УДК 004.056.53
ББК 22.127
К 38

Киздермишов А.А.
Кандидат физико-математических наук, доцент кафедры автоматизированных систем обработки информации и управления инженерно-физического факультета Адыгейского государственного университета, Майкоп, e-mail: Askhad_75@rambler.ru
Киздермишова С.Х.
Кандидат социологических наук, доцент кафедры экологии и защиты окружающей среды экологического факультета Майкопского государственного технологического университета, Майкоп, e-mail: Suliet@rambler.ru

Установка и настройка специального режима Squid (ssl-bump) на Ubuntu 12.04 TLS

(Рецензирована)

Аннотация. *Рассмотрены вопросы, связанные с вводом в эксплуатацию специального режима Squid (ssl-bump), даны рекомендации для администраторов ИТ с низким уровнем подготовки по установке и настройке специального режим Squid (ssl-bump) на Ubuntu 12.04 TLS, подготовке прокси-сервера для установки антивирусной защиты и анализаторов трафика.*

Ключевые слова: *Squid, HTTPS, Linux, Ubuntu, DLP-системы, антивирусная защита, фильтрация трафика.*

Kizdermishov A.A.
Candidate of Physics and Mathematics, Associate Professor of the Department of Automated Systems of Processing Information and Control Engineering-Physics Faculty, Adyghe State University, Maikop, ph. (8772) 593911, e-mail: Askhad_75@rambler.ru
Kizdermishova S.Kh.
Candidate of Sociology, Associate Professor of Department of Ecology and Environmental Protection of Environmental Faculty, Maikop StateUniversity of Technology, Maikop, e-mail: Suliet@rambler.ru

Installing and configuring a special Squid mode (ssl-bump) on Ubuntu 12.04 TLS

Abstract. *The paper deals with the issues associated with the commissioning of a special Squid mode (ssl-bump), recommendations are given for Administrators with a low level of training in installation and configuration of special Squid mode (ssl-bump) on Ubuntu 12.04 TLS, and preparation of the proxy server to install antivirus protection and traffic analyzers.*

Keywords: *Squid, HTTPS, Linux, Ubuntu, DLP systems, antivirus protection, traffic filtering.*

По состоянию на сегодняшний день программный пакет Squid (далее Squid), реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и HTTPS (при условии выполнения соответствующих настроек), широко применяется для обеспечения выхода в Интернет из локальных сетей небольших офисов, принадлежащих как государственным учреждениям, так и коммерческим организациям. Популярность Squid обусловлена несколькими факторами, основным из которых является то, что пакет бесплатный, а также не требует дорогой аппаратной платформы и относительно прост в настройке. В связи с этим целесообразно рассмотреть вопросы, связанные с фильтрацией HTTPS трафика в случае применения Squid. В данной статье рассматриваются только средства контроля трафика, межсетевые экраны – тема для отдельной статьи. Надеемся, что наша статья будет полезна администраторам ИТ небольших офисов для тонкой настройки серверов Squid, без которой невозможно обеспечить эффективную фильтрацию и антивирусную защиту трафика.

В первую очередь следует определиться с технологией, которая будет применяться для обеспечения анализа трафика. Как известно, благодаря протоколу HTTPS стало возможным в какой-то мере защитить личные данные пользователей Интернета. Однако, с другой стороны, в случае если пользователь работает в офисе, а не находится в публичной сети (кафе, аэропорту, метро и т.п.), протокол HTTPS не позволяет контролировать входящую и исходящую информацию из корпоративной сети, так как механизм передачи данных зашифрован. Речь идет не только о возможной утечке информации, например, через социальные сети, но и

об антивирусной защите. В частности, разработанное лидерами отечественного рынка антивирусное программное обеспечение «Dr.Web для Интернет-шлюзов Unix» и «Антивирус Касперского 5.5 для Proxy Server» не поддерживает проверку HTTPS трафика, так как антивирусные средства используют захват трафика через ICAP. В рассматриваемом случае проблемы безопасности можно было бы решить применением DLP систем, но для малых офисов это крайне дорогое решение [1]. Поэтому большинство экспертов для решения задачи контроля HTTPS трафика рекомендуют использовать специальный режим Squid (ssl-bump) (далее режим ssl-bump) [2].

