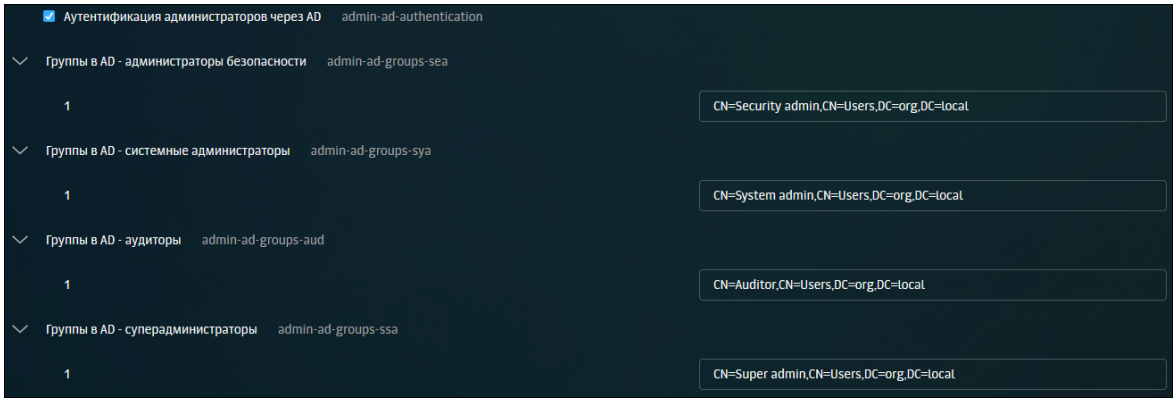

Рис. 6.11. Настройка play-server для AD-аутентификации

Внимание!

Функция смены пароля для доменных учётных записей недоступна в веб-интерфейсе.

6.12. Настройка вскрытия SSL-трафика (MITM)

Для настройки вскрытия шифрованных соединений АРМ пользователей корпоративной сети с ресурсами сети Интернет необходимо выполнить следующие действия:

1. Подключиться к серверу фильтрации кластера Solar webProxy по протоколу SSH. Если в кластере несколько серверов фильтрации, то приведённые ниже шаги следует выполнить для каждого из них.

2. Загрузить командную оболочку Solar webProxy, выполнив команду:

   ```
   /opt/dozor/bin/shell
   ```

3. При наличии в организации собственного УЦ, экспортировать сертификат организации как описано в разделе 6.12.1. В противном случае экспортировать сертификат УЦ Solar webProxy, выполнив команду:

   ```
   keytool --exportcert -rfc -keystore
   /opt/dozor/skvt/var/lib/authority.jks -alias "web proxy" > proxy1.crt
   ```

   Во время выполнения команды будет запрошен пароль, по умолчанию – **secret**. Файл сертификата появится в текущем каталоге (по умолчанию `/opt/dozor`).

4. Импортировать полученный сертификат в списки доверенных сертификатов браузеров АРМ пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, следует экспортировать сертификат на всех этих серверах. После экспорта выполнить импорт всех полученных сертификатов на АРМ пользователей.

6.12.1. Выпуск сертификата организации для вскрытия SSL-трафика

Если в организации имеется собственный УЦ, можно использовать его сертификат для вскрытия SSL-трафика. Допустимо использование сертификатов, сгенерированных алгоритмом строго выше SHA-1.

Для выпуска сертификата организации необходимо выполнить следующие действия на каждом сервере Solar webProxy с ролью **Фильтр HTTP-трафика**:

1. Открыть CLI и перейти во временный каталог (например, `/var/tmp/`), выполнив команду:

   ```
   # cd /var/tmp
   ```

2. Создать ключ RSA, выполнив команду:

   ```
   # openssl genrsa -out wp.key -aes256 2048
   ```

   Во время выполнения команды система потребует назначить пароль для ключа. Следует ввести пароль и запомнить его. После ввода необходимо подтвердить выбранный пароль.

3. Создать в текущем каталоге файл с именем **openssl.cnf** и записать в него следующие данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt=yes
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = RU

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow

localityName                    = Locality Name (eg, city)
localityName_default            = Moscow

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Organization

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept

commonName                      = Common Name (eg, your name or your
server\'s hostname)
commonName_default              = proxy.org.com

emailAddress                    = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

   Выделенные жирным значения параметров следует заменить на актуальные значения в организации:

   - **countryName_default** – двухбуквенный код страны.
   - **stateOrProvinceName_default** – регион.
   - **localityName_default** – город.

- **organizationName_default** – название организации.
- **organizationalUnitName_default** – название подразделения, департамента и т. д.
- **commonName_default** – FQDN сервера, на котором происходит настройка.
- **emailAddress_default** – контактный адрес электронной почты организации.
- **DNS.0** – значение, указанное в параметре **commonName_default**.
- **IP.0** – IP-адрес сервера, на котором происходит настройка.

4. Сгенерировать запрос на подпись сертификата, выполнив команду:

   ```
   # openssl req -new -key wp.key -out name.csr -config openssl.cnf
   ```

   В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверить используемый алгоритм шифрования. Для этого следует открыть программу **Командная строка** от имени администратора и выполнить в ней следующую команду:

   ```
   certutil - getreg ca \ csp \ CNGHashAlgorithm
   ```

   Если значение параметра **REG_SZ** равно **SHA1**, необходимо выполнить следующие команды:

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

   net stop CertSvc && net start CertSvc
   ```

6. Перевыписать корневой сертификат и перезапустить службу Certificate Services, выполнив следующие команды:

   ```
   certutil -renewCert ReuseKeys

