УДК 004.732

РАЗРАБОТКА КОМПЛЕКСА МЕРОПРИЯТИЙ ДЛЯ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ SSL-СЕРВЕРА

А.С. ЗАЙЦЕВ, О.Н. КОРОТЧЕНЯ, В.Ю. ЦВЕТКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 29 ноября 2017

Статья посвящена разработке технического комплекса мероприятий для обеспечения защиты от атак SSL-сервера в банковских сетях. Описаны основные технические средства, методики и протоколы для создания защиты SSL-сервера.

Ключевые слова: сеть передачи данных, протокол, SSL-сервер, SSL-сертификат, TLS, TACAS+, RADIUS, SNMP.

Введение

На сегодняшний день одним из самых простых и популярных способов установления безопасной сессии является использование протокола SSL.

Техническая реализация SSL протокола основана на использовании SSL-сервера (рис. 1). Актуальность темы по обеспечению защиты SSL-сервера обусловлена необходимостью совершенствования методов и средств защиты информации, применяемых в системах дистанционного банковского обслуживания.

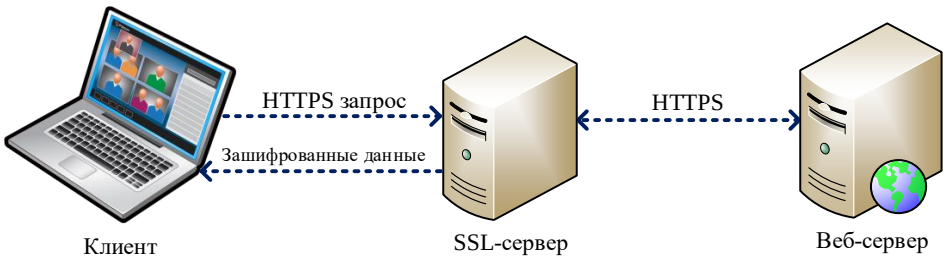

Рис. 1. Установление защищенного SSL соединения с помощью Веб-сервера

Помимо построения защищенного контура необходимо предпринимать ряд мер превентивного или проактивного характера для того, чтобы снизить риски.

Мероприятия, направленные на защиту сервера от атак, условно можно разделить на организационные и технические.

Организационные мероприятия включают в себя физическую защиту серверов: все оборудование должно находиться в специально оборудованных серверных комнатах с ограниченным доступом лиц.

Технические мероприятия защиты SSL-сервера на сетевом уровне

SSL-сервера должны представлять собой отказоустойчивую систему. Это можно достигнуть путем использования протокола VRRP (Virtual Router Redundancy Protocol). В рамках данного протокола используется понятие «виртуальный IP-адрес», который назначается на VRRP-группу. POS-терминалы подключаются на виртуальный IP-адрес. С помощью параметра

«Приоритет» назначается роль каждого из серверов в этой группе (Active, Standby). При доступности Active-устройства виртуальный IP-адрес «размещается» на нем. В случае неисправности Active-устройства виртуальный адрес «переходит» на Standby-устройство. Этот процесс занимает не более 1–2 с [1].

К основным мероприятиям защиты SSL-сервера при сетевых атаках можно отнести следующие.

1. Настройка безопасного метода аутентификации. Для реализации парольных политик и настройки аутентификации можно использовать как локальную базу, так и внешние серверы, например, TACAS+, RADIUS, LDAP, NTLM. Локальная база не поддерживает большое количество пользователей, а также не поддерживает некоторые сервисы по авторизации и аудиту, в связи с чем рекомендуется использование внешнего сервера.

На предприятии рекомендуется использовать централизованное управление доступом (centralized access control administration), которое предоставляет последовательные и унифицированные методы управления правами доступа пользователей и обеспечивает строгий контроль данных.

В качестве метода аутентификации необходимо выбрать аутентификацию с использованием RADIUS-сервера (рис. 2).