Рассмотрим подробнее технологию режима ssl-bump. Согласно официальной документации Squid [3], режим ssl-bump может быть применен в двух вариантах: без подмены сертификата и с подменой сертификата.

Преимуществом режима ssl-bump без подмены сертификата является то, что получить доменные имена в статистике сайтов можно без угрозы конфиденциальности передаваемых данных [4]. Однако в этом случае просматривается только заголовок пакета, поэтому невозможно установить, какая именно страница была открыта, нельзя провести фильтрацию по части имени доменов, строкам запросов (регулярным выражениям), не будет работать антивирусная защита при передаче данных по протоколу HTTPS. Поэтому далее этот вариант рассматриваться не будет.

В случае применения режима ssl-bump с подменой сертификата работу Squid можно сравнить с атакой Manin the middle (MITM). Суть технологии состоит в том, что устанавливается специальная сборка Squidc поддержкой SSL, средствами которой осуществляется SSL-соединение с веб-сервером от имени клиента, инициировавшего запрос. Другими словами, Squid использует для соединения с веб-сервером сертификат, полученный с веб-сервера, а для соединения с клиентом – сертификат, созданный прокси-сервером, в котором вместо имени прокси-сервера указано имя веб-сервера, извлеченное из сертификата веб-сервера. Таким образом, со стороны клиента все выглядит как SSL-соединение с веб-сервером. Так как сертификаты, используемые для взаимодействия с клиентом, подписываются специально созданным корневым сертификатом, для работы по такой схеме необходимо выполнить настройки и на клиентских станции, и браузере, а именно добавить этот корневой сертификат в хранилище сертификатов в раздел «Доверенные корневые центры». На сегодняшний день это единственный способ полной проверки HTTPS трафика.

Теперь необходимо рассмотреть сам процесс настройки режима ssl-bump. Теме настройки режима ssl-bump с подменой сертификата посвящено множество статей, опубликованных на известных в Linux сообществе информационных ресурсах в сети Интернет. На первый взгляд решение задачи не должно вызвать сложностей даже у слабо подготовленных администраторов ИТ, им нужно просто выбрать подходящую статью и действовать так, как в ней рекомендовано. Однако комментарии к этим статьям свидетельствуют о том, что далеко не все администраторы ИТ сумели повторить результаты их авторов. Анализ комментариев к статьям и вопросов к их авторам показал, что сложности, которые испытывают администраторы ИТ, в абсолютном большинстве случаев связаны с ошибками, возникающими при сборке пакета Squid с поддержкой SSL из исходных текстов. Вторая большая группа вопросов к авторам связана с тем, что установленный Squid «не слушается» команд, привычных для администраторов ИТ, по работе со Squid, установленном из репозитория. Мы не подвергаем сомнению квалификацию и результаты авторов, на наш взгляд, ошибки связаны с тем, что для администратора ИТ с низким уровнем подготовки требуется более полное и детальное описание действий. Проблему можно решить, если скачать уже собранный пакет Squid с поддержкой SSL по ссылкам, которые приводятся в отдельных статьях. Мы не будем проводить ссылки на эти статьи, так как считаем это решение крайне опасным. Опасность заключается в том, что в этом случае вы рискуете «подарить» содержимое HTTPS трафика вашей организации автору статьи. Рекомендуем обратить внимание на статьи, в которых описано, как собрать требуемые пакеты самостоятельно одним из способов с применением команд и пакетов dpkg-buildpackage,

checkinstall, make и т.п. На наш взгляд, для администратора ИТ с низким уровнем подготовки наиболее подходящим решением является процесс установки и настройки режима ssl-bump, описанный в работе [5] для ОС CentOS. В соответствии с целью, поставленной при написании статьи, мы дополним статью [5] более полным и детальным описанием действий, а также адаптируем ее для ОС Ubuntu 12.04 TLS. Выбор Ubuntu обусловлен тем, что Ubuntu популярней, чем CentOS, а выбор релиза Ubuntu 12.04 TLS связан с тем, что это высший релиз, с которым, согласно эксплуатационной документации, протестирована корректная работа программного обеспечения «Антивирус Касперского 5.5 для Proxy Server».

Процесс настройки специального режима Squid (ssl-bump) можно представить в виде шагов.