   net stop CertSvc && net start CertSvc
   ```

7. Зайти на портал УЦ Windows.

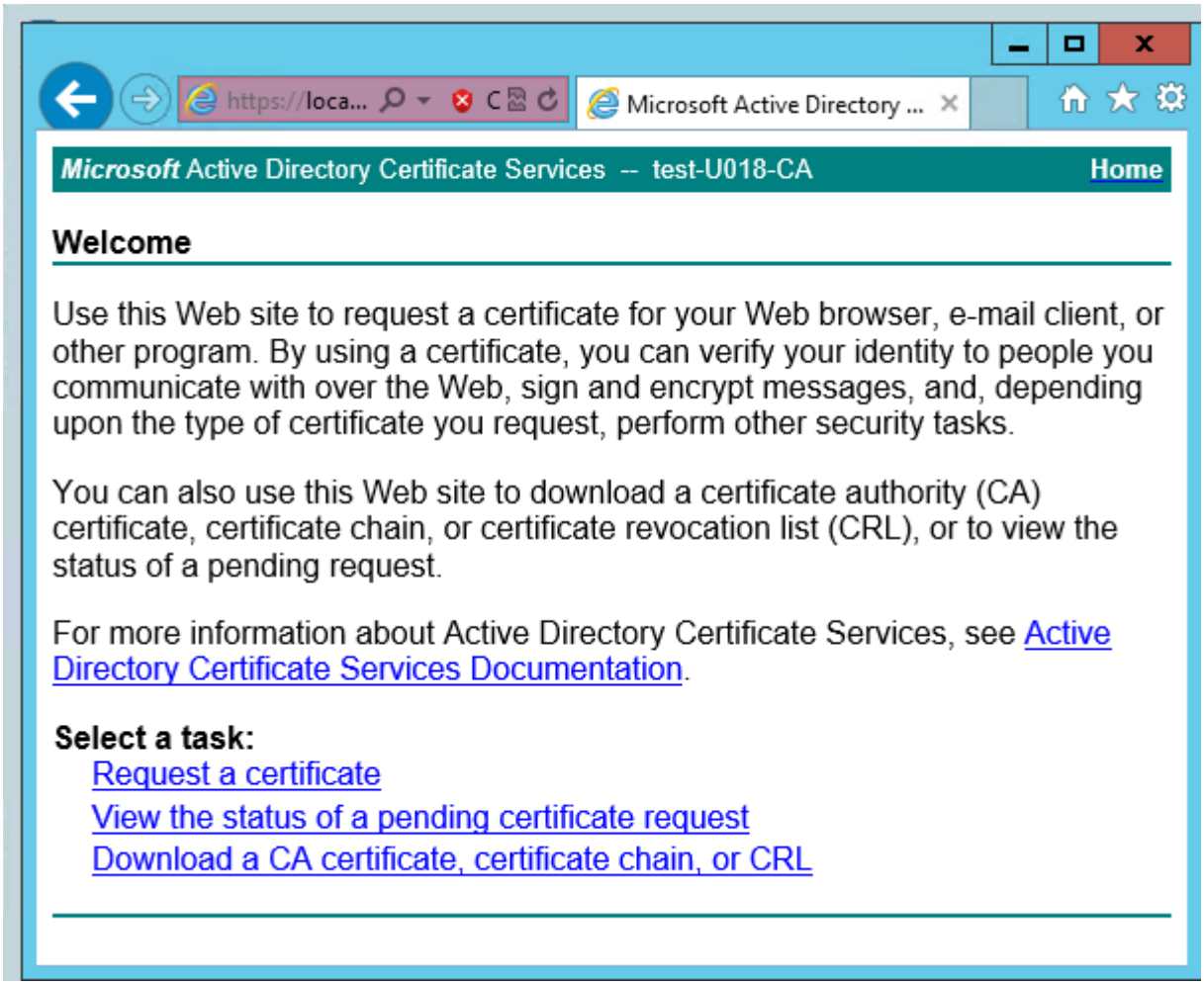

Рис. 6.12. Экран приветствия УЦ Windows

8. Нажать **Request a certificate**.

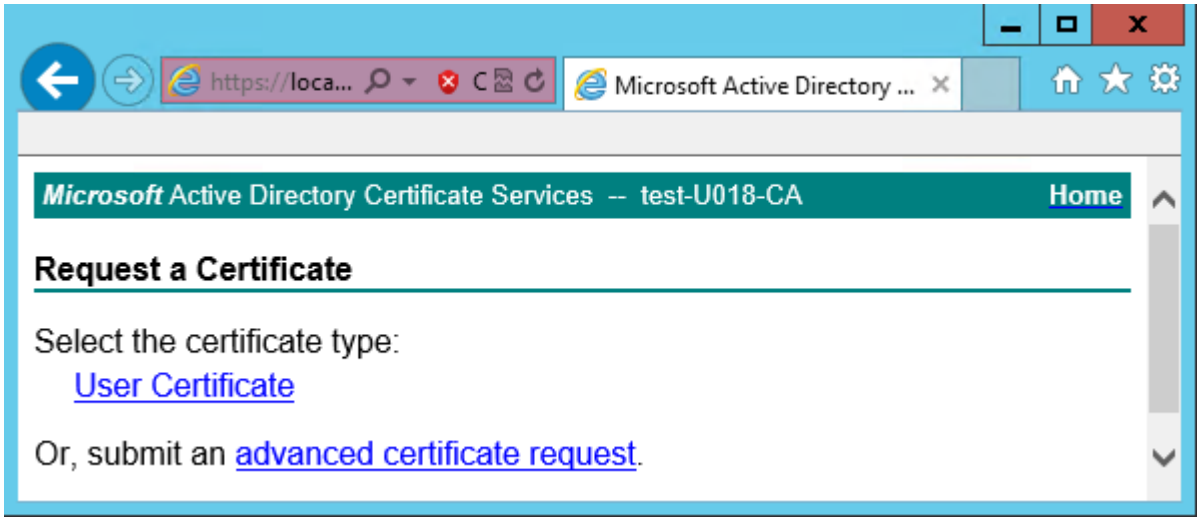

Рис. 6.13. Экран запроса сертификата

9. Нажать **advanced certificate request**.

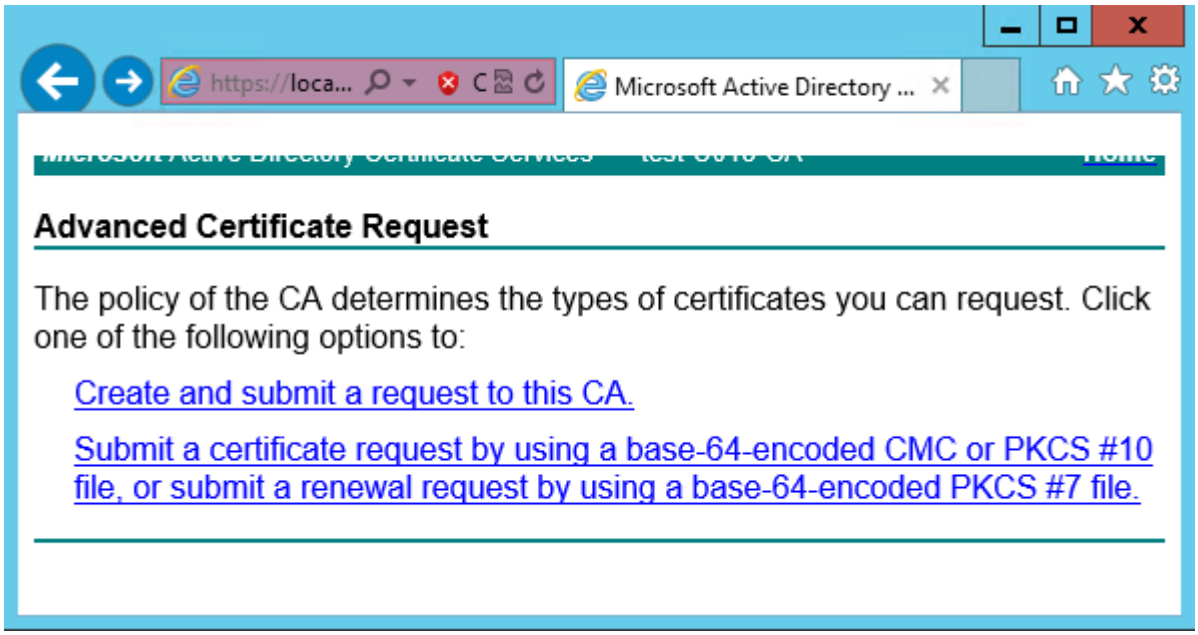

Рис. 6.14. Экран особого запроса сертификата

10. Нажать **Submit a certificate request by using...**.

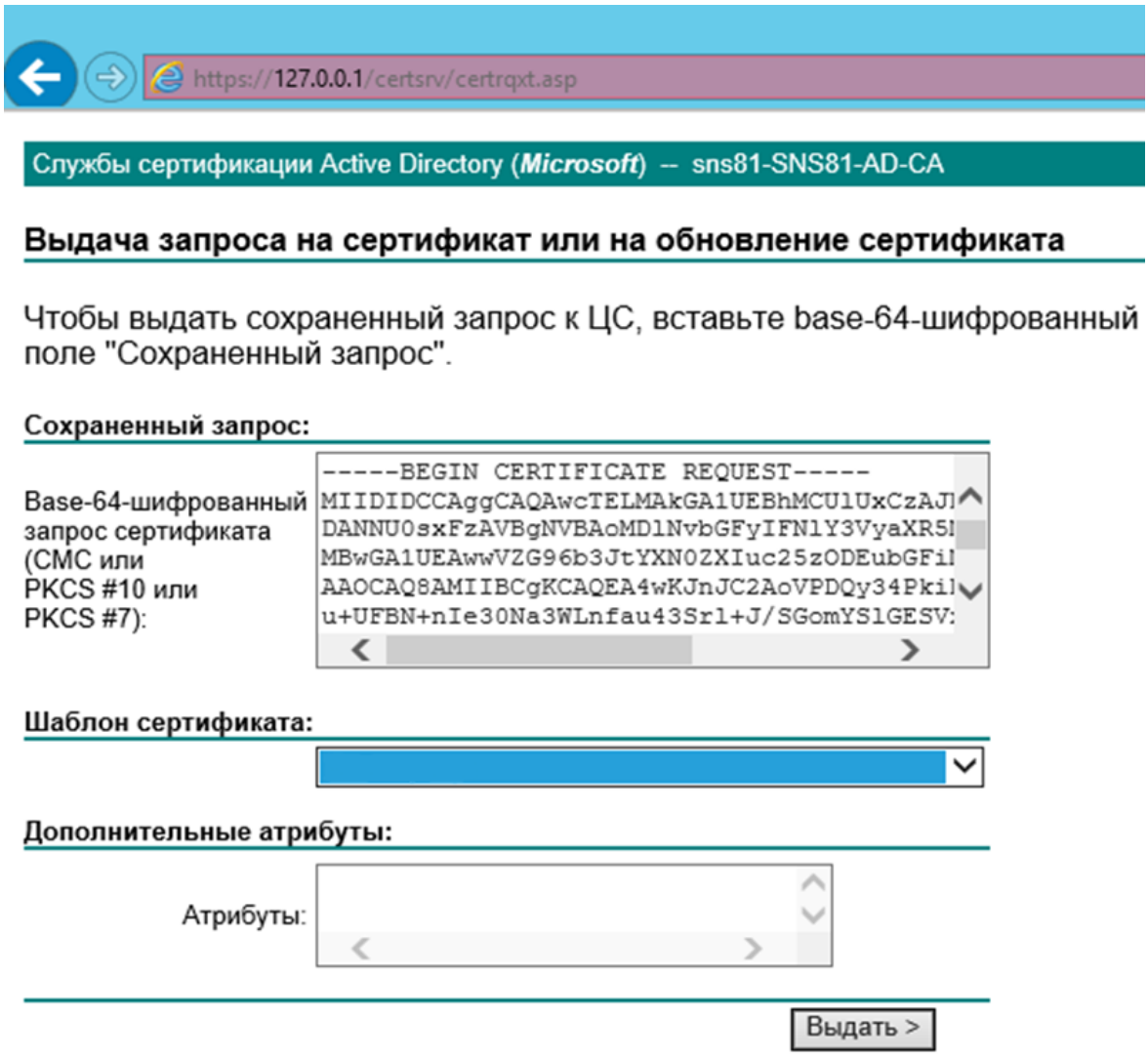

Рис. 6.15. Экран атрибутов сертификата

11. Выбрать шаблон сертификата **Subordinate authority** (**Подчинённый центр сертификации**) и вставить в поле **Base-64** содержимое файла, созданного на шаге 4. Нажать **Выдать**.

