Использование протокола Kerberos для авторизации пользователей прокси-сервера Squid на базе pfSense

М. К. Чернышов, email: mkch69@gmail.com

Воронежский государственный университет

Аннотация. *В данной работе рассматриваются вопросы применения механизма аутентификации Kerberos для получения доступа в Интернет пользователями корпоративных сетей с использованием прокси-сервера Squid на базе маршрутизатора pfSense.*

Ключевые слова: *компьютерные сети, сетевой протокол аутентификации Kerberos, служба каталогов операционных систем семейства MS Windows Active Directory, прокси-сервер Squid, программный маршрутизатор pfSense.*

Введение

Как правило, пользователям корпоративных сетей при получении авторизованного доступа в Интернет приходится использовать как минимум две пары («имя-пароль») учетных данных, одна из которых необходима для авторизации в сети, а другая – непосредственно для получения доступа в Интернет с заранее определенным для каждого пользователя набором прав, что на практике весьма неудобно. С помощью сетевого протокола аутентификации Kerberos, широко используемого в доменных сетях на основе Microsoft Active Directory, процесс авторизации пользователей при получении доступа в Интернет может быть совмещен с процедурой авторизации в компьютерной сети предприятия.

Данная работа посвящена описанию пошаговой инструкции настройки механизма Kerberos при использовании довольно популярного прокси-сервера Squid, установленного в качестве дополнительного пакета программного маршрутизатора pfSense [1]. При этом необходимо отметить, что несмотря на достаточное количество описанных, ранее полученных, схожих результатов (например, [2-4]), ни один их них не приводил к решению проблемы целиком.

Процесс настройки и внедрения механизма авторизации с помощью протокола Kerberos состоит из трех этапов:

– Создание на контроллере домена файла ключей с целью использования в дальнейшем протокола аутентификации Kerberos;

– Адаптация маршрутизатора pfSense к использованию механизма Kerberos-авторизации;

– Настройка прокси-сервера Squid для предоставления доступа в Интернет различным категориям пользователей домена, обладающим тем или иным набором прав.

1. Создание файла ключей Kerberos

Команда для создания файла ключей выполняется на контроллере домена (в рассматриваемом примере – *dc01.mydomain.ru*) и выглядит следующим образом:

```
ktpass.exe /princ HTTP/pfsense.mydomain.ru@MYDOMAIN.RU
/mapuser pfsense$@MYDOMAIN.RU /crypto RC4-HMAC-NT /ptype
KRB5_NT_PRINCIPAL /pass +rndpass /kvno 4 /out C:\krb5.keytab
```

Рассмотрим каждый параметр по отдельности:

1. **/princ HTTP/pfsense.mydomain.ru@MYDOMAIN.RU**

SPN (Service Principal Name) запись [5] *HTTP/pfsense.mydomain.ru* используется в Squid для авторизации с помощью протокола Kerberos. Соответственно, для компьютера домена, указанного в ключе */mapuser PFSENSE$@MYDOMAIN.RU* в его доменной записи структуры каталогов Active Directory этот примитив должен был прописан. Делается это с помощью следующей команды:

```
setspn -S HTTP/pfsense.mydomain.ru PFSENSE
```

Здесь *PFSENSE* – имя компьютера с установленным pfSense. К моменту выполнения указанной команды этот компьютер должен быть добавлен в Active Directory, а также в прямой и обратной зонах DNS-сервера должны быть сделаны соответствующие записи. Проверить правильность создания SPN-записи можно следующей командой:

```
setspn -L PFSENSE
```

Результат должен быть примерно таким:

```
Зарегистрирован ServicePrincipalNames для
CN=PFSENSE,CN=Computers,DC=mydomain,DC=ru:
        HTTP/pfsense.mydomain.ru
```

Отметим, что в случае, если выполнение команды создания SPN-записи осуществляется впервые, этих действий достаточно. Однако, если происходит повторная генерация ключей, необходимо убедиться в том, что упоминание данной записи удалено из параметров всех других учетных записей компьютеров и пользователей Active Directory.