Шаг 1. Установка операционной системы из образа «Ubuntu-12.04-server-amd64.iso». В ходе установки на этапе «Выбор программного обеспечения» необходимо выбрать следующее программное обеспечение «OpenSSHserver», «LAMPserver», «TomcatJavaserver».

После завершения установки операционной системы необходимо перейти в режим суперпользователя, применив команду «sudosu», и выполнить стандартные действия по обновлению системы в рамках установленного релиза, использовав команды:

#apt-get update

#apt-get upgrade

Проверить результат установки операционной системы можно командой

#uname -a&&lsb_release -a

В случае, если установка прошла успешно, получен результат выполнения команды:

Linux gate 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64x86_64 GNU/Linux

No LSB modules are available.

Distributor ID: Ubuntu

Description: Ubuntu 12.04.5 LTS

Release: 12.04

Codename: precise

Шаг 2. Установим пакеты, необходимые для сборки пакета SQUID с поддержкой SSL из исходных текстов:

 # apt-get installgcc g++ libssl-dev libgnutls28-devdevscriptsdebhelper dh-autoreconfcdbs

и создадим директорию для сборки и установки пакетов из исходных текстов

#mkdirmk

#cdmk

Шаг 3. Соберем и установим актуальную версию пакета openssl (здесь и далее под актуальной версией понимается последняя опубликованная на официальном репозитории стабильная версия по состоянию на дату написания статьи):

#wget www.openssl.org/source/openssl-1.0.2m.tar.gz

#tar -zxf openssl-1.0.2m.tar.gz

#cd openssl-1.0.2m

#./config shared --prefix=/opt/squid/openssl --opensslдir=/opt/squid/openssl

#make

#make install

Шаг 4. Соберем и установим актуальную версию пакета Squid:

#wget http://www.squid-cache.org/Versions/v3/3.5/squid-3.5.27.tar.gz

#tar -xf squid-3.5.27.tar.gz

#cd squid-3.5.27

#./configure

--prefix=/opt/squid

--enable-ssl# включает поддержку ssl режима

--enable-ssl-crtd #для разгрузки прокси-сервера запускает отдельный процесс для генерации сертификатов

--with-openssl #путь, куда на шаге 3 был установлен openssl

#makeall

#makeinstall

Если в завершении сборки на экране не были отображены ошибки, тогда следует выполнить команду:

#/opt/squid/sbin/squid -v

Если результат выполнения команды такой, как показано ниже,

Squid Cache: Version 3.5.27

Service Name: squid

This binary uses OpenSSL 1.0.1 14 Mar 2012. For legal restrictions on distribution see https://www.openssl.org/source/license.html

configure options: '--prefix=/opt/squid' '--enable-ssl' '--enable-ssl-crtd' '--with-openssl=/opt/squid/openssl'

то установка программного обеспечения завершена.

Шаг 5. Настройка конфигурации Squid. Целесообразно провести детальное описание настроек. Откроем файл конфигурации

#nano/opt/squid/etc/squid.conf

заменим строку

http_port 3128

на строку

http_port 3128 ssl-bump generate-host-certificates=ondynamic_cert_mem_cache_size=4MBcert=/opt/squid/etc/PCA.pem

и добавим строки:

always_direct allow all# не использовать кэш

acl broken_sites [dstdomain]# правило для исключения доменов из ssl-bump (о необходимости которого говорилось выше

ssl_bumpnonebroken_sites

Для тестирования настроек рекомендуем установить eicar.org в качестве dstdomain; это поможет в дальнейшем одновременно протестировать работоспособность установленных антивирусных средств и срабатывание исключения домена из ssl-bump; при верной настройке антивирусное средство должно блокировать закачку тестового вируса по ссылкам http://secure.eicar.org/eicar.com и https://secure.eicar.org/eicar.com; при закомментированной строке – только по ссылке http://secure.eicar.org/eicar.com. После тестирования настроек здесь необходимо подключить файл со списком доменов.

sslproxy_cert_errorallowall# разрешает обрабатывать запрос при ошибке проверки сертификата веб-сайта, является опасным, поскольку ошибка обычно подразумевает, что серверу нельзя доверять и соединение может быть небезопасным

sslproxy_flagsDONT_VERIFY_PEER# для усиления предыдущего правила; отключает проверку по списку CA по умолчанию и принимает сертификаты, издатель которых неизвестен; является опасным, поскольку ошибка обычно подразумевает, что серверу нельзя доверять и соединение может быть небезопасным

После завершения настроек две последних строки целесообразно закомментировать и настроить автоматическое обновление списков CA [6].