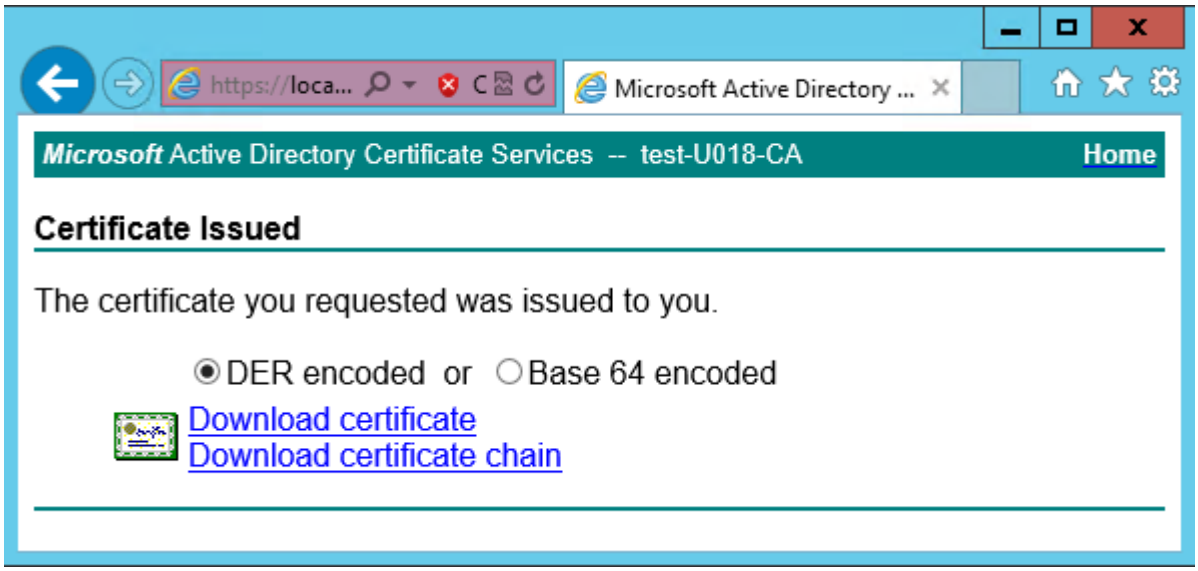

Рис. 6.16. Экран выдачи сертификата

12. Нажать **Download certificate**. Сохранить файл сертификата с именем **`wp.cer`** во временный каталог, выбранный в шаге 1.

13. Перейти на главную страницу портала УЦ и нажать **Download a CA certificate, certificate chain or CRL**. Сохранить сертификат УЦ с именем **`ca.cer`** в тот же каталог.

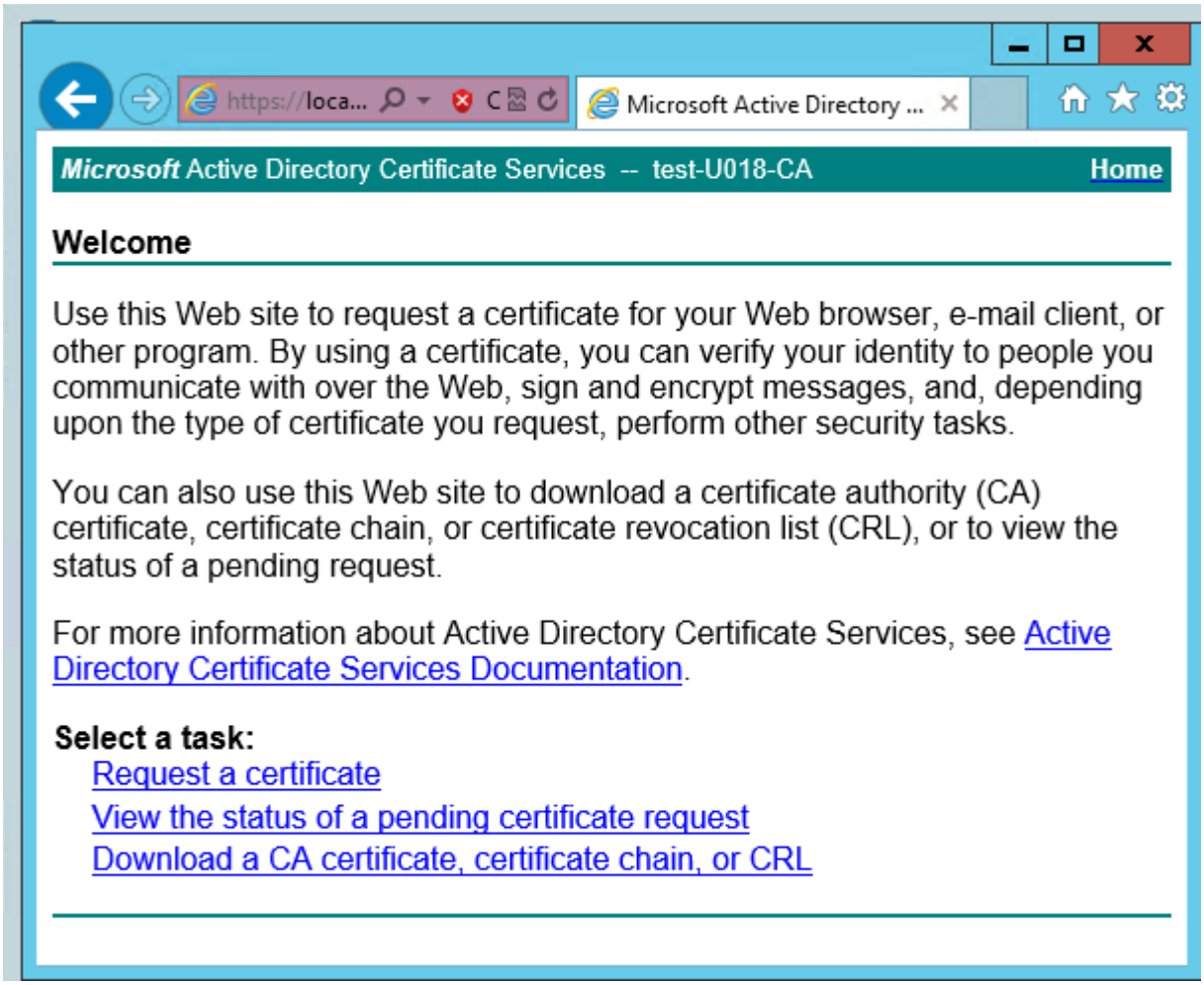

Рис. 6.17. Экран приветствия УЦ Windows

14. Вернуться в CLI Solar webProxy, перейти в выбранный временный каталог и сконвертировать загруженные сертификаты в формат PEM, выполнив команды:

```
# openssl x509 -inform der -in wp.cer -out wp.pem

# openssl x509 -inform der -in ca.cer -out ca.pem
```

15. Объединить сертификаты и ключ в сертификат pkcs12, выполнив команду:

```
# openssl pkcs12 -export -out wp.p12 -inkey wp.key -in wp.pem -
certfile ca.pem
```

Во время выполнения команды система потребует ввести пароль.

16. Импортировать Java-хранилище сертификатов, выполнив команду вида:

```
# keytool -importkeystore -deststorepass <password> -destkeypass
<password> -destkeystore <wpN>.jks -srckeystore wp.p12 -srcstorepass
<password>
```

где **<password>** – выбранный пароль, а **<wpN>** – имя сертификата для текущего сервера (например, **wp1**).

17. Скопировать Java-хранилище в каталог Solar webProxy, выполнив команду вида:

    # cp <wpN>.jks /opt/dozor/skvt/var/lib/

    где **<wpN>** – значение, выбранное в предыдущем шаге.

18. Сменить владельца хранилища, выполнив команду вида:

    # chown dozor:dozor /opt/dozor/etc/ssl/<wpN>.jks

19. Проверить, что сертификат находится в хранилище, выполнив команду вида:

    # keytool -list -keystore /opt/dozor/skvt/var/lib/<wpN>.jks

    О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

    ```
    1, Jul 10, 2018, PrivateKeyEntry,
    Certificate fingerprint (SHA1):
    B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
    ```

20. Перейти в GUI, выбрать раздел **Конфигурации > Фильтрация и кэширование трафика**, перейти в секцию **Настройки фильтрации и анализа трафика пользователей** и раскрыть группу параметров **HTTPS**. Задать значения следующих параметров:

    - **Путь к хранилищу ключей** – **/opt/dozor/skvt/var/lib/<wpN>.jks**
    - **Пароль к хранилищу ключей** – пароль.
    - **Общее имя сертификата** – 1.

21. Перезапустить сервис **skvt-wizor**, выполнив в CLI следующие команды:

    # /opt/dozor/bin/shell

    # dsctl restart skvt-wizor

6.12.2. Настройка хранилища сертификатов Windows для Mozilla Firefox

Браузер Mozilla Firefox по умолчанию использует собственное (не стандартное) хранилище сертификатов Windows. Процедура ручного добавления сертификатов Windows на АРМ пользователей, использующих этот браузер, как и процедура ручной настройки каждого браузера для использования стандартного хранилища, может быть весьма трудоёмкой. Поэтому рекомендуется автоматически настроить браузеры пользователей с помощью js-скрипта, распространяемого механизмом Group Policy в домене. Для этого необходимо выполнить следующие действия:

1. Создать файл скрипта с именем **Enable sec-enterprise_roots.js** и записать в него следующую строку:

   ```
   pref ("security.enterprise_roots.enabled", true);
   ```

2. С помощью Group Policy распространить полученный скрипт по АРМ пользователей, использующих Mozilla Firefox. Путь, по которому должен быть размещён скрипт (в зависимости от разрядности ОС АРМ):

- **C:\Program Files\Mozilla Firefox\defaults\pref**
- **C:\Program Files(x86)\Mozilla Firefox\defaults\pref**

При запуске браузера его конфигурация будет обновлена. Проверить, что браузер настроен правильно, можно введя в адресной строке **about:config** и выполнив поиск по подстроке **roots**. Параметр **security.enterprise_roots.enabled** должен иметь значение **true**.

6.13. Выпуск сертификата организации для web-интерфейса

Если в организации имеется собственный УЦ, можно использовать его сертификат для установления соединения с GUI Solar webProxy. Для выпуска сертификата организации необходимо выполнить следующие действия на master-узле Solar webProxy:

1. Открыть CLI и перейти во временный каталог (например, **/var/tmp/**), выполнив команду:

   # cd /var/tmp

2. **# openssl genrsa -out wp.key -aes256 2048**

   Во время выполнения команды система потребует назначить пароль для ключа. Следует ввести пароль и запомнить его. После ввода необходимо подтвердить выбранный пароль.

3. Создать в текущем каталоге файл с именем **openssl.cnf** и записать в него следующие данные:

```
[ req ]
req_extensions = v3_req
distinguished_name = req_distinguished_name
promt=yes
[ req_distinguished_name ]
countryName                     = Country Name (2 letter code)
countryName_default             = RU

stateOrProvinceName             = State or Province Name (full name)
stateOrProvinceName_default     = Moscow

localityName                    = Locality Name (eg, city)
localityName_default            = Moscow

0.organizationName              = Organization Name (eg, company)
0.organizationName_default      = Organization

organizationalUnitName          = Organizational Unit Name (eg, section)
organizationalUnitName_default  = Dept

commonName                      = Common Name (eg, your name or your
server\'s hostname)
commonName_default              = proxy.org.com

emailAddress                    = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
```

```
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

Выделенные жирным значения параметров следует заменить на актуальные значения в организации:

- **countryName_default** – двухбуквенный код страны.
- **stateOrProvinceName_default** – регион.
- **localityName_default** – город.
- **organizationName_default** – название организации.
- **organizationalUnitName_default** – название подразделения, департамента и т. д.
- **commonName_default** – FQDN master-узла.
- **emailAddress_default** – контактный адрес электронной почты организации.
- **DNS.0** – FQDN master-узла.
- **IP.0** – IP-адрес master-узла.