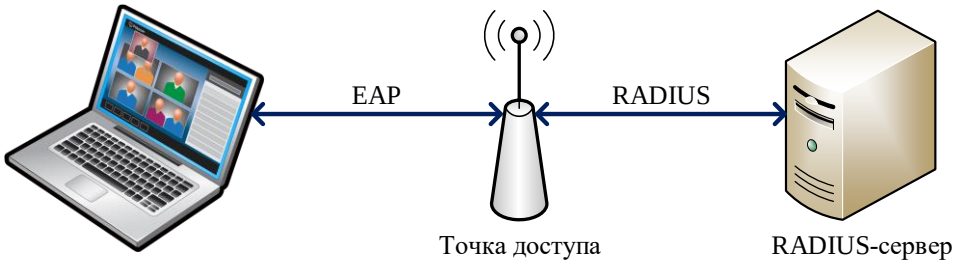

Рис. 2. Использование RADIUS-сервера для аутентификации

RADIUS (remote authentication dial-in user service) – это сетевой протокол, который обеспечивает клиент-серверную аутентификацию, авторизацию и аудит удаленных пользователей. Сервер доступа запрашивает у пользователя учетные данные для входа и передает их на RADIUS-сервер, на котором хранятся имена пользователей и пароли. При этом удаленный пользователь является клиентом сервера доступа, а сервер доступа является клиентом RADIUS-сервера. RADIUS позволяет компаниям хранить профили пользователей в централизованной базе данных. После успешной аутентификации пользователю присваивается предварительно настроенный профиль, определяющий, к каким ресурсам он может получить доступ. Эта технология позволяет компании иметь единую управляемую точку входа, что обеспечивает стандартизацию и предоставляет простой способ контроля использования удаленного доступа и сбора сетевой статистики.

При недоступности RADIUS-сервера будет использоваться локальная таблица пользователей. В данной таблице необходимо задать единственного пользователя с доступом READ-WRITE. Учетная запись этого пользователя должна храниться в службе безопасности предприятия. Учетную запись, используемую по умолчанию вендором, необходимо удалить.

В качестве RADIUS-сервера рекомендуется использовать сервер контроля доступа Cisco Secure ACS. Для пользователей, аутентифицированных RADIUS-сервером, необходимо использовать доменную парольную политику.

2. Настройка SNMP (Simple Network Management Protocol) – протокола, который используется для управления сетевыми устройствами. С помощью него программное обеспечение для управления сетевыми устройствами может получать доступ к информации, которая хранится на управляемых устройствах, в базе данных, которая называется MIB (рис. 3).

Устройство поддерживают первую, вторую и третью версии протокола. Наиболее безопасной является третья версия.

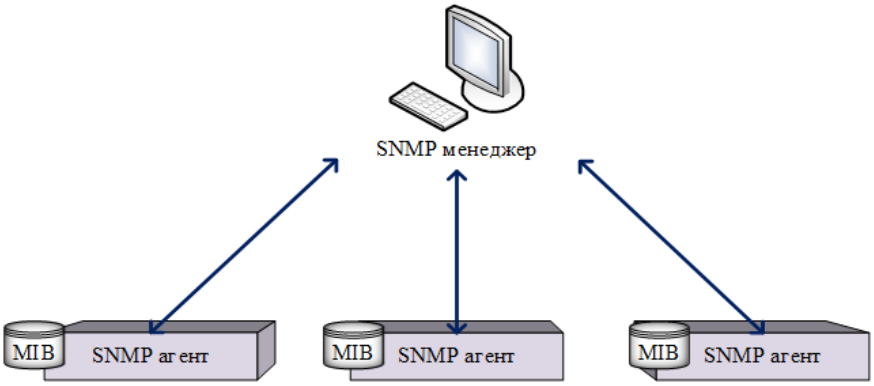

Рис. 3. Управление сетевыми устройствами с помощью SNMP

3. Использование двусторонней аутентификации для финансовых транзакций. Чтобы обеспечить целостность (защиту от фальсификации) и конфиденциальность, необходимо проводить аунтефикацию объектов, а также обеспечивать надежность. Аутентификация помогает установить доверие между сторонами при проведении любых видов транзакций. Обеспечение надежности заключается в предотвращении следующих явлений: «Спуфинг» (имитация соединения), несанкционированные действия, фальсификация данных [2].

Содержание транзакции может быть перехвачено и злонамеренно либо случайно изменено в процессе передачи. Сведения, составляющие имена пользователей, номера кредитных карт и финансовую информацию, передаваемые в виде «открытого текста», слишком уязвимы для вмешательства со стороны.

Необходимо настраивать двустороннюю аутентификацию для финансовых транзакций (рис. 4). Проверку должен пройти не только SSL-сервер, но и терминальное оборудование (на данном этапе в работу вступают загруженные сертификаты на терминалы). Данная настройка проводится путем конфигурации Client Authentication Policies для туннелей, предназначенных для финансовых транзакций.