Для начала можно дать команду для проверки уникальности всех SPN-записей в домене:

```
setspn -X
```

Команда должна сообщить, что повторов не было найдено.

Кроме того, в случае, если ранее данная SPN-запись использовалась для другого компьютера или пользователя домена, в свойствах этой записи необходимо вручную очистить параметры *userPrincipalName* и *servicePrincipalName.* Удобнее всего это сделать с помощью редактора атрибутов самой учетной записи Active Directory.

2. **/mapuser PFSENSE$@MYDOMAIN.RU**

Замечание. Согласно рекомендациям, сформулированным в [4], в процессе настройки осуществлялась попытка привязать ключи к учетной записи специально выделенного пользователя домена (*pfSenseUser*), а не компьютера, однако в итоге Squid не смог распознать ни одного алгоритма шифрования, несмотря на попытки соответствующего изменения свойств этой учетной записи. В итоге ключи генерируются для учетной доменной записи компьютера *PFSENSE* (имя компьютера в Web-интерфейсе pfSense и в настройках Active Directory должно быть одним и тем же – с точностью до использования прописных и строчных букв).

3. **/crypto RC4-HMAC-NT**

Попытка использования различных алгоритмов шифрования с помощью */crypto ALL* (например, [2]) не увенчалась успехом – в этом случае ни компьютер *PFSENSE,* ни пользователь *pfSenseUser* не могли в дальнейшем авторизоваться непосредственно в Squid. В Web-интерфейсе появлялась ошибка *"bad encryption type"*. Эта же ошибка возникала при использовании ключа */mapuser pfsenseuser* (см. описание ключа */mapuser*) даже при "правильном", указанном выше алгоритме шифрования.

4. **/pass +rndpass**

При попытке привязать SPN-запись к доменной учетной записи пользователя *pfSenseUser* здесь нужно было бы указать пароль этой учетной записи. В данном случае пароль учетной записи компьютера *PFSENSE* генерируется случайным образом.

Замечание. Отметим, что в случае, если с используемой доменной записью в Active Directory будут производиться какие-либо манипуляции (удаление/восстановление, изменение характеристик), старый пароль записи будет утерян, и весь процесс генерации ключей придется осуществлять заново, с нуля.

5. **/kvno 4**

По идее, этот ключ вроде бы указывать нет необходимости, однако его пришлось использовать явным образом из-за возникновения ошибок уже непосредственно на стадии проверки работоспособности прокси-сервера Squid. Дело в том, что при каждой попытке заново сгенерировать ключи для одной и той же доменной учетной записи на единицу увеличивается атрибут *msDS-KeyVersionNumber* этой учетной записи в Active Directory. В итоге при попытке использования новой версии файла ключей на компьютере PFSENSE прокси-сервер Squid может выдавать сообщение об ошибке

```
Cannot find key for HTTP/pfsense.mydomain.ru@MYDOMAIN.RU kvno
xxx in keytab
```

В этом случае "внутренняя" версия ключей Squid (*xxx*) может оказаться не совпадающей с той версией ключей, которые были получены в результате повторного выполнения команды *ktpass.exe* – именно в этой ситуации попытка явным образом указать "правильную" версию ключей при их создании помогает избавиться от данной ошибки.

Замечание. Нужно отметить, что величина параметра *msDS-KeyVersionNumber* не зависит от значения параметра в ключе /kvno – при каждом повторном запуске команды *ktpass.exe* для одной и той же учетной записи значение параметра по-прежнему будет увеличиваться на единицу.

Отметим, что в настоящий момент значения параметров KVNO в доменной учетной записи *PFSENSE* и непосредственно на прокси-сервере Squid вручную сделаны одинаковыми. Имеет ли это какое-либо значение – пока непонятно.

2. Установка файла ключей Kerberos на компьютер PFSENSE

После создания файла *C:\krb5.keytab* на контроллере домена его необходимо скопировать/перенести на компьютер *PFSENSE*. Для этого можно, например, использовать FTP-клиент FileZilla.