4. Сгенерировать запрос на подпись сертификата, выполнив команду:

   ```
   # openssl req -new -key wp.key -out name.csr -config openssl.cnf
   ```

   В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверить используемый алгоритм шифрования. Для этого следует открыть программу **Командная строка** от имени администратора и выполнить в ней следующую команду:

   ```
   certutil - getreg ca \ csp \ CNGHashAlgorithm
   ```

   Если значение параметра **REG_SZ** равно **SHA1**, необходимо выполнить следующие команды:

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

   net stop CertSvc && net start CertSvc
   ```

6. Перевыписать корневой сертификат и перезапустить службу Certificate Services, выполнив следующие команды:

   ```
   certutil -renewCert ReuseKeys

   net stop CertSvc && net start CertSvc
   ```

7. Зайти на портал УЦ Windows.

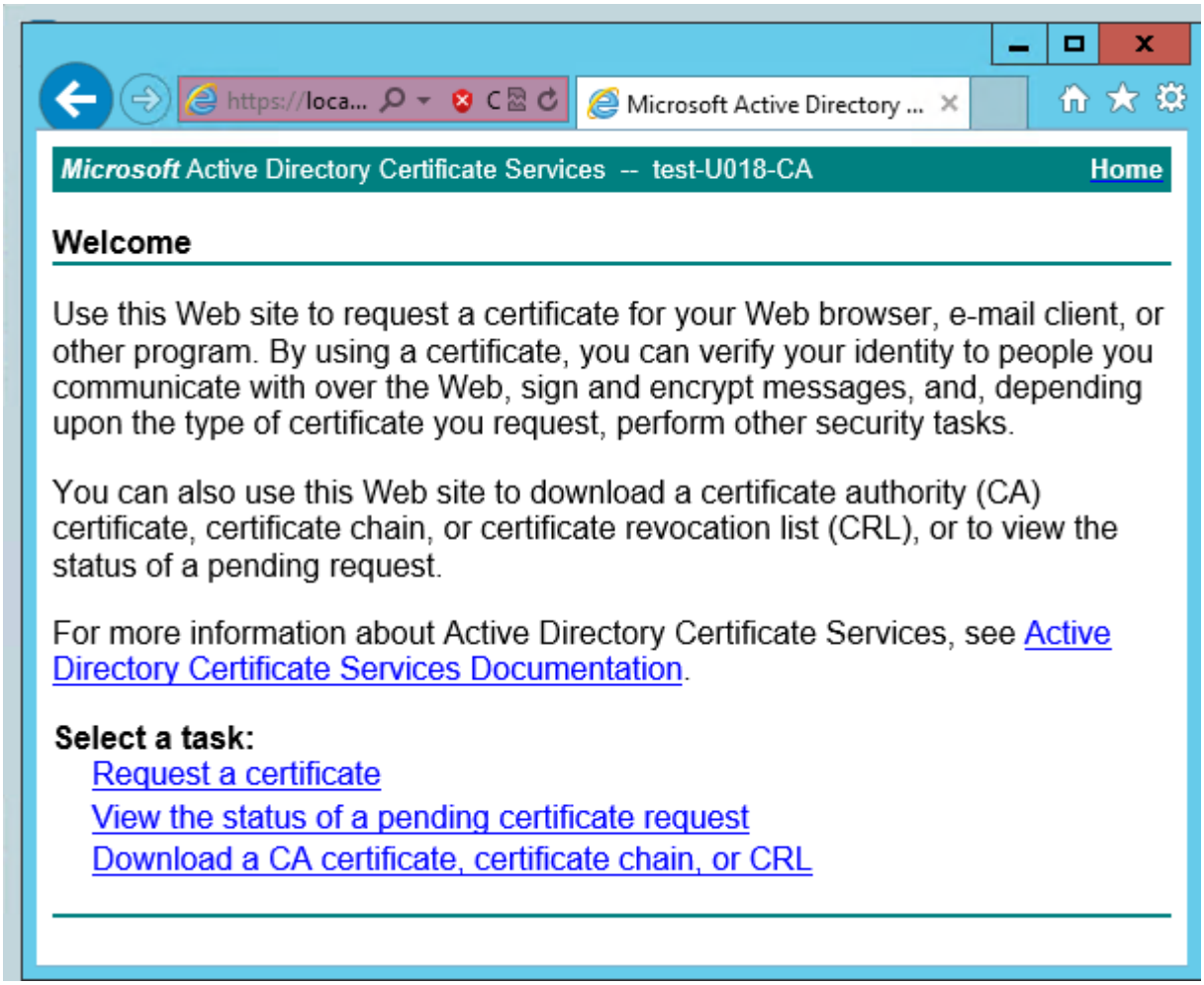

Рис. 6.18. Экран приветствия УЦ Windows

8. Нажать **Request a certificate**.

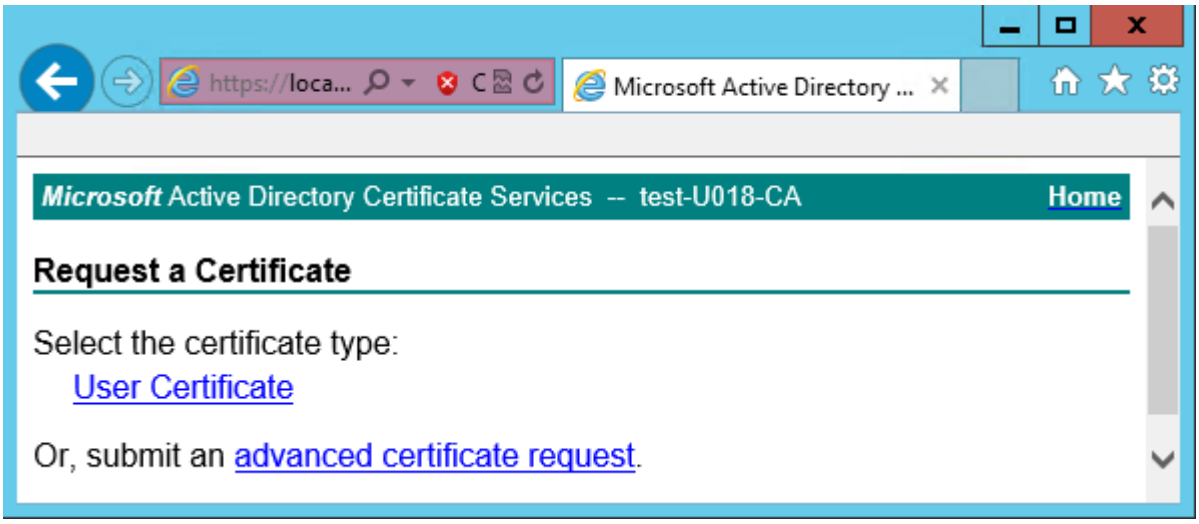