Далее необходимо указать режим работы ssl_bump. Существует несколько вариантов:

ssl_bumpclient-firstall – старый режим для установки соединения сначала с клиентом, затем с веб-сервером; не позволяет Squid сопоставлять SSL-сертификат сервера и работать с перехваченными SSL-соединениями, используется для прозрачного проксирования;

ssl_bumpserver-firstall – режим для установки соединения сначала с веб-сервером, затем SSL-соединения с клиентом, используя сопоставленный сертификат сервера, при этом работает как с запросами CONNECT, так и с перехваченными SSL-соединениями, но не позволяют принимать решения на основе информации о подтверждении SSL;

ssl_bumppeek-and-splice – режим предоставляет клиенту право решить, следует ли прервать или связать соединение на основе клиент-к-squid и сервер-к-squid SSL-приветствия;

ssl_bumpnoneall – режим позволяет получить туннель TCP без дешифрования прокси-трафика.

Для выбранной нами схемы работы из всех вышеперечисленных режимов необходимо установить в конфигурационном файле только один режим:

ssl_bump server-first all

На этом настройка конфигурации Squid завершена.

Шаг 6. Работа с сертификатами.

Сначала создадим корневой сертификат прокси-сервера, который будет использоваться для создания динамических сертификатов веб-сайтов.

#cd /opt/squid/etc/

#openssl req -new -newkey rsa:1024 -days 365 -nodes -x509 -keyoutPCA.pem -out PCA.pem

Подготавливаем кэширование сертификатов:

#mkdir /opt/squid/var/lib/

#opt/squid/libexec/ssl_crtd -c -s /opt/squid/var/lib/ssl_db

#chown -R nobody /opt/squid/var/lib/ssl_db

Следует отметить, что в случае замены корневого сертификат необходимо полностью очистить каталог /opt/squid/var/lib/ssl_db и заново инициализировать базу данных сертификатов.

Так как файл PCA.pem содержит закрытый ключ, устанавливаем доступ только для суперпользователя:

#chmod 400 PCA.pem

Теперь нужно изготовить сертификат для установки на клиентские станции и браузеры:

#cd /opt/squid/etc

#openssl x509 -in PCA.pem -outform DER -out PCA.der

Полученный файл PCA.der содержит необходимый сертификат.

Шаг 7. Инициализация и запуск прокси-сервера.

Необходимо назначить права и инициализировать прокси-сервер:

#chown -R nobody /opt/squid/var/logs

#/opt/squid/sbin/squid -z

Запустим прокси-сервер:

#/opt/squid/sbin/squid start

Проверим запуск режима ssl-bump:

#nano /opt/squid/var/logs/cache.log

Если нет ошибок и имеется строка

“AcceptingSSLbumpedHTTPSocketconnectionsatlocal=[::]:3128 remote=[::] FD 21 flags=9”,

то прокси-сервер в режим essl-bump запущен.

Как отмечалось выше, заметная часть вопросов связана с тем, что установленный Squid «не слушается» команд, привычных для администраторов ИТ, по работе со Squid, установленном из репозитория. Например, при попытке выполнить команду

#servicesquidrestart

результат – ошибка: «unrecognized service». Для того чтобы Squid начал работать как служба, необходимо поместить в каталог /etc/init.d/ скрипт запуска от Squid, установленного из репозитория, и редактировать его

#nano/etc/init.d/squid

заменить стандартные пути в заголовке скрипта на:

DAEMON=/opt/squid/sbin/squid

PIDFILE=/opt/squid/var/run/$NAME.pid

CONFIG=/opt/squid/etc/squid.conf

и по всему тексту скрипта:

run_dir=/opt/squid/var/run/squid

Сделать файл скрипта исполняемым:

#pushd/etc/init.d

#chmod +x squid

Добавим скрипт во все уровни автозапуска запуска:

 # update-rc.d squid start 99 2 3 4 5 .stop 01 0 1 6.

Перегружаем операционную систему и проверяем, сработала ли автозагрузка Squid, а также настройки сервиса подобной работы Squid:

#servicesquidstatus

результат выполнения команды должен быть:

**squidisrunning*

Выполнив вышеуказанные действия, вы получите Squid, подготовленный для установки средств антивирусной защиты и анализаторов трафика.