Сам процесс размещения файла на компьютере *PFSENSE*, по сути, состоит из нескольких команд, собранных в небольшой скрипт, выполняемый непосредственно в консоли данного компьютера. Текст данного скрипта приведен в листинге 1.

Листинг 1

Скрипт для размещения файла ключей на pfSense

```
#!/usr/local/bin/bash
rm -rf /etc/krb5.keytab
ktutil copy /root/krb5.keytab /etc/krb5.keytab
chown squid:squid /etc/krb5.keytab
chmod 0400 /etc/krb5.keytab
```

```
ls -al /etc/krb5.keytab
ktutil list
```

В конечном итоге файл должен располагаться по следующему пути: */etc/krb5.keytab*, однако к этому моменту должны быть исправлены права доступа к этому файлу, поэтому вначале файл переносится с контроллера домена в каталог */root* с тем же именем, а далее с помощью утилиты *ktutil* копируется в каталог */etc*. После этого назначается хозяин файла (*squid:squid*) и настраиваются права доступа к нему (*0400*).

С помощью команды

```
ktutil list
```

отображается содержимое файла *krb5.keytab* (пример вывода данной команды представлен в листинге 2):

Листинг 2

Пример содержимого файла ключей

```
FILE:/etc/krb5.keytab:

Vno     Type                    Principal               Aliases
 4 arcfour-hmac-md5 HTTP/pfsense.mydomain.ru@MYDOMAIN.RU
```

На следующем шаге проверяется работоспособность механизма Kerberos. После выполнения команды

```
kinit -k HTTP/pfsense.mydomain.ru
```

не должно появляться сообщений об ошибках! В этом случае с помощью команды *klist* на экран будет выведена информация о сформированных билетах на получение доступа к домену, представленная в листинге 3.

Отметим, что в случае появления сообщений о каких-либо ошибках на данном этапе придется возвращаться к разделу 1. К сожалению, скорее всего, это говорит о возникновении проблем на стадии формирования/очистки SPN-записей в домене.

Листинг 3

Информация о полученном билете на доступ к pfSense

```
Credentials cache: FILE:/tmp/krb5cc_0
        Principal: HTTP/pfsense.mydomain.ru@MYDOMAIN.RU

  Issued                Expires
Dec 9 09:16 2022 Dec 9 19:16 2022

         Principal
krbtgt/MYDOMAIN.RU@MYDOMAIN.RU
```

Последняя проверка с помощью команды

```
/usr/local/libexec/squid/negotiate_kerberos_auth_test
pfsense.mydomain.ru
```

позволяет получить окончательный ответ на вопрос, нормально ли функционирует механизм Kerberos. С помощью этой команды тестируется формирование прокси-сервером Squid токена непосредственно для компьютера *PFSENSE*. Эта команда должна выполняться только после успешного выполнения команды *kinit*. После получения токена удаление всех билетов, полученных во время тестирования работы механизма, осуществляется с помощью команды *kdestroy*.

3. Настройка Squid

Стоит отметить, что многие рекомендации, связанные с настройкой Squid, встречающиеся в Интернете, как правило, не имеют привязки к особенностям использования Squid в качестве пакета pfSense. В частности, при работе с pfSense не требуется создание конфигурационного файла */etc/krb5.conf*. Кроме того, как уже было сказано ранее, расположение файла с ключами для работоспособности Kerberos фиксировано – файл по умолчанию расположен по пути */etc/krb5.keytab*.

Перейдем непосредственно к процедуре настройки Kerberos-аутентификации в Squid, осуществляемой с помощью механизма Negotiate. Для этого, используя Web-интерфейс pfSense, на основной странице, содержащей настройки Squid, в окне Custom Options (Before Auth) *Расширенных опций* Squid необходимо разместить набор команд, представленный в листинге 4.