Рис. 6.19. Экран запроса сертификата

9. Нажать **advanced certificate request**.

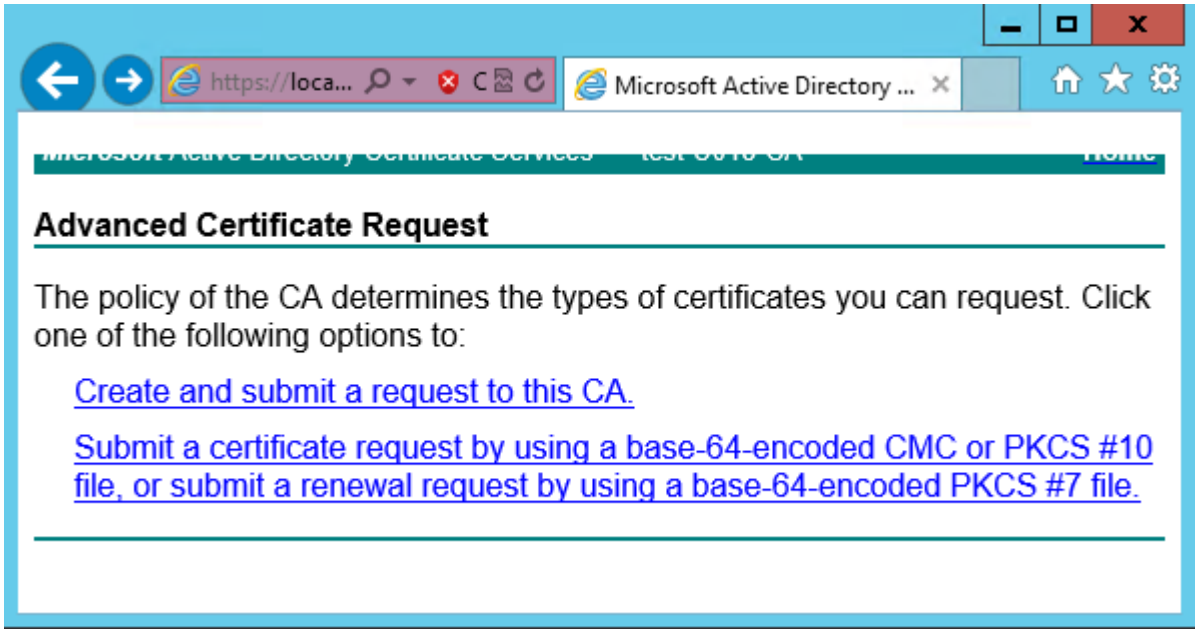

Рис. 6.20. Экран особого запроса сертификата

10. Нажать **Submit a certificate request by using...**.

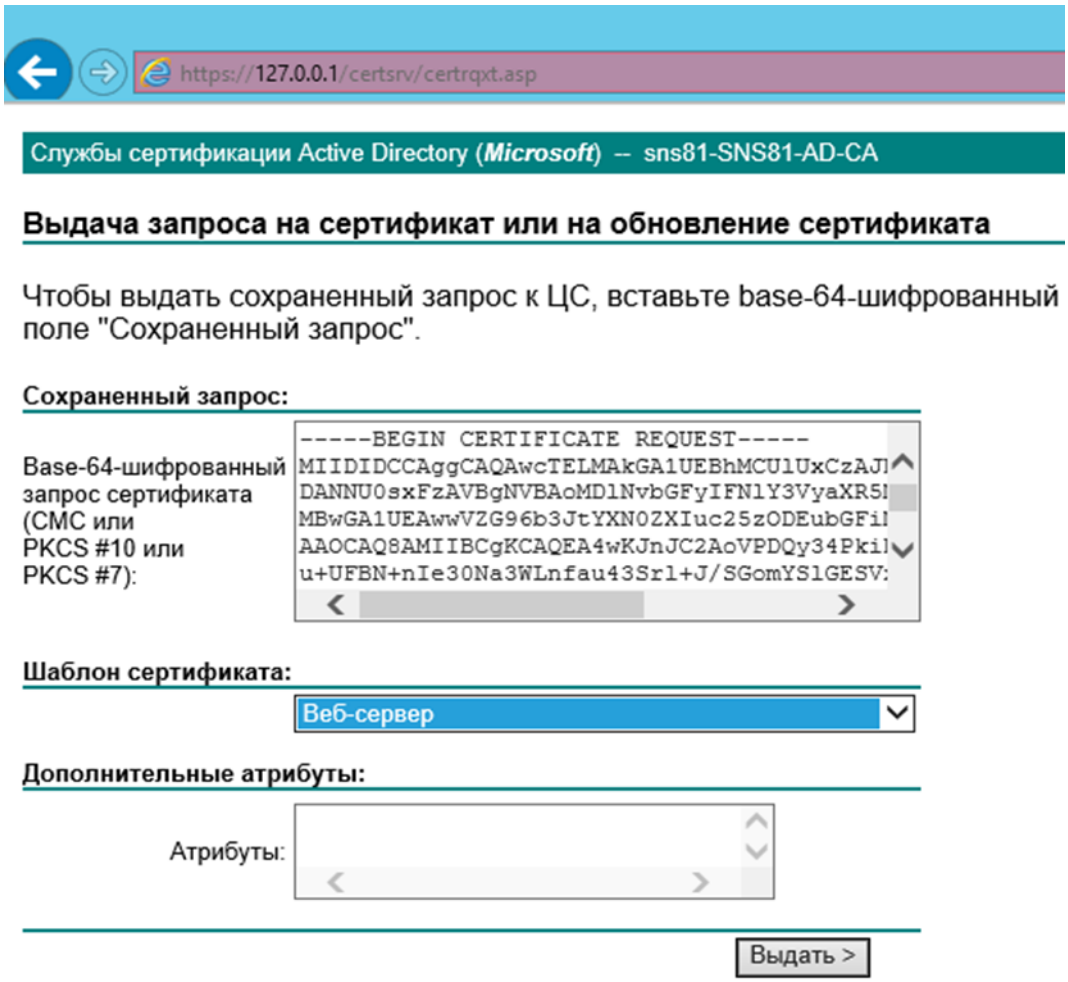

Рис. 6.21. Экран атрибутов сертификата

11. Выбрать шаблон сертификата **Веб-сервер** и вставить в поле **Base-64** содержимое файла, созданного на шаге 4. Нажать **Выдать**.

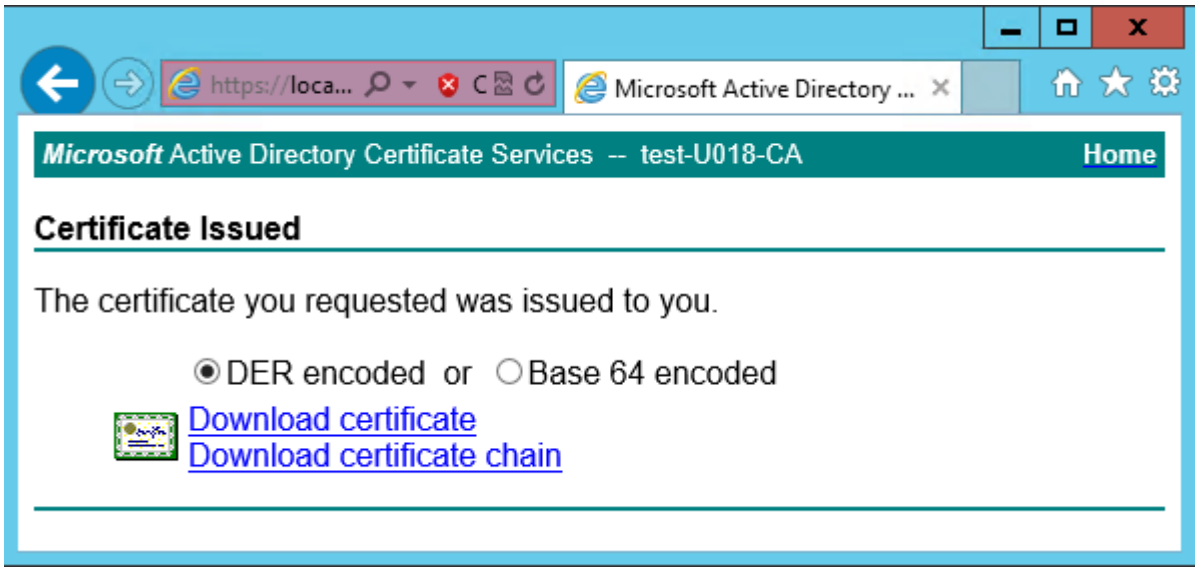

Рис. 6.22. Экран выдачи сертификата

12. Нажать **Download certificate**. Сохранить файл сертификата с именем **`wp.cer`** во временный каталог, выбранный в шаге 1.

13. Перейти на главную страницу портала УЦ и нажать **Download a CA certificate, certificate chain or CRL**. Сохранить сертификат УЦ с именем **`ca.cer`** в тот же каталог.

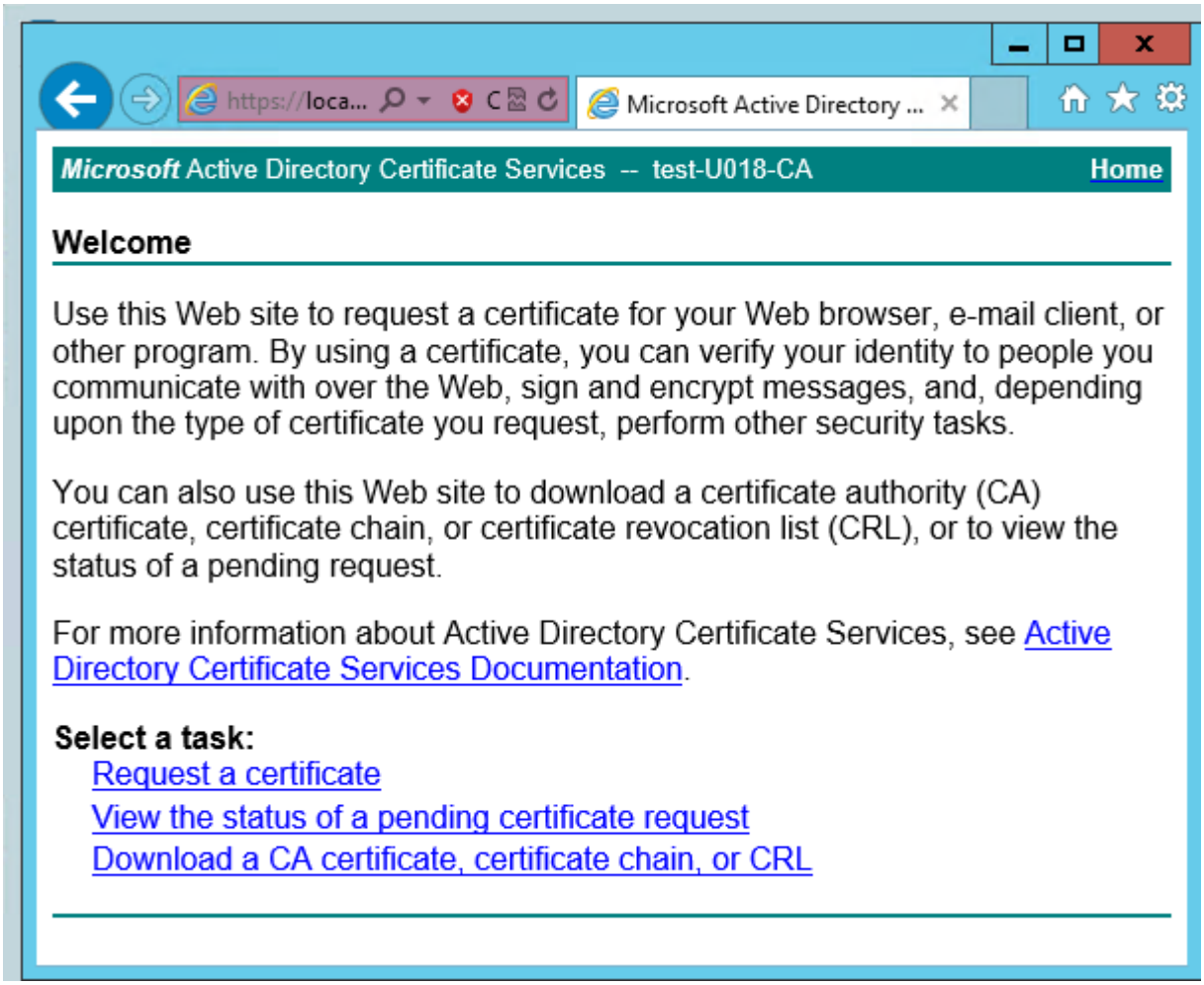

Рис. 6.23. Экран приветствия УЦ Windows

14. Вернуться в CLI Solar webProxy, перейти в выбранный временный каталог и сконвертировать загруженные сертификаты в формат PEM, выполнив команды:

```
# openssl x509 -inform der -in wp.cer -out wp.pem

# openssl x509 -inform der -in ca.cer -out ca.pem
```

15. Объединить сертификаты и ключ в сертификат pkcs12, выполнив команду:

```
# openssl pkcs12 -export -out wp.p12 -inkey wp.key -in wp.pem -
certfile ca.pem
```

Во время выполнения команды система потребует ввести пароль.

16. Импортировать Java-хранилище сертификатов, выполнив команду вида:

```
# keytool -importkeystore -deststorepass <password> -destkeypass
<password> -destkeystore WEB.jks -srckeystore wp.p12 -srcstorepass
<password>
```

где **<password>** – выбранный пароль.

17. Скопировать Java-хранилище в каталог Solar webProxy, выполнив команду:

```
# cp WEB.jks /opt/dozor/skvt/var/lib/
```

18. Сменить владельца хранилища, выполнив команду вида:

```
# chown dozor:dozor /opt/dozor/etc/ssl/WEB.jks
```

19. Проверить, что сертификат находится в хранилище, выполнив команду вида:

```
# keytool -list -keystore /opt/dozor/skvt/var/lib/WEB.jks
```

О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

```
1, Jul 10, 2018, PrivateKeyEntry,
Certificate fingerprint (SHA1):
B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