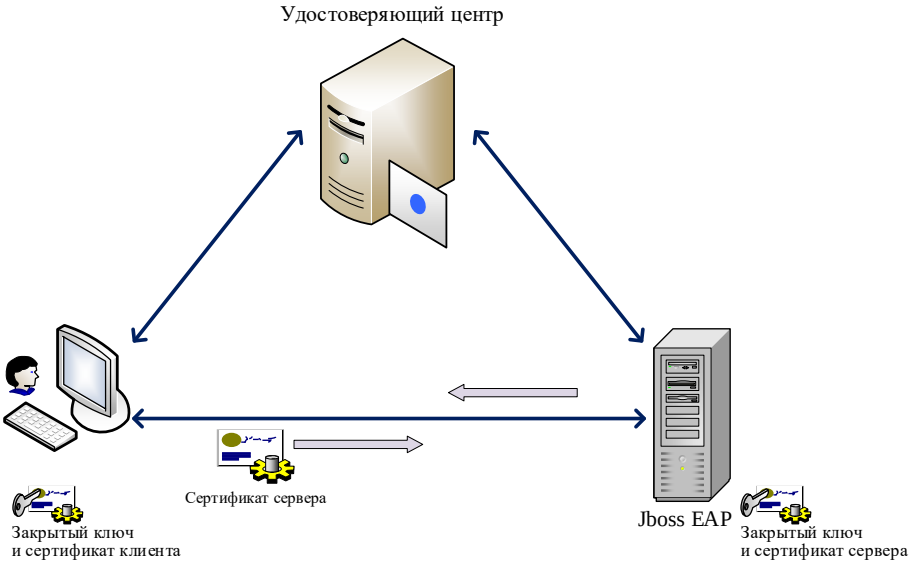

Рис. 4. Двусторонняя аутентификации с использование удостоверяющего центра

4. Создание и загрузка сертификатов. Первоначальным этапом должна выступать подготовка терминального оборудования. В зависимости от используемого банка-эквайера на терминалы должны быть загружены конфигурационный профайл и клиентский сертификат [3].

Первоначально администратору SSL-сервера необходимо сгенерировать запрос на подписание сертификата, который передается в отдел информационной безопасности для подписания (рис. 5). При генерации запроса необходимо установить максимальную длину ключа. В зависимости от модели терминала запросы для него должны подписываться отделом

информационной безопасности либо различными партнерами-интеграторами. Далее после подписания запроса сертификат загружается администратором обратно на сервер.

Рис. 5. Пример генерации запроса нового сертификата

Технические мероприятия защиты SSL-сервера на системном уровне

Управление уязвимостями играет важную роль в процессе управления (обеспечения) безопасностью предприятия. Эксплуатация уязвимостей хакером может привести к несанкционированному доступу в сеть, раскрытию или краже конфиденциальной информации, нарушению требований законов и регуляторов, прерыванию бизнес-операций. Новые уязвимости появляются каждый день из-за недостатков в программном обеспечении, неправильной конфигурации приложений. Среди них могут быть выделены следующие.

1. Проверка информации о доступных обновлениях ПО. Для поддержания серверной платформы в актуальном состоянии, устранения выявленных ошибок и обеспечения требований безопасности необходимо своевременно производить обновление программного обеспечения [4].

Информацию о новых версиях ПО следует регулярно просматривать на сайте производителя серверного оборудования.

2. Разнесение оборудования по разным серверным площадям. Это позволит серверу всегда оставаться доступным, благодаря наличию возможности перехода на резерв.

3. Систематическое сканирование серверов для обнаружения уязвимостей/вирусов.

Интеллектуальный сканнер способен выявить максимальное количество уязвимостей в информационной системе до того, как они будут обнаружены и использованы злоумышленниками (рис. 6). Регулярное автоматическое сканирование требует минимального вмешательства специалиста.