Далее рекомендуем установить пакеты из официального репозитория:

– для лучшего управление процессом фильтрации SquidGuard;

– для анализа лог-файлов SARG (Squid Analysis Report Generator) [7];

– для быстрого просмотра запрашиваемых соединений Squidview (необходимо изменить путь, по умолчанию выполнив команду *#ln -s /opt/squid/var/logs/ /var/log/squid*);

– средства антивирусной защиты «Dr.Web для Интернет-шлюзов Unix» или «Антивирус Касперского 5.5 для ProxyServer», в крайнем случае бесплатный Clam AntiVirus.

Установка и эффективная работа этих средств обеспечена предварительной настройкой специального режима Squid (ssl-bump).

Таким образом, в статье показано, что:

1. Специальный режим Squid (ssl-bump) – единственный способ полной проверки HTTPS трафика.

2. Ввод в эксплуатацию специального режима Squid (ssl-bump) должен сопровождаться такими же организационно-правовыми мероприятиями, как и ввод в эксплуатацию DLP-систем.

3. Администратор ИТ с низким уровнем подготовки способен самостоятельно установить и настроить специальный режим Squid (ssl-bump), провести подготовку прокси-сервера для установки антивирусной защиты и анализаторов трафика.

Примечания:

1. Киздермишов А.А., Киздермишова С.Х. К вопросу о вводе в эксплуатацию DLP-систем // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2017. Вып. 3. С 128–133. URL: http://vestnik.adygnet.ru
2. Материалы сайта HTTPS это зло: обратная сторона шифрования // Хакер: журнал. 2011. № 3. URL: https://xakep.ru/2011/03/28/55161
3. Официальный сайт разработчика Squid. URL: http://www.squid-cache.org
4. Киздермишов А.А. Защита персональных данных при их обработке посредством информационно-телекоммуникационной сети «Интернет» // Вестник Адыгейского государственного университета. Сер. Естественно-математические и технические науки. 2015. № 4 (171). С. 139–143. URL: http://vestnik.adygnet.ru
5. Хабрахабр. Squid3 в режиме SSLBump с динамической генерацией сертификатов. URL: https://habrahabr.ru/post/168515
6. Linux по-русски: виртуальная энциклопедия. Сертификаты Certificate Authority. URL: http://rus-linux.net/nlib.php?name=/MyLDP/BOOKS/BLFS-ru/blfs-ru-04-18.html
7. IT-блог Жаконды. Анализируем трафик Squid с помощью Sarg. URL: http://jakondo.ru/analiziruem-trafik-squid-s-pomoshhyu-sarg/

References:

1. Kizdermishov AA, Kizdermishova S.Kh. On the issue of the commissioning of DLP-systems // Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2017. Iss. 3. P. 128–133. URL: http://vestnik.adygnet.ru
2. HTTPS site materials are evil: the reverse side of encryption // Hacker: a journal. 2011. [Electronic resource]. URL: https://xakep.ru/2011/03/28/55161
3. Official website of the Squid developer. [Electronic resource]. URL: http://www.squid-cache.org
4. Kizdermishov A.A. Protection of personal information at its processing by means of the Internet telecommunication network // Bulletin of the Adyghe State University. Ser. Natural-Mathematical and Technical Sciences. 2015. Iss. 4 (171). P. 139–143. URL: http://vestnik.adygnet.ru
5. Habrahabr. Squid3 in SSLBump mode with dynamic generation of certificates. [Electronic resource]. URL: https://habrahabr.ru/post/168515
6. Russian Linux: a virtual encyclopedia. Certificate Authority. [Electronic resource]. URL: http://rus-linux.net/nlib.php?name=/MyLDP/BOOKS/BLFS-en/blfs-en-04-18.html
7. IT-blog of Jaconda. Let's analyze Squid traffic by means of Sarg. [Electronic resource]. URL: http://jakondo.ru/analiziruem-trafik-squid-s-pomoshhyu-sarg/