20. Открыть для редактирования файл **/opt/dozor/service/skvt-play-server/run**, и внести следующие изменения (выделено жирным):

```
#!/bin/sh

SERVICE_NAME="skvt-play-server"

. ${PREFIX}/etc/env.dsctl/base

check_last_start "$SERVICE_NAME.start" 10 5

eval `${PREFIX}/bin/load-environment ${SERVICE_NAME} ${SERVICE_NAME}.scm`

export HOME=${DOZOR_HOME}

CURRENT_NODE=`node_name`
CONFIG_FILE=${CONFIG_FINAL_REPOS}/${CURRENT_NODE}/${SERVICE_NAME}/application.conf
SSL_CONFIG="-J-Djavax.net.ssl.trustStore=/opt/dozor/etc/ssl/bus.jks"
SSL_WEB="-Dhttps.keyStore=/opt/dozor/skvt/var/lib/WEB.jks -
Dhttps.keyStorePassword=<password>"
REAL_PORT=8443
COMMAND="${PREFIX}/${SERVICE_NAME}/bin/skvt-server $SSL_CONFIG $SSL_WEB \
                                                    -J-Xmx256m \
                                                  -Dpidfile.path=/dev/null
 \
                                                 -Dhttps.port=${REAL_PORT}
 \
                                                    -Dhttp.port=8080 \
                                                    -Dfile.encoding=UTF-8
\

-Dconfig.file=$CONFIG_FILE"

iptables -D PREROUTING -t nat -d `hostname --ip-address` -p tcp --dport
${HTTPS_PORT} -j REDIRECT --to-port ${REAL_PORT} 2> /dev/null || /bin/true
iptables -I PREROUTING -t nat -d `hostname --ip-address` -p tcp --dport
${HTTPS_PORT} -j REDIRECT --to-port ${REAL_PORT}

chown ${DOZOR_USER} ${PREFIX}/${SERVICE_NAME}/conf
```

```
exec 2>&1
exec ${PREFIX}/bin/setuidgid ${DOZOR_USER} ${COMMAND}
```

где **<password>** – пароль к хранилищу ключей.

21. Перезапустить сервис **skvt-play-server**, выполнив в CLI следующие команды:

```
# /opt/dozor/bin/shell

# dsctl restart skvt-play-server
```

6.14. Настройка шифрования HTTP-соединений

Для защиты локального трафика от прослушивания и MITM-атак при обращении к ресурсам сети Интернет по протоколу HTTP используется TLS-порт Solar webProxy – 2443.

Для АРМ, использующих TLS-порт, все передаваемые данные на участке клиент-прокси шифруются. При установлении TLS-соединения браузер АРМ проверяет сертификат Solar webProxy, и соединение устанавливается только при наличии доверенного сертификата. Соединение на участке прокси-назначение осуществляется в обычном режиме, шифрование не выполняется.

Для работы TLS-порта требуется следующее:

1. Solar webProxy должен обладать сертификатом, подписанным доверенным УЦ. Работа с самоподписанными сертификатами не поддерживается. Можно использовать УЦ организации, в этом случае необходимо настроить Solar webProxy на использование настроенного системным администратором ключа и сертификата (см. раздел 6.12.1). Системный администратор должен добавить УЦ, подписавший ключ Solar webProxy в список доверенных у пользователей АРМ.

   Solar webProxy по умолчанию создаёт свой УЦ и сертификат. Сертификат и ключ УЦ Solar webProxy находятся в файле **/opt/dozor/skvt/var/lib/authority.jks**. Сертификат можно экспортировать с помощью следующей команды:

   ```
   keytool --exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias ca
   ```

   Полученный сертификат следует добавить в список доверенных на АРМ, использующих TLS-порт (в случае выбора УЦ Solar webProxy).

2. Настройка прокси в браузере должна быть выполнена с помощью PAC-файла, поскольку через обычную конфигурацию такая настройка не поддерживается. В настройке прокси требуется использовать FQDN Solar webProxy. Задача создания PAC-файла ложится на системного администратора организации (см. раздел 6.15).

3. Работа TLS-порта поддерживается только для браузеров Mozilla Firefox и Google Chrome и только для протокола HTTP.

6.15. Настройка Proxy auto-config

Для настройки Proxy auto-config необходимо выполнить следующие действия (пример для двух фильтров):

1. На master-узле установить пакет **nginx**, выполнив команды:

   ```
   # yum install epel-release

   # yum install nginx
   ```

2. В каталоге **/usr/share/nginx/html/** создать файл с именем **proxy.pac** и записать в него следующее:

```
function FindProxyForURL(url, host) {
    var myIp = myIpAddress();
    var ipBits = myIp.split(".");
    var mySeg = parseInt(ipBits[3]);
   if (isPlainHostName(host) || shExpMatch(host, "^10\.\d+\.\d+\.\d+$/"))

    {
          return "DIRECT";
    }
    if((mySeg % 2) == 0)
    {
        return "PROXY 10.10.0.1:2270; PROXY 10.10.0.2:2270";
    } else
    {
        return "PROXY 10.10.0.2:2270; PROXY 10.10.0.1:2270";
    }
}
```

   Вместо **10.10.0.1:2270** и **10.10.0.2:2270** следует подставить актуальные IP-адреса и порты, на которых фильтры ожидают соединения с АРМ пользователей.

3. Открыть для редактирования файл **/etc/nginx/mime.types** и добавить в блок **types** строку **application/x-ns-proxy-autoconfig pac;** как показано на рисунке:

Рис. 6.24. Файл /etc/nginx/mime.types

   Сохранить и закрыть файл.

4. Открыть для редактирования файл **/etc/nginx/conf.d/default**. В строках, начинающихся с **listen**, указать порт, доступный пользователям (например, 8080). Этот порт не может совпадать с портом, используемым сервисом skvt-wizor (по умолчанию 2270).

5. Выполнить команды:

```
# chkconfig nginx on

# service nginx start
```

6. Проверить правильность настройки, введя в браузер АРМ пользователя адрес **http://<master-ip>:<port>/proxy.pac**, где **<master-ip>** – IP-адрес master-узла Solar webProxy, а **<port>** – значение, заданное в шаге 4. Если настройка выполнена правильно, то начнётся загрузка файла **proxy.pac**. Если настройка выполнена правильно, то следует записать в настройки браузеров АРМ пользователей этот PAC-файл.

6.16. Редактирование политики

Процедуры создания, редактирования, применения и отладки политики фильтрации трафика описаны в документе *Руководство администратора безопасности*.

6.17. Рекомендации по назначению ролей

В кластере Solar webProxy рекомендуется распределять роли по узлам следующим образом:

- Если master-узел хранит основное хранилище Досье (то есть не в подчинённом режиме), назначить ему роль **Центральное файловое хранилище**.

- slave-узлу (узлам) назначить роль **Фильтр HTTP-трафика** (для применения политики фильтрации трафика), роли **Сервер NTLM-аутентификации** или **Сервер Kerberos-аутентификации** (в зависимости от используемого типа аутентификации пользователей, см. раздел 6.5.3), и роль **Анализатор трафика** (если политика фильтрации трафика предусматривает возможность блокировки соединения в зависимости от типа содержимого).

- При наличии достаточного количества оперативной памяти, slave-узлам с ролью **Фильтр HTTP-трафика** следует также назначить роль **Сервис репликации Досье на подчинённых узлах**. Чтобы оценить требуемый объём памяти, следует выполнить следующую команду:

  ```
  curl -k -H "Content-type: application/json" --key /opt/dozor/etc/ssl/bus.key
   --cert /opt/dozor/etc/ssl/bus.pem --data-binary '{}'
  https://<hostname>:2269/persons/info?groups=true\&addresses=true\&department=true\&ctl=true
   | wc -c
  ```

  Полученное значение умножить на 10 – получится требуемое значение объёма памяти в байтах. Необходимо его перевести в мегабайты и записать в качестве значения параметра конфигурации **Максимальное количество оперативной памяти** в разделе **Конфигурации > Досье > Настройки сервиса репликации Досье на подчиненных узлах**. Если полученное значение оказалось меньше значения параметра по умолчанию, то уменьшать значения параметра не нужно.