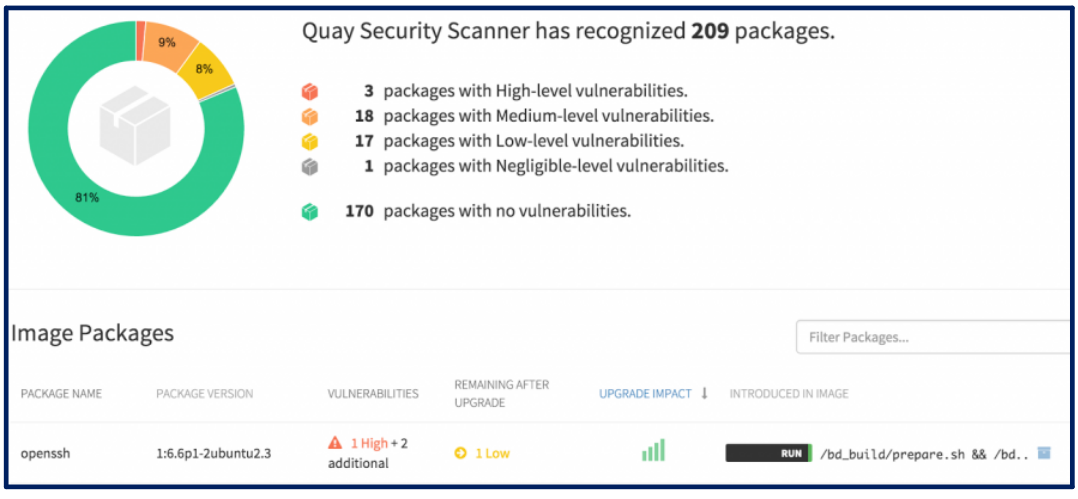

Рис. 6. Сканер уязвимостей сервера

4. Настройка аудита. Syslog (system log – системный журнал) – стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), работающих по протоколу IP.

Необходимо настроить syslog на систему мониторинга и анализа данных предприятия, также E-mail оповещения и смс-рассылку (рис. 7). Оповещение будет приходить на почту администраторов, заведенных в таблице пользователей.

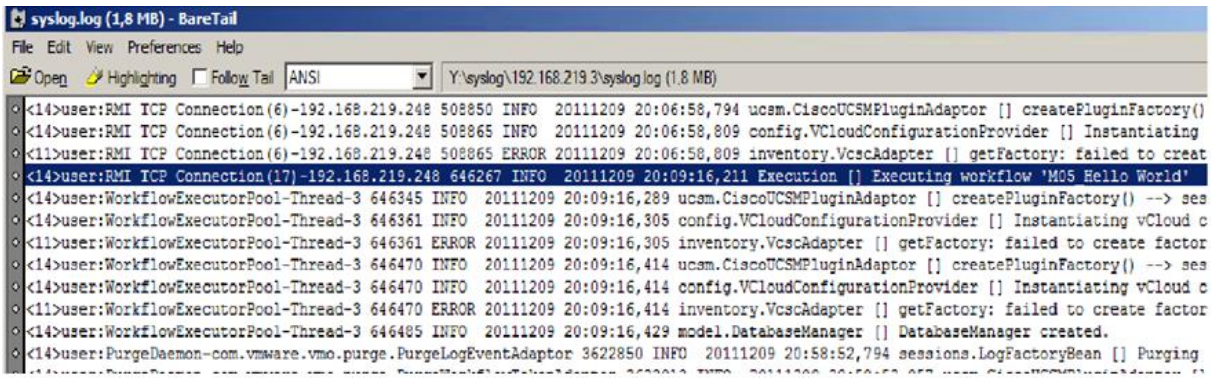

Рис. 7. Syslog-сервер на базе Windows

5. Хранение резервных копий конфигураций. Необходимо делать копии системы после внесения каждого изменения в конфигурацию сервера. Файлы конфигураций загружаются администратором серверов на сервера резервного хранения, что позволит в экстренных ситуациях «откатиться» до нужной конфигурации системы.

Заключение

Разработаны основные принципы организации защищенного подключения с помощью SSL протокола. Использование этих принципов позволит не только снизить риски и защитить сервер от атак, но и поддерживать в актуальном состоянии всю систему процессинга, а также обеспечить отказоустойчивость системы.

DEVELOPMENT OF THE COMPLEX OF ACTIVITIES FOR PROTECTION OF SSL-SERVER

A.S. ZAITSEV, O.N. KOROTCHENJA, V.Yu. TSVIATKOU

Abstract

The article is devoted to the development of a technical complex to protect the SSL server in banking networks from attacks. The main technical means, methods and protocols for creating SSL server security are described.

Keywords: data network, protocol, SSL-server, SSL-certificate, TLS, TACAS+, RADIUS, SNMP.

Список литературы

1. *Смелянский Р.Л.* Компьютерные сети. М., 2011.
2. Уязвимость SSL протокола. [Электронный ресурс]. – Режим доступа: www.sciencedirect.com/science/article/pii/S0167404802003127.
3. Уязвимость криптографического протокола SSLv3 «Poodle». [Электронный ресурс]. – Режим доступа: http://www.pwc.ru/ru/blogs/ekaterina_starostina/posts/9thpost.html.
4. Исследователями обнаружена новая атака, нацеленная на SSL/TLS. [Электронный ресурс]. – Режим доступа: http://www.ssl.ua/news/security-researchers-to-present-new-crime-attack.