В этом случае пользователи домена, входящие в группу *SQUID_Full* (расположенную в домене по адресу *OU=Service,OU=Groups,DC=mydomain,DC=ru*), получат расширенные права доступа в Интернет по сравнению с пользователями, входящими в группу *SQUID_Common*. Непосредственное описание конкретных прав доступа в Интернет, предоставляемых различным группам пользователей, оставим за пределами данной работы.

Листинг 4

Вариант настройки прокси-сервера Squid с использованием механизма Kerberos

```
# Kerberos authorization
auth_param negotiate program
/usr/local/libexec/squid/negotiate_kerberos_auth -d -r -s
HTTP/pfsense.mydomain.ru@MYDOMAIN.RU -t none
```

```
auth_param negotiate children 20
auth_param negotiate keep_alive on

# Basic authorization (login and password)
auth_param basic program
/usr/local/libexec/squid/basic_ldap_auth -R -v 3 -b
"dc=mydomain,dc=ru" -D pfSenseUser@mydomain.ru -w XYZXYZXYZ -f
"sAMAccountName=%s" -u cn -P dc01.mydomain.ru

auth_param basic children 20
auth_param basic realm Mydomain Proxy Authentification
auth_param basic credentialsttl 60 minutes

# Check of belonging of the user to the required group
external_acl_type ldap_groups ttl=30 grace=15 %LOGIN
/usr/local/libexec/squid/ext_ldap_group_acl -R -v 3 -b
"dc=mydomain,dc=ru" -D pfSenseUser@mydomain.ru -w XYZXYZXYZ -f
"(&(objectclass=user)(sAMAccountName=%v)(memberOf=CN=%a,
OU=Service,OU=Groups,DC=mydomain,DC=ru))" -P dc01.mydomain.ru

# Connection to groups for distribution of access to the sites
acl SQUID_Full external ldap_groups SQUID_Full
acl SQUID_Common external ldap_groups SQUID_Common
```

Проверка принадлежности того или иного пользователя к определенной группе осуществляется доменным пользователем *pfSenseUser* на контроллере домена *dc01.mydomain.ru*. В соответствующих командах указаны учетные данные данного пользователя, IP-адрес и имя контроллера домена, осуществляющего проверку.

Пользователям, не прошедшим процедуру авторизации с помощью механизма Negotiate, будет предоставлена дополнительная возможность ввести свои учетные данные в браузере при осуществлении попытки открыть ту или иную страницу в Интернете. При этом правильность введенных данных в рассматриваемом случае также будет проверяться доменным пользователем *pfSenseUser*.

Заключение

Несколько лет назад использование механизма Kerberos-аутентификации применительно к прокси-серверу Squid, установленному в качестве пакета программного маршрутизатора pfSense, прошло апробацию в виртуальной среде с помощью виртуальной сетевой лаборатории EVE-NG, после чего автором было успешно внедрено в производство на одном из предприятий города Воронежа. Однако в связи с недавним внесением изменений в сетевую инфраструктуру предприятия возникла необходимость корректного

перезапуска используемого механизма. Итогом проделанной работы является уточненное и углубленное пошаговое описание алгоритма Kerberos-аутентификации, изложенное в данной статье.

Список литературы

1. pfSense – Open Source Security [Электронный ресурс] : сайт. – Режим доступа : https://www.pfsense.org/
2. Записки IT специалиста [Электронный ресурс] : сайт. – Режим доступа : https://interface31.ru/tech_it/2015/06/nastraivaem-squid-dlya-raboty-s-active-directory-chast-2-kerberos-autentifikaciya.html
3. Аутентификация и авторизация squid (Basic, Digest, NTLM, Negotiate) [Электронный ресурс] : сайт. – Режим доступа : https://www.k-max.name/linux/avtorizaciya-autentifikaciya-squid/
4. Авторизация на Squid через Active Directory [Электронный ресурс] : сайт. – Режим доступа : https://www.dmosk.ru/miniinstruktions.php?mini=squid-ad
5. Создание SPN и Keytab файла [Электронный ресурс] : сайт. – Режим доступа : https://www.altlinux.org/Создание_SPN_и_Keytab_файла